Kerberos for BI

Régis Baccaro

@regbac

About.me : Regis Baccaro

@regbac

http://theblobfarm.wordpress.com

Data Platform MVP

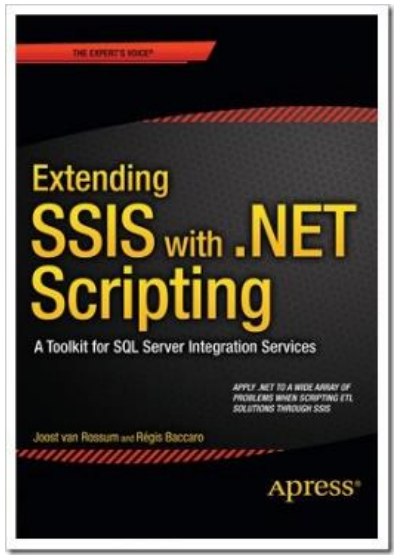
APS (PDW), BIML, SSIS, BI development

Performance tuning

Farmer

Gin aficionado

SQL Nexus lead



Agenda

What is it?

How does it work?

Who can configure it?

Why so many issues?

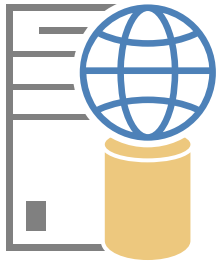
Power BI, SSRS, SSAS and SQL

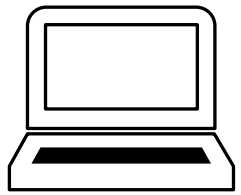
Troubleshooting Tools

Setup

DC +
Tabular

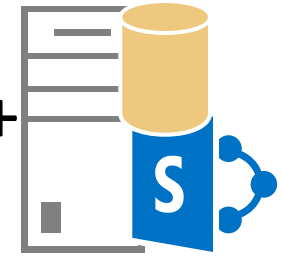
SSRS +
SQL
+ OOS





Client

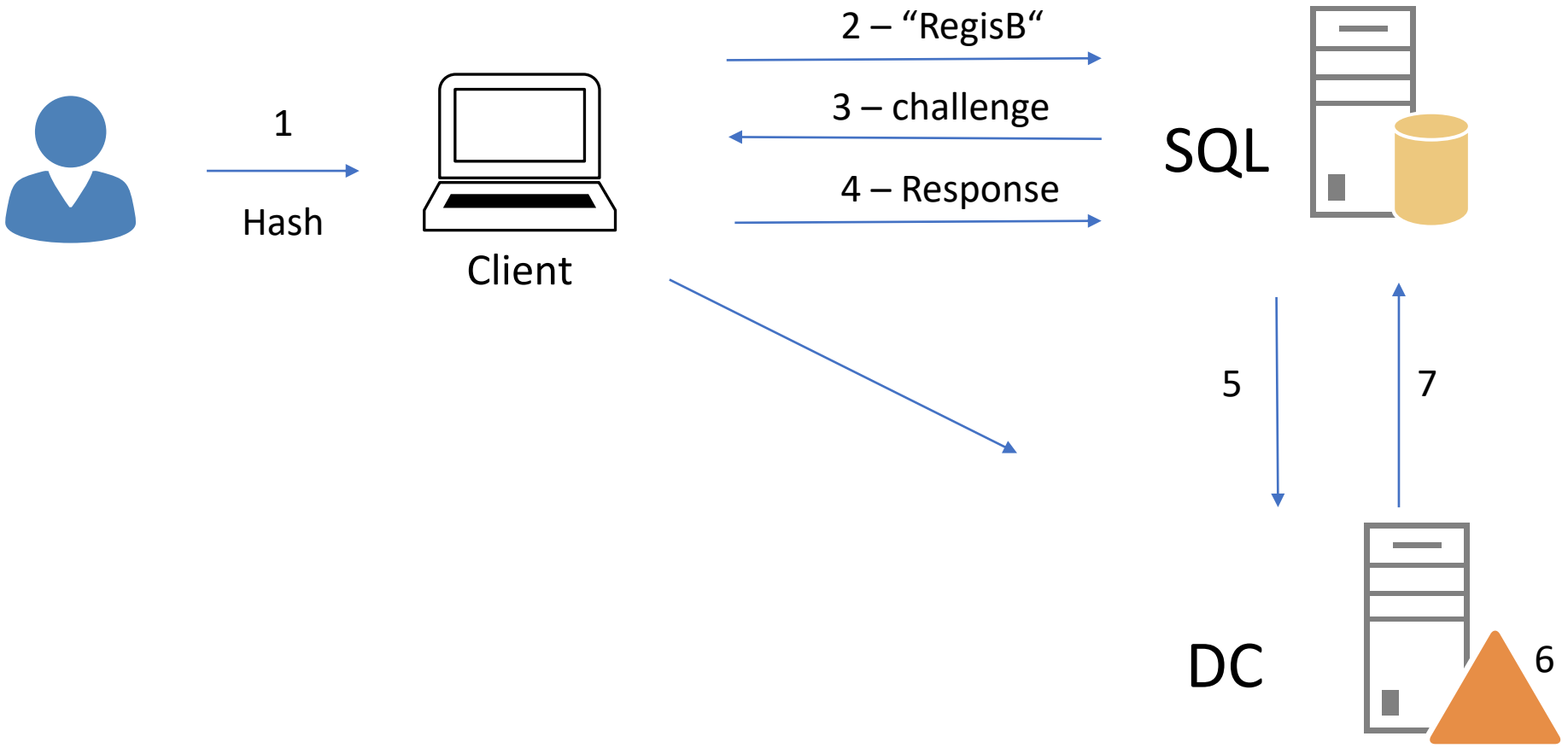
SHP +
SQL



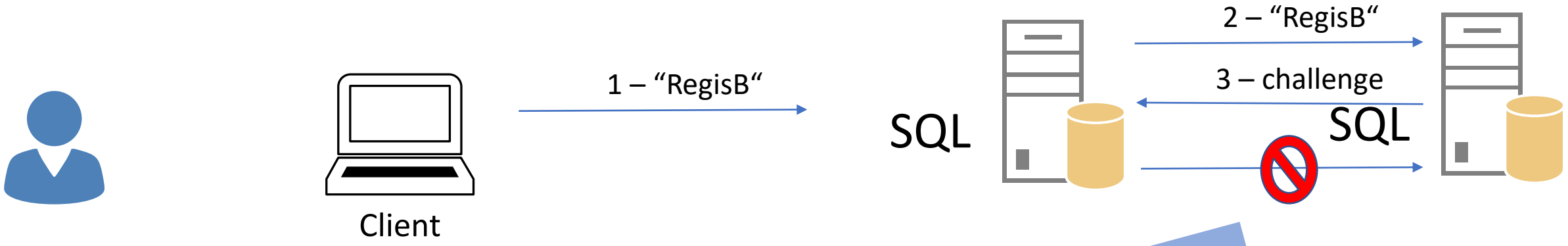
OFL\SQLSvc

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

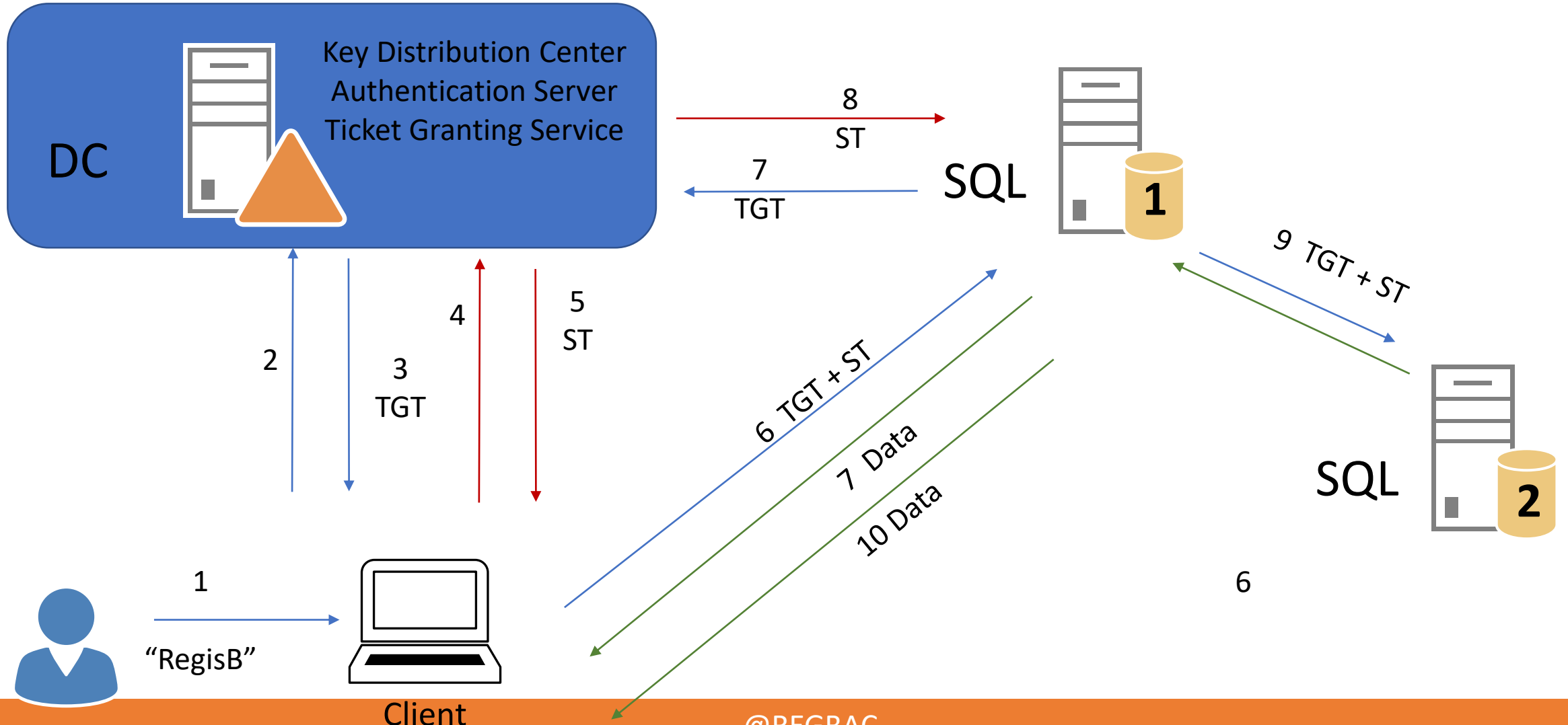
Revert to NTLM

Uses Cryptographic tickets

http://web.mit.edu/kerberos

TGT Ticket Granting Ticket
ST Service Ticket

Kerberos - how it works

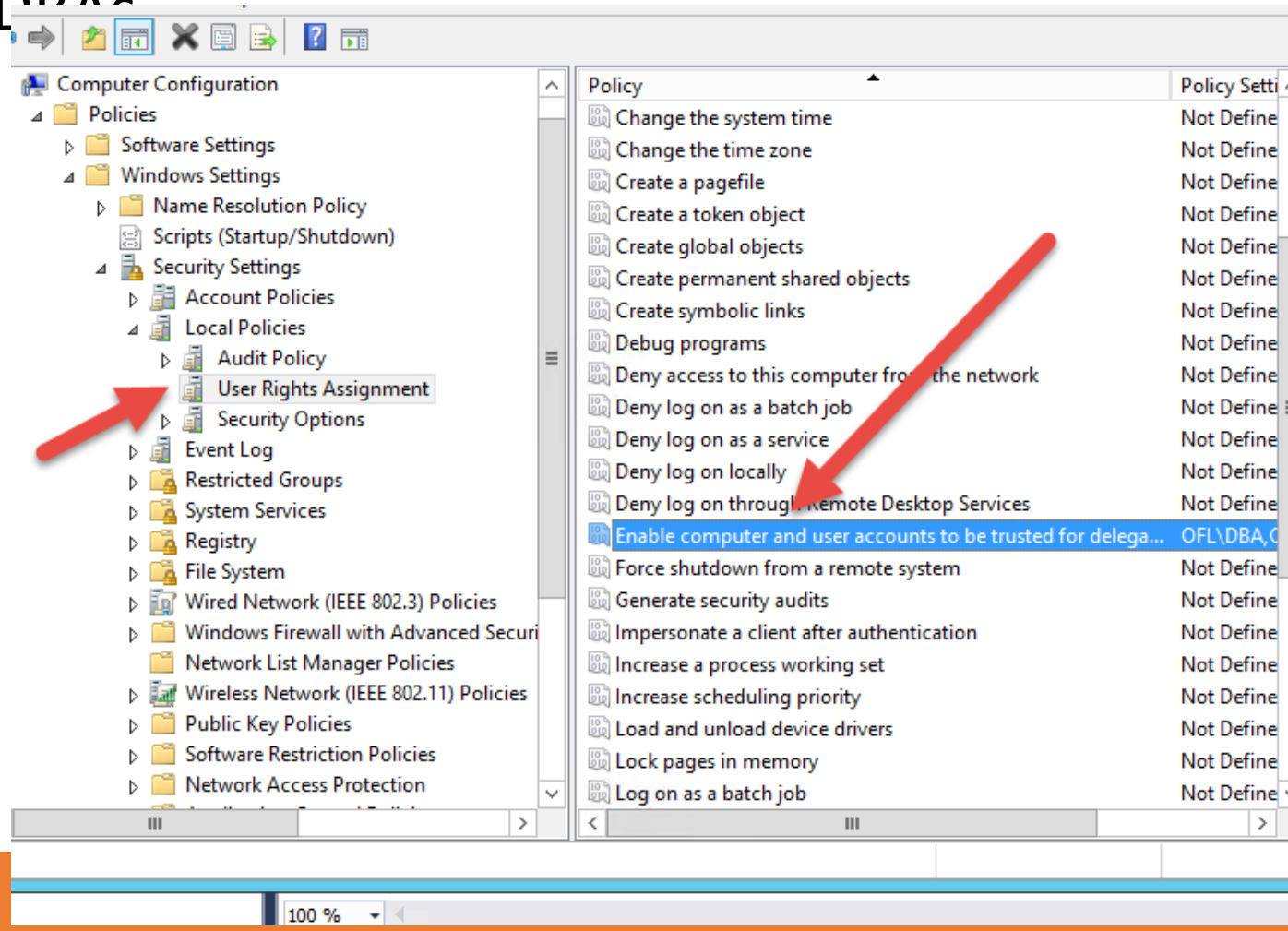


Who can configure it?

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



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 Power BI Report Server step by step

Gather information

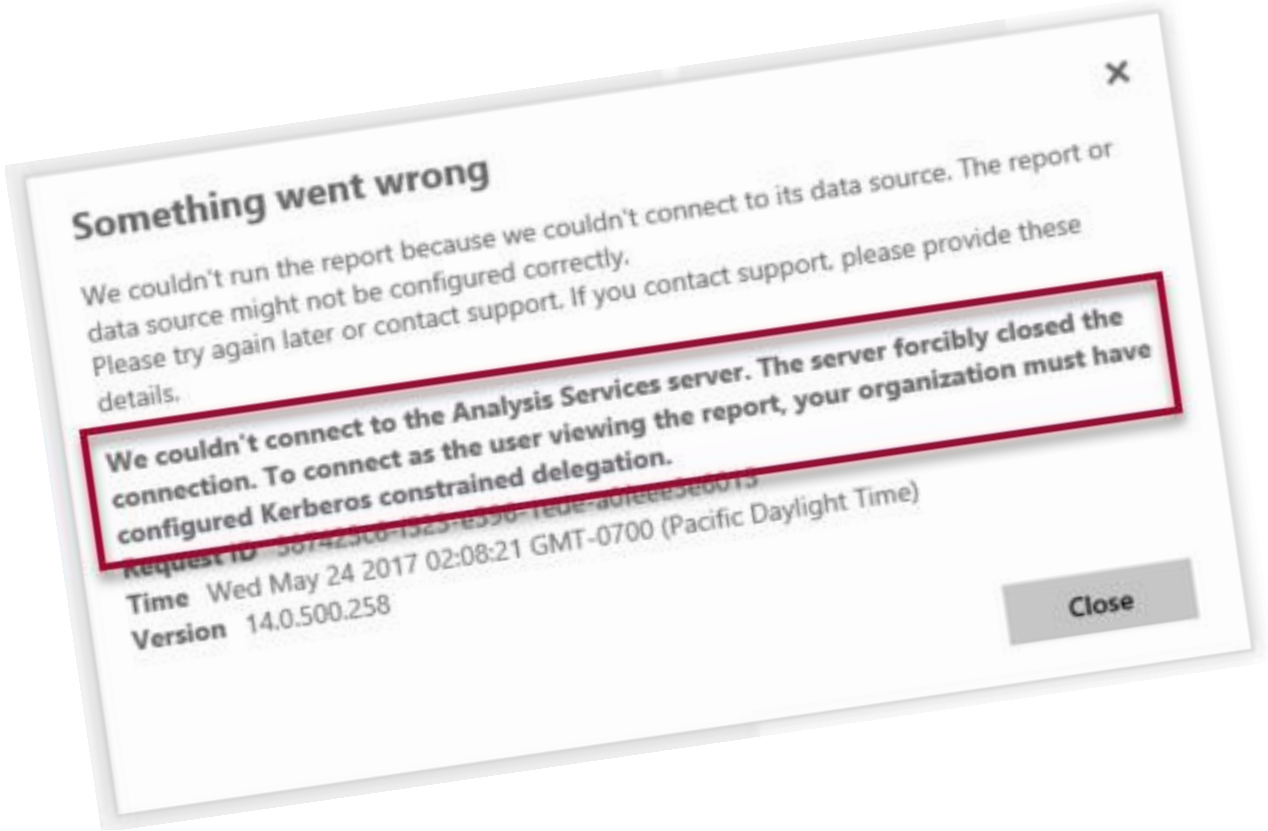
SPNs

Allow delegation

SSRS Configuration

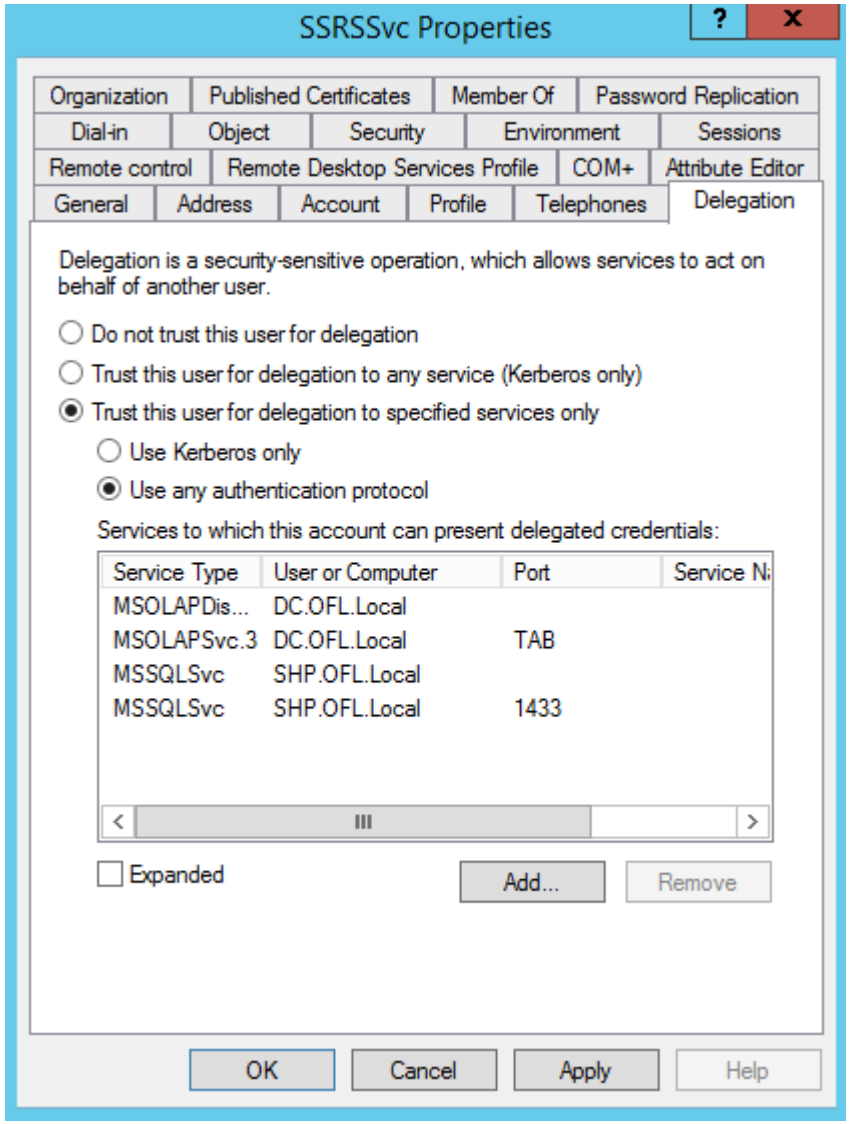
Restart Server

Test



Power BI front-end is on SQL1
Databases are on SHP
SSRS User = OFL\SSRSSvc

Demo 3



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

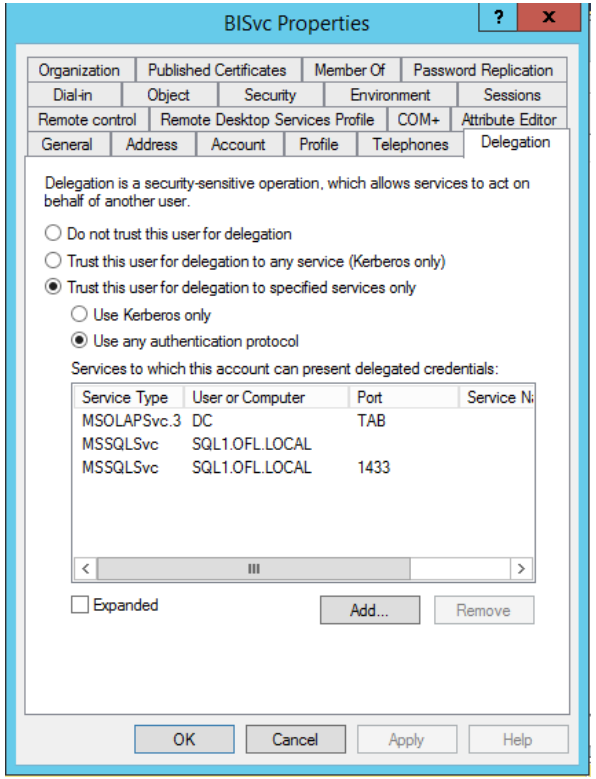
SPNs (don't need SPN setup but needed for the tab)

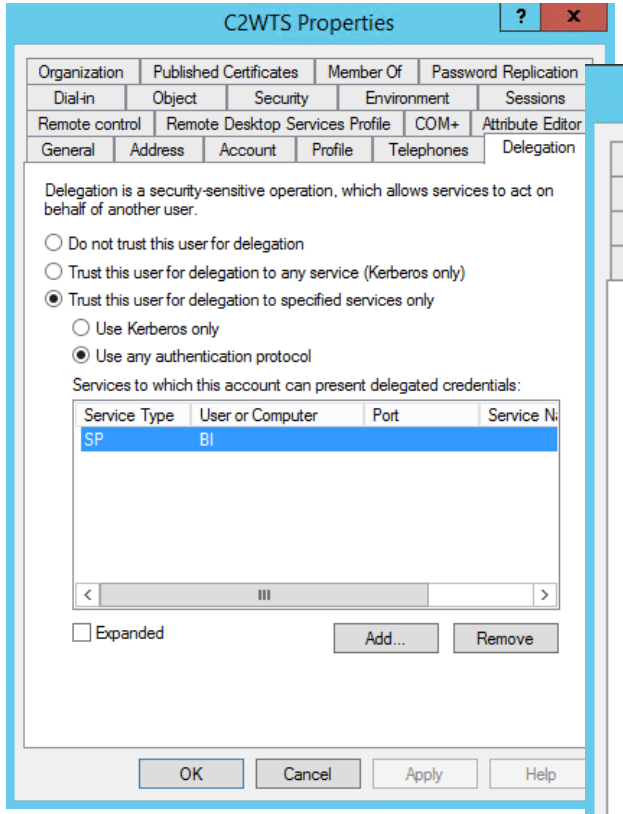
Configure delegation

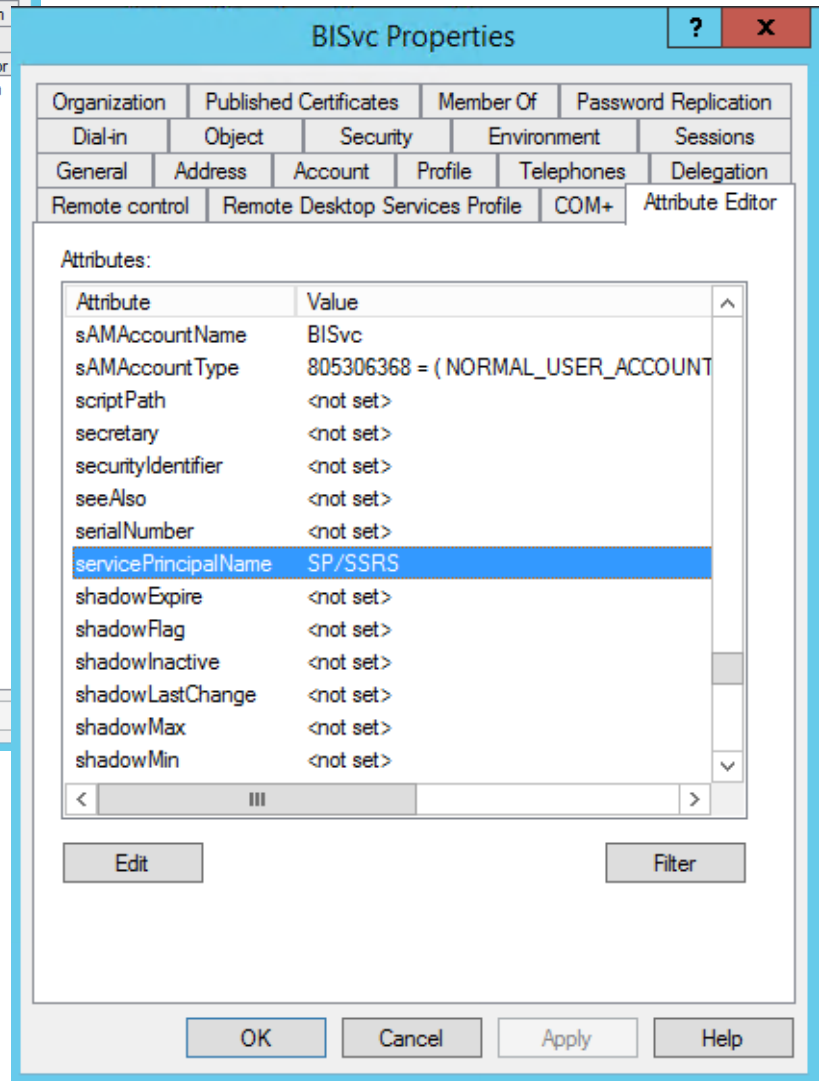
SSRS Configuration

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
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
Add...
Remove
OK
Cancel
Apply
Help


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
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
Add...
Remove
OK
Cancel
Apply
Help


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
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>
Edit
Filter
OK
Cancel
Apply
Help

Demo 4

Walkthrough demo 4

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

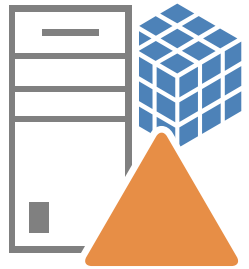
$w.GrantAccessToProcessIdentity(“OFL\BISVC”)

Change Report Config : <RSWindowsNegotiate />

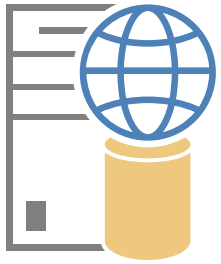
Change C2WTS config file : <add value="WSS_WPG" />

Setup

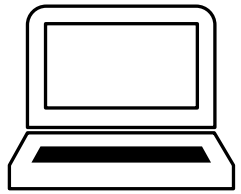
DC +
Tabular



SSRS +
SQL

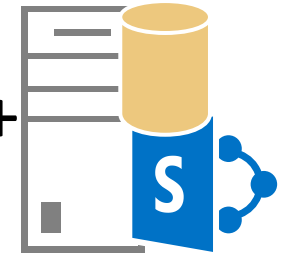


Office Online Server



Client

SHP +
SQL



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`

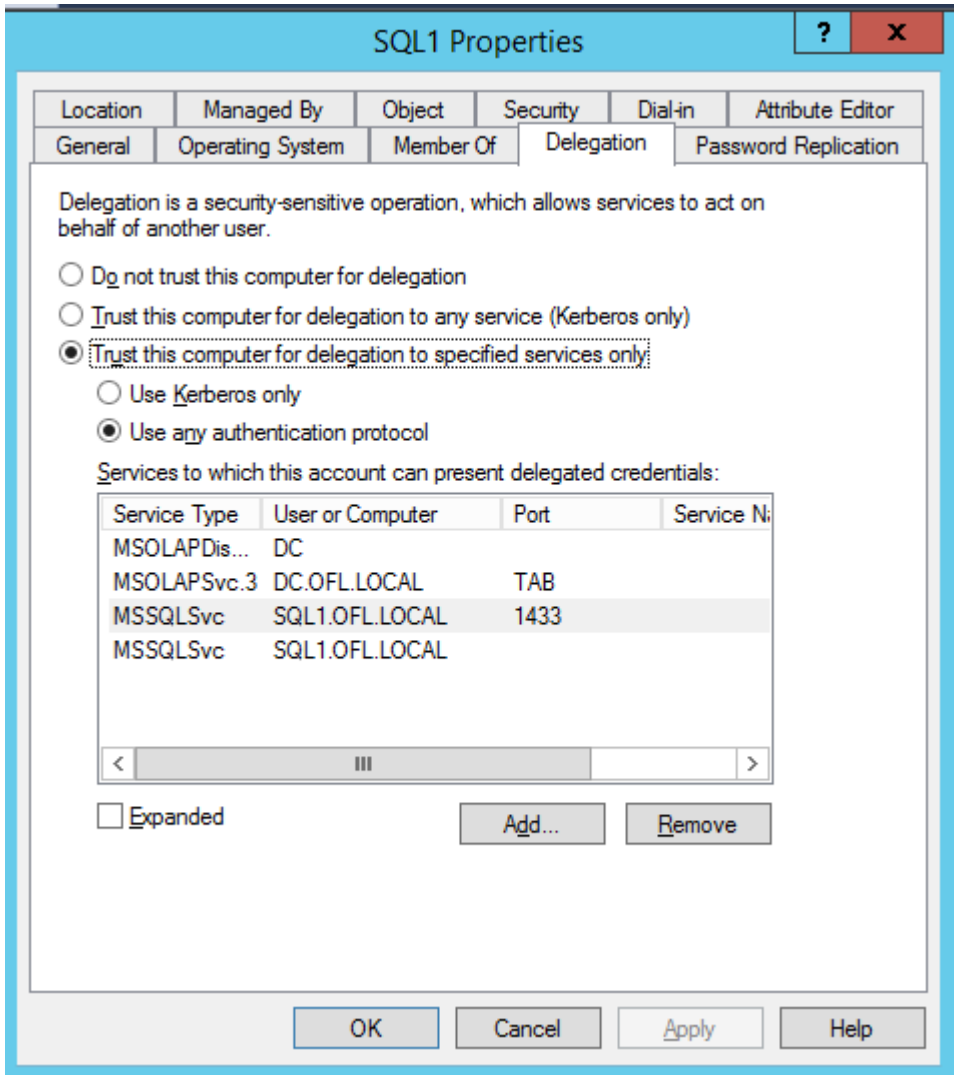
Configure C2WTS

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
Add...
Remove
OK
Cancel
Apply
Help

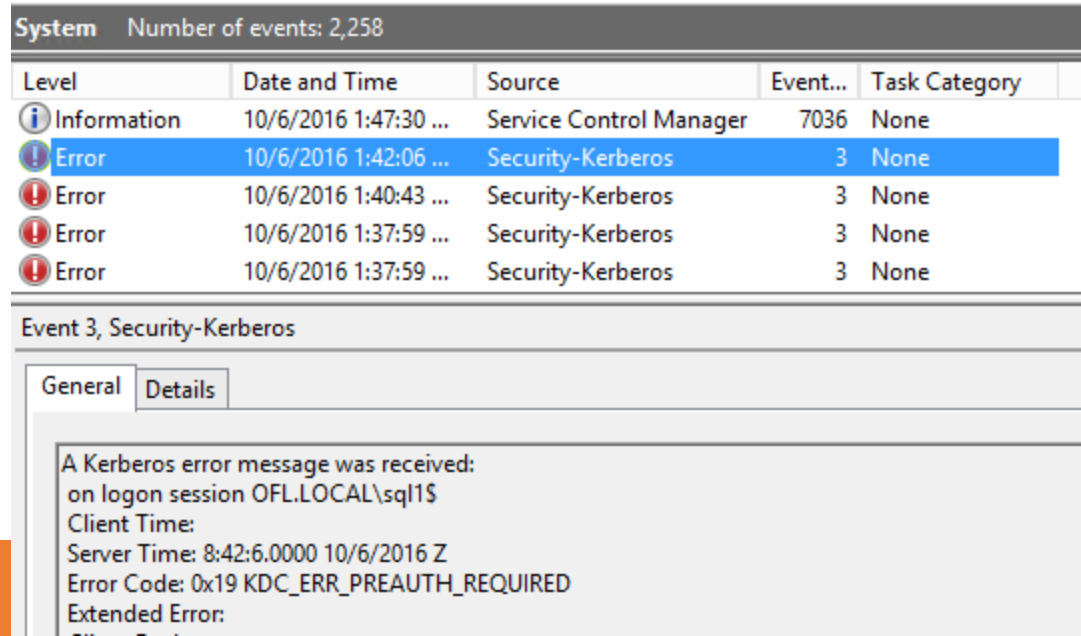
Troubleshooting

Klist

ULSViewer

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

Fiddler



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

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