Event-ID 4697

Wenn dieses Event durch ein Tool, wie z.B. AD-Audit von Manage Engine überwacht wird, dann kommt es folgender E-Mail-Benachrichtigung, sofern diese konfiguriert ist.

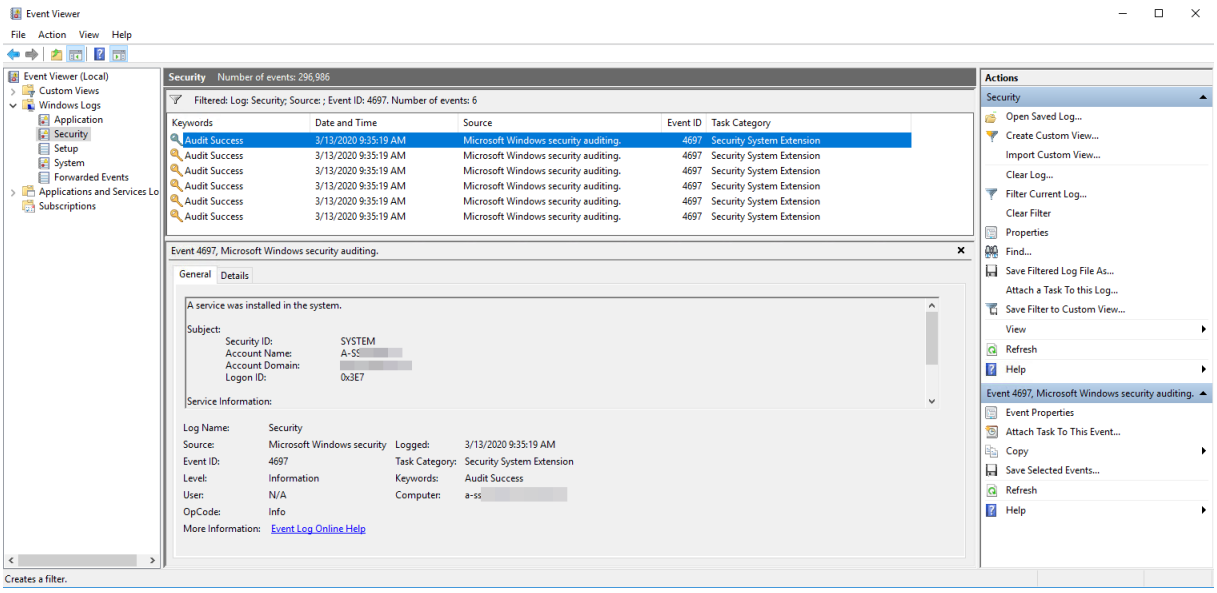
Viele Fragen sich was das bedeutet und was sie mit dieser Benachrichtigung anfangen sollen.

In diesem Dokument möchte ich lediglich erklären, was das Event zu bedeuten hat.

Alert Profile Name: Joern : View Alerts
Alert Message: Unable to install a service for the machine a-s
Severity: Critical

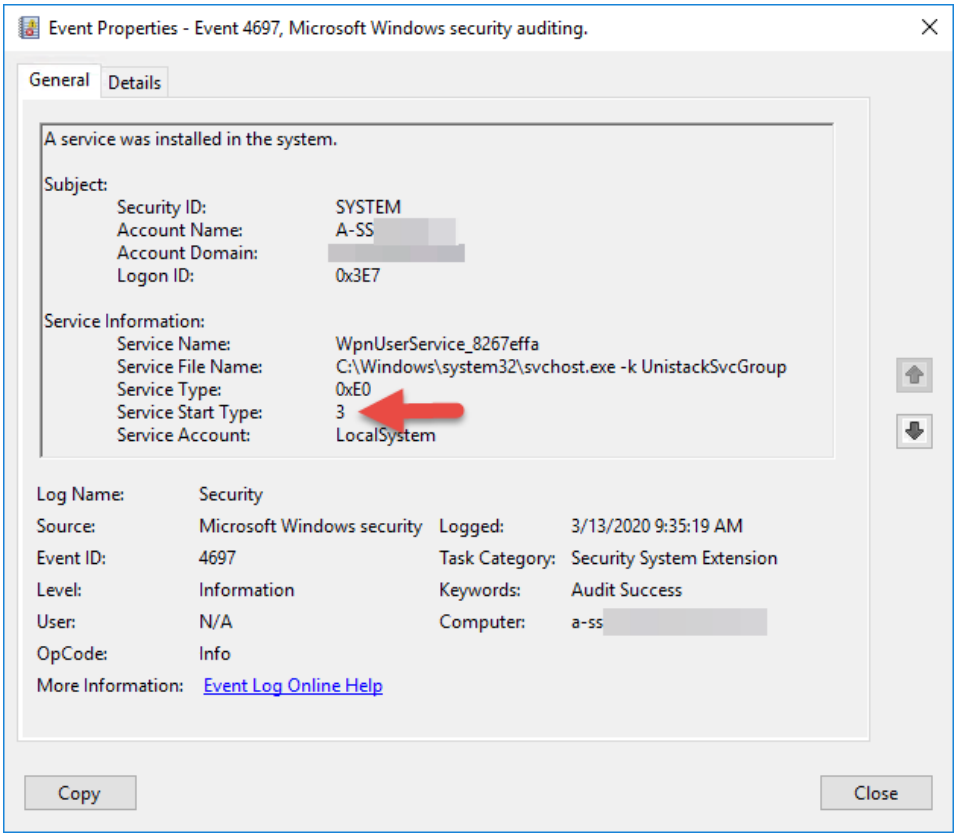
Event Details	
Event Code	8
Message	Unable to install a service for the machine a-ssb-ads1.easycash.de
Name	-
Account Name	-
Type	-
When	13/03/2020 09:35:19 AM
Remarks	A service was installed in the system.
Event Number	4697
Event Type Text	Success
File Name	-
Where	a-ss
Record number	1965789263
Start Type	-

Einsicht in den Event Viewer:

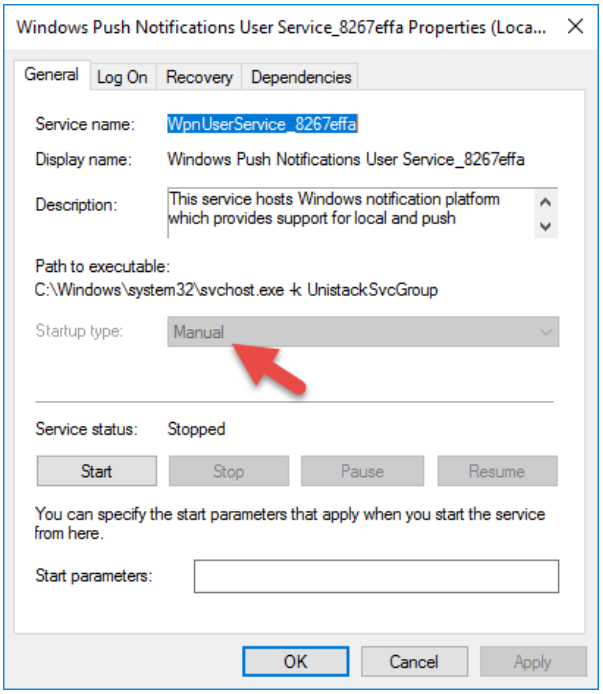


Event-ID 4697

Dieser Eintrag wird geschrieben, sobald ein Dienst der auf „Manuell" eingestellt ist, gestartet wurde. Es folgt je nach Einstellung ein Success oder Failure.



Der Service Start Type ist = 3. Das bedeutet „Manuell".



Event-ID 4697

Service-Start-Typen:

Value	Diensttyp	Description
0	Boot	Ein vom Systemladeprogramm gestarteter Gerätetreiber. Dieser Wert ist nur für Treiber Dienste gültig.
1	System	Ein Gerätetreiber, der von der Funktion IoInitSystem () gestartet wurde. Dieser Wert ist nur für Treiber Dienste gültig.
2	Automatisch	Ein Dienst, der vom Dienststeuerungs-Manager beim Systemstart automatisch gestartet wurde.
2	Automatisch verzögert	Ein Dienst, der nach dem Start aller automatischen Startdienste gestartet wurde, sowie eine Verzögerung. Verzögerte automatische Start Dienste werden einzeln in serieller Manier gestartet.
3	Manual	Manueller Start. Ein Dienst, der vom Dienststeuerungs-Manager gestartet wird, wenn ein Prozess die Start-Funktion aufruft.
4	Deaktiviert	Ein Dienst, der nicht gestartet werden kann. Versuche, den Dienst zu starten, führen zum Fehlercode ERROR_SERVICE_DISABLED.

https://docs.microsoft.com/de-de/windows/security/threat-protection/auditing/event-4697