Kerberos for BI

Régis Baccaro

@regbac

GOLD SPONSORS

Atos
Profisee®
Zerto

SILVER SPONSORS

PROMISE GRUPA APN PROMISE
ELITMIND
ITMAGINATION Imagine it. Done.
THEOBALD SOFTWARE

BRONZE SPONSORS

it KONTRAKT®
JCommerce
IT Krajowy Rejestr Długów
KSIĄŻKI IT Z CAŁEGO ŚWIATA NOVATECH www.novatech.com.pl
PEPCO
dbWatch DATABASE CONTROL
querona
Data Scientist as a Service
UBS
VOLVO Volvo Group IT

STRATEGIC PARTNER

Microsoft

About.me : Regis Baccaro

Consultant

Developer

Speaker

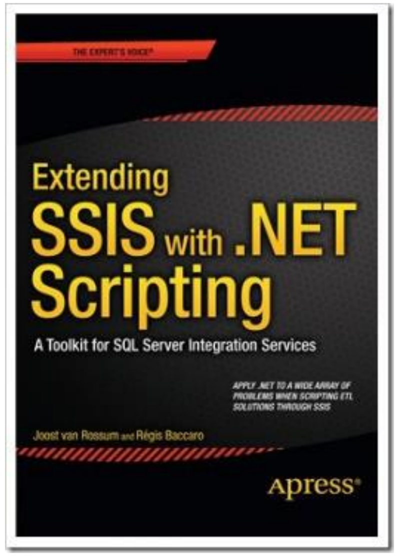
Author

Data Platform MVP

Farmer

Gin afficionado

SQL Nexus lead



THE EXPERT'S VOICE®

Extending SSIS with .NET Scripting

A Toolkit for SQL Server Integration Services

APPLY .NET TO A WIDE ARRAY OF PROBLEMS WHEN SCRIPTING ETL SOLUTIONS THROUGH SSIS

Joost van Rossum and Régis Baccaro

Apress®

Agenda

What is it?

How does it work?

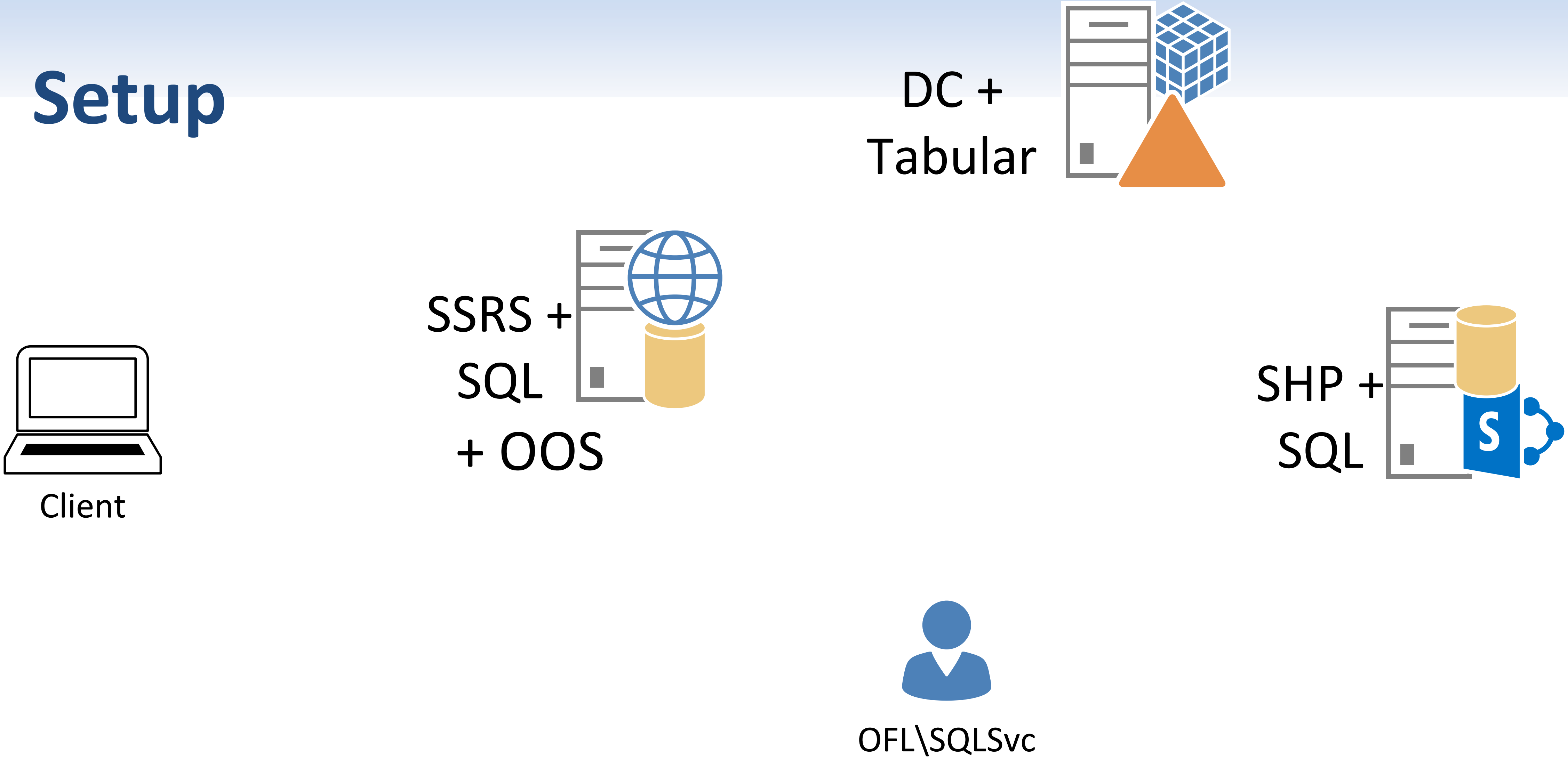
Who can configure it?

Why so many issues?

SSRS, SSAS and SQL

Troubleshooting Tools

Setup



DC + Tabular

SSRS + SQL + OOS

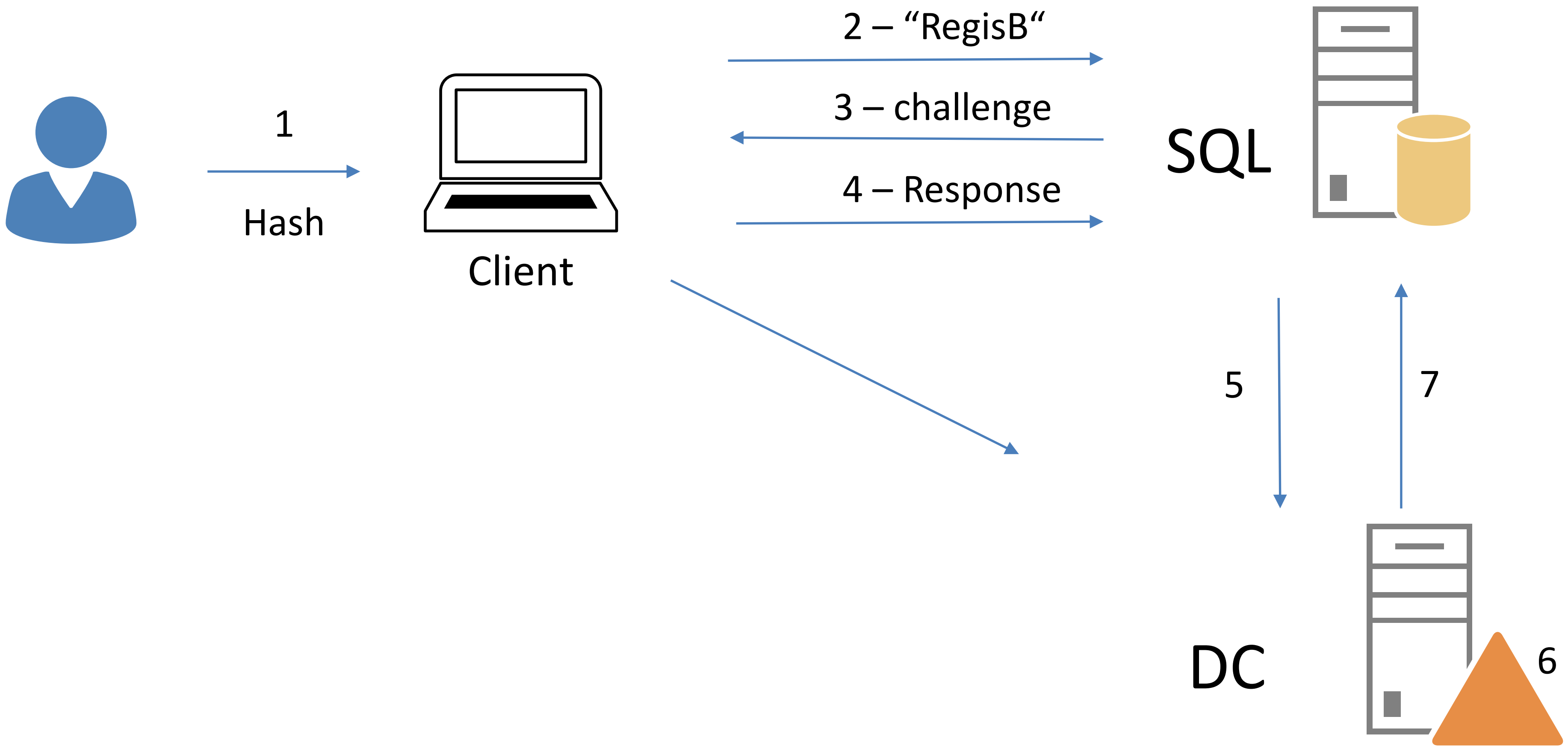
Client

SHP + SQL

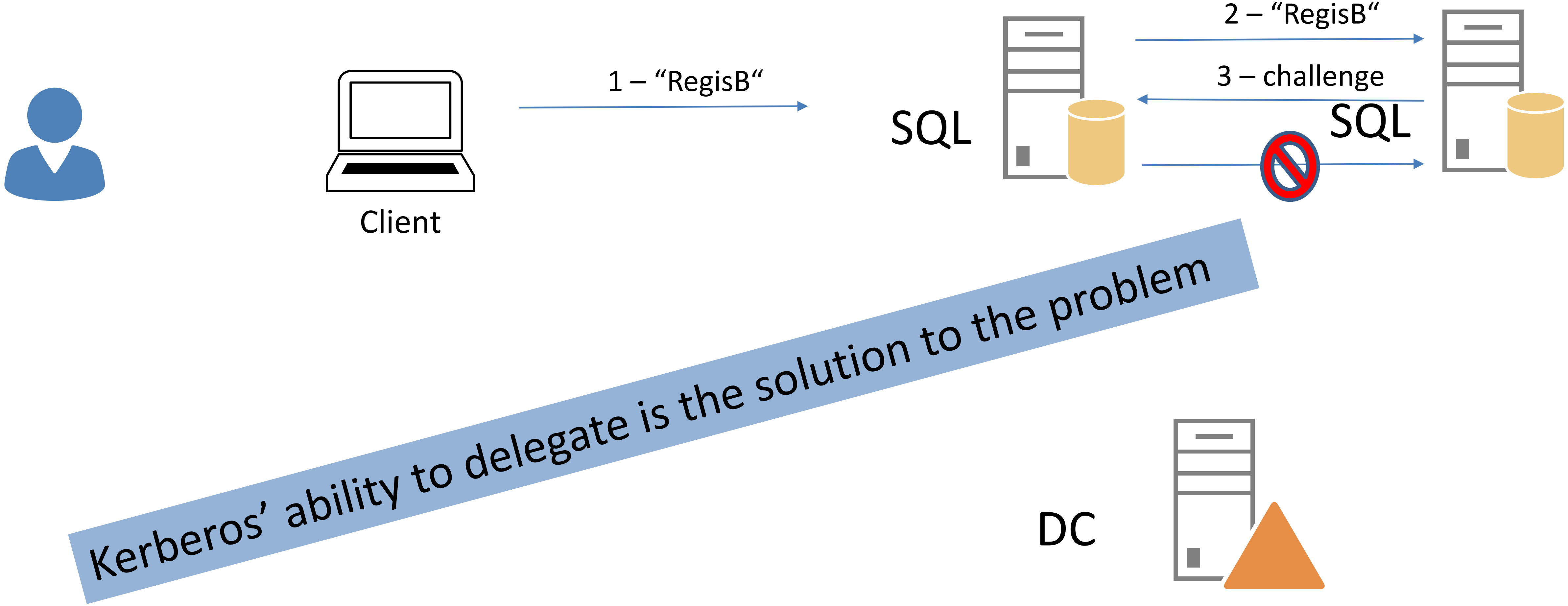
OFL\SQLSvc

DEMO 1

NTLM authentication – how it works



NTLM authentication – Why it fails



Kerberos' ability to delegate is the solution to the problem

What is Kerberos

Default AD authentication protocol

Created by MIT

RFC1510

Available in Windows since 2000

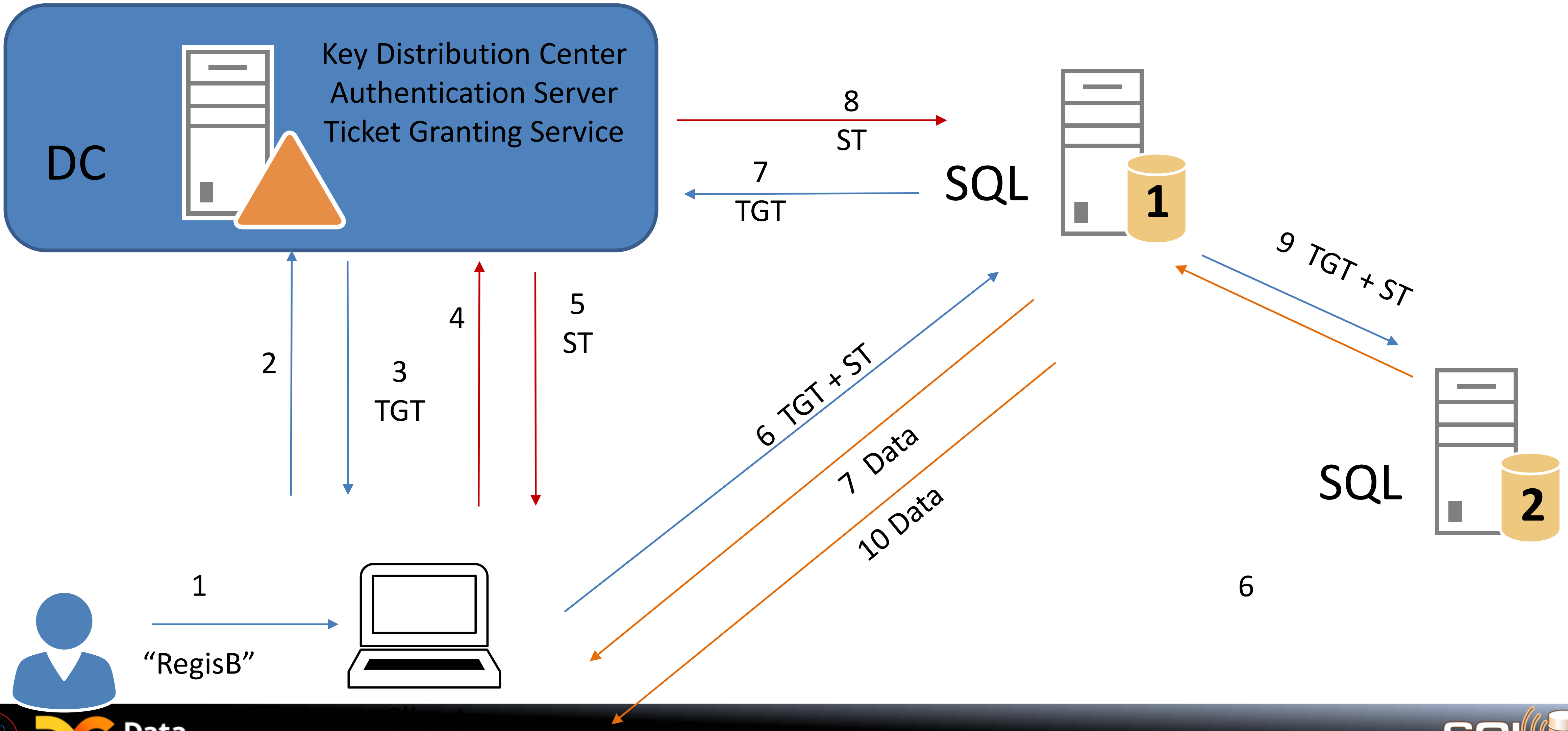
Revert to NTLM

Uses Cryptographic tickets

http://web.mit.edu/kerberos

TGT Ticket Granting Ticket
ST Service Ticket

Kerberos - how it works



DC

Key Distribution Center
Authentication Server
Ticket Granting Service

8
ST

7
TGT

SQL

1

9 TGT + ST

2

3
TGT

4

5
ST

6 TGT + ST

7 Data

10 Data

SQL

2

6

1

"RegisB"

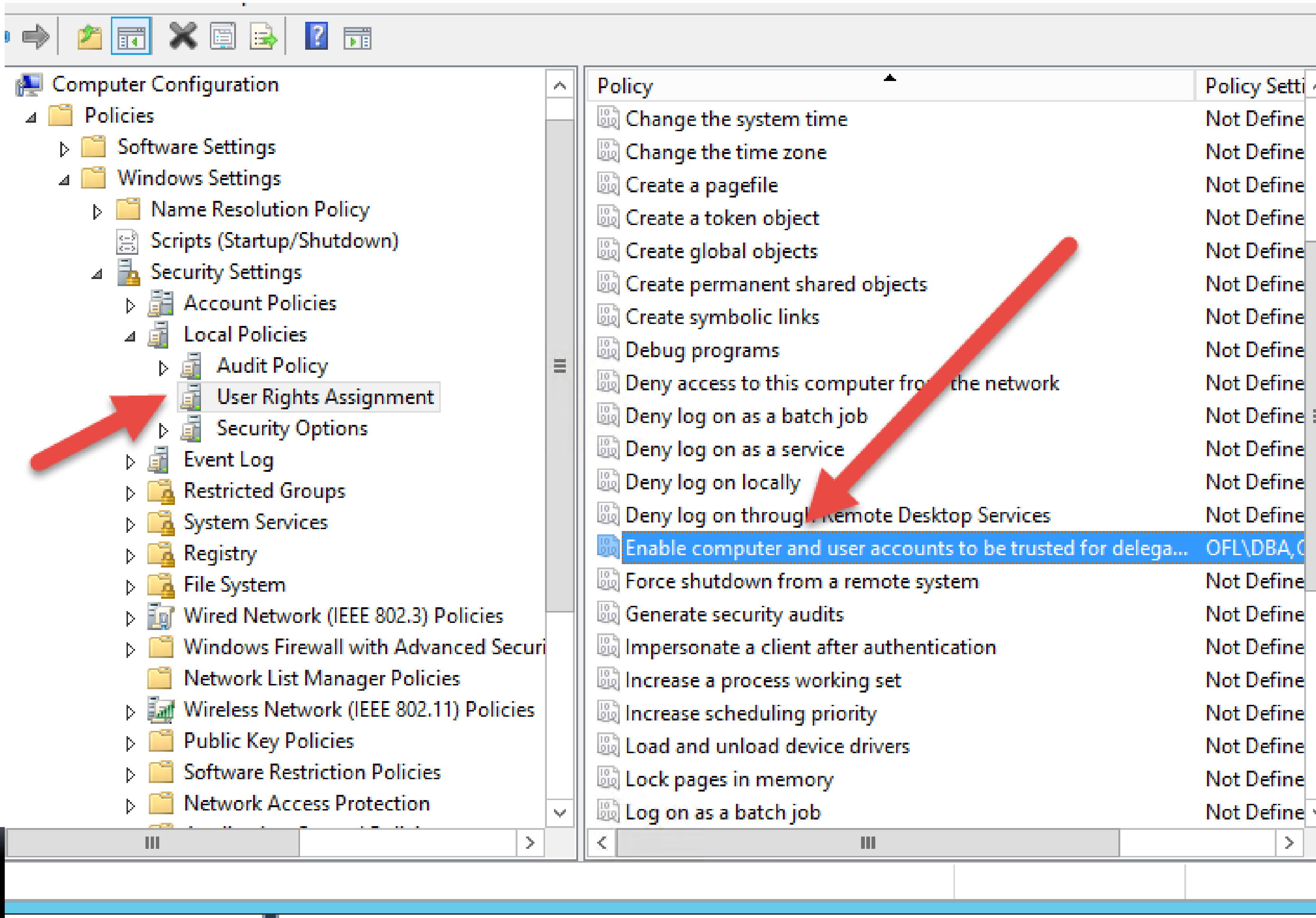
Client

Who can configure it?

Done by Windows Admin – not DBAs

Or use Group Policy and a OU

Usually Windows Admin don’t know how to do the work, so you’ll be telling hem



- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Firewall with Advanced Securi
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policies
        - Public Key Policies
        - Software Restriction Policies
        - Network Access Protection

Policy	Policy Setti
Change the system time	Not Define
Change the time zone	Not Define
Create a pagefile	Not Define
Create a token object	Not Define
Create global objects	Not Define
Create permanent shared objects	Not Define
Create symbolic links	Not Define
Debug programs	Not Define
Deny access to this computer from the network	Not Define
Deny log on as a batch job	Not Define
Deny log on as a service	Not Define
Deny log on locally	Not Define
Deny log on through Remote Desktop Services	Not Define
Enable computer and user accounts to be trusted for delega...	OFL\DBA,C
Force shutdown from a remote system	Not Define
Generate security audits	Not Define
Impersonate a client after authentication	Not Define
Increase a process working set	Not Define
Increase scheduling priority	Not Define
Load and unload device drivers	Not Define
Lock pages in memory	Not Define
Log on as a batch job	Not Define

Configuring Kerberos for SQL

SetSPN.exe

```
SetSPN -L <object>
SetSPN -S <ServiceClass>/<HostName> <domain>\<AccountName>
SetSPN -S <ServiceClass>/<HostName>:<portnumber> <domain>\<AccountName>
SetSPN -S <ServiceClass>/<HostName>:<instance> <domain>\<AccountName>
SetSPN -S <ServiceClass>/<HostName> <domain>\<host>$
```

DEMO 2

Configuring Kerberos for SSRS Native step by step

Gather information

SPNs

Allow delegation

SSRS Configuration

Restart Server

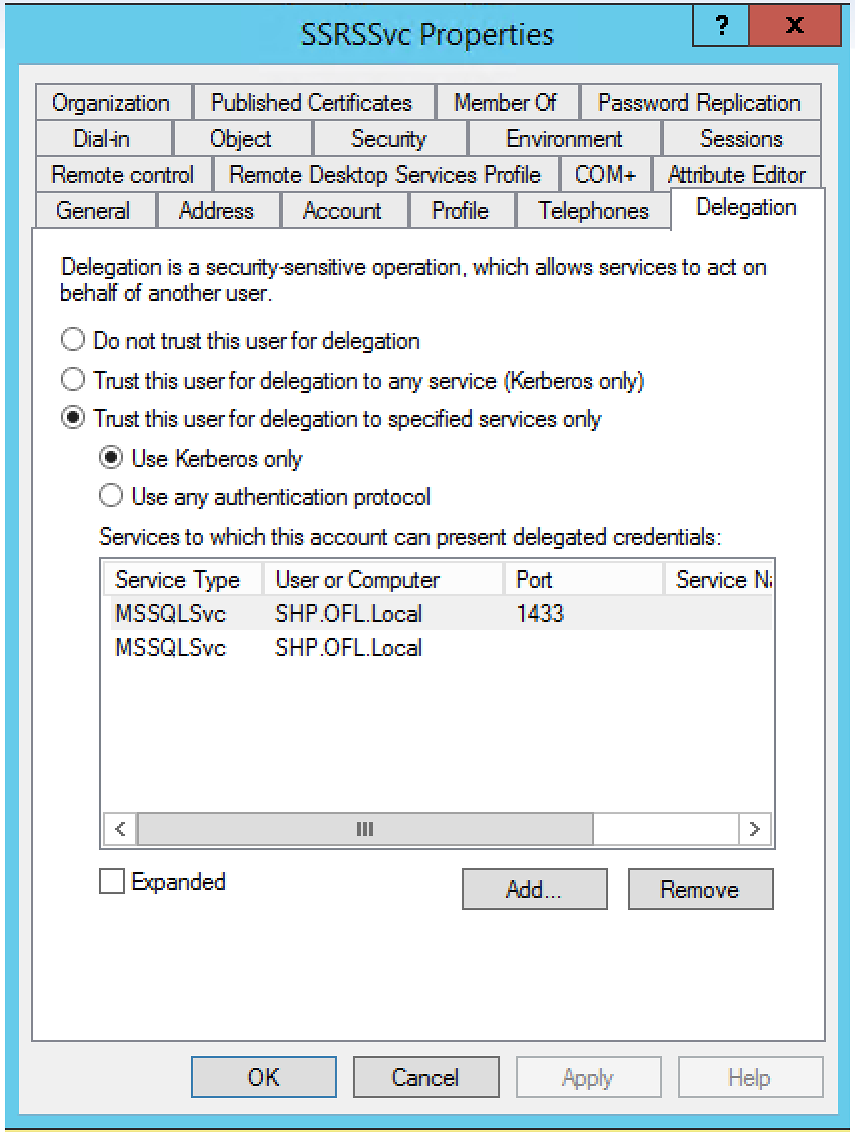
Test

SSRS front-end is on SQL1

Databases are on SHP

SSRS User = OFL\SSRSSvc

DEMO 3



SSRSSvc Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N:
MSSQLSvc	SHP.OFL.Local	1433	
MSSQLSvc	SHP.OFL.Local		

□ Expanded

Configuring Kerberos for SSRS Integrated step by step

Gather information

Set up Claim account (Act as Part of the OS, Impersonate a client, Log on as a Service)

Add Claim account to local admin

Make changes to Windows Identity Foundation config file

Grant access to Process Identity

Make sure the C2WTS service is started

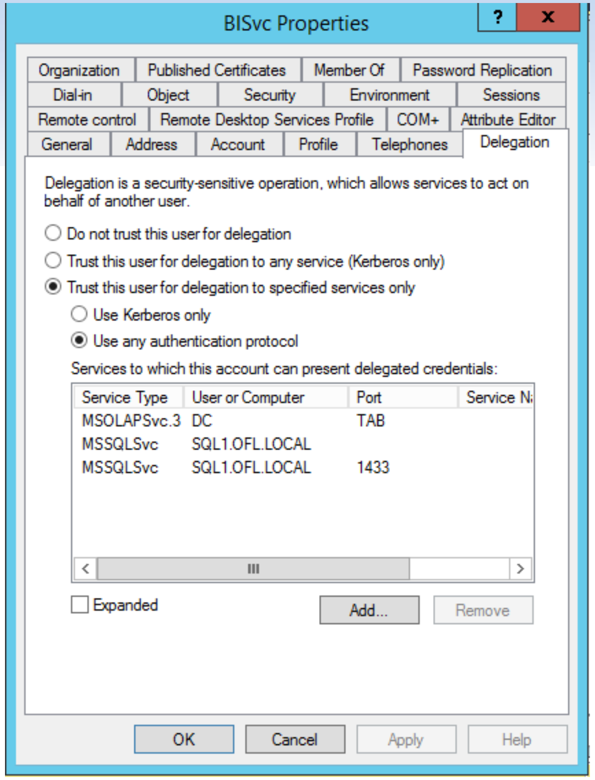
SPNs (don’t need SPN setup but needed for the tab)

Configure delegation

SSRS Configuration

Test

SharePoint farm account never gets a Claims token !!!


BISvc Properties
Organization | Published Certificates | Member Of | Password Replication
Dial-in | Object | Security | Environment | Sessions
Remote control | Remote Desktop Services Profile | COM+ | Attribute Editor
General | Address | Account | Profile | Telephones | Delegation
Add... | Remove
OK | Cancel | Apply | Help

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

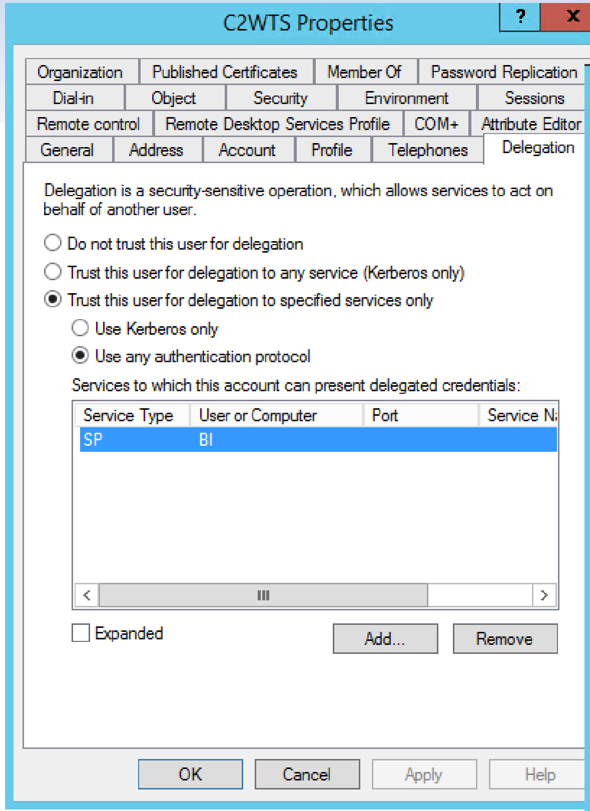
○ Use Kerberos only

● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
MSOLAPSvc.3	DC	TAB	
MSSQLSvc	SQL1.OFL.LOCAL		
MSSQLSvc	SQL1.OFL.LOCAL	1433	

□ Expanded


C2WTS Properties
Organization | Published Certificates | Member Of | Password Replication
Dial-in | Object | Security | Environment | Sessions
Remote control | Remote Desktop Services Profile | COM+ | Attribute Editor
General | Address | Account | Profile | Telephones | Delegation
Add... | Remove
OK | Cancel | Apply | Help

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

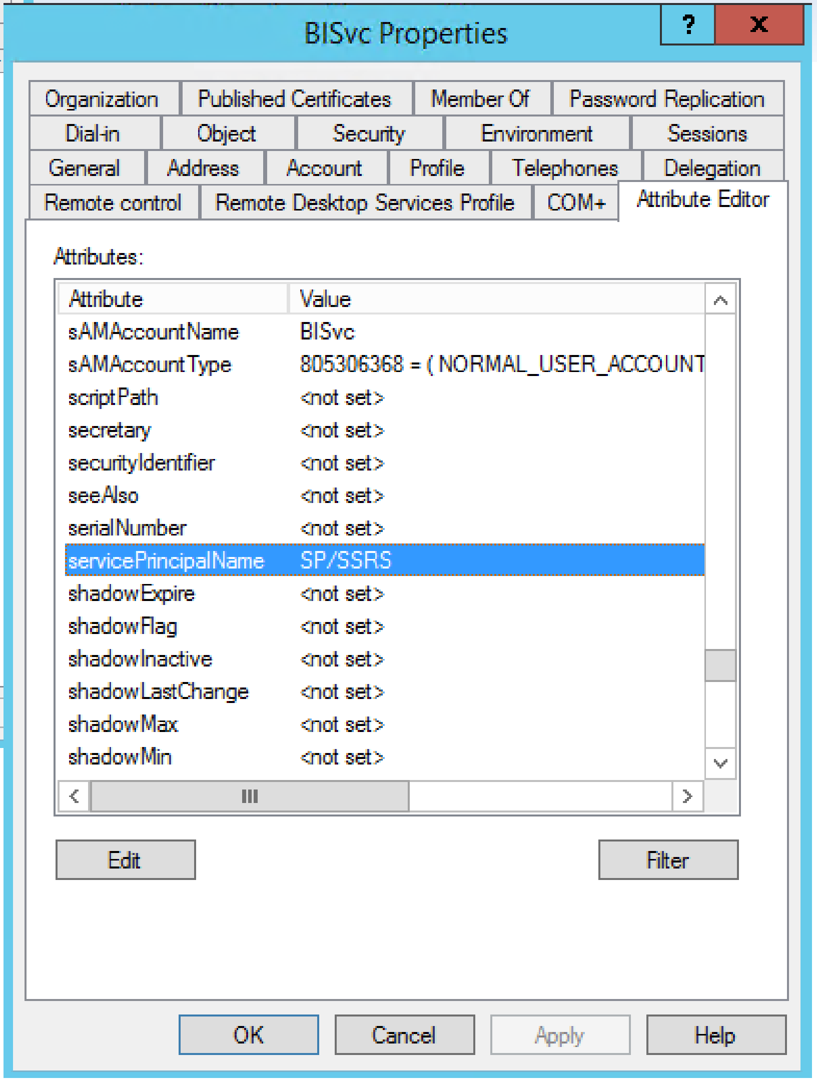
○ Use Kerberos only

● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
SP	BI		

□ Expanded


BISvc Properties
Organization | Published Certificates | Member Of | Password Replication
Dial-in | Object | Security | Environment | Sessions
General | Address | Account | Profile | Telephones | Delegation
Remote control | Remote Desktop Services Profile | COM+ | Attribute Editor
Edit | Filter
OK | Cancel | Apply | Help

Attributes:

Attribute	Value
sAMAccountName	BISvc
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	SP/SSRS
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>
shadowMax	<not set>
shadowMin	<not set>

DEMO 4

Walkthrough demo 4

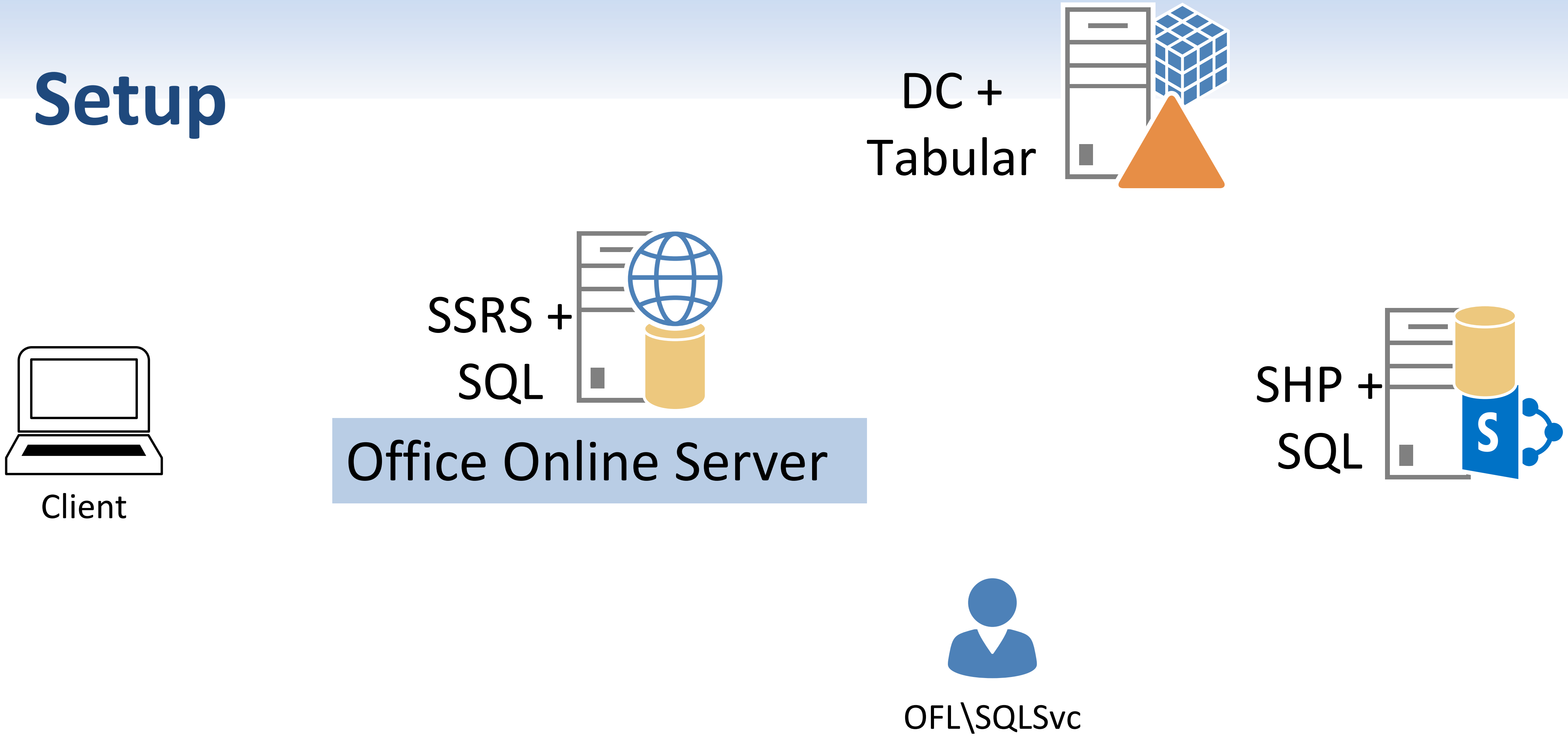
$w = Get-SPWebApplication -Identity http://SHP

$w.GrantAccessToProcessIdentity(“OFL\BISVC”)

Change Report Config : <RSWindowsNegotiate />

Change C2WTS config file : <add value="WSS_WPG" />

Setup



DC + Tabular

SSRS + SQL

Office Online Server

SHP + SQL

Client

OFL\SQLSvc

Configuring Kerberos for SSAS Tabular in SharePoint

New story for Excel Services!!

Setup Office Online Server for working with ShP 2016: https://blogs.msdn.microsoft.com/analysisservices/2015/12/08/white-paper-published-deploying-sql-server-2016-powerpivot-and-power-view-in-sharepoint-2016/

Cheating is OK : `Set-OfficeWebAppsFarm -ExcelUseEffectiveUserName:$true`

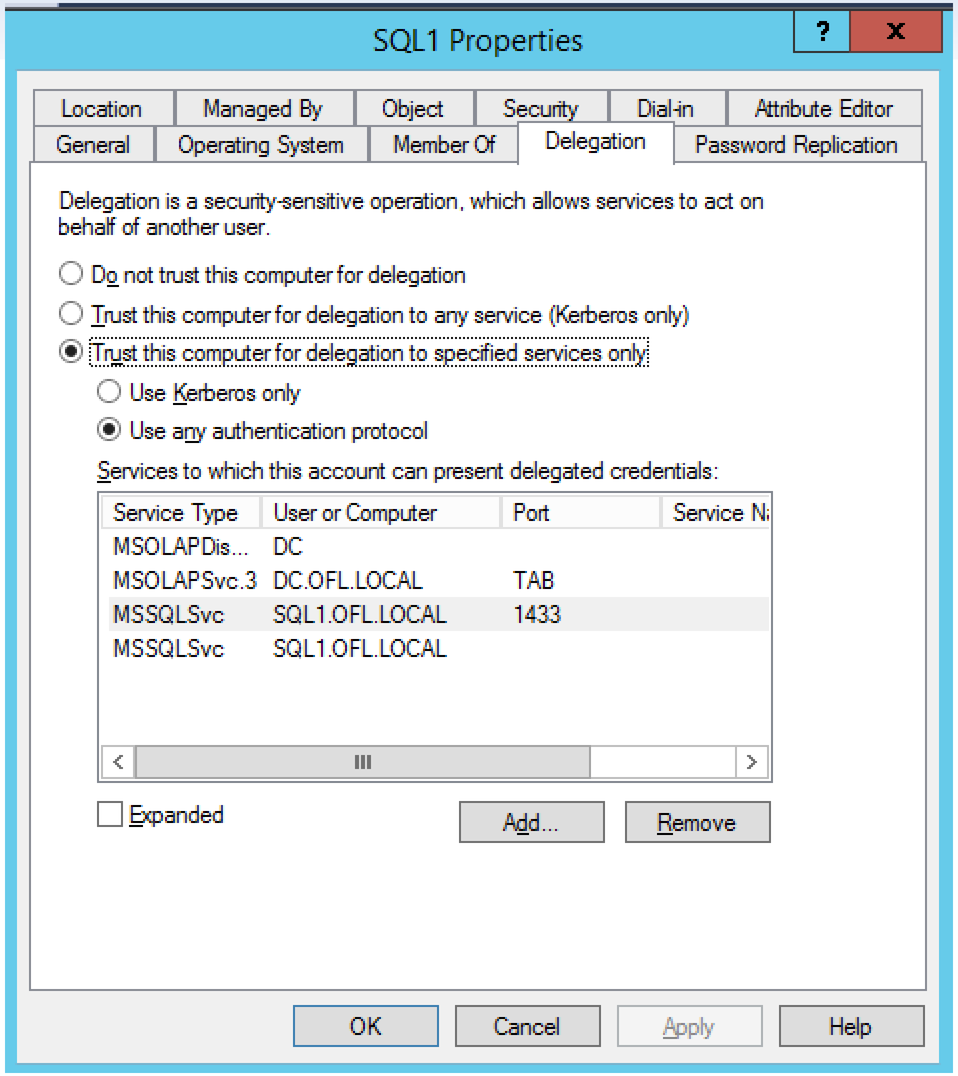
Configure C2WTS

Configure delegation

What about the Disco Service ?

Test it!!

DEMO 5



SQL1 Properties

Location | Managed By | Object | Security | Dial-in | Attribute Editor
General | Operating System | Member Of | Delegation | Password Replication

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

○ Use Kerberos only

● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
MSOLAPDis...	DC		
MSOLAPSvc.3	DC.OFL.LOCAL	TAB	
MSSQLSvc	SQL1.OFL.LOCAL	1433	
MSSQLSvc	SQL1.OFL.LOCAL		

□ Expanded

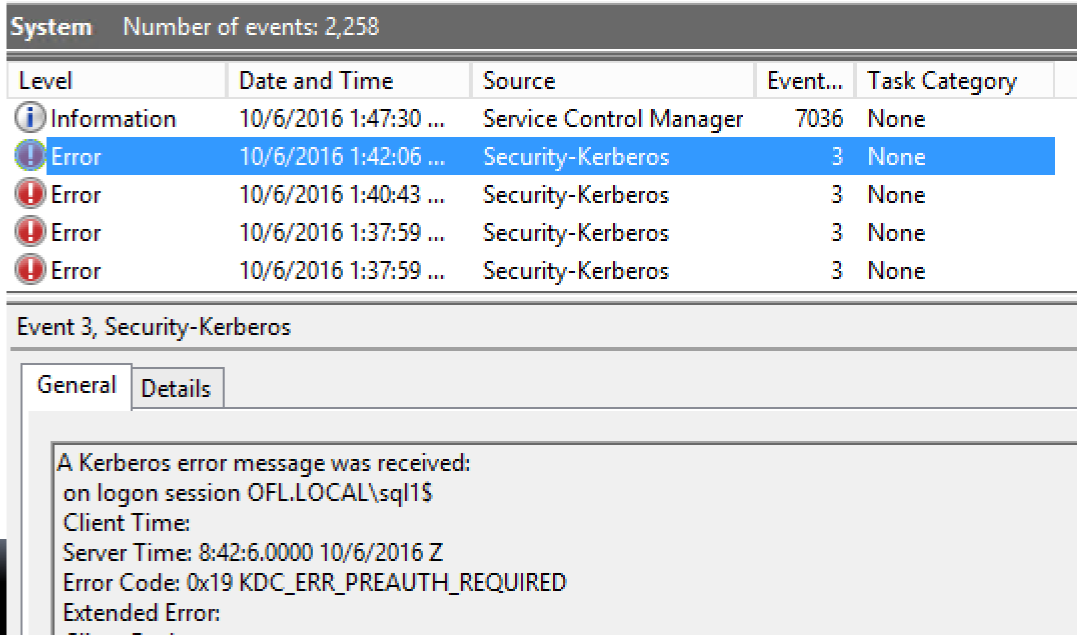
Troubleshooting

Klist

ULSViewer

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
"LogLevel"=dword:00000001
```

Fiddler



System Number of events: 2,258

Level	Date and Time	Source	Event...	Task Category
Information	10/6/2016 1:47:30 ...	Service Control Manager	7036	None
Error	10/6/2016 1:42:06 ...	Security-Kerberos	3	None
Error	10/6/2016 1:40:43 ...	Security-Kerberos	3	None
Error	10/6/2016 1:37:59 ...	Security-Kerberos	3	None
Error	10/6/2016 1:37:59 ...	Security-Kerberos	3	None

Event 3, Security-Kerberos

```
A Kerberos error message was received:
 on logon session OFL.LOCAL\sql1$
 Client Time:
 Server Time: 8:42:6.0000 10/6/2016 Z
 Error Code: 0x19 KDC_ERR_PREAUTH_REQUIRED
 Extended Error:
```

Conclusion

Kerberos is better than NTLM

Gather info and script

Turn the beast into a poodle

Questions?

Contact me : regis@Baccaro.com

Twitter : @regbac

GOLD SPONSORS

Atos
Profisee®
Zerto

SILVER SPONSORS

PROMISE GRUPA APN PROMISE
ELITMIND
ITMAGINATION Imagine it. Done.
THEOBALD SOFTWARE

BRONZE SPONSORS

it KONTRAKT®
JCommerce
KRD Krajowy Rejestr Długów
KSIĄŻKI IT Z CAŁEGO ŚWIATA NOVATECH www.novatech.com.pl
PEPCO
dbWatch DATABASE CONTROL
querona
Data Scientist as a Service
UBS
VOLVO Volvo Group IT

STRATEGIC PARTNER

Microsoft