AEQUITAS INTEGRATION

Zertifikatsmanagement mit Azure Automation und Let's Encrypt

Fabian Bader

Über mich…

- Senior Consultant @ Aequitas Integration
- @fabian_bader auf Twitter
- Organisator der @HHPSUG
- fabian [at] cloudbrothers.info

Warum automatisieren

- Zertifikatslaufzeiten werden immer weiter verkürzt
- Seit 2008 – 825 Tage Laufzeit
- Eventuell ab 2020 – Maximal 398 Tage

Let‘s Encrypt?

Was ist Let‘s Encrypt?

We give people the digital certificates they need in order to enable HTTPS (SSL/TLS) for websites, for free, in the most user-friendly way we can. We do this because we want to create a more secure and privacy-respecting Web.

Was ist Let‘s Encrypt?

- Kostenfreie Zertifikate
- 100% automatisiert mittels eines offenen Standards (ACME Protokoll)
- Transparent durch Certificate Transparency
- Betrieben durch die Internet Security Research Group
- Finanziert durch Spenden und Sponsoren
- Wird von den wichtigsten Plattformen als Trusted Root CA anerkannt

Wie funktioniert Let‘s Encrypt?

- Zertifikatsanfrage wird mittels ACME Protocol an Let‘s Encrypt Server gesendet
  - z.B. mittels certbot
- Let‘s Encrypt prüft anhand einer Challenge ob es sich um eine legitime Anfrage handelt
  - HTTP-01
    Eine Datei mit einem Token wird per HTTP veröffentlich
  - DNS-01
    Für die angefragten Domains muss ein TXT DNS Records mit einem Token erstellt werden
  - TLS-ALPN-01
    Der Token wird im TLS Handshake mit dem Server übergeben

Azure Automation

Was ist Azure Automation?

- Serverless Automatisierungslösung
- Unterstützt PowerShell und Python
- Ein Skript entspricht einem Runbook
- Ausführen der Runbooks auf Shared Ressourcen
  - Kein Zugriff auf interne Ressourcen
  - Kein persistenten Speicherort
  - Keine Möglichkeit zusätzliche Binärdateien auszuführen

Komponenten von Azure Automation

- Azure Automation besteht aus mehreren Komponenten
  - Runbooks
    Skripte in den Sprachen PowerShell und Python 2 (Preview), sowie grafische Runbooks
  - Schedules
    Ermöglichen ein Runbook zu bestimmten Zeiten wiederkehrend zu starten
  - Jobs
    Gestartete Runbooks werden als Jobs dargestellt
  - Hybrid Worker Groups
    Beim Kunden installierte Agenten, die eine Ausführung der Skripte on-Premise erlauben
  - Assets
    Informationen und Ressourcen die von Runbooks genutzt werden können

Assets

- Credentials
  - PSCredential Objekte = Benutzername / Passwort
- Connections
  - Verbindungsinformationen für Azure Services
- Zertifikate
  - Zertifikate inkl. privatem Schlüssel
- Variablen
  - String, Boolean, DateTime, Integer und Not specified
  - Können verschlüsselt abgelegt werden

Posh-ACME

Posh-ACME

- Implementierung des ACME Protokolls als PowerShell Modul von Ryan Bolger (@rmbolger)
- Unterstützt ACME v2 und somit Wildcard Zertifikate
- Integration von verschiedenen DNS Anbietern
- DNS Challenge mit CNAME Unterstützung
- PowerShell Core Unterstützung
- Lokale Speicherung der Account Daten für Erneuerung und Neuausstellung
- Lokale Speicherung der ausgestellten Zertifikate

Unterstützte DNS Anbieter

- AcmeDns
- Aliyun
- AutoDNS
- Azure
- BlueCat
- Cloudflare
- ClouDNS
- DeSEC
- DMEasy
- DNSimple
- DOcean
- Domeneshop
- Dreamhost
- Dynu
- EasyDNS
- FreeDNS
- Gandi
- GCloud
- GoDaddy
- HurricaneElectric
- IBMSoftLayer
- Infoblox
- Linode
- LuaDns
- Manual
- Namecheap
- NameCom
- NS1
- OVH
- Rackspace
- Route53
- SimpleDNSPlus
- UnoEuro
- Windows
- Zonomi

Zertifikatsaustellung mit Posh-ACME

- Modul importieren
- Account mit Kontaktinformationen erstellen
- Definition der gewünschten SAN im Zertifikat (z.B. test.aequitas-integration.de)
- Zertifikat erstellen mittels DNS Validierung

```
Import-Module Posh-ACME -Force
New-PAAccount -Contact "mailto:certcontanct@aequitas-integration.de" –AcceptTOS
$paPluginArgs = @{
    AZSubscriptionId = "SubscriptionID"
    AZAccessToken    = "AccessToken";
}
New-PACertificate -Domain "test.aequitas-integration.de" -DnsPlugin Azure
    -PluginArgs $paPluginArgs
```

Workfolder

- Das Ergebnis ist ein ausstelltes Zertifikat im Ordner %LOCALAPPDATA%\Posh-ACME
- Die Ordner Struktur ist aufgeteilt nach
  - Verwendeter Server
    - Account ID
      - Domain
- Die PFX Datei wird mit dem Standardpasswort „poshacme“ erstellt

```
.
├── current-server.txt
│
└── acme-staging-v02.api.letsencrypt.org
    ├── current-account.txt
    ├── dir.json
    │
    └── 123456789
        ├── acct.json
        ├── current-order.txt
        ├── plugindata.xml
        │
        └── test.aequitas-integration.de
            cert.cer
            cert.key
            cert.pfx
            chain.cer
            fullchain.cer
            fullchain.pfx
            order.json
            request.csr
```

Herausforderungen

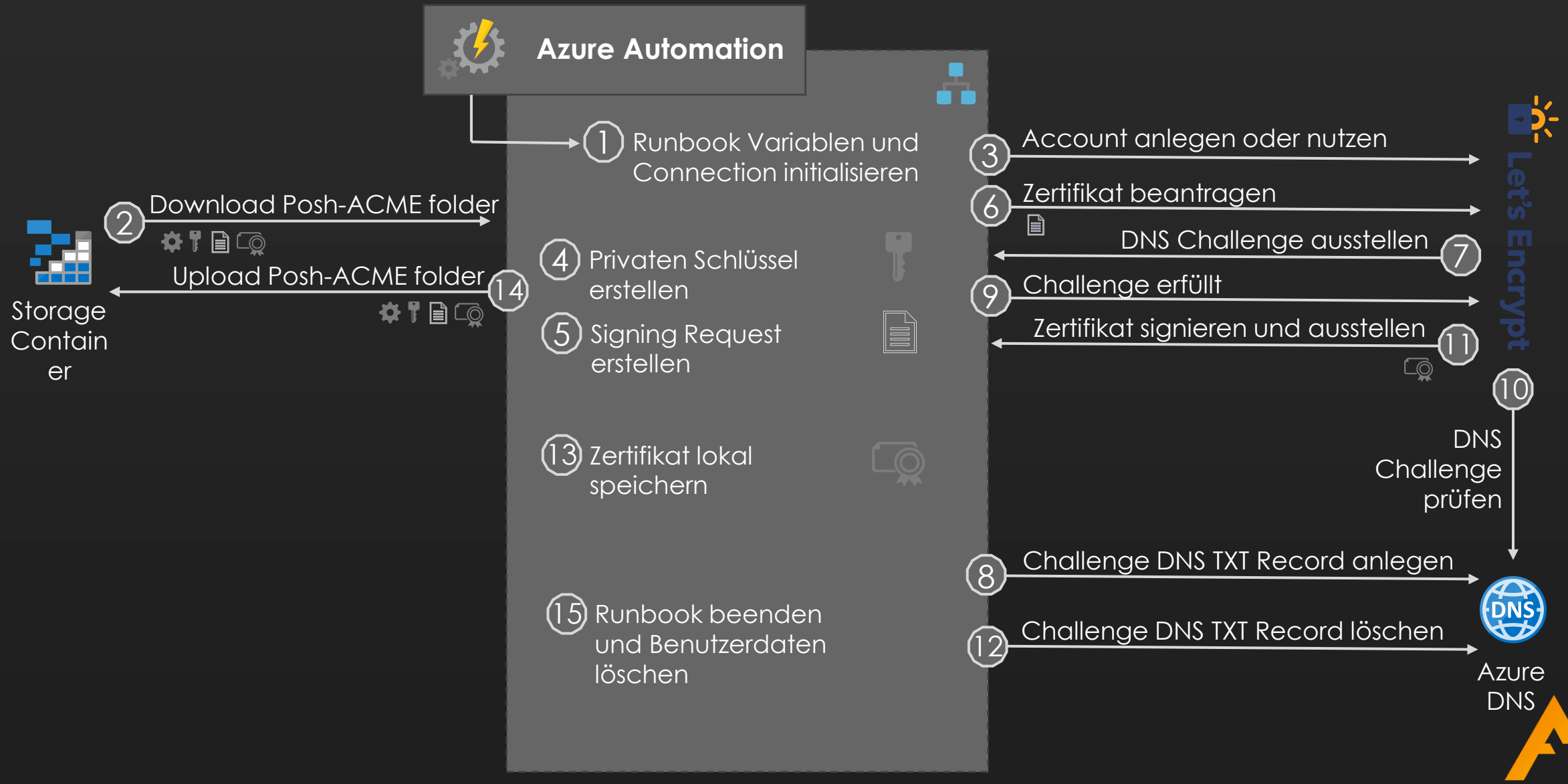
- Posh-ACME speichert die Daten im lokalen Benutzerprofil
- Azure Automation verwirft alle Benutzerdaten nach der Ausführung des Runbooks
- Standardkennwort für PFX Datei
- Authentifizierung an Azure DNS notwendig

Herausforderungen

- Posh-ACME speichert die Daten im lokalen Benutzerprofil
- Azure Automation verwirft alle Benutzerdaten nach der Ausführung des Runbooks
  - ☑ Speicherung der Konfigurationsdaten in einem Azure Storage Container
- Standardkennwort für PFX Datei
  - ☑ Setzten eines selbst definierten Kennworts und Speicherung als Azure Automation verschlüsselte Variable
- Authentifizierung an Azure DNS notwendig
  - ☑ Anlage und Berechtigung eines Azure Run Accounts für die Verwaltung der DNS Zone und des Storage Containers

Wie arbeitet das alles zusammen?

Lösungsübersicht



DNS Validierung mit CNAME Support

- Herausforderung
  - Das Team, das den externen DNS verwaltet, nutzt einen DNS Anbieter ohne API Unterstützung und kann/möchte nicht migrieren
  - Aus Sicherheitsbedenken ist ein API Schlüssel für eine Company TLD nicht erlaubt
  - Organisatorischen Gründe machen es unmöglich per API auf den DNS zuzugreifen
- Lösung
  - DNS Validierung mit CNAME Support

DNS Validierung mit CNAME Support

DNS
ohne API

DNS Zone	aequitas-integration.de	Type	Content
DNS Record:	test	A	127.0.0.1
ACME Validation Record	_acme-challenge.test	CNAME	⬇
	_acme-challenge.test.aequitas-integration.de.levalidation.aequitas-integration.de		
	levalidation	NS	ns1-09.azure-dns.com.

Azure DNS

DNS Zone	levalidation.aequitas-integration.de	
ACME Validation Record	_acme-challenge.test.aequitas-integration.de	TXT

DNS Validierung mit CNAME Support

DNS
ohne API

DNS Zone	aequitas-integration.de	Type	Content
DNS Record:	test	A	127.0.0.1
ACME Validation Record	_acme-challenge.test	CNAME	⬇
	_acme-challenge.test.aequitas-integration.de.levalidation.de		

Azure DNS

DNS Zone	levalidation.de	
ACME Validation Record	_acme-challenge.test.aequitas-integration.de	TXT

Hands-On

```
# git clone https://github.com/f-bader/AzAutomation-PoshACME
# cd .\AzAutomation-PoshACME\
# code .
```

Food for thought

Kosten

- Let‘s Encrypt
  - € 0,00 € / Zertifikat
- Azure DNS
  - € 0,422 / Zone / Monat
  - € 0,3381 / 1.000.000 DNS Abfragen / Monat
- Azure Storage Account (LRS-Standard/Hot)
  - € 0,0166 / GB / Monat
- Azure Automation
  - € 0,00 / <=500 Minuten / Monat
  - € 0,002 / Minute
- Erwartete Gesamtkosten für Azure Ressourcen: 0,78 €

1 Euro ?


WAS KANNST DU IN EUROPA FÜR 1 EURO KAUFEN?
ISLAND
1 LITER MILCH
IRLAND
SALATKOPF
VEREINIGTES KÖNIGREICH
1 SCHOKORIEGEL
FRANKREICH
BAGUETTE
BELGIEN
KAUGUMMI
SPEARMINT
DEUTSCHLAND
BRETZEL


ITALIEN
ESPRESSO
NORWEGEN
1/2 KILO KARTOFFELN
TSCHECHIEN
2 BIER IM SUPERMARKT
KROATIEN
1 GROSSES EIS
UNGARN
1 GLAS WEIN
MAZEDONIEN
HOT DOG
GRIECHENLAND
1 GLAS RETSINA
RUMÄNIEN
1 STÜCK PIZZA
WEISSRUSSLAND
1 LITER BENZIN
LITAUEN
1 FLASCHE COLA
FINNLAND
1 BECHER SCHLAGSAHNE
TÜRKEI
1 STÜCK BAKLAVA
HOSTELWORLD.com

Integration in

- Azure KeyVault
- Azure Application Proxy
- …

Scheduler

Event basierter Zertifikatsaustausch