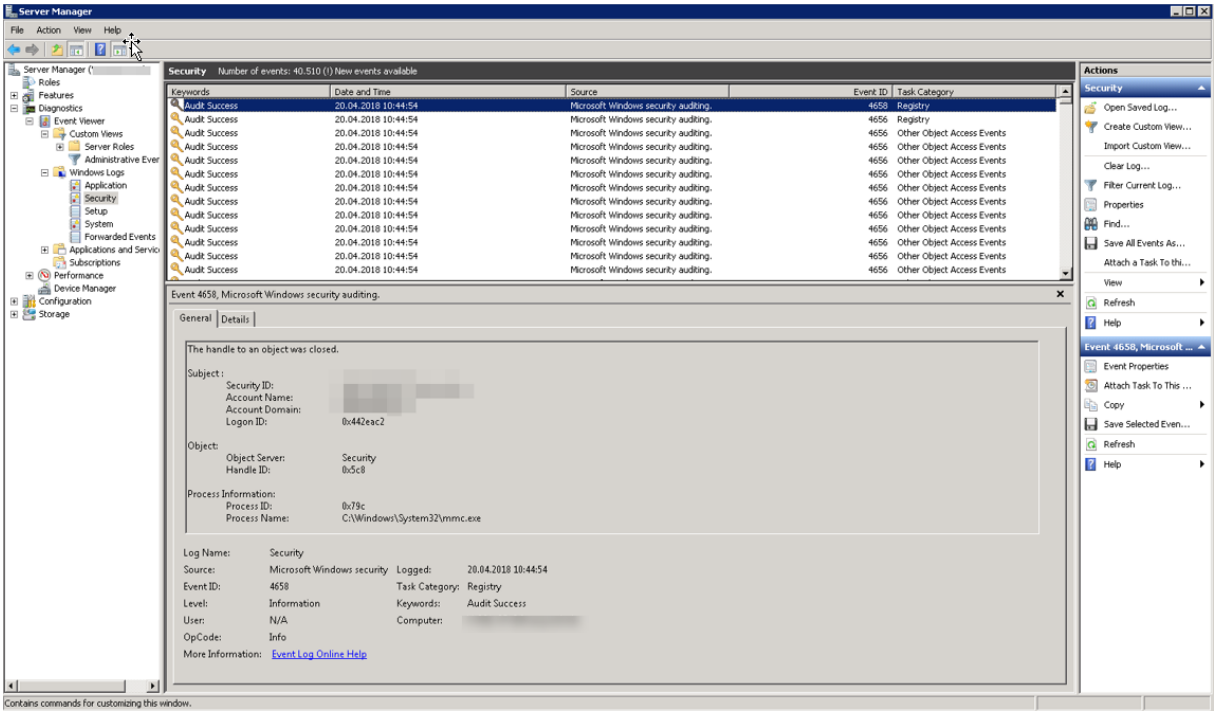
Windows-Filtering-Platform

Sollte das Security LOG mit Event-IDs 5156 volllaufen, dann kann folgendes unternommen werden.



Abschalten des Loggings über die CMD:

auditpol /set /subcategory:"Filtering Platform Connection" /success:disable /failure:enable

auditpol /set /subcategory:"Filtering Platform Connection" /success:disable

Abschalten des Loggings über eine Richtlinie:

POLICIES > WINDOWS SETTINGS > SECURITY SETTINGS > AUDIT POLICY > AUDIT OBJECT ACCESS settings:

Was steckt dahinter?

Die Windows Firewall Verbindungen werden durch die Aktivierung von "Filter Platform Policy Change" überwacht. Je nach Einstellung werden gescheiterte oder/auch erfolgreiche Verbindungen ins Ereignissprotokoll geschrieben. Durch die Aktivierung der Überwachung gehören diese Ereignisse nachher zu den TOP 10 der Vorkommnisse.

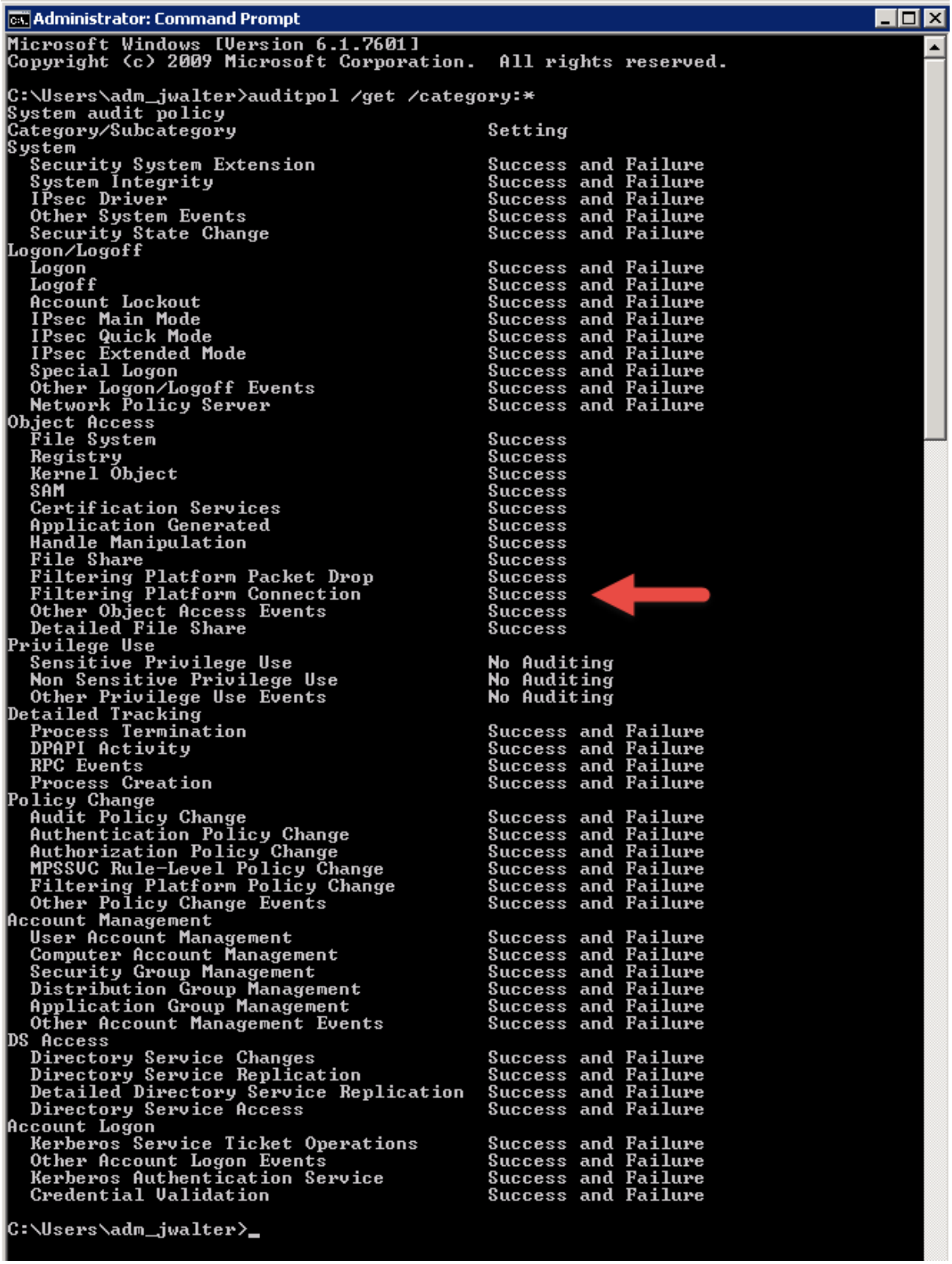
Windows-Filtering-Platform

Events:

5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
5140	A network share object was accessed.
5150	The Windows Filtering Platform blocked a packet.
5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
5156	The Windows Filtering Platform has allowed a connection.
5157	The Windows Filtering Platform has blocked a connection.
5158	The Windows Filtering Platform has permitted a bind to a local port.
5159	The Windows Filtering Platform has blocked a bind to a local port.

Windows-Filtering-Platform

Vorher aktiv:



Windows-Filtering-Platform

Nachher inaktiv:

Es werden ab sofort keine Logs mehr geschrieben.

Erstellt von Jörn Walter **24.04.2018**