

Inhalt

1.	Szenario.....	1
2.	Bereitstellung	1
	Bereitstellung des neuen Servers	1
	Erstkonfiguration.....	3
	Installation der Gateways	5
	Konfiguration der Mail-Benachrichtigung	10
	Problem: DC-Synchronisierung funktioniert nicht	10
	Austausch des Zertifikates und Isolation der IP-Adresse für die Webanwendung	11
3.	Testphase	16
	Analyse der Entitäten	16
	Angriff - DNS Recon (illegaler Zonentransfer).....	17
	Angriff – Remote Execution.....	18
4.	Abbruch der Evaluierung	19
	nach einigen Tagen	19
	Rückbau.....	19

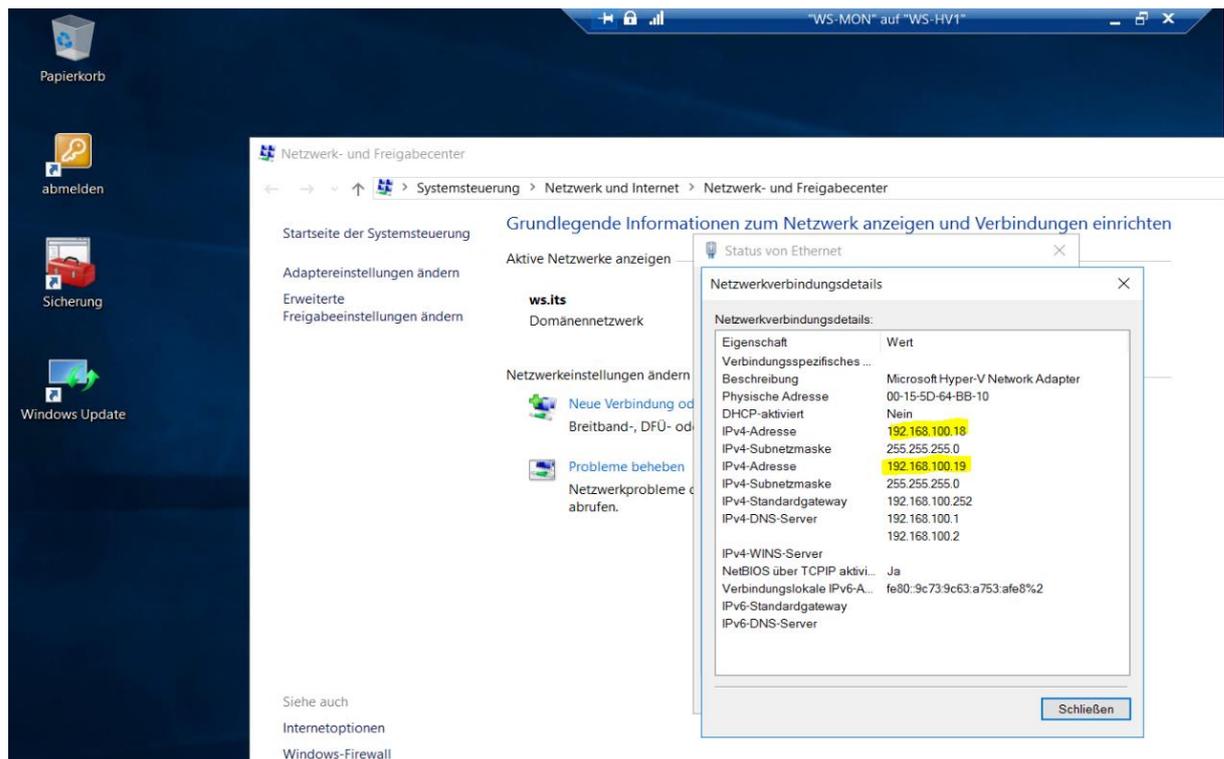
1. Szenario

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.

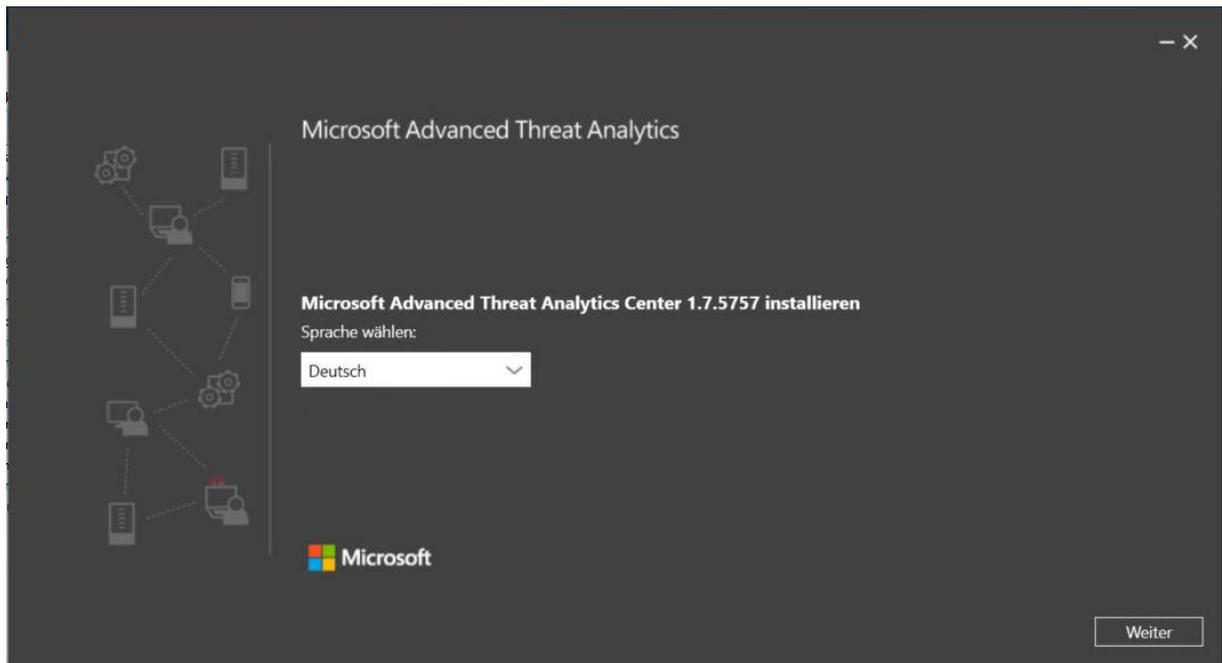
2. Bereitstellung

Bereitstellung des neuen Servers

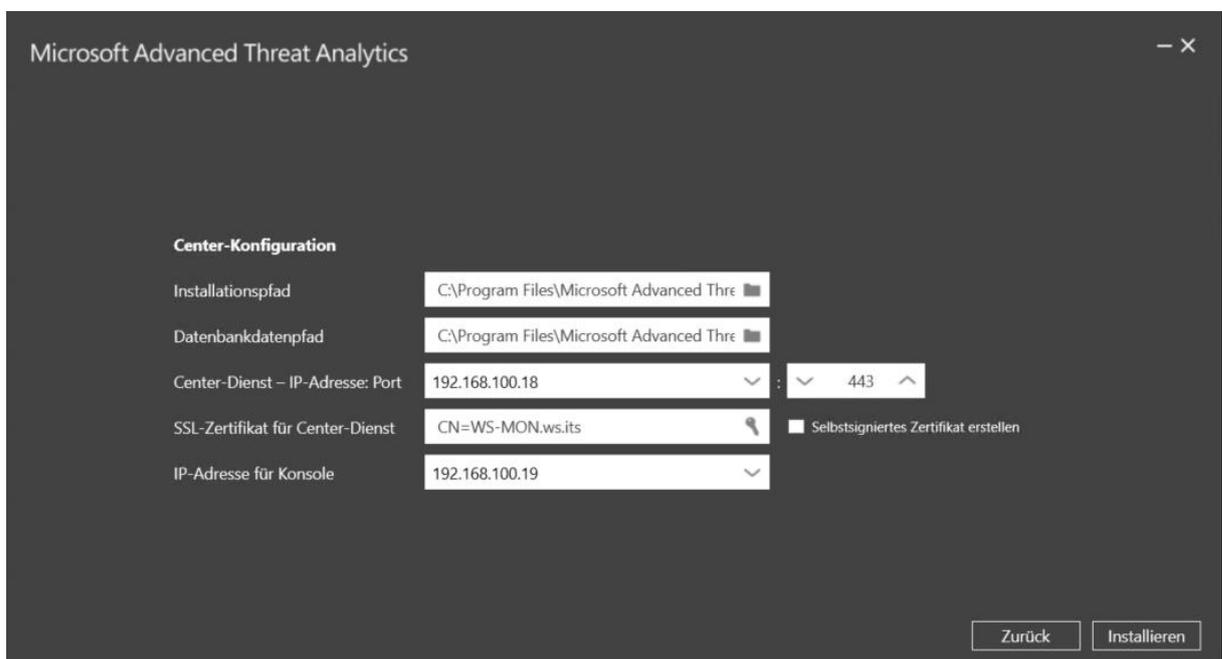
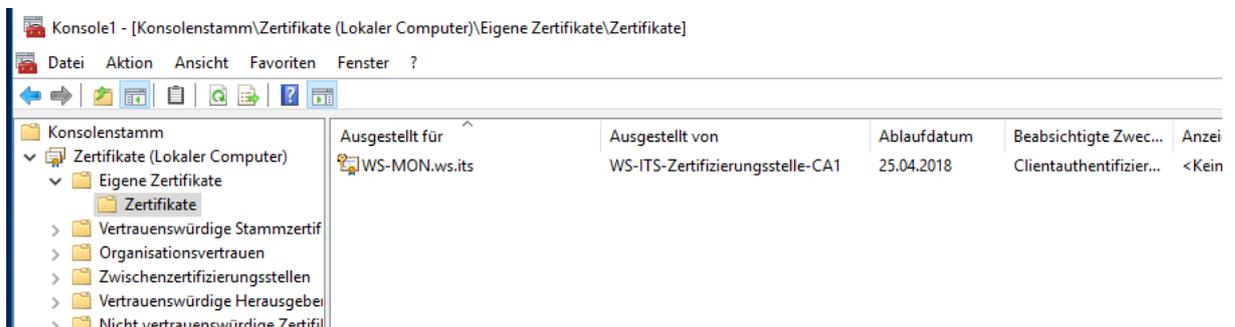
Der neue Server benötigt eine AD-Integration und 2 IP-Adressen: eine für den Monitor-Service und eine für die administrative Konsole (WebApp). In meinem Fall installiere ich einen Windows Server 2016 als VM:



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



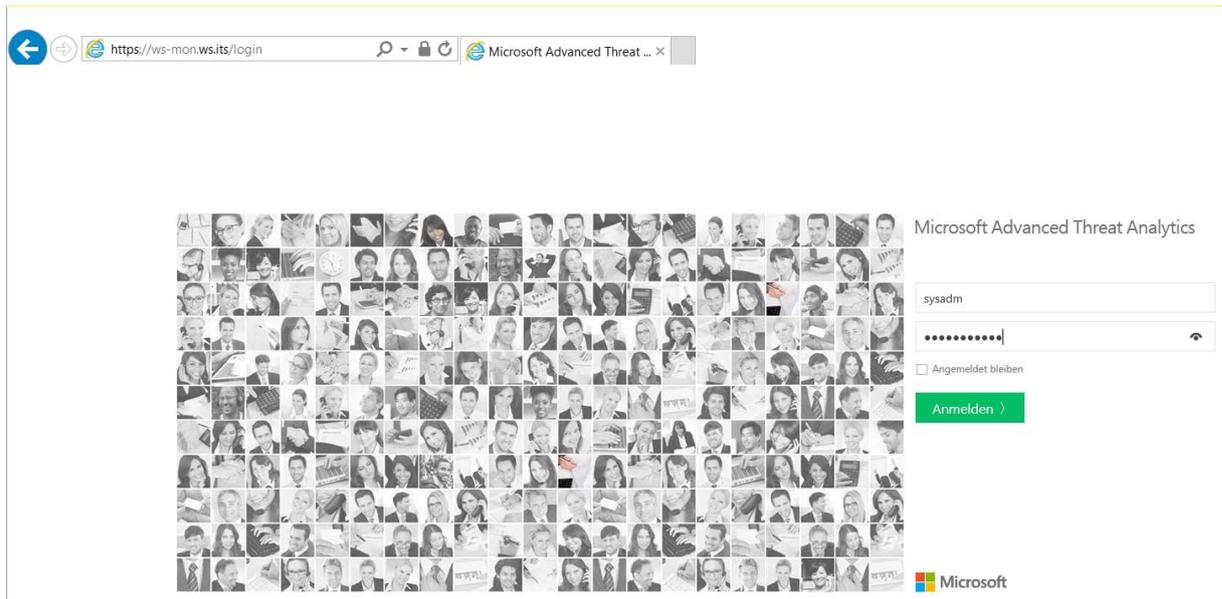
Der Webservice wird über ein Sicherheitszertifikat abgesichert. Das Setup bietet hier ein SelfSigned an. Dank der eigenen CA mit AD-Integration liegt bereits ein Zertifikat für die VM vor. Noch kann ich den Verwendungszweck nicht abschätzen, aber wenn ich später ein anderes Zertifikat verwenden möchte,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



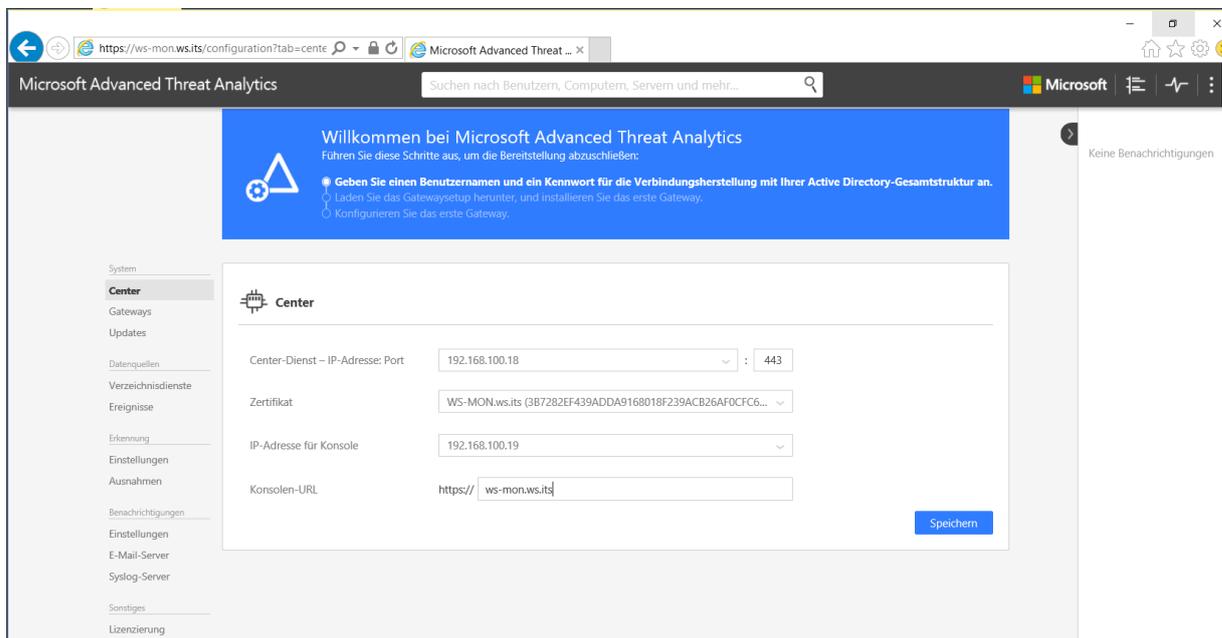
Die Installation dauert nicht lange und läuft problemlos durch.

Erstkonfiguration

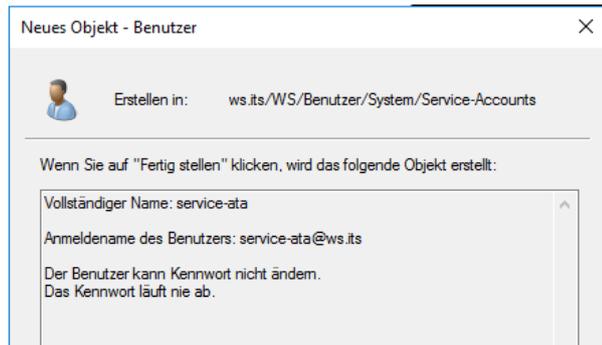
Nach der kurzen Installation steht die Konfiguration über eine Website bereit. Diese startet leider über die IP in der URL. Das habe ich im Browser-Aufruf bereits angepasst:



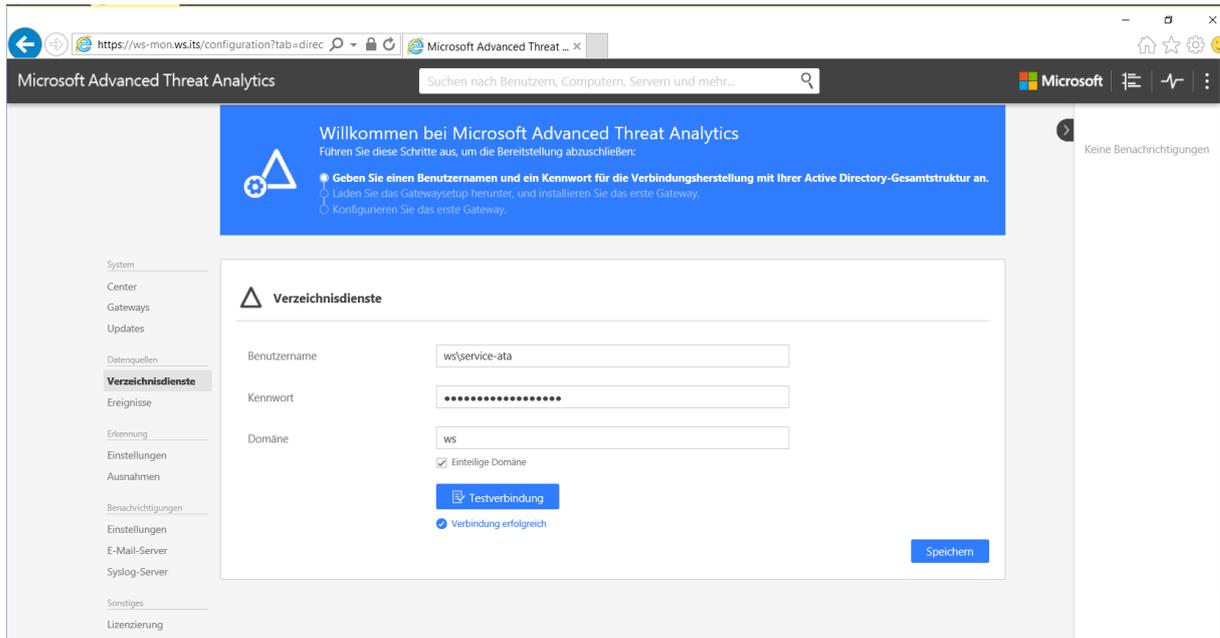
Direkt auf der Hauptseite finde ich den Punkt, um das Zertifikat auszutauschen:



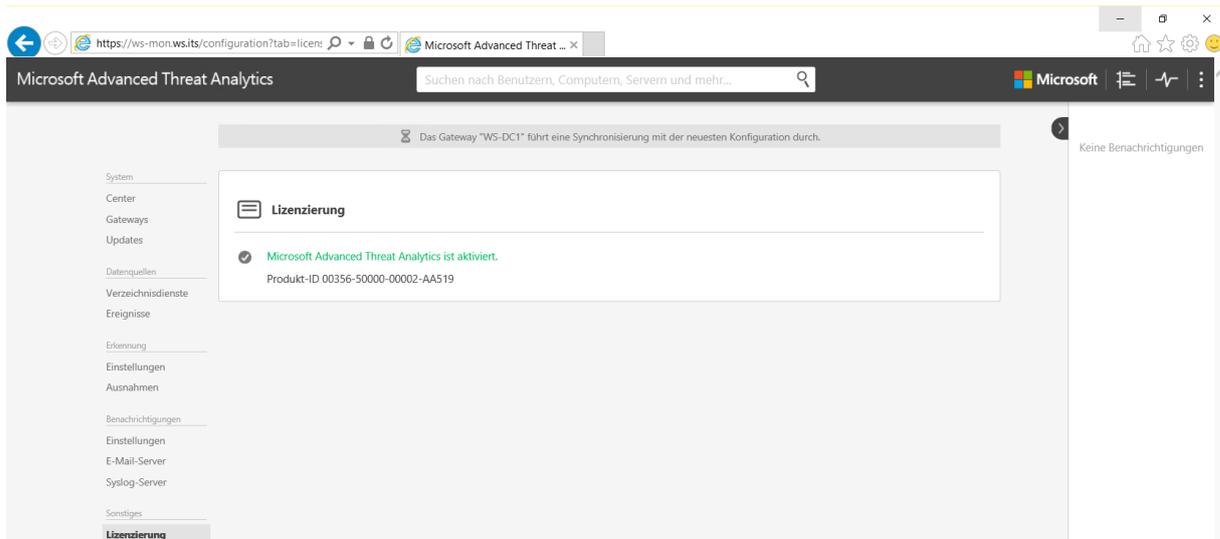
Für den Zugriff zu den Verzeichnisdiensten wird ein Benutzer benötigt. Dafür erstelle ich einen nicht-privilegierten AD-Benutzer. Da keine Rechte erforderlich sind, setze ich das Kennwort auf „läuft nie ab“:



Diesen Benutzer trage ich ein. Der Test funktioniert:

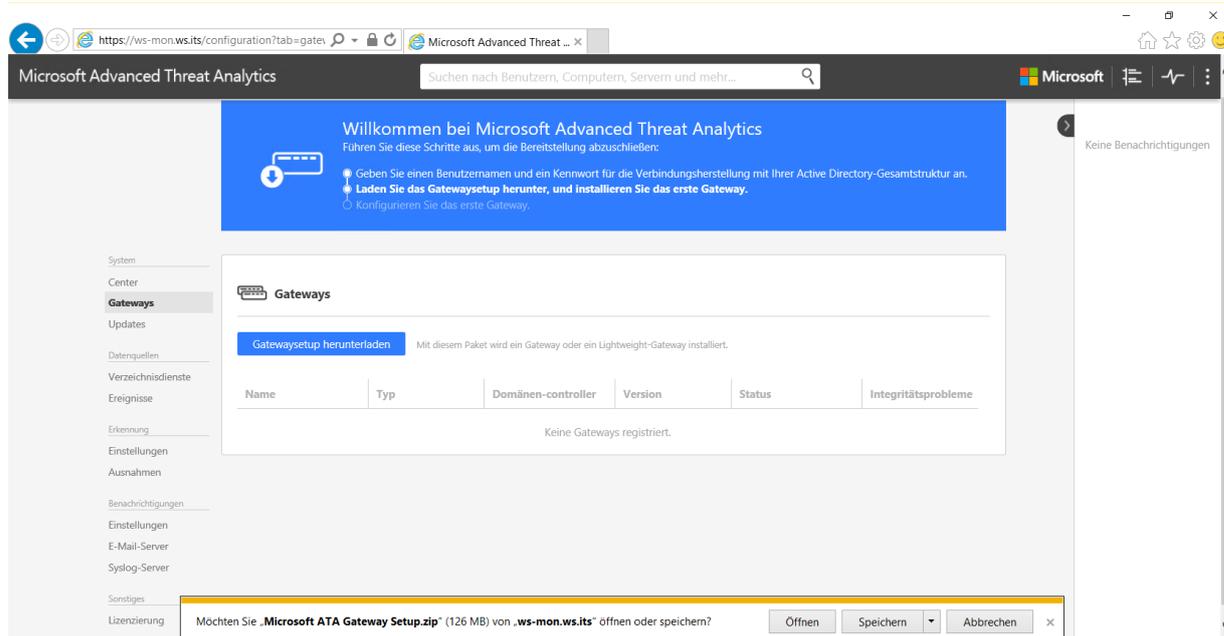


Nun fehlt noch die Aktivierung des ATA:

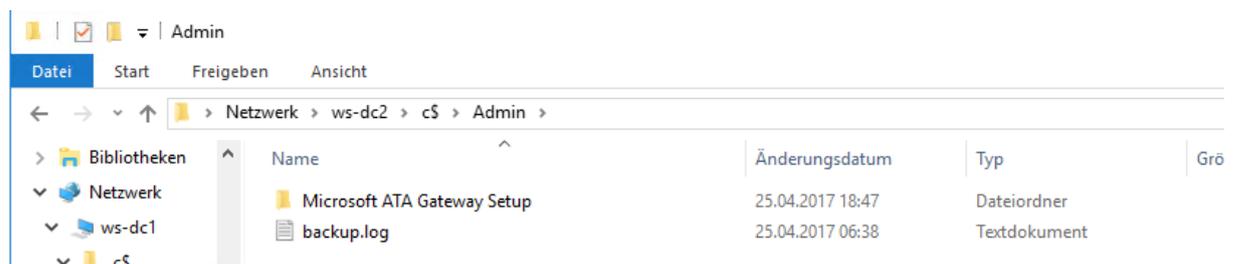


Installation der Gateways

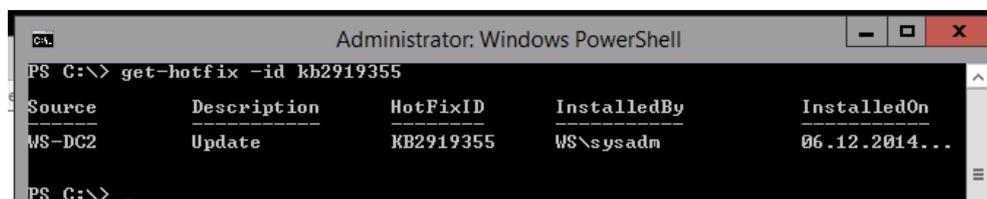
Nun muss ich den Gateway-Service auf meinen DCs installieren. Den Installer kann ich direkt in der WebAnwendung herunterladen. Die Alternative mit der PortSpiegelung teste ich vielleicht später.



Das Setup kopiere ich auf meine beiden DCs:

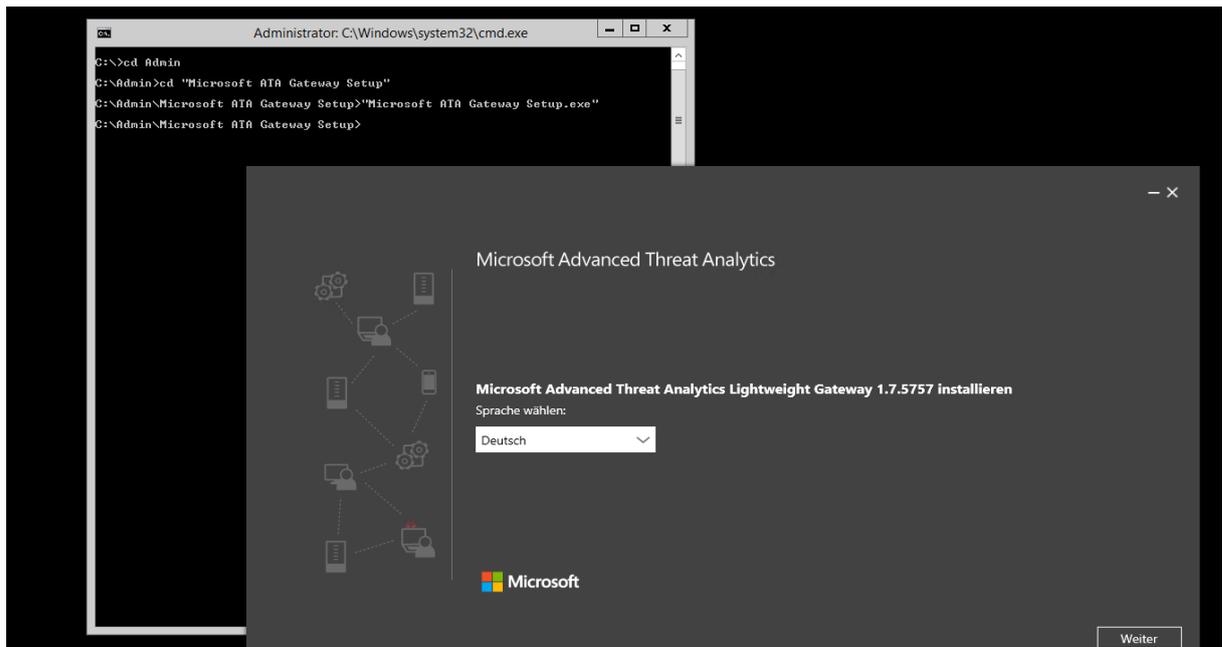


Meine 3 DCs laufen unter Windows Server 2012 R2 als ServerCore. Als Voraussetzung auf Windows Server 2012 R2 ist ein Update erforderlich. Dieses ist bereits installiert:

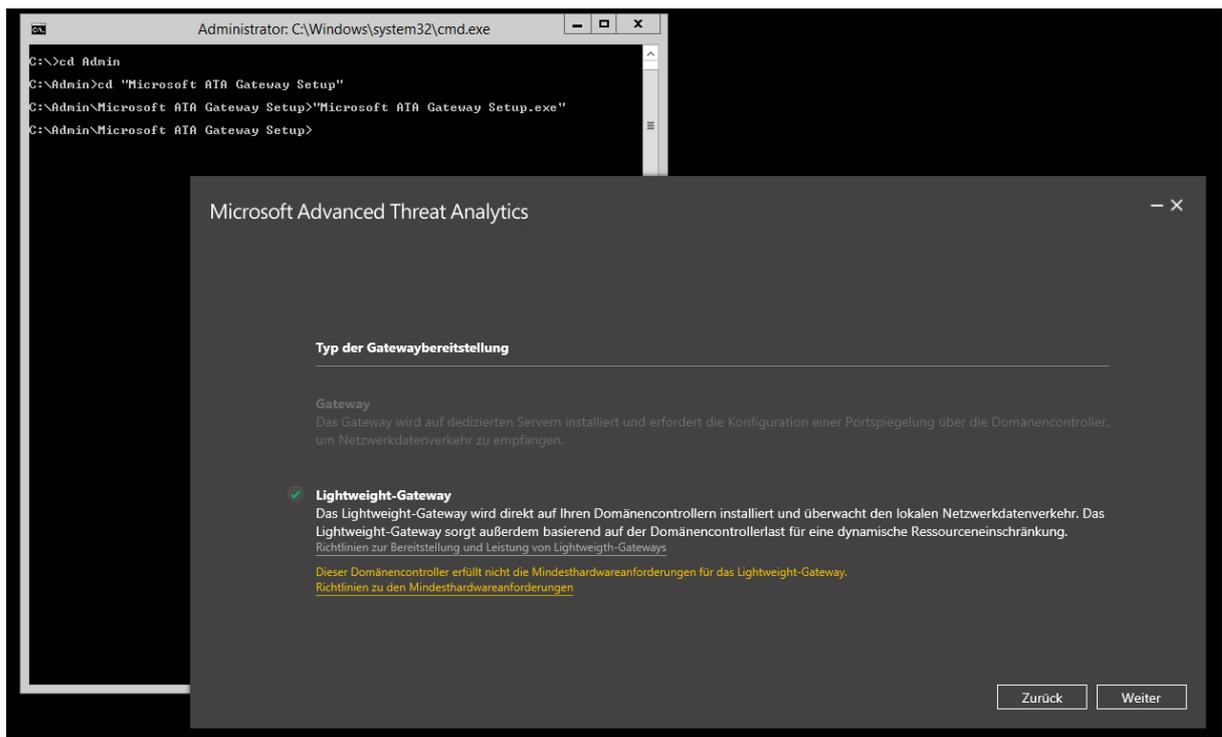


Ich installiere das Gateway zunächst nur auf 2 DCs. Der 3. DC steht in einem anderen Standort und aktuell kann ich den erforderlichen Traffic über die WAN-Verbindung nicht abschätzen.

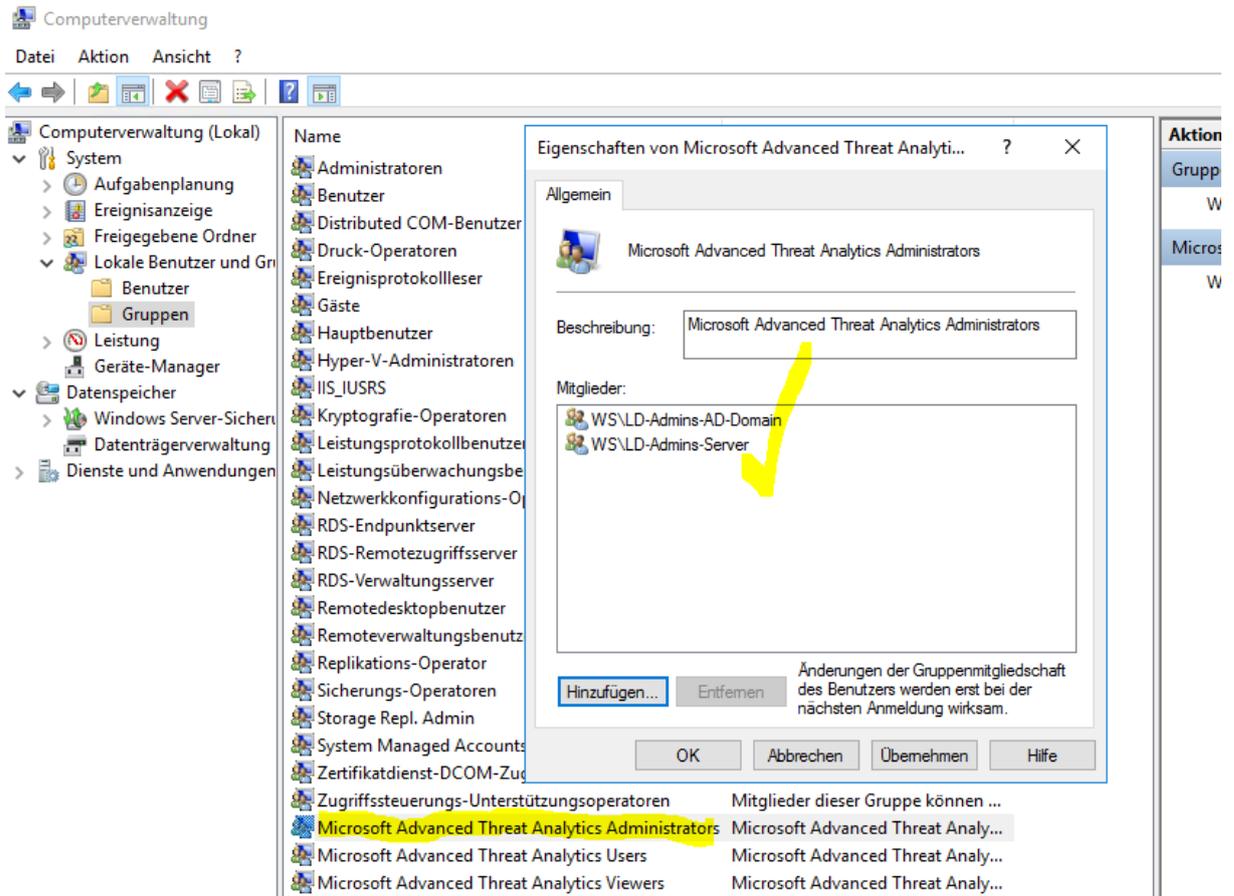
Das Setup lässt sich über die cmd des Server-Core starten:



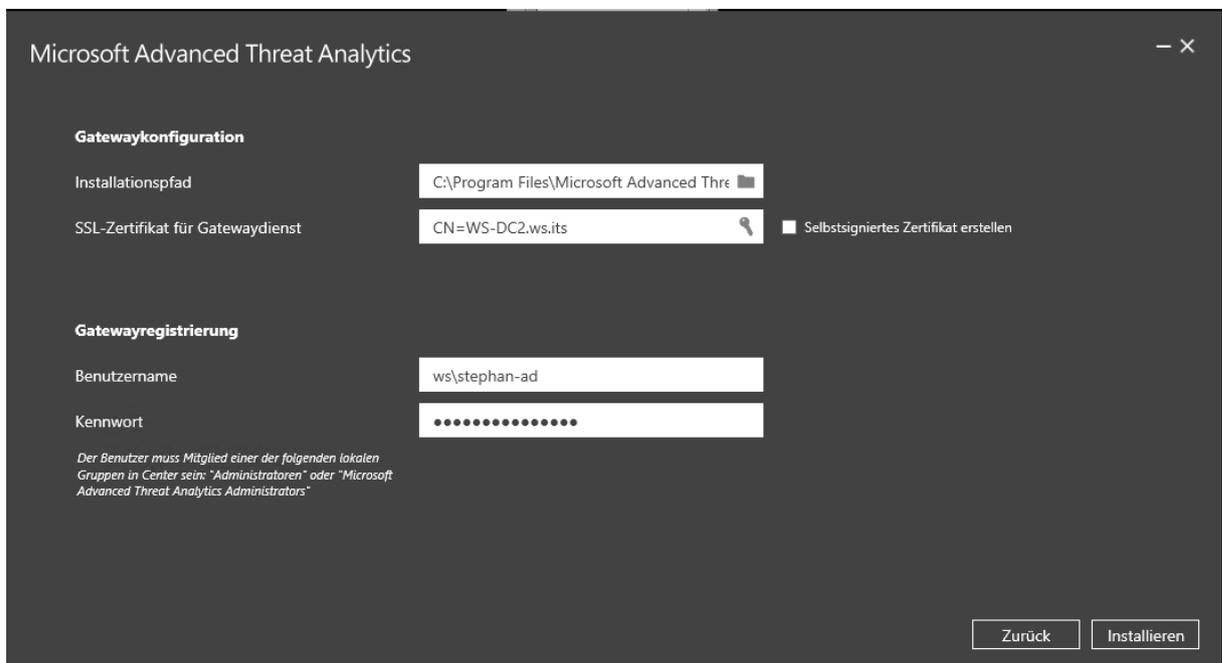
Die Meldung zu den Mindesthardwareanforderungen ignoriere ich und setze das Setup fort:



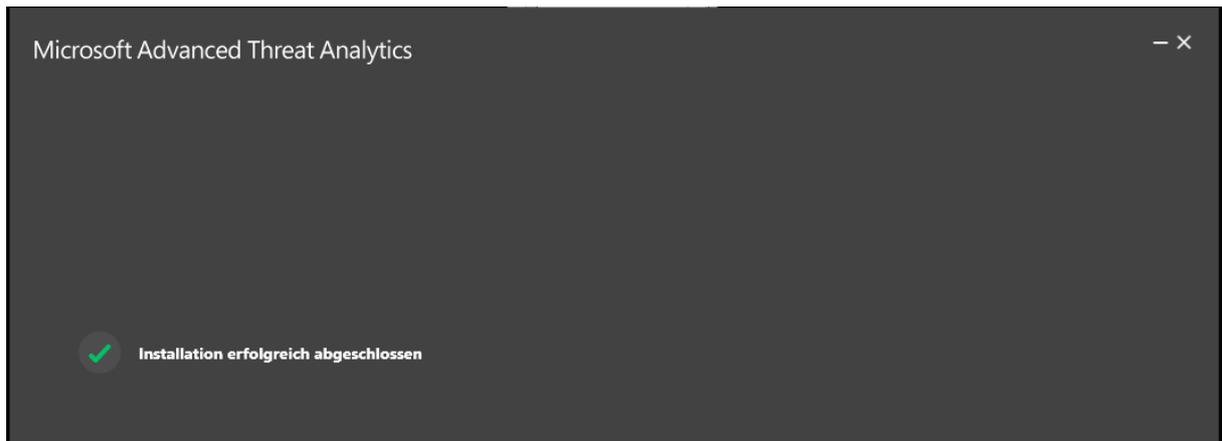
Das Gateway muss sich am ATA registrieren. Dafür wird ein Benutzer benötigt, der auf dem ATA die erforderlichen Rechte hat. Auch die WebAnwendung wird durch eine Anmeldung gesichert. Ich trage auf dem ATA 2 Gruppen als ATA-Admins ein:



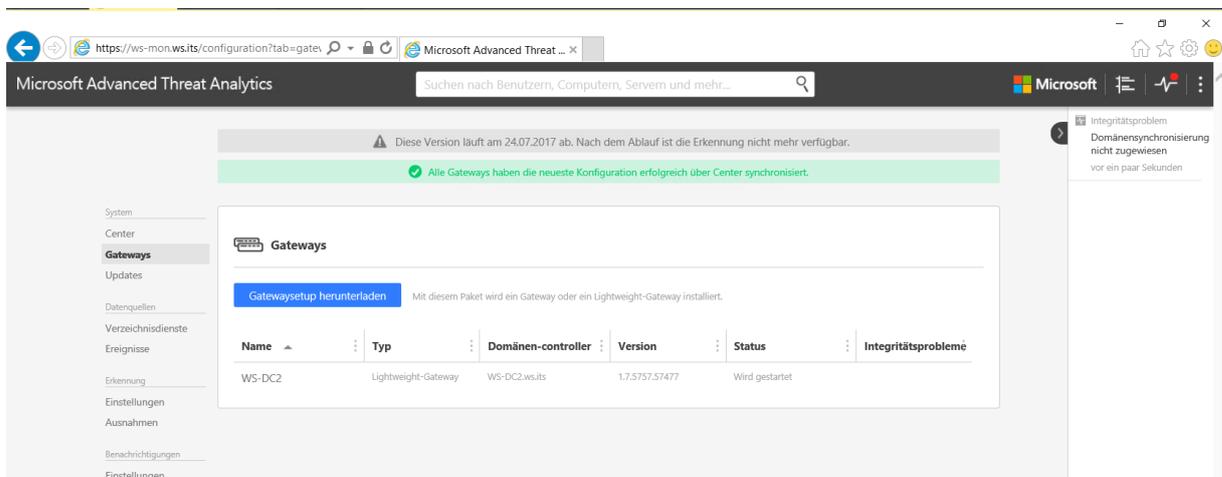
Auf dem DC setze ich nun noch das Zertifikat des DCs ein:



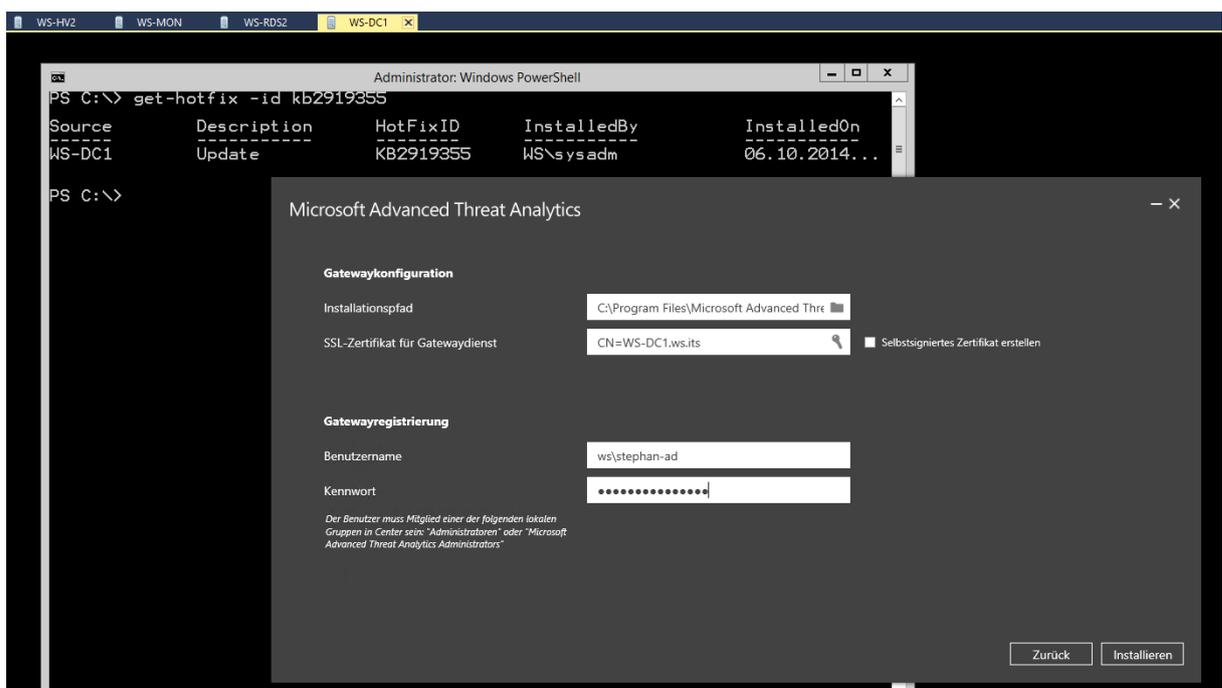
Das Setup läuft nun durch.



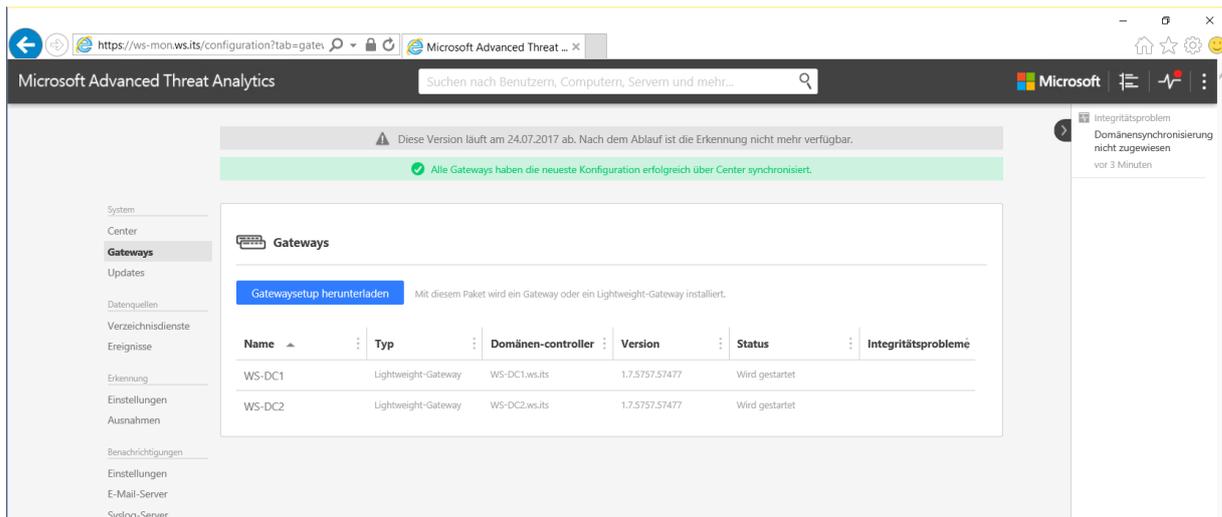
Im ATA meldet sich der DC:



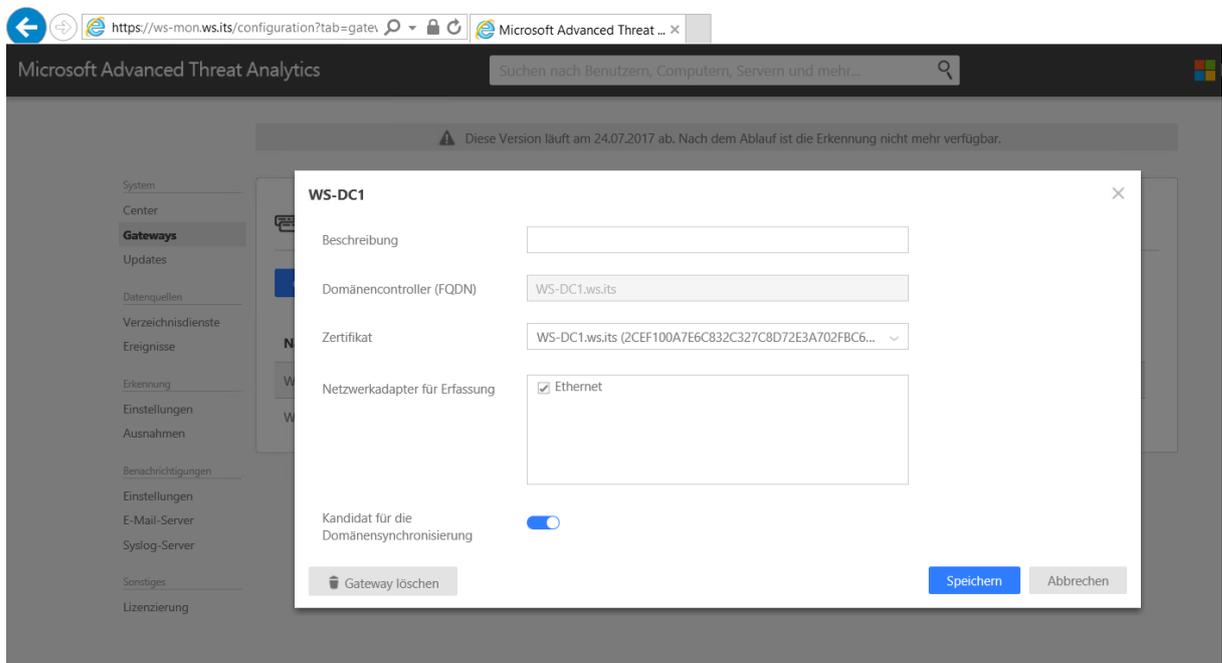
Den Prozess wiederhole ich auf dem 2. DC:



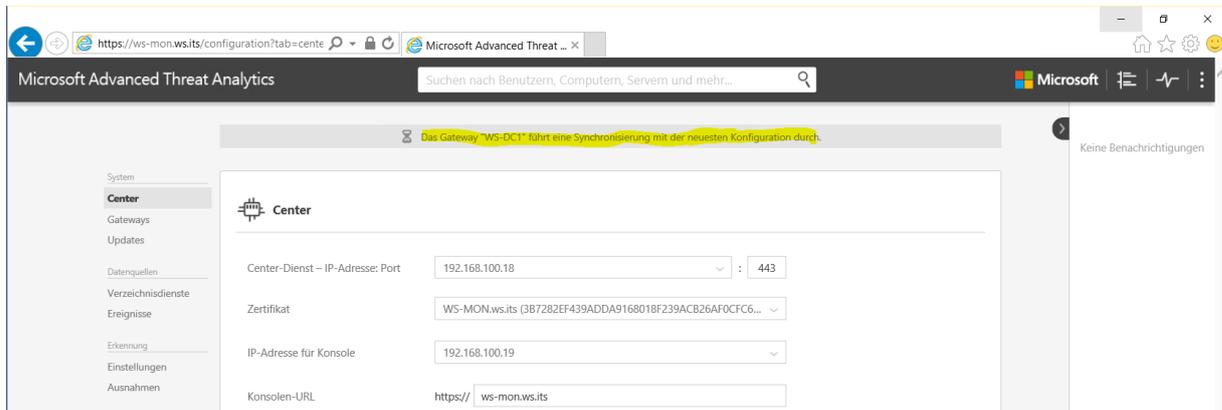
Auch dieser meldet sich beim ATA:



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:

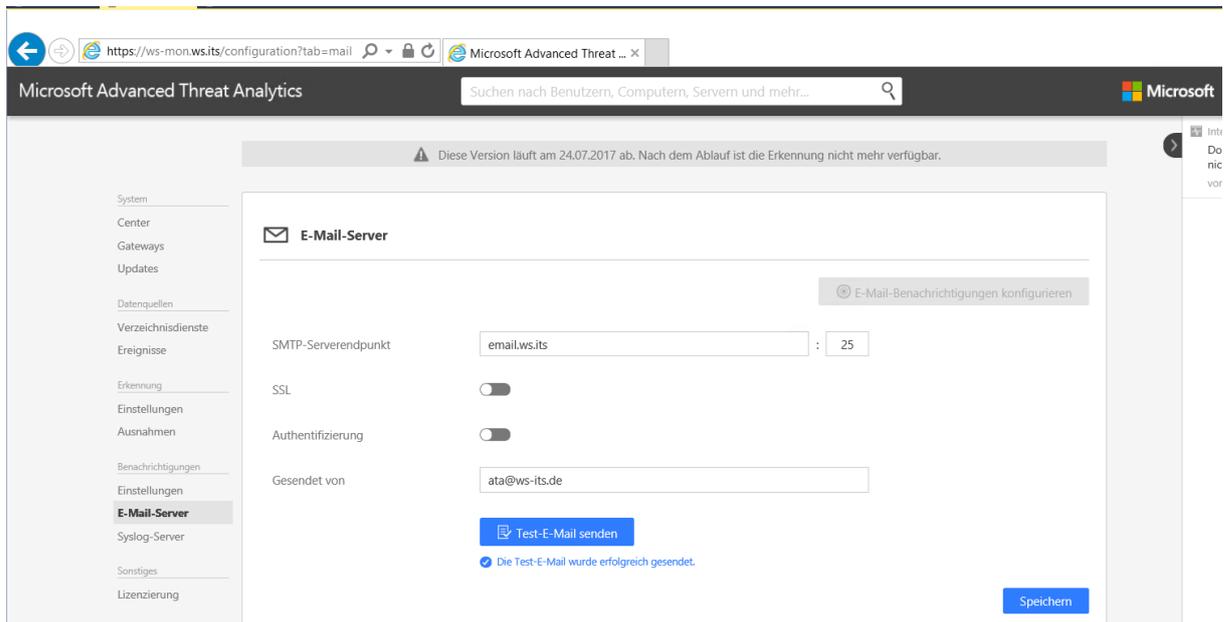


Der Sync wird automatisch gestartet:

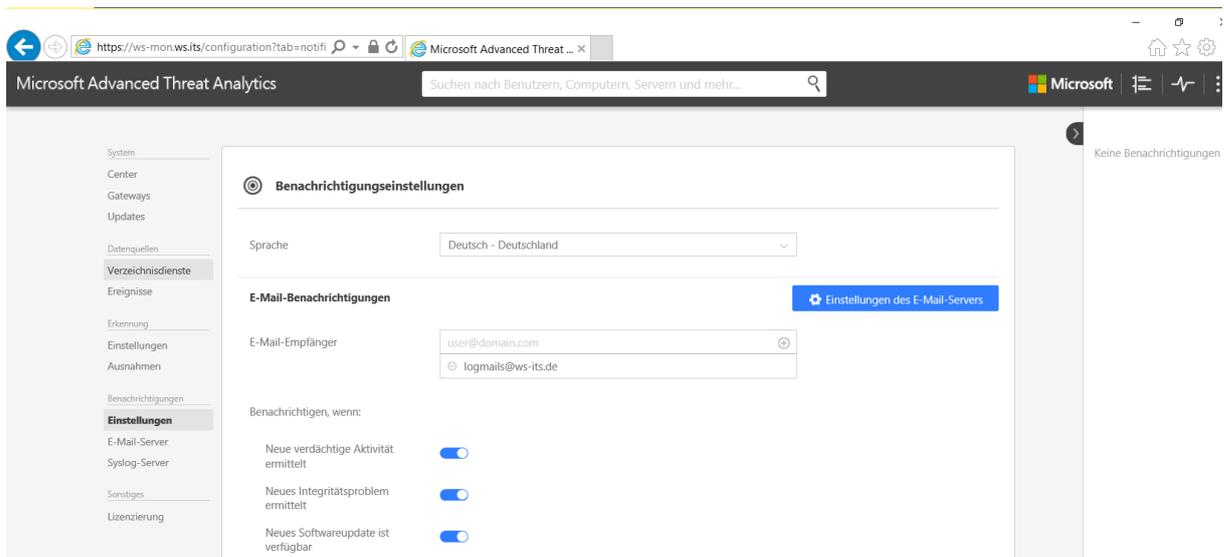


Konfiguration der Mail-Benachrichtigung

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



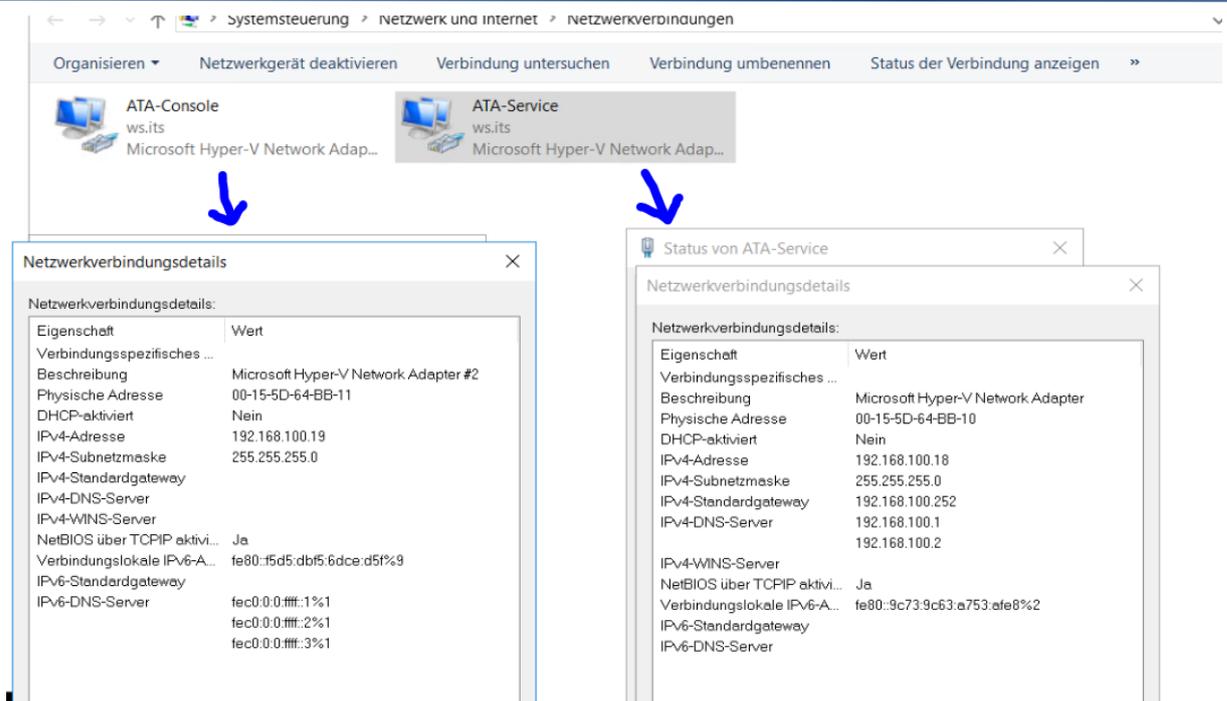
Die Operatoren werden bei den Benachrichtigungen konfiguriert:



Problem: DC-Synchronisierung funktioniert nicht

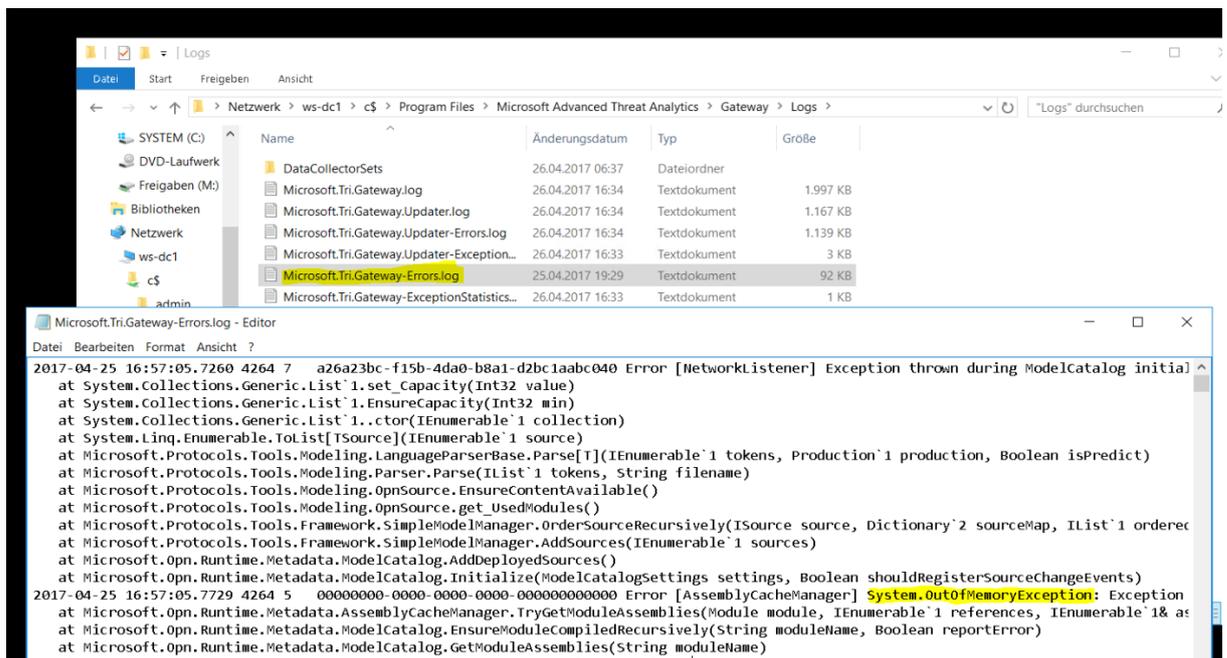
Auch nach längerer Zeit melden sich die beiden DCs nicht einsatzbereit. Ich kontrolliere den Zugriff. Da der ATA 2 IP-Adressen auf einer Netzwerkkarte konfiguriert hat und beide im DNS registriert, ist er aus Sicht des DCs über 2 IPs erreichbar. Da beide im gleichen Subnetz liegen, aber nur eine den 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:

Microsoft Active Directory-Zertifikatsdienste - WS-ITS-Zertifizierungsstelle-CA1

Erweiterte Zertifikatanforderung

Zertifikatvorlage:
WS-ITS-Webserver

Identifikationsinformationen für Offlinevorlage:

Name: ata.ws.its
 E-Mail-Adresse: support@ws-its.de
 Firma: WS IT-Solutions
 Abteilung: IT-Services
 Stadt: Ergoldsbach
 Bundesland/Kanton: Bayern
 Land/Region: DE

Schlüsseloptionen:

Neuen Schlüsselsatz erstellen Bestehenden Schlüsselsatz verwenden

Kryptografiedienstanbieter: Microsoft RSA SChannel Cryptographic Provider

Schlüsselverwendung: Austausch

Schlüsselgröße: 2048 (Allgemeine Schlüsselgrößen: 2048 4096 8192 16384)

Automatischer Schlüsselcontaineiname Vom Benutzer angegebener Containeiname

Schlüssel als "Exportierbar" markieren

Verstärkte Sicherheit für den privaten Schlüssel aktivieren

Zusätzliche Optionen:

Anforderungsformat: CMC PKCS 10

Hashalgorithmus: sha1
 Wird nur zum Signieren der Anforderung verwendet.

Anforderung speichern

Attribut:

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

Microsoft Active Directory-Zertifikatsdienste - WS-ITS-Zertifizierungsstelle-CA1

Zertifikat wurde installiert

Das neue Zertifikat wurde installiert.

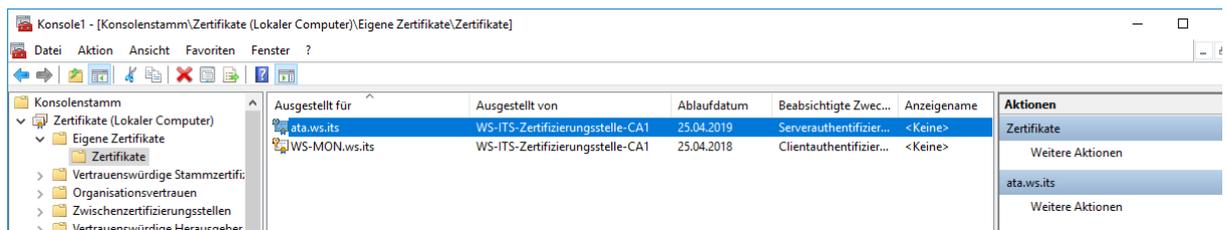
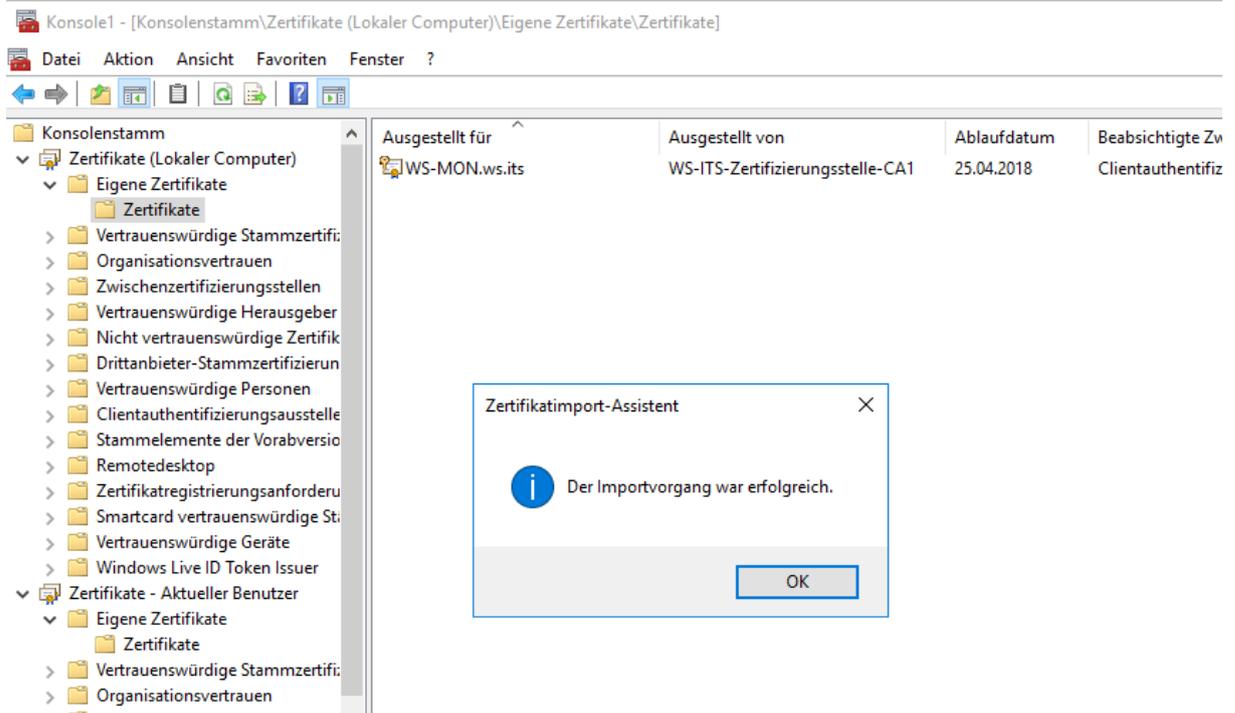
Ausgestellt für	Ausgestellt von	Ablaufdatum
ata.ws.its	WS-ITS-Zertifizierungsstelle-CA1	25.04.2019

Fertigstellen des Assistenten

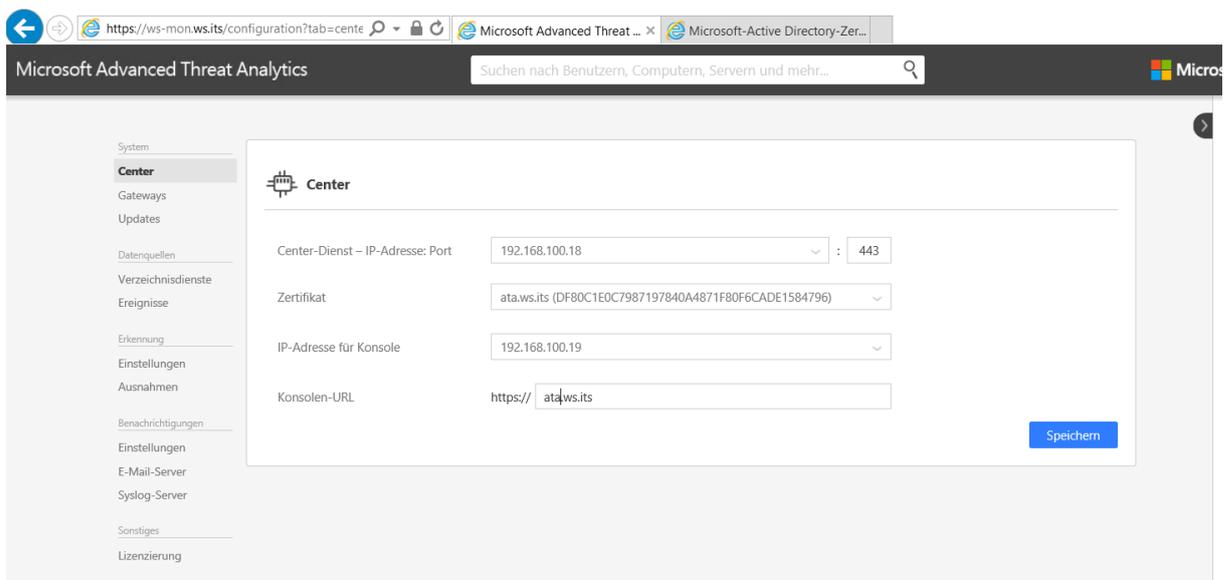
Der Zertifikatexport-Assistent wurde erfolgreich abgeschlossen.

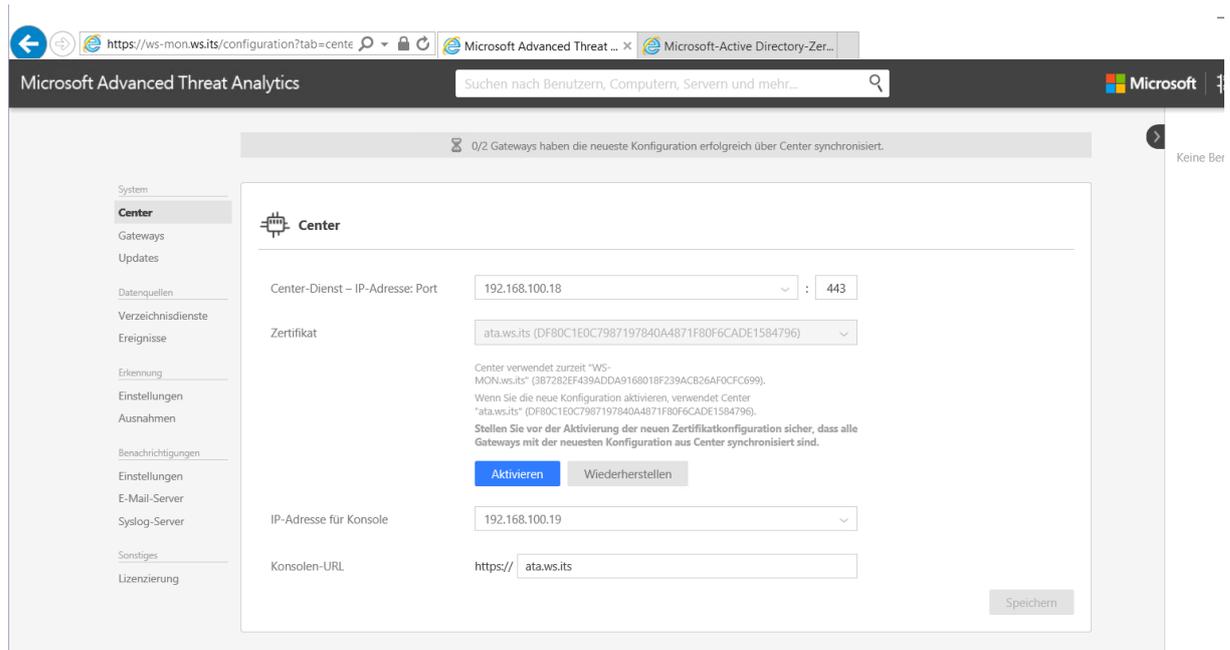
Sie haben folgende Einstellungen ausgewählt:

- Dateiname: c:\admn\2017-04-25\ata.ws.its.pfx
- Exportschlüssel: Ja
- Alle Zertifikate im Zertifizierungspfad einbeziehen: Ja
- Dateiformat: Privater Informationsaustausch (*.pfx)

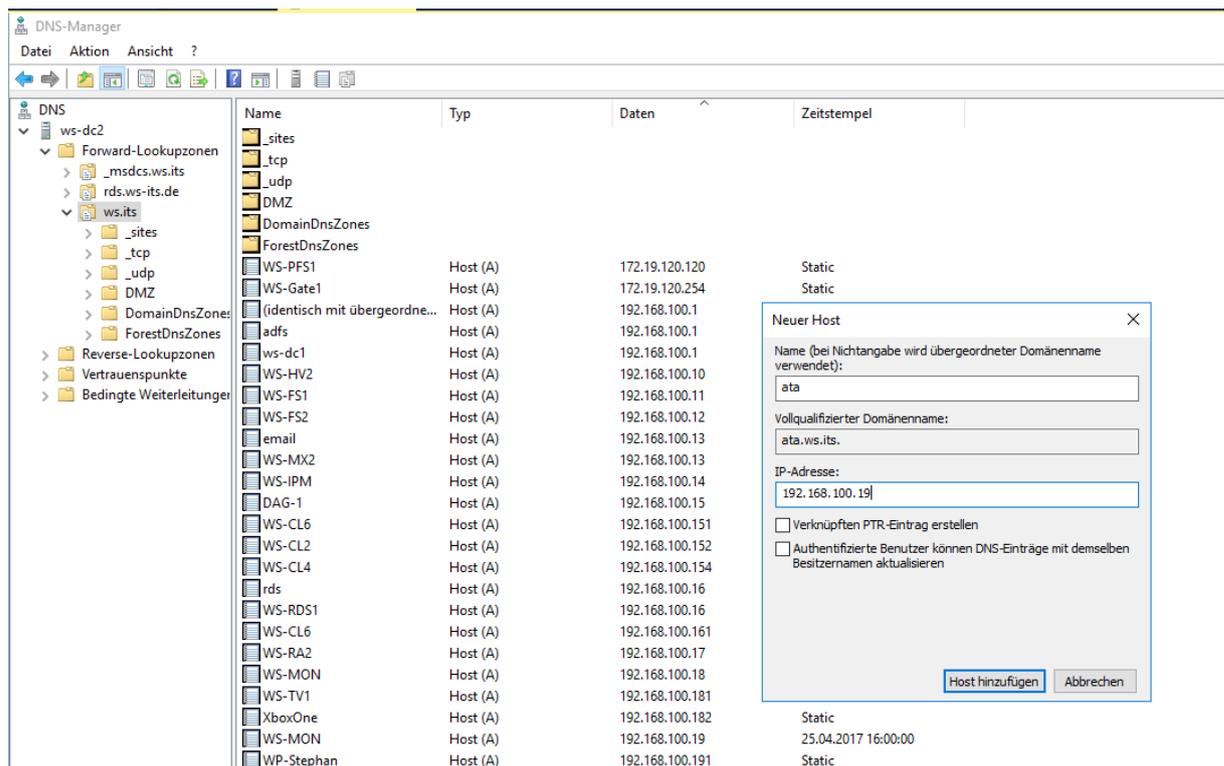


In der Webanwendung ändere ich nun das Zertifikat:





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:

The screenshot shows a web browser window with the URL <https://ata.ws.its/configuration?tab=center>. The page title is "Microsoft Advanced Threat Analytics". In the top right corner, there is a search bar with the text "Suchen nach Benutzern". On the left side, there is a navigation menu with the following items: "System", "Center" (which is highlighted), "Gateways", and "Updates". The main content area on the right displays a "Center" icon (a stylized chip) and the word "Center" next to it.

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:

Microsoft Advanced Threat Analytics
Walther, Stephan
M

Walther, Stephan

ws.its
Erstellt am 16.08.2013
Stephan.Walther@ws-its.de

Info
Kontoinformationen
Verdächtige Aktivitäten
Verzeichnisänderungen

Mitgliedschaften (25)

- LD-Admins-HyperV
- LD-Zugriff-Privat-Fami...
- LD-Zugriff-JB
- LD-Zugriff-Business
- LD-Admins-IPAM
- LD-Zugriff-Privat-Amtl...

Benutzeraktivität

● Kerberos 0
● NTLM 0

Kennwort

Läuft nie ab

Letzter Fehler
Freitag, 21. April 2017 um 08:51

Letzte Änderung
Sonntag, 18. August 2013 um 13:03

Läuft ab
Nie festlegen

Kollegen

Keine

Standorte

- Ergoldsbach
- 192.168.100.13
Zuletzt angezeigt
Mittwoch, 26. April 2017 um 07:47
- 192.168.100.3
Zuletzt angezeigt
Mittwoch, 26. April 2017 um 07:47
- 192.168.100.151
Zuletzt angezeigt
Mittwoch, 26. April 2017 um 06:18
- 192.168.100.154
Zuletzt angezeigt
Dienstag, 25. April 2017 um 21:12
- 192.168.100.161
Zuletzt angezeigt
Dienstag, 25. April 2017 um 20:19

Computer, an denen sich dieser Benutzer zuletzt angemeldet hat

- WS-CL6
Mittwoch, 26. April 2017 um 06:18
- WS-CL4
Dienstag, 25. April 2017 um 21:09
- WS-MX2
Mittwoch, 26. April 2017 um 07:47
- WS-MX1
Mittwoch, 26. April 2017 um 07:47

Kürzlich verwendete Ressourcen

- WS-MX2
an HOST
Mittwoch, 26. April 2017 um 07:47
- WS-MX1
an HOST
Mittwoch, 26. April 2017 um 07:47
- WS.ITS
an KRBTGT
Mittwoch, 26. April 2017 um 06:17
- WS-FS2
an CIFS
Mittwoch, 26. April 2017 um 06:17
- WS-DC2
an LDAP
Mittwoch, 26. April 2017 um 06:17

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:

```

Eingabeaufforderung - nslookup
C:\>nslookup
Standardserver: ws-dc1.ws.its
Address: 192.168.100.1

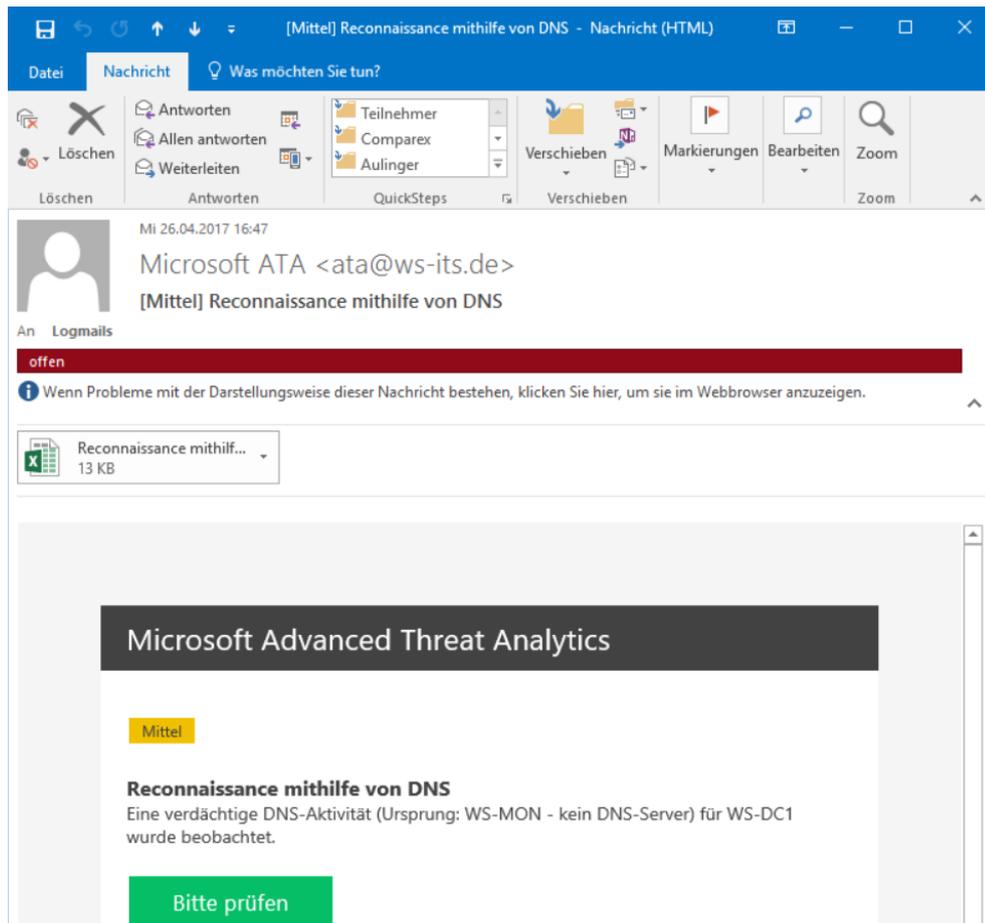
> ls ws.its
[ws-dc1.ws.its]
*** Domäne ws.its kann nicht aufgeführt werden: Query refused
Die Zone ws.its wurde nicht auf den Computer übertragen. Wenn das
nicht zutrifft, überprüfen Sie die Sicherheitseinstellungen für die Zonenübertragung für ws.its auf dem DNS-
Server mit IP-Adresse 192.168.100.1.

>
    
```

ATA zeigt kurz darauf die Meldung an:

The screenshot shows the Microsoft Advanced Threat Analytics (ATA) interface. At the top, there is a search bar with the text "Suchen nach Benutzern, Computern, Servern und mehr...". On the left side, there is a "Filtern nach" (Filter by) section with the following options: "Alle [2]", "Offen [1]", "Hoch [0]", "Mittel [1]", "Niedrig [0]", "Gelöst [1]", and "Verworfen [0]". The main content area displays an alert titled "Reconnaissance mithilfe von DNS" (Reconnaissance using DNS) with a timestamp of "16:43 Mittwoch, 26. April 2017" and a "Neu" (New) status. The alert text reads: "Eine verdächtige DNS-Aktivität (Ursprung: WS-MON - kein DNS-Server) für WS-DC1 wurde beobachtet." (A suspicious DNS activity (origin: WS-MON - no DNS server) for WS-DC1 was observed). Below the alert text, there are icons for "Notiz" (Note), "Teilen" (Share), "In Excel exportieren" (Export to Excel), "Details", and "Eingabe" (Input). A blue banner asks: "Ist die Ausführung von Scantools vom unten aufgeführten Computer aus zulässig?" (Is the execution of Scantools from the computer listed below allowed?). Below this, there is a diagram titled "DNS-Abfragen" (DNS queries) showing a computer icon labeled "WS-MON" on the left and a document icon labeled "DNS-Abfragen" on the right, with an arrow pointing from WS-MON to the document. Underneath the diagram, there is a section titled "Computer (1)" with a search icon. It lists "WS-MON" with a plus sign next to it. To the right of the list is a toggle switch labeled "Nein" (No) and "Ja" (Yes), currently set to "Nein". At the bottom of this section are "Speichern" (Save) and "Abbrechen" (Cancel) buttons. A note at the bottom of the interface states: "Nach dem Speichern könnte die verdächtige Aktivität verworfen werden" (After saving, the suspicious activity could be rejected).

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:

```

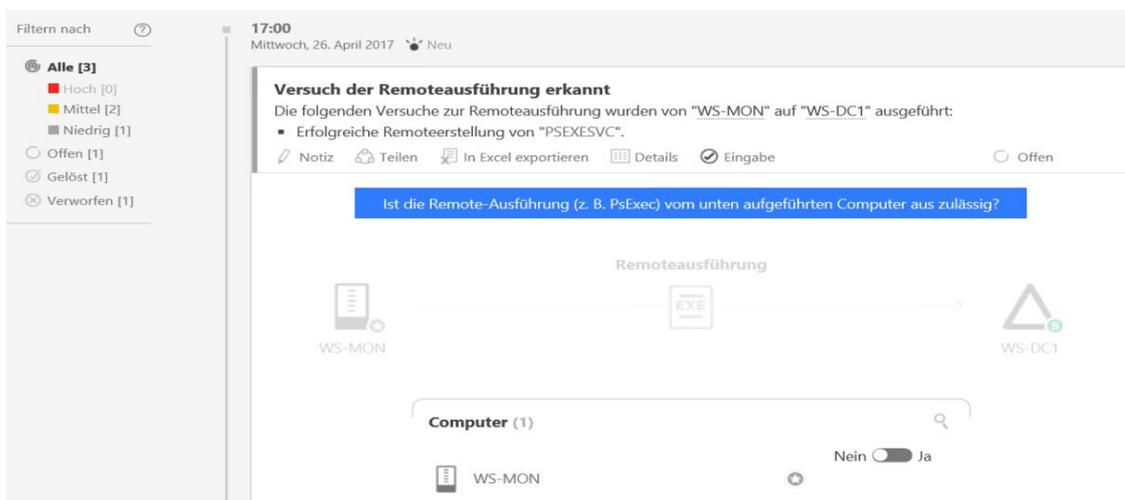
Eingabeaufforderung

C:\Admin>PsExec.exe \\ws-dc1 whoami

PsExec v2.11 - Execute processes remotely
Copyright (C) 2001-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

ws\sysadm
whoami exited on ws-dc1 with error code 0.
    
```

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 Penetrationstests mit verschiedenen Tools ausgeführt. Darunter waren mehrere aggressive nmap-Attacken, hyenaFE 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.