



# مرکز تخصصی آپا دانشگاه کردستان

## معرفی مولفه‌ها و ابزارهای ممیزی

---

هادی گلباگی

۱۳۹۷/۱/۲۱



[www.cert.uok.ac.ir](http://www.cert.uok.ac.ir)



[apa@uok.ac.ir](mailto:apa@uok.ac.ir)



087-33662932



## فهرست مطالب

۲ .....	بخش اول : ممیزی، مولفه‌های ممیزی و کار با ابزار Audit Policies
۶ .....	ابزار ممیزی
۷ .....	انجام ممیزی با Audit Policies
۷ .....	Audit account logon events
۱۱ .....	Account Management
۱۶ .....	Detailed Tracking
۱۸ .....	DS Access
۲۱ .....	Logon/Logoff
۲۶ .....	Object Access
۳۴ .....	Policy Change
۳۸ .....	Privilege Us
۳۹ .....	System Audit
۴۱ .....	Global Object Access Auditing
۴۲ .....	بخش دوم : معرفی دیگر ابزارها
۴۲ .....	بازرس سیستم ( ESET SysInspector)
۴۴ .....	Microsoft Baseline Security Analyzer
۴۶ .....	مجموعه ابزار Windows Sysinternals Suite

## بخش اول : ممیزی، مولفه‌های ممیزی و کار با ابزار Audit Policies

### ❖ تعریفی از عملیات ممیزی

عملیات ممیزی<sup>۱</sup> یا حسابرسی امنیتی سیستم یا برنامه کاربردی، یک ارزیابی فنی و قابل سنجش از سیستم است که برای مدیران IT و امنیت، بسیار اطلاعات مفیدی را استخراج می‌کند. در این ارزیابی هم می‌توان به اطلاعات کلی در مورد امنیت سیستم و هم با جزئیات دقیق گزارش‌گیری انجام گیرد. عملیات ممیزی هم به صورت دستی و هم به صورت خودکار قابل انجام است. سیستم‌هایی که عملیات ممیزی روی آن‌ها انجام می‌گیرند شامل رایانه‌های شخصی، سرورها، کامپیوترهای بزرگ، روترهای شبکه و سوئیچ‌ها خواهد بود. در بخش‌های بعد مولفه‌ها، ابزار و ابعاد مختلف عملیات ممیزی مورد بررسی قرار خواهند گرفت.

### ❖ پیکربندی سیاست‌های ممیزی

برنامه‌ریزی یکی از مهمترین مراحل در خصوص فرآیند ممیزی یا حسابرسی است. مدیران سیستم باید اهداف و محدوده را برای ممیزی تعیین کنند. فرآیند ممیزی برای سیستم سربار دارد بنابراین ممیزی کردن محدوده وسیعی از موارد را منجر می‌شود که ورود به سیستم‌های امنیتی و بزرگ دشوار گردد. قبل از ورود به ممیزی، باید یک سیاست ممیزی اتخاذ شود.

این سیاست‌گذاری در خصوص ممیزی، نوع، میزان رویدادها و محدوده آن‌ها را برای یک کاربر خاص و یا گروهی از کاربران تعیین می‌کنند. با این وجود باید کنترل خاصی بر تنظیم ممیزی انجام گیرد. اجرای ممیزی چندین مرحله دارد که در زیر توضیح داده شده‌اند.

۱. فعال کردن ممیزی بر روی کنترل‌کننده دامنه
۲. انتخاب اهداف و محدوده‌ها برای ممیزی و ایجاد یک لیست کنترل دسترسی در سیستم<sup>۲</sup> SACL برای اهداف تعیین شده
۳. پیکربندی لاگ<sup>۳</sup> رویدادها
۴. محافظت داده‌های ممیزی از دسترسی‌ها و تغییرات غیر مجاز
۵. بررسی و نگهداری لاگ ممیزی

سیاست‌گذاری ممیزی یک دسته‌بندی در خصوص رویدادهای مرتبط امنیتی است که باید حسابرسی شوند. وقتی که ویندوز ۲۰۰۰ برای اولین بار نصب شد، همه موارد بررسی ممیزی غیرفعال می‌شوند. با فعال کردن دسته‌های مختلف رویدادهای ممیزی، مدیر سیستم می‌تواند یک سیاست‌گذاری که نیازهای سازمان را برآورده کند را مدنظر قرار دهد.

<sup>1</sup> Audit

<sup>2</sup> system access control lists

<sup>3</sup> Log

## ❖ مولفه‌های ممیزی

می‌توان دسته‌بندی‌ها و موارد زیادی را در زیرمجموعه مولفه‌های ممیزی در نظر گرفت اما در قالب یک دسته‌بندی کلی و استاندارد موارد زیر را می‌توان نام برد که در ادامه هر کدام به طور مفصل توضیح داده خواهند شد و جزئیات هر کدام مورد بررسی قرار می‌گیرند.

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

همچنین می‌توان مولفه‌ها را با جزئیات بیشتر و زیر مجموعه‌های آن‌ها نیز بیان کرد که به صورت زیر است.

### ➤ Account Logon

- Audit Credential Validation
- Audit Kerberos Authentication Service
- Audit Kerberos Service Ticket Operations
- Audit Other Logon/Logoff Events
- 

### ➤ Account Management

- Audit Application Group Management
- Audit Computer Account Management
- Audit Distribution Group Management
- Audit Other Account Management Events
- Audit Security Group Management
- Audit User Account Management
- 

### ➤ Detailed Tracking

- Audit DPAPI Activity
- Audit PNP activity
- Audit Process Creation
- Audit Process Termination
- Audit RPC Events

### ➤ **DS Access**

- **Audit Detailed Directory Service Replication**
- **Audit Directory Service Access**
- **Audit Directory Service Changes**
- **Audit Directory Service Replication**

### ➤ **Logon/Logoff**

- **Audit Account Lockout**
- **Audit User/Device Claims**
- **Audit IPsec Extended Mode**
- **Audit Group Membership**
- **Audit IPsec Main Mode**
- **Audit IPsec Quick Mode**
- **Audit Logoff**
- **Audit Logon**
- **Audit Network Policy Server**
- **Audit Other Logon/Logoff Events**
- **Audit Special Logon**

### ➤ **Object Access**

- **Audit Application Generated**
- **Audit Certification Services**
- **Audit Detailed File Share**
- **Audit File Share**
- **Audit File System**
- **Audit Filtering Platform Connection**
- **Audit Filtering Platform Packet Drop**
- **Audit Handle Manipulation**
- **Audit Kernel Object**
- **Audit Other Object Access Events**
- **Audit Registry**
- **Audit Removable Storage**
- **Audit SAM**
- **Audit Central Access Policy Staging**

### ➤ Policy Change

- Audit Policy Change
- Audit Authentication Policy Change
- Audit Authorization Policy Change
- Audit Filtering Platform Policy Change
- Audit MPSSVC Rule-Level Policy Change
- Audit Other Policy Change Events

### ➤ Privilege Use

- Audit Non-Sensitive Privilege Use
- Audit Sensitive Privilege Use
- Audit Other Privilege Use Events

### ➤ System

- Audit IPsec Driver
- Audit Other System Events
- Audit Security State Change
- Audit Security System Extension
- Audit System Integrity

### ➤ Global Object Access Auditing

- File System (Global Object Access Auditing)
- Registry (Global Object Access Auditing)

❖ بهترین روش برای ممیزی

برای به حداقل رساندن خطر چند تهدید امنیتی خاص، مدیر سیستم می تواند مراحل مختلف ممیزی را طی کند. مدیر سیستم می تواند رویدادها برای ممیزی را بر اساس مجموعه ای از تهدیدات خاص در محیط های متفاوت انتخاب کند. جدول زیر نمونه هایی از رویدادهای متفاوت است که می توان ممیزی کرد که تهدیدات امنیتی خاص را با استفاده از ممیزی رویدادها مانیتور می کند.

تهدیدات بالقوه	ممیزی رویداد
Random password hack	ممیزی در logon/logoff
Stolen password break-in	ممیزی در logon/logoff
Misuse of privileges	ممیزی در user and group management
Improper access to sensitive files	ممیزی در user and group management
Improper access to printers	ممیزی در file-access printers and object-access events
Virus outbreak	ممیزی در extensions program files EXE and .DLL

### ❖ فعال کردن ممیزی شی

اگر دسترسی ممیزی برای شی به عنوان بخشی از سیاست گذاری ممیزی انتخاب شده باشد یا سطح سرویس دایکتوری دسترسی (برای ممیزی شی بر روی دامنه کنترلی) و یا سطح دسترسی ممیزی شی (برای ممیزی شی برای سرور) باید فعال گردد. هنگامی که سطح دسترسی شی فعال شد، هر یک از ویژگی‌های شی برای ممیزی موفق یا غیر موفق برای درخواست دسترسی خاص در رده کاربر و یا گروهی را می‌توان استفاده کرد. ممیزی را می‌توان بر روی دامنه کنترلی به صورتی که در ادامه توضیح داده خواهد شد فعال کرد.

### ❖ ابزار ممیزی

این مرجع برای متخصصان حوزه IT اطلاعات وسیعی در مورد تنظیمات پیشرفته سیاست گذاری در خصوص ممیزی و رویدادهای ممیزی که در ویندوز موجود است را فراهم می‌کند.

- یکی از ابزار ممیزی Audit Policies که در خود سیستم عامل ویندوز موجود هستند. در بخش بعدی نیز سه ابزار دیگر به نام‌های ESET SysInspector، Microsoft Baseline Security Analyzer و Sysinternals Suite که برای ممیزی کاربرد دارند توضیح داده خواهند شد.

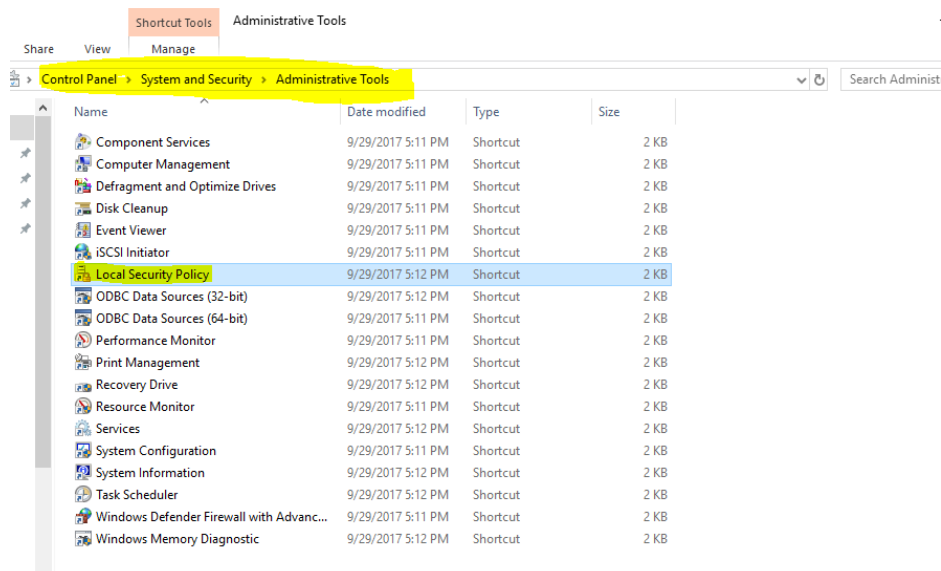
### ❖ نحوه اجرای Audit Policies :

ابتدا با مراجعه به آدرس زیر :

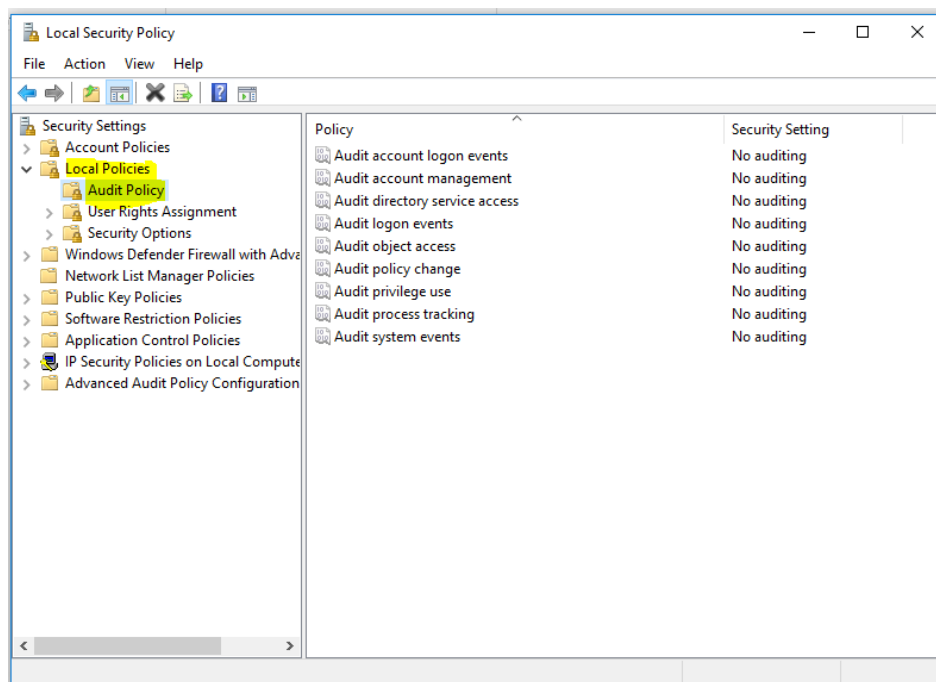
## Control Panel\System and Security\Administrative Tools

سپس کلیک بر روی :

### Local Security Policy



بعد از آن گزینه Local Policies و سپس Audit Policy را کلیک می کنیم.



همچنین اجرای پیشرفته مورد زیر مدنظر خواهد بود.



## Advanced security audit policy settings

❖ انجام ممیزی با Audit Policies :

### **Audit account logon events.۱**

پیکربندی تنظیمات سیاست گذاری در این دسته‌بندی می‌تواند برای به دست آوردن اطلاعات از کاربرهای معتبر بر روی دامنه کنترلی و یا در مدیریت امنیتی محلی اکانت (SAM) به ساده‌ترین شکل ممکن کمک کند. این تنظیم امنیتی نشان دهنده یک نمونه ممیزی از کنش‌های کاربر معتبر است که به سیستم وارد و یا خارج شده‌اند و رویداد ورود و خروج به سیستم ثبت می‌شود. بر خلاف تنظیمات سیاست‌های ورود و خروج و رویدادها که سعی در دسترسی به کامپیوترهای خاص دارند، این تنظیمات و رویدادها متمرکز بر بانک اطلاعاتی اکانت مورد استفاده هستند. این دسته شامل زیر مجموعه‌های زیر است :

- Audit Credential Validation
- Audit Kerberos Authentication Service
- Audit Kerberos Service Ticket Operations
- Audit Other Logon/Logoff Events

#### **Audit Credential Validation •**

تصدیق اعتبار ممیزی نشان می‌دهد که آیا سیستم عامل، رویداد ممیزی را برای تصدیق درخواست ورود به یک حساب کاربری فعال کرده است یا خیر. این رویداد بر روی یک سیستم معتبر شامل موارد حساب‌های روی دامنه، کنترل کننده دامنه معتبر، حساب‌های محلی و کامپیوترهای محلی معتبر خواهد بود. حجم رویدادها برای دامنه‌های کنترلی بسیار زیاد و برای سرورهای عضو و ایستگاه‌های کاری کم است. به این دلیل که حساب‌های بر روی دامنه بسیار بیشتر از حساب‌های محلی در محیط‌های سازمانی استفاده می‌شوند و بیشتر رویدادهای مربوط به ورود و خروج حساب‌ها در یک محیط سازمانی بر دامنه‌های کنترلی که اعتبارسنجی برای حساب‌های دامنه شده‌اند انجام می‌گیرد. نتایج مربوط به این بخش و اطلاعات در خصوص ممیزی در جدول زیر نشان داده شده است.

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	Yes	Yes	Yes	Expected volume of events is high for domain controllers, because this subcategory will generate events when an authentication attempt is made using any domain account and NTLM authentication. IF – We recommend Success auditing to keep track of domain-account authentication events using the NTLM protocol. Expect a high volume of events. For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections. Just collecting Success auditing events in this subcategory for future use in case of a security incident is not very useful, because events in this subcategory are not always informative. We recommend Failure auditing, to collect information about failed authentication attempts using domain accounts and the NTLM authentication protocol.
Member Server	Yes	Yes	Yes	Yes	Expected volume of events is low for member servers, because this subcategory will generate events when an authentication attempt is made using a local account, which should not happen too often. We recommend Success auditing, to keep track of authentication events by local accounts. We recommend Failure auditing, to collect information about failed authentication attempts by local accounts.
Workstation	Yes	Yes	Yes	Yes	Expected volume of events is low for workstations, because this subcategory will generate events when an authentication attempt is made using a local account, which should not happen too often. We recommend Success auditing, to keep track of authentication events by local accounts. We recommend Failure auditing, to collect information about failed authentication attempts by local accounts.

## Audit Kerberos Authentication Service •

این بخش شامل رویدادهای مربوط به TGT های صادر شده و درخواستهای TGT شکست خورده است. همچنین شامل رویدادهای تایید نشده از اعتبارسنجی که یا به دلیل رمزهای ورود اشتباه و یا رمزهای منقضی شده بوده‌اند است و دارای اطلاعات مفیدی در خصوص ممیزی می‌باشد که این اطلاعات به صورت جدول زیر است.

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	We recommend Success auditing, because you will see all Kerberos Authentication requests (TGT requests), which are a part of domain account logons. Also, you can see the IP address from which this account requested a TGT, when TGT was requested, which encryption type was used and so on. We recommend Failure auditing, because you will see all failed requests with wrong password, username, revoked certificate, and so on. You will also be able to detect Kerberos issues or possible attack attempts. Expected volume is high on domain controllers.
Member Server	No	No	No	No	This subcategory makes sense only on domain controllers.
Workstation	No	No	No	No	This subcategory makes sense only on domain controllers.

## • Audit Kerberos Service Ticket Operations

این بخش شامل رویدادهای امنیتی ممیزی از طرف سیستم عامل در خصوص service ticket requests است. رویدادها در هر زمانی برای یک کاربر معتبر که خواهان دسترسی به یک شبکه منبع محافظت شده باشد ثبت خواهند شد. حجم بالایی از اطلاعات بر روی سرورهای مرکزی توزیع شده خواهند بود. در جدول اطلاعاتی که برای ممیزی در گزارش نهایی خواهند بود ذکر شده است.

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	Yes	Yes	Yes	Expected volume is very high on domain controllers.  IF - We recommend Success auditing, because you will see all Kerberos Service Ticket requests (TGS requests), which are part of service use and access requests by specific accounts. Also, you can see the IP address from which this account requested TGS, when TGS was requested, which encryption type was used, and so on. For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections.  We recommend Failure auditing, because you will see all failed requests and be able to investigate the reason for failure. You will also be able to detect Kerberos issues or possible attack attempts.
Member Server	No	No	No	No	This subcategory makes sense only on domain controllers.
Workstation	No	No	No	No	This subcategory makes sense only on domain controllers.

## • ممیزی بر روی رویدادهای Logon/Logoff

اطلاعاتی را در خصوص ورود به حساب کاربری و خروج از آن نشان می دهد. این رویدادها شامل :

- وصل و یا قطع شدن از Remote desktop session
- قفل و یا باز شدن ایستگاه کاری
- فراخوانی یا رد شدن Screen saver
- حملات بازیابی شناسایی شده که می تواند شامل یک تهدید و یا وضعیت ناشی از یک خطای شبکه باشد.
- اعطای دسترسی به یک کاربر برای شبکه بی سیم که می تواند یک حساب کاربری و یا یک اکانت کامپیوتر باشد.
- اعطای دسترسی به یک کاربر برای شبکه کابلی که می تواند یک حساب کاربری و یا یک اکانت کامپیوتر باشد.

این رویداد در اصل برای بررسی کنش های یک کاربر و شناسایی حملات بالقوه مورد استفاده است و دارای حجم کاری کمی می باشد و گزارش این رویداد شامل موارد زیر است

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	We recommend Success auditing, to track possible Kerberos replay attacks, terminal session connect and disconnect actions, network authentication events, and some other events. Volume of these events is typically very low. Failure events will show you when requested credentials <a href="#">CredSSP</a> delegation was disallowed by policy. The volume of these events is very low—typically you will not get any of these events.
Member Server	Yes	Yes	Yes	Yes	We recommend Success auditing, to track possible terminal session connect and disconnect actions, network authentication events, and some other events. Volume of these events is typically very low. Failure events will show you when requested credentials <a href="#">CredSSP</a> delegation was disallowed by policy. The volume of these events is very low—typically you will not get any of these events.
Workstation	Yes	Yes	Yes	Yes	We recommend Success auditing, to track possible terminal session connect and disconnect actions, network authentication events, and some other events. Volume of these events is typically very low. Failure events will show you when requested credentials <a href="#">CredSSP</a> delegation was disallowed by policy. The volume of these events is very low—typically you will not get any of these events.

## Account Management.۲

تنظیمات سیاست‌گذاری امنیتی ممیزی در این بخش می‌تواند برای مانیتور تغییرات کاربر، اکانت‌های کامپیوتر و گروه‌ها استفاده شود. این بخش شامل زیر مجموعه‌های زیر است.

- Audit Application Group Management
- Audit Computer Account Management
- Audit Distribution Group Management
- Audit Other Account Management Events
- Audit Security Group Management
- Audit User Account Management

### • Audit Application Group Management

این بخش رویدادهایی در خصوص کنشهای برنامه‌ها در سطح گروه‌ها ثبت می‌کند که شامل ایجادهای گروهی، تغییرات، اضافه و یا حذف عضوها در گروه و دیگر فعالیت‌ها خواهد بود. برنامه‌های گروهی به وسیله مدیران اعتبارسنجی شده استفاده می‌شود و گزارش این رویداد شامل موارد زیر است.

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	-	-	-	-	This subcategory is outside the scope of this document.
Member Server	-	-	-	-	This subcategory is outside the scope of this document.
Workstation	-	-	-	-	This subcategory is outside the scope of this document.

### • Audit Computer Account Management

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	We recommend monitoring changes to critical computer objects in Active Directory, such as domain controllers, administrative workstations, and critical servers. It's especially important to be informed if any critical computer account objects are deleted. Additionally, events in this subcategory will give you information about who deleted, created, or modified a computer object, and when the action was taken. Typically volume of these events is low on domain controllers. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	No	No	No	No	This subcategory generates events only on domain controllers.
Workstation	No	No	No	No	This subcategory generates events only on domain controllers.

## Audit Distribution Group Management •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	No	IF	No	IF - Typically actions related to distribution groups have low security relevance, much more important to monitor Security Group changes. But if you want to monitor for critical distribution groups changes, such as member was added to internal critical distribution group (executives, administrative group, for example), you need to enable this subcategory for Success auditing. Typically volume of these events is low on domain controllers. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	No	No	No	No	This subcategory generates events only on domain controllers.
Workstation	No	No	No	No	This subcategory generates events only on domain controllers.

## Audit Other Account Management Events •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	The only reason to enable Success auditing on domain controllers is to monitor "4782(S): The password hash an account was accessed." This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	No	No	No	No	The only event which is generated on Member Servers is "4793(S): The Password Policy Checking API was called.", this event is a typical information event with little to no security relevance. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	No	No	No	No	The only event which is generated on Workstations is "4793(S): The Password Policy Checking API was called.", this event is a typical information event with little to no security relevance. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

## Audit Security Group Management •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	<p>We recommend Success auditing of security groups, to see new group creation events, changes and deletion of critical groups. Also you will get information about new members of security groups, when a member was removed from a group and when security group membership was enumerated.</p> <p>We recommend Failure auditing, to collect information about failed attempts to create, change, or delete new security groups.</p>
Member Server	Yes	No	Yes	No	<p>We recommend Success auditing of security groups, to see new group creation events, changes and deletion of critical groups. Also you will get information about new members of security groups, when a member was removed from a group and when security group membership was enumerated.</p> <p>We recommend Failure auditing, to collect information about failed attempts to create, change, or delete new security groups.</p>
Workstation	Yes	No	Yes	No	<p>We recommend Success auditing of security groups, to see new group creation events, changes and deletion of critical groups. Also you will get information about new members of security groups, when a member was removed from a group and when security group membership was enumerated.</p> <p>We recommend Failure auditing, to collect information about failed attempts to create, change, or delete new security groups.</p>

## Audit User Account Management •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	This subcategory contains many useful events for monitoring, especially for critical domain accounts, such as domain admins, service accounts, database admins, and so on. We recommend Failure auditing, mostly to see invalid password change and reset attempts for domain accounts, DSRM account password change failures, and failed SID History add attempts.
Member Server	Yes	Yes	Yes	Yes	We recommend monitoring all changes related to local user accounts, especially built-in local Administrator and other critical accounts. We recommend Failure auditing, mostly to see invalid password change and reset attempts for local accounts.
Workstation	Yes	Yes	Yes	Yes	We recommend monitoring all changes related to local user accounts, especially built-in local Administrator and other critical accounts. We recommend Failure auditing, mostly to see invalid password change and reset attempts for local accounts.

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	This subcategory contains many useful events for monitoring, especially for critical domain accounts, such as domain admins, service accounts, database admins, and so on. We recommend Failure auditing, mostly to see invalid password change and reset attempts for domain accounts, DSRM account password change failures, and failed SID History add attempts.
Member Server	Yes	Yes	Yes	Yes	We recommend monitoring all changes related to local user accounts, especially built-in local Administrator and other critical accounts. We recommend Failure auditing, mostly to see invalid password change and reset attempts for local accounts.
Workstation	Yes	Yes	Yes	Yes	We recommend monitoring all changes related to local user accounts, especially built-in local Administrator and other critical accounts. We recommend Failure auditing, mostly to see invalid password change and reset attempts for local accounts.



## Detailed Tracking.۳

### Audit DPAPI Activity •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	IF	IF	IF	IF – Events in this subcategory typically have an informational purpose and it is difficult to detect any malicious activity using these events. It's mainly used for DPAPI troubleshooting.
Member Server	IF	IF	IF	IF	IF – Events in this subcategory typically have an informational purpose and it is difficult to detect any malicious activity using these events. It's mainly used for DPAPI troubleshooting.
Workstation	IF	IF	IF	IF	IF – Events in this subcategory typically have an informational purpose and it is difficult to detect any malicious activity using these events. It's mainly used for DPAPI troubleshooting.

### Audit PNP Activity •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	This subcategory will help identify when and which Plug and Play device was attached, enabled, disabled or restricted by device installation policy. You can track, for example, whether a USB flash drive or stick was attached to a domain controller, which is typically not allowed. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	Yes	No	Yes	No	This subcategory will help identify when and which Plug and Play device was attached, enabled, disabled or restricted by device installation policy. You can track, for example, whether a USB flash drive or stick was attached to a critical server, which is typically not allowed. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	Yes	No	Yes	No	This subcategory will help identify when and which Plug and Play device was attached, enabled, disabled or restricted by device installation policy. You can track, for example, whether a USB flash drive or stick was attached to an administrative workstation or VIP workstation. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

## Audit Process Creation •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	It is typically useful to collect Success auditing information for this subcategory for forensic investigations, to find information who, when and with which options\parameters ran specific process. Additionally, you can analyse process creation events for elevated credentials use, potential malicious process names and so on. The event volume is typically medium-high level, depending on the process activity on the computer. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	Yes	No	Yes	No	It is typically useful to collect Success auditing information for this subcategory for forensic investigations, to find information who, when and with which options\parameters ran specific process. Additionally, you can analyse process creation events for elevated credentials use, potential malicious process names and so on. The event volume is typically medium-high level, depending on the process activity on the computer. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	Yes	No	Yes	No	It is typically useful to collect Success auditing information for this subcategory for forensic investigations, to find information who, when and with which options\parameters ran specific process. Additionally, you can analyse process creation events for elevated credentials use, potential malicious process names and so on. The event volume is typically medium-high level, depending on the process activity on the computer. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

## Audit Process Termination •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	No	IF	No	<p>IF - This subcategory typically is not as important as <a href="#">Audit Process Creation</a> subcategory. Using this subcategory you can, for example get information about for how long process was run in correlation with <a href="#">4688</a> event.</p> <p>If you have a list of critical processes that run on some computers, you can enable this subcategory to monitor for termination of these critical processes.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>
Member Server	No	No	IF	No	<p>IF - This subcategory typically is not as important as <a href="#">Audit Process Creation</a> subcategory. Using this subcategory you can, for example get information about for how long process was run in correlation with <a href="#">4688</a> event.</p> <p>If you have a list of critical processes that run on some computers, you can enable this subcategory to monitor for termination of these critical processes.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>
Workstation	No	No	IF	No	<p>IF - This subcategory typically is not as important as <a href="#">Audit Process Creation</a> subcategory. Using this subcategory you can, for example get information about for how long process was run in correlation with <a href="#">4688</a> event.</p> <p>If you have a list of critical processes that run on some computers, you can enable this subcategory to monitor for termination of these critical processes.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>

## Audit RPC Events •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	No	No	No	Events in this subcategory occur rarely.
Member Server	No	No	No	No	Events in this subcategory occur rarely.
Workstation	No	No	No	No	Events in this subcategory occur rarely.

## DS Access.۴

### Audit Detailed Directory Service Replication •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	No	IF	IF	IF - Events in this subcategory typically have an informational purpose and it is difficult to detect any malicious activity using these events. It's mainly used for Active Directory replication troubleshooting.
Member Server	No	No	No	No	This subcategory makes sense only on domain controllers.
Workstation	No	No	No	No	This subcategory makes sense only on domain controllers.

### Audit Directory Service Access •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	Yes	No	Yes	<p>It is better to track changes to Active Directory objects through the <a href="#">Audit Directory Service Changes</a> subcategory. However, <a href="#">Audit Directory Service Changes</a> doesn't give you information about failed access attempts, so we recommend Failure auditing in this subcategory to track failed access attempts to Active Directory objects.</p> <p>For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections. Also, develop an Active Directory auditing policy (<a href="#">SACL</a> design for specific classes, operation types which need to be monitored for specific Organizational Units, and so on) so you can audit only the access attempts that are made to specific important objects.</p>
Member Server	No	No	No	No	This subcategory makes sense only on domain controllers.
Workstation	No	No	No	No	This subcategory makes sense only on domain controllers.

## Audit Directory Service Changes •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	<p>It is important to track actions related to high value or critical Active Directory objects, for example, changes to <a href="#">AdminSDHolder</a> container or Domain Admins group objects.</p> <p>This subcategory shows you what actions were performed. If you want to track failed access attempts for Active Directory objects you need to take a look at <a href="#">Audit Directory Service Access</a> subcategory.</p> <p>For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections. Also, develop an Active Directory auditing policy (SACL design for specific classes, operation types which need to be monitored for specific Organizational Units, and so on) so you can audit only the access attempts that are made to specific important objects.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>
Member Server	No	No	No	No	This subcategory makes sense only on domain controllers.
Workstation	No	No	No	No	This subcategory makes sense only on domain controllers.

## Audit Directory Service Replication •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	No	IF	IF	IF - Events in this subcategory typically have an informational purpose and it is difficult to detect any malicious activity using these events. It's mainly used for Active Directory replication troubleshooting.
Member Server	No	No	No	No	This subcategory makes sense only on domain controllers.
Workstation	No	No	No	No	This subcategory makes sense only on domain controllers.

## Logon/Logoff.۵

### Audit Account Lockout •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	Yes	No	Yes	We recommend tracking account lockouts, especially for high value domain or local accounts (database administrators, built-in local administrator account, domain administrators, service accounts, domain controller accounts, and so on). This subcategory doesn't have Success events, so there is no recommendation to enable Success auditing for this subcategory.
Member Server	No	Yes	No	Yes	We recommend tracking account lockouts, especially for high value domain or local accounts (database administrators, built-in local administrator account, domain administrators, service accounts, domain controller accounts, and so on). This subcategory doesn't have Success events, so there is no recommendation to enable Success auditing for this subcategory.
Workstation	No	Yes	No	Yes	We recommend tracking account lockouts, especially for high value domain or local accounts (database administrators, built-in local administrator account, domain administrators, service accounts, domain controller accounts, and so on). This subcategory doesn't have Success events, so there is no recommendation to enable Success auditing for this subcategory.

### Audit User/Device Claims •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	No	IF	No	IF – if claims are in use in your organization and you need to monitor user/device claims, enable Success auditing for this subcategory. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	IF	No	IF	No	IF – if claims are in use in your organization and you need to monitor user/device claims, enable Success auditing for this subcategory. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	IF	No	IF	No	IF – if claims are in use in your organization and you need to monitor user/device claims, enable Success auditing for this subcategory. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

## Audit IPsec Extended Mode •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	IF	IF	IF	IF - This subcategory is mainly used for IPsec Extended Mode troubleshooting, or for tracing or monitoring IPsec Extended Mode operations.
Member Server	IF	IF	IF	IF	IF - This subcategory is mainly used for IPsec Extended Mode troubleshooting, or for tracing or monitoring IPsec Extended Mode operations.
Workstation	IF	IF	IF	IF	IF - This subcategory is mainly used for IPsec Extended Mode troubleshooting, or for tracing or monitoring IPsec Extended Mode operations.

## Audit Group Membership •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	Group membership information for logged in user can help to detect that member of specific domain or local group logged in to the machine (for example, member of database administrators, built-in local administrators, domain administrators, service accounts group or other high value groups). For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	Yes	No	Yes	No	Group membership information for logged in user can help to detect that member of specific domain or local group logged in to the machine (for example, member of database administrators, built-in local administrators, domain administrators, service accounts group or other high value groups). For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	Yes	No	Yes	No	Group membership information for logged in user can help to detect that member of specific domain or local group logged in to the machine (for example, member of database administrators, built-in local administrators, domain administrators, service accounts group or other high value groups). For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

## Audit IPsec Main Mode •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	IF	IF	IF	IF - This subcategory is mainly used for IPsec Main Mode troubleshooting, or for tracing or monitoring IPsec Main Mode operations.
Member Server	IF	IF	IF	IF	IF - This subcategory is mainly used for IPsec Main Mode troubleshooting, or for tracing or monitoring IPsec Main Mode operations.
Workstation	IF	IF	IF	IF	IF - This subcategory is mainly used for IPsec Main Mode troubleshooting, or for tracing or monitoring IPsec Main Mode operations.

## Audit IPsec Quick Mode •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	IF	IF	IF	IF - This subcategory is mainly used for IPsec Quick Mode troubleshooting, or for tracing or monitoring IPsec Quick Mode operations.
Member Server	IF	IF	IF	IF	IF - This subcategory is mainly used for IPsec Quick Mode troubleshooting, or for tracing or monitoring IPsec Quick Mode operations.
Workstation	IF	IF	IF	IF	IF - This subcategory is mainly used for IPsec Quick Mode troubleshooting, or for tracing or monitoring IPsec Quick Mode operations.



## Audit Logoff •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	No	Yes	No	<p>This subcategory typically generates huge amount of “4634(S): An account was logged off.” events which, typically has little security relevance. It is more important to audit Logon events using <a href="#">Audit Logon</a> subcategory, rather than Logoff events.</p> <p>Enable Success audit if you want to track, for example, for how long session was active (in correlation with <a href="#">Audit Logon</a> events) and when user actually logged off.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>
Member Server	No	No	Yes	No	<p>This subcategory typically generates huge amount of “4634(S): An account was logged off.” events which, typically has little security relevance. It is more important to audit Logon events using <a href="#">Audit Logon</a> subcategory, rather than Logoff events.</p> <p>Enable Success audit if you want to track, for example, for how long session was active (in correlation with <a href="#">Audit Logon</a> events) and when user actually logged off.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>
Workstation	No	No	Yes	No	<p>This subcategory typically generates huge amount of “4634(S): An account was logged off.” events which, typically has little security relevance. It is more important to audit Logon events using <a href="#">Audit Logon</a> subcategory, rather than Logoff events.</p> <p>Enable Success audit if you want to track, for example, for how long session was active (in correlation with <a href="#">Audit Logon</a> events) and when user actually logged off.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>

## Audit Logon •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	<p>Audit Logon events, for example, will give you information about which account, when, using which Logon Type, from which machine logged on to this machine.</p> <p>Failure events will show you failed logon attempts and the reason why these attempts failed.</p>
Member Server	Yes	Yes	Yes	Yes	<p>Audit Logon events, for example, will give you information about which account, when, using which Logon Type, from which machine logged on to this machine.</p> <p>Failure events will show you failed logon attempts and the reason why these attempts failed.</p>
Workstation	Yes	Yes	Yes	Yes	<p>Audit Logon events, for example, will give you information about which account, when, using which Logon Type, from which machine logged on to this machine.</p> <p>Failure events will show you failed logon attempts and the reason why these attempts failed.</p>

## Audit Network Policy Server •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	IF	IF	IF	IF – if a server has the <a href="#">Network Policy Server (NPS)</a> role installed and you need to monitor access requests and other NPS-related events, enable this subcategory.
Member Server	IF	IF	IF	IF	IF – if a server has the <a href="#">Network Policy Server (NPS)</a> role installed and you need to monitor access requests and other NPS-related events, enable this subcategory.
Workstation	No	No	No	No	<a href="#">Network Policy Server (NPS)</a> role cannot be installed on client OS.

## Audit Other Logon/Logoff Events •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	We recommend Success auditing, to track possible Kerberos replay attacks, terminal session connect and disconnect actions, network authentication events, and some other events. Volume of these events is typically very low. Failure events will show you when requested credentials <a href="#">CredSSP</a> delegation was disallowed by policy. The volume of these events is very low—typically you will not get any of these events.
Member Server	Yes	Yes	Yes	Yes	We recommend Success auditing, to track possible terminal session connect and disconnect actions, network authentication events, and some other events. Volume of these events is typically very low. Failure events will show you when requested credentials <a href="#">CredSSP</a> delegation was disallowed by policy. The volume of these events is very low—typically you will not get any of these events.
Workstation	Yes	Yes	Yes	Yes	We recommend Success auditing, to track possible terminal session connect and disconnect actions, network authentication events, and some other events. Volume of these events is typically very low. Failure events will show you when requested credentials <a href="#">CredSSP</a> delegation was disallowed by policy. The volume of these events is very low—typically you will not get any of these events.

## Audit Special Logon •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	<p>This subcategory is very important because of <a href="#">Special Groups</a> related events, you must enable this subcategory for Success audit if you use this feature.</p> <p>At the same time this subcategory allows you to track account logon sessions to which sensitive privileges were assigned.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>
Member Server	Yes	No	Yes	No	<p>This subcategory is very important because of <a href="#">Special Groups</a> related events, you must enable this subcategory for Success audit if you use this feature.</p> <p>At the same time this subcategory allows you to track account logon sessions to which sensitive privileges were assigned.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>
Workstation	Yes	No	Yes	No	<p>This subcategory is very important because of <a href="#">Special Groups</a> related events, you must enable this subcategory for Success audit if you use this feature.</p> <p>At the same time this subcategory allows you to track account logon sessions to which sensitive privileges were assigned.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>

## Object Access.۶

## Audit Application Generated •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	IF	IF	IF	<p>IF – if you use <a href="#">Authorization Manager</a> in your environment and you need to monitor events related to Authorization Manager <a href="#">applications</a>, enable this subcategory.</p>
Member Server	IF	IF	IF	IF	<p>IF – if you use <a href="#">Authorization Manager</a> in your environment and you need to monitor events related to Authorization Manager <a href="#">applications</a>, enable this subcategory.</p>
Workstation	IF	IF	IF	IF	<p>IF – if you use <a href="#">Authorization Manager</a> in your environment and you need to monitor events related to Authorization Manager <a href="#">applications</a>, enable this subcategory.</p>

## Audit Certification Services •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	IF	IF	IF	IF – if a server has the <a href="#">Active Directory Certificate Services</a> (AD CS) role installed and you need to monitor AD CS related events, enable this subcategory.
Member Server	IF	IF	IF	IF	IF – if a server has the <a href="#">Active Directory Certificate Services</a> (AD CS) role installed and you need to monitor AD CS related events, enable this subcategory.
Workstation	No	No	No	No	<a href="#">Active Directory Certificate Services</a> (AD CS) role cannot be installed on client OS.

## Audit Detailed File Share •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	Yes	No	Yes	Audit Success for this subcategory on domain controllers typically will lead to very high volume of events, especially for SYSVOL share. We recommend monitoring Failure access attempts: the volume should not be very high. You will be able to see who was not able to get access to a file or folder on a network share on a computer.
Member Server	IF	Yes	IF	Yes	IF – If a server has shared network folders which typically get many access requests (File Server, for example), the volume of events might be very high. If you really need to track all successful access events for every file or folder located on a shared folder, enable Success auditing or use the <a href="#">Audit File System</a> subcategory, although that subcategory excludes some information in Audit Detailed File Share, for example, the client's IP address. The volume of Failure events for member servers should not be very high (if they are not File Servers). With Failure auditing, you will be able to see who was not able to get access to a file or folder on a network share on this computer.
Workstation	IF	Yes	IF	Yes	IF – If a workstation has shared network folders which typically get many access requests, the volume of events might be very high. If you really need to track all successful access events for every file or folder located on a shared folder, enable Success auditing or use Audit File System subcategory, although that subcategory excludes some information in Audit Detailed File Share, for example, the client's IP address. The volume of Failure events for workstations should not be very high. With Failure auditing, you will be able to see who was not able to get access to a file or folder on a network share on this computer.

## Audit File Share •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	We recommend Success auditing for domain controllers, because it's important to track deletion, creation, and modification events for network shares. We recommend Failure auditing to track failed SMB SPN checks and failed access attempts to network shares.
Member Server	Yes	Yes	Yes	Yes	We recommend Success auditing to track deletion, creation, modification, and access attempts to network share objects. We recommend Failure auditing to track failed SMB SPN checks and failed access attempts to network shares.
Workstation	Yes	Yes	Yes	Yes	We recommend Success auditing to track deletion, creation, modification and access attempts to network share objects. We recommend Failure auditing to track failed SMB SPN checks and failed access attempts to network shares.

## Audit File System •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	IF	IF	IF	We strongly recommend that you develop a File System Security Monitoring policy and define appropriate <a href="#">SACLs</a> for file system objects for different operating system templates and roles. Do not enable this subcategory if you have not planned how to use and analyze the collected information. It is also important to delete non-effective, excess <a href="#">SACLs</a> . Otherwise the auditing log will be overloaded with useless information. Failure events can show you unsuccessful attempts to access specific file system objects. Consider enabling this subcategory for critical computers first, after you develop a File System Security Monitoring policy for them.
Member Server	IF	IF	IF	IF	
Workstation	IF	IF	IF	IF	

## Audit Filtering Platform Connection •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	Yes	IF	Yes	<p>Success auditing for this subcategory typically generates a very high volume of events, for example, one event for every connection that was made to the system. It is much more important to audit Failure events (blocked connections, for example). For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections.</p> <p>IF - Enable Success audit in case you need to monitor successful outbound or inbound connections to and from untrusted IP addresses on high value computers or devices.</p>
Member Server	No	Yes	IF	Yes	<p>Success auditing for this subcategory typically generates a very high volume of events, for example, one event for every connection that was made to the system. It is much more important to audit Failure events (blocked connections, for example). For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections.</p> <p>IF - Enable Success audit in case you need to monitor successful outbound or inbound connections to and from untrusted IP addresses on high value computers or devices.</p>
Workstation	No	Yes	IF	Yes	<p>Success auditing for this subcategory typically generates a very high volume of events, for example, one event for every connection that was made to the system. It is much more important to audit Failure events (blocked connections, for example). For recommendations for using and analyzing the collected information, see the <b>Security Monitoring Recommendations</b> sections.</p> <p>IF - Enable Success audit in case you need to monitor successful outbound or inbound connections to and from untrusted IP addresses on high value computers or devices.</p>

## Audit Filtering Platform Packet Drop •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	No	No	No	Failure events volume typically is very high for this subcategory and typically used for troubleshooting. If you need to monitor blocked connections, it is better to use "5157(F): The Windows Filtering Platform has blocked a connection," because it contains almost the same information and generates per-connection, not per-packet. There is no recommendation to enable Success auditing, because Success events in this subcategory rarely occur.
Member Server	No	No	No	No	Failure events volume typically is very high for this subcategory and typically used for troubleshooting. If you need to monitor blocked connections, it is better to use "5157(F): The Windows Filtering Platform has blocked a connection," because it contains almost the same information and generates per-connection, not per-packet. There is no recommendation to enable Success auditing, because Success events in this subcategory rarely occur.
Workstation	No	No	No	No	Failure events volume typically is very high for this subcategory and typically used for troubleshooting. If you need to monitor blocked connections, it is better to use "5157(F): The Windows Filtering Platform has blocked a connection," because it contains almost the same information and generates per-connection, not per-packet. There is no recommendation to enable Success auditing, because Success events in this subcategory rarely occur.

## Audit Handle Manipulation •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	No	No	No	Typically, information about the duplication or closing of an object handle has little to no security relevance and is hard to parse or analyze. There is no recommendation to enable this subcategory for Success or Failure auditing, unless you know exactly what you need to monitor in Object's Handles level.
Member Server	No	No	No	No	Typically, information about the duplication or closing of an object handle has little to no security relevance and is hard to parse or analyze. There is no recommendation to enable this subcategory for Success or Failure auditing, unless you know exactly what you need to monitor in Object's Handles level.
Workstation	No	No	No	No	Typically, information about the duplication or closing of an object handle has little to no security relevance and is hard to parse or analyze. There is no recommendation to enable this subcategory for Success or Failure auditing, unless you know exactly what you need to monitor in Object's Handles level.

## Audit Kernel Object •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	No	No	No	Typically Kernel object auditing events have little to no security relevance and are hard to parse or analyze. Also, the volume of these events is typically very high. There is no recommendation to enable this subcategory, unless you know exactly what you need to monitor at the Kernel objects level.
Member Server	No	No	No	No	Typically Kernel object auditing events have little to no security relevance and are hard to parse or analyze. Also, the volume of these events is typically very high. There is no recommendation to enable this subcategory, unless you know exactly what you need to monitor at the Kernel objects level.
Workstation	No	No	No	No	Typically Kernel object auditing events have little to no security relevance and are hard to parse or analyze. Also, the volume of these events is typically very high. There is no recommendation to enable this subcategory, unless you know exactly what you need to monitor at the Kernel objects level.

## Audit Other Object Access Events •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	We recommend Success auditing first of all because of scheduled tasks events. We recommend Failure auditing to get events about possible ICMP DoS attack.
Member Server	Yes	Yes	Yes	Yes	We recommend Success auditing first of all because of scheduled tasks events. We recommend Failure auditing to get events about possible ICMP DoS attack.
Workstation	Yes	Yes	Yes	Yes	We recommend Success auditing first of all because of scheduled tasks events. We recommend Failure auditing to get events about possible ICMP DoS attack.



## Audit Registry •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	IF	IF	IF	We strongly recommend that you develop a Registry Objects Security Monitoring policy and define appropriate <a href="#">SACLs</a> for registry objects for different operating system templates and roles. Do not enable this subcategory if you have not planned how to use and analyze the collected information. It is also important to delete non-effective, excess <a href="#">SACLs</a> . Otherwise the auditing log will be overloaded with useless information. Failure events can show you unsuccessful attempts to access specific registry objects. Consider enabling this subcategory for critical computers first, after you develop a Registry Objects Security Monitoring policy for them.
Member Server	IF	IF	IF	IF	
Workstation	IF	IF	IF	IF	

## Audit Removable Storage •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	This subcategory will help identify when and which files or folders were accessed or modified on removable devices. It is often useful to track actions with removable storage devices and the files or folders on them, because malicious software very often uses removable devices as a method to get into the system. At the same time, you will be able to track which files were written or executed from a removable storage device. You can track, for example, actions with files or folders on USB flash drives or sticks that were inserted into domain controllers or high value servers, which is typically not allowed. We recommend Failure auditing to track failed access attempts.
Member Server	Yes	Yes	Yes	Yes	
Workstation	Yes	Yes	Yes	Yes	

## Audit SAM •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	-	-	-	-	There is no recommendation for this subcategory in this document, unless you know exactly what you need to monitor at <a href="#">Security Account Manager</a> level.
Member Server	-	-	-	-	There is no recommendation for this subcategory in this document, unless you know exactly what you need to monitor at <a href="#">Security Account Manager</a> level.
Workstation	-	-	-	-	There is no recommendation for this subcategory in this document, unless you know exactly what you need to monitor at <a href="#">Security Account Manager</a> level.

## Audit Central Access Policy Staging •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	No	IF	No	IF - Enable this subcategory if you need to test or troubleshoot Dynamic Access Control Proposed <a href="#">Central Access Policies</a> . This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	IF	No	IF	No	IF - Enable this subcategory if you need to test or troubleshoot Dynamic Access Control Proposed <a href="#">Central Access Policies</a> . This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	IF	No	IF	No	IF - Enable this subcategory if you need to test or troubleshoot Dynamic Access Control Proposed <a href="#">Central Access Policies</a> . This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

## Policy Change.۷

### Audit Policy Change •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	Almost all events in this subcategory have security relevance and should be monitored. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	Yes	No	Yes	No	Almost all events in this subcategory have security relevance and should be monitored. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	Yes	No	Yes	No	Almost all events in this subcategory have security relevance and should be monitored. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

### Audit Authentication Policy Change •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	On domain controllers, it is important to enable Success audit for this subcategory to be able to get information related to operations with domain and forest trusts, changes in Kerberos policy and some other events included in this subcategory. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	Yes	No	Yes	No	On member servers it is important to enable Success audit for this subcategory to be able to get information related to changes in user logon rights policies and password policy changes. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	Yes	No	Yes	No	On workstations it is important to enable Success audit for this subcategory to be able to get information related to changes in user logon rights policies and password policy changes. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

## Audit Authorization Policy Change •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	No	IF	No	<p>IF – With Success auditing for this subcategory, you can get information related to changes in user rights policies, or changes of resource attributes or Central Access Policy applied to file system objects.</p> <p>However, if you are using an application or system service that makes changes to system privileges through the AdjustPrivilegesToken API, we do not recommend Success auditing because of the high volume of event “4703(S): A user right was adjusted” that may be generated. As of Windows 10, event 4703 is generated by applications or services that dynamically adjust token privileges. An example of such an application is System Center Configuration Manager, which makes WMI queries at recurring intervals and quickly generates a large number of 4703 events (with the WMI activity listed as coming from <b>svchost.exe</b>).</p> <p>If one of your applications or services is generating a large number of 4703 events, you might find that your event-management software has filtering logic that can automatically discard the recurring events, which would make it easier to work with Success auditing for this category.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>
Member Server	IF	No	IF	No	<p>IF – With Success auditing for this subcategory, you can get information related to changes in user rights policies, or changes of resource attributes or Central Access Policy applied to file system objects.</p> <p>However, if you are using an application or system service that makes changes to system privileges through the AdjustPrivilegesToken API, we do not recommend Success auditing because of the high volume of event “4703(S): A user right was adjusted” that may be generated. As of Windows 10, event 4703 is generated by applications or services that dynamically adjust token privileges. An example of such an application is System Center Configuration Manager, which makes WMI queries at recurring intervals and quickly generates a large number of 4703 events (with the WMI activity listed as coming from <b>svchost.exe</b>).</p> <p>If one of your applications or services is generating a large number of 4703 events, you might find that your event-management software has filtering logic that can automatically discard the recurring events, which would make it easier to work with Success auditing for this category.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>
Workstation	IF	No	IF	No	<p>IF – With Success auditing for this subcategory, you can get information related to changes in user rights policies, or changes of resource attributes or Central Access Policy applied to file system objects.</p> <p>However, if you are using an application or system service that makes changes to system privileges through the AdjustPrivilegesToken API, we do not recommend Success auditing because of the high volume of event “4703(S): A user right was adjusted” that may be generated. As of Windows 10, event 4703 is generated by applications or services that dynamically adjust token privileges. An example of such an application is System Center Configuration Manager, which makes WMI queries at recurring intervals and quickly generates a large number of 4703 events (with the WMI activity listed as coming from <b>svchost.exe</b>).</p> <p>If one of your applications or services is generating a large number of 4703 events, you might find that your event-management software has filtering logic that can automatically discard the recurring events, which would make it easier to work with Success auditing for this category.</p> <p>This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.</p>

### Audit Filtering Platform Policy Change •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	-	-	-	-	This subcategory is outside the scope of this document.
Member Server	-	-	-	-	This subcategory is outside the scope of this document.
Workstation	-	-	-	-	This subcategory is outside the scope of this document.

### Audit MPSSVC Rule-Level Policy Change •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	Success events shows you changes in Windows Firewall rules and settings, active configuration and rules after Windows Firewall Service startup and default configuration restore actions. Failure events may help to identify configuration problems with Windows Firewall rules or settings.
Member Server	Yes	Yes	Yes	Yes	Success events shows you changes in Windows Firewall rules and settings, active configuration and rules after Windows Firewall Service startup and default configuration restore actions. Failure events may help to identify configuration problems with Windows Firewall rules or settings.
Workstation	Yes	Yes	Yes	Yes	Success events shows you changes in Windows Firewall rules and settings, active configuration and rules after Windows Firewall Service startup and default configuration restore actions. Failure events may help to identify configuration problems with Windows Firewall rules or settings.

## Audit Other Policy Change Events •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	IF	Yes	IF	Yes	<p>IF - We do not recommend Success auditing because of event "5447: A Windows Filtering Platform filter has been changed"—this event generates many times during group policy updates and typically is used for troubleshooting purposes for Windows Filtering Platform filters. But you would still need to enable Success auditing for this subcategory if, for example, you must monitor changes in Boot Configuration Data or Central Access Policies.</p> <p>We recommend Failure auditing, to detect errors in applied Security settings which came from Group Policy, and failure events related to Cryptographic Next Generation (CNG) functions.</p>
Member Server	IF	Yes	IF	Yes	<p>IF - We do not recommend Success auditing because of event "5447: A Windows Filtering Platform filter has been changed"—this event generates many times during group policy updates and typically is used for troubleshooting purposes for Windows Filtering Platform filters. But you would still need to enable Success auditing for this subcategory if, for example, you must monitor changes in Boot Configuration Data or Central Access Policies.</p> <p>We recommend Failure auditing, to detect errors in applied Security settings which came from Group Policy, and failure events related to Cryptographic Next Generation (CNG) functions.</p>
Workstation	IF	Yes	IF	Yes	<p>IF - We do not recommend Success auditing because of event "5447: A Windows Filtering Platform filter has been changed"—this event generates many times during group policy updates and typically is used for troubleshooting purposes for Windows Filtering Platform filters. But you would still need to enable Success auditing for this subcategory if, for example, you must monitor changes in Boot Configuration Data or Central Access Policies.</p>

## Privilege Us.۸

### Audit Non Sensitive Privilege Use •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	IF	No	IF	We do not recommend Success auditing because the volume of events is very high and typically they are not as important as events from <a href="#">Audit Sensitive Privilege Use</a> subcategory. IF – You can enable Failure auditing if you need information about failed attempts to use non-sensitive privileges, for example, <b>SeShutdownPrivilege</b> or <b>SeRemoteShutdownPrivilege</b> .
Member Server	No	IF	No	IF	We do not recommend Success auditing because the volume of events is very high and typically they are not as important as events from <a href="#">Audit Sensitive Privilege Use</a> subcategory. IF – You can enable Failure auditing if you need information about failed attempts to use non-sensitive privileges, for example, <b>SeShutdownPrivilege</b> or <b>SeRemoteShutdownPrivilege</b> .
Workstation	No	IF	No	IF	We do not recommend Success auditing because the volume of events is very high and typically they are not as important as events from <a href="#">Audit Sensitive Privilege Use</a> subcategory. IF – You can enable Failure auditing if you need information about failed attempts to use non-sensitive privileges, for example, <b>SeShutdownPrivilege</b> or <b>SeRemoteShutdownPrivilege</b> .

### Audit Sensitive Privilege Use •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	We recommend tracking Success and Failure for this subcategory of events, especially if the sensitive privileges were used by a user account.
Member Server	Yes	Yes	Yes	Yes	We recommend tracking Success and Failure for this subcategory of events, especially if the sensitive privileges were used by a user account.
Workstation	Yes	Yes	Yes	Yes	We recommend tracking Success and Failure for this subcategory of events, especially if the sensitive privileges were used by a user account.

## Audit Other Privilege Use Events •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	No	No	No	No	This auditing subcategory doesn't have any informative events inside.
Member Server	No	No	No	No	This auditing subcategory doesn't have any informative events inside.
Workstation	No	No	No	No	This auditing subcategory doesn't have any informative events inside.

## System Audit.۹

## Audit IPsec Driver •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	-	-	-	-	There is no recommendation for this subcategory in this document, unless you know exactly what you need to monitor at IPsec Driver level.
Member Server	-	-	-	-	There is no recommendation for this subcategory in this document, unless you know exactly what you need to monitor at IPsec Driver level.
Workstation	-	-	-	-	There is no recommendation for this subcategory in this document, unless you know exactly what you need to monitor at IPsec Driver level.

## Audit Other System Events •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	We recommend enabling Success and Failure auditing because you will be able to get Windows Firewall Service and Windows Firewall Driver status events.
Member Server	Yes	Yes	Yes	Yes	We recommend enabling Success and Failure auditing because you will be able to get Windows Firewall Service and Windows Firewall Driver status events.
Workstation	Yes	Yes	Yes	Yes	We recommend enabling Success and Failure auditing because you will be able to get Windows Firewall Service and Windows Firewall Driver status events.



## Audit Security State Change •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	The volume of events in this subcategory is very low and all of them are important events and have security relevance. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	Yes	No	Yes	No	The volume of events in this subcategory is very low and all of them are important events and have security relevance. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	Yes	No	Yes	No	The volume of events in this subcategory is very low and all of them are important events and have security relevance. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

## Audit Security System Extension •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	No	Yes	No	The main reason why we recommend Success auditing for this subcategory is "4697(S): A service was installed in the system." For other events we strongly recommend monitoring a whitelist of allowed security extensions (authenticated packages, logon processes, notification packages, and security packages). Otherwise it's hard to pull useful information from these events, except event 4611 which typically should have "SYSTEM" as value for "Subject" field. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Member Server	Yes	No	Yes	No	The main reason why we recommend Success auditing for this subcategory is "4697(S): A service was installed in the system." For other events we strongly recommend monitoring a whitelist of allowed security extensions (authenticated packages, logon processes, notification packages, and security packages). Otherwise it's hard to pull useful information from these events, except event 4611 which typically should display "SYSTEM" for the "Subject" field. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.
Workstation	Yes	No	Yes	No	The main reason why we recommend Success auditing for this subcategory is "4697(S): A service was installed in the system." For other events we strongly recommend monitoring a whitelist of allowed security extensions (authenticated packages, logon processes, notification packages, and security packages). Otherwise it's hard to pull useful information from these events, except event 4611 which typically should display "SYSTEM" for the "Subject" field. This subcategory doesn't have Failure events, so there is no recommendation to enable Failure auditing for this subcategory.

## Audit System Integrity •

Computer Type	General Success	General Failure	Stronger Success	Stronger Failure	Comments
Domain Controller	Yes	Yes	Yes	Yes	<p>The main reason why we recommend Success auditing for this subcategory is to be able to get RPC integrity violation errors and auditing subsystem errors (event 4612). However, if you are planning to manually invoke "4618(S): A monitored security event pattern has occurred", then you also need to enable Success auditing for this subcategory.</p> <p>The main reason why we recommend Failure auditing for this subcategory is to be able to get <a href="#">Code Integrity</a> failure events.</p>
Member Server	Yes	Yes	Yes	Yes	<p>The main reason why we recommend Success auditing for this subcategory is to be able to get RPC integrity violation errors and auditing subsystem errors (event 4612). However, if you are planning to manually invoke "4618(S): A monitored security event pattern has occurred", then you also need to enable Success auditing for this subcategory.</p> <p>The main reason why we recommend Failure auditing for this subcategory is to be able to get <a href="#">Code Integrity</a> failure events.</p>
Workstation	Yes	Yes	Yes	Yes	<p>The main reason why we recommend Success auditing for this subcategory is to be able to get RPC integrity violation errors and auditing subsystem errors (event 4612). However, if you are planning to manually invoke "4618(S): A monitored security event pattern has occurred", then you also need to enable Success auditing for this subcategory.</p> <p>The main reason why we recommend Failure auditing for this subcategory is to be able to get <a href="#">Code Integrity</a> failure events.</p>

## 1. Global Object Access Auditing

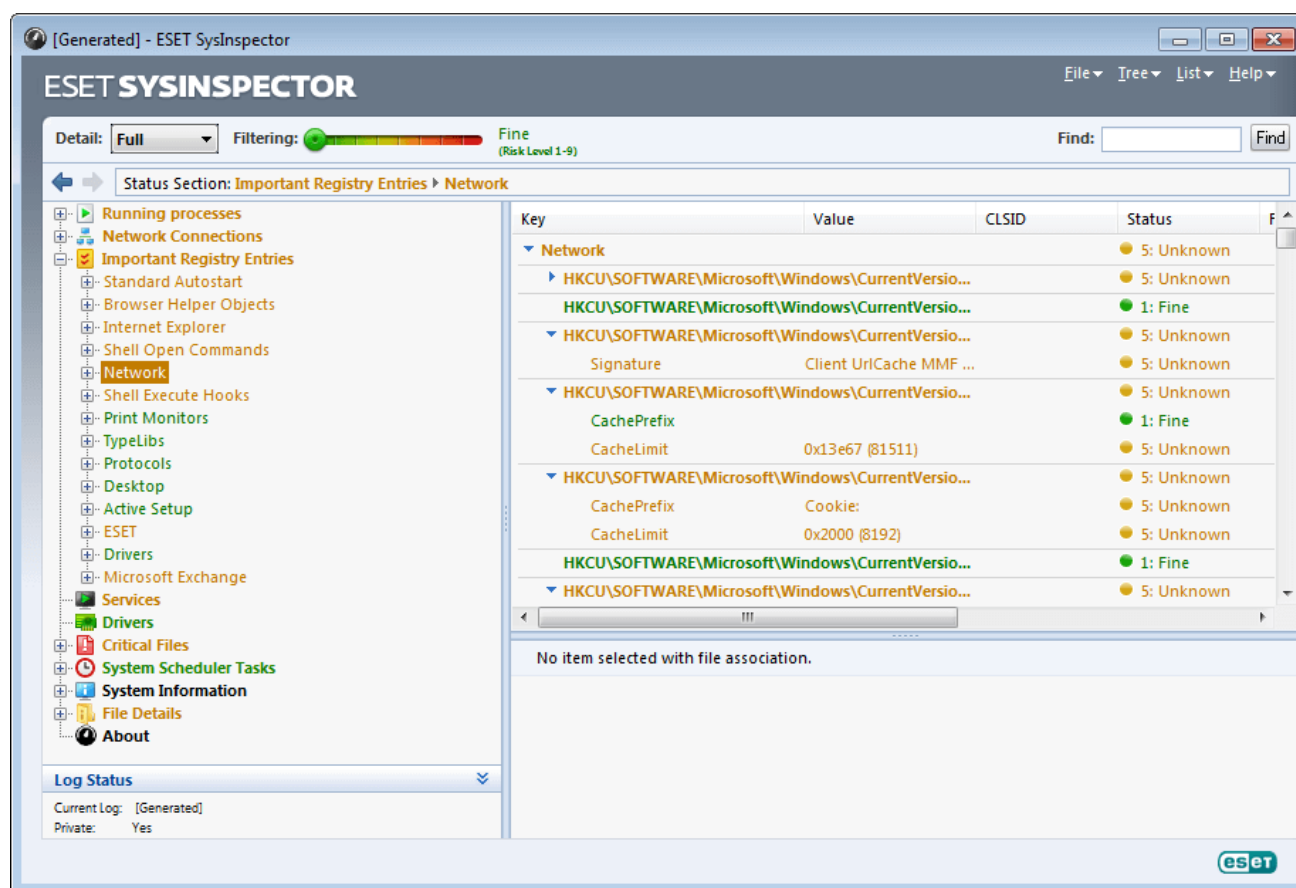
File System (Global Object Access Auditing) •

Registry (Global Object Access Auditing) •

## بخش دوم : معرفی دیگر ابزارها

### ۱. بازرس سیستم (ESET SysInspector)

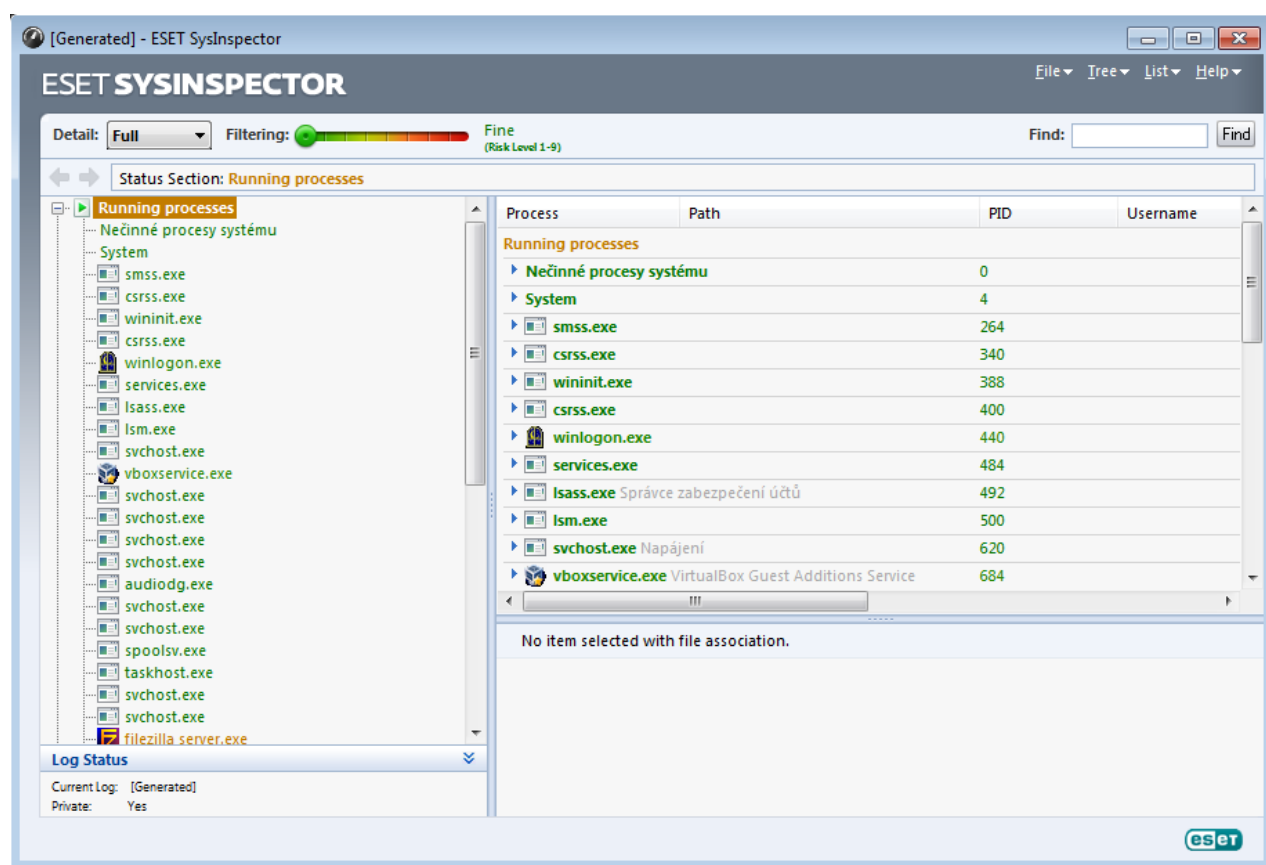
یک ابزار تشخیصی فوق العاده مدرن است که داده‌های کلیدی را از سیستم گرفته و مجموعه‌ای وسیع از مسائل امنیت و سازگاری را بررسی و عیب‌یابی می‌کند. این ابزار در واقع با سیستم‌عامل شما یکپارچه شده و شروع به رصد فعالیت‌های سیستم خواهد کرد. به طور مثال پردازش‌های جاری سیستم، محتوای رجیستری ویندوز، آیتم‌های موجود در استارت آپ و اتصالات شبکه‌ای رصد خواهند شد. بنابراین اگر فعالیت مشکوکی در سیستم صورت گیرد، این بخش می‌تواند به شما هشدارهای لازم را بدهد و یا در کشف تهدید به شما کمک کند. مسلماً چنین ابزاری می‌تواند به یک متخصص فناوری اطلاعات یا مدیر یک شبکه کمک شایانی کند.



برای شروع باید روی Create که در پایین این بخش قرار دارد کلیک کرده و به اصطلاح یک Snapshot تهیه کنید. تنها کافیست یک نام برای snapshot خود انتخاب کنید. پس از گذشت حدود یک دقیقه می‌توانید روی snapshot ایجاد شده راست کلیک کرده و گزینه Show را بزنید تا پنجره موردنظر باز شود. اکنون می‌توانید به دنیایی از اطلاعات مربوط به فعالیت‌های سیستمی و شبکه‌ای دسترسی داشته باشید. البته اگر تخصص کافی در زمینه امنیت ندارید، بهتر است که تغییری در تنظیمات این بخش ایجاد نکنید.

در زمانی که نیازمند راهکاری جهت شناسایی کدهای مخرب ناشناخته روی رایانه می باشید نرم افزار "ESET SysInspector" به عنوان یک ابزار کمکی فوق العاده قادر به شناسایی مشکلات مربوط به موارد زیر می باشد.

- سرویس ها و فرایندهای در حال اجرا
- وجود فایل های مشکوک بدون نشانه و علامت
- مسائل نرم افزاری
- ناسازگاری های سخت افزاری
- درایورهایی با عملکرد نادرست و یا قدیمی
- فایل های خراب سیستم عامل
- رجیستری های ناقص و معیوب
- اتصالات مشکوک شبکه ای



همچنین برای عیب یابی سریع در نرم افزار "ESET SysInspector" هر یک از داده ها را بر اساس درجه اولویت و حساسیت بر طبق رنگ خاصی از سبز تا قرمز نمایش می دهد و با استفاده از یک نوار کشویی می توان داده های موجود را بر اساس درجه و سطح امنیتی فیلتر

نمود. قابلیت مقایسه گزارش‌ها یا اصطلاحاً "Compare Log" در این محصول شما را قادر می‌سازد تا با بررسی گزارشات مختلف فایل‌ها یا فرآیندهای مشکوک را شناسایی نمایید.

## ۲. Microsoft Baseline Security Analyzer

یکی از نرم‌افزارهای جالب و بسیار کاربردی برای فعالان، مدیران شبکه و مدیران سیستم می‌توان به نرم‌افزار Microsoft Baseline Security Analyzer (MBSA) اشاره کرد که از سری محصولات شرکت مایکروسافت می‌باشد. با استفاده از این نرم‌افزار می‌توان به راحتی حفره‌های امنیتی موجود در شبکه را شناسایی و کانفیگ‌های نادرست انجام شده به راحتی تجزیه و تحلیل و آنالیز کرد.

از این نرم‌افزار می‌توان جهت شناسایی و ارزیابی امنیتی کلیه سیستم‌هایی که از سیستم عامل‌های شرکت مایکروسافت استفاده می‌کنند، بهره برد. به این صورت که mbsa با استفاده از ابزار اسکن خود وضعیت پیچ‌های سیستم عامل را بررسی و پیکره‌بندی‌های امنیتی را آنالیز و گزارشی از وضعیت امنیتی سیستم ارائه می‌دهد.

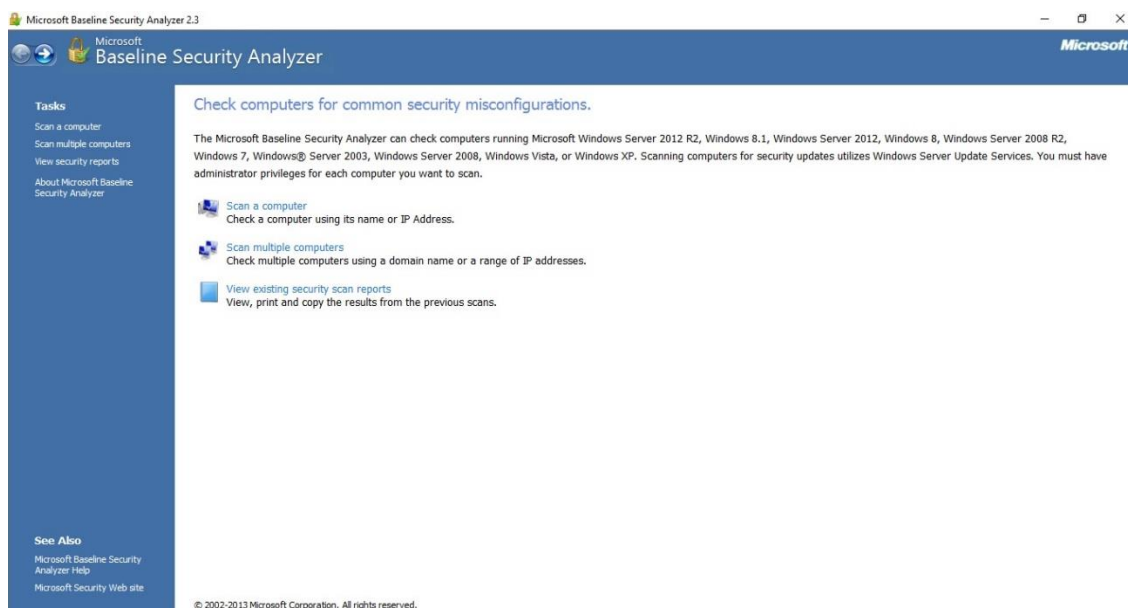
این ابزار توسط شرکت مایکروسافت ارائه شده است و به منظور آنالیز سیستم از دیدگاه امنیتی مورد استفاده قرار می‌گیرد و راهکارهایی را برای برطرف نمودن ریسک‌های امنیتی ارائه می‌دهد و سیستم‌عامل‌های زیر را می‌تواند مورد بررسی قرار دهد.

- Windows Server ۲۰۱۲R2
- Windows ۸/۷
- Windows Server ۲۰۱۲
- Windows ۸
- Windows Server ۲۰۰۸R2
- Windows ۷
- Windows® Server 2003
- Windows Server ۲۰۰۸
- Windows Vista
- Windows XP

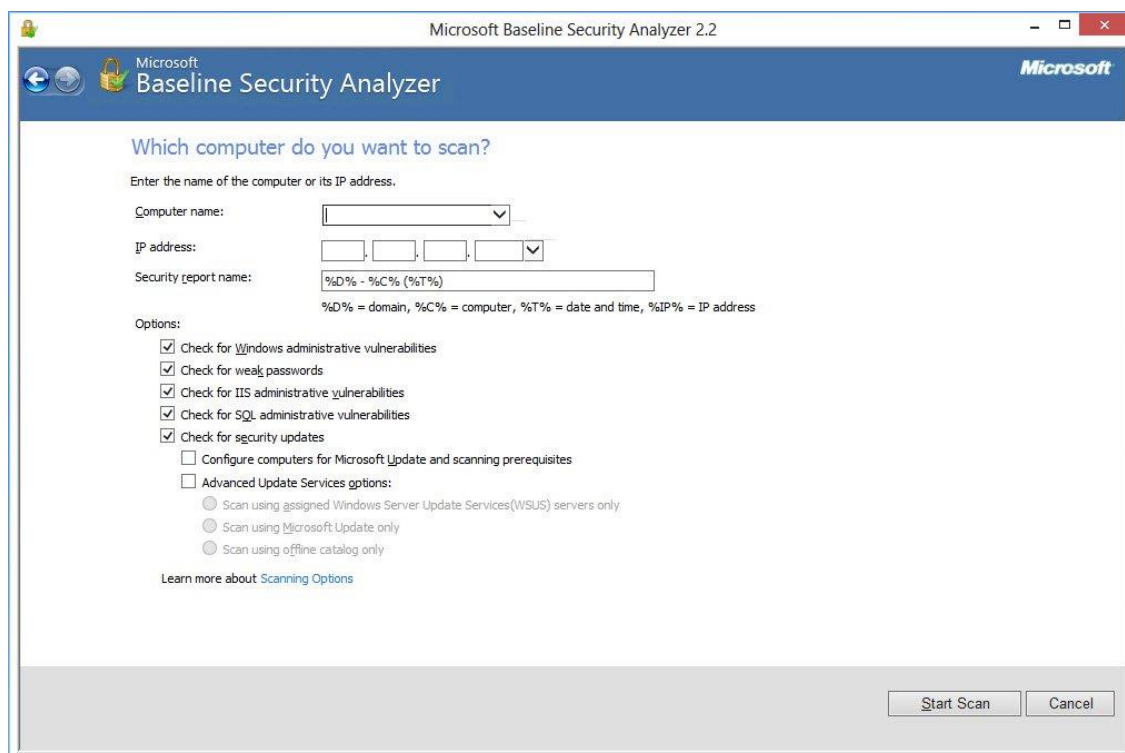
برای دانلود برنامه به لینک زیر می‌توان مراجعه کرد.

<https://www.microsoft.com/en-us/download/details.aspx?id=7558>

با اجرای برنامه و انتخاب گزینه Scan a computer می‌توان اسکن را شروع کرد.



در این بخش برنامه نام سیستم شما را شناسایی نموده و از شما درخواست آی پی سیستم خود را دارد. آی پی سیستم را وارد نموده و بسته به نیاز خود تیک‌های گزینه‌های مربوطه را بزنید هر کدام در زیر جداگانه توضیح داده شده‌اند.



Check for Windows administrative vulnerabilities: برای چک کردن آسیب‌پذیری‌های مدیریتی سیستم می‌باشد و در صورت که مدیر سیستم تنظیماتی را اعمال کرده باشد که سیستم دچار آسیب پذیری شده باشد به ما اطلاع می‌دهد.

Check for weak passwords: تمامی رمزهای عبور را از لحاظ پیچیدگی رمز عبور چک می‌نمایند و رمزهای عبوری را که ضعیف می‌باشند به ما اطلاع می‌دهد.

Check for IIS administrative vulnerabilities : آسیب‌پذیری‌های سرویس IIS موجود در سیستم را به ما اطلاع می‌دهد تا آن‌ها را برطرف نماییم. این آسیب‌پذیری‌ها ممکن است بدلیل اینکه تنظیمات توسط مدیر سیستم بدرستی انجام نشده است وجود آید.

Check for SQL administrative vulnerabilities : آسیب‌پذیری‌های پایگاه داده SQL را به ما اطلاع می‌دهد تا آن‌ها را برطرف نمایید. این آسیب‌پذیری‌ها ممکن است بدلیل اینکه تنظیمات توسط مدیر سیستم بدرستی انجام نشده است وجود آید.

Check for security updates : این بخش سیستم مورد نظر را بررسی نموده و تمامی به روزرسانی‌های امنیتی را که سیستم نیازمند به نصب آن‌ها بوده را شناسایی نموده و سپس نصب می‌نماید.

همچنین می‌توانید در بخش Security report name نامی را برای گزارشی که در آخر ارائه می‌شود در نظر بگیرید.

### Report Details for VCP - WIN-10-TEST (2016-08-29 09:47:35)

**Security assessment:**  
Incomplete Scan (Could not complete one or more requested checks.)

Computer name: VCP\WIN-10-TEST  
IP address: 192.168.56.1  
Security report name: VCP - WIN-10-TEST (8-29-2016 9:47 AM)  
Scan date: 8/29/2016 9:47 AM  
Scanned with MBSA version: 2.3.2211.0  
Catalog synchronization date: Security updates scan not performed

Sort Order:

#### Windows Scan Results

##### Administrative Vulnerabilities

Score	Issue	Result
	Automatic Updates	The Automatic Updates system service is not running. <a href="#">What was scanned</a> <a href="#">How to correct this</a>
	Password Expiration	Some user accounts (4 of 7) have non-expiring passwords. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
	Incomplete Updates	No incomplete software update installations were found. <a href="#">What was scanned</a>
	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
	Local Account Password Test	Some user accounts (2 of 7) have blank or simple passwords, or could not be analyzed. <a href="#">What was scanned</a> <a href="#">Result details</a>
	File System	All hard drives (6) are using the NTFS file system.

با کلیک نمودن بر روی What was scanned می‌توانید توضیحات بیشتری در مورد ریسک امنیتی مذکور را مشاهده نمایید. با کلیک نمودن بر روی How to correct this می‌توانید نحوه برطرف نمودن آن را مشاهده کرده و در آخر نیز بر روی OK کلیک نمایید و همچنین برای مشاهده گزارش پایش‌هایی که تا به حال انجام داده‌اید می‌توانید از سمت راست گزینه View security reports را انتخاب نمایید.

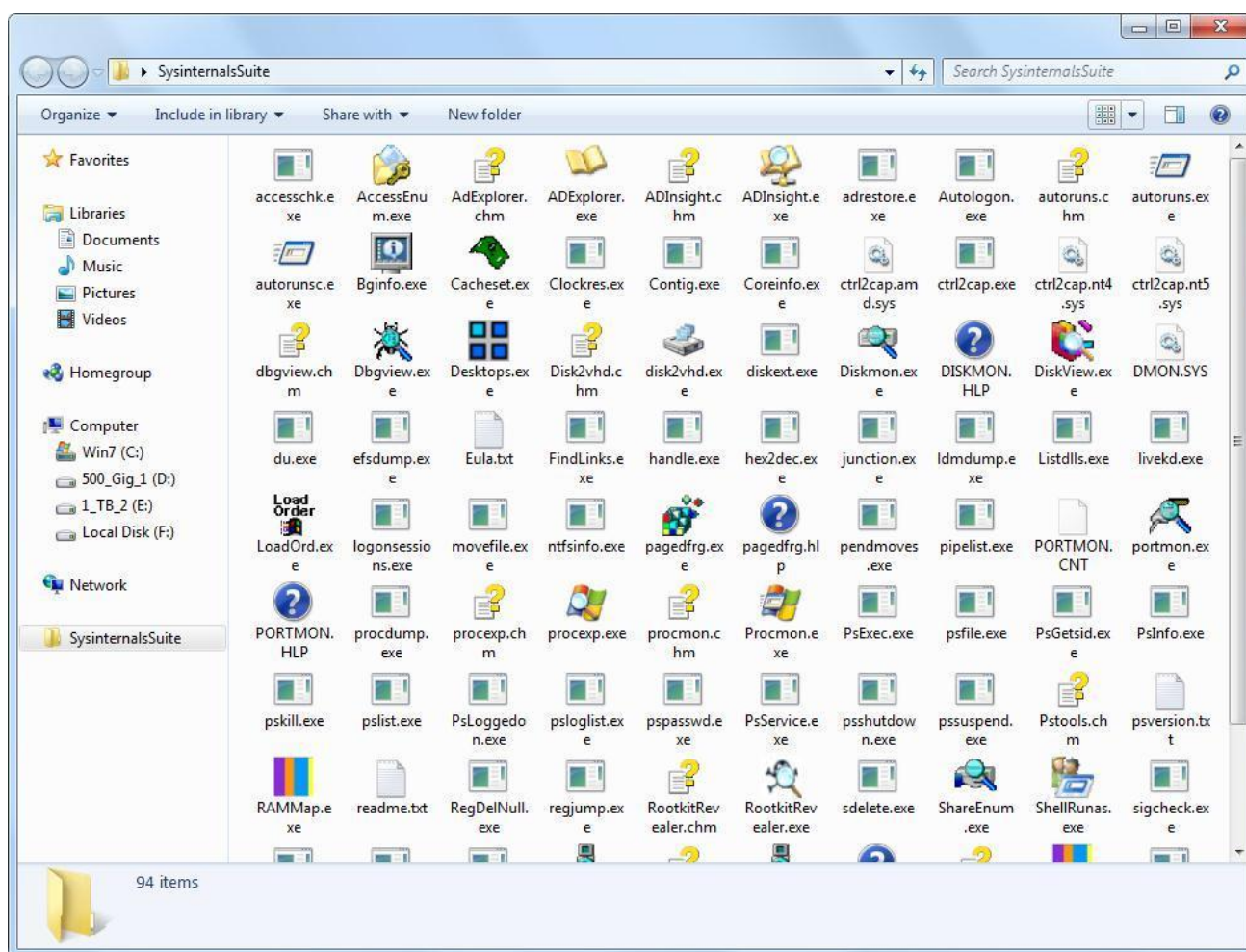
### ۳. مجموعه ابزار Windows Sysinternals Suite

کمپانی مایکروسافت یک ست کامل از ابزارهای تشخیص و رفع ایرادات برای سیستم عامل ویندوز طراحی و توسعه داده و آن را به رایگان در اختیار کاربران قرار داده است. این ست ابزار "Windows Sysinternals" نام دارد که تا چند سال پیش تعدادی ابزار جدا از هم بودند و باید آن‌ها را با زحمت به صورت تک تک دانلود می‌کردید. اما هم اکنون مایکروسافت تمامی این ابزارهای مفید را در یک بسته‌بندی به نام "Windows Sysinternals Suite" قرار داده که با دانلود این ست کامل به تمامی این ابزارها دسترسی پیدا می‌کنید.



این ست حاوی بیش از ۴۰ ابزار سبک و ساده، اما کاربردی و حرفه‌ای می‌باشد که هر کدام به یک منظور طراحی شده‌اند. از این ابزار برای حسابرسی یا Audit نیز استفاده می‌کنند و مجموعه آن شامل ابزارهای زیر است.

AccessChk | AccessEnum | AdExplorer | AdInsight | AdRestore | Autologon | Autoruns | BgInfo | BlueScreen | CacheSet | ClockRes | Contig | Coreinfo | Ctrl2Cap | DebugView | Desktops | Disk2vhd | DiskExt | DiskMon | DiskView | Disk Usage (DU) | EFSDump | FileMon | FindLinks | Handle | Hex2dec | Junction | LDMDump | ListDLLs | LiveKd | LoadOrder | LogonSessions | MoveFile | NewSid | NotMyFault | NTFSInfo | PageDefrag | PendMoves | PipeList | PortMon | ProcDump | Process Explorer | ProcFeatures | Process Monitor | PsExec | PsFile | PsGetSid | PsInfo | PsKill | PsList | PsLoggedOn | PsLogList | PsPasswd | PsPing | PsService | PsShutdown | PsSuspend | PsTools | RAMMap | RegDelNull | RegHide | RegJump | RegMon | Rootkit Reveal | Registry Usage (RU) | SDelete | ShareEnum | ShellRunas | Sigcheck | Streams | Strings | Sync | Sysmon | TCPView | VMMMap | VolumeID | WhoIs | WinObj | ZoomIt |





کار کردن با هر یک از ابزار دارای آموزش جداگانه است و به صورت مداوم نیز به این ابزارها اضافه می‌شود که به آپدیت‌های اخیر این مجموعه در زیر اشاره شده است.

#### What's New (November 19, 2017)

- Sysmon v6.20
- Whois v1.20

#### What's New (September 11, 2017)

- Sysmon v6.10
- Process Monitor v3.40
- Autoruns v13.80

#### What's New (May 16, 2017)

- ProcDump v9.0

#### What's New (February 17, 2017)

- Sysmon v6.”
- Autoruns v13.7
- AccessChk v6.1

## منابع :

- <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings>
- <https://www.microsoft.com/en-us/download/details.aspx?id=7558>
- [http://www.itsecure.hu/.../CIS\\_Microsoft\\_Windows\\_8.1\\_Workstation\\_Benchmark\\_v2.2.1.pdf](http://www.itsecure.hu/.../CIS_Microsoft_Windows_8.1_Workstation_Benchmark_v2.2.1.pdf)
- <http://msdn.microsoft.com/en-us/library/aa302360.aspx>
- <http://technet.microsoft.com/en-us/security/cc184922.aspx>
- <https://www.centrel-solutions.com/xiaconfiguration/capabilities.aspx?capability=windows-server-security-audit-tool>
- <http://www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/Pages/ViewDiscussion.aspx?PostID=1>
- <https://www.eset.com/int/support/sysinspector>