



## Danny de Haan

he/him



I am a SQL Server Infrastructure Specialist and Product Architect for on-premises Database Management Systems for a large pension provider in the Netherlands.

I've always placed a strong emphasis on Security, Risk Management and Compliance for the SQL Server landscape, ensuring industry best practices and regulatory requirements.

- Nearly 20 years IT Experience
- 10+ years DBA
- SQL Server Infrastructure Specialist

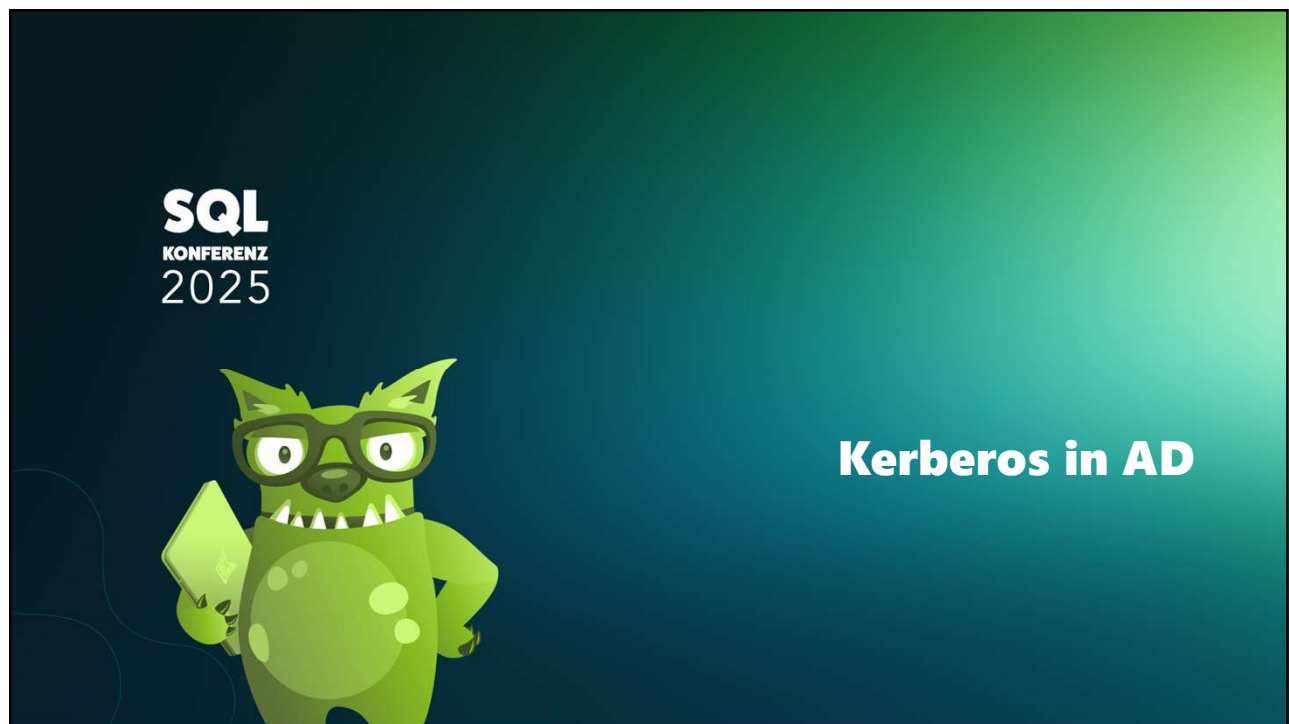
 /in/dannydh/  
 ThatInfraDb@pm.me



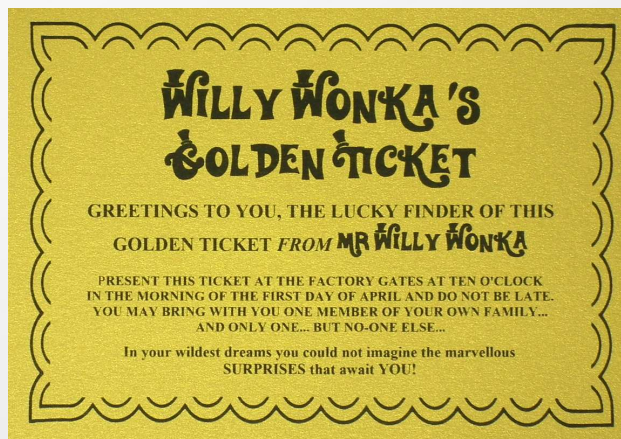


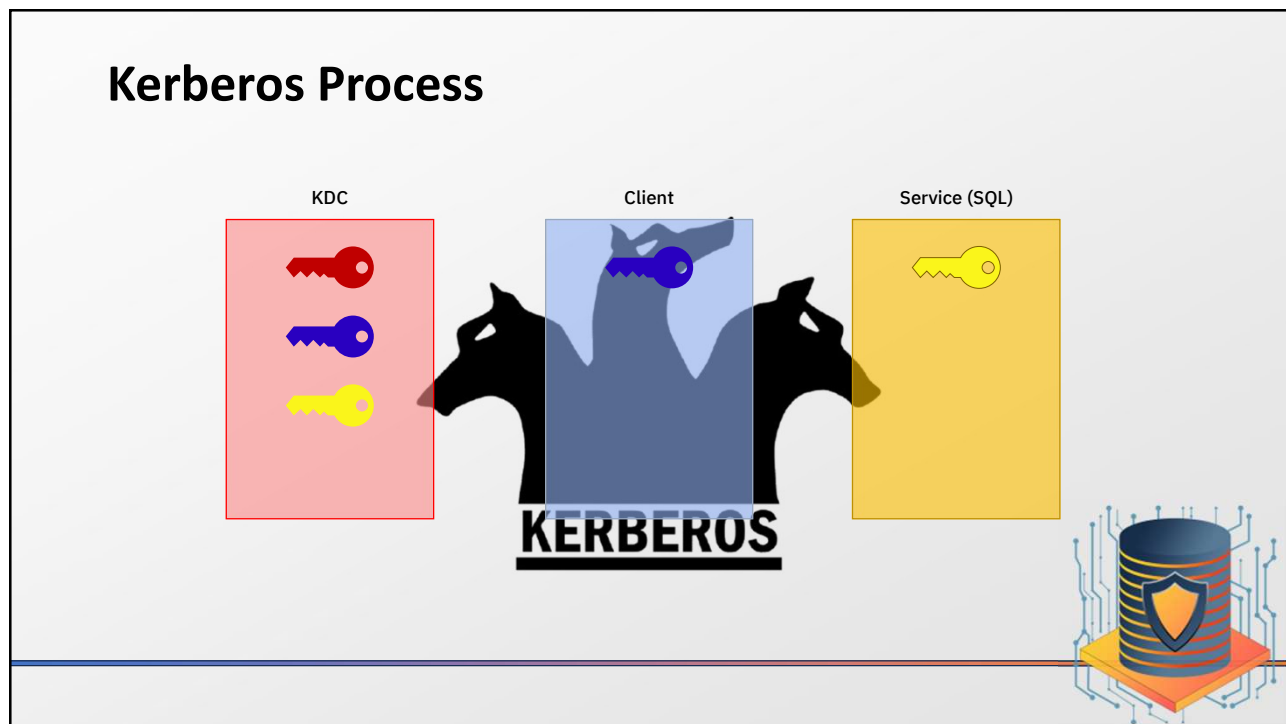
## Session Breakdown

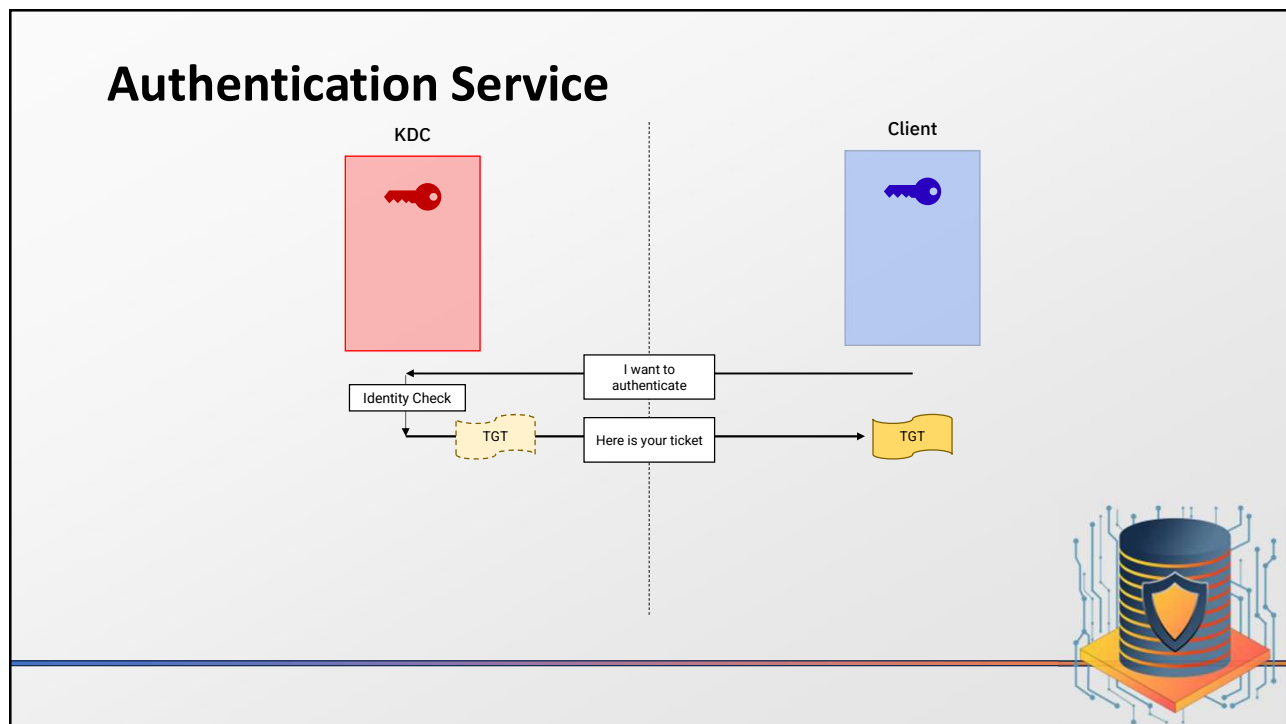
- Kerberos Process in AD
- Service Principal Names
- Database Engine
- Delegation
- Reporting Services
- Troubleshooting Tips
- Attack Scenario's

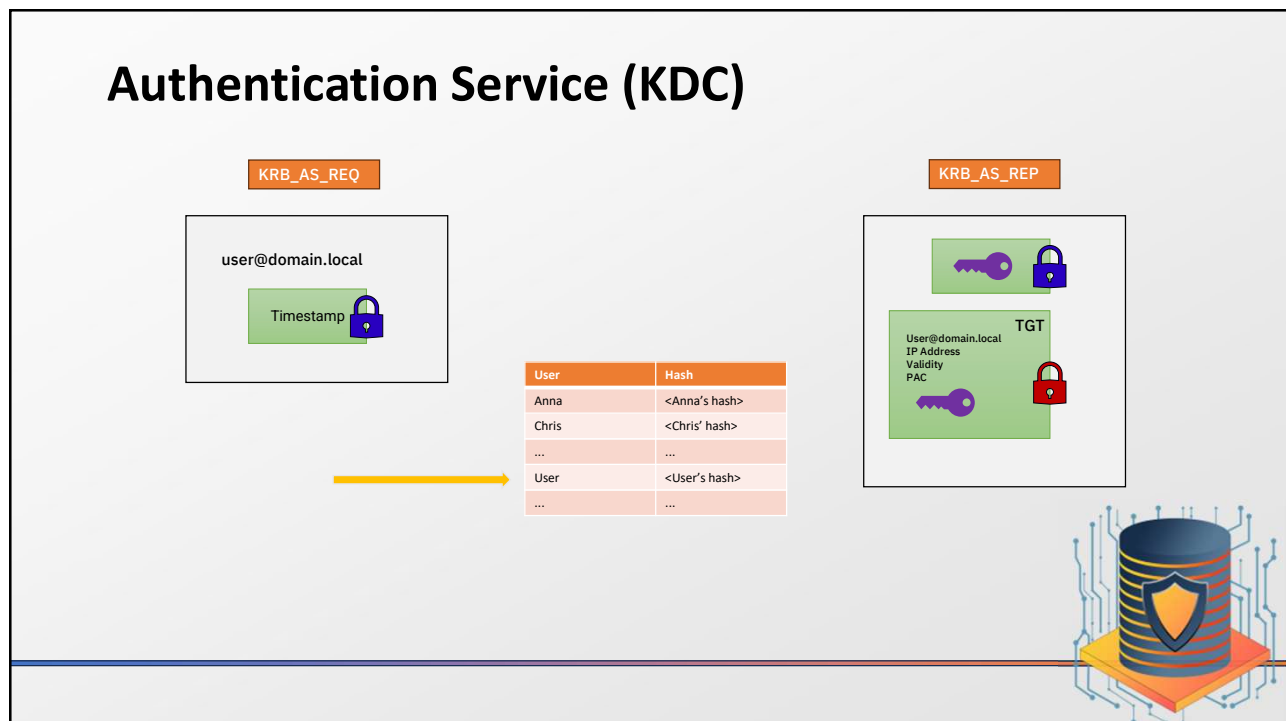


## Something with tickets?

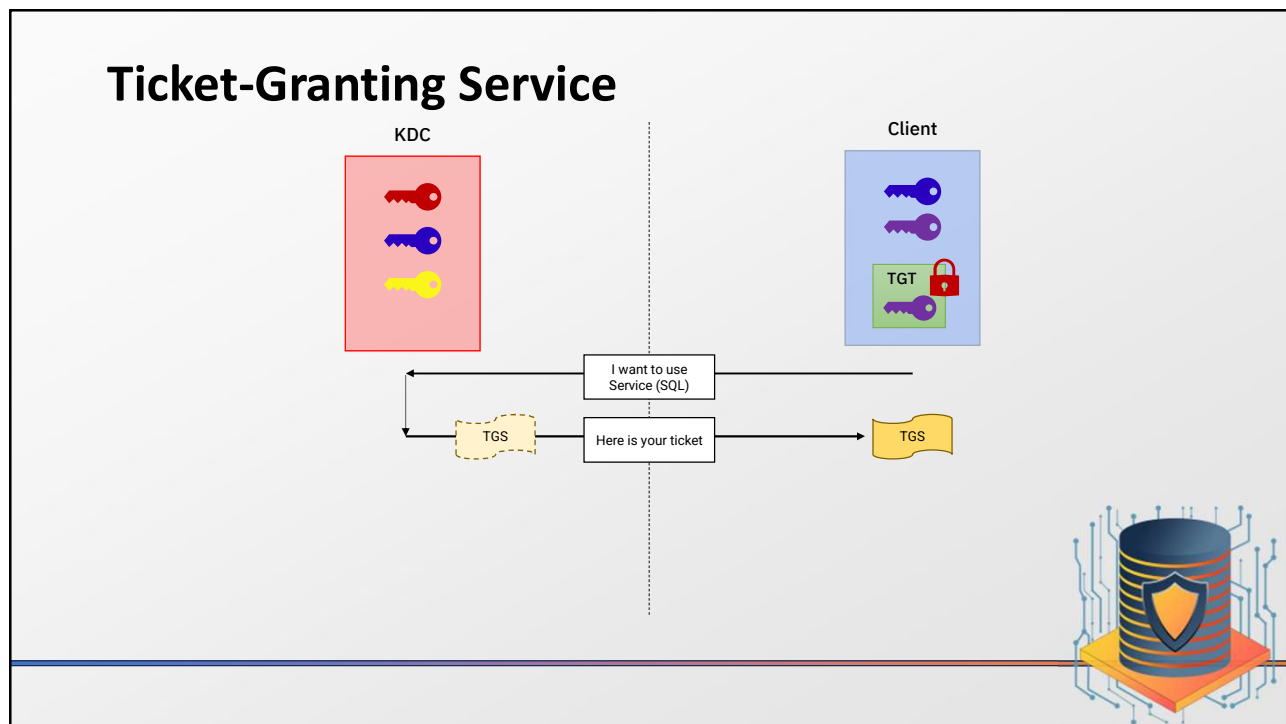








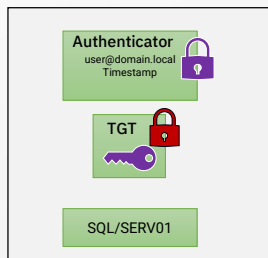




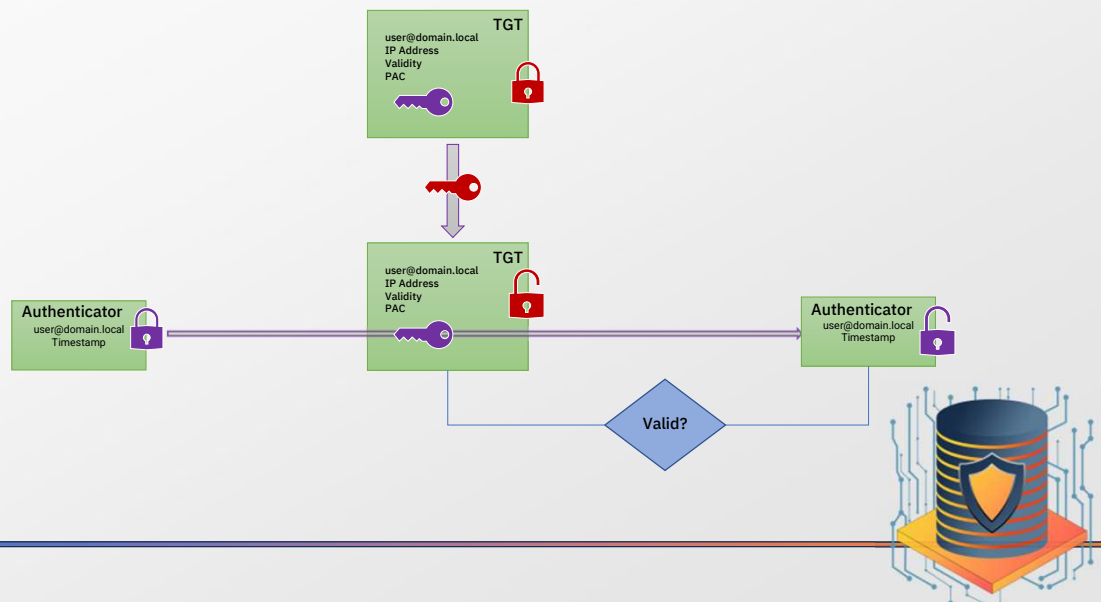
## Ticket-Granting Service (tickets)

KRB\_TGS\_REQ

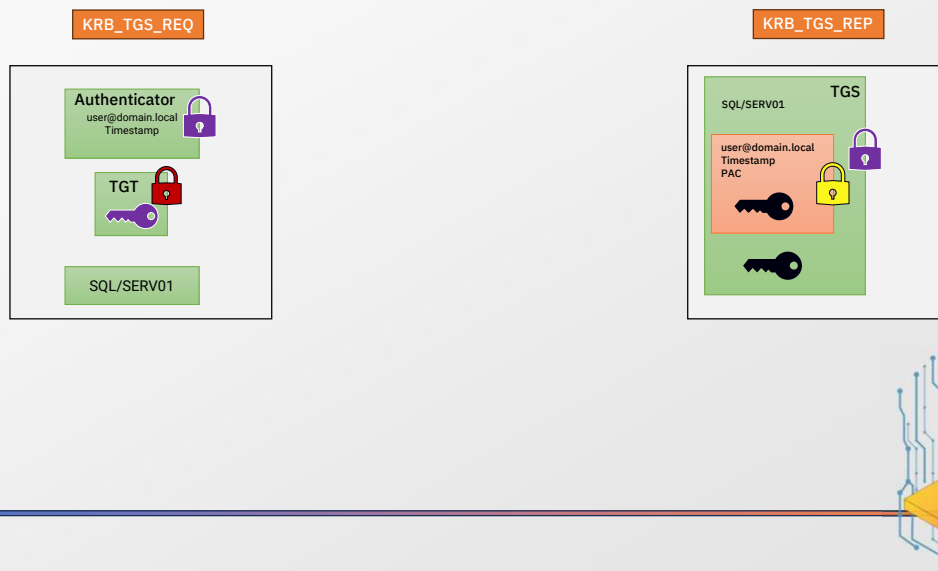
KRB\_TGS\_REP



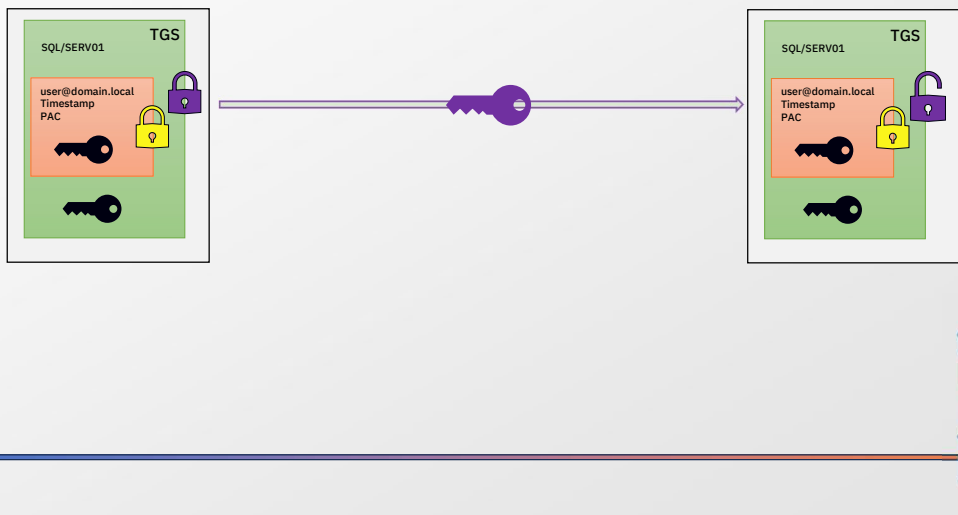
## Ticket-Granting Service (KDC)

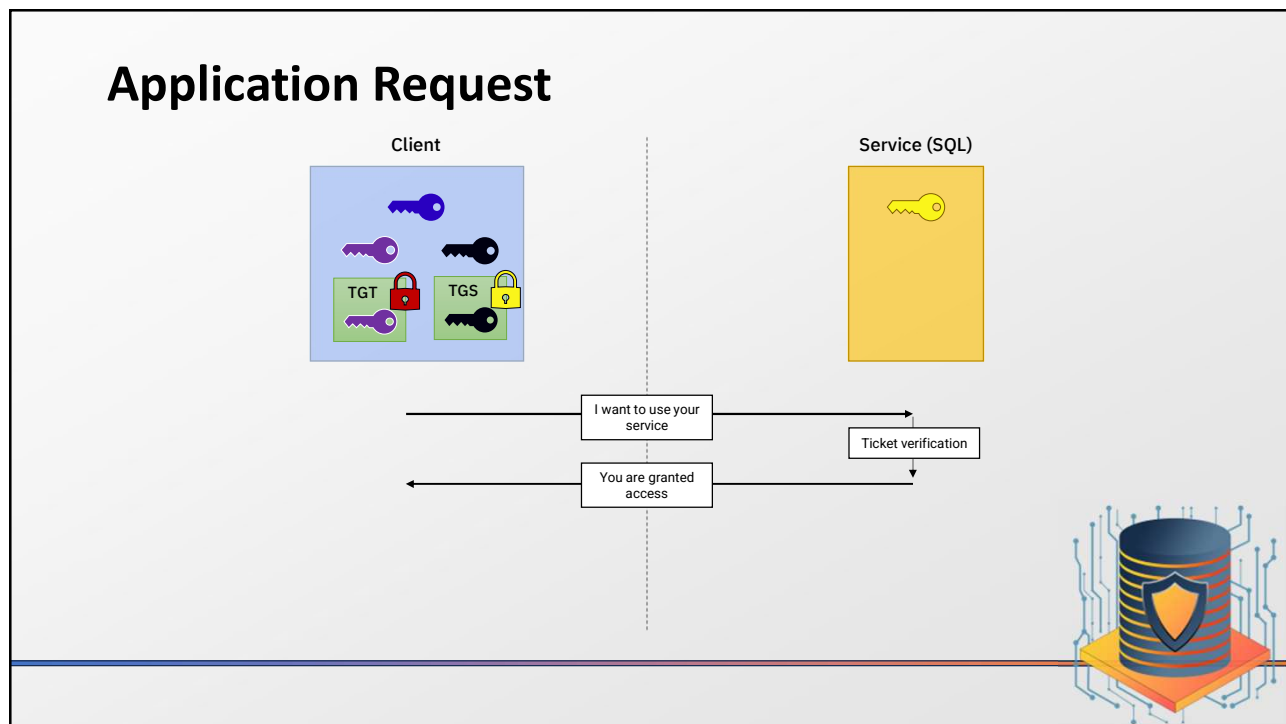


## Ticket-Granting Service (tickets)



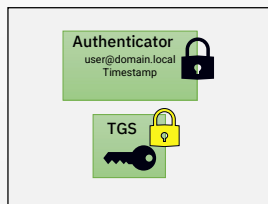
## Ticket-Granting Service (Client)



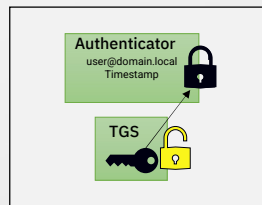


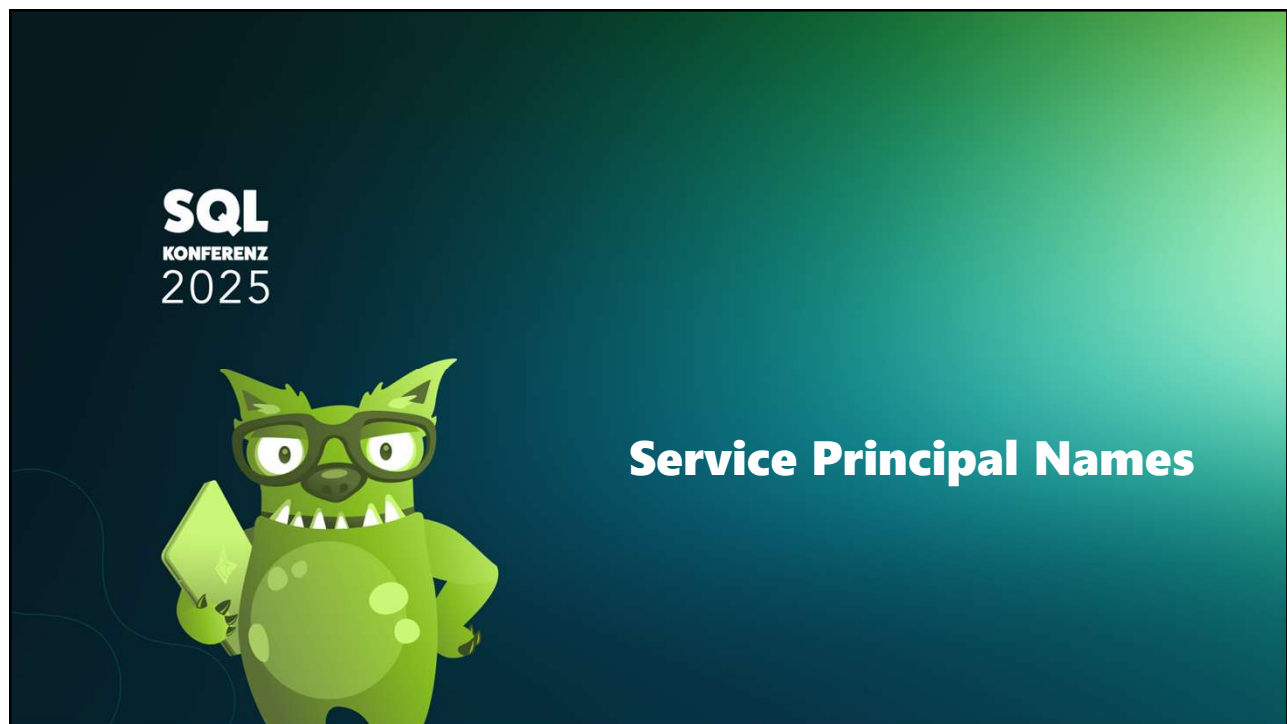
## Application Request (Service)

KRB\_AP\_REQ



KRB\_AP\_REP







## Service Principal Names

- What is a Service?
- SPN Definition
- Service Class
- SQL Server

alerter	eventlog	netlogon	rpc	snmp
anonymmt	eventsystem	netman	rpclocator	spooler
		nmagent	rpcss	tapisrv
cifs	http	oakley	rsvp	time
cisvc	ias	plugplay	samss	trksvr
clipsrv	iisadmin	poli	scardsvr	trkwks
dcom	messenger			ups
dhcp				w3svc
dmserver		remot		wins
dns	netdce		seclogon	www
dnscache				

service\_class/host(:port)

MSSQLSvc

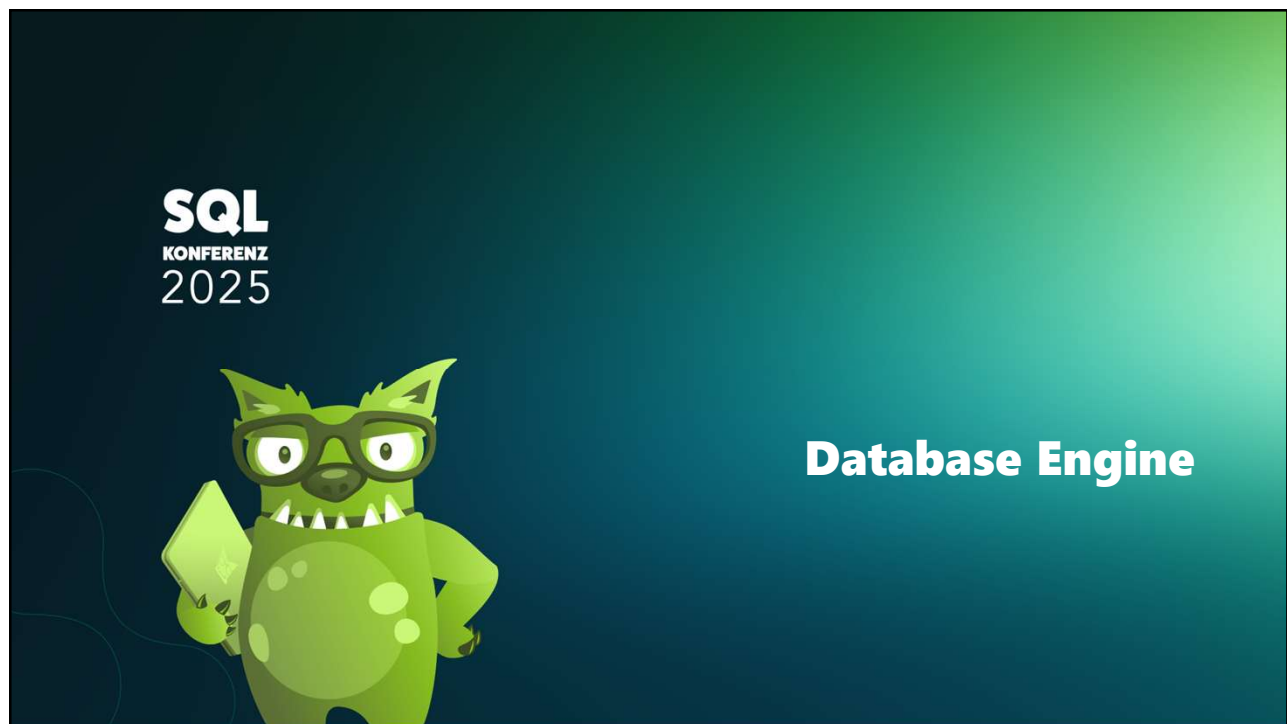
MSSQLSvc/Server01:1433



## Commands

- SETSPN
  - setspn -l (list)
  - setspn -s (create)
  - setspn -d (remove)





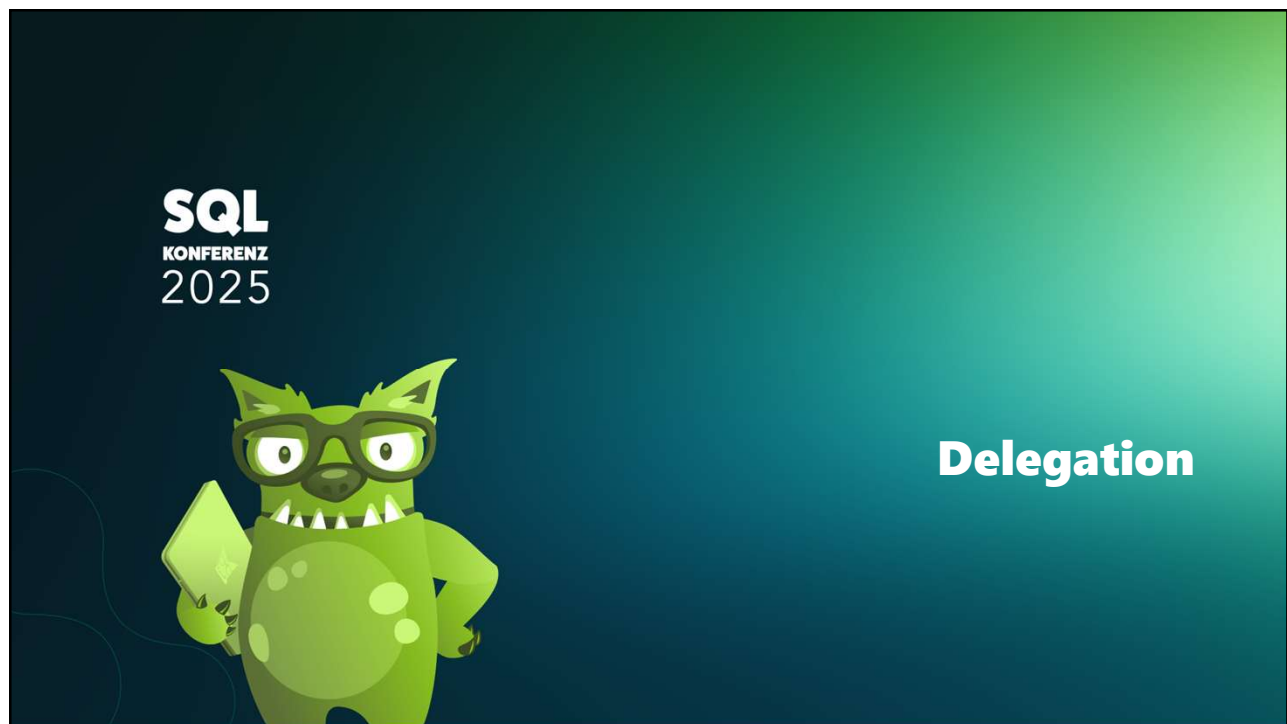
## Database Engine

### Setup:

- Domain Controller (purplel2c)
- SQL Server Host (sql22-01)
- Workstation (ws11)

DEMO



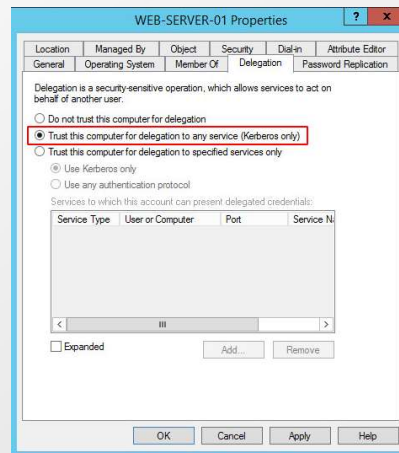
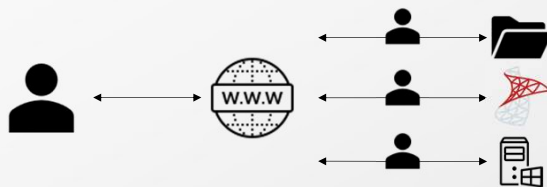


## Delegation

- What is delegation?

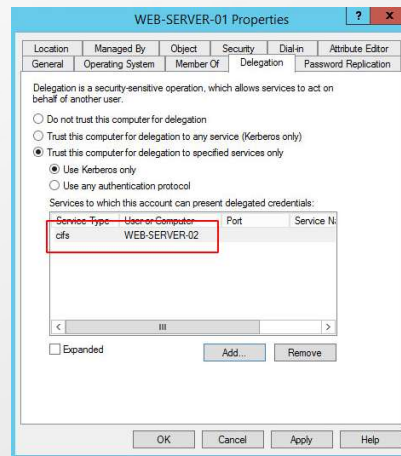
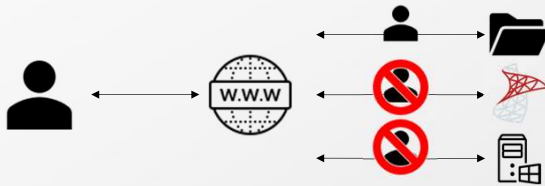


## Unconstrained Delegation



## Constrained Delegation

Constrained Delegation:  
CIFS/WEB-SERVER-02



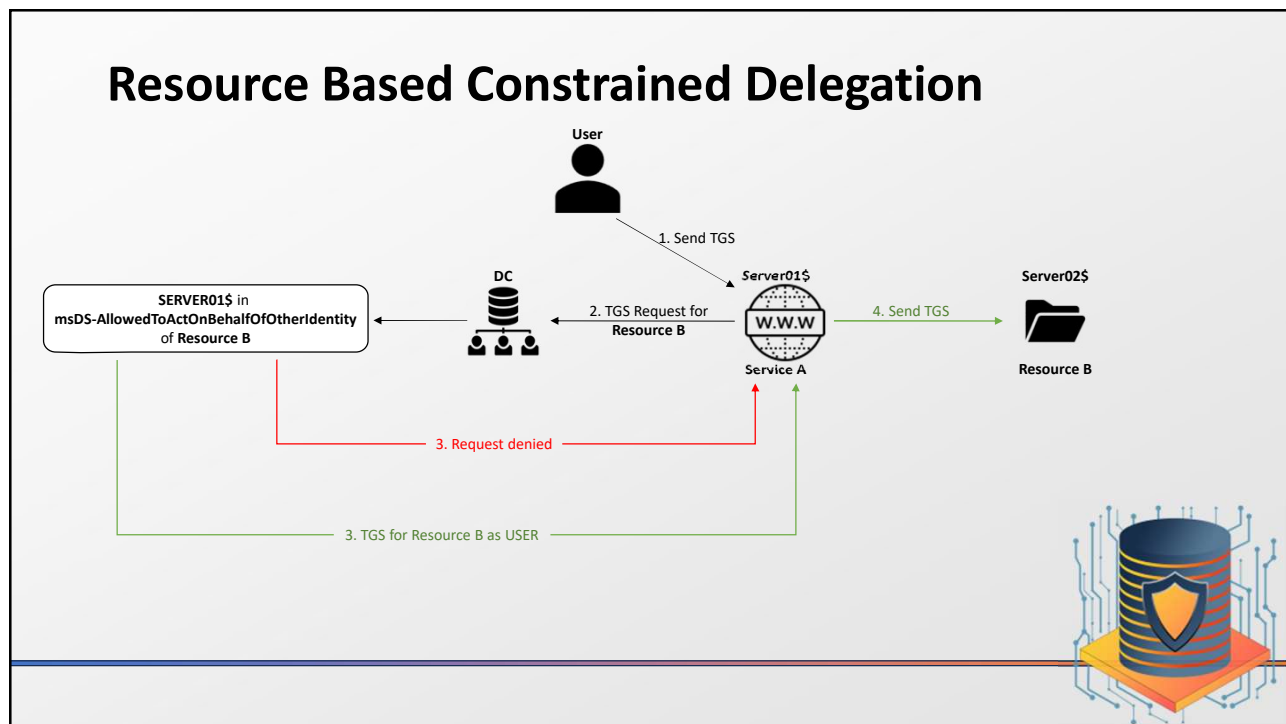


## Resource Based Constrained Delegation

- Responsibility lies with the Back-end Service
- Inter-Domain delegation
- Can be configured using PowerShell or Extended Attributes

New-ADComputer	Set-ADComputer
New-ADServiceAccount	Set-ADServiceAccount
New-ADUser	Set-ADUser
<b>PrincipalsAllowedToDelegateToAccount</b>	

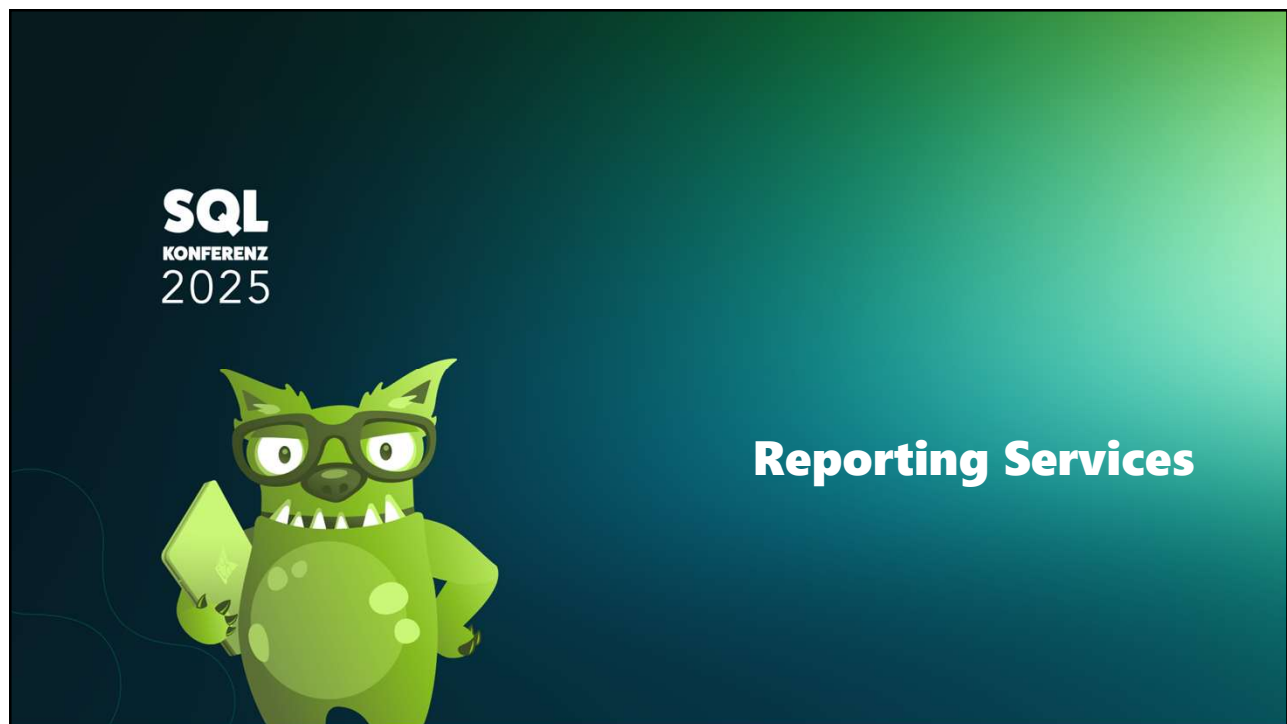




## Delegation Summary

- **Unconstrained delegation:** In this case, the client sends a copy of his TGT to a service, and that service uses it to impersonate the client to any other service. *Only an administrator can set this option on an account.*
- **Constrained delegation:** A list of resources is set on the service that wishes to delegate authentication. If protocol transition is allowed, then the service can pretend to be anyone when accessing resources in its list. *In any case, only an administrator can set this option.*
- **Resource-based Constraint Delegation:** The final resource has a list of trusted accounts. All accounts in this list can delegate authentication when accessing the resource. *Resources can modify this list as they wish, they don't need an administrator to update it.*





## Reporting Services

- WinRM uses HTTP Service Class on machine name
- SPN on different A-record for Reporting Services
- Constrained Delegation to HTTP SPN
- Constrained Delegation to SPN of Data Source (MSSQLSvc)



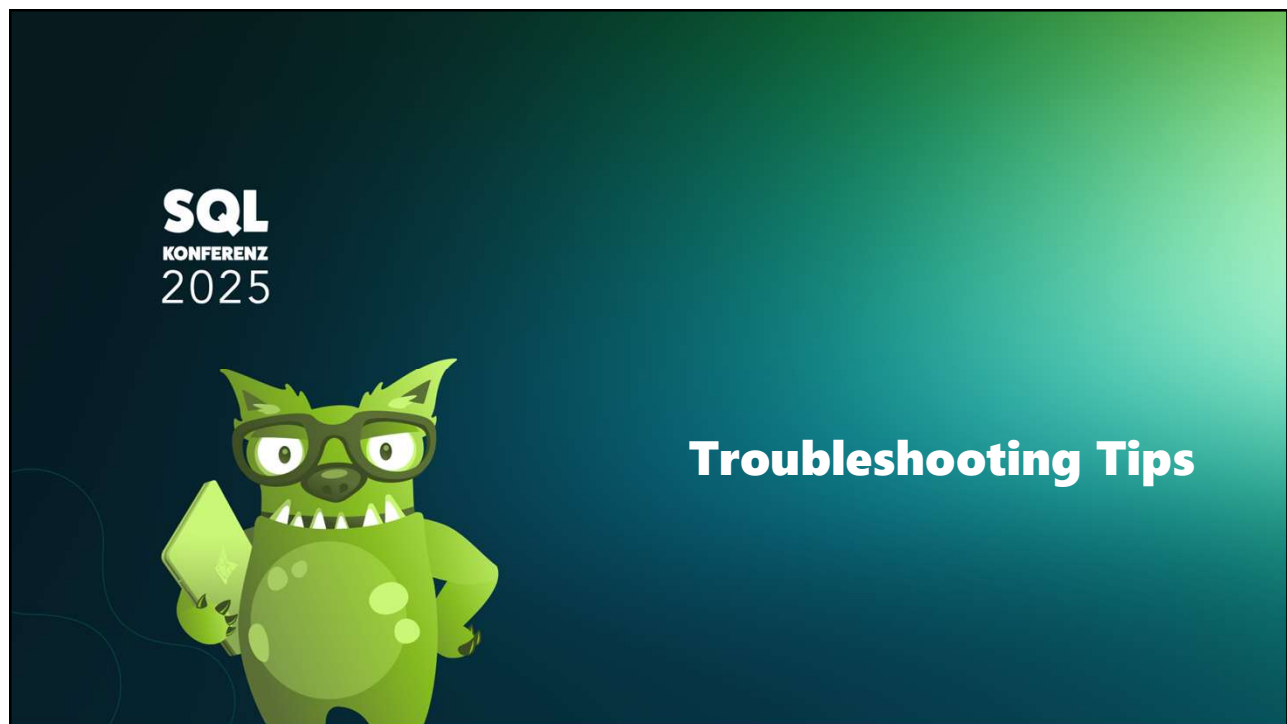
## Reporting Services Demo

### Setup:

- Domain Controller (purplel2c)
- SQL Server Host (sql22-01)
- Reporting Services (ssrs01 on sql22-01)
- SQL Server Host (sql22-02)
- Workstation (WS11)

DEMO

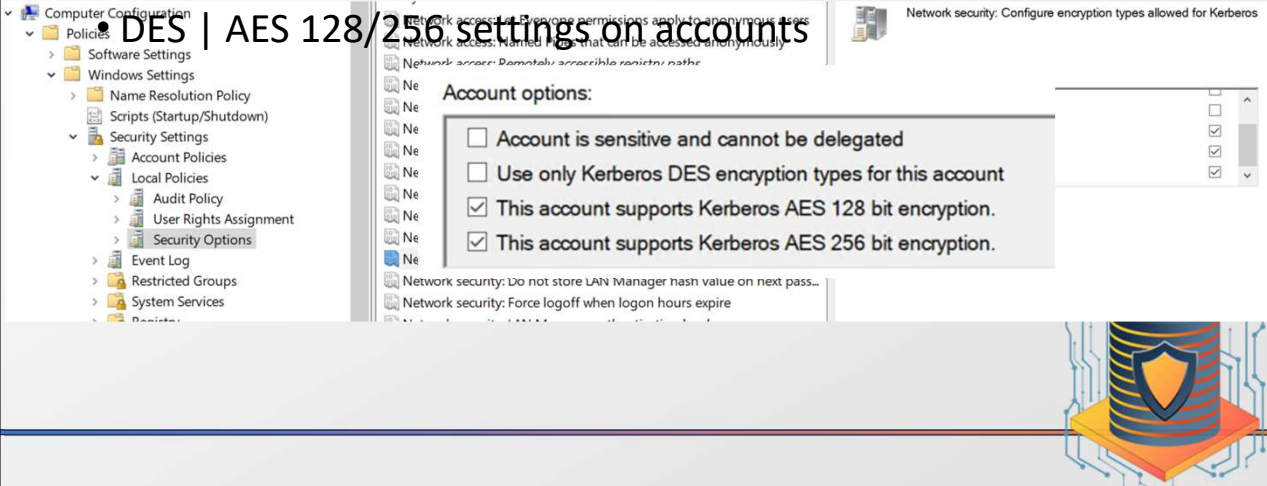




## Ciphers

- Network Security Settings (Network security: Configure encryption types allowed for Kerberos)


• DES | AES 128/256 settings on accounts



The screenshot shows the Windows Security Settings application. On the left, the 'Computer Configuration' tree is expanded to 'Security Settings' > 'Local Policies' > 'Security Options'. The main pane displays the 'Network security: Configure encryption types allowed for Kerberos' policy. Under 'Account options:', the following settings are visible:

- ☐ Account is sensitive and cannot be delegated
- ☐ Use only Kerberos DES encryption types for this account
- ☒ This account supports Kerberos AES 128 bit encryption.
- ☒ This account supports Kerberos AES 256 bit encryption.

Below these options, there are additional network security settings, including 'Do not store LAN Manager hash value on next pass...' and 'Force logoff when logon hours expire'.



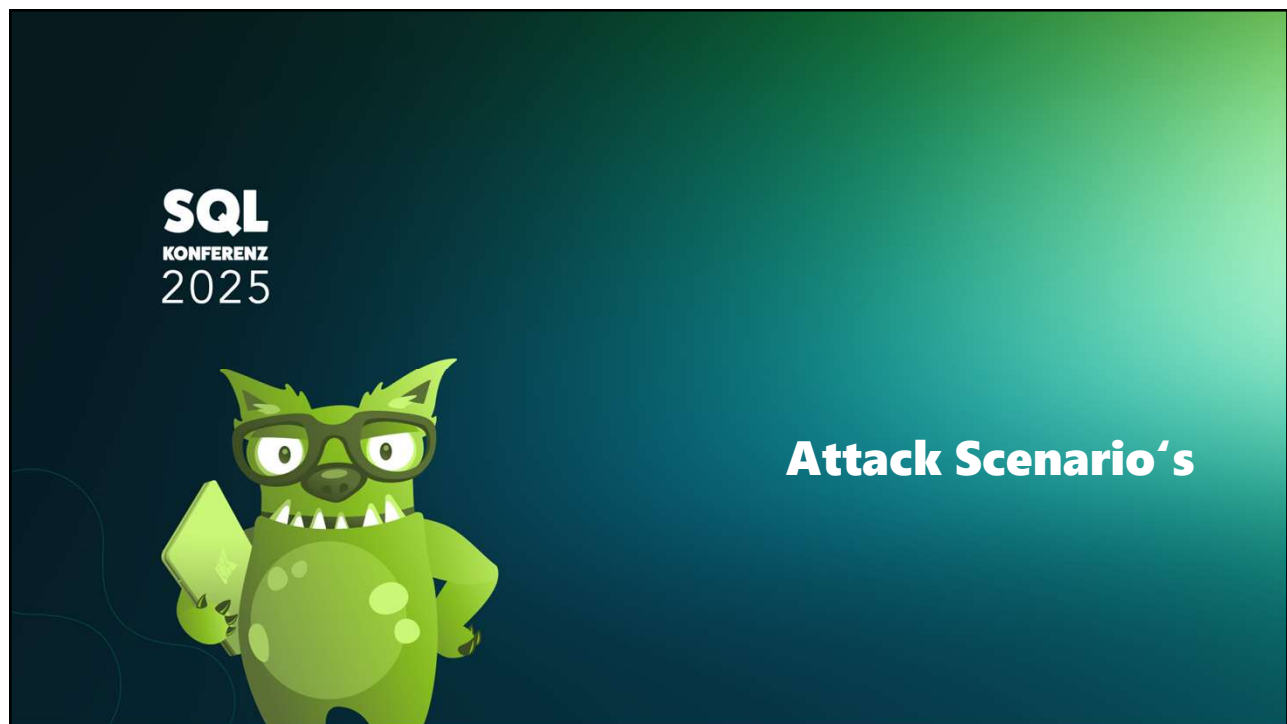


## Troubleshooting Tips

- Verify SPN's
- Verify delegation settings
- Microsoft Kerberos Configuration Manager / SQLCHECK
- Ensure the account can be delegated

<https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/connect/resolve-connectivity-errors-checklist>



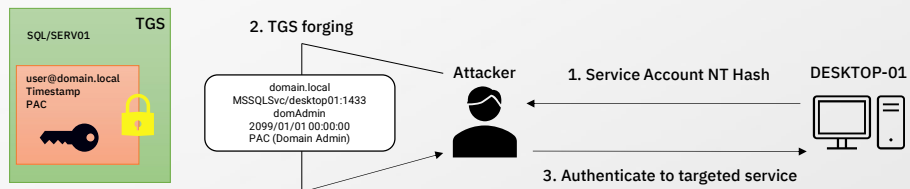


## Attack Scenario's

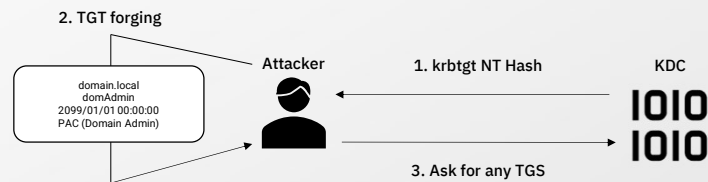
- Pass the Hash
- Pass the Ticket
- Kerberoasting
- Silver / Golden Tickets



## Silver Ticket



## Golden Ticket



## How to protect?

- Encryption ciphers (only AES128/128/future ciphers)
- Honey pots (weak account security)
- Credential Guard





## Lesson's Learned

- Kerberos phases
- Service Principal Names
- Delegation
- How to set up SQL Server & Reporting Services
- Troubleshooting tips
- Attack scenario's

