Inhalt

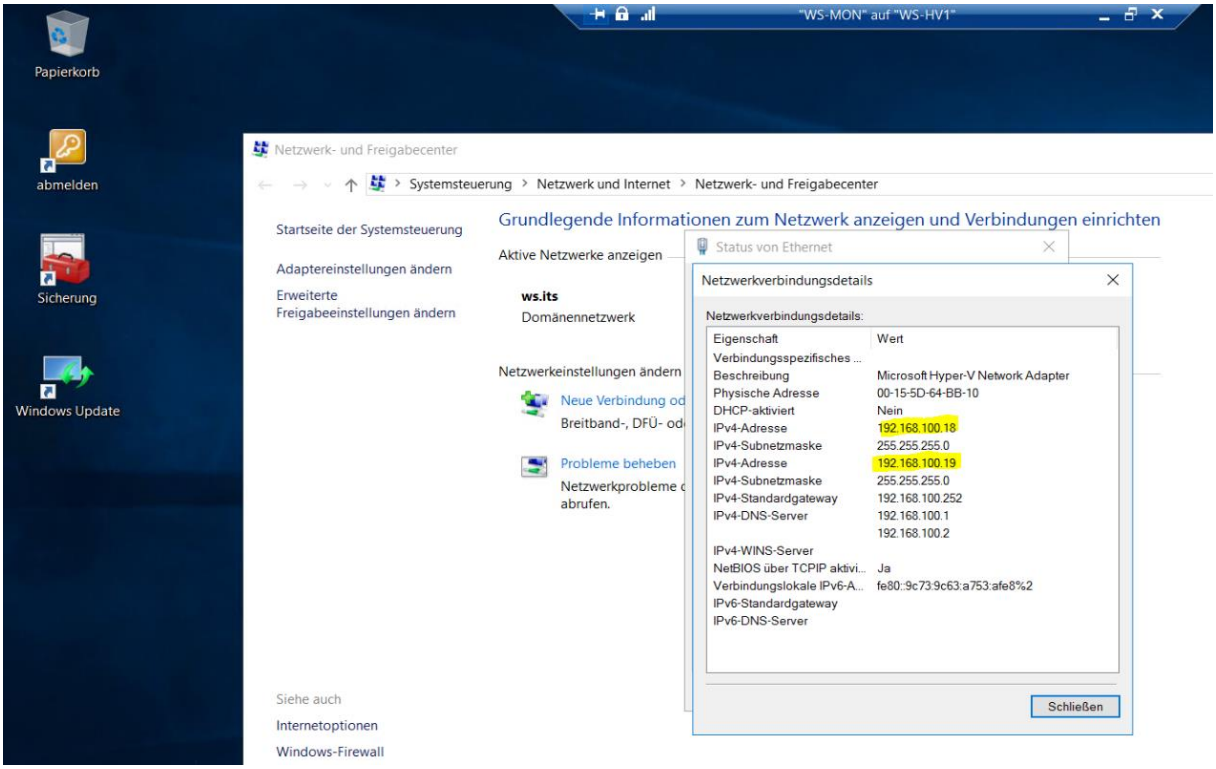
1. Szenario

Im Netzwerk soll Microsoft Advanced Thread Analysis (ATA) bereitgestellt werden. Es liegen mir kaum Erfahrungswerte vor. Da die Installation abgesehen von den Gateway-Services auf den DCs keinerlei Änderungen im Netzwerk bedingt, installiere ich nativ.

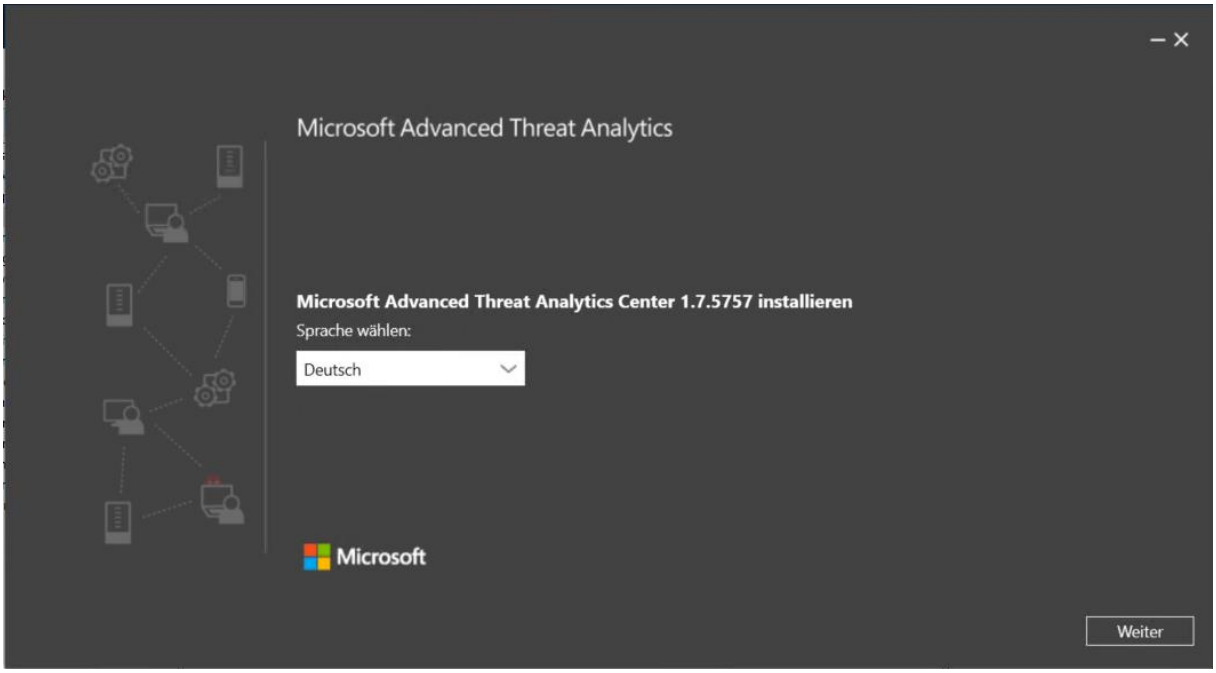
2. Bereitstellung

Bereitstellung des neuen Servers

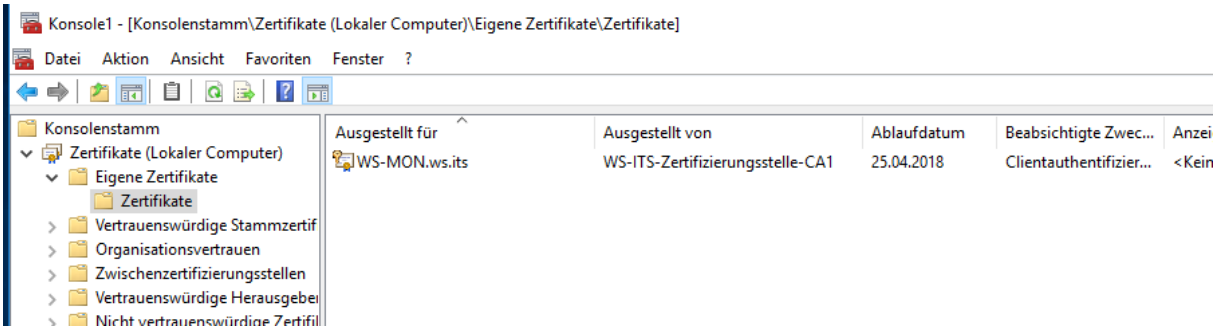
Der neue Server benötigt eine AD-Integration und 2 IP-Adressen: eine für den Monitor-Service und eine für die administrative Konsole (WebApp). In meinem Fall installiere ich einen Windows Server 2016 als VM:

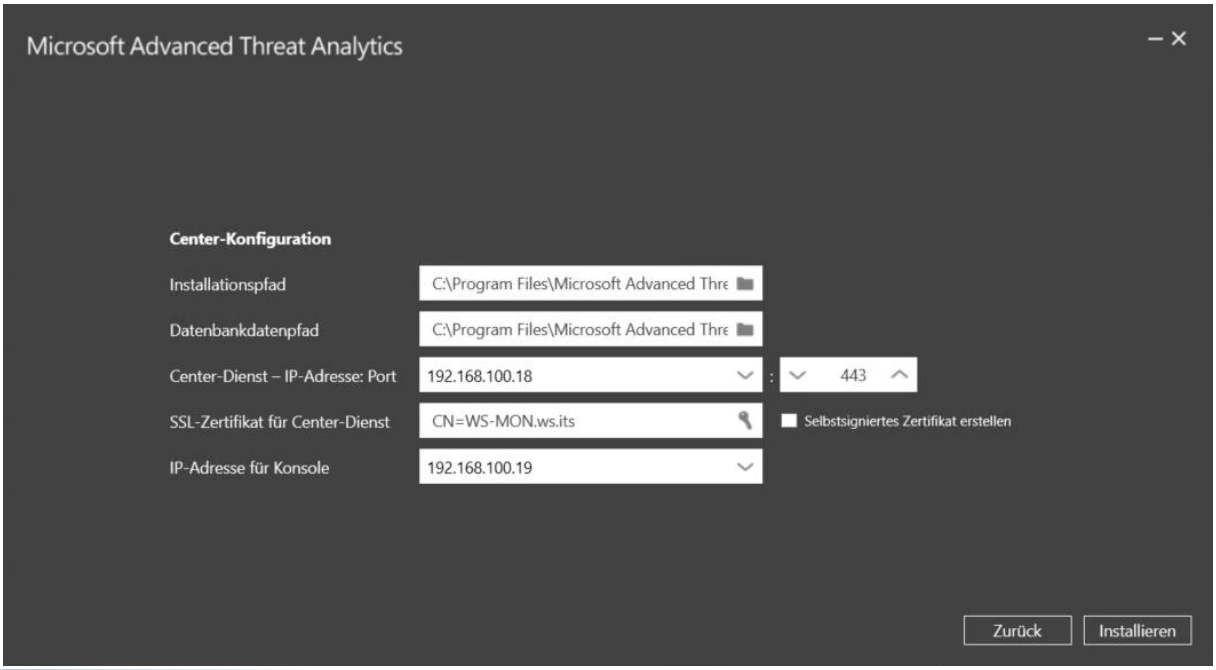


Nun starte ich das Setup über ein ISO. Die Anzeigesprache lege ich auf Deutsch fest:



Der WebService wird über ein Sicherheitszertifikat abgesichert. Das Setup bietet hier ein SelfSigned an. Dank der eigenen CA mit AD-Integration liegt bereits ein Zertifikat für die VM vor. Noch kann ich den Verwendungszweck nicht abschätzen, aber wenn ich später ein anderes Zertifikat verwenden möchte, wird es mit Sicherheit eine Möglichkeit zum Austausch geben (Zertifikate laufen ja auch ab!):

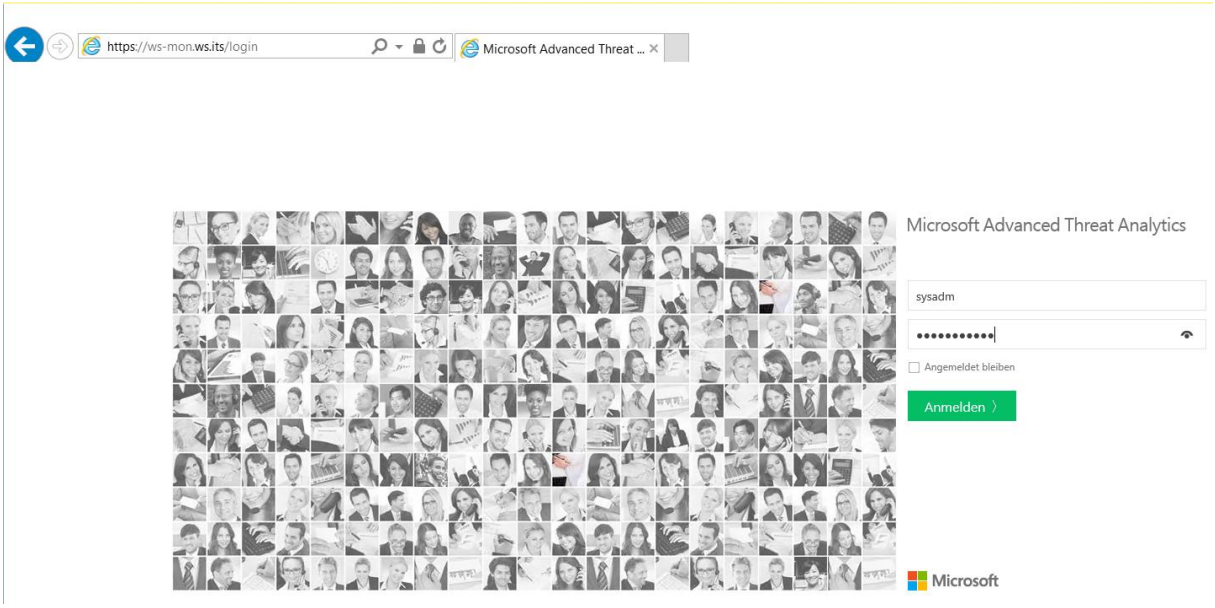




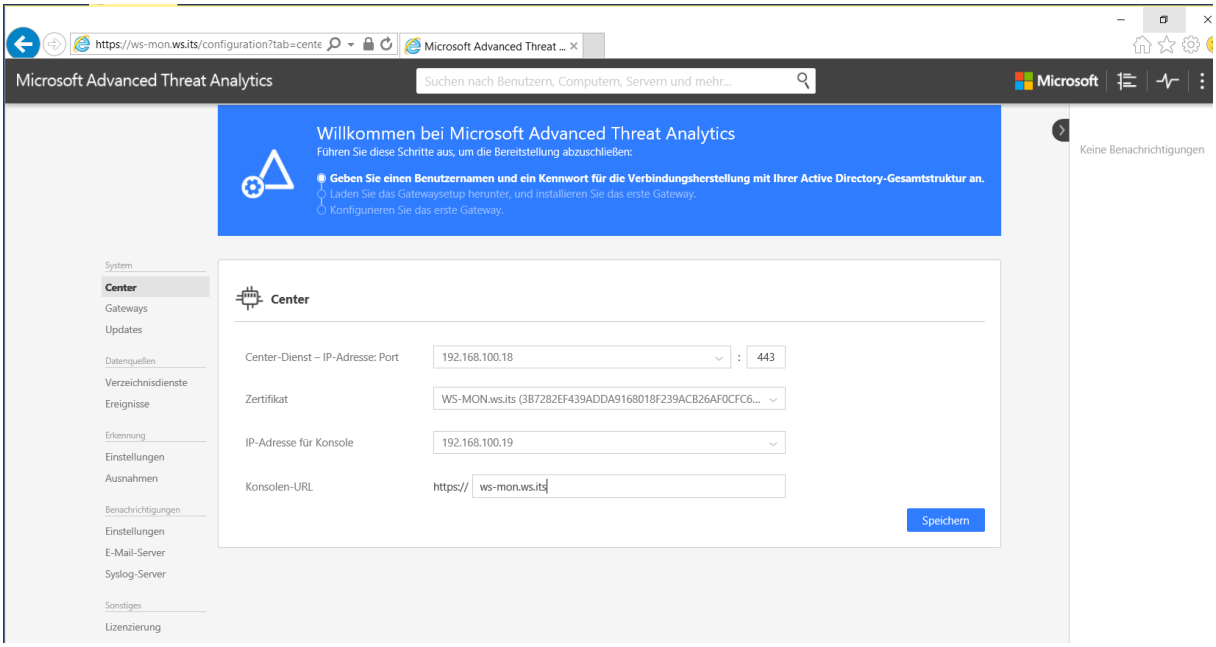
Die Installation dauert nicht lange und läuft problemlos durch.

Erstkonfiguration

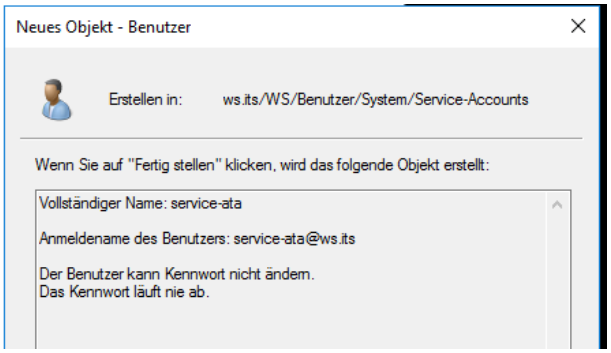
Nach der kurzen Installation steht die Konfiguration über eine Website bereit. Diese startet leider über die IP in der URL. Das habe ich im Browser-Aufruf bereits angepasst:



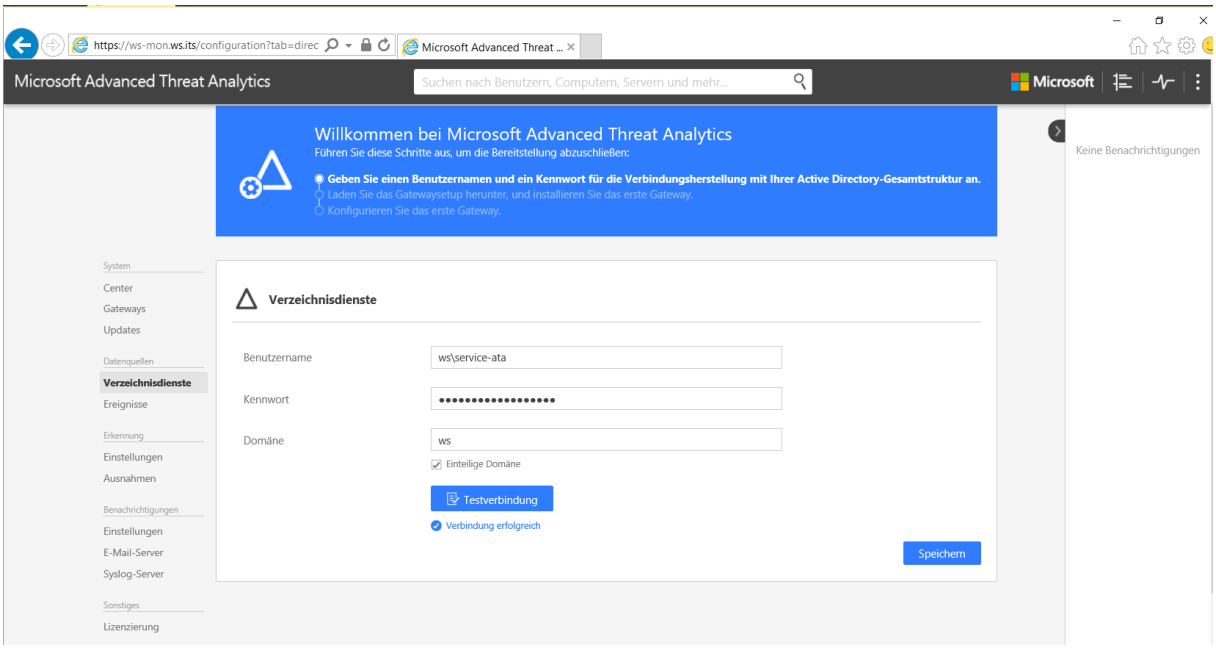
Direkt auf der Hauptseite finde ich den Punkt, um das Zertifikat auszutauschen:



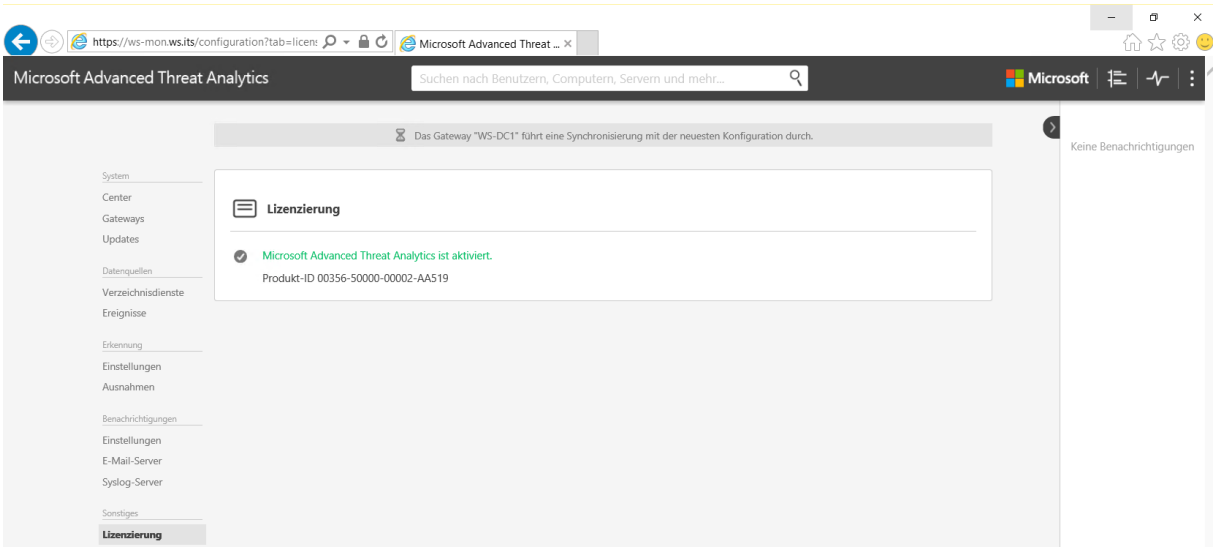
Für den Zugriff zu den Verzeichnisdiensten wird ein Benutzer benötigt. Dafür erstelle ich einen nicht-privilegierten AD-Benutzer. Da keine Rechte erforderlich sind, setze ich das Kennwort auf „läuft nie ab“:



Diesen Benutzer trage ich ein. Der Test funktioniert:

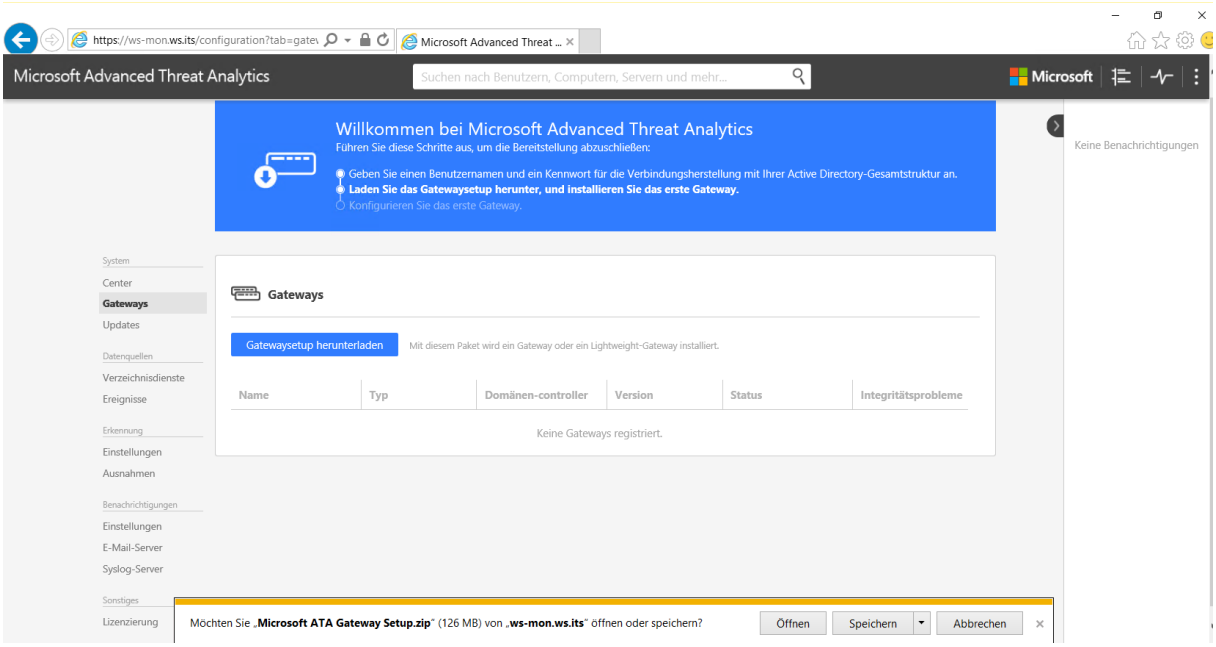


Nun fehlt noch die Aktivierung des ATA:

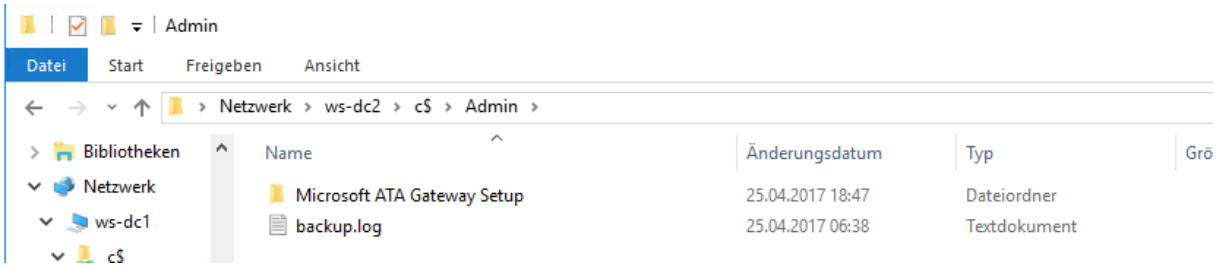


Installation der Gateways

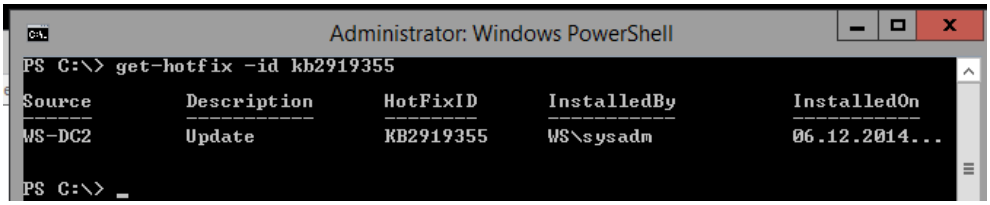
Nun muss ich den Gateway-Service auf meinen DCs installieren. Den Installer kann ich direkt in der WebAnwendung herunterladen. Die Alternative mit der PortSpiegelung teste ich vielleicht später.



Das Setup kopiere ich auf meine beiden DCs:

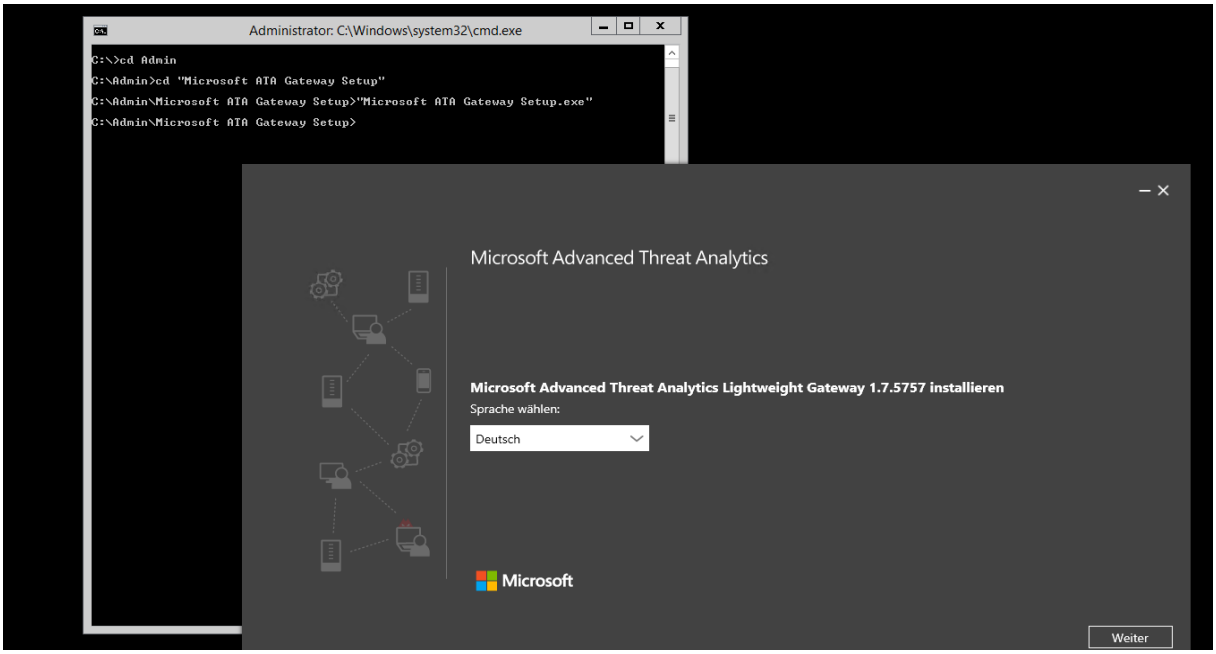


Meine 3 DCs laufen unter Windows Server 2012 R2 als ServerCore. Als Voraussetzung auf Windows Server 2012 R2 ist ein Update erforderlich. Dieses ist bereits installiert:

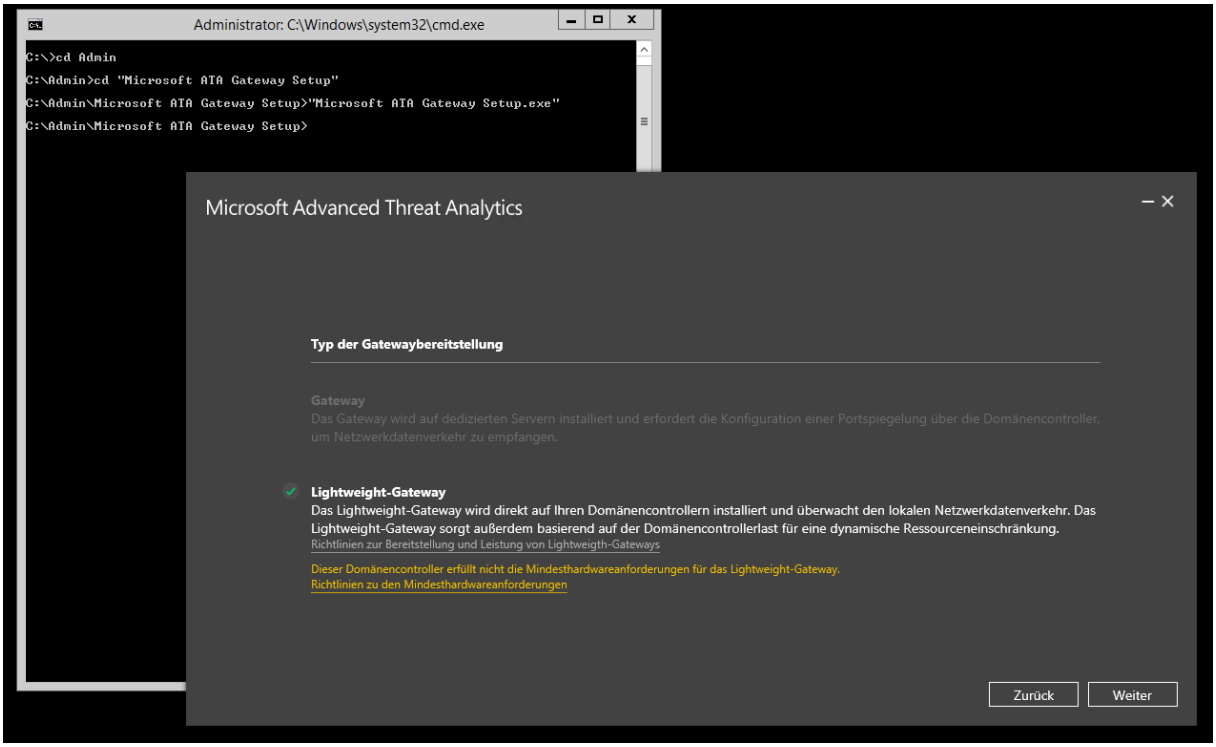


Ich installiere das Gateway zunächst nur auf 2 DCs. Der 3. DC steht in einem anderen Standort und aktuell kann ich den erforderlichen Traffic über die WAN-Verbindung nicht abschätzen.

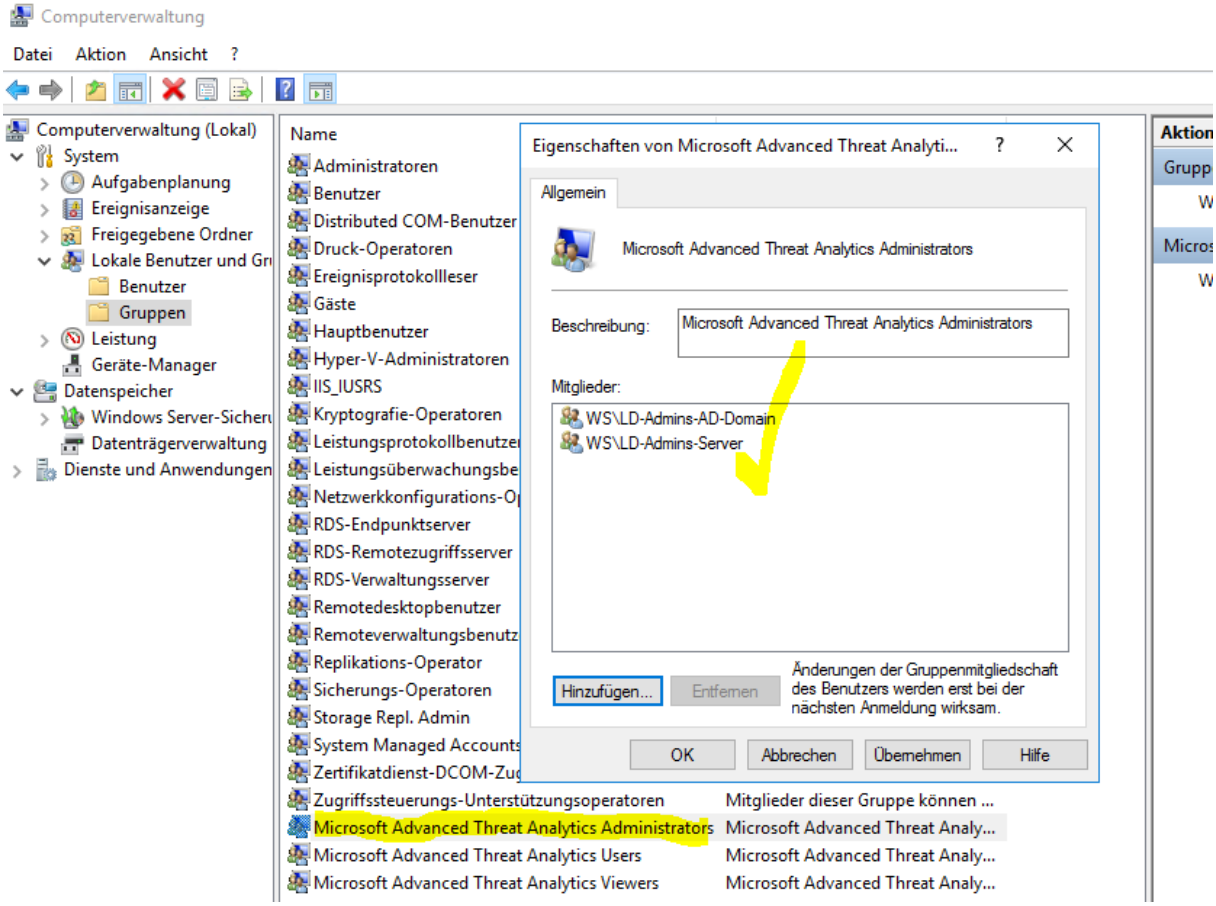
Das Setup lässt sich über die cmd des Server-Core starten:



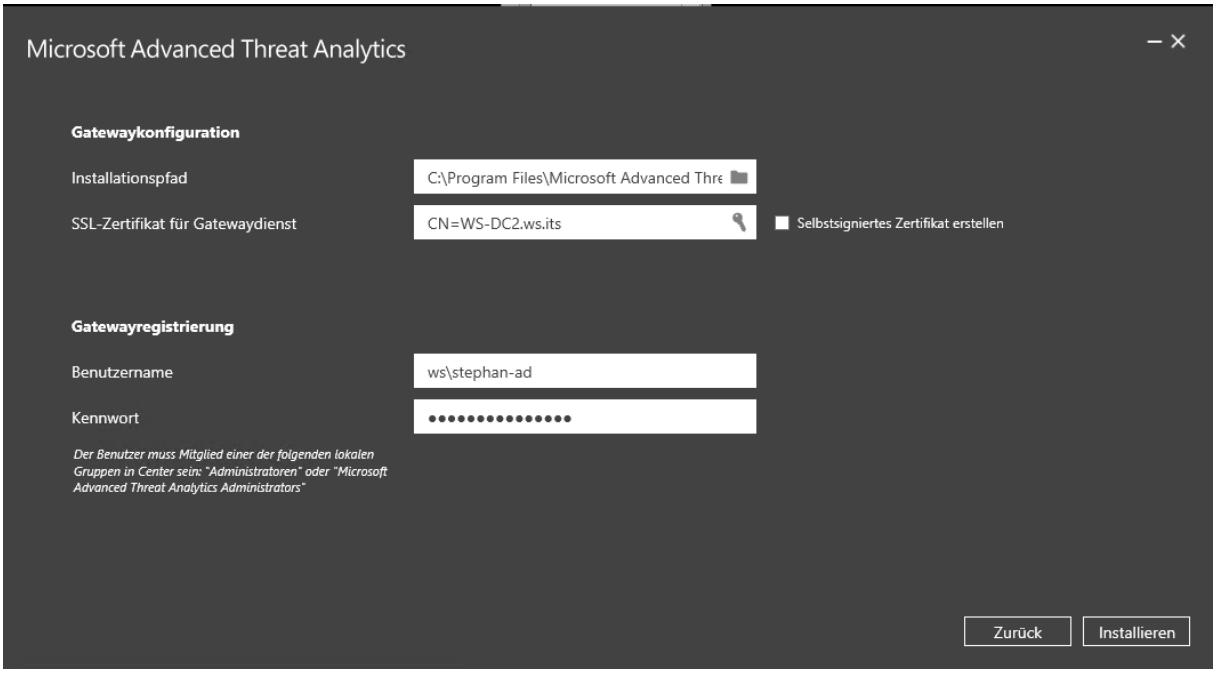
Die Meldung zu den Mindesthardwareanforderungen ignoriere ich und setze das Setup fort:



Das Gateway muss sich am ATA registrieren. Dafür wird ein Benutzer benötigt, der auf dem ATA die erforderlichen Rechte hat. Auch die WebAnwendung wird durch eine Anmeldung gesichert. Ich trage auf dem ATA 2 Gruppen als ATA-Admins ein:

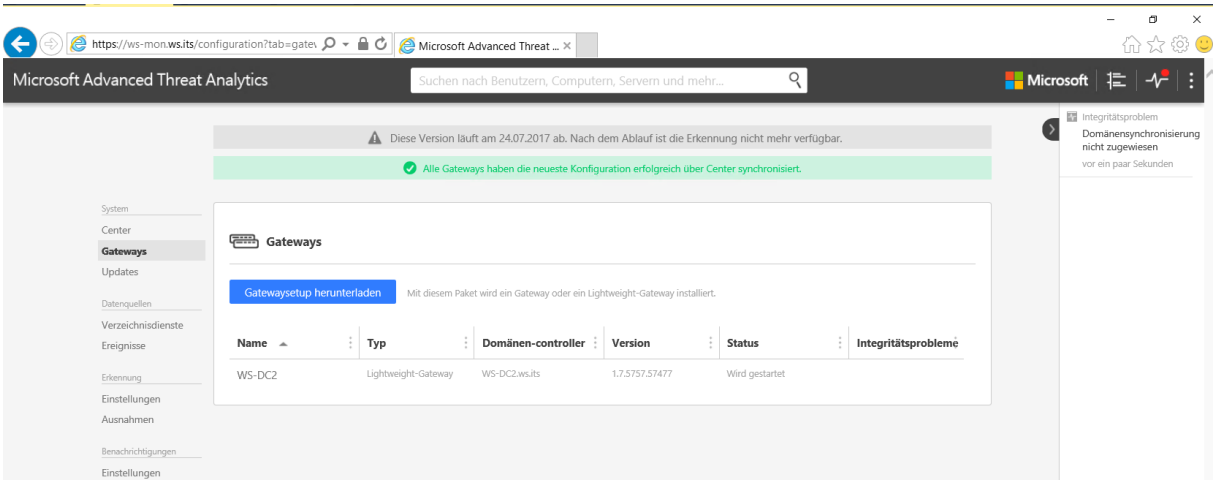


Auf dem DC setze ich nun noch das Zertifikat des DCs ein:

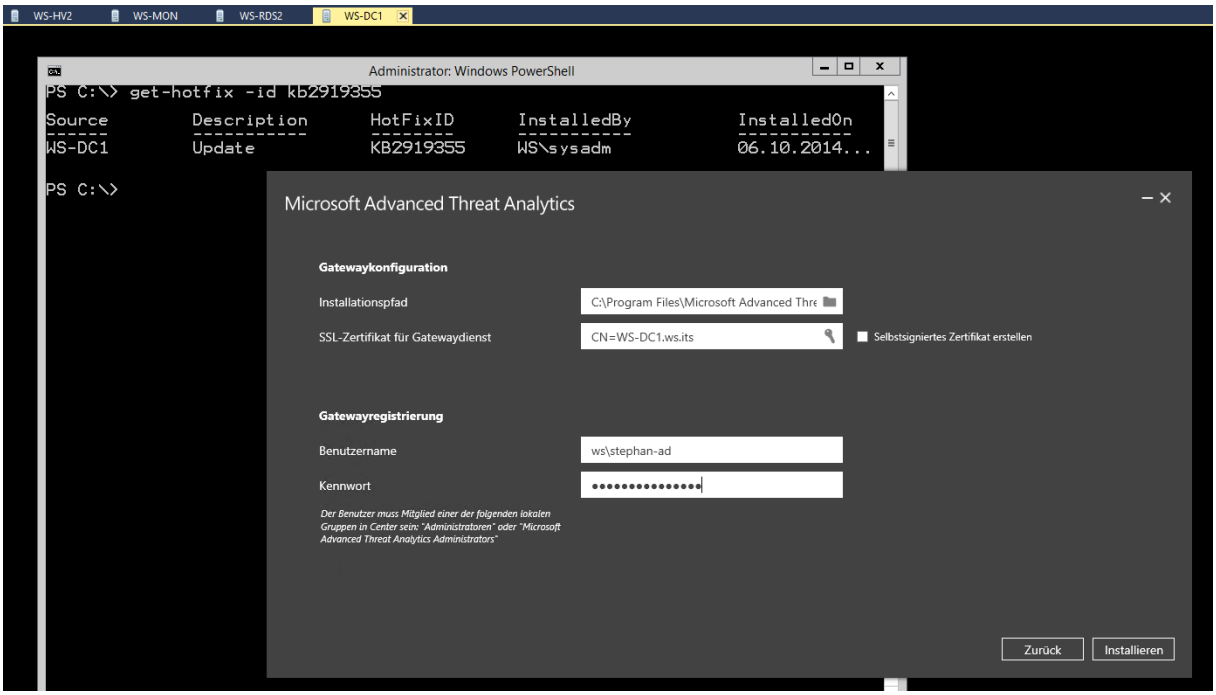


Das Setup läuft nun durch.

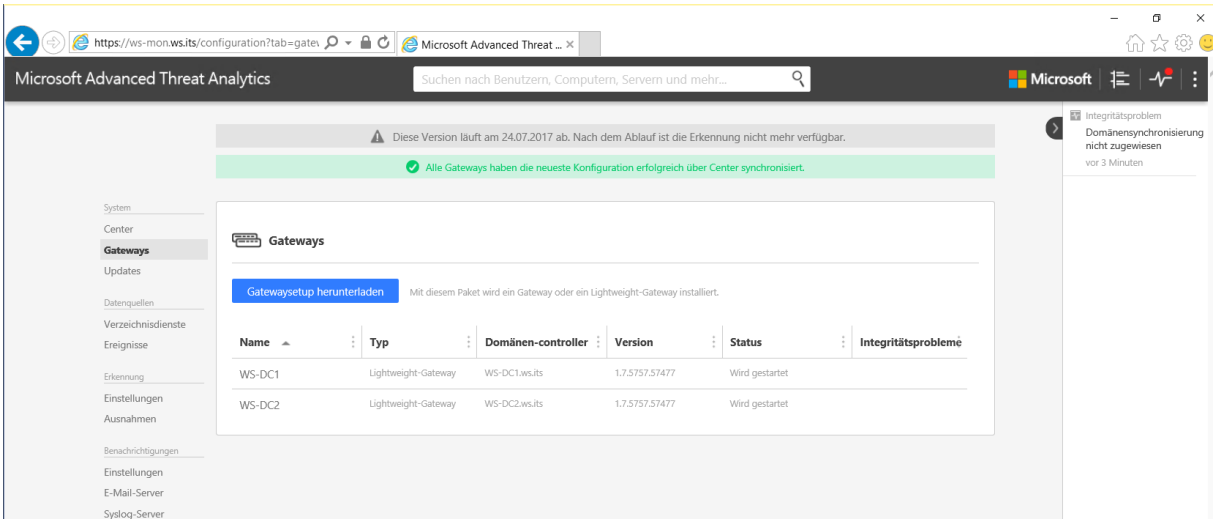
Im ATA meldet sich der DC:



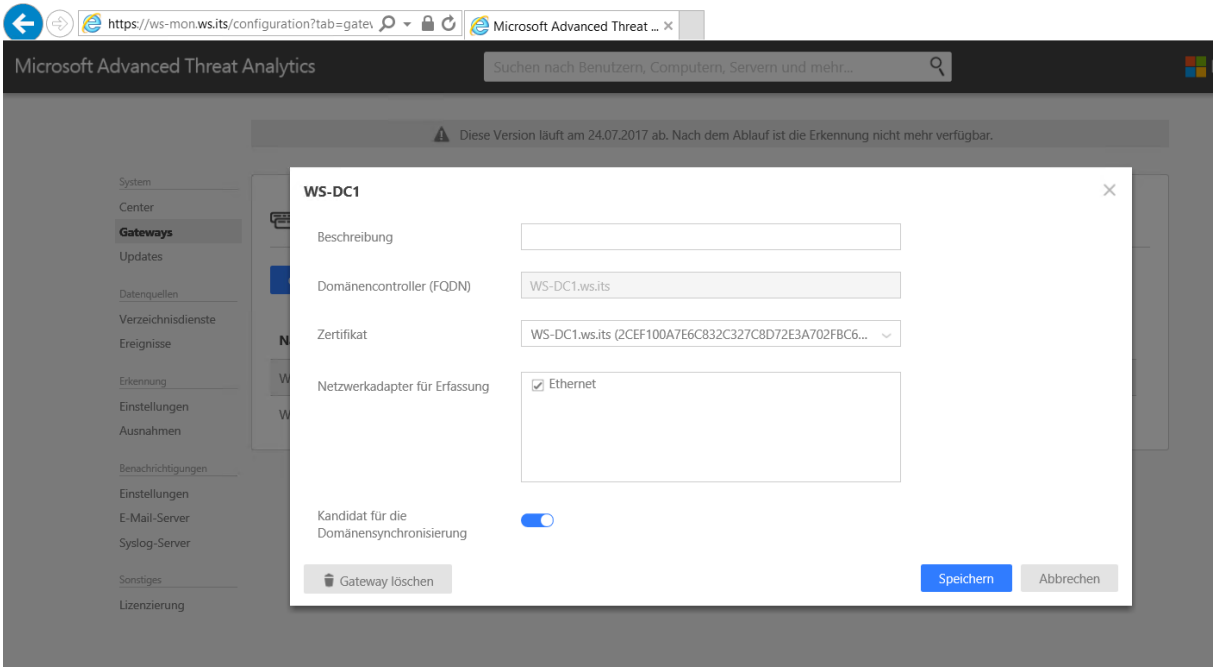
Den Prozess wiederhole ich auf dem 2. DC:



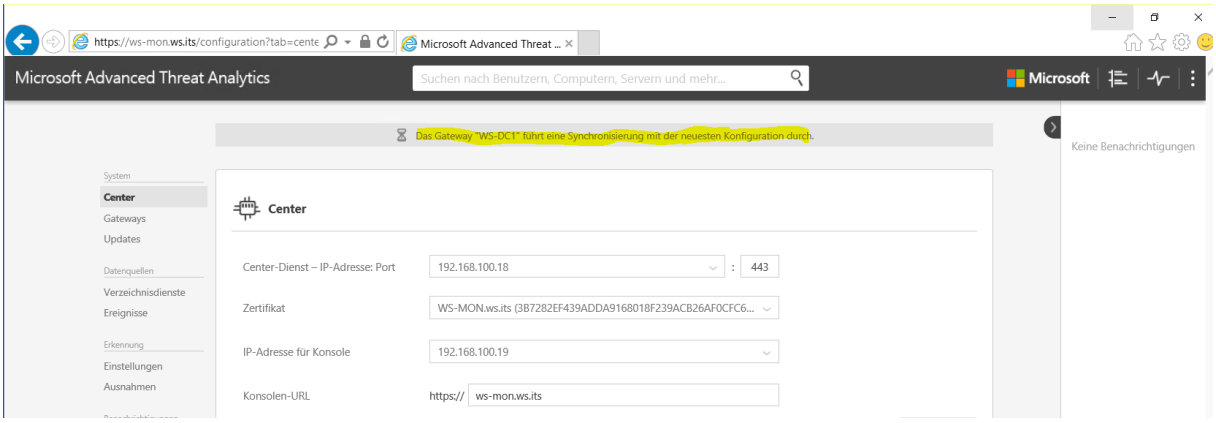
Auch dieser meldet sich beim ATA:



Mindestens ein (schreibbarer) DC muss als Synchronisierungs-DC konfiguriert sein, um dem ATA Änderungen des Ads bekannt zu machen. Ich konfiguriere beide DCs als Kandidaten:

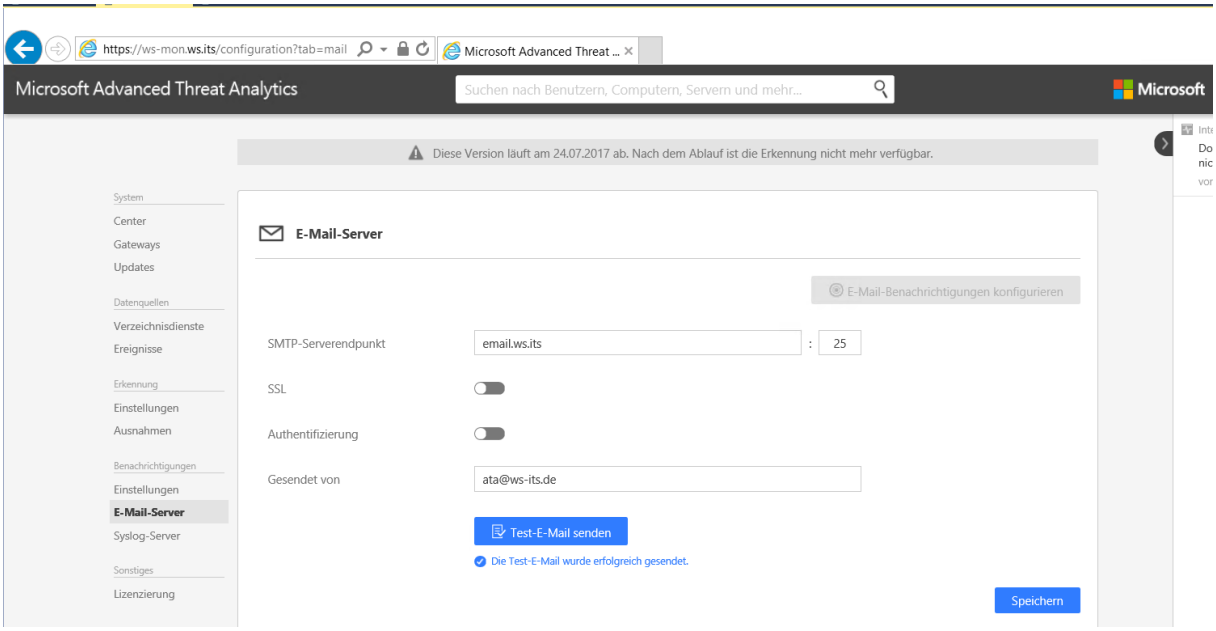


Der Sync wird automatisch gestartet:

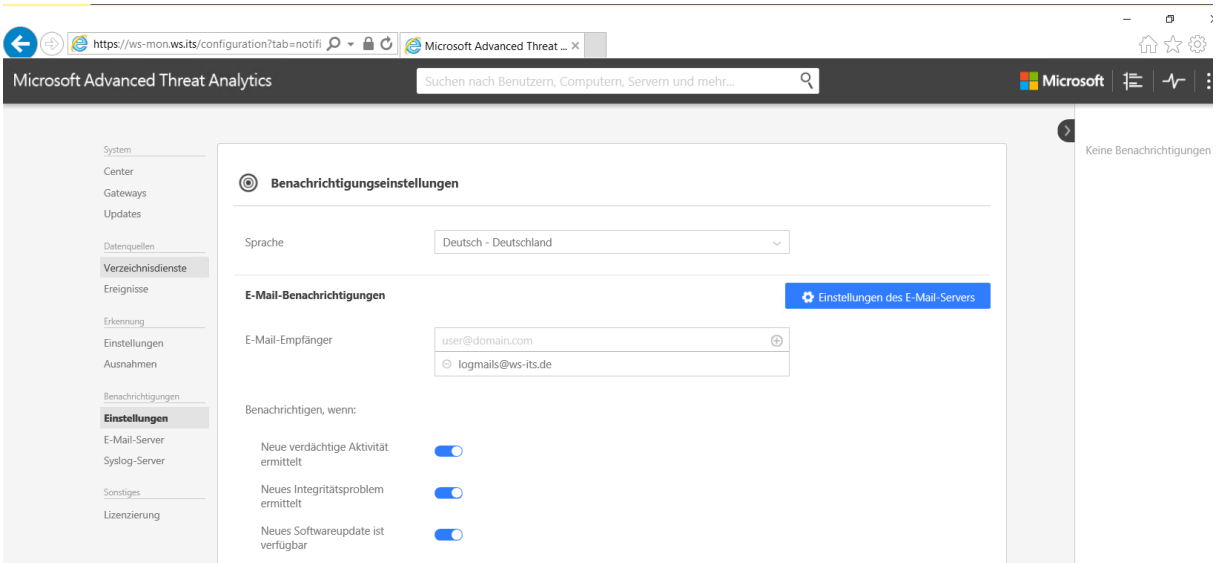


Konfiguration der Mail-Benachrichtigung

Das Monitoring ist nur dann sinnvoll, wenn wichtige Meldungen an Administratoren zugestellt werden können. In der Webanwendung kann man dazu den Mailversand konfigurieren:



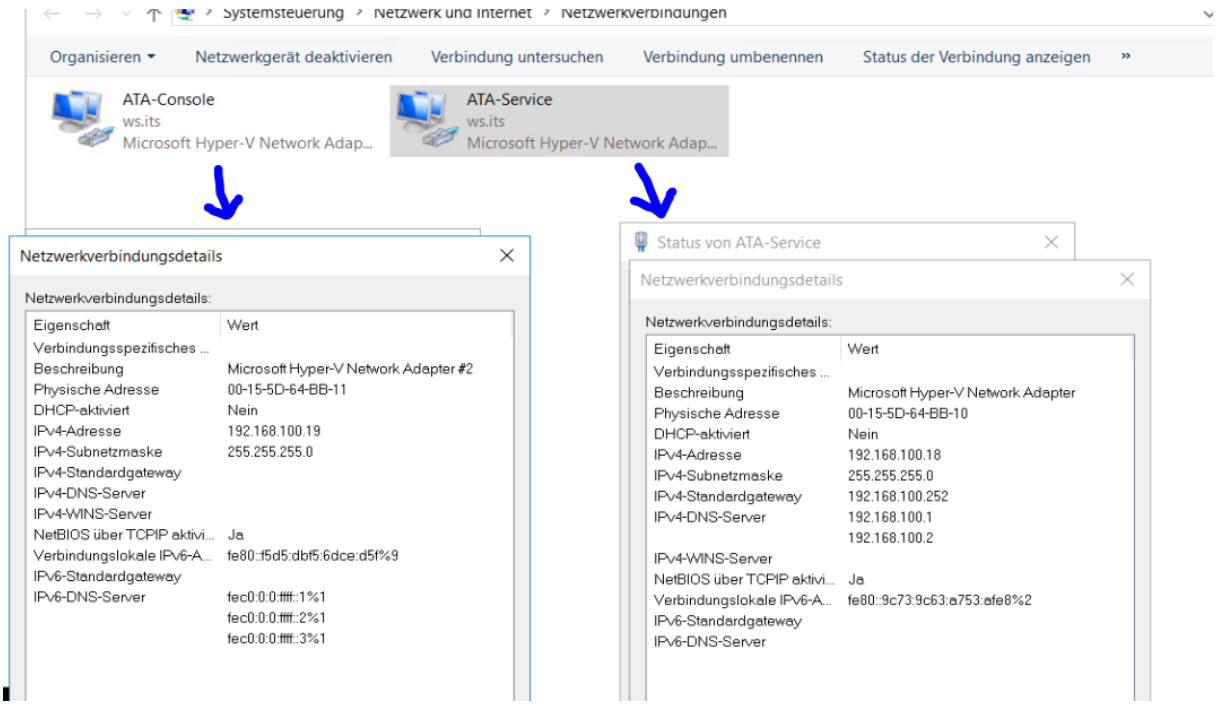
Die Operatoren werden bei den Benachrichtigungen konfiguriert:



Problem: DC-Synchronisierung funktioniert nicht

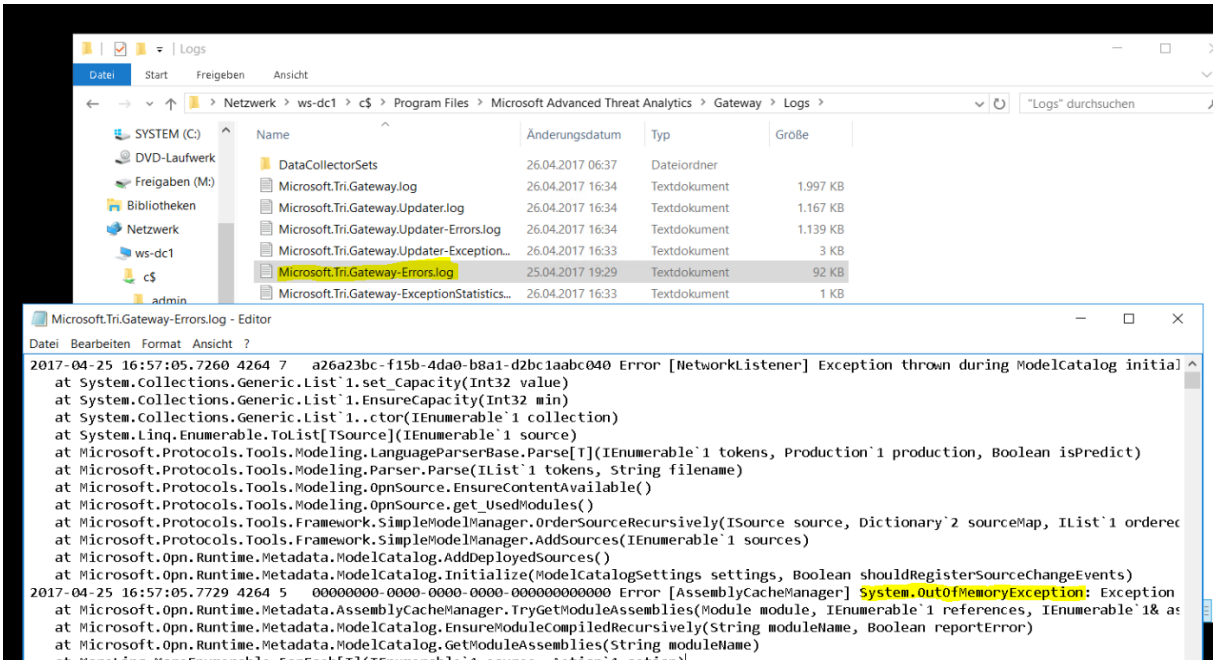
Auch nach längerer Zeit melden sich die beiden DCs nicht einsatzbereit. Ich kontrolliere den Zugriff. Da der ATA 2 IP-Adressen auf einer Netzwerkkarte konfiguriert hat und beide im DNS registriert, ist er aus Sicht des DCs über 2 IPs erreichbar. Da beide im gleichen Subnetz liegen, aber nur eine den ATA-Service aufgeschaltet hat, kann es eine 50-50-Chance geben, dass der DC seine Daten übertragen kann…

Ich gebe dem ATA-Server eine 2. Netzwerkkarte und übertrage die IP der WebAnwendung auf die 2. NIC. In den Optionen konfiguriere ich, dass die Adresse nicht im DNS eingetragen wird:



Im DNS lösche ich nun den Verweis auf die 2. IP, lösche auf den DCs den DNS-Cache und warte auf die Verbindung.

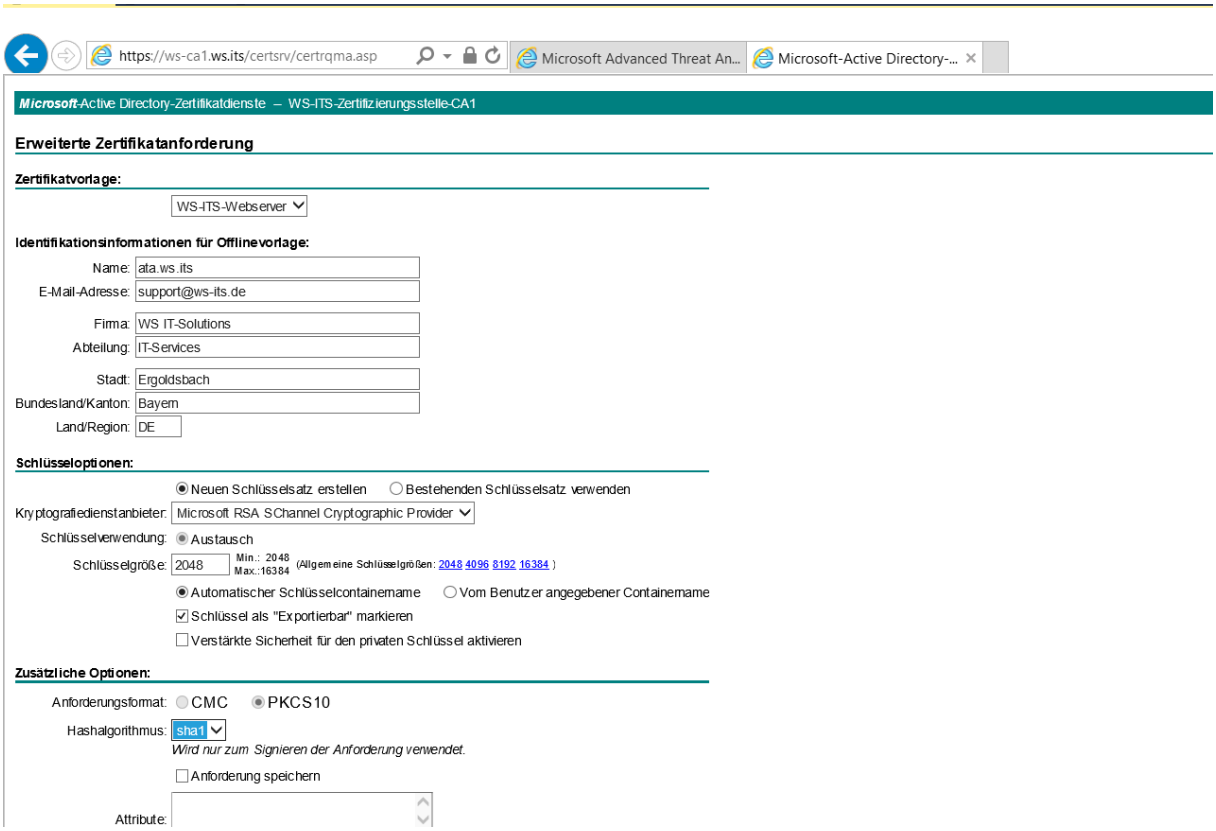
Leider startet der Gateway-Service auf den DCs immer wieder neu. In einem Logfile auf dem DC finde ich die Ursache: zu wenig Arbeitsspeicher (das Setup hat dies bereits angedeutet):



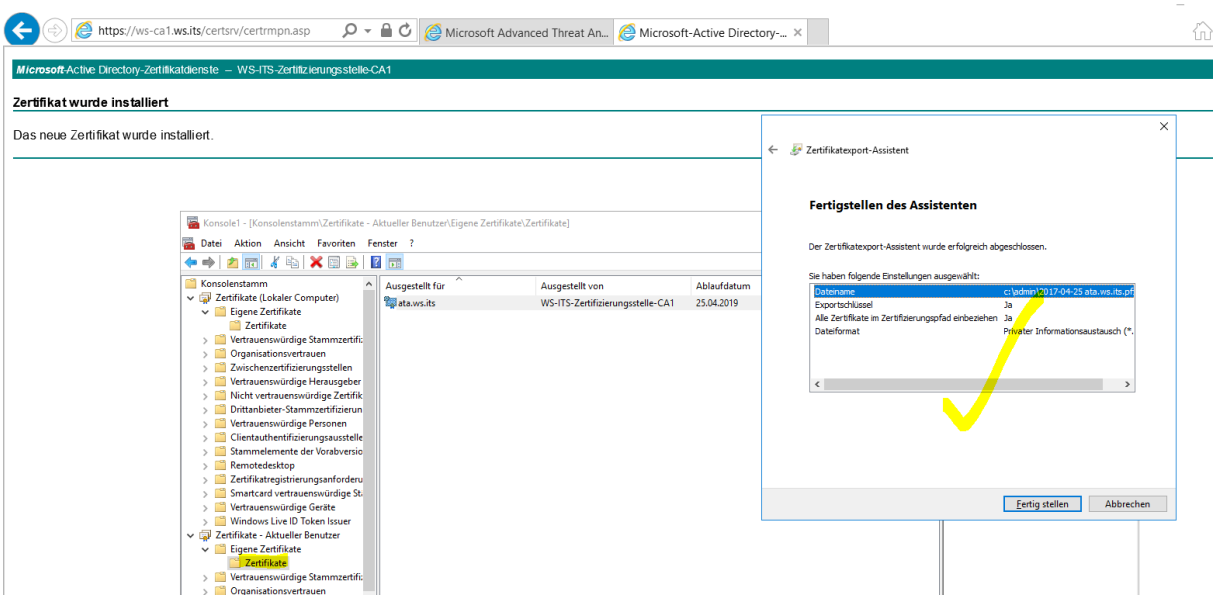
Da beide DCs VMs sind, konfiguriere ich einfach mehr RAM (3GB). Nun starten die Dienste. Und die Synchronisierung funktioniert. 😊

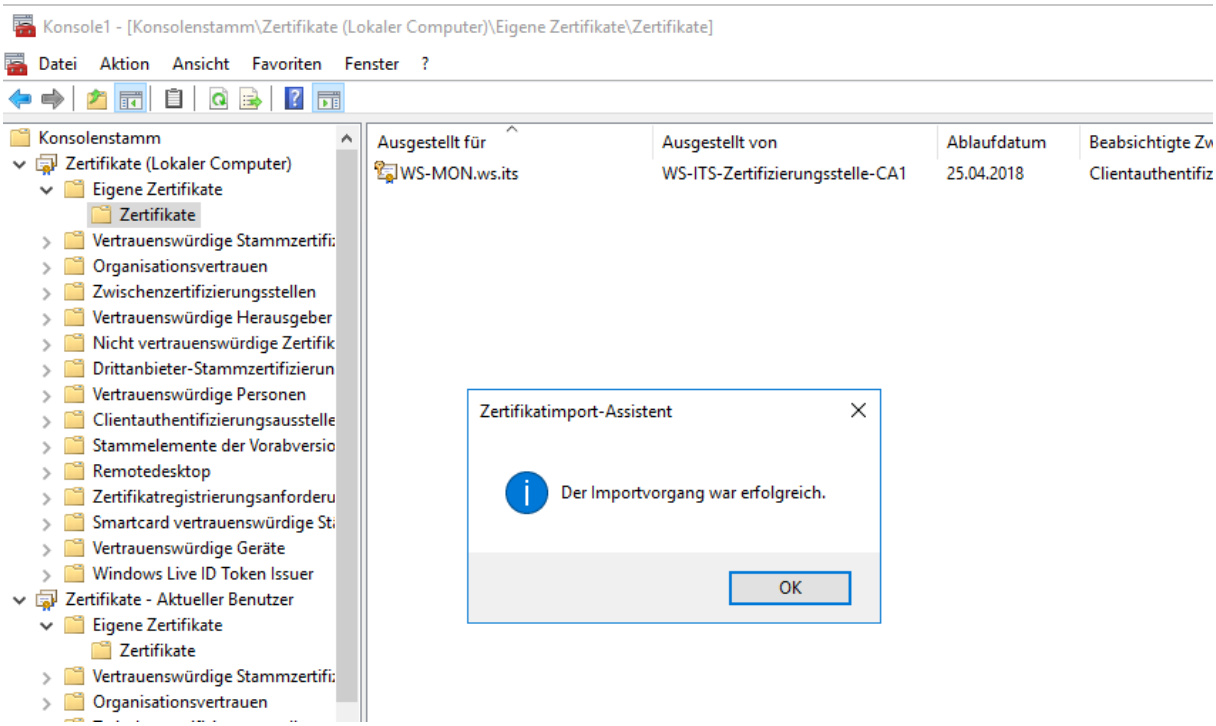
Austausch des Zertifikates und Isolation der IP-Adresse für die Webanwendung

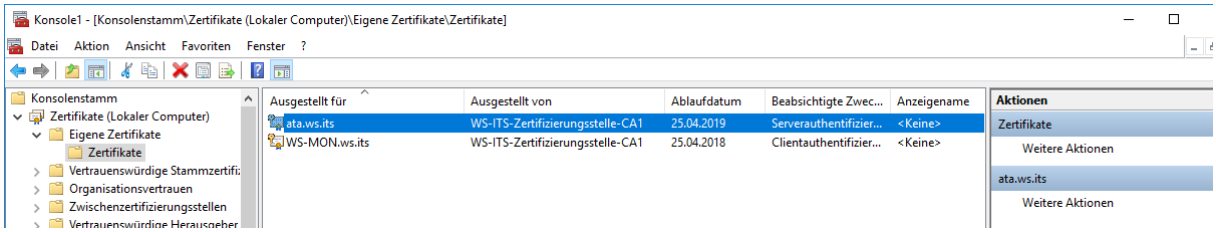
Damit ich nun die Webanwendung sauber ansprechen kann, stelle ich ein neues Zertifikat für den Namen ata.ws.its aus:



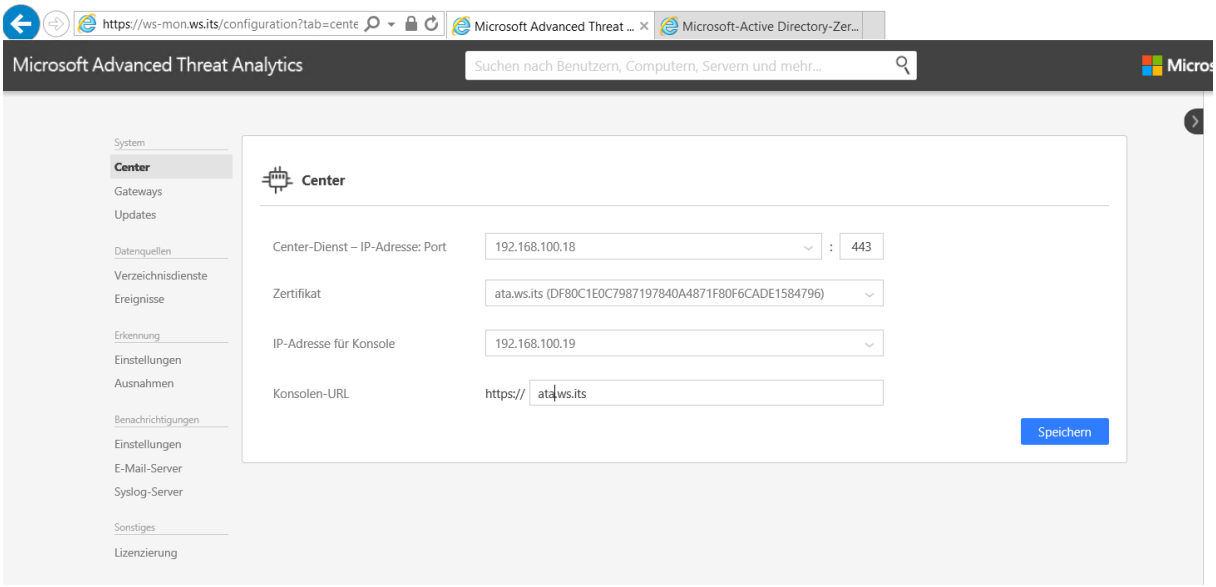
Das Zertifikat übertrage ich vom Benutzer auf den Computer durch Export und Import:

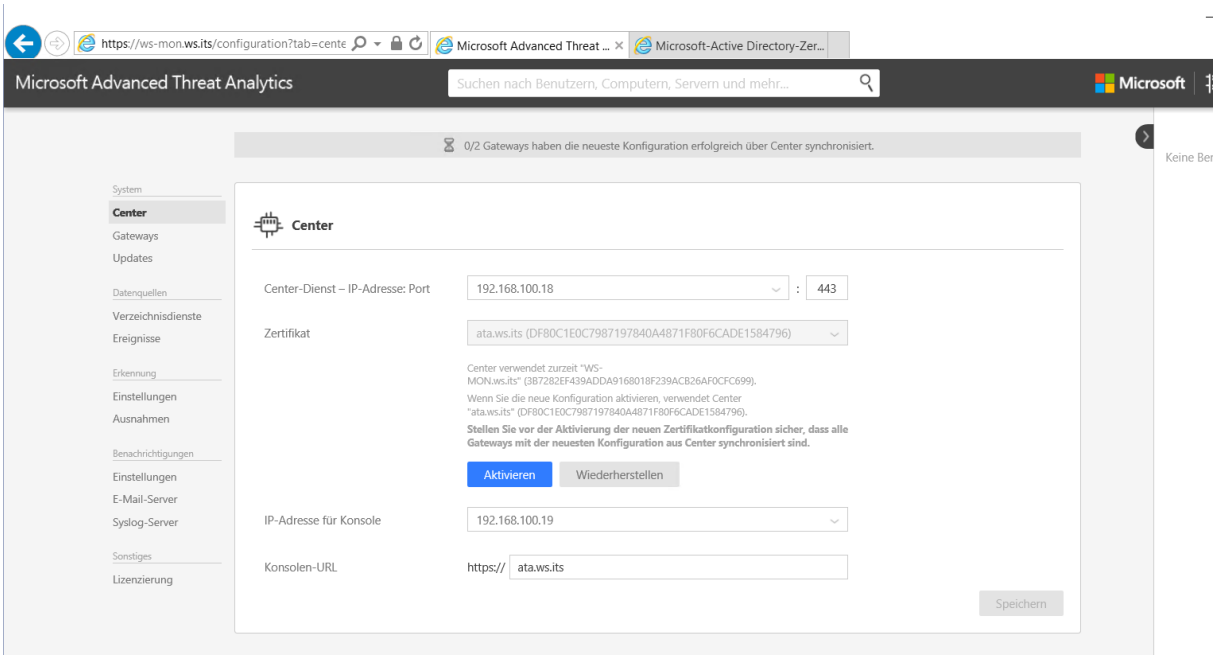




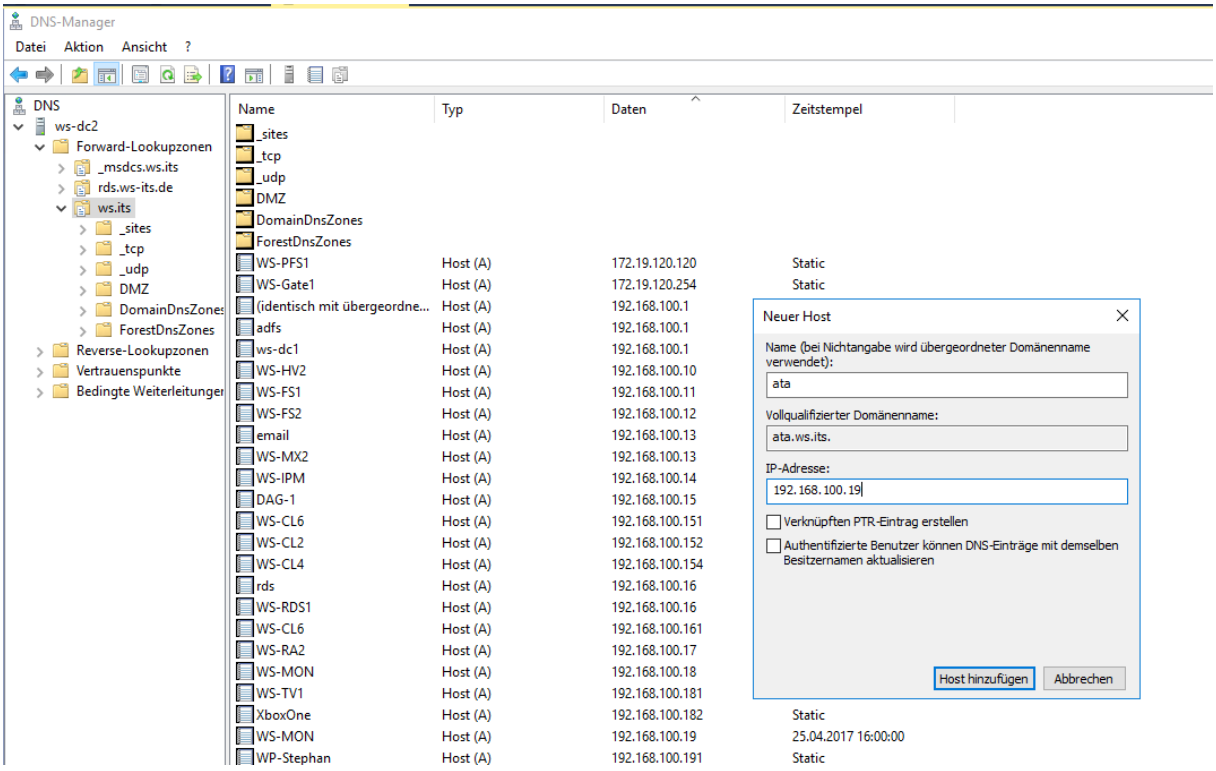


In der Webanwendung ändere ich nun das Zertifikat:

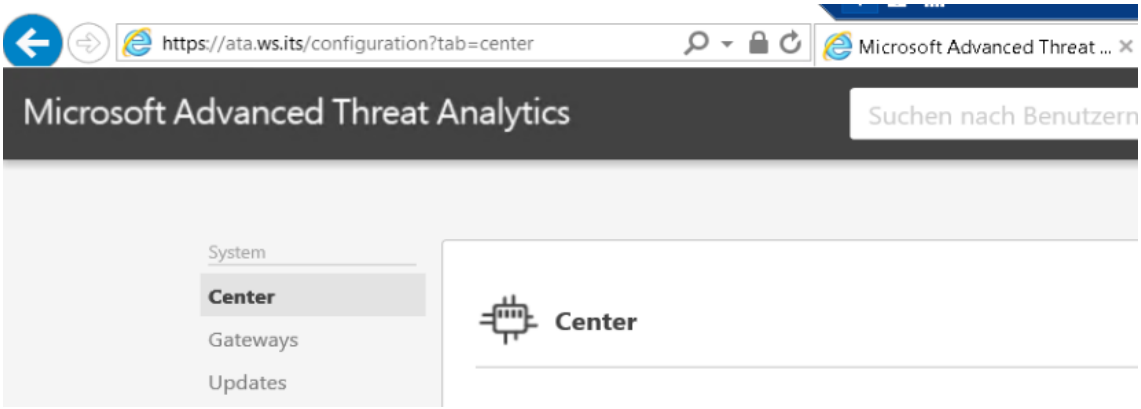




Im DNS trage ich nun einen HOST-A für ata.ws.its auf die IP des Servers ein:



Der Service ist nun über den neuen Namen erreichbar:

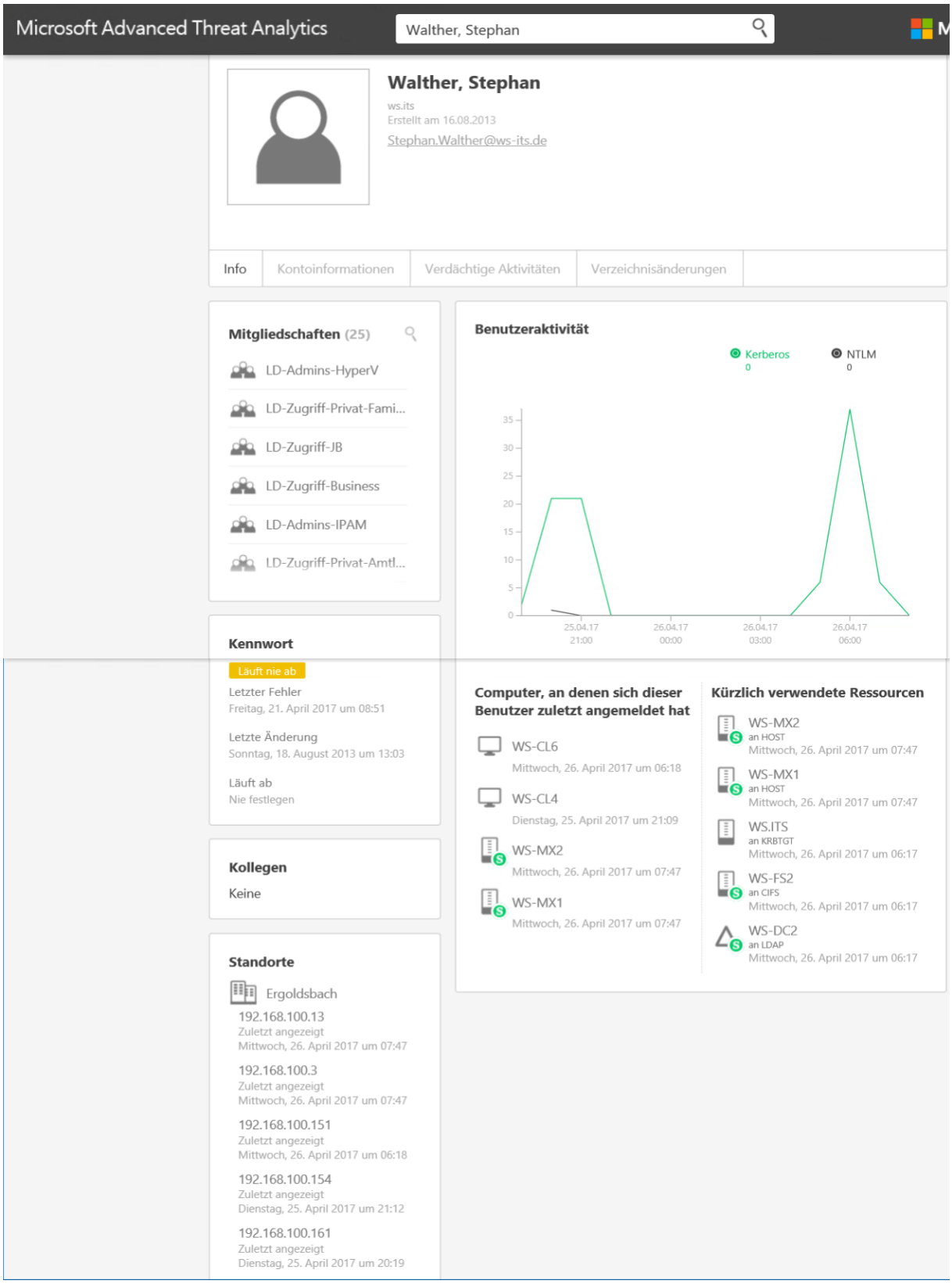

https://ata.ws.its/configuration?tab=center
Microsoft Advanced Threat ...
Microsoft Advanced Threat Analytics
Suchen nach Benutzern
System
Center
Gateways
Updates
Center

3. Testphase

Analyse der Entitäten

Mit der Zeit lernt ATA die Benutzer und die Domänencomputer kennen. Dabei merkt sich das System auch, welche Benutzer sich wo und wann anmelden.

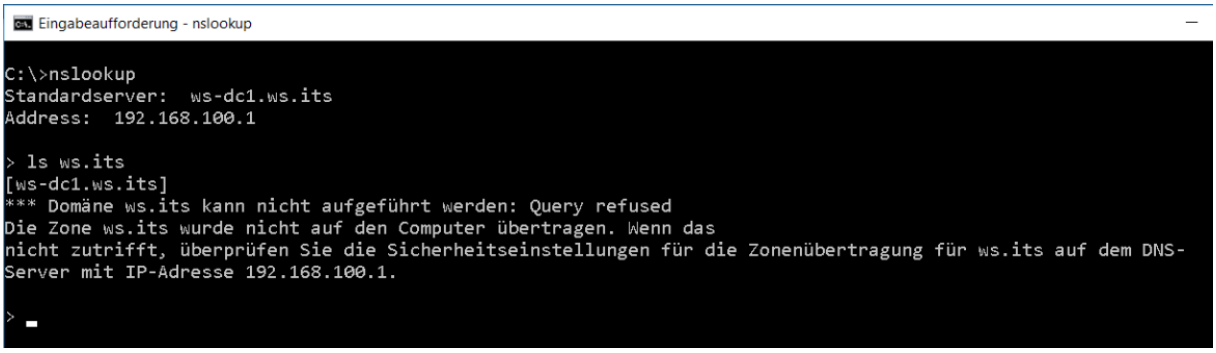
Mit der Suchleiste können diese Benutzer und Computer gesucht werden. Zu diesen werden dann viele Informationen angezeigt. Alle verknüpften Objekte können dann als Hyper-Link weiter verfolgt werden:



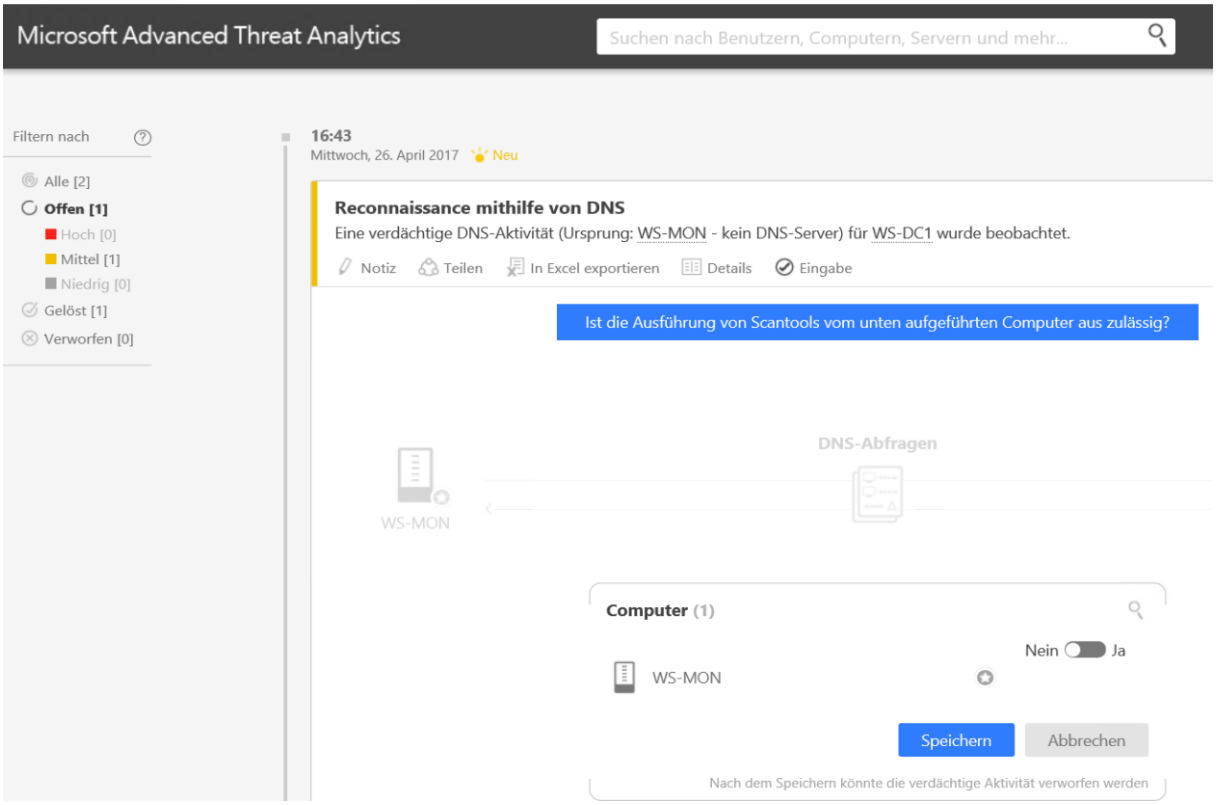
Angriff - DNS Recon (illegaler Zonentransfer)

Ein Angreifer könnte versuchen, die DNS-Zonen vom DNS-Server mit einem Zonentransfer herunterzuladen. Mit den Informationen des DNS kann man leichter das Netzwerk analysieren und Services erkennen. Ein Zonentransfer muss auf dem DNS-Server autorisiert werden. Das ist per Default nicht der Fall, weshalb eine Transferanfrage abgelehnt wird. ATA erkennt diese Anfrage und gibt einen Alarm.

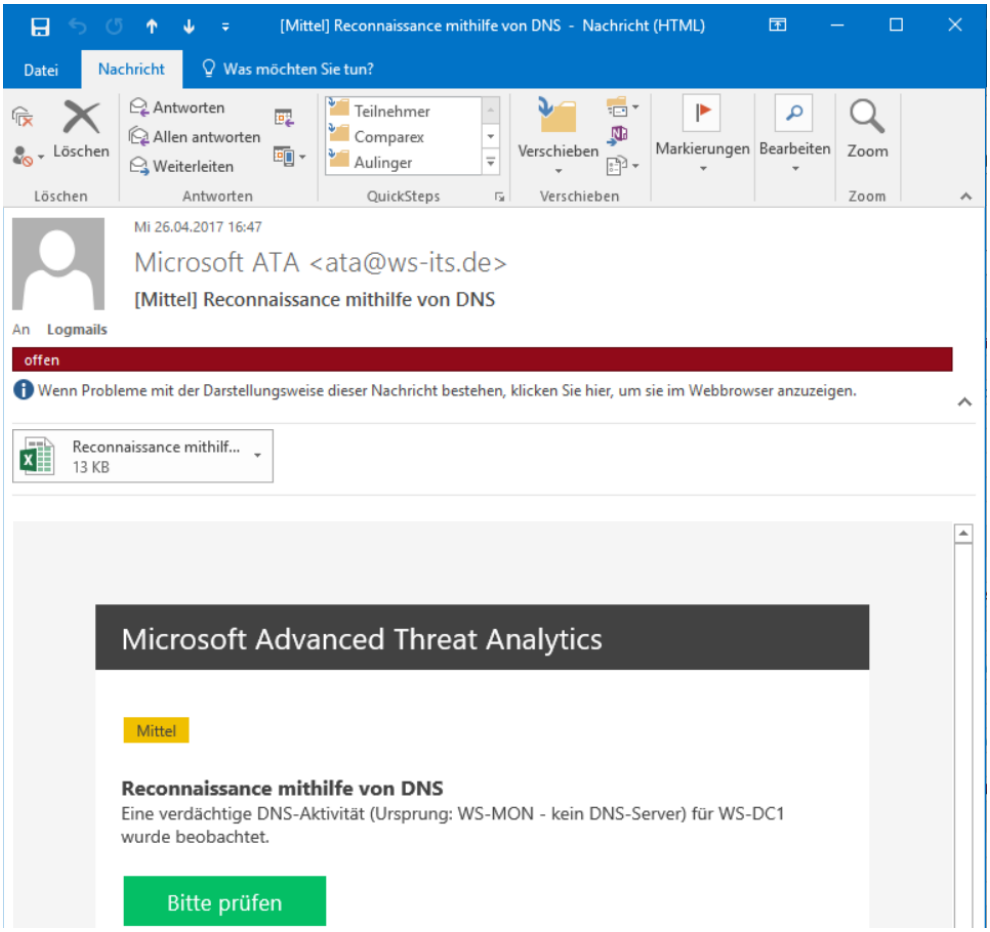
Das könnte der „Angriff“ sein:



ATA zeigt kurz darauf die Meldung an:

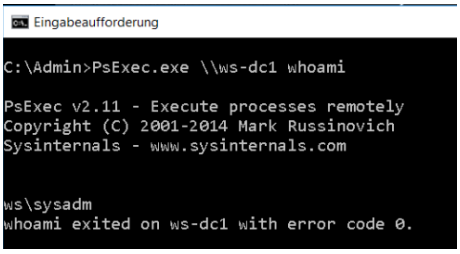


Die Benachrichtigung kommt auch per Mail

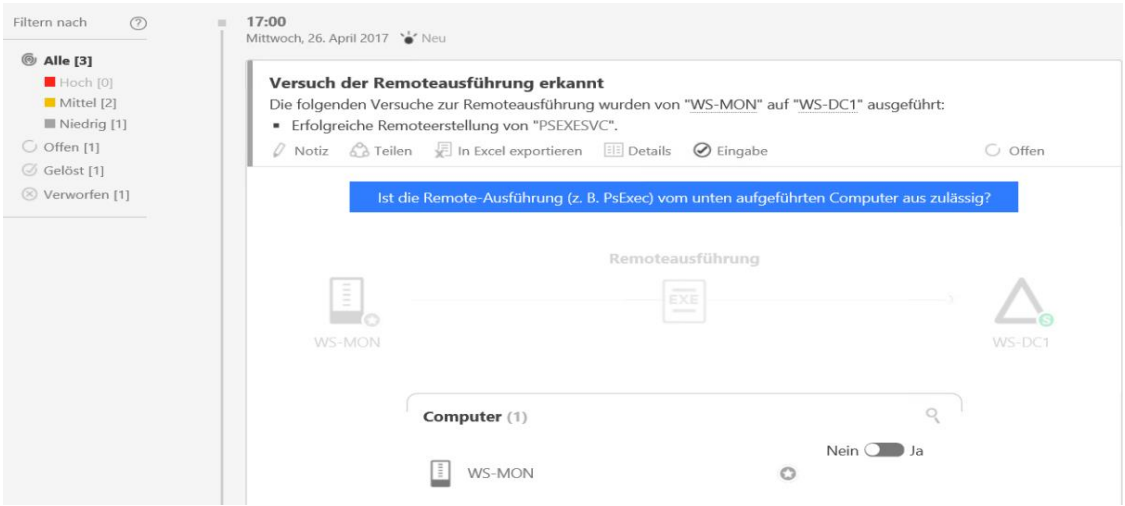


Angriff – Remote Execution

Ein Angreifer kann versuchen, mit den Anmeldeinformationen, die er auf einem Client erbeutet hat, einen Befehl auf einem DC remote auszuführen:



Auch hier schlägt ATA Alarm:



4. Abbruch der Evaluierung

nach einigen Tagen

Das System verbraucht immer mehr Hardware-Ressourcen. Vor allem wird Arbeitsspeicher benötigt. Wenn es der Sicherheit dient, dann sollte hier nicht gespart werden.

Zusätzlich habe ich einige Penetrationtests mit verschiedenen Tools ausgeführt. Darunter waren mehrere aggressive nmap-Attacken, hyenaeFE quälte verschiedene Dienste mit DoS und eine schärfere Scan-Attacke von nessus gab meiner Infrastruktur kurzzeitig den Rest. Von alldem bemerkte ATA nichts…

Rückbau

Der Rückbau der Software war recht einfach:

- mein neuer Monitorserver mit ATA konnte einfach aus dem AD herausgenommen werden
- die beiden DCs wurden kurz darauf durch neue Windows Server 2016 ersetzt. Daher habe ich auf beiden DCs einfach den Service vom ATA deaktiviert.
- die zusätzlichen Objekte im AD konnten nun einfach gelöscht werden.