

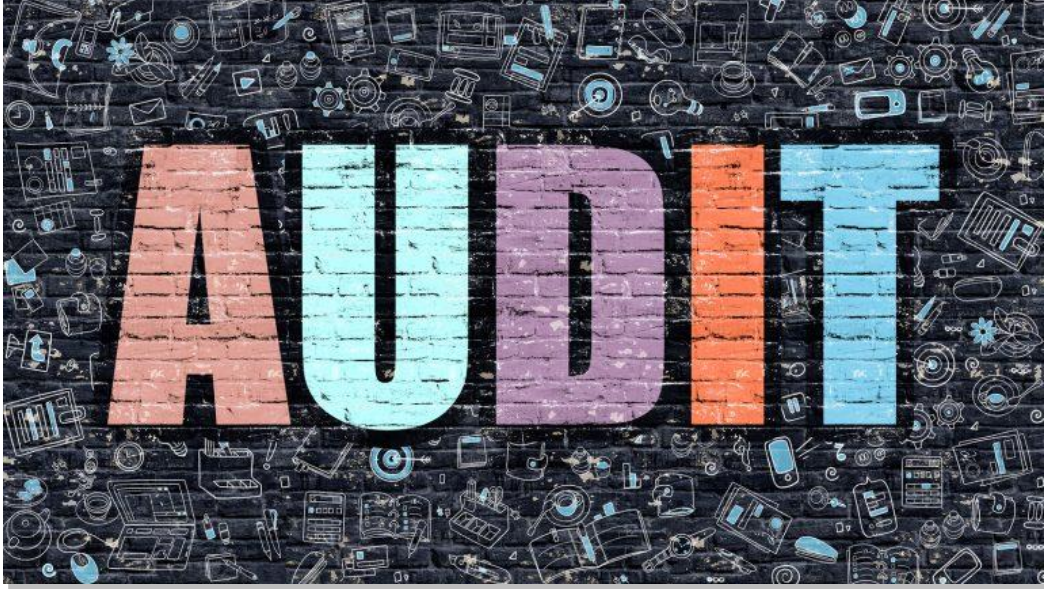
# Denetim ve Log'lamanın Elli Tonu



Hasan Dimdik | Cloud and Datacenter MVP

[www.hasandimdik.com](http://www.hasandimdik.com)

[www.mshowto.org](http://www.mshowto.org)



## İçindekiler

Giriş.....	4
Denetim(Audit) ve Log'lama Neden Önemli .....	4
Account Logon.....	5
Audit Credential Validation .....	5
Audit Kerberos Authentication Service .....	6
Audit Kerberos Service Ticket Operations.....	6
Account Management.....	8
Audit Computer Account Management .....	8
Audit User Account Management .....	10
Audit Security Group Management .....	11
Detailed Tracking.....	13
Audit Process Creation .....	13
Audit Token Right Adjust.....	14
DC Access.....	16

Audit Directory Service Access & Service Changes .....	16
Logon /Logoff .....	18
Audit Logon .....	18
Audit Logoff .....	19
Audit Group Membership .....	20
Audit Account Lockout .....	21
Object Access .....	22
Audit File System .....	22
Audit File Share.....	25
Audit Registry .....	28
Audit Filtering Platform Connection Properties.....	31
Policy Change .....	33
Audit Policy Change.....	33
Audit Authentication Policy Change.....	34
Audit MPSSVC Rule-Level Policy Change.....	36
Privilege Use .....	38
Audit Non Sensitive Privilege Use .....	38
Audit Sensitive Privilege Use .....	40
Active Directory için Tavsiye Edilen Log'lama Ayarları .....	42
Tavsiye Edilen Minimum Denetim Kuralı .....	42
Tavsiye Edilen NTLM Audit Events .....	44
Azure Security Center ile Log'ların Anlamlandırılması .....	44
Azure Security Center – Events .....	48
Sysmon .....	50
Log'ların Kibana ile Anlamlandırılması .....	52
Winlogbeat .....	52
Event Log'ların Kibana ile Anlamlandırılması.....	57
Powershell' i Nasıl Log'larım ? .....	60
Script Block Logging.....	61
Module Logging .....	62
Logging Powershell Activity.....	64

## Giriş

Merhaba,

Bu döküman serisini yazmamın en önemli sebebi birden fazla güvenlik ürününe sahip olmamıza rağmen neleri izleyeceğiz, hangi Log'lar önemli, hangileri kritik kıyaslamasını yapamıyor olmamız veya eksik olmasıdır. Buradaki açığı kapatmak amacıyla en azından Windows platformları için neler yapabilirizi düşünürken bu seriyi yazmak aklıma geldi. Keyifle okumanız dileğiyle...

## Dikkat

Konular içerisinde tüm audit GPO'larına yer verilmeyeceği için içerikte eksiklikler olacaktır. İlgili döküman rehber niteliğindedir, fakat bütünü kapsamamaktadır.

## Denetim(Audit) ve Log'lama Neden Önemli

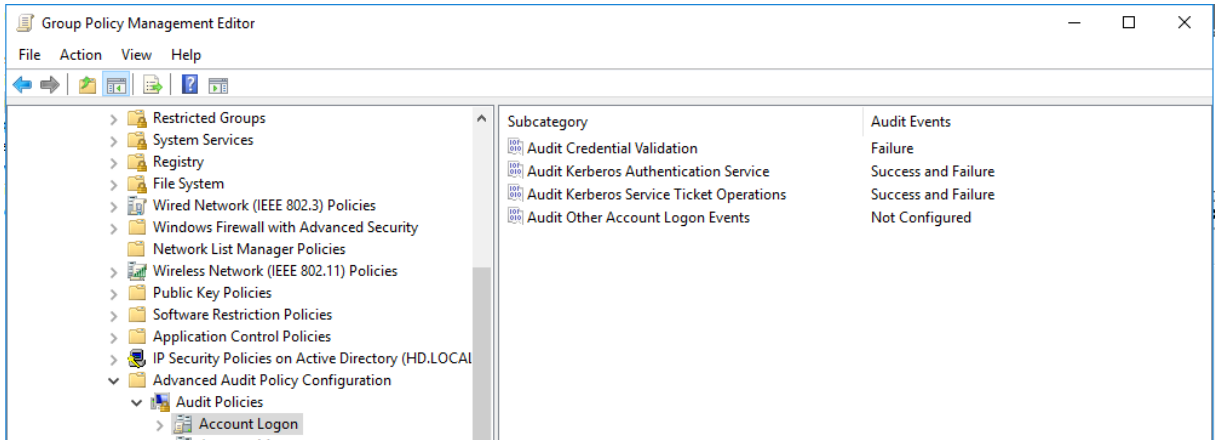
Yapımız içerisinde olan biten hareketleri izlemek ve anormal davranışları öğrenmek için önemli uç noktaları denetlemeye ve Log'lamaya ihtiyacımız bulunmaktadır. Bu durumu örnekle açıklamak gerekirse cinayet işlendiğinde izleri takip edebilirsek cinayeti işleyeni hızlı şekilde bulabiliriz. Doğru şekilde denetleyemediğimiz, Log'layamadığımız ve günün sonunda bu oluşan dataları anlamlandıramadığımız vakaları çözme imkanımız da bulunmamaktadır. Bu bilinmezlik de bizi her zaman diken üstünde tutacaktır. Bu yazı serisi tam da burada devreye giriyor. Neden önemli kısmının geri kalanını yazı içerisinde bulacağınızı umuyorum...

# Advanced Audit Policy Configuration

## Account Logon

### Audit Credential Validation

Kimlerin NTLM protokolünü kullandığını öğrenmek için veya NTLM protokolü ile kimlik doğrulama denemesi yaptığını ilgili kural ile denetleyebiliriz. Bu kuralı DC lerde yapılandırmanız tavsiye edilmektedir.



Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-credential-validation>

## Audit Kerberos Authentication Service

İlgili kural yapılandırıldığında Kerberos doğrulama TGT( Ticket-Granting- ticket) talepleri izlenebilmektedir. Bu kuralın KDC (Key Distribution Center) sunucusu üzerinde yapılandırılması tavsiye edilmektedir. İlgili kuralın **Success ve Failure** izlenmesi tavsiye edilmektedir.

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-kerberos-authentication-service>

## Audit Kerberos Service Ticket Operations

Özellikle yetkisiz kişiler network kaynaklarına erişmek istediğinde Kerberos biletine ihtiyaç duyacaktır. İlgili kuralımız sayesinde erişim talepleri Log'lanabilecektir. Bu sayede düzgün bir Log'lama yöntemi ile bu şüpheli hareket izlenebilecektir. Bu kuralın KDC(Key Distribution Center) sunucusu üzerinde yapılandırılması tavsiye edilmektedir. İlgili kuralın **Success ve Failure** olarak izlenmesi tavsiye edilmektedir.

Aşağıdaki örnekte hasan kullanıcısı şifresini yanlış yazdığına oluşan Log'u görüyoruz.



Aynı kullanıcı ile başarılı şekilde oturum açtığımda aşağıdaki gibi Log oluşmaktadır.

Security Number of events: 26

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	11/2/2018 10:54:56 AM	Microsoft Windows security auditing.	4769	Kerberos Service T
Audit Success	11/2/2018 10:54:56 AM	Microsoft Windows security auditing.	4768	Kerberos Authent
Audit Failure	11/2/2018 10:54:51 AM	Microsoft Windows security auditing.	4771	Kerberos Authent
Audit Failure	11/2/2018 10:54:49 AM	Microsoft Windows security auditing.	4771	Kerberos Authent
Audit Success	11/2/2018 10:54:45 AM	Microsoft Windows security auditing.	4769	Kerberos Service T
Audit Success	11/2/2018 10:54:45 AM	Microsoft Windows security auditing.	4769	Kerberos Service T
Audit Success	11/2/2018 10:54:30 AM	Microsoft Windows security auditing.	4769	Kerberos Service T
Audit Success	11/2/2018 10:54:30 AM	Microsoft Windows security auditing.	4768	Kerberos Authent

Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:  
Account Name: hasan@HD.LOCAL

Log Name: Security  
Source: Microsoft Windows security Logged: 11/2/2018 10:54:56 AM  
Event ID: 4769 Task Category: Kerberos Service Ticket Operations  
Level: Information Keywords: Audit Success  
User: N/A Computer: dc01.hd.local  
OpCode: Info  
More Information: [Event Log Online Help](#)

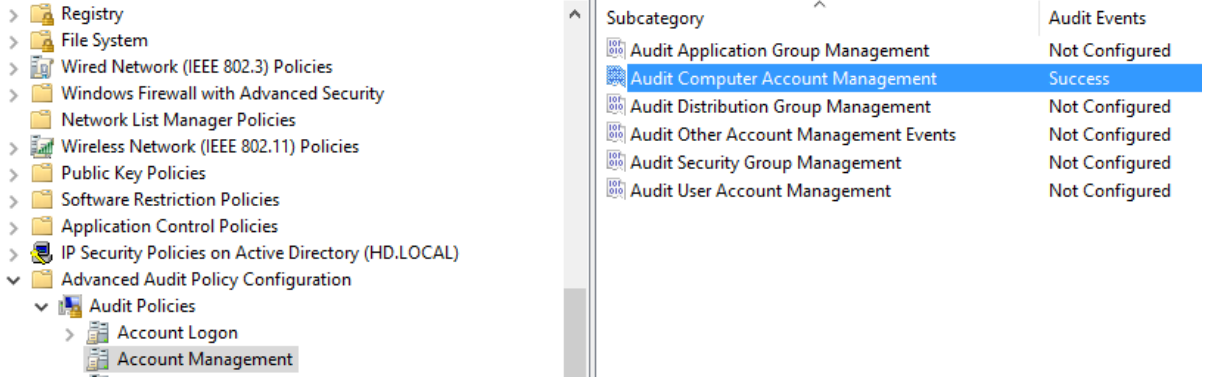
Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-kerberos-service-ticket-operations>

## Account Management

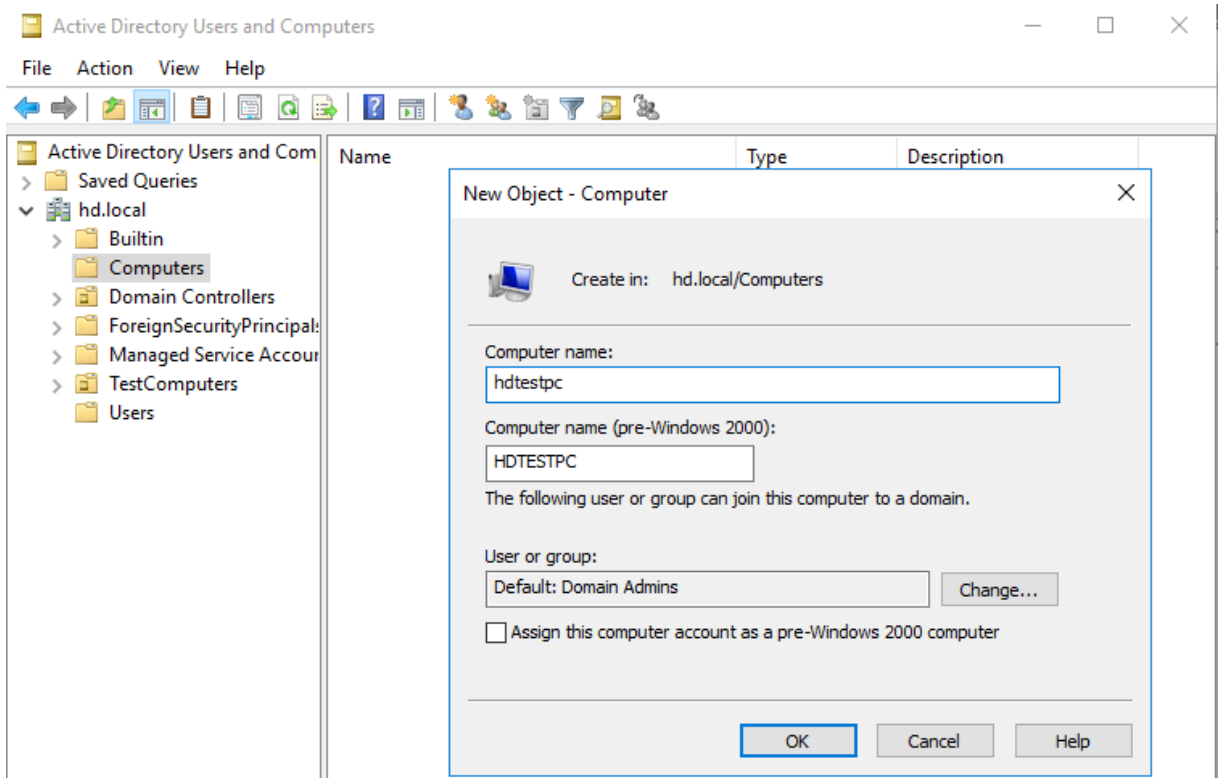
### Audit Computer Account Management

İlgili kuralın yapılandırılması ile birlikte bilgisayar hesabı oluşturma, modifiye etme veya silme işlemi Log'lanabilmektedir. Özellikle kritik bilgisayar objeleri, DomainController lar için yapılandırılması tavsiye edilmektedir.

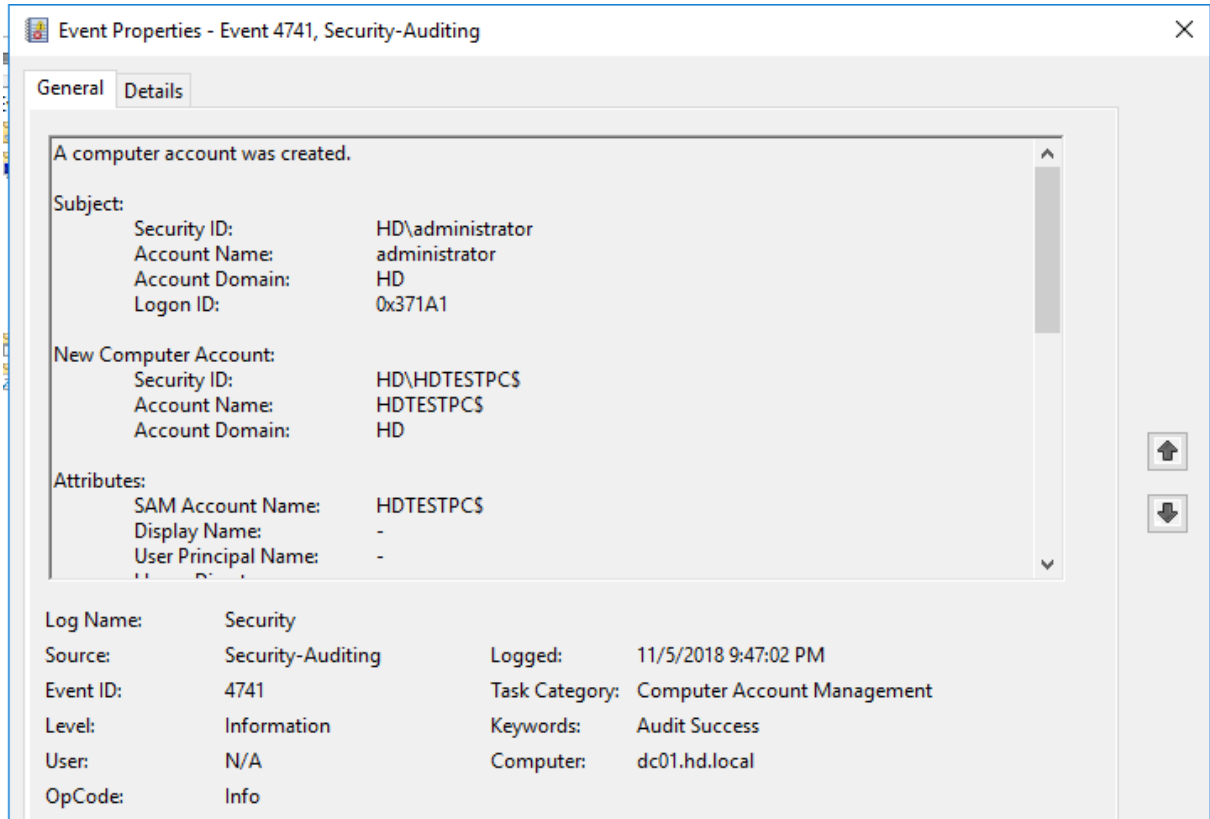




Örneğimizde hdtestpc isimli bilgisayar hesabını oluştuyorum.



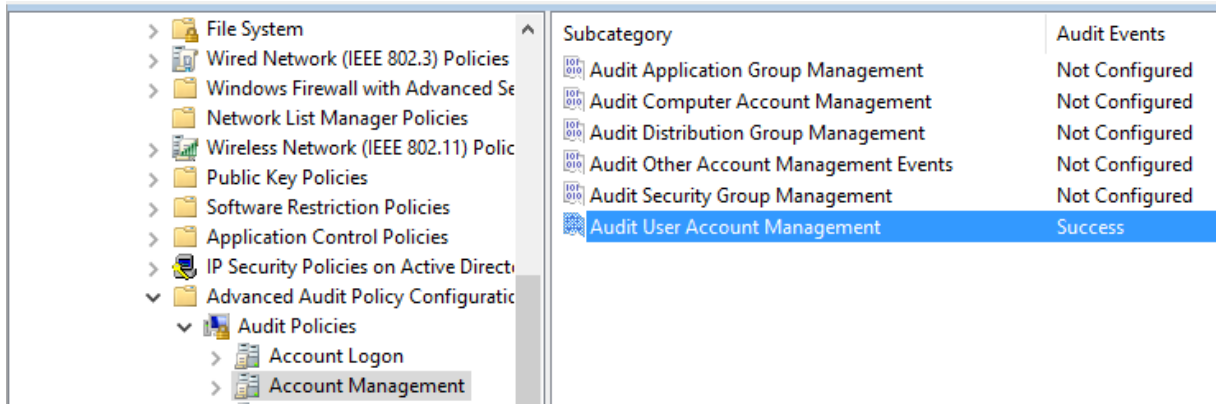
Olay günlüğüne baktığımda 4741 nolu olayın oluştuğunu görüyorum.



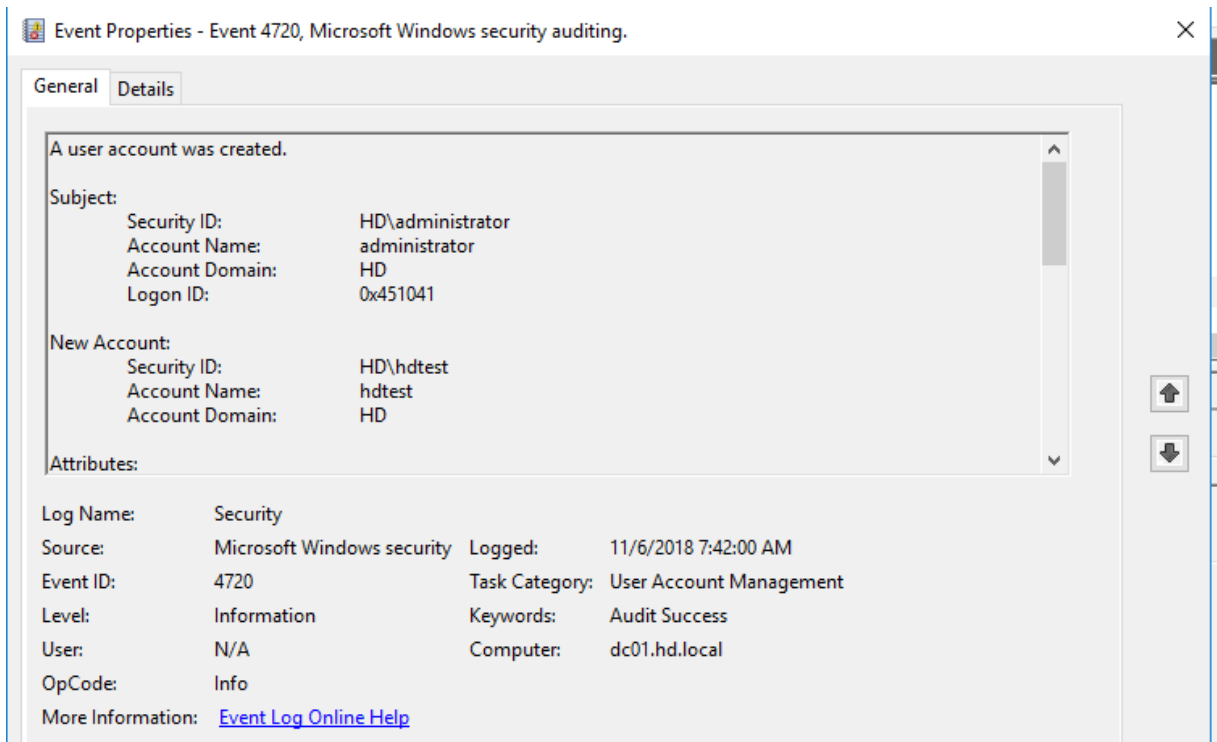
Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-computer-account-management>

## Audit User Account Management

Bir önceki bölümde yer alan kuralın benzeridir. Kullanıcı oluşturma, silme, isim değişikliği, kilitlenmesi gibi durumlarda Log üretmektedir. Özellikle kritik domain hesapları, yetkili hesaplar, servis hesapları için yapılandırılması tavsiye edilmektedir. İlgili kuralın **success ve Failure** olarak yapılandırılması tavsiye edilmektedir.









Örneğimizde administrator kullanıcısının Active Directory' de hctest kullanıcısını oluşturduğunu görüyoruz.



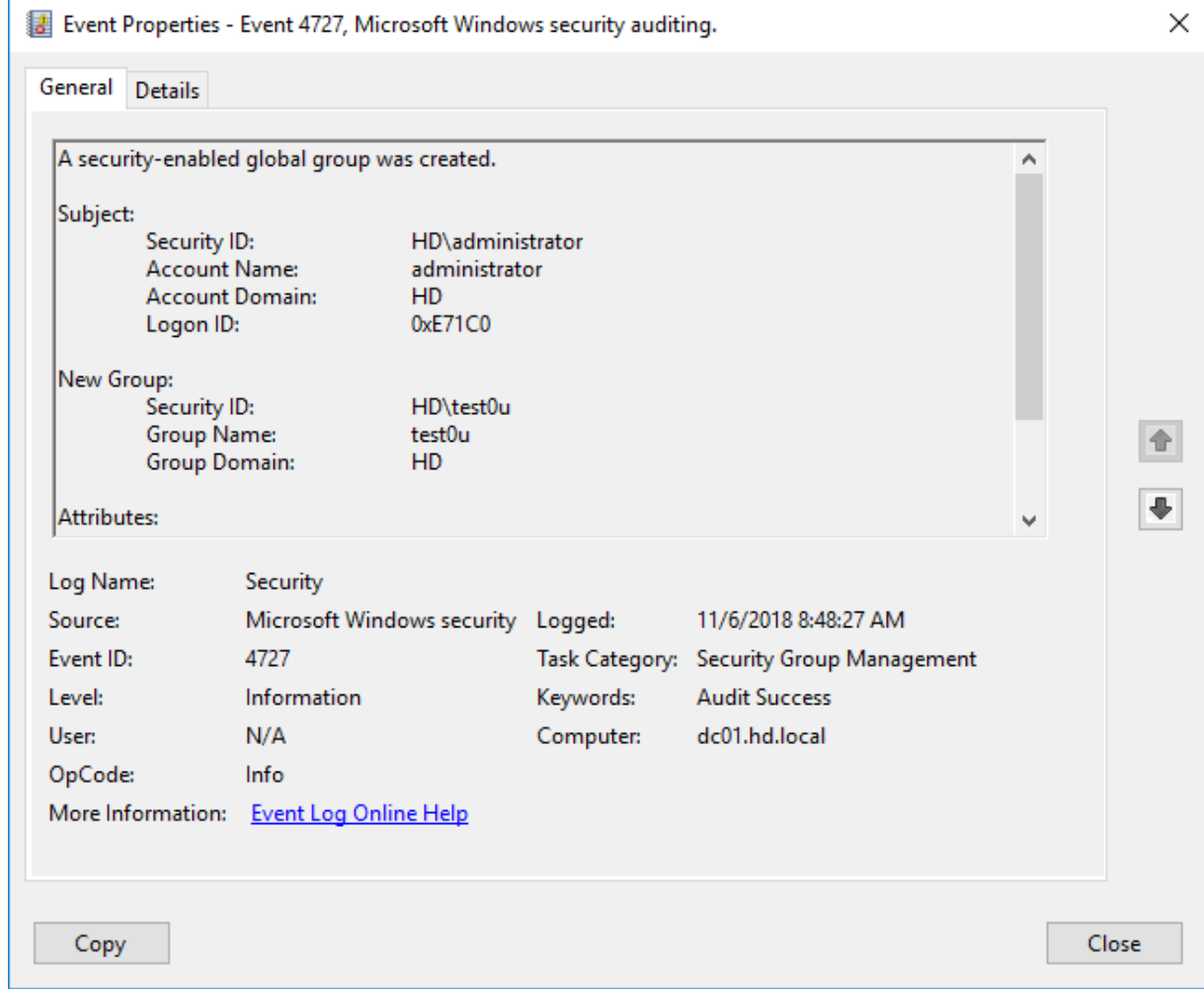
Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-user-account-management>

Audit Security Group Management

İlgili kuralın yapılandırılması ile güvenlik gruplarının oluşturulması, değiştirilmesi, silinmesi veya bu gruba kullanıcı eklenmesi-çıkarılması gibi hareketler Log'lanabilecektir. İlgili kuralın **Success, Failure** olarak yapılandırılması tavsiye edilmektedir.

Subcategory	Audit Events
 Audit Application Group Management	Not Configured
 Audit Computer Account Management	Not Configured
 Audit Distribution Group Management	Not Configured
 Audit Other Account Management Events	Not Configured
 Audit Security Group Management	Success and Failure
 Audit User Account Management	Not Configured

Örneğimizde test0u isimli güvenlik grubunun oluşturulduğunu görüyoruz.









Kaynak: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management>

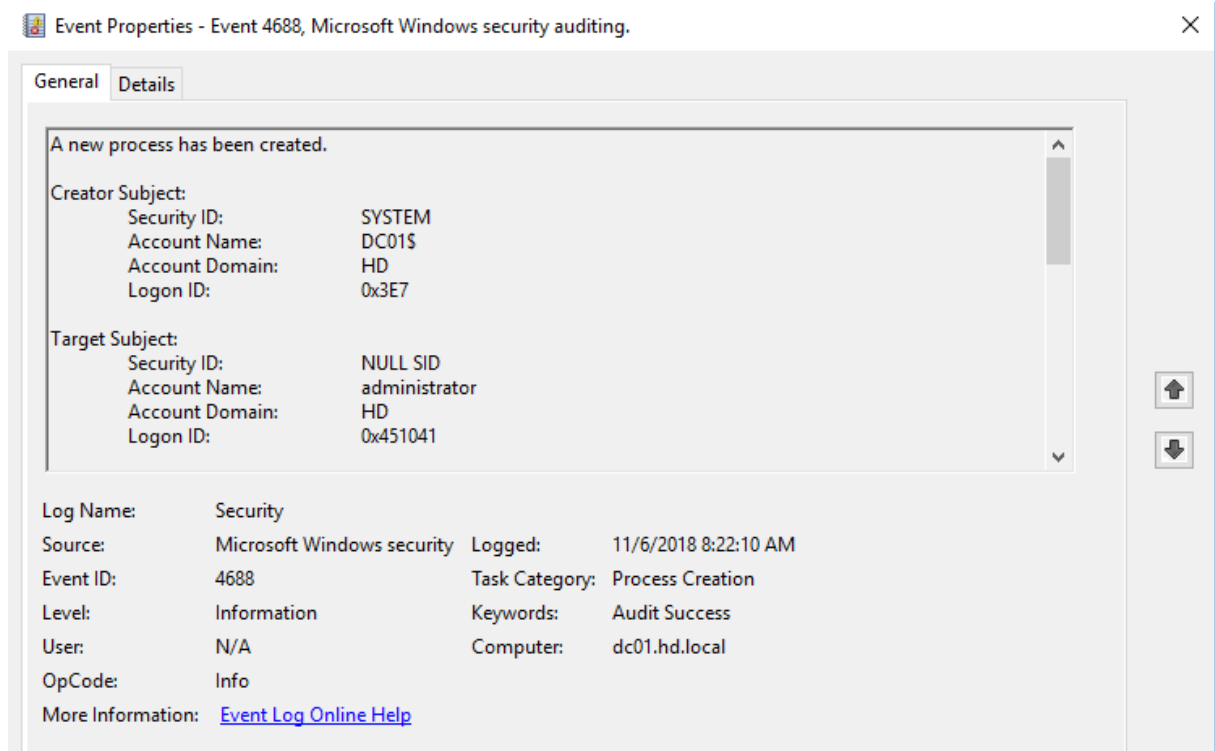
## Detailed Tracking

### Audit Process Creation

İlgili kural ile birlikte herhangi bir işlem başlatıldığında Log'lanacaktır. Bu kuralı yapılandırırken çok dikkatli olmak gerekmektedir. Birden çok işlem başlayacağı için çok hızlı Log'ların büyümesine sebep olacaktır. İlgili kuralın **Success** olarak yapılandırılması tavsiye edilmektedir.

Subcategory	Audit Events
 Audit DPAPI Activity	Not Configured
 Audit PNP Activity	Not Configured
 Audit Process Creation	Success and Failure
 Audit Process Termination	Not Configured
 Audit RPC Events	Not Configured
 Audit Token Right Adjusted	Not Configured







Örneğimizde bir işlem başladığında oluşan Log'u görüyoruz.



Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-process-creation>

Audit Token Right Adjust

Kritik kurallardan bir tanesidir fakat bu kural için bir handikap vardır. Eğer yapı içerisinde SCCM varsa WMI kullanımından dolayı çok sayıda 4703 Log'u üretilecektir. Güvenlik açısından duruma bakarsak zararlı aktivitelerinin tespiti, ayrıcalıklarla alakalı suistimal için önemli bir kuraldır.

Subcategory	Audit Events
 Audit DPAPI Activity	Not Configured
 Audit PNP Activity	Not Configured
 Audit Process Creation	Not Configured
 Audit Process Termination	Not Configured
 Audit RPC Events	Not Configured
 Audit Token Right Adjusted	Success and Failure

Event Properties - Event 4703, Microsoft Windows security auditing.

GeneralDetails

A token right was adjusted.

Subject:

Security ID:SYSTEM  
Account Name:DC01S  
Account Domain:HD  
Logon ID:0x3E7

Target Account:

Security ID:NULL SID  
Account Name:DC01S  
Account Domain:HD  
Logon ID:0x3E7

Process Information:

Process ID:0x210  
Process Name:C:\Windows\System32\lsass.exe

Log Name:Security  
Source:Microsoft Windows security  
Event ID:4703  
Level:Information  
User:N/A  
OpCode:Info  
More Information:[Event Log Online Help](#)

Logged:11/6/2018 8:41:04 AM  
Task Category:Token Right Adjusted Events  
Keywords:Audit Success  
Computer:dc01.hd.local





Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4703>

## DC Access

### Audit Directory Service Access & Service Changes

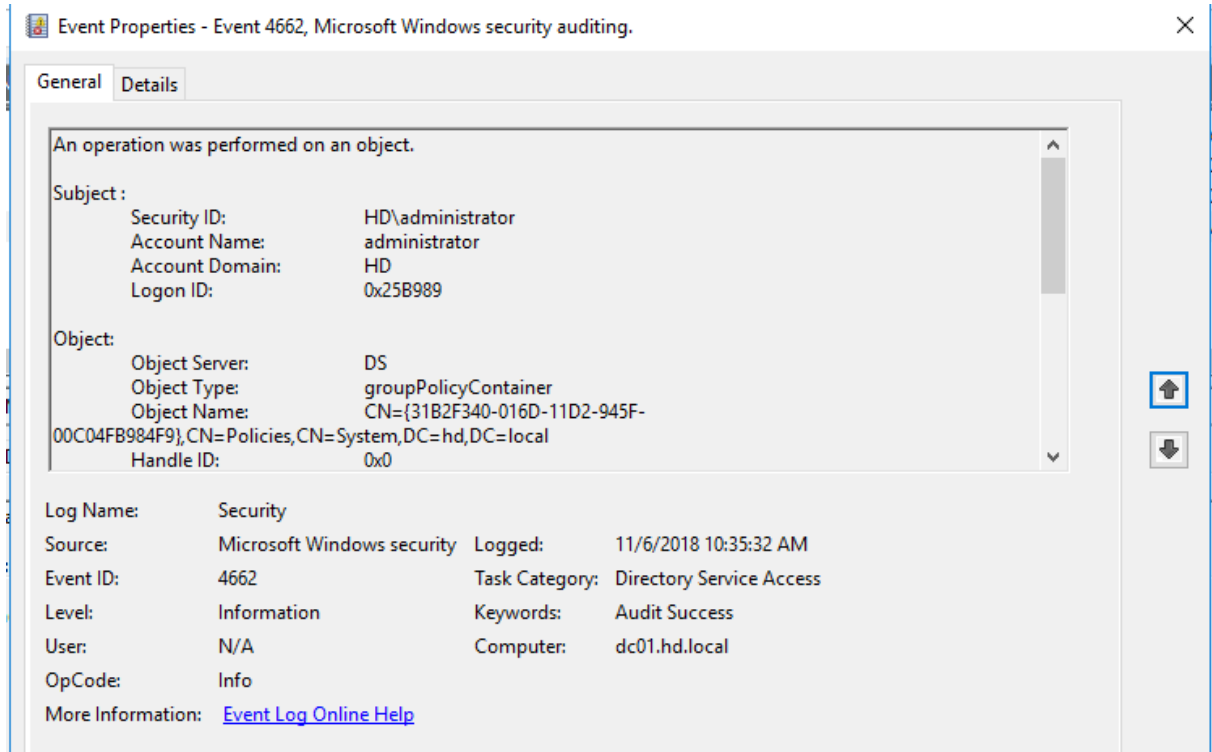
İlgili iki kuralı aynı başlık altında toplamamın sebebi birbiri ile çok yakın ilişki içerisinde olmalarını sebep gösterebilirim. Özellikle Active Directory objeleri ile alakalı değişiklik, güncelleme, yeni bir gpo yazılması gibi durumların Log'lanmasını sağlamaktadır.

Domain Controller lar için yapılandırılması tavsiye edilmektedir.

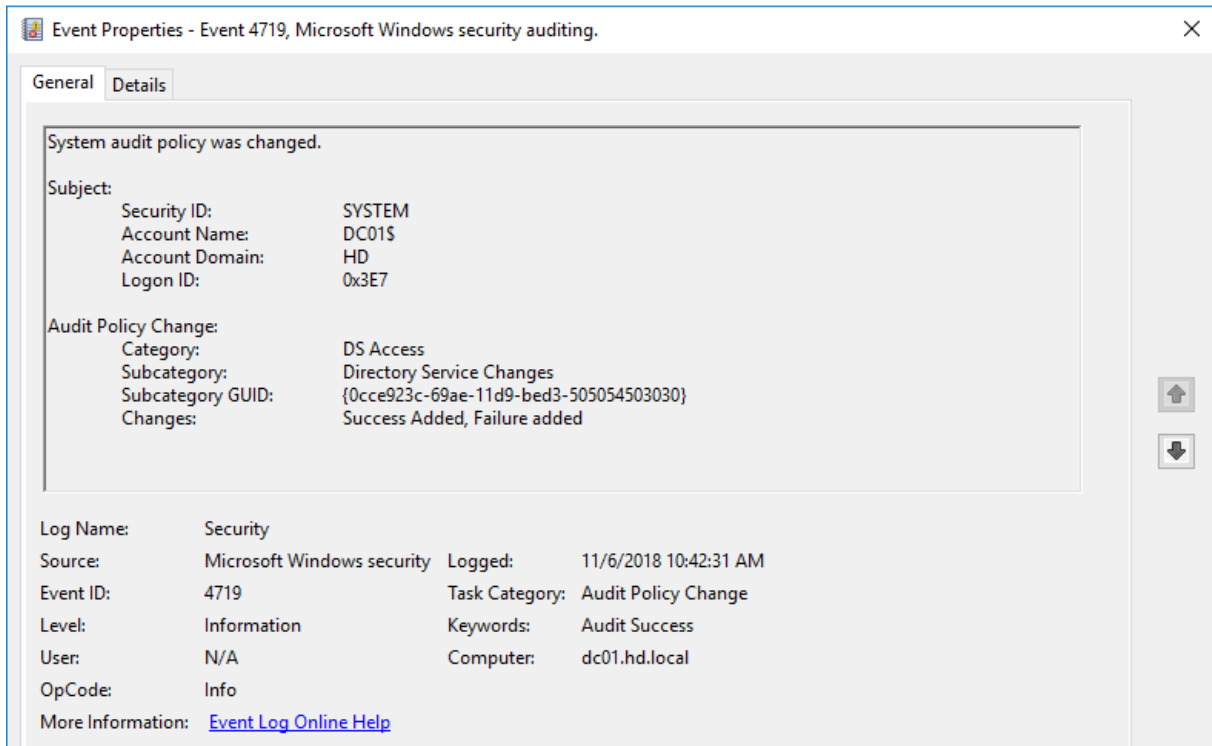
Subcategory	Audit Events
 Audit Detailed Directory Service Replication	Not Configured
 Audit Directory Service Access	Success and Failure
 Audit Directory Service Changes	Success and Failure
 Audit Directory Service Replication	Not Configured

Örneğimizi inceleyecek olursak administrator kullanıcım AD DS objelerine eriştiğini ifade etmektedir.





Diğer Log'da ise Audit Policy de değişiklik yapıldığını göstermektedir.



Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-directory-service-changes>

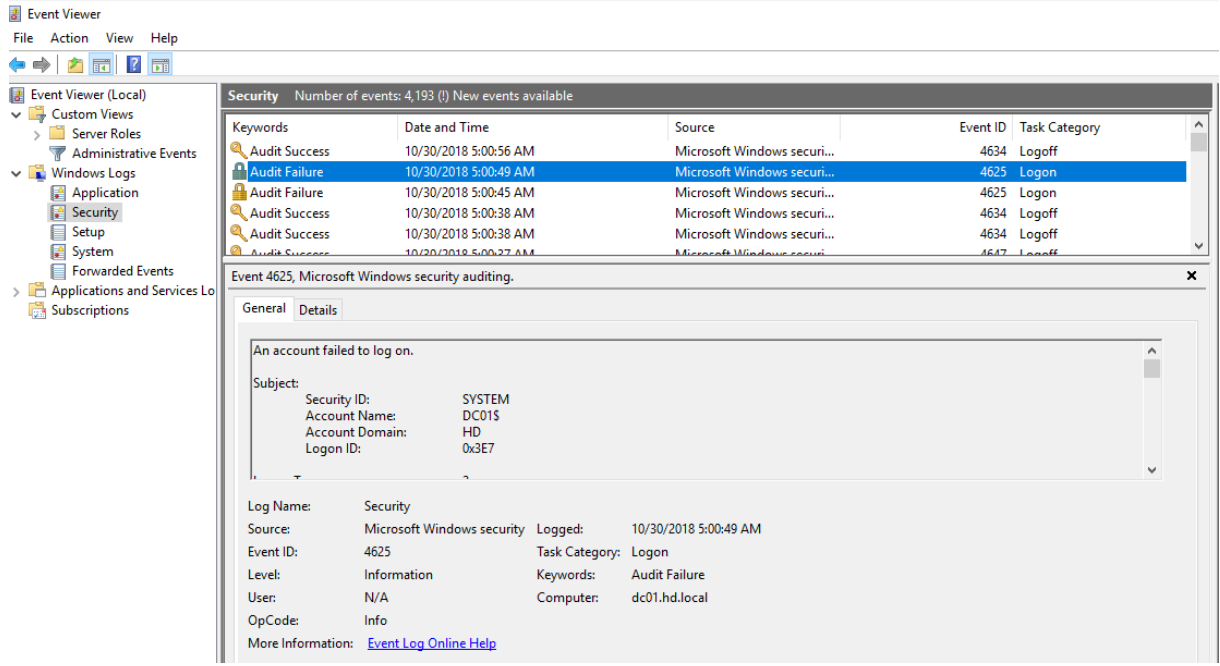
<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-directory-service-access>

## Logon /Logoff

### Audit Logon

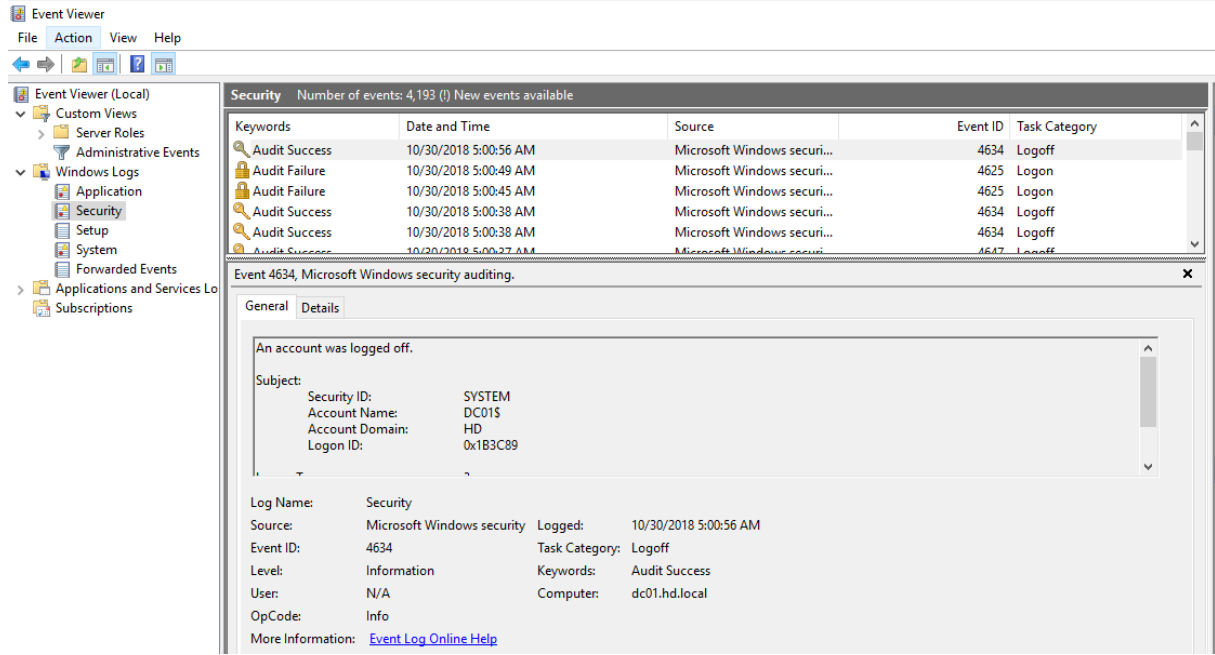
İlgili kural aktif edilirse ve failure seçilirse, başarısız oturum açma denemeleri Log'lanmış olur. İlgili kuralın **Failure** olarak istemci makinalar için yapılandırılması tavsiye edilmektedir.

	Subcategory	Audit Events
> User Rights Assignment	Audit Account Lockout	Not Configured
> Security Options	Audit User / Device Claims	Not Configured
> Event Log	Audit Group Membership	Not Configured
> Restricted Groups	Audit IPsec Extended Mode	Not Configured
> System Services	Audit IPsec Main Mode	Not Configured
> Registry	Audit IPsec Quick Mode	Not Configured
> File System	Audit Logoff	Success
> Wired Network (IEEE 802.3) Policies	Audit Logon	Failure
> Windows Firewall with Advanced S	Audit Network Policy Server	Not Configured
> Network List Manager Policies	Audit Other Logon/Logoff Events	Not Configured
> Wireless Network (IEEE 802.11) Poli	Audit Special Logon	Not Configured
> Public Key Policies		
> Software Restriction Policies		
> Application Control Policies		
> IP Security Policies on Active Direct		
> Advanced Audit Policy Configurati		
> Audit Policies		
> Account Logon		
> Account Management		
> Detailed Tracking		
> DS Access		
> Logon/Logoff		



## Audit Logoff

Yukarıda yazmış olduğumuz kuralın bir benzeri niteliğindedir. Tek farkı oturum kapatma süreçleri Log'lanmaktadır.



Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events>

## Audit Group Membership

İlgili kural Audit Logon kuralı aktif edilmezse kullanılamamaktadır. Bu kuralımız, kullanıcımız bir istemciye bağlanmayı denediğinde Log üretmektedir. Anlatımı daha da sadeleştirecek olursak bir paylaşım alanına erişmek istediğimizde Log üretilmektedir. İlgili kuralın **success ve failure** olarak yapılandırılması tavsiye edilmektedir.

<ul style="list-style-type: none"> <li>Restricted Groups</li> <li>System Services</li> <li>Registry</li> <li>File System</li> <li>Wired Network (IEEE 802.3) Policies</li> <li>Windows Firewall with Advanced Security</li> <li>Network List Manager Policies</li> <li>Wireless Network (IEEE 802.11) Policies</li> <li>Public Key Policies</li> <li>Software Restriction Policies</li> <li>Application Control Policies</li> <li>IP Security Policies on Active Directory</li> <li>Advanced Audit Policy Configuration <ul style="list-style-type: none"> <li>Audit Policies <ul style="list-style-type: none"> <li>Account Logon</li> <li>Account Management</li> <li>Detailed Tracking</li> <li>DS Access</li> <li>Logon/Logoff</li> </ul> </li> </ul> </li> </ul>	<table> <tr> <th>Subcategory</th><th>Audit Events</th></tr> <tr> <td>Audit Account Lockout</td><td>Failure</td></tr> <tr> <td>Audit User / Device Claims</td><td>Not Configured</td></tr> <tr> <td>Audit Group Membership</td><td>Success and Failure</td></tr> <tr> <td>Audit IPsec Extended Mode</td><td>Not Configured</td></tr> <tr> <td>Audit IPsec Main Mode</td><td>Not Configured</td></tr> <tr> <td>Audit IPsec Quick Mode</td><td>Not Configured</td></tr> <tr> <td>Audit Logoff</td><td>Success and Failure</td></tr> <tr> <td>Audit Logon</td><td>Success and Failure</td></tr> <tr> <td>Audit Network Policy Server</td><td>Not Configured</td></tr> <tr> <td>Audit Other Logon/Logoff Events</td><td>Not Configured</td></tr> <tr> <td>Audit Special Logon</td><td>Not Configured</td></tr> </table>	Subcategory	Audit Events	Audit Account Lockout	Failure	Audit User / Device Claims	Not Configured	Audit Group Membership	Success and Failure	Audit IPsec Extended Mode	Not Configured	Audit IPsec Main Mode	Not Configured	Audit IPsec Quick Mode	Not Configured	Audit Logoff	Success and Failure	Audit Logon	Success and Failure	Audit Network Policy Server	Not Configured	Audit Other Logon/Logoff Events	Not Configured	Audit Special Logon	Not Configured
Subcategory	Audit Events																								
Audit Account Lockout	Failure																								
Audit User / Device Claims	Not Configured																								
Audit Group Membership	Success and Failure																								
Audit IPsec Extended Mode	Not Configured																								
Audit IPsec Main Mode	Not Configured																								
Audit IPsec Quick Mode	Not Configured																								
Audit Logoff	Success and Failure																								
Audit Logon	Success and Failure																								
Audit Network Policy Server	Not Configured																								
Audit Other Logon/Logoff Events	Not Configured																								
Audit Special Logon	Not Configured																								

İlgili kurala ait Log örneği aşağıdaki gibidir;

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
- Subscriptions

Security Number of events: 27

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	11/2/2018 11:20:42 AM	Micros...	4627	Group Membership
Audit Success	11/2/2018 11:20:42 AM	Micros...	4624	Logon

Event Properties - Event 4627, Microsoft Windows security auditing.

General Details

Group Membership:

- HD\Domain Users
- Everyone
- BUILTIN\Users
- BUILTIN\Administrators
- NT AUTHORITY\INTERACTIVE
- CONSOLE LOGON
- NT AUTHORITY\Authenticated Users
- NT AUTHORITY\This Organization
- LOCAL
- HD\Group Policy Creator Owners
- HD\Domain Admins
- HD\Enterprise Admins

Log Name: Security

Source: Microsoft Windows security

Event ID: 4627

Level: Information

User: N/A

OpCode: Info

Logged: 11/2/2018 11:20:42 AM

Task Category: Group Membership

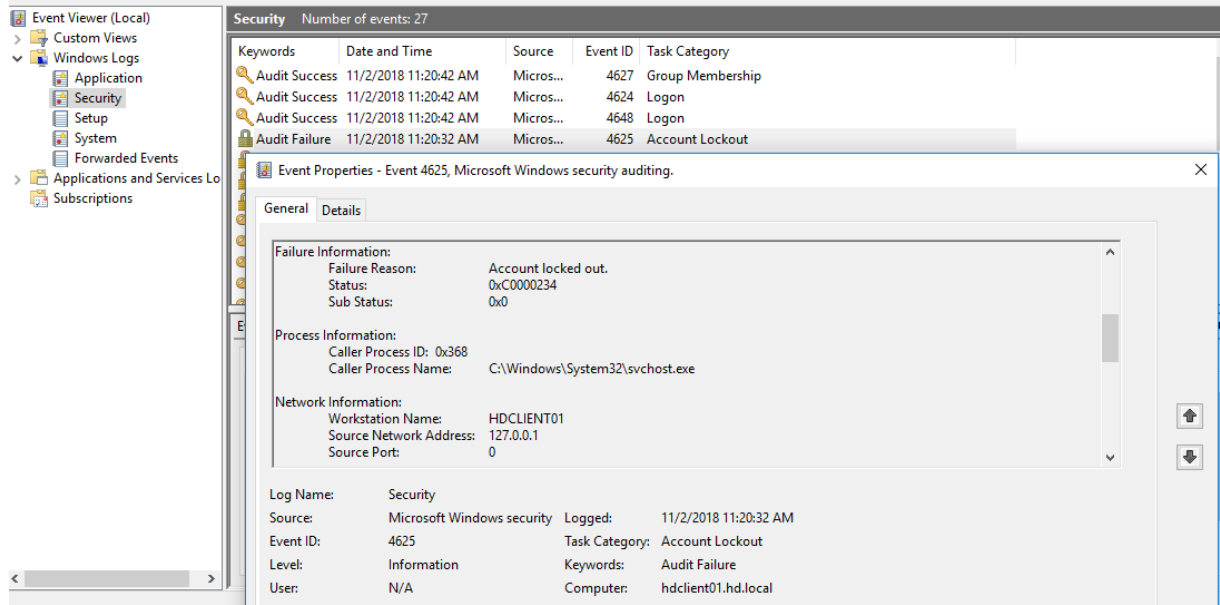
Keywords: Audit Success

Computer: hdclient01.hd.local

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-group-membership>

Audit Account Lockout

Konular içerisinde sanırım en bilinen gpo ayarlarından biridir desem yanlış olmaz. İlgili kural ile belirli sayıda yanlış şifre girildiğinde hesabı bloke edilen kullanıcının Log'lanması sağlanmaktadır ve aşağıdaki Log üretilmektedir. İlgili kural özellikle yetkili kullanıcılar ( Domain Admin, Backup Admin, Database Admin , servis hesapları ) için **Failure** olarak yapılandırılmalıdır.



Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-account-lockout>

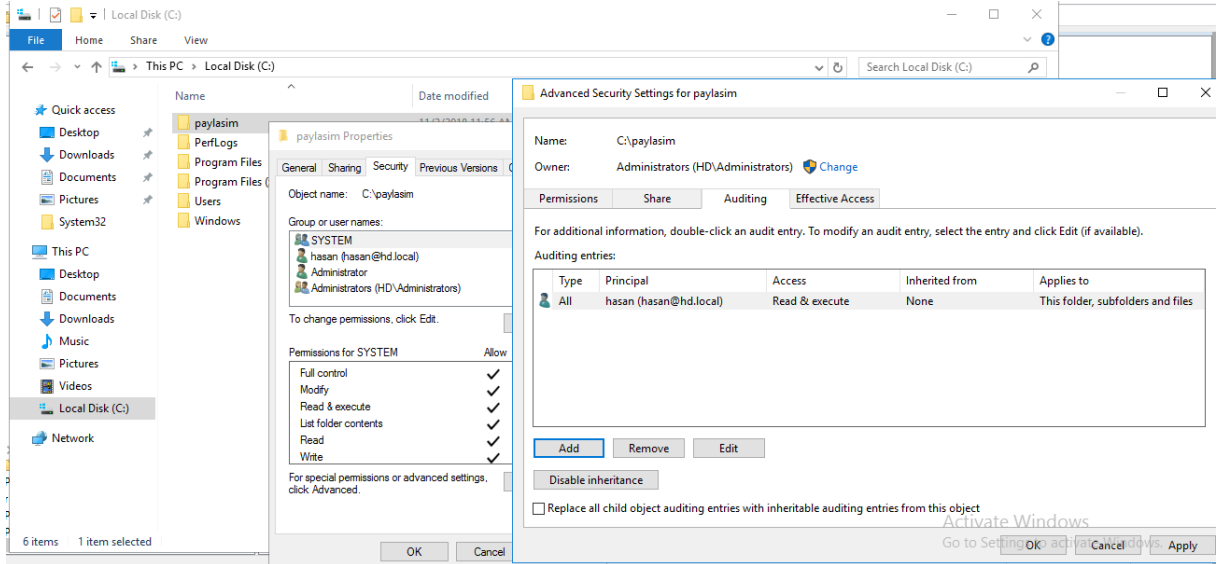
## Object Access

### Audit File System

Dosya sistemine erişim denemeleri Log'lanmaktadır. Bu kuralın yapılandırılması ile birlikte herhangi bir objenin silinmesi veya izin değişiklikleri Log'lanabilmektedir. İlgili kuralı **Success ve Failure** olarak yapılandırılması tavsiye edilmektedir.

> Restricted Groups	Subcategory	Audit Events
> System Services	[Not Configured] Audit Application Generated	Not Configured
> Registry	[Not Configured] Audit Certification Services	Not Configured
> File System	[Not Configured] Audit Detailed File Share	Not Configured
> Wired Network (IEEE 802.3) Policies	[Not Configured] Audit File Share	Not Configured
> Windows Firewall with Advanced Security	[Not Configured] Audit File System	Success and Failure
> Network List Manager Policies	[Not Configured] Audit Filtering Platform Connection	Not Configured
> Wireless Network (IEEE 802.11) Policies	[Not Configured] Audit Filtering Platform Packet Drop	Not Configured
> Public Key Policies	[Not Configured] Audit Handle Manipulation	Not Configured
> Software Restriction Policies	[Not Configured] Audit Kernel Object	Not Configured
> Application Control Policies	[Not Configured] Audit Other Object Access Events	Not Configured
> IP Security Policies on Active Directory	[Not Configured] Audit Registry	Not Configured
> Advanced Audit Policy Configuration	[Not Configured] Audit Removable Storage	Not Configured
> Audit Policies	[Not Configured] Audit SAM	Not Configured
> Account Logon	[Not Configured] Audit Central Access Policy Staging	Not Configured
> Account Management		
> Detailed Tracking		
> DS Access		
> Logon/Logoff		
> Object Access		

İlgili kuralın yapılandırılması ile işimiz malesef bitmiyor. Yapmamız gereken ek bir adım da hangi klasör üzerinde denetim sağlayacaksa auditing altında ilgili kullanıcıyı eklememiz gerekmektedir.



Yapılandırmamız tamamlandıktan sonra üretilen Log'lar aşağıdaki gibi olacaktır.

Security Number of events: 21				
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	11/2/2018 12:21:22 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:22 PM	Microsoft Windows security auditing.	4663	File System
Audit Success	11/2/2018 12:21:22 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:22 PM	Microsoft Windows security auditing.	4663	File System
Audit Success	11/2/2018 12:21:22 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:22 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:13 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:13 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:13 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:13 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:13 PM	Microsoft Windows security auditing.	4663	File System
Audit Success	11/2/2018 12:21:13 PM	Microsoft Windows security auditing.	4663	File System
Audit Success	11/2/2018 12:21:13 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:13 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:13 PM	Microsoft Windows security auditing.	4656	File System
Audit Success	11/2/2018 12:21:12 PM	Microsoft Windows security auditing.	4656	File System

Log'un detayını incelediğimde hasan kullanıcısının hd.txt üzerinde okuma yaptığını anlıyorum.

Event Properties - Event 4656, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:

Security ID: HD\hasan  
Account Name: hasan  
Account Domain: HD  
Logon ID: 0xA66A5F

Object:

Object Server: Security  
Object Type: File  
Object Name: C:\paylasim\hd.txt  
Handle ID: 0xdc4  
Resource Attributes: -

Process Information:

Process ID: 0x4  
Process Name:

Access Request Information:

Transaction ID: {00000000-0000-0000-0000-000000000000}  
Accesses: ReadAttributes

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4656  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 11/2/2018 12:21:22 PM  
Task Category: File System  
Keywords: Audit Success  
Computer: dc01.hd.local

İlgili kural ihtiyaca göre istemci ve sunucu tarafında aktif edilebilir.



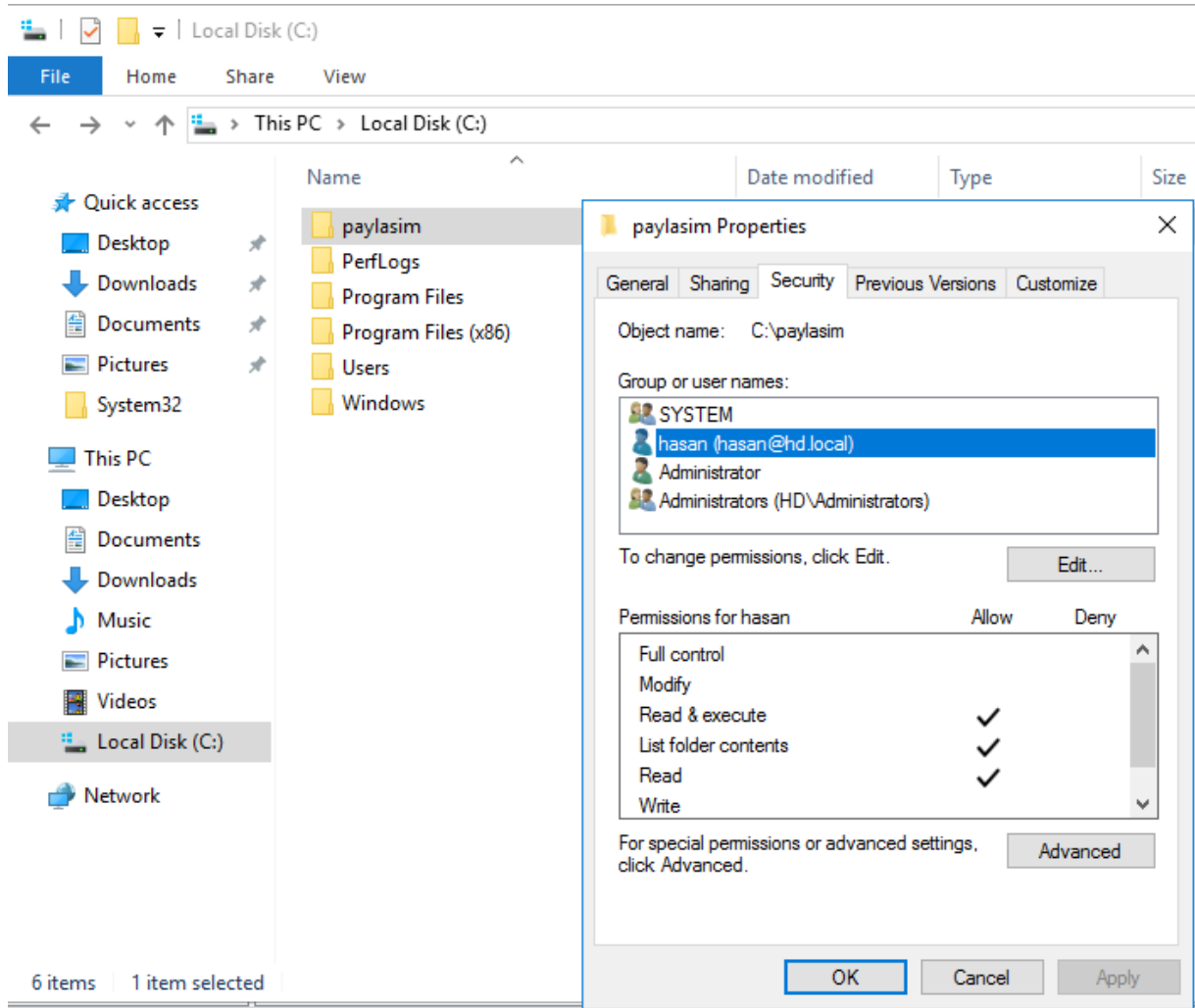
Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-file-system>

## Audit File Share

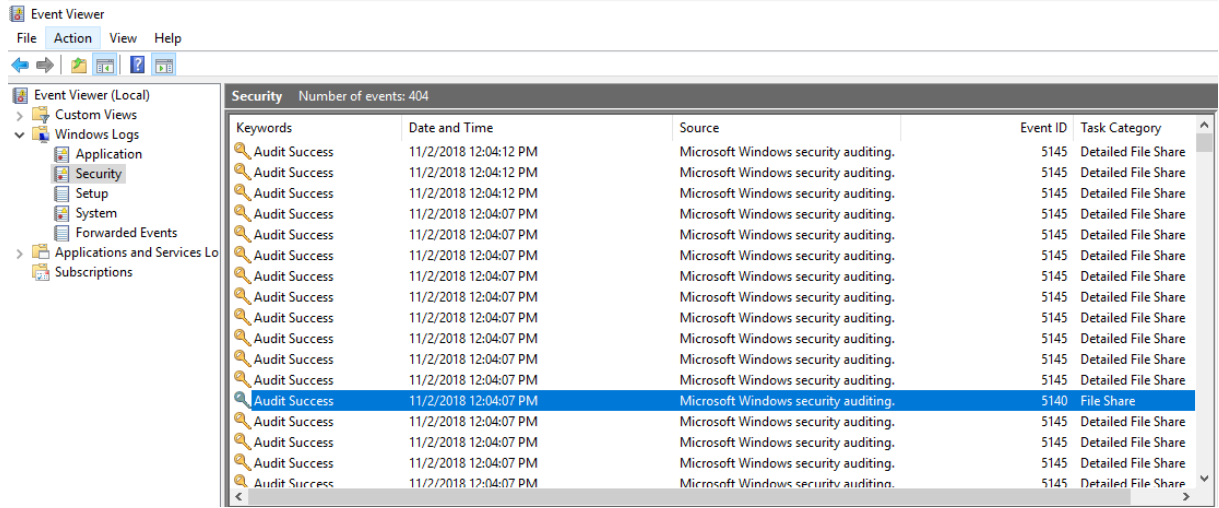
İlgili kural dosya paylaşımları, oluşturma, değiştirme veya silme gibi işlemlerin denetlenmesini ve Log'lanmasını sağlamaktadır. Aynı zamanda hangi kaynağa erişildi, kaynak ip ve port bilgisi ile Log'lanmaktadır. İlgili kuralın **success ve Failure** olarak özellikle dosya sunucuları ve Domain Controller lar üzerinde yapılandırılması tavsiye edilmektedir.

Security Settings	Subcategory	Audit Events
> Account Policies	Audit Application Generated	Not Configured
> Local Policies	Audit Certification Services	Not Configured
> Event Log	Audit Detailed File Share	Not Configured
> Restricted Groups	Audit File Share	Success and Failure
> System Services	Audit File System	Not Configured
> Registry	Audit Filtering Platform Connection	Not Configured
> File System	Audit Filtering Platform Packet Drop	Not Configured
> Wired Network (IEEE 802.3)	Audit Handle Manipulation	Not Configured
> Windows Firewall with Advanced Security	Audit Kernel Object	Not Configured
> Network List Manager Policies	Audit Other Object Access Events	Not Configured
> Wireless Network (IEEE 802.11)	Audit Registry	Not Configured
> Public Key Policies	Audit Removable Storage	Not Configured
> Software Restriction Policies	Audit SAM	Not Configured
> Application Control Policies	Audit Central Access Policy Staging	Not Configured
> IP Security Policies on Incoming Traffic		
> Advanced Audit Policy Configuration		
> Audit Policies		
> Account Logon		
> Account Management Events		
> Detailed Tracking		
> DS Access		
> Logon/Logoff		
> Object Access		

Örneğimizde paylaşım klasörü üzerinde hasan kullanıcısının hakları aşağıdaki gibidir.

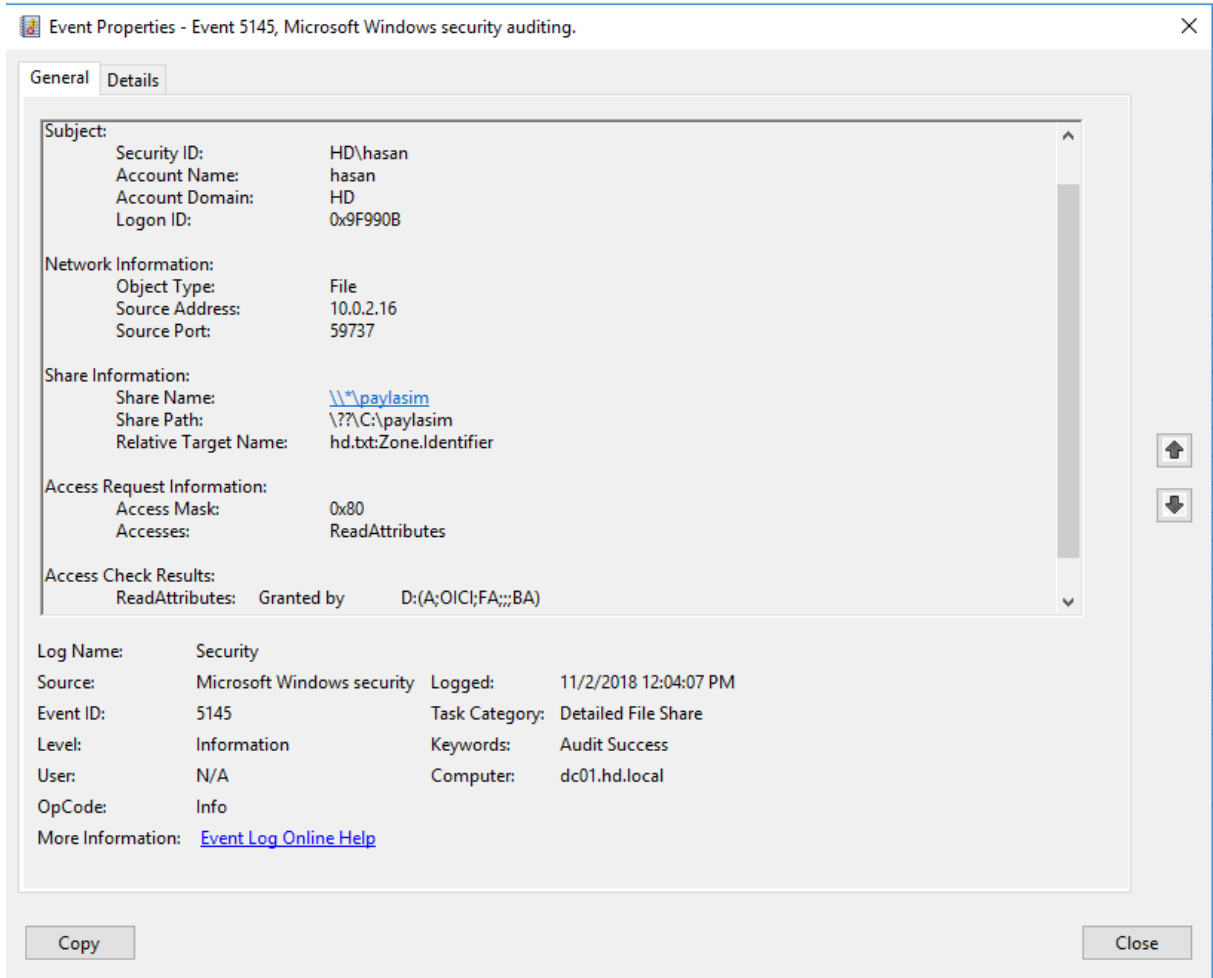


Hasan kullanıcım ile ilgili dosyaya erişmek istediğimde aşağıdaki Log'un üretildiğini gözlemliyorum.



Access Mask ın 0x80 olması dosya üzerinde kullanıcının okuma yetkisi olduğunu ifade etmektedir. Hasan kullanıcısının hangi ip üzerinden eriştiği ve kullandığı port da artık Log'lanabilmektedir.

ReadAttributes	0x80	Okuma hakkı olduğunu ifade eder
WriteAttributes	0x100	Yazma hakkı olduğunu ifade eder.
Delete	0x10000	Silme hakkı olduğunu ifade eder

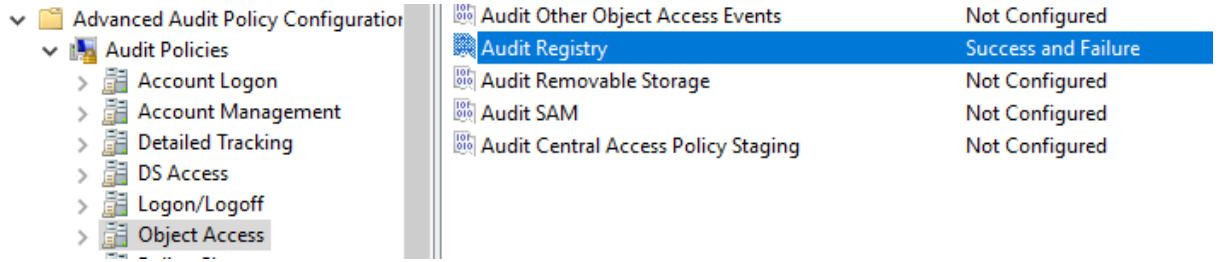


Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-file-share>

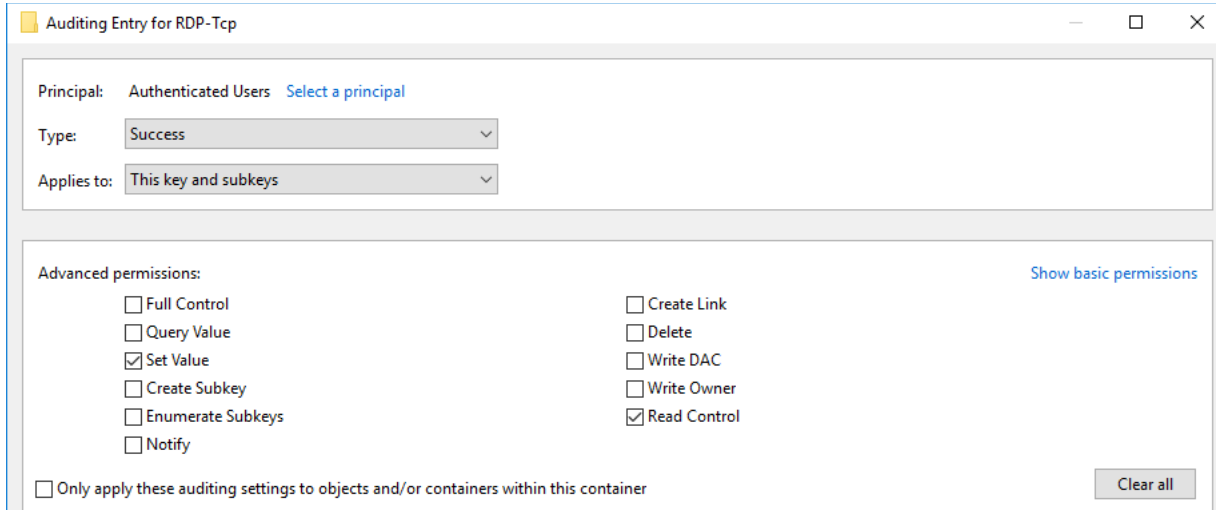
<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5145>

## Audit Registry

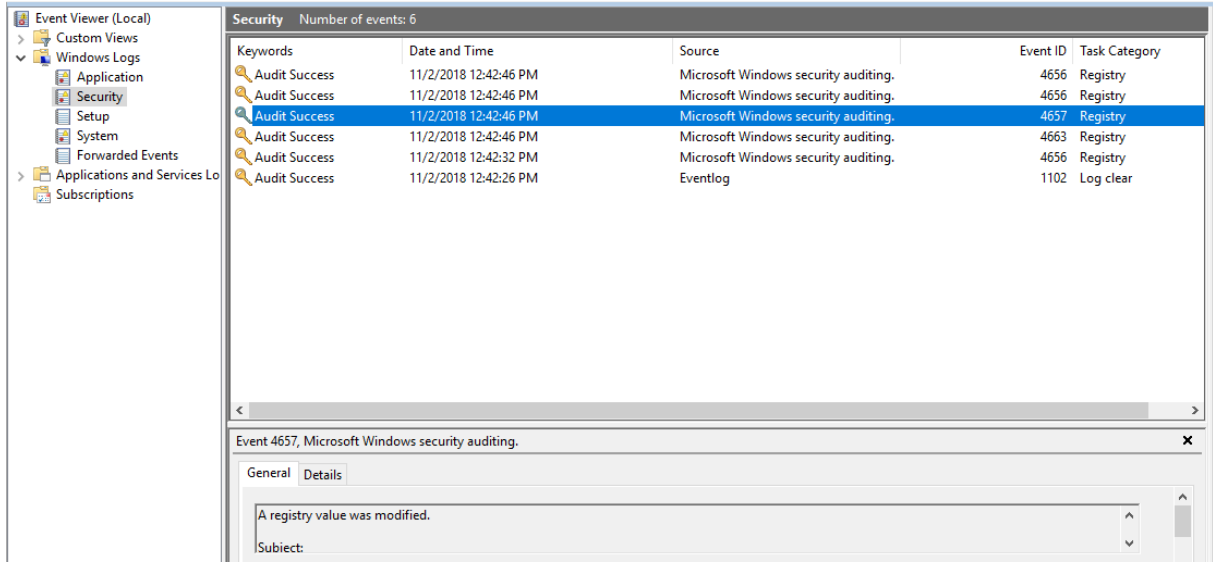
Registry kayıtlarındaki herhangi bir değişikliği Log'lamak için ilgili kuralın yapılandırılması gerekmektedir. İlgili kural için **success**, **failure** şeklinde yapılandırabilirsiniz. İlgili kuralın yapılandırılması Access List e göre değişiklik gösterebilir. Kural yapılandırılan Log'un çok fazla şişmemesi de son derece önemli ve ilgili kuralın nerede yapılandırılacağı ihtiyaca göre değişebilir.



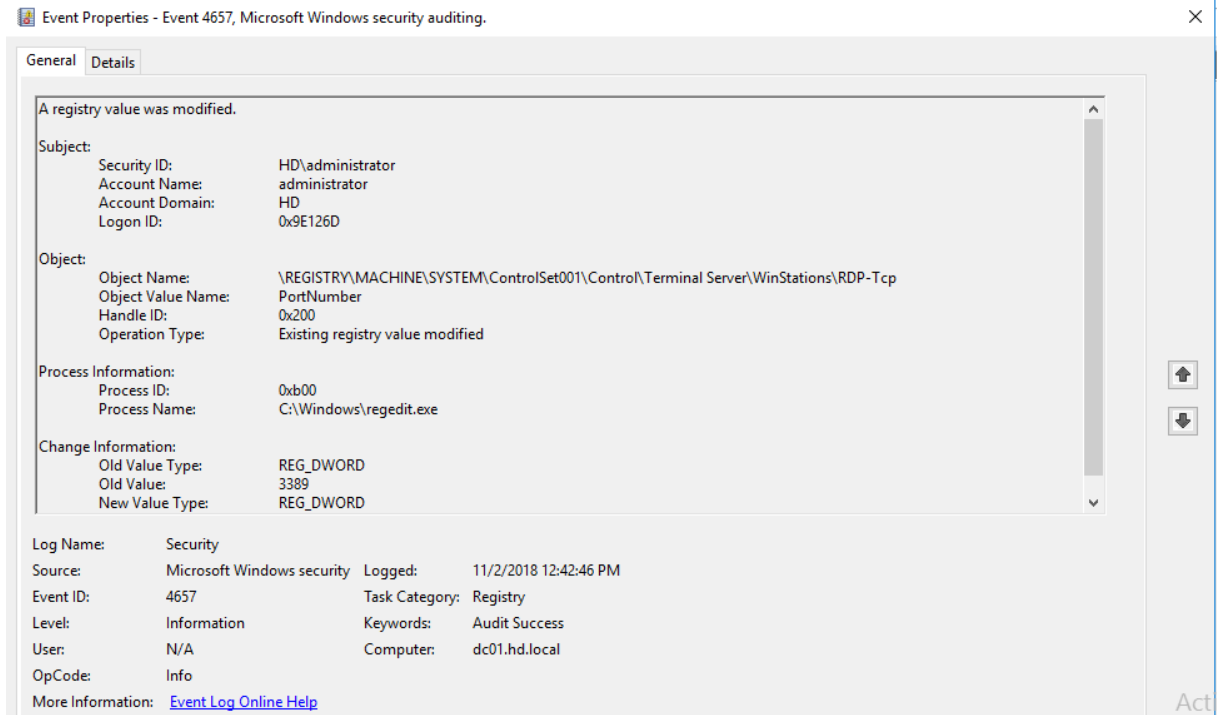
Kuralımızı yapılandırdıktan sonra hangi registry kaydı üzerindeki değişikliği Log'lamak istiyorsak ilgili kaydın özellikleri altında yer alan denetim kısmını yapımıza göre yapılandırmamız gerekmektedir.



Örneğimde Registry kaydı içerisinde yer alan RDP-Tcp kaydını değiştirdiğimde oluşan Log'u görüyorum.









Log'un detayını incelediğimde hangi obje üzerinde değişiklik yapıldığını görüyorum.



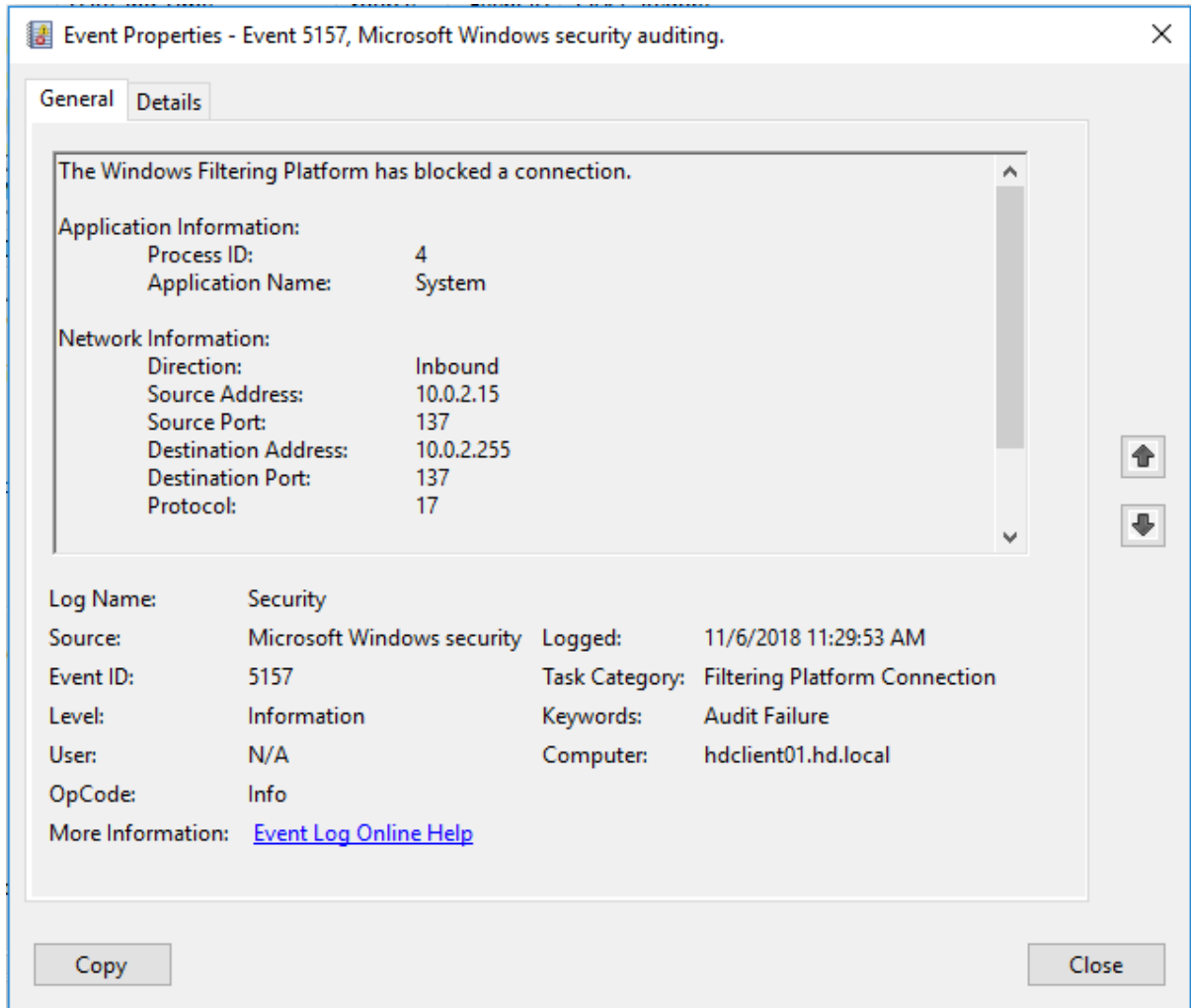
Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-registry>

## Audit Filtering Platform Connection Properties

İzinli veya bloklanan bağlantıları ilgili kural sayesinde Log'layabiliyoruz. İlgili kural eğer Success olarak yapılandırılırsa çok fazla olay üretecektir. Özellikle bloklanan bağlantıları görebilmek için yapılandırılması tavsiye edilmektedir.

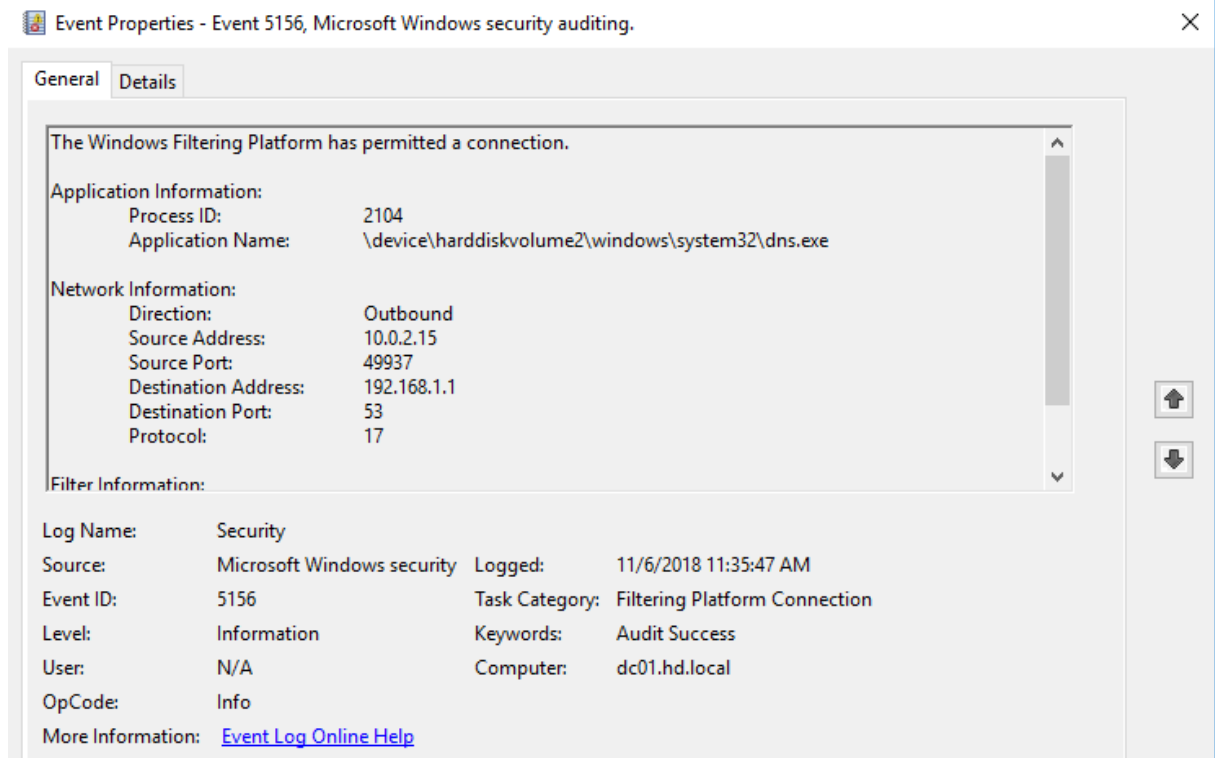
Subcategory	Audit Events
 Audit Application Generated	Not Configured
 Audit Certification Services	Not Configured
 Audit Detailed File Share	Not Configured
 Audit File Share	Not Configured
 Audit File System	Not Configured
 Audit Filtering Platform Connection	Success and Failure

Örneğimizde 10.0.2.255 e 137 portu üzerinden erişemediğimi görüyorum.



Diğer bir örneğimizde ise 192.168.1.1 53 portu ile başarılı şekilde konuştuğumu görüyorum.











Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-filtering-platform-connection>

## Policy Change

### Audit Policy Change

User Right Assignment policy, audit policy veya trust policies de yapılan değişiklikleri ilgili kural ile Log'layabiliyoruz. İlgili kuralın DC ler üzerinde **Success** olarak yapılandırılması tavsiye edilmektedir.

Subcategory	Audit Events
 Audit Audit Policy Change	Success
 Audit Authentication Policy Change	Not Configured
 Audit Authorization Policy Change	Not Configured
 Audit Filtering Platform Policy Change	Not Configured
 Audit MPSSVC Rule-Level Policy Change	Not Configured
 Audit Other Policy Change Events	Not Configured

Örneğimizde Object Access kategorisi içerisinde yer alan Filtering Platform Connection kuralının silindiğini görüyoruz.

Event Properties - Event 4719, Microsoft Windows security auditing.

General Details

System audit policy was changed.

Subject:

Security ID: SYSTEM  
Account Name: DC01\$  
Account Domain: HD  
Logon ID: 0x3E7

Audit Policy Change:

Category: Object Access  
Subcategory: Filtering Platform Connection  
Subcategory GUID: {0cce9226-69ae-11d9-bed3-505054503030}  
Changes: Success removed, Failure removed







Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4719  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 11/7/2018 10:58:19 AM  
Task Category: Audit Policy Change  
Keywords: Audit Success  
Computer: dc01.hd.local














Kaynak: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-policy-change>

## Audit Authentication Policy Change

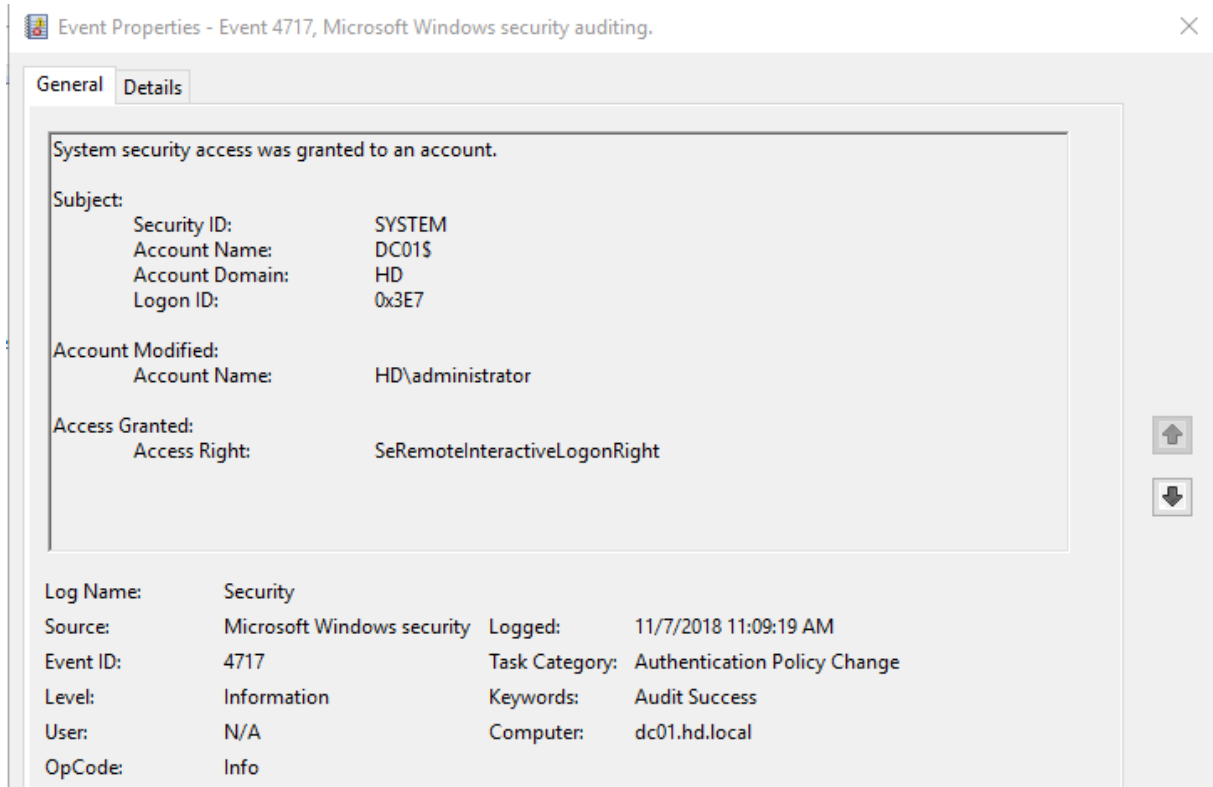
Authentication (kimlik doğrulama) ile ilgili kurallarda deęişiklik olup olmadığını ilgili kural ile Log'layabiliyoruz veya Allow logon locally, Logon as a batch job hakları belirli kiři veya gruplara atanırsa Log'layabiliyoruz. İlgili kuralın **Success** olarak yapılandırılması tavsiye edilmektedir.

Subcategory	Audit Events
 Audit Audit Policy Change	Not Configured
 Audit Authentication Policy Change	Success
 Audit Authorization Policy Change	Not Configured
 Audit Filtering Platform Policy Change	Not Configured
 Audit MPSSVC Rule-Level Policy Change	Not Configured
 Audit Other Policy Change Events	Not Configured

Örneğimizde aşağıdaki kural tanımlanmıştır.

	Policy	Policy Setting
 Audit Policy [DC01.HD.LOCAL] Policy Computer Configuration Policies Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdow Deployed Printers Security Settings Account Policies Local Policies Audit Policy User Rights Assig Security Options	 Access Credential Manager as a trusted caller	Not Defined
	 Access this computer from the network	Not Defined
	 Act as part of the operating system	Not Defined
	 Add workstations to domain	Not Defined
	 Adjust memory quotas for a process	Not Defined
	 Allow log on locally	Not Defined
	 Allow log on through Remote Desktop Services	HD\Administrator
	 Back up files and directories	Not Defined
	 Bypass traverse checking	Not Defined
	 Change the system time	Not Defined
	 Change the time zone	Not Defined
	 Create a pagefile	Not Defined







İlgili deęişiklik ile birlikte oluşan Log'u aşağıda görüyoruz.







Kaynak: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-authentication-policy-change>

### Audit MPSSVC Rule-Level Policy Change

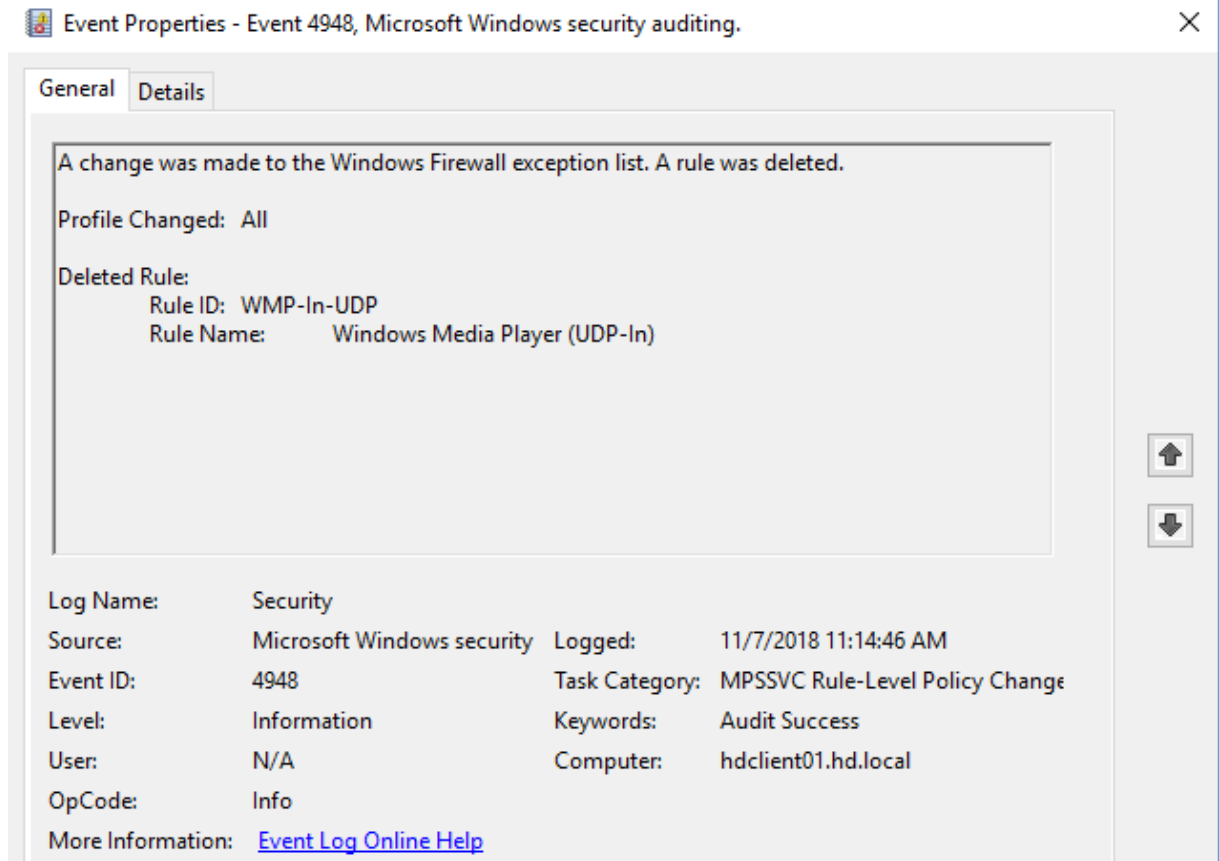
Microsoft Protection servisi Windows Firewall'un bir parçasıdır ve yetkisiz kullanıcıların ağ üzerinden erişimini engeller. Aynı durum internet erişimi için de geçerlidir. İlgili kuralın **Success** olarak yapılandırılması tavsiye edilmektedir. Eğer konfigürasyon ile alakalı sorunlar varsa **Failure** yapılandırılarak Log'lanması sağlanabilir.

Subcategory	Audit Events
 Audit Audit Policy Change	Not Configured
 Audit Authentication Policy Change	Not Configured
 Audit Authorization Policy Change	Not Configured
 Audit Filtering Platform Policy Change	Not Configured
 Audit MPSSVC Rule-Level Policy Change	Success
 Audit Other Policy Change Events	Not Configured

Örneğimizde Inbound Firewall Rules' da Windows Media Player block kuralını sildim.

Inbound Rules					
Name	Group	Profile	Enabled	Acti	
 Windows Media Player (UDP-In)	Windows Media Player	All	Yes	Bloc	
 Windows Media Player x86 (UDP-In)	Windows Media Player	All	Yes	Bloc	
 AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allo	
 AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allo	

İlgili değişikliğin Log'landığını görüyoruz.






Kaynak: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-mpssvc-rule-level-policy-change>

## Privilege Use

### Audit Non Sensitive Privilege Use

Yetkili olmayan kullanıcıların bazı hareketlerini (linkte detayı bulabilirsiniz) Log'layabiliyoruz. İlgili kuralın **Failure** olarak yapılandırılması tavsiye edilmektedir.

Subcategory	Audit Events
 Audit Non Sensitive Privilege Use	Failure
 Audit Other Privilege Use Events	Not Configured
 Audit Sensitive Privilege Use	Not Configured

Örneğimde Change the time zone kuralını set ettim ve istemci makinamda değiştirmeyi denediğimde aşağıdaki Log üretildi.

Event Properties - Event 4673, Microsoft Windows security auditing.

General Details

A privileged service was called.

Subject:

Security ID: LOCAL SERVICE  
Account Name: LOCAL SERVICE  
Account Domain: NT AUTHORITY  
Logon ID: 0x3E5

Service:

Server: Security  
Service Name: -

Process:

Process ID: 0x354  
Process Name: C:\Windows\System32\svchost.exe

Service Request Information:

Privileges: SeProfileSingleProcessPrivilege

Log Name: Security

Source: Microsoft Windows security Logged: 11/7/2018 11:41:00 AM

Event ID: 4673 Task Category: Non Sensitive Privilege Use

Level: Information Keywords: Audit Failure

User: N/A Computer: hdclient01.hd.local

OpCode: Info

More Information: [Event Log Online Help](#)




Kaynak: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-non-sensitive-privilege-use>

## Audit Sensitive Privilege Use

İlgili kural aşağıdaki hassas ayrıcalıklardaki değişikliğin Log'lanmasını sağlamaktadır.

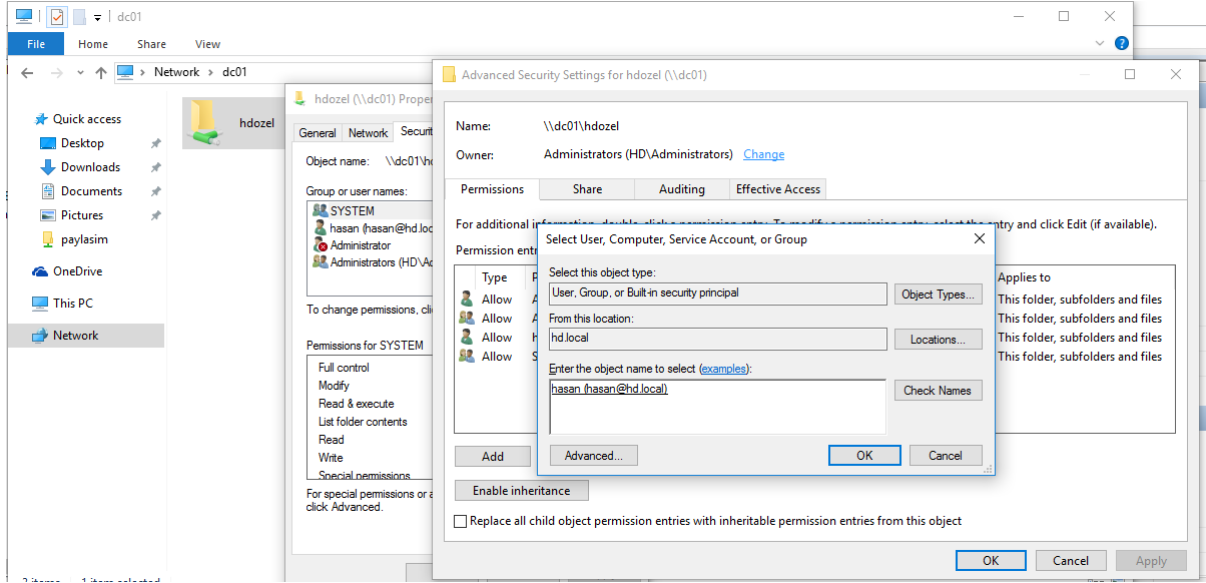
- Act as part of the operating system
- Back up files and directories
- Restore files and directories
- Create a token object
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Generate security audits
- Impersonate a client after authentication
- Load and unload device drivers
- Manage auditing and security log
- Modify firmware environment values
- Replace a process-level token
- Take ownership of files or other objects

İlgili kuralın **Success, Failure** olarak yapılandırılması tavsiye edilmektedir.

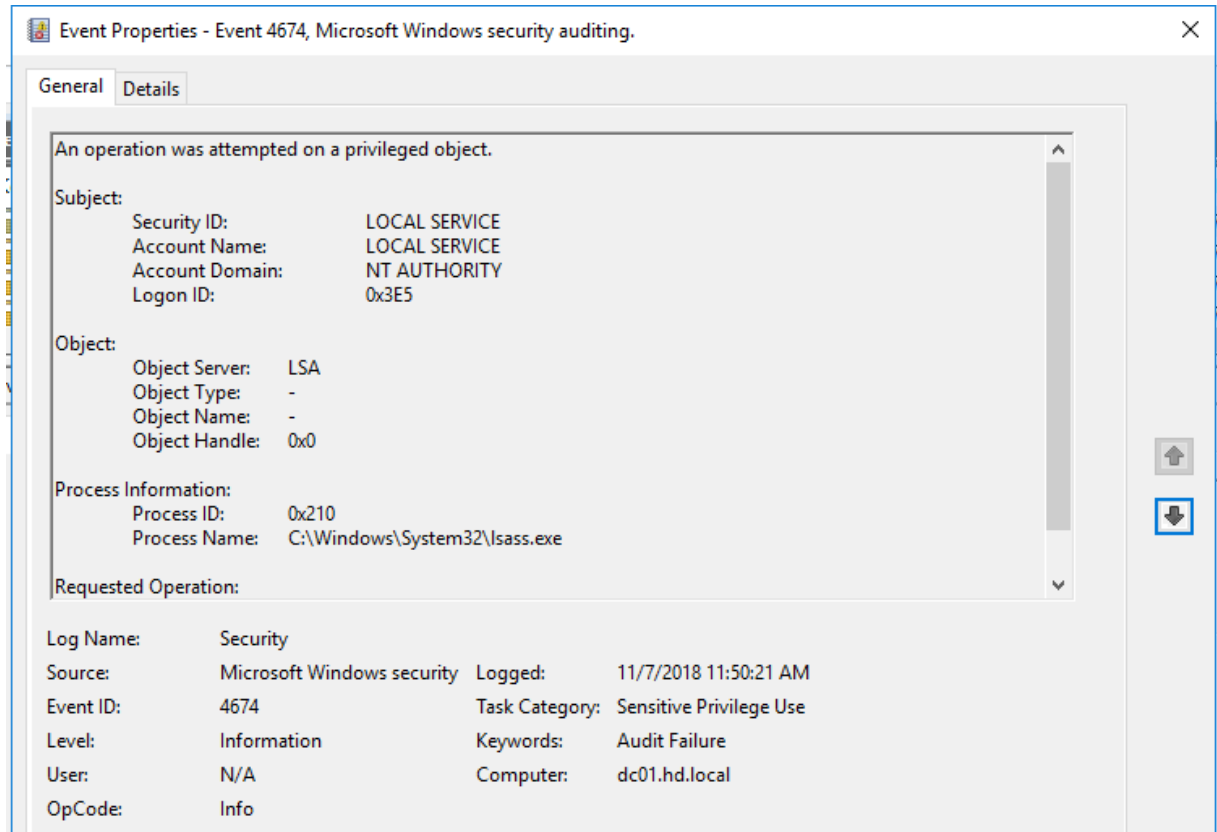
Subcategory	Audit Events
 Audit Non Sensitive Privilege Use	Not Configured
 Audit Other Privilege Use Events	Not Configured
 Audit Sensitive Privilege Use	Success and Failure

Örneğimde DC01 sunucum üzerinde hdozel isimli dosyamanın sahipliğini değiştirmeye çalışıyorum.

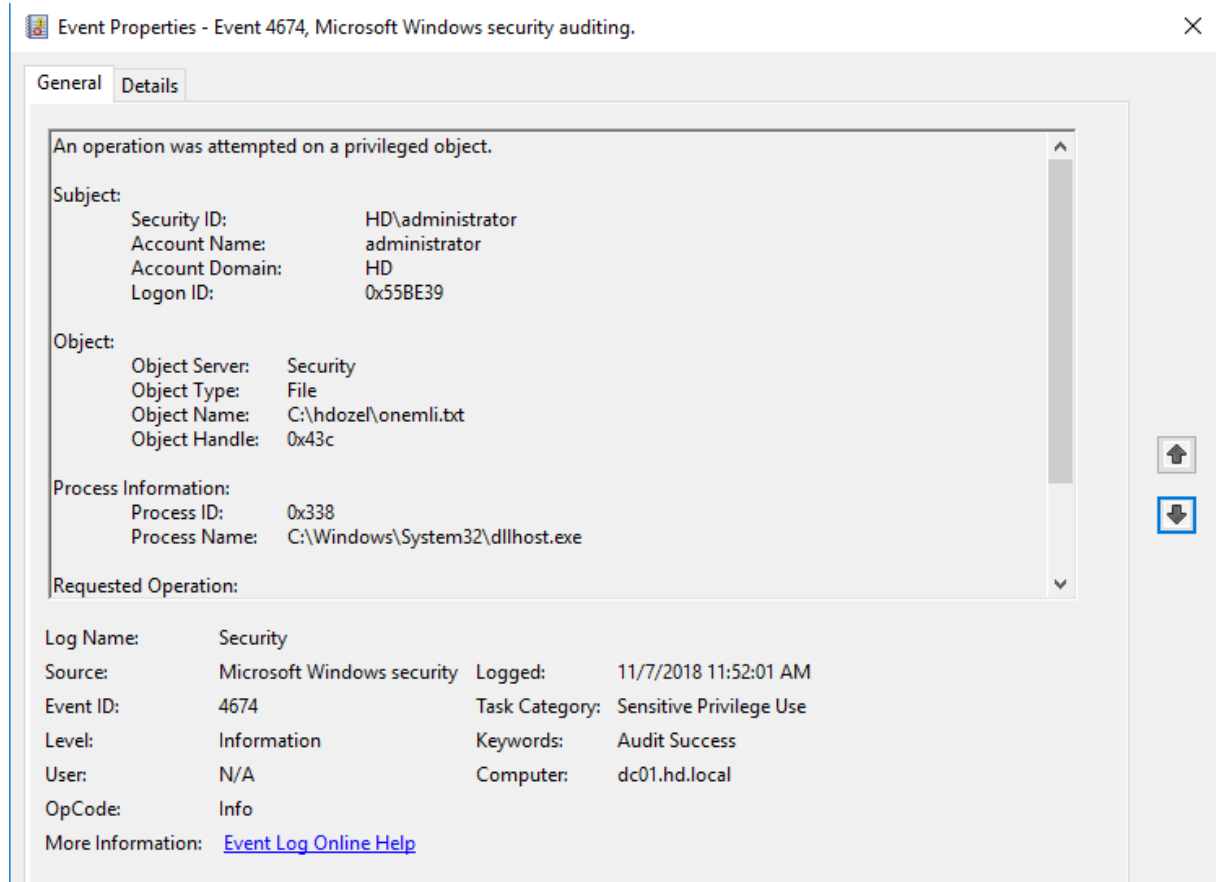




İlgili hareket sonucunda aşağıdaki Log'un üretildiğini görüyorum ve yetkisiz işlem yapıldığı için başarısız olduğunu gözlemliyorum.



Yetkili kullanıcım ile aynı işlemi tekrar yaptığımda ise aşağıdaki Log'un üretildiğini görüyorum. Aynı zamanda hangi dosya üzerinde işlem yapıldığını da görebiliyorum.



Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-sensitive-privilege-use>

## Active Directory için Tavsiye Edilen Log'lama Ayarları

### Tavsiye Edilen Minimum Denetim Kuralı

S: Success

F: Failure ü ifade etmektedir.

Category

Subcategory

Audit Settings

Account Logon	Credential Validation	S & F
Account Management	Security Group Management	S & F
Account Management	User Account Management	S & F
Account Management	Computer Account Management	S & F
Account Management	Other Account Management Events	S & F
Detailed Tracking	Audit DPAPI Activity	S & F
Detailed Tracking	Audit PNP Activity	S & F
Detailed Tracking	Process Creation	S
Detailed Tracking	Process Termination	S
Logon / Logoff	Logon	S & F
Logon / Logoff	Logoff	S
Logon / Logoff	Other Logon/Logoff Events	S & F
Logon / Logoff	Special Logon	S & F
Logon / Logoff	Account Lockout	S
Object Access	File Share	S
Object Access	Removable Storage	S
Policy Change	Audit Policy Change	S & F
Policy Change	MPSSVC Rule-Level Policy Change	S & F
Policy Change	Other Policy Change Events	S & F
Policy Change	Authentication Policy Change	S & F
Policy Change	Authorization Policy Change	S & F
System	Security State Change	S & F
System	Security System Extension	S & F
System	System Integration	S & F

Kaynak : <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

### Tavsiye Edilen NTLM Audit Events

Category	Subcategory	Audit Settings
Account Logon	Credential Validation	S & F
Account Management	Security Group Management	S & F
Account Management	User Account Management	S & F

## Azure Security Center ile Log'ların Anlamlandırılması

Azure Security Center ile ilgili detay bilgiyi [Windows Güvenliği' nin Kara Kutusu](#) isimli E-Kitabımda bulabilirsiniz. Bölüm içerisinde Azure Security Center' a sunucumu nasıl bağladım gibi kavramlar işlenmeyecektir.

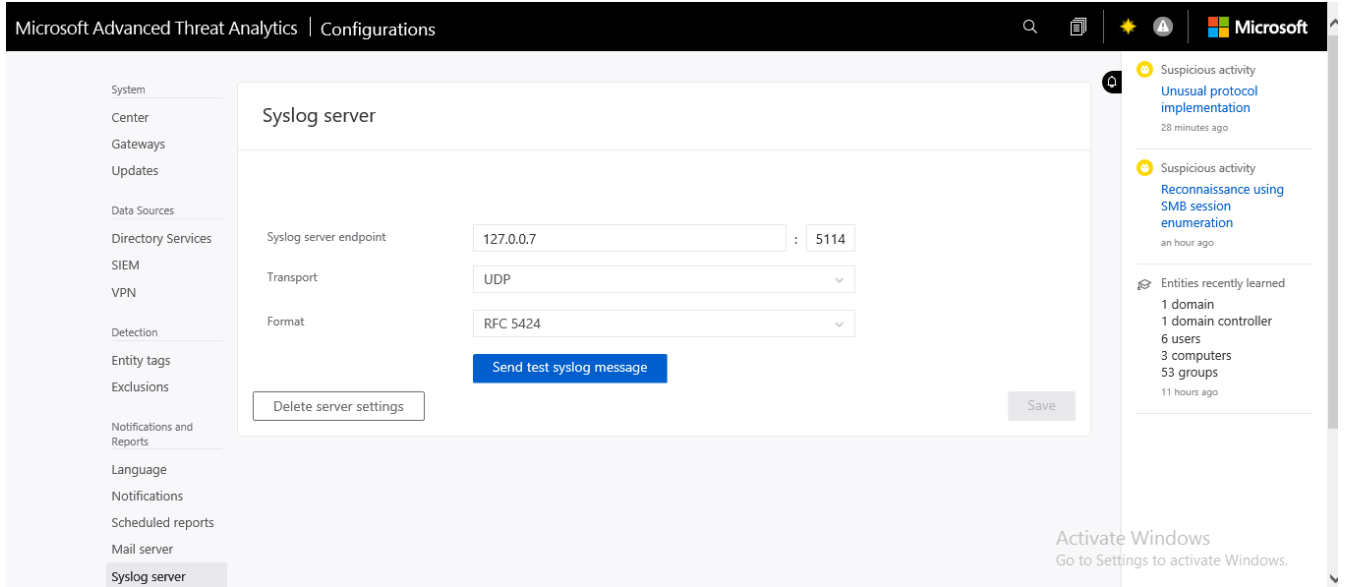
Bu bölümümüzde ise güvenlik Log'larını nasıl Azure Security Center' a gönderebiliriz, bir olay oluşması durumunda nasıl alarm oluşur gibi kavramları işleyeceğiz.

Eğer yapınızda kurulu hali hazırda Microsoft ATA ürünü var ise işimiz birazcık daha kolaylaşıyor. Bildiğiniz üzere Microsoft ATA Active Directory ortamlarını izleyip anormal bir davranış olması durumunda bize alarm üreten bir araç.

Senaryomuzda Microsoft ATA' nın kurulu olduğu varsayılmıştır. Bildiğiniz üzere Microsoft ATA Log'larını Azure' a gönderebiliyoruz. Bunun için Microsoft ATA tarafında yapılması gereken iki adım var. Birincisi monitoring ajanının kurulması ve ikincisi ise aşağıdaki gibi Syslog Server ayarlarının aşağıdaki şekilde yapılandırılması ve elbette sabır 😊

Eğer ATA mevcut değilse diğer SIEM ürünleri ile de benzer şekilde Azure' a Log'ları yönlendirebiliyoruz. Bu tarz ürünler merkezi olarak Log'ları topladığı için işimizi de kolaylaştırmış oluyor. Diğer bir seçenek ise aşağıdaki kaynaktaki adımları uygulamak olabilir.

<https://docs.microsoft.com/tr-tr/advanced-threat-analytics/configure-event-collection>



Örneğimizde mimikatz ile Windows 10 istemci makina üzerinde oturum açmış olan Domain Admin' in ntlm hash bilgisini yakalıyorum ve bunu DC01 isimli domain controller makinama erişim için kullanıyorum. ( Amacım mimikatz ile hash nasıl çalınır vs olmadığı için detaylıca anlatmıyorum,internette çok faydalı kaynaklar mevcut) Daha sonra **dir** komutu ile dc01 makinasının dosya yoluna gidebildim.

```
mimikatz 2.1.1 x64 (oe.oe)
* Domain : HD
* Password : (null)
kerberos :
* Username : hdcclient01$
* Domain : HD.LOCAL
* Password : (null)
ssp :
credman :

mimikatz # sekurlsa::pth /user:administrator /ntlm:c39f2b3d2ec06a62cb887fb391dee0
user : administrator
domain : hd.local
program : cmd.exe
impers. : no
NTLM : c39f2b3d2ec06a62cb887fb391dee0
PID 1876
TID 4812
LSA Process is now R/W
LUID 0 ; 16061296 (00000000:00f51370)
msv1_0 - data copy @ 0000029094D2F500 : OK !
kerberos - data copy @ 0000029094F69988
aes256_hmac -> null
aes128_hmac -> null
rc4_hmac_nt OK
rc4_hmac_old OK
rc4_md4 OK
rc4_hmac_nt_exp OK
rc4_hmac_old_exp OK
*Password replace @ 0000029094F86718 (32) -> null

mimikatz #

Administrator: C:\Windows\SYSYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
hdcclient01\ghost

C:\Windows\system32>dir \\dc01\c$
Volume in drive \\dc01\c$ has no label.
Volume Serial Number is 9822-016F

Directory of \\dc01\c$

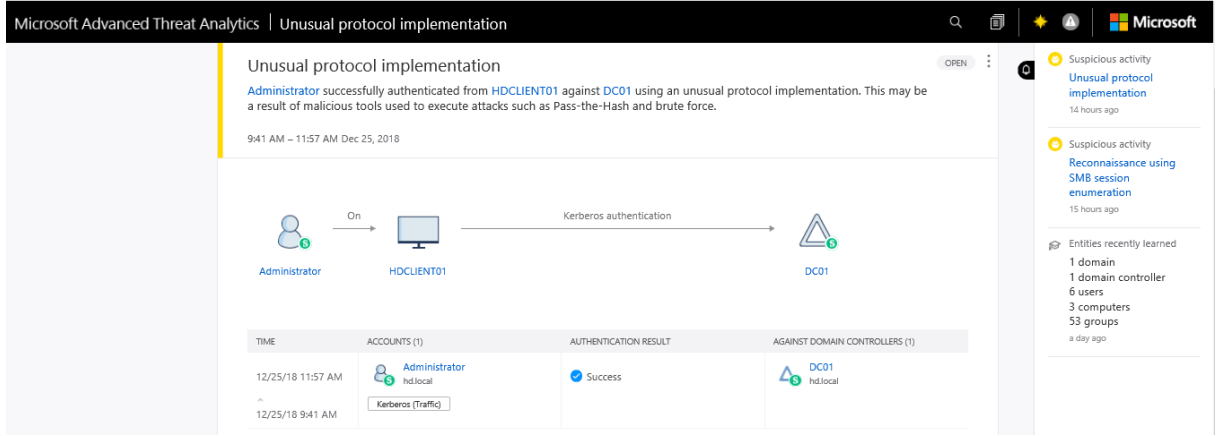
11/07/2018 11:45 AM <DIR> hdozel
07/16/2016 05:23 AM <DIR> PerfLogs
12/20/2018 11:00 PM <DIR> Program Files
10/30/2018 03:03 AM <DIR> Program Files (x86)
12/24/2018 11:31 PM <DIR> TLogs
10/30/2018 05:19 AM <DIR> Users
12/21/2018 01:03 PM <DIR> WER
10/30/2018 02:14 AM <DIR> Windows
0 File(s) 0 bytes
8 Dir(s) 46,721,245,184 bytes free

C:\Windows\system32>klist
Current LogonId is 0:0xf51370

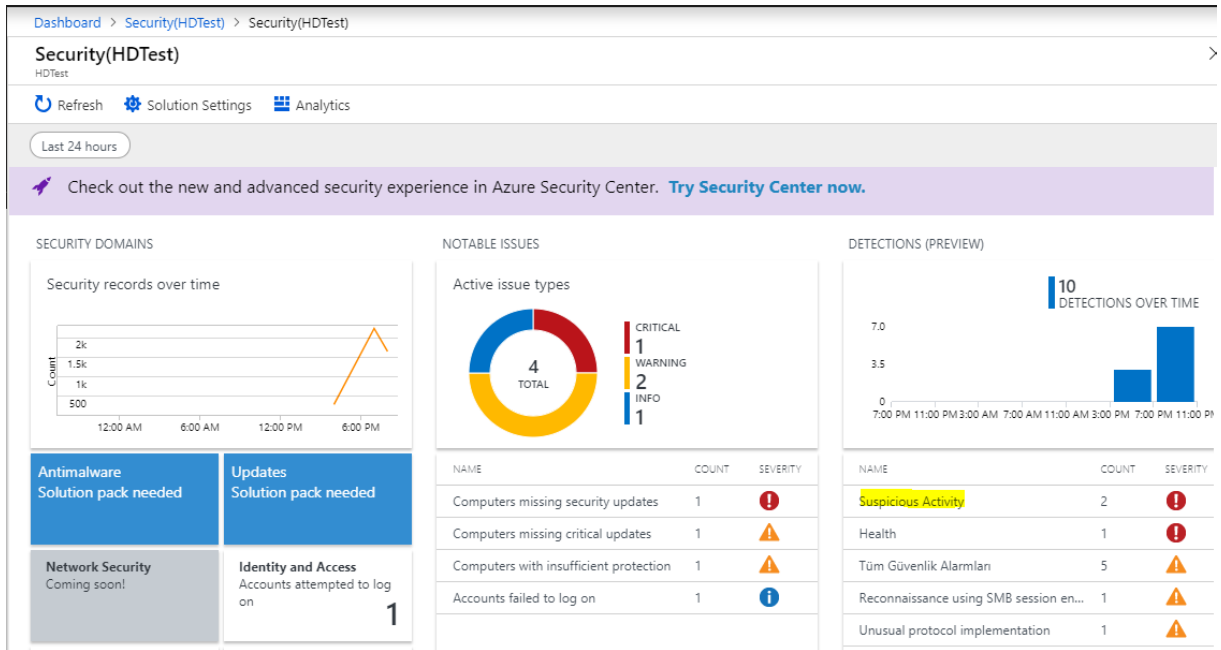
Cached Tickets: (3)

#0> Client: administrator @ HD.LOCAL
Server: krbtgt/HD.LOCAL @ HD.LOCAL
Kerberos Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_auth name_canonicalize
Start Time: 12/25/2018 9:41:31 (local)
End Time: 12/25/2018 19:41:31 (local)
Renew Time: 1/1/2019 9:41:31 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
```

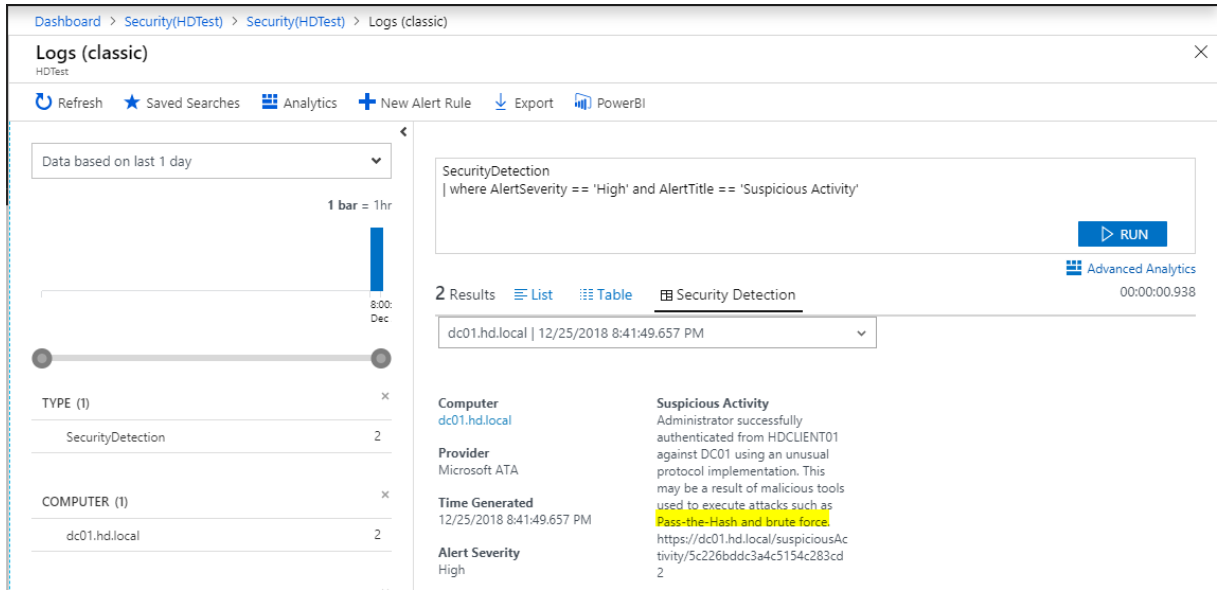
Microsoft ATA tarafına baktığımda ise Pass-the-hash atağı olduğunu belirtiyor.



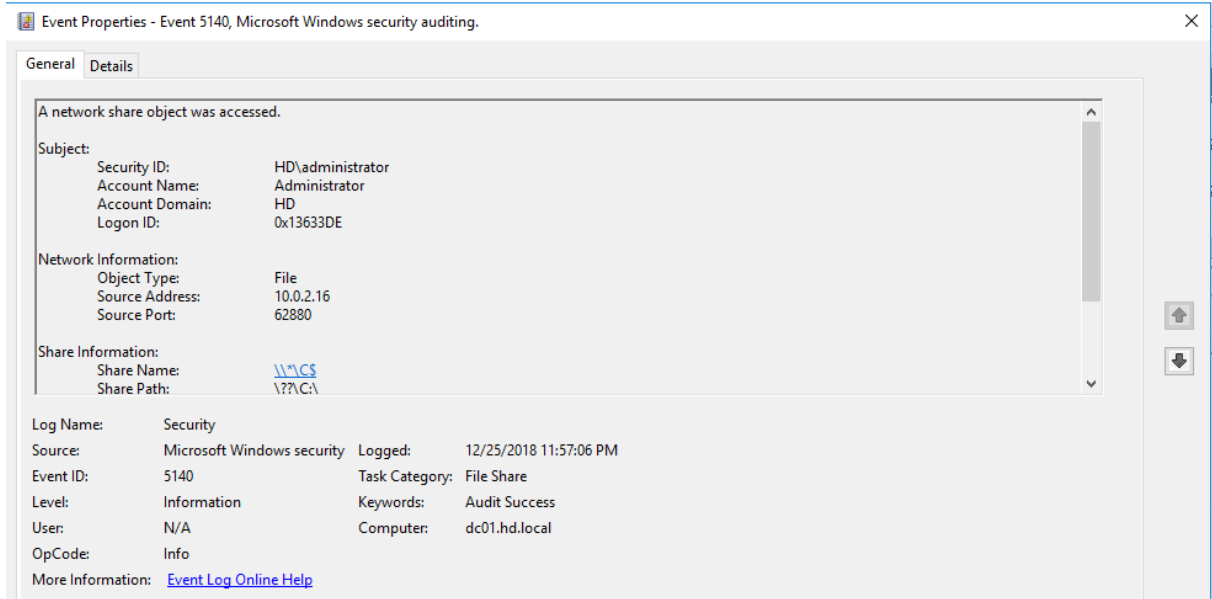
Microsoft Azure tarafında OMS içerisinde yer alan **Security'** e geldiğimizde ise Suspicious Activity algılandı.



Log'un detayını incelediğimizde ise Pass-the-hash atağı olabileceğini belirtiyor.



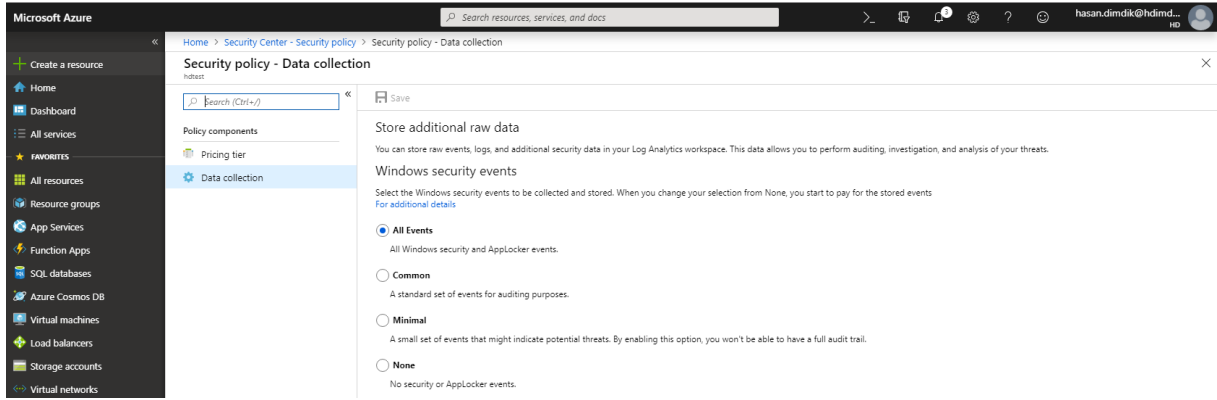
Diğer taraftan birde event Log'a bakalım. Eventviewer dan ilgili Log'a baktığımda aslında erişenin administrator olduğunu belirtiyor. Sizcede biraz garip değil mi ? **whoami** komutu çalıştırdığımda ghost olarak gözüküyordum. Bildiğiniz üzere bunun sebebi administrator un hash bilgisini çalmış olmam. Sanırım bu görüntüden neden Domain Admin hesabı ile istemci veya sunucu makinalarına bağlanmamız gerektiğini bir defa daha anlamış oluyoruz !



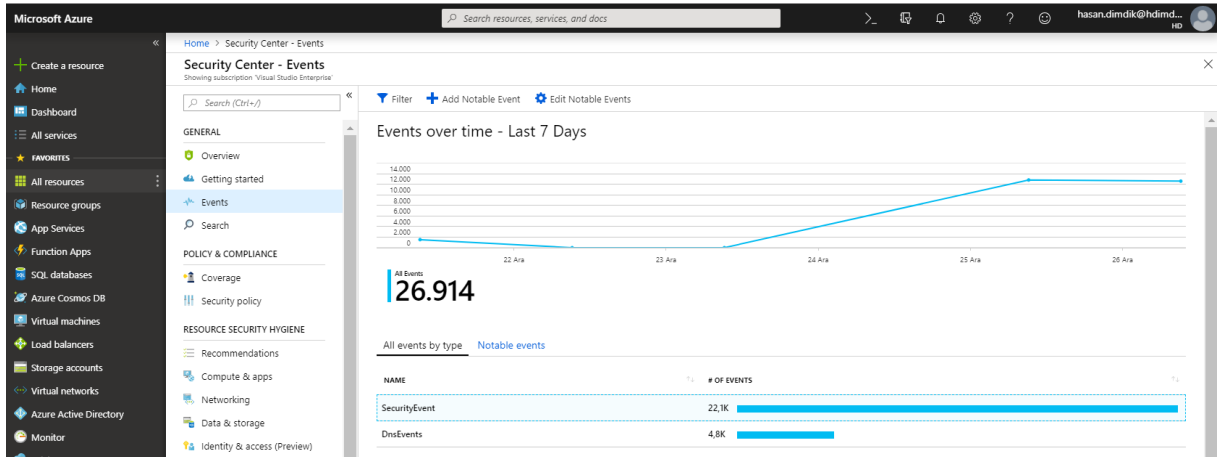
## Azure Security Center – Events

Azure Security Center’ da hangi Log’ların toplanacağını aşağıdaki bölümde belirliyoruz. **Security Center > Security Policy > Security policy – Data Collection** sekmesinde toplayacağımız Log’un seviyesini belirliyoruz. Hangi seçenek benim için uygundur diye aklınızda soru var ise aşağıdaki kaynak son derece faydalı olacaktır.

Kaynak : <https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection#data-collection-tier>



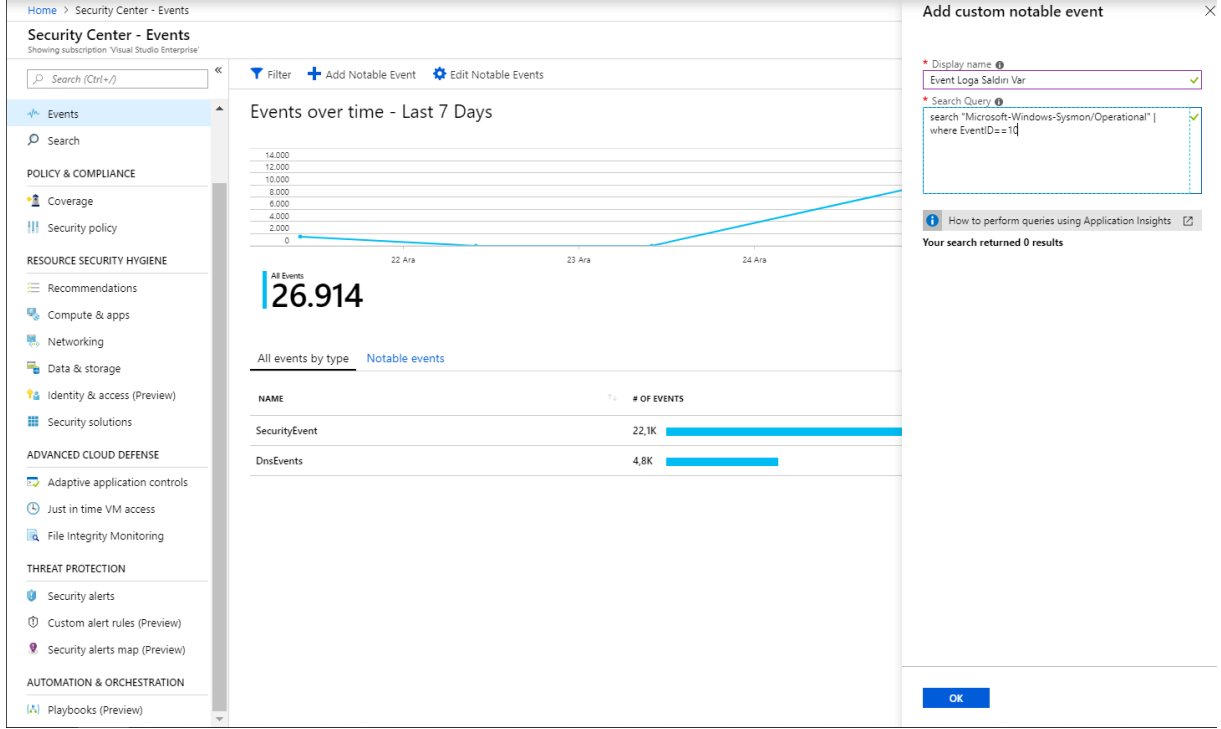
Bildiğiniz üzere yapımızda Microsoft ATA mevcut ve buradaki Log’larımızı Azure’ a da yönlendirmiştik. Log’larımızın artık Microsoft Security Center’ a geldiğini görüyoruz..





Eğer özel olarak belirli bir olay oluştuğunda alarm üretilmesini isterseniz **Add notable Event** seçeneği ile manuel olarak yazabilirsiniz.

Örneğin ;



Kaynak : <https://azure.microsoft.com/tr-tr/blog/detecting-in-memory-attacks-with-sysmon-and-azure-security-center/>

**SecurityEvent** i tıkladığımda tüm güvenlik ile alakalı oluşan Log'ların detayını görebiliyorum ve elbette belirli bir olay oluştuğunda alarm oluşturulup mail atırabiliyoruz.

Logs  
hctest

New Query 1\*

+

hctest

Run

Time range: Custom

Save

Copy link

Export

SchemaFilter (preview)SecurityEvent

Filter by name or type...

🔍

🔍 Collapse all

► DnsAnalytics

► LogManagement

▼ Security

► CommonSecurityLog

► LinuxAuditLog

► ProtectionStatus

► SecurityAlert

► SecurityBaseline

► SecurityBaselineSummary

► SecurityDetection

▼ SecurityEvent

Account

AccountDomain

AccountExpires

AccountName

AccountSessionIdentifier

AccountType

Activity

AdditionalInfo

AdditionalInfo2

AllowedToDelegateTo

Attributes

AuditPolicyChanges

# AuditsDiscarded

AuthenticationLevel

AuthenticationPackageName

Completed. Showing partial results from the custom time range. 00:0

TABLE

CHART

Columns ▼

Drag a column header and drop it here to group by that column

TenantId	TimeGenerated [UTC]	SourceSystem	Account	AccountType	Computer	EventSourceName	
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-23T14:29:53.517	OpsManager	-\\-	User	dc01.hd.local	Microsoft-Windows-Security-Auditing	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-23T14:29:53.517	OpsManager	-\\-	User	dc01.hd.local	Microsoft-Windows-Security-Auditing	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-23T15:06:04.083	OpsManager			dc01.hd.local	Microsoft-Windows-Eventlog	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-23T15:57:20.553	OpsManager			dc01.hd.local	Microsoft-Windows-Eventlog	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-22T09:01:27.440	OpsManager	\\guest	User	dc01.hd.local	Microsoft-Windows-Security-Auditing	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:43.610	OpsManager	HD\\DC01\$	Machine	dc01.hd.local	Microsoft-Windows-Security-Auditing	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:52.440	OpsManager			dc01.hd.local	Microsoft-Windows-Security-Auditing	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:52.443	OpsManager			dc01.hd.local	Microsoft-Windows-Security-Auditing	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:55.397	OpsManager			dc01.hd.local	Microsoft-Windows-Security-Auditing	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:55.400	OpsManager			dc01.hd.local	Microsoft-Windows-Security-Auditing	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:55.410	OpsManager			dc01.hd.local	Microsoft-Windows-Security-Auditing	S
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:55.413	OpsManager			dc01.hd.local	Microsoft-Windows-Security-Auditing	S

Completed. Showing partial results from the custom time range. 00:0

TABLE

CHART

Columns ▼

Drag a column header and drop it here to group by that column

TenantId	TimeGenerated [UTC]	Activity	Account	Computer	AccountType	EventSourceName	Channel
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-23T14:29:53.517	4625 - An account failed to log on.	-\\-	dc01.hd.local	User	Microsoft-Windows-Security-Auditing	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-23T14:29:53.517	4625 - An account failed to log on.	-\\-	dc01.hd.local	User	Microsoft-Windows-Security-Auditing	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-23T15:06:04.083	1102 - The audit log was cleared.		dc01.hd.local		Microsoft-Windows-Eventlog	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-23T15:57:20.553	1102 - The audit log was cleared.		dc01.hd.local		Microsoft-Windows-Eventlog	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-22T09:01:27.440	4625 - An account failed to log on.	\\guest	dc01.hd.local	User	Microsoft-Windows-Security-Auditing	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:43.610	4672 - Special privileges assigned to new logon.	HD\\DC01\$	dc01.hd.local	Machine	Microsoft-Windows-Security-Auditing	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:52.440	5061 - Cryptographic operation.		dc01.hd.local		Microsoft-Windows-Security-Auditing	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:52.443	5061 - Cryptographic operation.		dc01.hd.local		Microsoft-Windows-Security-Auditing	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:55.397	5061 - Cryptographic operation.		dc01.hd.local		Microsoft-Windows-Security-Auditing	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:55.400	5061 - Cryptographic operation.		dc01.hd.local		Microsoft-Windows-Security-Auditing	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:55.410	5061 - Cryptographic operation.		dc01.hd.local		Microsoft-Windows-Security-Auditing	Security
19313ac5-9566-4e8e-8360-a79221b000cb	2018-12-26T11:40:55.413	5061 - Cryptographic operation.		dc01.hd.local		Microsoft-Windows-Security-Auditing	Security

## Sysmon

Mark Russinovich tarafından yazılan Sysinternals içerisinde yer alan normal şartlarda elde edemeyeceğimiz Log'ları elde etmemize imkan sağlayan son derece faydalı bir araç. Yazı içerisinde kurulum adımlarına değinmeyeceğim. Basit kurulumu aşağıdaki şekildedir.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\ghost\Desktop\SysinternalsSuite

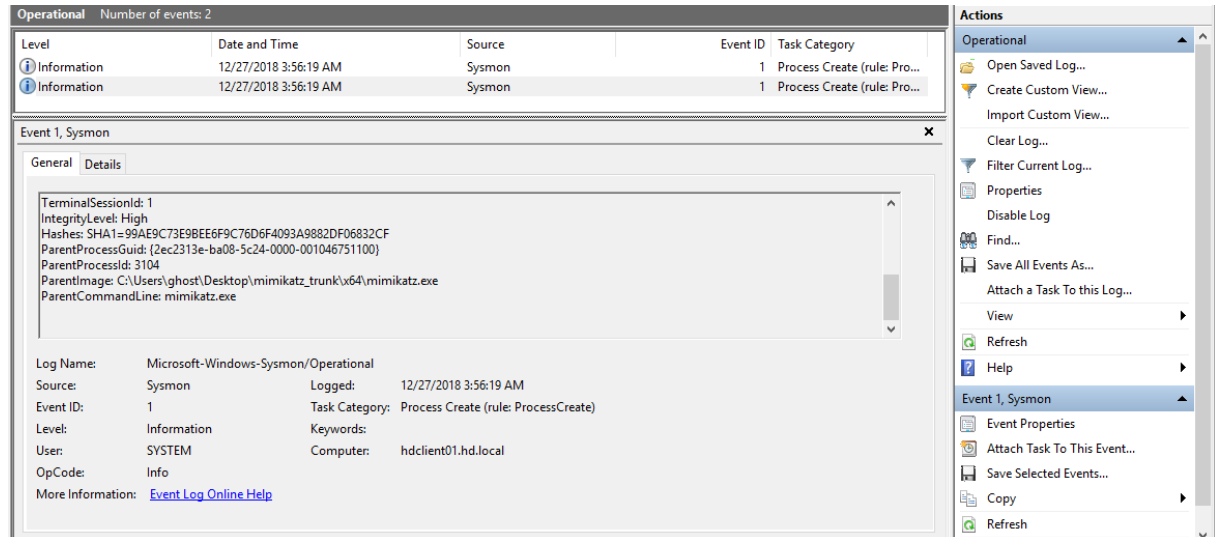
C:\Users\ghost\Desktop\SysinternalsSuite>Sysmon.exe -i

System Monitor v8.04 - System activity monitor
Copyright (C) 2014-2018 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.

C:\Users\ghost\Desktop\SysinternalsSuite>
```

Yazı içerisinde hatırlayacak olursanız mimikatz ile saldırı yapmıştık ve Log'lara baktığımızda normal bir davranış gibi algılanmıştı. Aynı adımı tekrar uyguladığımda artık detay bilgileri elde edebiliyorum. Hatırlarsanız şu ifadeyi kullanmıştım, Log'layamadığımız herhangi bir uç nokta her zaman tehlike arz edecektir. Aynı örnekte aldığımız iki farklı sonuç bunu kanıtlamaktadır.



Kaynak : <https://docs.microsoft.com/en-us/sysinternals/>

<https://blogs.technet.microsoft.com/motiba/2017/12/07/sysinternals-sysmon-suspicious-activity-guide/>

## Log'ların Kibana ile Anlamlandırılması

Bu bölümümüzde Kibana ile Log'larımızı merkezi olarak nasıl toplayabileceğimizi göreceğiz.

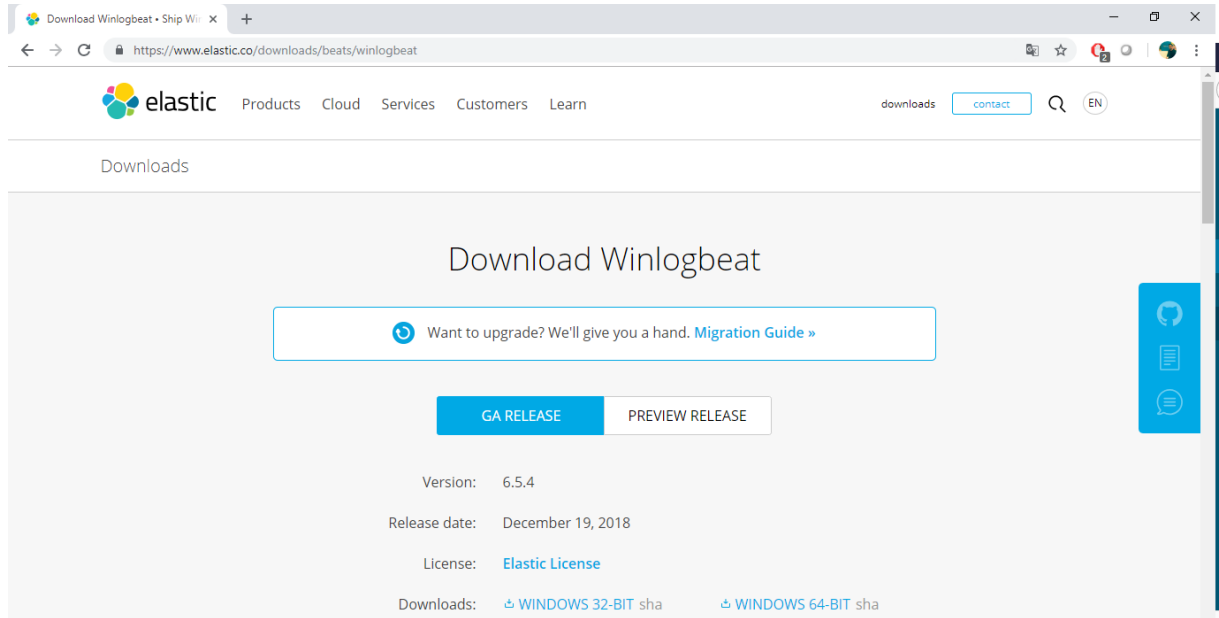
Konu bütünlüğünü bozmamak için Kibana ürününün tüm özelliklerine değinmeyeceğim.

### Winlogbeat

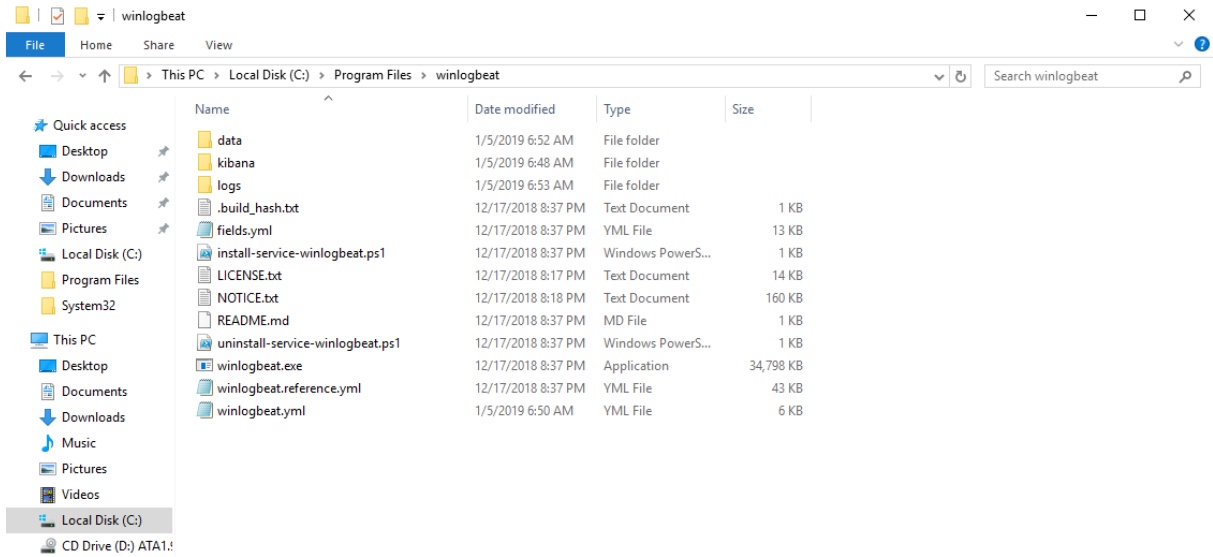
Amacım windows Log'larını merkezi olarak monitor etmek olduğu için **Winlogbeat** ajanından faydalanacağım. İlgili ajanı aşağıdaki linkten indirip Log'ları toplamak istediğimiz sunucu üzerinde kurmamız gerekiyor. ( SCCM gibi merkezi dağıtım araçları ile çoklu kurulum yapılabilir)

<https://www.elastic.co/downloads/beats/winlogbeat>

Aynı sitede kurulum adımları yer almaktadır. (Bu bölümün tamamında buradaki kaynaktan faydalandım )

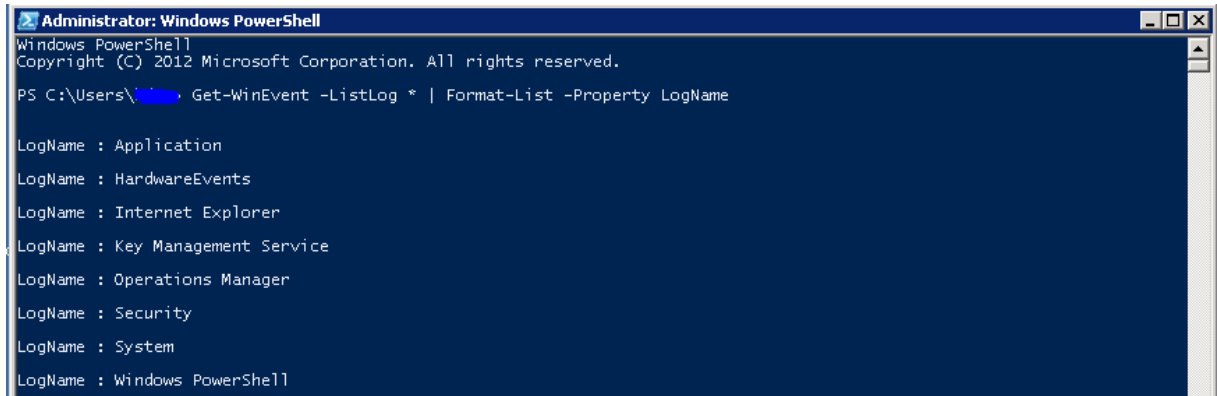


İndirdiğim **Winlogbeat** ajanını Program Files altına kopyalıyorum. **Winlogbeat.yml** konfig dosyasını yapımıza göre düzenlememiz gerekiyor.



**Winlogbeat.event\_logs:** kısmı bizim için önemli hangi Log'ların toplanacağını bu kısımda belirtiyoruz. Kendi yapım için security Log'larını toplayacağım için ;

**-name: Security** önündeki (#) işaretini kaldırıyorum. Daha spesifik ayarlarda yapabiliriz. Belirli Log'ları toplamak isterseniz **Get-WinEvent -Listing \* | Format-List -Property LogName** komutu ile listeledikten sonra konfig dosyasına dahil edebilirsiniz.



Benim örneğimde

**-name : Security** şekline olduğu için güvenlik Log'larını toplayacağım. Yukarıdaki komut yardımı ile bunu çoğaltabiliriz.

```
filebeat.yml x winlogbeat.yml x
10 #----- Winlogbeat specific options -----
11
12 # event_logs specifies a list of event logs to monitor as well as any
13 # accompanying options. The YAML data type of event_logs is a list of
14 # dictionaries.
15 #
16 # The supported keys are name (required), tags, fields, fields_under_root,
17 # forwarded, ignore_older, level, event_id, provider, and include_xml. Please
18 # visit the documentation for the complete details of each option.
19 # https://go.es.io/WinlogbeatConfig
20 winlogbeat.event_logs:
21   # - name: Application
22   #   ignore_older: 72h
23   - name: Security
24   # - name: System
25
```

Setup.kibana kısmında ise Kibana sunucumuzun url sini gösteriyoruz.

```
65 setup.kibana:
66
67   # Kibana Host
68   # Scheme and port can be left out and will be set to the default (http and 5601)
69   # In case you specify and additional path, the scheme is required: http://localhost:5601/path
70   # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
71   host: ["http://elastic.hd.local:5601"]
72
```

Elasticsearch output dosyası da aşağıdaki şekilde olmalıdır.

```
96 #----- Elasticsearch output -----
97 output.elasticsearch:
98   hosts: ["http://elastic.hd.local:9200"]
99   username: "elastic"
100   password: " "
101 setup.kibana:
102   host: "http://elastic.hd.local:5601"
103
```

Konfigürasyon dosyamızı düzenledikten sonra **.\Install-service-winlogbeat.ps1** komutu ile winlogbeat servisini kuruyoruz.

```
Administrator: Windows PowerShell
PS C:\Program Files\winlogbeat> .\install-service-winlogbeat.ps1

Status  Name      DisplayName
-----
Stopped winlogbeat winlogbeat

PS C:\Program Files\winlogbeat> _
```

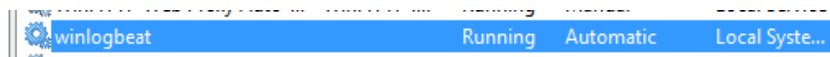
Servisi kurduktan sonra eğer konfig dosyasında hata varmı gibi kontrolleri yapmak isterseniz **.\winlogbeat.exe test config -c .\winlogbeat.yml -e** komutu ile kontrol edebilirsiniz.

```
Administrator: Windows PowerShell
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test config -c .\winlogbeat.yml -e
2019-01-06T07:18:17.998-0800 INFO instance/beat.go:592 Home path: [C:\Program Files\winlogbeat] Config path: [C
:\Program Files\winlogbeat] Data path: [C:\Program Files\winlogbeat\data] Logs path: [C:\Program Files\winlogbeat\logs]
2019-01-06T07:18:18.001-0800 INFO instance/beat.go:599 Beat UUID: 5c8d6c87-ad0a-4c1d-80bf-78c04ca0c182
2019-01-06T07:18:18.002-0800 INFO [beat] instance/beat.go:825 Beat info {"system_info": {"beat": {"path"
: {"config": "C:\\Program Files\\winlogbeat", "data": "C:\\Program Files\\winlogbeat\\data", "home": "C:\\Program Files\\
\\winlogbeat", "logs": "C:\\Program Files\\winlogbeat\\logs"}, "type": "winlogbeat", "uuid": "5c8d6c87-ad0a-4c1d-80bf-78c
04ca0c182"}}}}
2019-01-06T07:18:18.003-0800 INFO [beat] instance/beat.go:834 Build info {"system_info": {"build": {"comm
it": "bd8922f1c7e93d12b07e0b3f7d349e17107f7826", "libbeat": "6.5.4", "time": "2018-12-17T20:37:05.000Z", "version": "6.5
.4"}}}}
2019-01-06T07:18:18.003-0800 INFO [beat] instance/beat.go:837 Go runtime info {"system_info": {"go": {"os": "wi
ndows", "arch": "amd64", "max_procs": 1, "version": "go1.10.6"}}}}
2019-01-06T07:18:18.007-0800 INFO [beat] instance/beat.go:841 Host info {"system_info": {"host": {"archi
tecture": "x86_64", "boot_time": "2019-01-06T02:41:51.98-08:00", "name": "dc01", "ip": ["10.0.2.15/24", ":1/128", "127.0.0.1/8",
"fe80::5efe:a00:20f:128"], "kernel_version": "10.0.14393.447 (rs1_release_inmarket.161102-0100)", "mac": ["08:00:27:96:97:26
", "00:00:00:00:00:00:e0"], "os": {"family": "windows", "platform": "windows", "name": "Windows Server 2016 Standard", "versio
n": "10.0", "major": 10, "minor": 0, "patch": 0, "build": "14393.447"}, "timezone": "PST", "timezone_offset_sec": -28800, "id": "0f543a
aa-7b3a-41af-b18d-3a7f07c6db63"}}}}
2019-01-06T07:18:18.010-0800 INFO [beat] instance/beat.go:870 Process info {"system_info": {"process": {"cw
d": "C:\\Program Files\\winlogbeat", "exe": "C:\\Program Files\\winlogbeat\\winlogbeat.exe", "name": "winlogbeat.exe", "
pid": 4688, "ppid": 1328, "start_time": "2019-01-06T07:18:17.952-0800"}}}}
2019-01-06T07:18:18.010-0800 INFO instance/beat.go:278 Setup Beat: winlogbeat; Version: 6.5.4
2019-01-06T07:18:21.014-0800 INFO add_cloud_metadata/add_cloud_metadata.go:319 add_cloud_metadata: hosting prov
ider type not detected.
2019-01-06T07:18:21.015-0800 INFO elasticsearch/client.go:163 Elasticsearch url: http://elastic.hd.local:9200
2019-01-06T07:18:21.017-0800 INFO [publisher] pipeline/module.go:110 Beat name: dc01
2019-01-06T07:18:21.017-0800 INFO beater/winlogbeat.go:68 State will be read from and persisted to C:\Program File
s\winlogbeat\data\winlogbeat.yml
Config OK
PS C:\Program Files\winlogbeat>
```

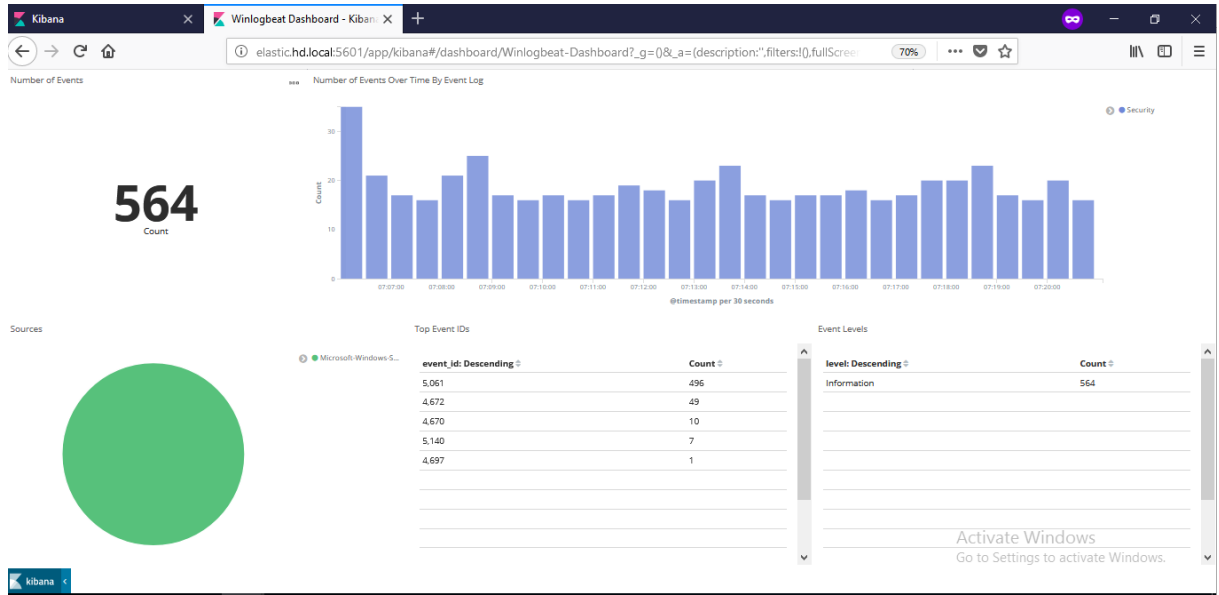
Son olarak da **setup** parametresi ile Kibana dashboard kurulumunu tamamlıyoruz.

```
Administrator: Windows PowerShell
PS C:\Program Files\winlogbeat> .\winlogbeat.exe setup
Loaded index template
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
```

Winlogbeat servisini başlatmayı da unutmuyoruz.



Kibana'yı açtığımızda Log'larımızın sağlıklı olarak Dashboard a yansıdığını görüyoruz.



Test amaçlı Event Log'ları siliyorum.

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
- Subscriptions

Security Number of events: 1

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	1/6/2019 7:24:23 AM	Eventlog	1102	Log clear

Event 1102, Eventlog

General Details

The audit log was cleared.

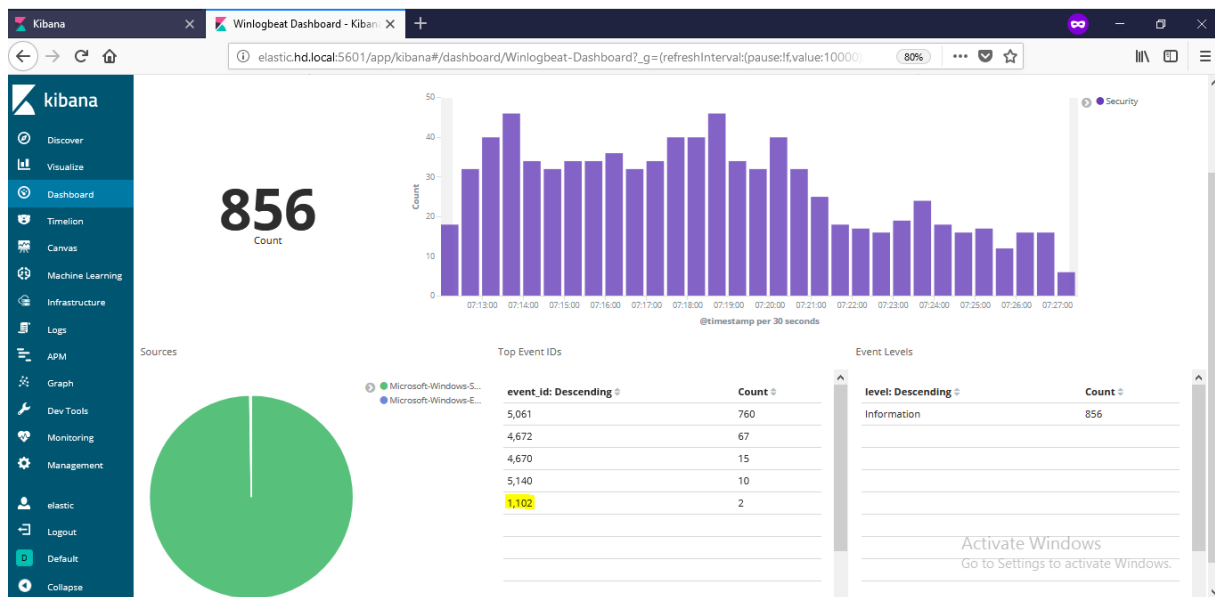
Subject: Security ID: HD\administrator

Log Name: Security  
Source: Eventlog  
Event ID: 1102  
Level: Information  
User: N/A  
OnCode: Info

Logged: 1/6/2019 7:24:23 AM  
Task Category: Log clear  
Keywords: Audit Success  
Computer: dc01.hd.local

Kısa bir süre sonra 1102 Log'unun yansıdığını görüyoruz. İsterseniz bu olaylardan alarm üretebilirsiniz. Tavsiye edilen de budur. Yazımın başında da dediğim gibi birçok yerde Log'lar bulunuyor fakat bu Log'ları merkezi olarak toplayamadıktan sonra, izleyemedikten sonra ve alarm üretemedikten sonra kimseye faydası olmayacaktır.





## Event Log'ların Kabusu PhantOm



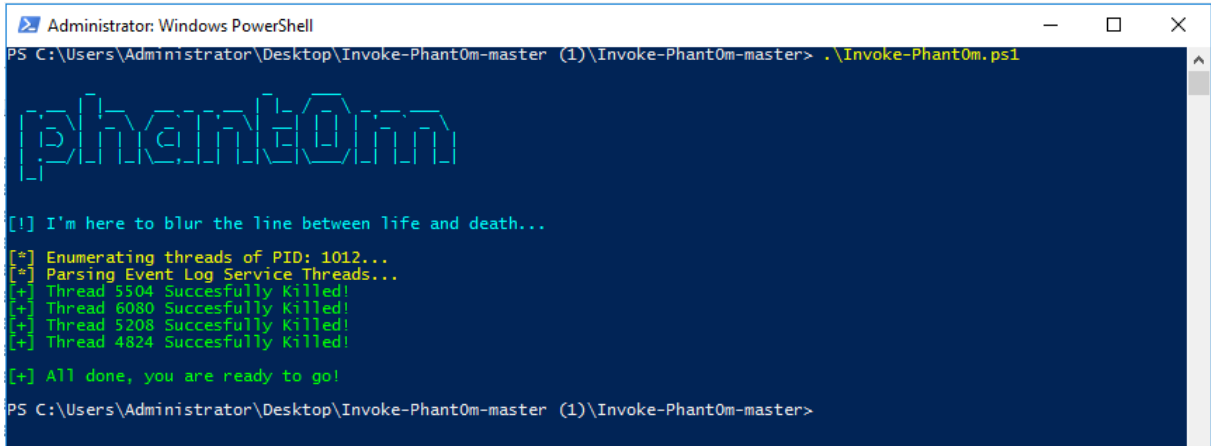
Yazım içerisinde sürekli Log'ların ne kadar önemli olduğundan bahsetmeye çalıştım. Bizler savunma tarafında Windows içerisindeki event Log'ları toplayıp merkezi bir araca gönderip buralardan anlam çıkarmaya, varsa bir anormallik alarm üretme, ilgili departmanın durumun farkında olmasını sağlarken veya bir olay olursa nasıl olduğunu anlamaya çalışırken, saldırgan gözüyle bakıldığında aşılması, manupile edilmesi veya Log'lamanın yapılamaması, sisteme sızdıktan sonra tüm izleri silmek, herşey olağan şekilde çalışıyormuş gibi gösterip arka planda iz bırakmadan saldırıyı planladığı şekilde yapmak olacaktır. Halil Dalabasmaz hocamızın yazdığı phant0m aracı burada devreye giriyor. Bu bölümü yazmamın en önemli sebebi gereksiz verilen haklar, kullanılmayan veya kullanımı gerekli olmayan Powershell aracının cihazlarda kurulu olması veya kullanımına izin verilmesi başımıza ciddi sorunlar açabileceğini göstermekti.

Örneğimizde Phant0m kullanarak Windows event Log'larını kill edeceğiz. İlgili aracı github dan indirdim.

<https://github.com/hlldz/Invoke-Phant0m>

Bu bölümün amacı hack nasıl yapılırı göstermek değildir. Amacım neden sıkılaştırma yapmalıyız, yapmazsak başımıza ne gelebilir Event Log tarafında göstermektir. Lütfen bu bölümü bu gözle okuyunuz.

Saldırı yaptığımız sunucu üzerinde Phant0m aracını powershell yardımı ile çalıştırdım ve eventlog servisini aslında çalışmaz hale getirdim.

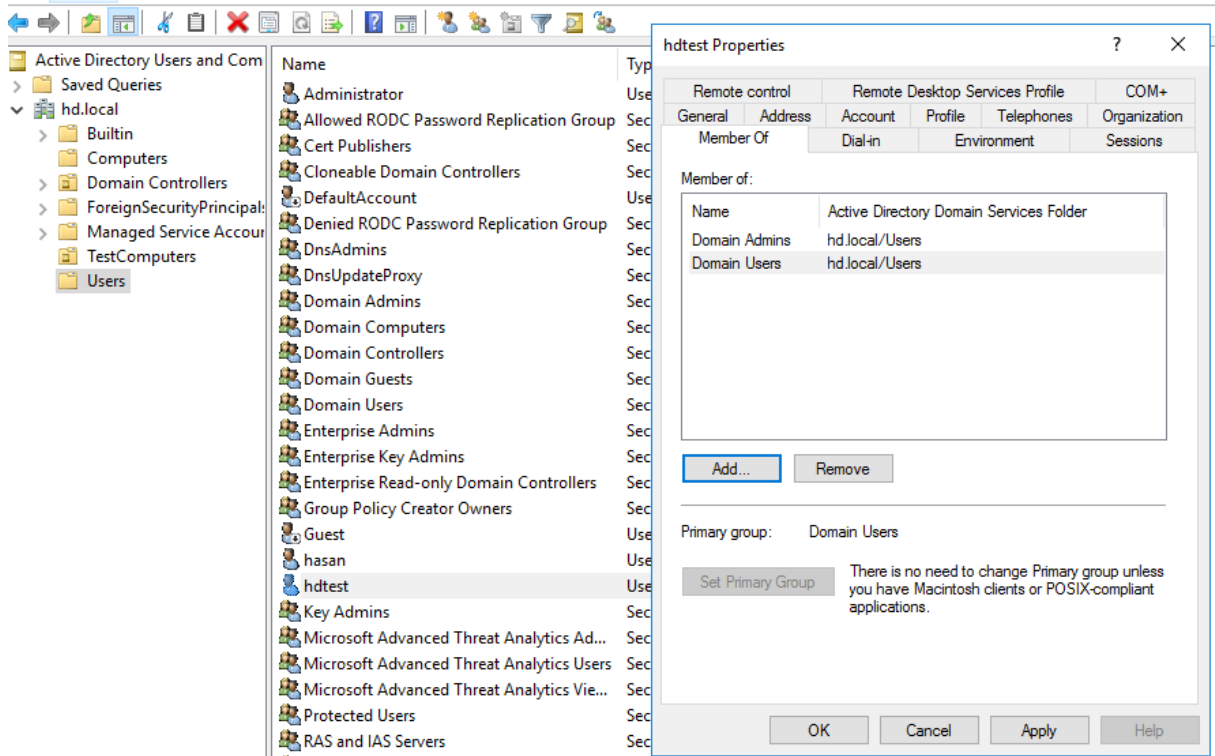


```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\Invoke-Phant0m-master (1)\Invoke-Phant0m-master> .\Invoke-Phant0m.ps1

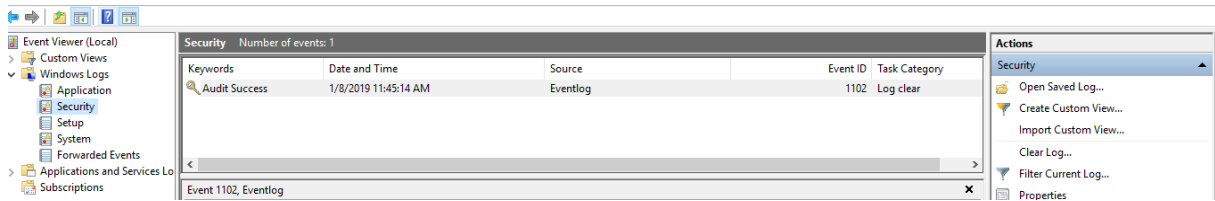
phant0m

[!] I'm here to blur the line between life and death...
[*] Enumerating threads of PID: 1012...
[*] Parsing Event Log Service Threads...
[+] Thread 5504 Successfully Killed!
[+] Thread 6080 Successfully Killed!
[+] Thread 5208 Successfully Killed!
[+] Thread 4824 Successfully Killed!
[+] All done, you are ready to go!
PS C:\Users\Administrator\Desktop\Invoke-Phant0m-master (1)\Invoke-Phant0m-master>
```

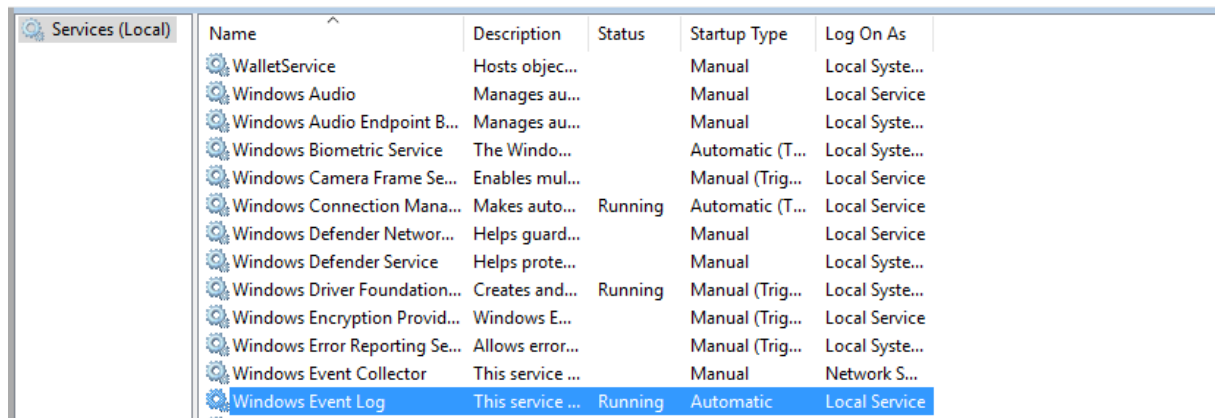
Örnek olarak hctest kullanıcıma Domain Admin hakkı veriyorum. Normal şartlar altında Log'lanmasını bekliyorum.



Event Log a baktığımda ise herhangi bir Log'un gelmediğini görüyorum.



Windows Event Log servisini kontrol ettiğimde çalışıyor olarak gözüküyor.



Görüldüğü üzere artık hiçbirşeyi Log'layamıyoruz. Doğru şekilde denetleyemediğimiz, Log'layamadığımız ve günün sonunda bu oluşan dataları anlamlandıramadığımız vakaları çözme imkanımız da bulunmamaktadır.

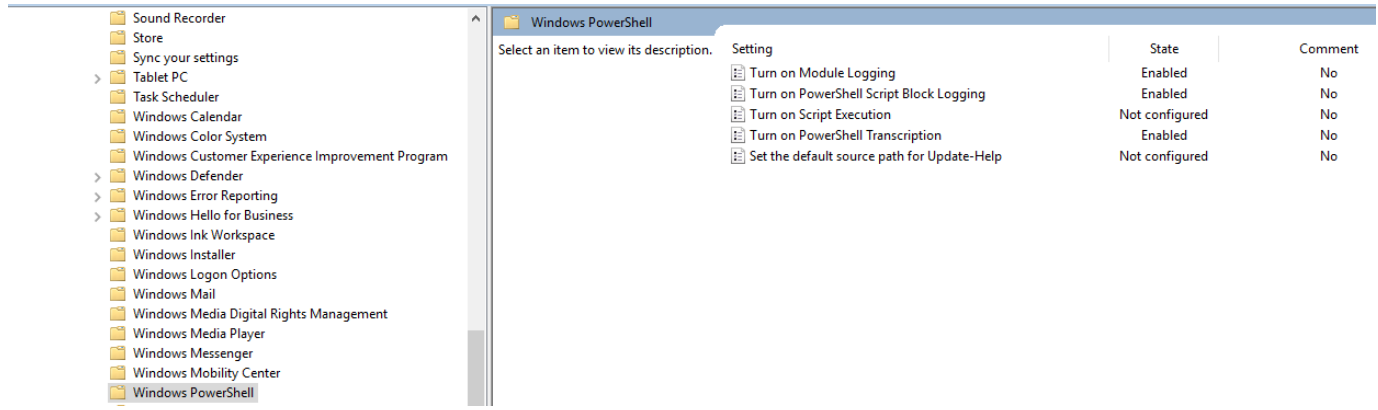
Kaynak :

<https://artofpwn.com/>

## Powershell' i Nasıl Log'larım ?



Powershell' i Log'layabilmek için ilk olarak v3 veya üzeri sürüm kullanıyor olmanız gerekmektedir. Powershell ortamların otomatize edilmesi veya arayüzde yapılamayan işlemlerin yapılması için son derece faydalı bir komut arabirimi. Hem yanlış kullanımların Log'lanması, aynı zamanda Powershell üzerinden gelebilecek saldırıları daha hızlı fark etmek için Log'lamamız gerekmektedir.



## Script Block Logging

Encode haldeki bir kod decode edildikten sonra ve çalıştırılır hale geldikten sonra Event Log'a iletilir ve akabinde ilgili kod çalışır. Bu özellik sayesinde daha henüz kod çalıştırılmadan durumdan haberdar olmuş oluyoruz. **Administrative Templates > Windows Components > Windows Powershell > Turn on Powershell Script Block Logging** aktif edilmelidir.

Turn on PowerShell Script Block Logging

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

☒ Log script block invocation start / stop events:

Help:

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. If you enable this policy setting, Windows PowerShell will log the processing of commands, script blocks, functions, and scripts - whether invoked interactively, or through automation.

If you disable this policy setting, logging of PowerShell script input is disabled.

If you enable the Script Block Invocation Logging, PowerShell additionally logs events when invocation of a command, script block, function, or script starts or stops. Enabling Invocation Logging generates a high volume of event logs.

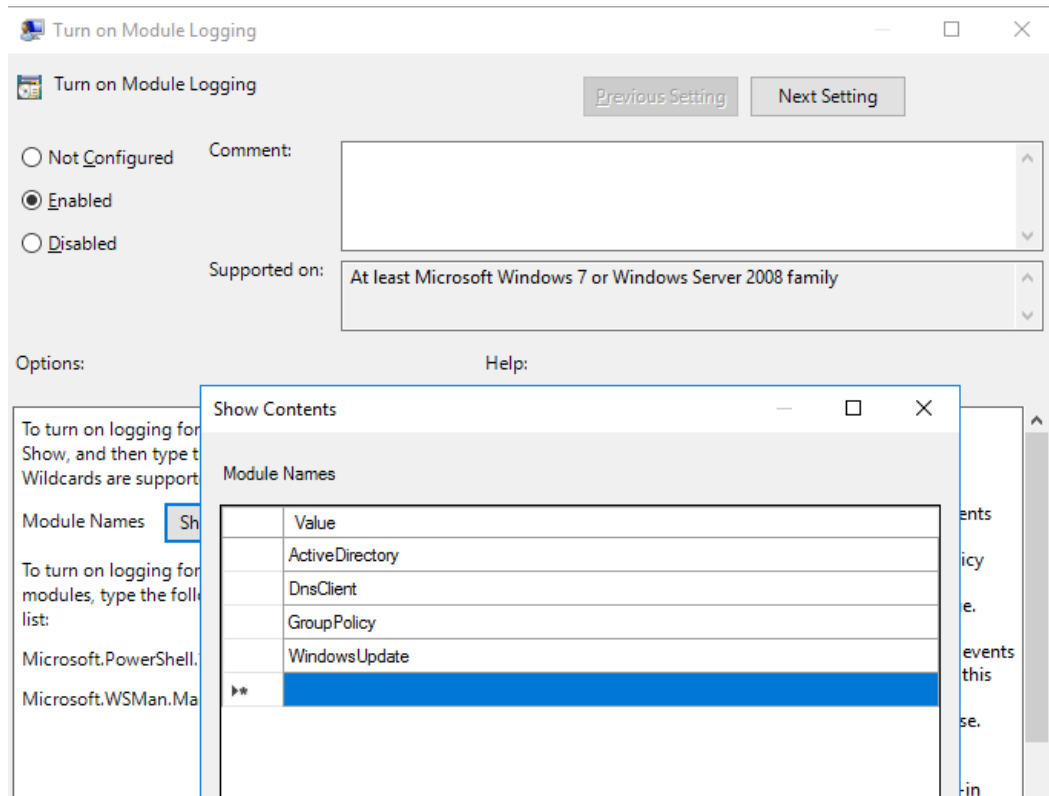
Note: This policy setting exists under both Computer Configuration and User Configuration in the Group Policy Editor. The Computer Configuration policy setting takes precedence over the User Configuration policy setting.

Kaynak : [https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit\\_script](https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script)

## Module Logging

Cmdlet lere ait modüller için Log üretilmesi sağlanır. **Administrative Templates > Windows Components > Windows Powershell > Turn on Module Logging** aktif edilmelidir.

Örneğimizde ActiveDirectory, DnsClient, GroupPolicy, WindowsUpdate modülleri çalıştırılması durumunda Log üretilmesi için kural tanımladım.



**Get-WindowsUpdateLog** komutunu kullandığımda Log'landığını görüyorum.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

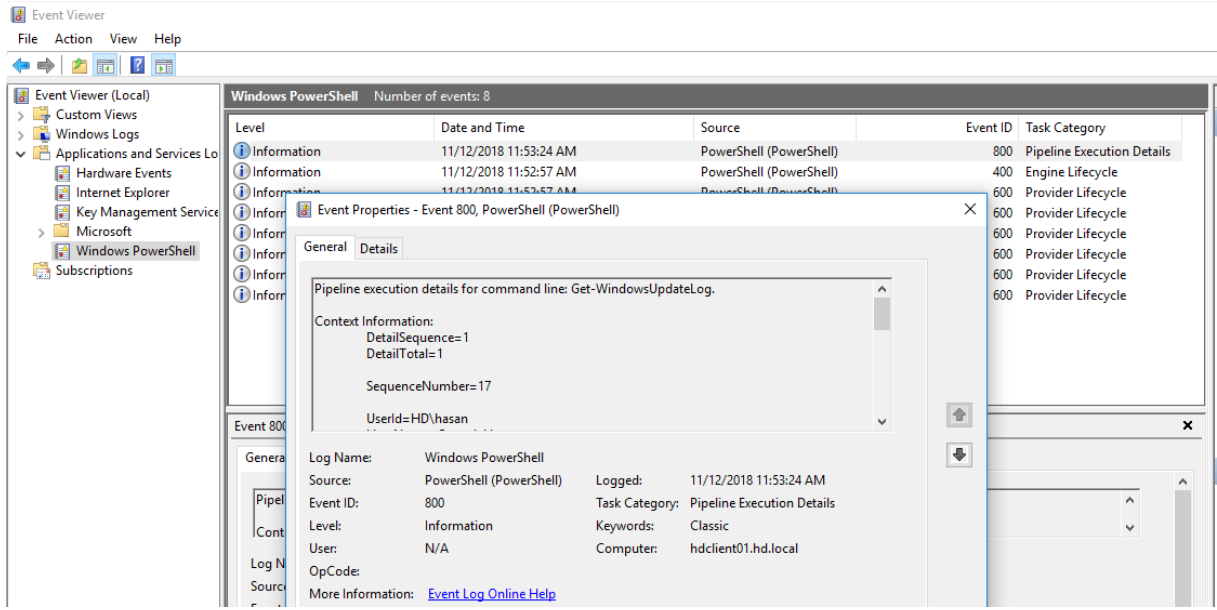
PS C:\Users\Administrator> Get-WindowsUpdateLog

Converting C:\Windows\Logs\WindowsUpdate into C:\Users\Administrator\Desktop\WindowsUpdate.log ...

Directory: C:\Users\ADMINI~1\AppData\Local\Temp\WindowsUpdateLog

Mode                LastWriteTime         Length Name
----                -
d-----         11/12/2018  11:46 AM             SymCache

Input
-----
File(s):
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181028.134536.441.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181028.134814.058.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181028.140610.593.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181030.031640.570.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181030.034724.408.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181030.045305.047.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181030.051130.247.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181030.052241.136.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181030.055338.399.1.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20181030.061055.270.1.etl
  
```



## Logging Powershell Activity

Powershell üzerinde çalıştırılan komutlar her kullanıcı için Log'lanmaktadır. Burada önemli olan ilgili Log'ların merkezi bir yerde toplanmasıdır. İlgili Log'ları zaman damgası ile de damgalamak isterseniz **Administrative Templates > Windows Components > Windows Powershell > Turn on Powershell Transcription** aktif edilmeli.

Örneğimde C:\Tlogs altında Log'ların oluşması için dosya yolu gösterdim.



Turn on PowerShell Transcription

Turn on PowerShell Transcription

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

Transcript output directory

C:\TLogs

☒ Include invocation headers:

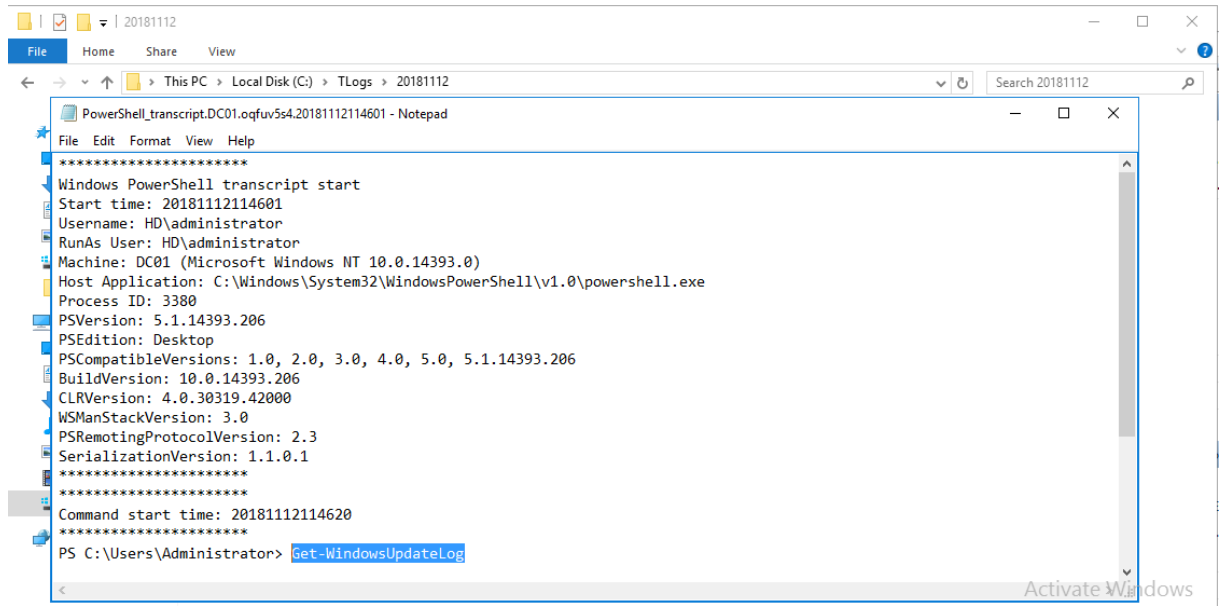
Help:

This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

If you enable this policy setting, Windows PowerShell will enable transcribing for Windows PowerShell, the Windows PowerShell ISE, and any other applications that leverage the Windows PowerShell engine. By default, Windows PowerShell will record transcript output to each users' My Documents directory, with a file name that includes 'PowerShell\_transcript', along with the computer name and time started. Enabling this policy is equivalent to calling the Start-Transcript cmdlet on each Windows PowerShell session.

If you disable this policy setting, transcribing of PowerShell-based applications is disabled by default, although transcribing can still be enabled through the Start-Transcript cmdlet.

**Get-WindowsUpdateLog** komutunu çalıştırdıktan sonra aşağıdaki şekilde Log'un üretildiğini görüyorum.



Kaynak : [https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit\\_transcript](https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_transcript)

Umuyorum Faydası Dokunmuştur.

Hasan DİMDİK

Cloud and Datacenter MVP