TeleTrusT-EBCA "PKI-Workshop" 2021

Berlin, 30.09.2021

Azure-basierte Referenzarchitektur zur Anbindung der EBCA

Sebastian Heil, Uniper

Agenda

- Ausgangslage
- Zielsetzung
- Designüberlegungen
- Auf der Suche nach dem besten LDAP Server…
- Datenfluss
- Infrastruktur
- Implementierungsdetails

Ausgangslage (Anfang 2020)

- Uniper, ehemals ein Teil der E.ON
- Ca. 9000 User mit Zertifikaten
- Uniper nutzt die Anbindung der EBCA an die E.ON Umgebung → geteiltes IAM, geteiltes Meta-Directory
- Geplanter Auszug aus dem gemeinsamen Rechenzentrum, Auszug aus dem gemeinsamen Directory

→ Uniper benötigt eine eigene Anbindung an die EBCA

Zielsetzung

- Cloud-First Ansatz
- Nutzung / Evaluierung vorhandener Azure-Features
- Kosteneffiziente und schlanke Lösung
- Da Zugriff von außen: verstärkte Betrachtung sicherheitsrelevanter Aspekte

Was wird eigentlich benötigt? / Designüberlegungen

- Directory mit allen Zertifikaten und dazugehörigen Email-Adressen

  → wir brauchen nicht das komplette Active Directory
- Zugriff aus dem Internet per LDAPS, Quelle sind bekannte IP-Adressen

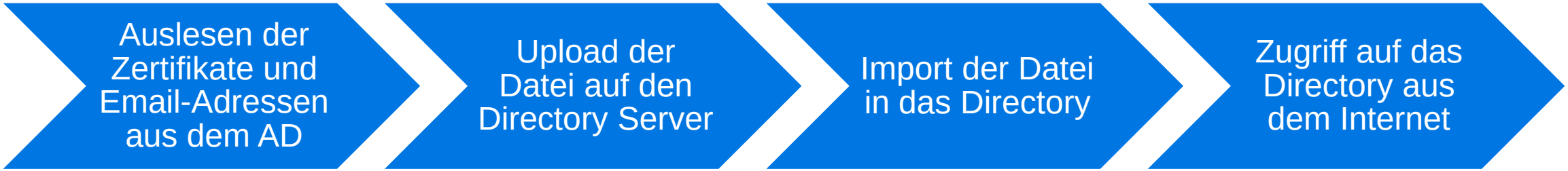
  → mit welcher Methode lässt sich das am besten absichern? Reverse Proxy, DMZ, WAF, …?

  → VMs in Azure bekommen keine öffentliche IP
- Zertifikate sollten stets aktuell sein

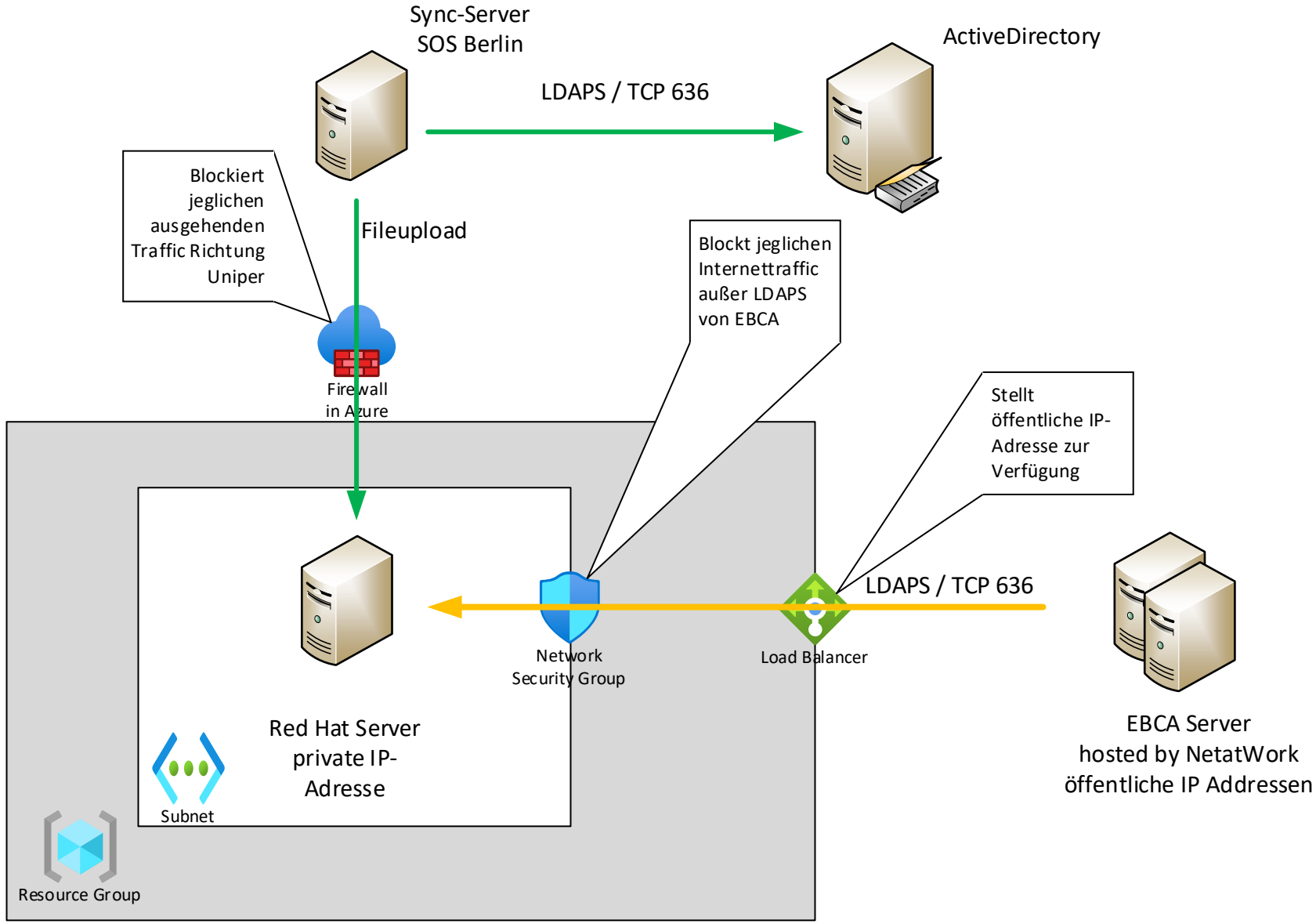
Auf der Suche nach dem besten LDAP Server…

- Können wir den offiziellen Red Hat Enterprise Directory Server verwenden?
  → Kosten lange unklar, Lizenzierung und Rahmenvertrag ebenso
  → stattdessen Open-Source Directory Server: **389 DS**
- Wie kann man den Zugriff aus dem Internet absichern?
  → **Azure Loadbalancer** mit öffentlicher IP-Adresse und **NSG**
- Wie kann man von dort den Zugriff aufs AD sicher gestalten?
  → Statt direktem Zugriff **Upload einer Datei** mit allen Daten AUF den Directory Server

Datenfluss


Auslesen der Zertifikate und Email-Adressen aus dem AD
Upload der Datei auf den Directory Server
Import der Datei in das Directory
Zugriff auf das Directory aus dem Internet

Infrastruktur



Implementierungsdetails

- Directory basiert auf “389 DS” (Open Source Directory Server)
- Täglicher Komplett-Import der exportierten Zertifikate
  → vereinfacht das Import-Skript
- Reduzierte Angriffsfläche
  → Directory Server enthält nur Email-Adressen und Zertifikate, keine weiteren Daten
- Upload der Daten per SSH auf den Red Hat Server
  → keinerlei ausgehende Verbindungen vom Server
- Lösung ist 1:1 als Testumgebung geklont
  → Testserver ist dauerhaft heruntergefahren (keine Kosten für die Maschine) und wird nur bei Bedarf gestartet
- Skalierbarkeit
  → Durch Verwendung des Loadbalancer kann die Umgebung bei Bedarf leicht um weitere Server erweitert werden
  → Der Server selbst kann relativ schnell auf eine größere oder kleinere VM-Klasse angepasst werden
  → 389 DS unterstützt Replikation zu weiterem Server

Vielen Dank für die Aufmerksamkeit

Vielen Dank an
almanid Deutschland GmbH / Alexander Sommer

für das Design und die erfogreiche Implementierung der Lösung