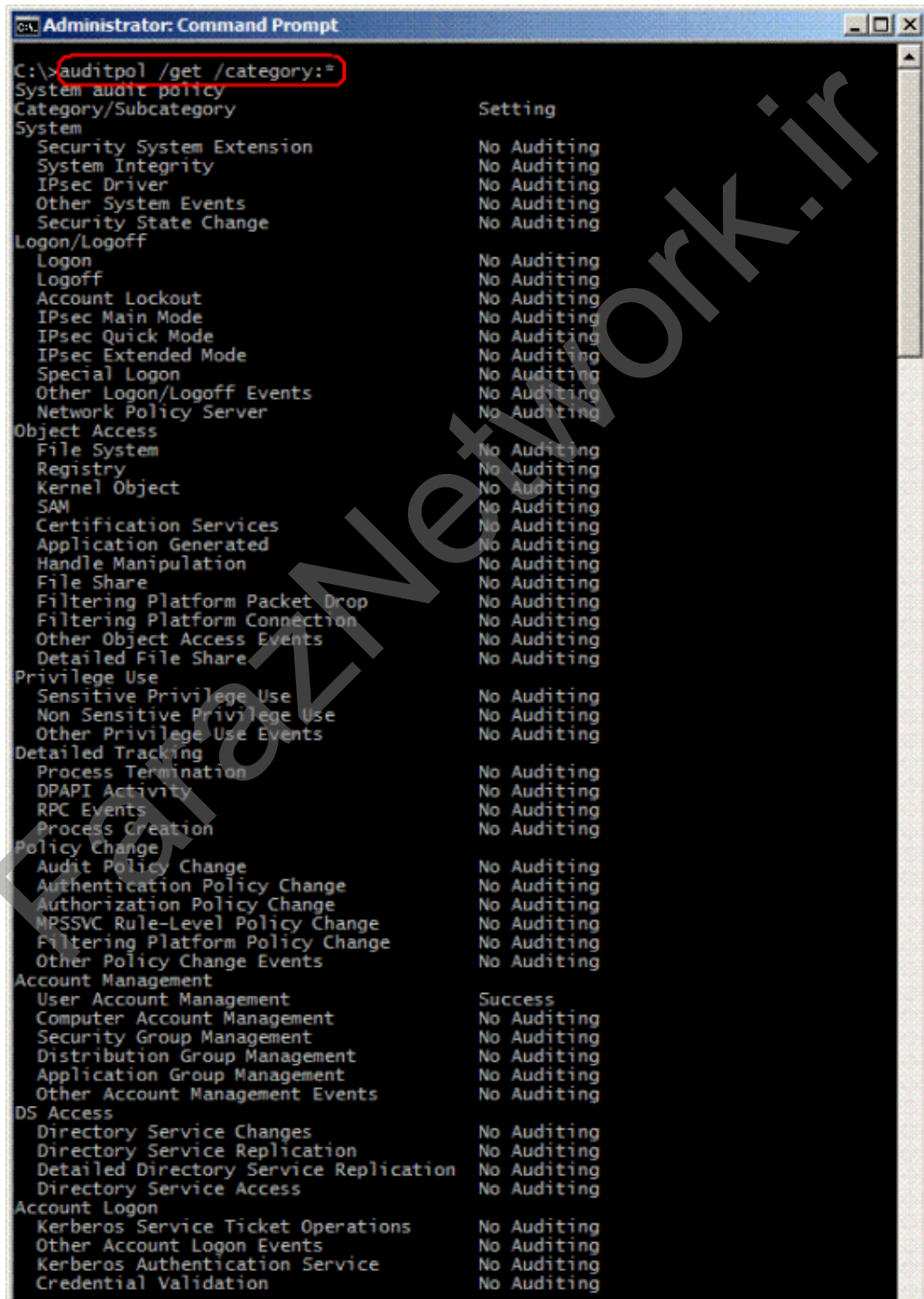


بیکربندی قابلیت Advanced Audit Policy از طریق Command Prompt

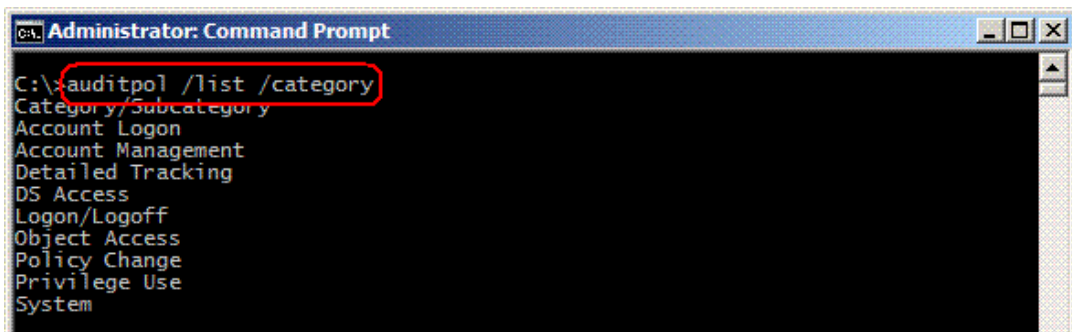
مدیریت و بیکربندی قابلیت Advanced Audit Policy از طریق محیط Command Prompt

جهت مشاهده تمامی Audit Policy های موجود و مشاهده فعال و یا غیر فعال بودن آنها کفایت از دستور زیر استفاده کنید:



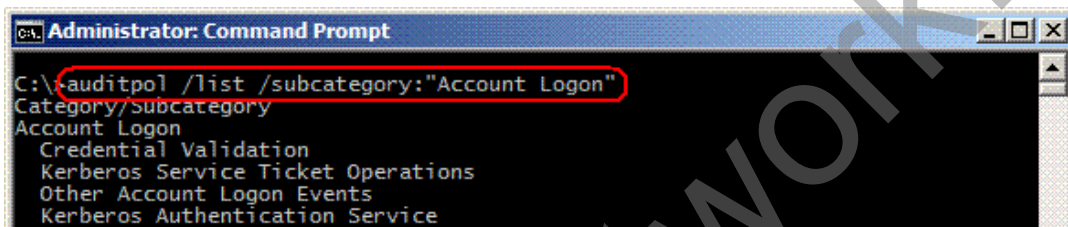
```
Administrator: Command Prompt
C:\>auditpol /get /category:='
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    No Auditing
  System Integrity             No Auditing
  IPsec Driver                 No Auditing
  Other System Events         No Auditing
  Security State Change       No Auditing
Logon/Logoff
  Logon                       No Auditing
  Logoff                      No Auditing
  Account Lockout             No Auditing
  IPsec Main Mode             No Auditing
  IPsec Quick Mode           No Auditing
  IPsec Extended Mode        No Auditing
  Special Logon               No Auditing
  Other Logon/Logoff Events   No Auditing
  Network Policy Server      No Auditing
Object Access
  File System                 No Auditing
  Registry                   No Auditing
  Kernel Object              No Auditing
  SAM                       No Auditing
  Certification Services     No Auditing
  Application Generated       No Auditing
  Handle Manipulation         No Auditing
  File Share                  No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events  No Auditing
  Detailed File Share        No Auditing
Privilege Use
  Sensitive Privilege Use     No Auditing
  Non Sensitive Privilege Use No Auditing
  Other Privilege Use Events  No Auditing
Detailed Tracking
  Process Termination        No Auditing
  DPAPI Activity             No Auditing
  RPC Events                 No Auditing
  Process Creation           No Auditing
Policy Change
  Audit Policy Change         No Auditing
  Authentication Policy Change No Auditing
  Authorization Policy Change No Auditing
  MPSSVC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events  No Auditing
Account Management
  User Account Management     Success
  Computer Account Management No Auditing
  Security Group Management   No Auditing
  Distribution Group Management No Auditing
  Application Group Management No Auditing
  Other Account Management Events No Auditing
DS Access
  Directory Service Changes   No Auditing
  Directory Service Replication No Auditing
  Detailed Directory Service Replication No Auditing
  Directory Service Access    No Auditing
Account Logon
  Kerberos Service Ticket Operations No Auditing
  Other Account Logon Events    No Auditing
  Kerberos Authentication Service No Auditing
  Credential Validation        No Auditing
```

نکته 1: به منظور نمایش عنوان هر گروه از Audit Policy ها می توانید از دستور زیر استفاده کنید:



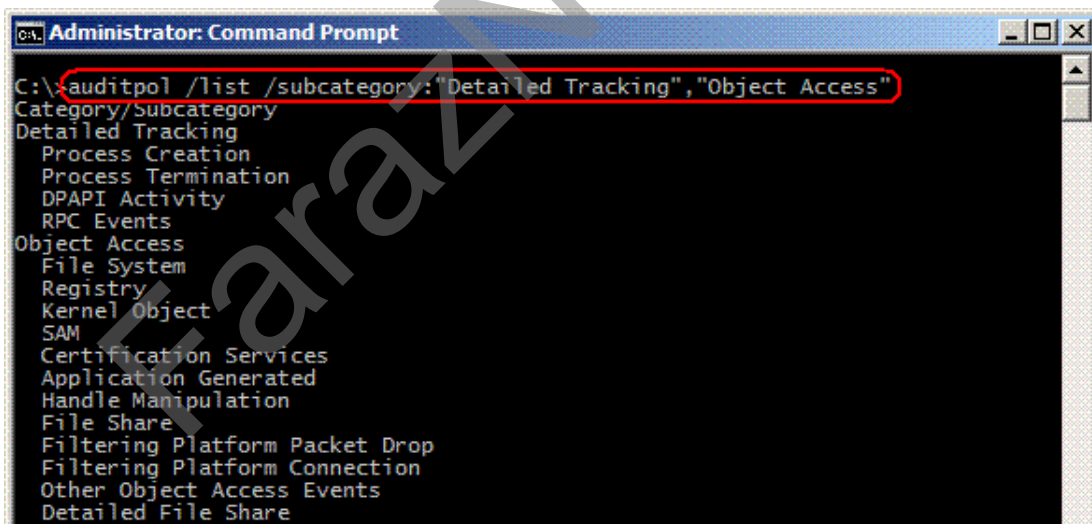
```
Administrator: Command Prompt
C:\>auditpol /list /category
Category/Subcategory
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
```

نکته 2: به منظور نمایش policy های زیر مجموعه یک Audit Policy می بایست مانند مثال زیر عمل کنید:



```
Administrator: Command Prompt
C:\>auditpol /list /subcategory:"Account Logon"
Category/Subcategory
Account Logon
  Credential Validation
  Kerberos Service Ticket Operations
  Other Account Logon Events
  Kerberos Authentication Service
```

نکته 3: به منظور نمایش policy های زیر مجموعه چندین Audit Policy می بایست همانند مثال زیر عمل کنید:



```
Administrator: Command Prompt
C:\>auditpol /list /subcategory:"Detailed Tracking","Object Access"
Category/Subcategory
Detailed Tracking
  Process Creation
  Process Termination
  DPAPI Activity
  RPC Events
Object Access
  File System
  Registry
  Kernel Object
  SAM
  Certification Services
  Application Generated
  Handle Manipulation
  File Share
  Filtering Platform Packet Drop
  Filtering Platform Connection
  Other Object Access Events
  Detailed File Share
```

به منظور فعال نمودن یکی از policy های زیر مجموعه یک Audit Policy اصلی می بایست طبق مثال زیر عمل کنید:

```
Administrator: Command Prompt
C:\>auditpol /set /category:"Object Access" /success:enable
The command was successfully executed.
C:\>_
```

نتیجه عملیات فوق را در شکل زیر مشاهده می نمایید:

```
Administrator: Command Prompt
C:\>auditpol /get /category:"Object Access"
System audit policy
Category/Subcategory          Setting
Object Access
File System                    Success
Registry                      Success
Kernel Object                 Success
SAM                          Success
Certification Services        Success
Application Generated          Success
Handle Manipulation           Success
File Share                    Success
Filtering Platform Packet Drop Success
Filtering Platform Connection Success
Other Object Access Events    Success
Detailed File Share           Success
C:\>_
```

نکته: به منظور تغییر تنها یک policy زیر مجموعه یک Audit Policy اصلی می بایست طبق مثال زیر عمل کنید:

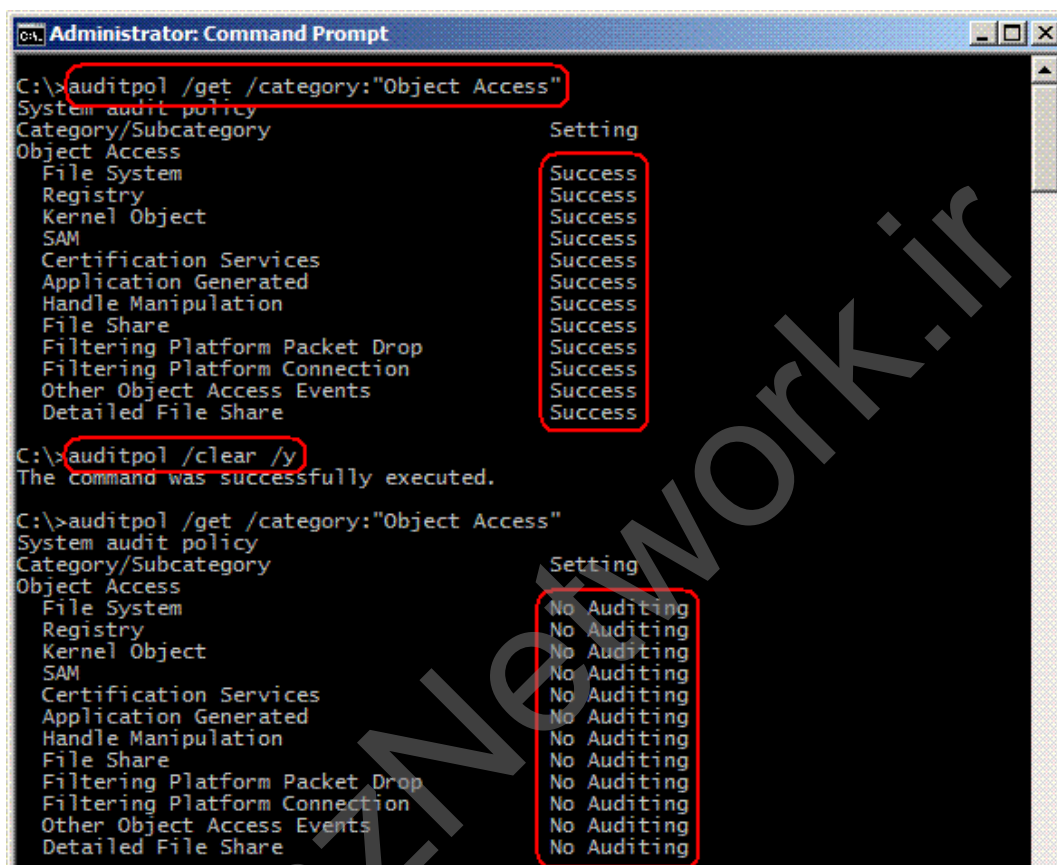
```
Administrator: Command Prompt
C:\>auditpol /set /subcategory:"File System" /success:enable
The command was successfully executed.
C:\>
```

نتیجه انجام عملیات فوق را در شکل زیر مشاهده می نمایید:

```
Administrator: Command Prompt
C:\>auditpol /get /category:"Object Access"
System audit policy
Category/Subcategory          Setting
Object Access
File System                    Success
Registry                      No Auditing
Kernel Object                 No Auditing
SAM                          No Auditing
Certification Services        No Auditing
Application Generated          No Auditing
Handle Manipulation           No Auditing
File Share                    No Auditing
Filtering Platform Packet Drop No Auditing
Filtering Platform Connection No Auditing
Other Object Access Events    No Auditing
Detailed File Share           No Auditing
C:\>_
```

به منظور غیر فعال کردن یک Audit Policy می بایست همانند مورد قبل عمل نمود. اما با این تفاوت که به جای استفاده از عبارت Enable می بایست از عبارت Disable استفاده کرد.

برای بازگرداندن تنظیمات انجام شده در Advanced Audit Policy به حالت اولیه، به مثال زیر نگاه کنید:

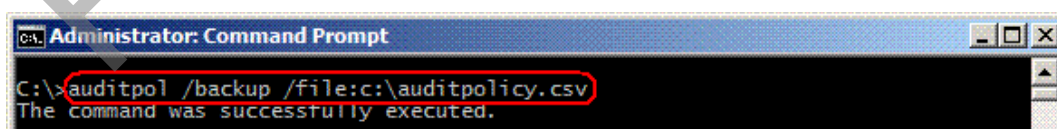


```
Administrator: Command Prompt
C:\>auditpol /get /category:"Object Access"
System audit policy
Category/Subcategory      Setting
Object Access
File System                Success
Registry                   Success
Kernel Object              Success
SAM                        Success
Certification Services     Success
Application Generated      Success
Handle Manipulation        Success
File Share                  Success
Filtering Platform Packet Drop Success
Filtering Platform Connection Success
Other Object Access Events Success
Detailed File Share        Success

C:\>auditpol /clear /y
The command was successfully executed.

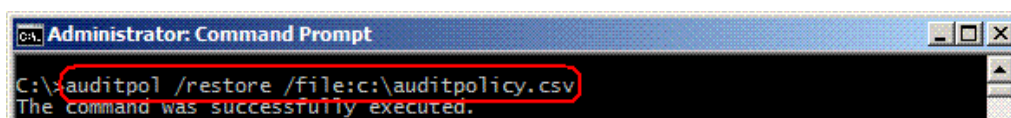
C:\>auditpol /get /category:"Object Access"
System audit policy
Category/Subcategory      Setting
Object Access
File System                No Auditing
Registry                   No Auditing
Kernel Object              No Auditing
SAM                        No Auditing
Certification Services     No Auditing
Application Generated      No Auditing
Handle Manipulation        No Auditing
File Share                  No Auditing
Filtering Platform Packet Drop No Auditing
Filtering Platform Connection No Auditing
Other Object Access Events No Auditing
Detailed File Share        No Auditing
```

گرفتن پشتیبان از تنظیمات موجود در قسمت Advanced Audit Policy: بدین منظور کافیت طبق مثال زیر عمل کنید:



```
Administrator: Command Prompt
C:\>auditpol /backup /file:c:\auditpolicy.csv
The command was successfully executed.
```

برای بازگرداندن پشتیبان گرفته شده از تنظیمات موجود در قسمت Advanced Audit Policy بدین منظور کافیت طبق مثال زیر عمل کنید:



```
Administrator: Command Prompt
C:\>auditpol /restore /file:c:\auditpolicy.csv
The command was successfully executed.
```