Kerberos, SQL Server & Azure AD DS

Lars Lawrenz
SARPEDON Quality Lab GmbH

SARPEDON QUALITY LAB

Migration von Legacy Systemen oder Software in die Cloud…

Legacy Software und System

- Kann nicht direkt als Clouddienst betrieben werden
- Benötigt Dienste wie das Active Directory
- Benötigen direkten Zugriff auf Windows Dienste
- Kerberos (Delegation)

Azure Active Directory Domain Services

Azure Active Directory Domain Services (Azure AD DS) ist ein Cloud-Dienst, der verwaltete Domänendienste wie Domänenbeitritt, Gruppenrichtlinien, LDAP und Kerberos-Authentifizierung bereitstellt, ohne dass Domänencontroller erforderlich sind.

Azure AD DS nutzt den vorhandenen Azure AD-Mandanten, um die Identität und den Zugriff auf Cloud-Ressourcen zu verwalten.



Azure AD DS

- Verwalteter Cloud Dienst
- Basiert auf Azure AD
- Keine Domänen Admins, Enterprise Admins



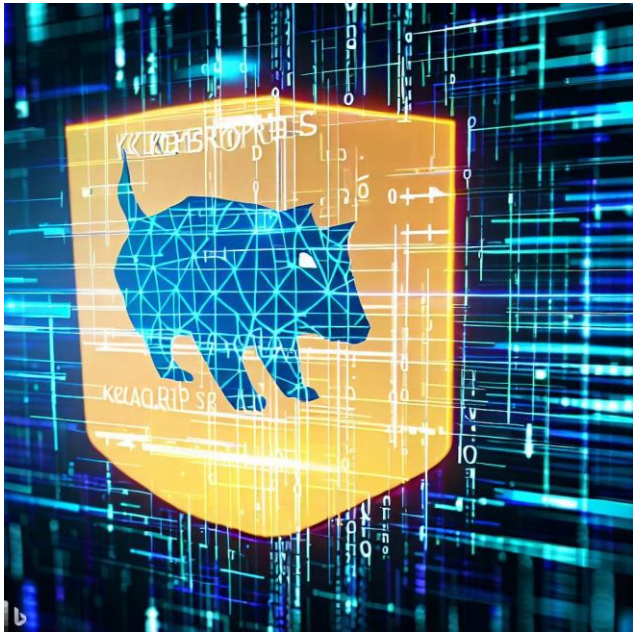
- Betrieb einer Active Directory CA nicht möglich
- Nur Constraint Delegation möglich

Was ist Kerberos?

Kerberos ist ein Netzwerkprotokoll, das eine sichere Authentifizierung zwischen Client, Server und einer vertrauenswürdigen dritten Partei ermöglicht. Kerberos verwendet Tickets, die vom Kerberos-Server ausgestellt werden, um die Identität der Kommunikationspartner zu überprüfen und den Zugriff auf Dienste zu gewähren. Kerberos vermeidet die Übertragung von Passwörtern über das Netzwerk und unterstützt Single Sign-on...



Warum Kerberos?



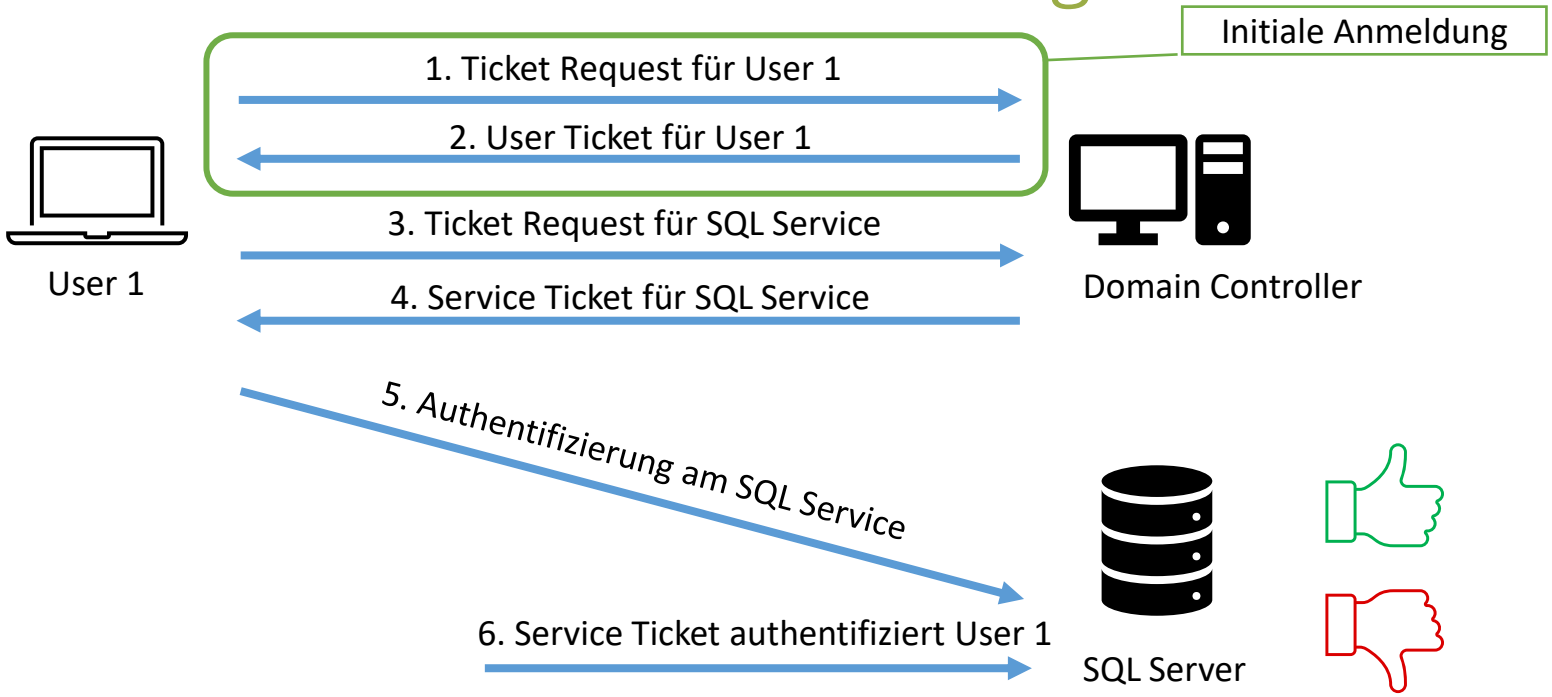
Warum Kerberos?

- Schnelle Authentifizierung durch Tickets
- Gegenseitige Authentifizierung von Diensten und Clients
- Sichere Authentifizierungszeitraum durch Zeitstempel
- Anpassung an moderne verteilte Systeme
- Wichtig für die Sicherheit von Daten und Diensten in offenen oder unsicheren Netzwerken wie dem Internet.
- Schützt vor Hackerangriffen wie Abhören, Wiederholen oder Manipulieren von Datenpaketen.

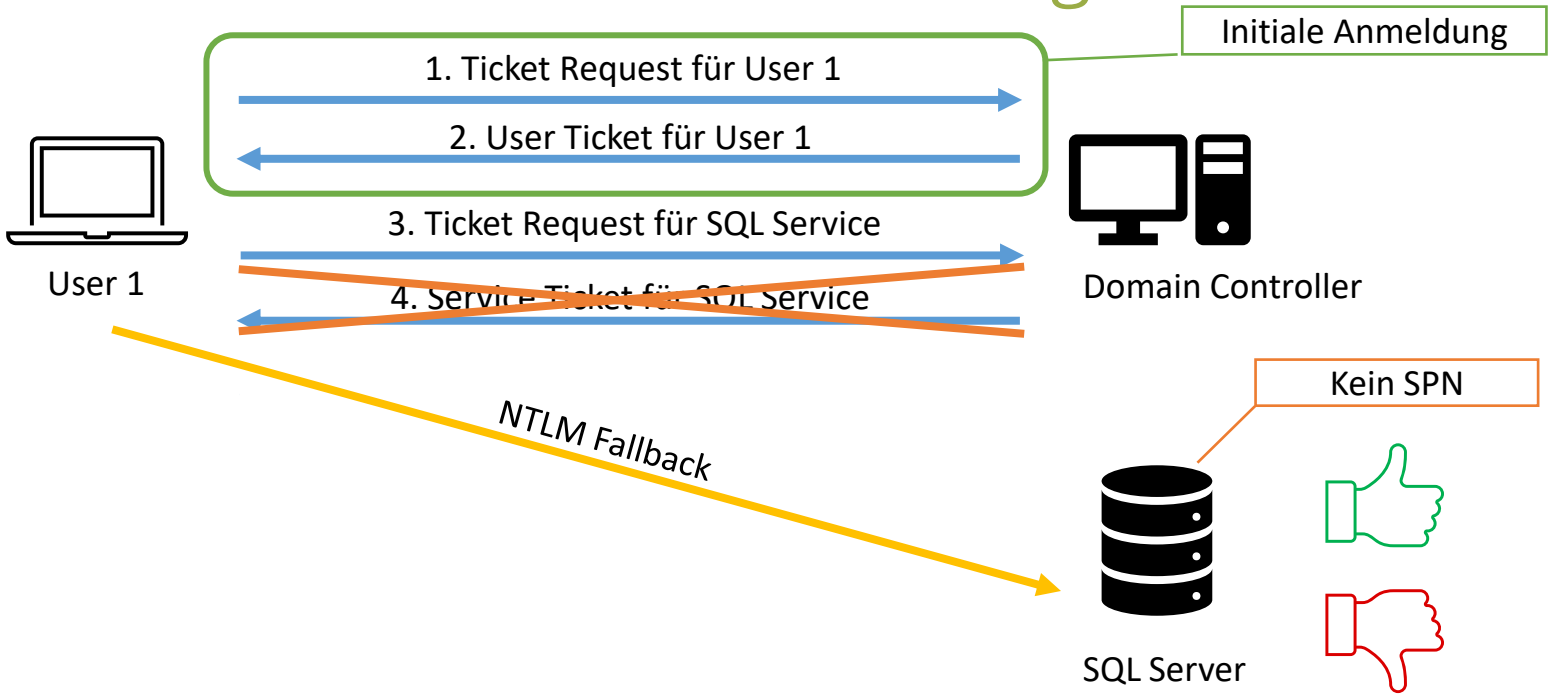
Nichts ist zu 100% sicher…

- Silver Ticket Attack
- Golden Ticket Attack
- Kerberosting

Ablauf Kerberos Authentifizierung



Ablauf Kerberos Authentifizierung




sqlpass.de
PASS

Architektur



Demo-Architektur



Azure AD



Azure AD DS



Virtuelles Netzwerk



DEMOSQL1



DEMOSQL2

Die nächsten Schritte...

Vorbereitet

- Azure AD DS aufgesetzt
- Synchronisation aus AAD
- SQLDEMO1
- SQLDEMO2
- Dienstkonten erstellen

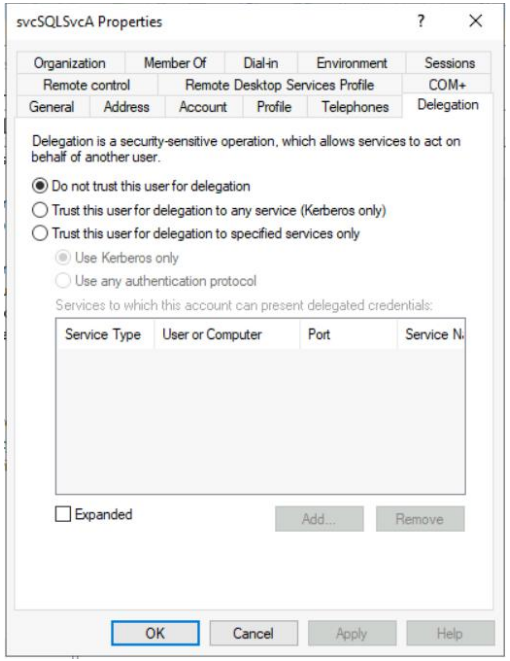
To Do..

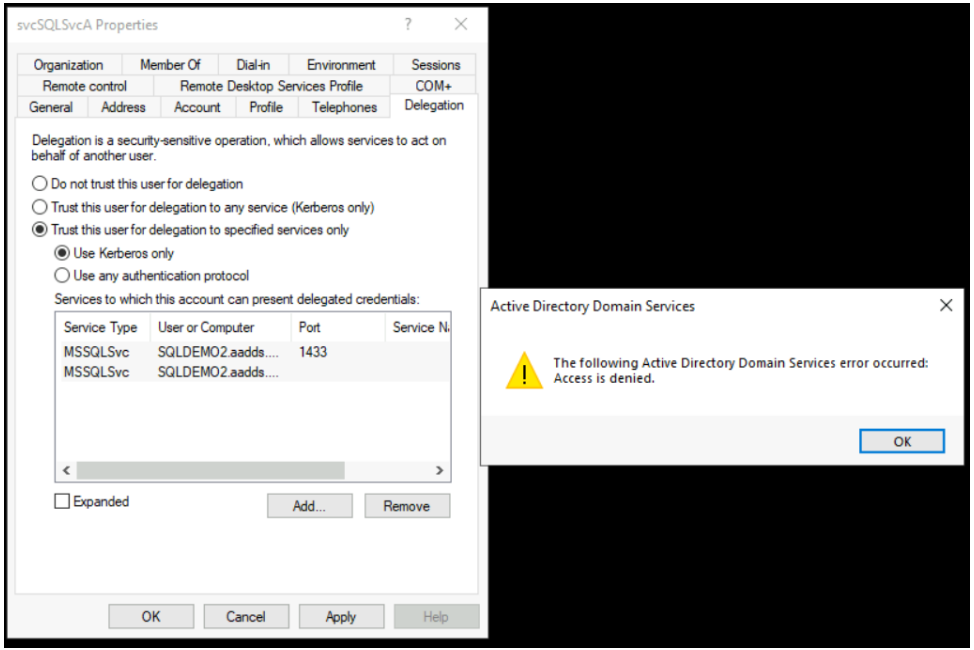
- Dienstkonten hinterlegen
- SPNs registrieren
- Constraint Delegation

DEMO



Delegation in Azure AD DS aktivieren

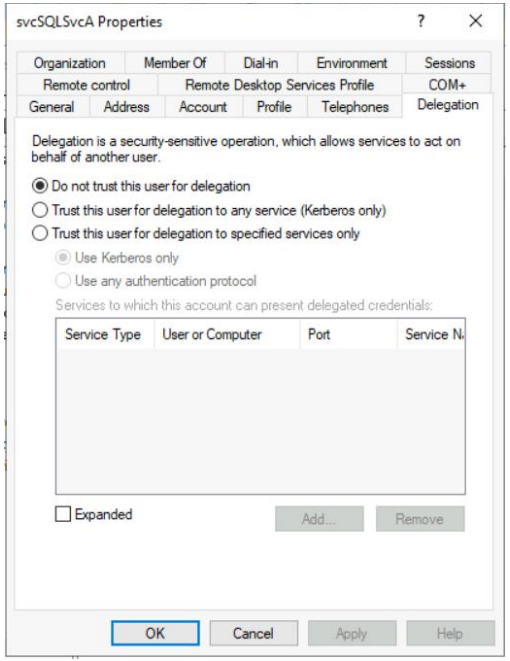




Delegation in Azure AD DS aktivieren

```
Set-ADUser -Identity svcSQLSvcA
        -PrincipalsAllowedToDelegateToAccount svcSQLSvcB
```

Nach der Aktivierung der Delegation..



Delegation prüfen

```
Get-ADUser -Identity svcSQLSvcA -Properties
        PrincipalsAllowedToDelegateToAccount
```

Zusammengefasst…

- Viele Dienste und Software lässt sich hiermit problemlos migrieren
- Vorab muss eine gründliche Inventur vorgenommen werden



Der Teufel liegt im Detail. Es gibt Konfigurationen oder auch Prozesse, die angepasst werden müssen. Es ist nicht alles 1:1 abbildbar.

Quellen

Kerberos

- Is a Kerberos ticket valid with only one-way external trust between domains? (in Englisch)

https://security.stackexchange.com/questions/128600/is-a-kerberos-ticket-valid-with-only-one-way-external-trust-between-domains

- Kerberos authentication with one-way forest trust (in Englisch)

https://learn.microsoft.com/en-us/answers/questions/1126926/kerberos-authentication-with-one-way-forest-trust

- How trusts work for Azure AD Domain Services (in Englisch)

https://learn.microsoft.com/en-us/azure/active-directory-domain-services/concepts-forest-trust

- Kerberos Explained

https://www.youtube.com/watch?v=snGeZlDQL2Q

Quellen

Azure AD DS

- Overview of Azure Active Directory Domain Services | Microsoft Learn

https://learn.microsoft.com/en-us/azure/active-directory-domain-services/overview

- Tutorial - Create an Azure Active Directory Domain Services managed domain | Microsoft Learn

https://learn.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance

Feedback

https://sqlkonferenzeval.azurewebsites.net/78827056125031



THANK YOU TO OUR SPONSORS

PASS DEUTSCHLAND e.V.
Microsoft Data Platform Community

pmOne

SOLARWINDS

smart casual datadesign

Mainzer Datenfabrik

b.telligent
smart data. smart decisions.

HMS analytical software

ORAYLIS
turn your data into value

TIMEXTENDER

Microsoft

ITGAIN

SOLISYON
www.solisyon.de

GDS BUSINESS INTELLIGENCE GmbH



Thank you very much for your attention.

Vielen Dank für Eure Aufmerksamkeit.