

Vestas

Wind. It means the world to us.™

Vestas

Wind. It means the world to us.™



Microsoft
CERTIFIED
Solutions Expert
Data Management and
Analytics

Charter Member
Microsoft Professional Program
Data Science Certificate



AARHUS
UNIVERSITY



Bjørn Dörr Jensen - Decision Intelligence Specialist,
contributed in developing a system that turns raw
data into recommended actions to improve turbine
availability.

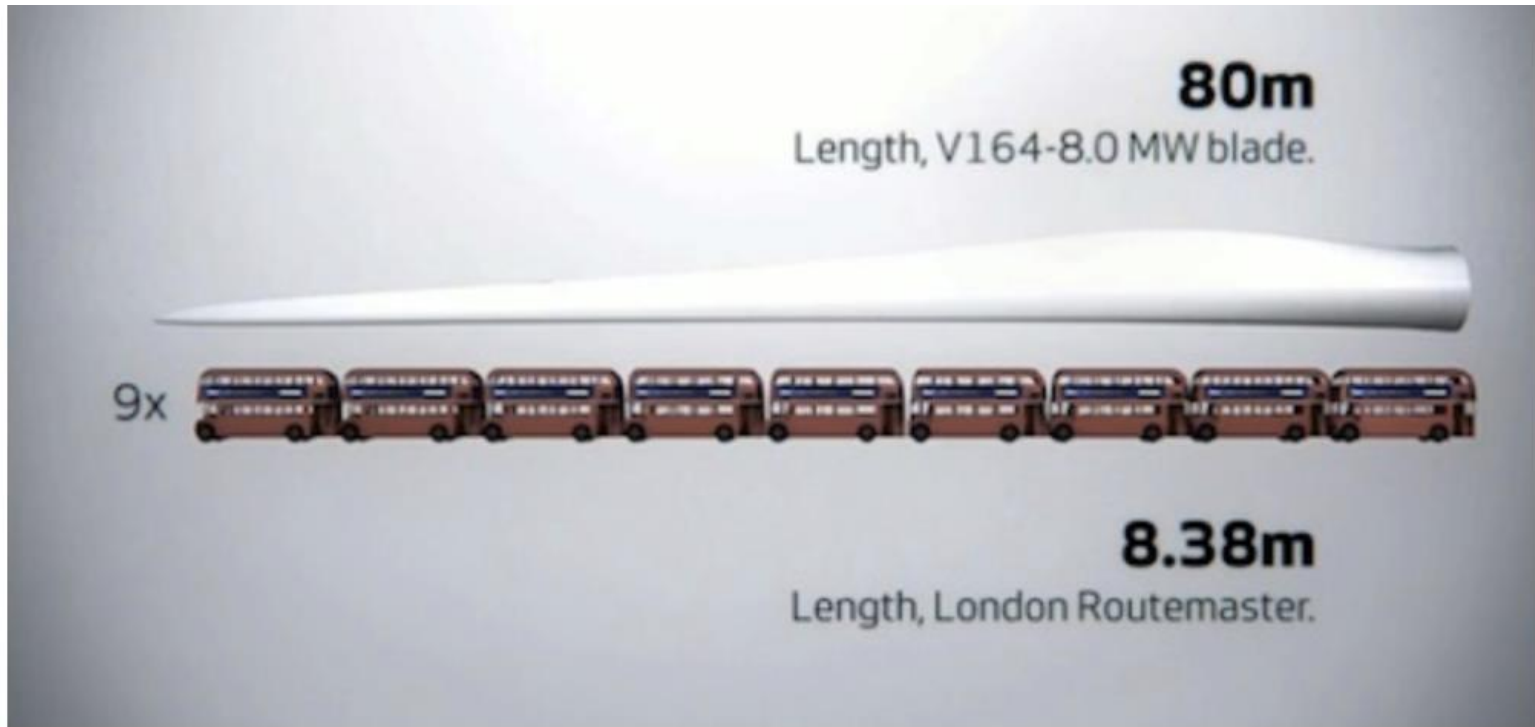


Just like Jimi Hendrix ...



We love to get feedback

Please complete the session feedback
forms



This new turbine is being built to be able to harness the wind and withstand conditions in the wild North Sea, and it will be capable of generating an unprecedented 8 megawatts of power. That's enough to power about 2000 homes from just one wind turbine.

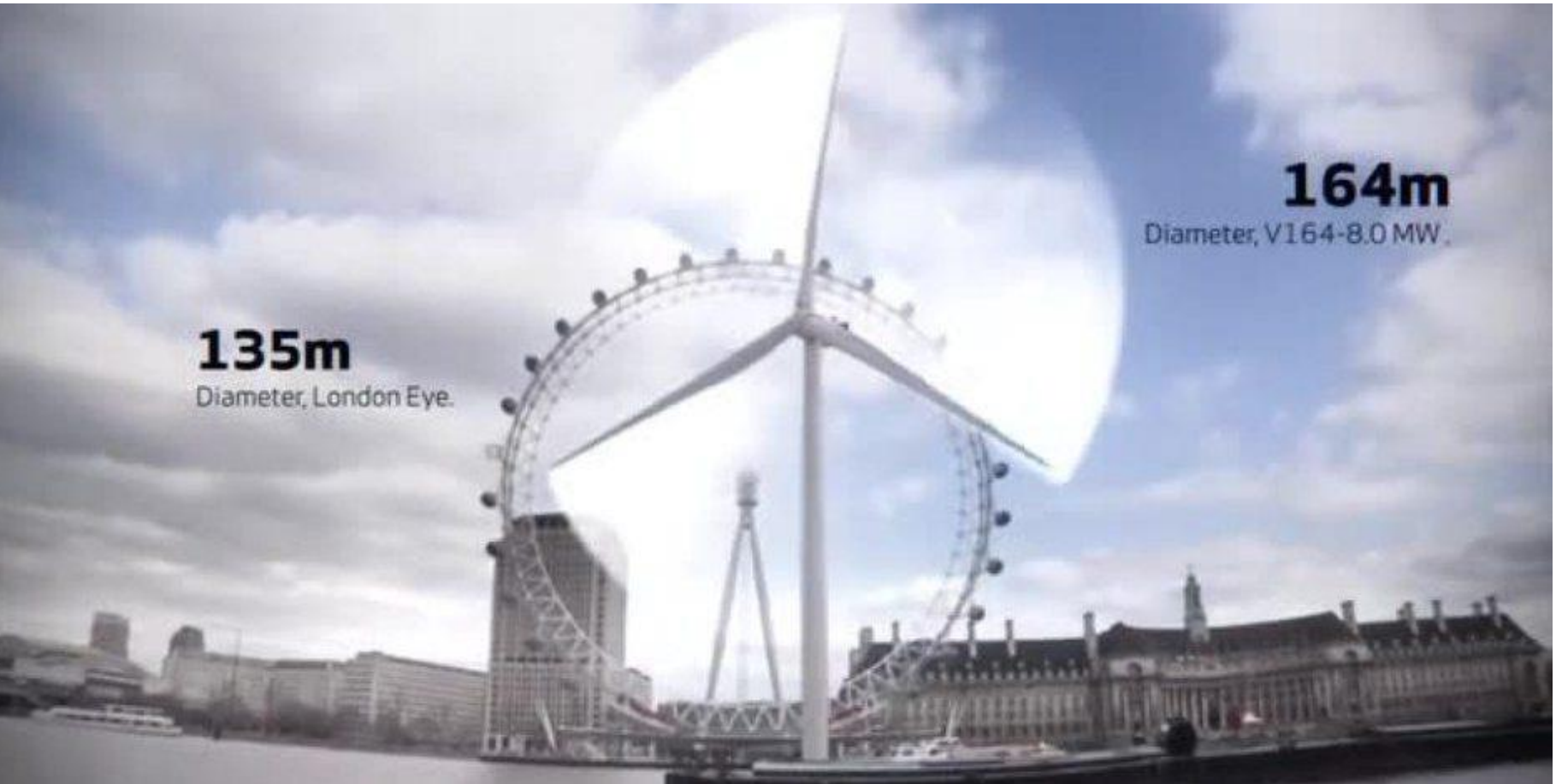


135m

Diameter, London Eye.

164m

Diameter, V164-8.0 MW.



Row Level Security – A real world example

You don't like the idea to change the data model to create kind of virtual private database?

- Why does it matter?
- SQL login vs Integrated security
- How foreign key relationships can be used
- Why to avoid is_member
- How to cache AD-role membership
- How to write tests to check TVF's working correctly
- Role split – “sysadmin” being admin without data access
- Q & A



Promise:

*"At least one of you
will not leave empty-
handed!"*

Row Level Security – A real world example

You don't like the idea to change the data model to create kind of virtual private database?



- Why does it matter?
- SQL login vs Integrated security
- How foreign key relationships can be used
- Why to avoid is_member
- How to cache AD-role membership
- How to write tests to check TVF's working correctly
- Role split – “sysadmin” being admin without data access
- Q & A

Promise:

“At least one of you will not leave empty-handed!”



Cyber attacks cost UK business more than £34bn a year, study shows



Warwick Ashford
Security Editor

14 Jul 2016 12:45



Nearly half of UK firms lack advanced cyber defences, despite the high level of concern about cyber attacks and associated costs

Cyber security incidents cost UK firms £34.1bn in the past year, but under half have enhanced defences, a survey has revealed.

Managing malware alone cost £7.5bn, while data theft incidents cost £6.2bn, compared with the estimated financial impact of burglary over the same period of £5.8bn, according to the study commissioned by business [internet service provider](#) (ISP) [Beaming](#).



THIS ARTICLE COVERS

Cybercrime ▶

RELATED TOPICS

Antivirus

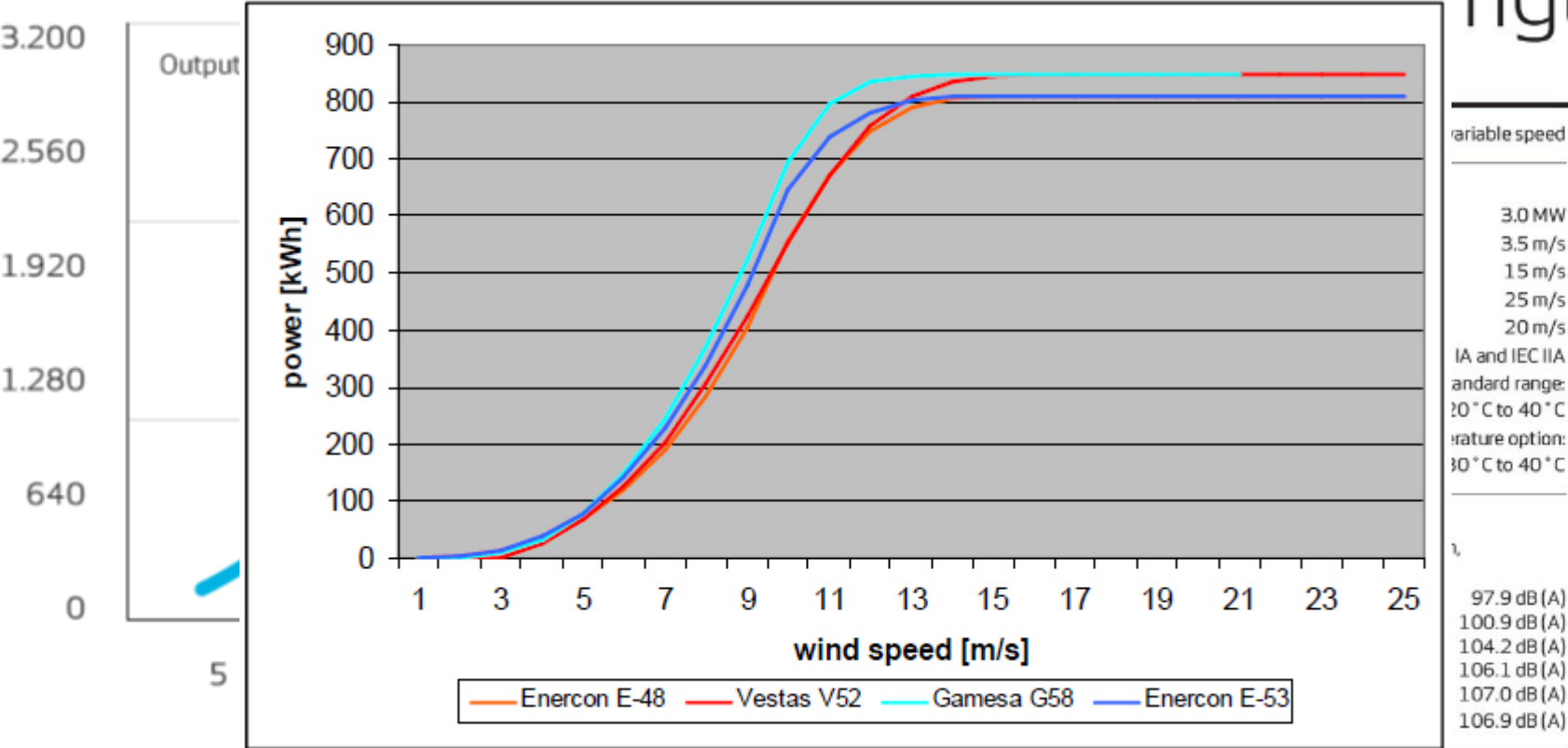
Secure Coding and
Application
Programming

Continuity

Power Curve: $E \sim v^3$

V90-3.0 MW[®]

Facts and figures



ROTOR	
Rotor diameter	90 m
Swept area	6,362 m ²
Nominal revolutions	16.1 rpm
Operational interval	8.6 - 18.4 rpm
Air brake	full blade feathering with 3 pitch cylinders
ELECTRICAL	
Frequency	50/60 Hz
Generator type	4-pole doubly fed generator

Row Level Security – A real world example

You don't like the idea to change the data model to create kind of virtual private database?



- Why does it matter?
- **SQL login vs Integrated security**
- How foreign key relationships can be used
- Why to avoid is_member
- How to cache AD-role membership
- How to write tests to check TVF's working correctly
- Role split – “sysadmin” being admin without data access
- Q & A

Promise:

“At least one of you will not leave empty-handed!”



Robert Sheldon

29 April 2015



How to Get SQL Server Security Horribly Wrong

It is no good doing some or most of the aspects of SQL Server security right. You have to get them all right, because any effective penetration of your security is likely to spell disaster. If you fail in any of the ways that Robert Sheldon lists and describes, then you can't assume that your data is secure, and things are likely to go horribly wrong.

- Failure #1: Not securing the physical environment
- Failure #2: Not protecting the server environments
- Failure #3: Implementing inadequate network security
- Failure #4: Not updating and patching your systems
- Failure #5: Maintaining a large surface attack area
- Failure #6: Using improper authentication ←
- Failure #7: Assigning the wrong service accounts
- Failure #8: Failing to control access to SQL Server resources
- Failure #9: Failing to encrypt sensitive data
- Failure #10: Following careless coding practices
- Failure #11: Not verifying SQL Server implementations
- Failure #12: Failing to audit your SQL Server instances

SQL login – pw "recovery"



```
CREATE LOGIN getme WITH PASSWORD = 'M3n0g1s3';
```

```
-- Requires VIEW permission on the login. When requesting the password hash,  
-- also requires CONTROL SERVER permission  
select name, LOGINPROPERTY(name, 'PasswordHash') as password_hash  
from sys.syslogins  
where LOGINPROPERTY(name, 'PasswordHash') is not NULL  
  
-- Any SQL Server authentication login can see their own login name and the sa login.  
-- To see other logins, requires ALTER ANY LOGIN or permission on the login.  
select name, password_hash from sys.sql_logins
```

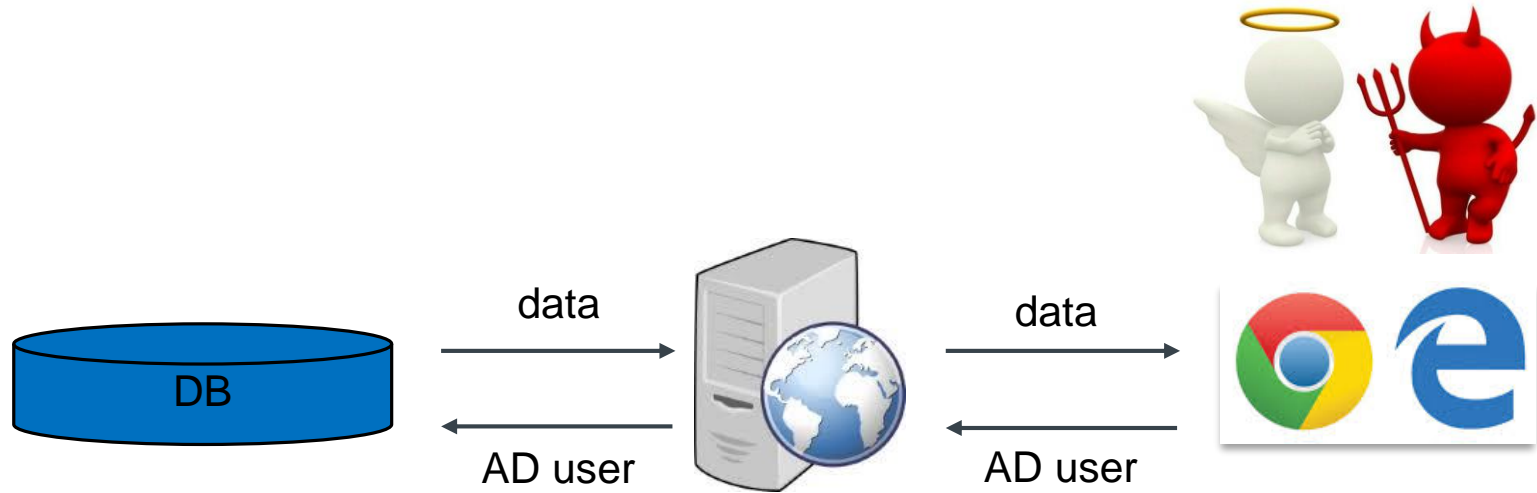
150 %

Results Messages

	name	password_hash
1	sa	0x0200BBA4909165A77C70753A45406F64EEDB7C393C1B4B5...
2	##MS_PolicyEventProcessingLogin##	0x020006763683A85441E46F2F8394F05EF0015259373756FB0...
3	##MS_PolicyTsqlExecutionLogin##	0x0200C1A1784E2AE575A2393BD38F5CBE978ECFFB05CF170...
4	getme	0x0200B130FCB251BBA815D301E1CA9710915D247C043C8D...

```
oclHashcat64 -m 1731 -a 3 -o "C:\Data\pw1.txt" 0x0200B130FCB251BBA815D301E1CA9710915D2...
```

Impersonation



Create another user...



Computer Management

File Action View Help



Computer Management (Local)

- System Tools
 - Task Scheduler
 - Event Viewer
 - Shared Folders
 - Local Users and Groups
 - Users
 - Groups
 - Performance
 - Device Manager
- Storage
 - Windows Server Backup
 - Disk Management
- Services and Applications

Name	Full Name	Description
bdjensen		Built-in account for administering...
DefaultAccount		A user account managed by the s...
Guest		Built-in account for guest access t...
MSSQLSERVER00	MSSQLSERVER00	Local user account for execution ...
MSSQLSERVER01	MSSQLSERVER01	Local user account for execution ...
MSSQLSERVER02	MSSQLSERVER02	Local user account for execution ...
MSSQLSERVER03	MSSQLSERVER03	Local user account for execution ...
MSSQLSERVER04	MSSQLSERVER04	Local user account for execution ...
MSSQLSERVER05	MSSQLSERVER05	Local user account for execution ...
MSSQLSERVER06	MSSQLSERVER06	Local user account for execution ...
MSSQLSERVER07	MSSQLSERVER07	Local user account for execution ...
MSSQLSERVER08	MSSQLSERVER08	Local user account for execution ...
MSSQLSERVER09	MSSQLSERVER09	Local user account for execution ...
MSSQLSERVER10	MSSQLSERVER10	Local user account for execution ...
MSSQLSERVER11	MSSQLSERVER11	Local user account for execution ...
MSSQLSERVER12	MSSQLSERVER12	Local user account for execution ...
MSSQLSERVER13	MSSQLSERVER13	Local user account for execution ...
MSSQLSERVER14	MSSQLSERVER14	Local user account for execution ...
MSSQLSERVER15	MSSQLSERVER15	Local user account for execution ...
MSSQLSERVER16	MSSQLSERVER16	Local user account for execution ...
MSSQLSERVER17	MSSQLSERVER17	Local user account for execution ...
MSSQLSERVER18	MSSQLSERVER18	Local user account for execution ...
MSSQLSERVER19	MSSQLSERVER19	Local user account for execution ...
MSSQLSERVER20	MSSQLSERVER20	Local user account for execution ...

New User



User name:

another

Full name:

another Users

Description:

Password:

.....

Confirm password:

.....

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

Help

Create

Close

Row Level Security – A real world example

You don't like the idea to change the data model to create kind of virtual private database?



- Why does it matter?
- SQL login vs Integrated security
- How foreign key relationships can be used
- Why to avoid is_member
- How to cache AD-role membership
- How to write tests to check TVF's working correctly
- Role split – “sysadmin” being admin without data access
- Q & A

Promise:

“At least one of you will not leave empty-handed!”

Foreign keys



Status (pc)			
	Column Name	Data Type	Allow Nulls
🔑	StatusID	int	<input type="checkbox"/>
	Name	varchar(100)	<input type="checkbox"/>
			<input type="checkbox"/>



Generator (pc)			
	Column Name	Data Type	Allow Nulls
🔑	GeneratorID	bigint	<input type="checkbox"/>
	GeneratorNbr	int	<input type="checkbox"/>
	Name	varchar(50)	<input type="checkbox"/>
	StatusID	int	<input type="checkbox"/>
	ChangeBy	varchar(50)	<input type="checkbox"/>
	ChangeDate	smalldatetime	<input type="checkbox"/>
			<input type="checkbox"/>



WTGDetail (pc)	
Column Name	Data Type
GeneratorID	bigint
Nbr	smallint

Demo steps



- Create tables
- Insert data
- Show data
- Creating TVF's (trap)
- Creating TVF's correct
- Implicit knowledge derived from statistics
- Deploying changes to TVF's used for row level security

```

EXECUTE as login='PWrecover\bdjensen';
select  suser_sname() currentUser;
select * from pc.status;
select * from pc.Generator;
select *
FROM pc.WTGDdetail w
INNER JOIN pc.Generator g ON g.GeneratorID=w.GeneratorID;
REVERT;

```

00 %

Results Messages

	currentUser
1	PWrecover\bdjensen

	StatusID	Name
1	1	InField
2	2	Planned
3	3	TopSecret

	GeneratorID	GeneratorNbr	Name	StatusID	ChangeBy	ChangeDate
1	1024	101	HundredOne	1	PWrecover\bdjensen	2017-12-30 08:29:00
2	1025	102	HundredTwo	2	PWrecover\bdjensen	2017-12-30 08:29:00
3	1026	103	HundredThree	3	PWrecover\bdjensen	2017-12-30 08:29:00

	GeneratorID	Nbr	GeneratorID	GeneratorNbr	Name	StatusID	ChangeBy	ChangeDate
1	1024	1	1024	101	HundredOne	1	PWrecover\bdjensen	2017-12-30 08:29:00
2	1024	2	1024	101	HundredOne	1	PWrecover\bdjensen	2017-12-30 08:29:00
3	1024	3	1024	101	HundredOne	1	PWrecover\bdjensen	2017-12-30 08:29:00
4	1025	1	1025	102	HundredTwo	2	PWrecover\bdjensen	2017-12-30 08:29:00
5	1025	2	1025	102	HundredTwo	2	PWrecover\bdjensen	2017-12-30 08:29:00
6	1025	3	1025	102	HundredTwo	2	PWrecover\bdjensen	2017-12-30 08:29:00
7	1026	1	1026	103	HundredThree	3	PWrecover\bdjensen	2017-12-30 08:29:00
8	1026	2	1026	103	HundredThree	3	PWrecover\bdjensen	2017-12-30 08:29:00
9 17	1026	3	1026	103	HundredThree	3	PWrecover\bdjensen	2017-12-30 08:29:00



Wind. It means the world to us.™



```
EXECUTE as login='PWrecover\another';
select suser_sname() currentUser;
select * from pc.status;
select * from pc.Generator;
select *
FROM pc.WTGDdetail w
INNER JOIN pc.Generator g ON g.GeneratorID=w.GeneratorID;
REVERT;
```

.00 %

Results Messages

	currentUser
1	PWRECOVER\another

	StatusID	Name
1	1	InField
2	2	Planned

	GeneratorID	GeneratorNbr	Name	StatusID	ChangeBy	ChangeDate
1	1024	101	HundredOne	1	PWrecover\bdjensen	2017-12-30 08:29:00
2	1025	102	HundredTwo	2	PWrecover\bdjensen	2017-12-30 08:29:00

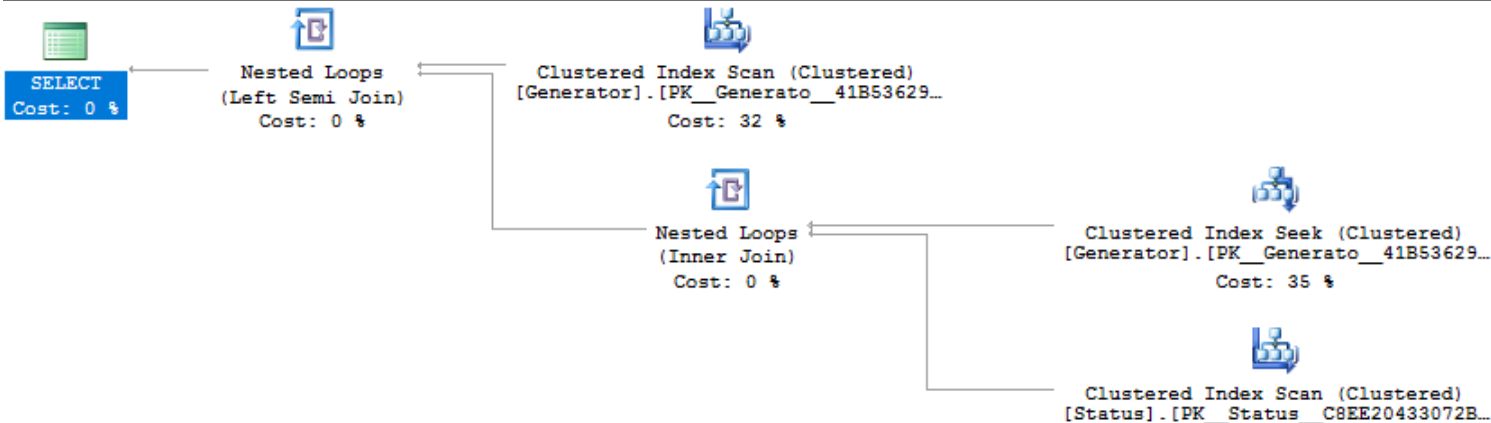
	GeneratorID	Nbr	GeneratorID	GeneratorNbr	Name	StatusID	ChangeBy	ChangeDate
1	1024	1	1024	101	HundredOne	1	PWrecover\bdjensen	2017-12-30 08:29:00
2	1024	2	1024	101	HundredOne	1	PWrecover\bdjensen	2017-12-30 08:29:00
3	1024	3	1024	101	HundredOne	1	PWrecover\bdjensen	2017-12-30 08:29:00
4	1025	1	1025	102	HundredTwo	2	PWrecover\bdjensen	2017-12-30 08:29:00
5	1025	2	1025	102	HundredTwo	2	PWrecover\bdjensen	2017-12-30 08:29:00
6	1025	3	1025	102	HundredTwo	2	PWrecover\bdjensen	2017-12-30 08:29:00

Statistics can tell you something...



Query 1: Query cost (relative to the batch): 100%

select * from pc.Generator



Clustered Index Scan (Clustered)	
Scanning a clustered index, entirely or only a range.	
Physical Operation	Clustered Index Scan
Logical Operation	Clustered Index Scan
Estimated Execution Mode	Row
Storage	RowStore
Estimated I/O Cost	0.0032035
Estimated Operator Cost	0.0034489 (33%)
Estimated CPU Cost	0.0000818
Estimated Subtree Cost	0.0034489
Estimated Number of Executions	3
Estimated Number of Rows	3
Estimated Number of Rows to be Read	3
Estimated Row Size	65 B
Ordered	False
Node ID	4

Row Level Security – A real world example



You don't like the idea to change the data model to create kind of virtual private database?

- Why does it matter?
- SQL login vs Integrated security
- How foreign key relationships can be used
- **Why to avoid is_member**
- How to cache AD-role membership
- How to write tests to check TVF's working correctly
- Role split – “sysadmin” being admin without data access
- Q & A

Promise:

“At least one of you will not leave empty-handed!”

is_member



```
--https://docs.microsoft.com/en-us/sql/t-sql/functions/is-member-transact-sql
--IS_MEMBER ( { 'group' | 'role' } )
select is_member('Mydomain\MyADgroup') MemberInMyAD, is_member('db_owner') dbowner
      , IS_SRVROLEMEMBER('sysadmin') sysadmin, is_member('PWrecover\bdjensen') ismember
      , suser_sname() username
```

results				
Messages				
MemberInMyAD	dbowner	sysadmin	ismember	username
NULL	1	1	1	PWrecover\bdjensen

High

*PREEMPTIVE_OS_LOOKUPACCSID &
PREEMPTIVE_OS_AUTHORIZATIONOPS*



*select * from pc.Generator*

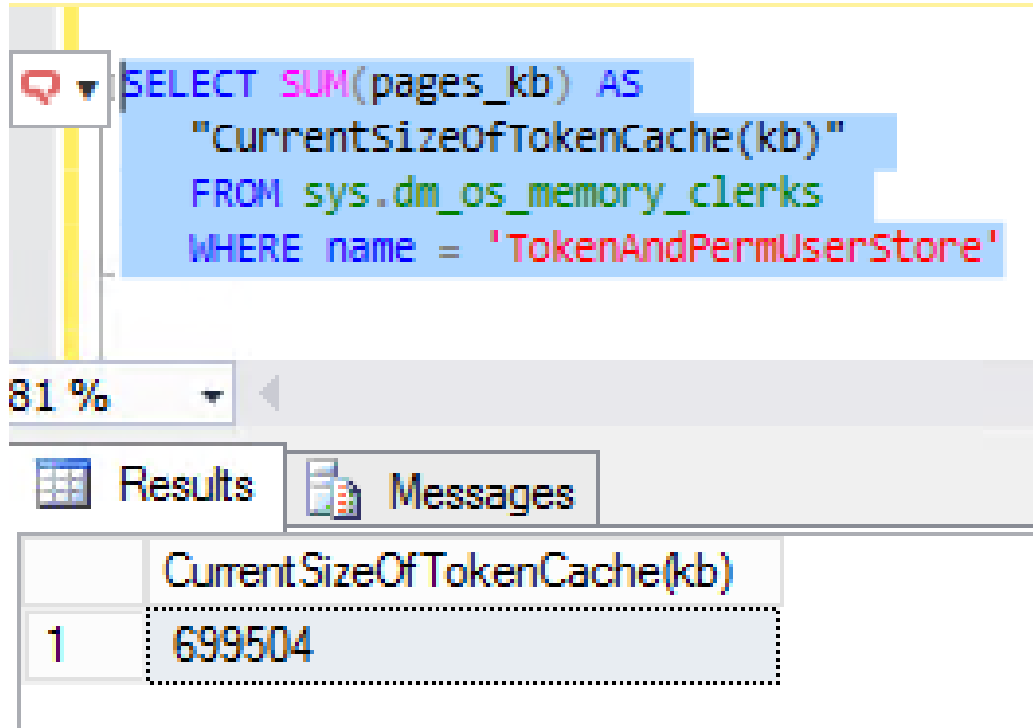
WaitType="PREEMPTIVE_OS_LOOKUPACCSID"

WaitTimeMs="8851" WaitCount="10007"

WaitType="PREEMPTIVE_OS_AUTHORIZATIONOPS"

WaitTimeMs="21900" WaitCount="10007"

Don't include is_member in RLS functions to check AD role



The screenshot shows a SQL query window with the following text:

```
SELECT SUM(pages_kb) AS  
    "CurrentSizeOfTokenCache(kb)"  
FROM sys.dm_os_memory_clerks  
WHERE name = 'TokenAndPermUserStore'
```

Below the query, the 'Results' tab is active, displaying a single row of data:

	CurrentSizeOfTokenCache(kb)
1	699504

<https://docs.microsoft.com/en-us/sql/relational-databases/security/row-level-security>

Has example with user_name(), but...

DBCC FREESYSTEMCACHE ('TokenAndPermUserStore')

<https://blogs.technet.microsoft.com/bulentozkir/2014/01/09/tokenandpermuserstore-related-information-on-sql-server-2012/>



Row Level Security – A real world example

You don't like the idea to change the data model to create kind of virtual private database?

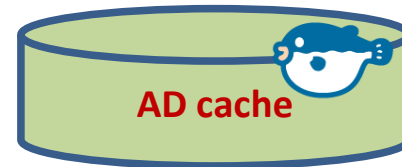
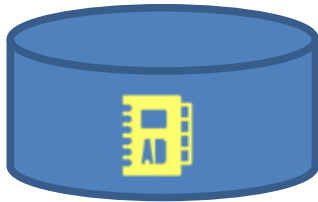


- Why does it matter?
- SQL login vs Integrated security
- How foreign key relationships can be used
- Why to avoid is_member
- **How to cache AD-role membership**
- How to write tests to check TVF's working correctly
- Role split – “sysadmin” being admin without data access
- Q & A

Promise:

“At least one of you will not leave empty-handed!”

Caching AD-role membership



ADinfo

View to extract
info from AD
source via
Power-Shell.

CacheADmembership

Procedure to merge
into table
Membership

UserMembership

View on top of
table Membership.
To be used in TVF
for RLS.

```
$list=(Get-ADGroupMember -identity "MyADgroupName" -Recursive )  
$list.SamAccountName -join ","
```

Job Properties - GetADInfo

Select a page

General

Steps

Schedules

Alerts

Notifications

Targets

Script

Help

Job step list:

Step	Name	Type	On Success	On Failure
1	Lookup_App-Role1	PowerShell	Go to the next step	Quit the job reporting failure
2	Lookup_App-Role2	PowerShell	Go to the next step	Quit the job reporting failure
3	CacheADmembership	Transact-SQL script (T-SQL)	Quit the job reporting s...	Quit the job reporting failure

Job Step Properties - Lookup_App-Role1

Select a page

General

Advanced

Script

Help

On success action:

Go to the next step

Retry attempts:

0

Retry interval (minutes):

0

On failure action:

Quit the job reporting failure

PowerShell

Output file:

...

View

☐ Append output to existing file

☒ Log to table

☐ Append output to existing entry in table

☐ Include step output in history

View

Connection

Server: PWrecover

Connection: PWrecover\bdjensen



26

Row Level Security – A real world example



You don't like the idea to change the data model to create kind of virtual private database?

- Why does it matter?
- SQL login vs Integrated security
- How foreign key relationships can be used
- Why to avoid is_member
- How to cache AD-role membership
- **How to write tests to check TVF's working correctly**
- Role split – “sysadmin” being admin without data access
- Q & A

Promise:

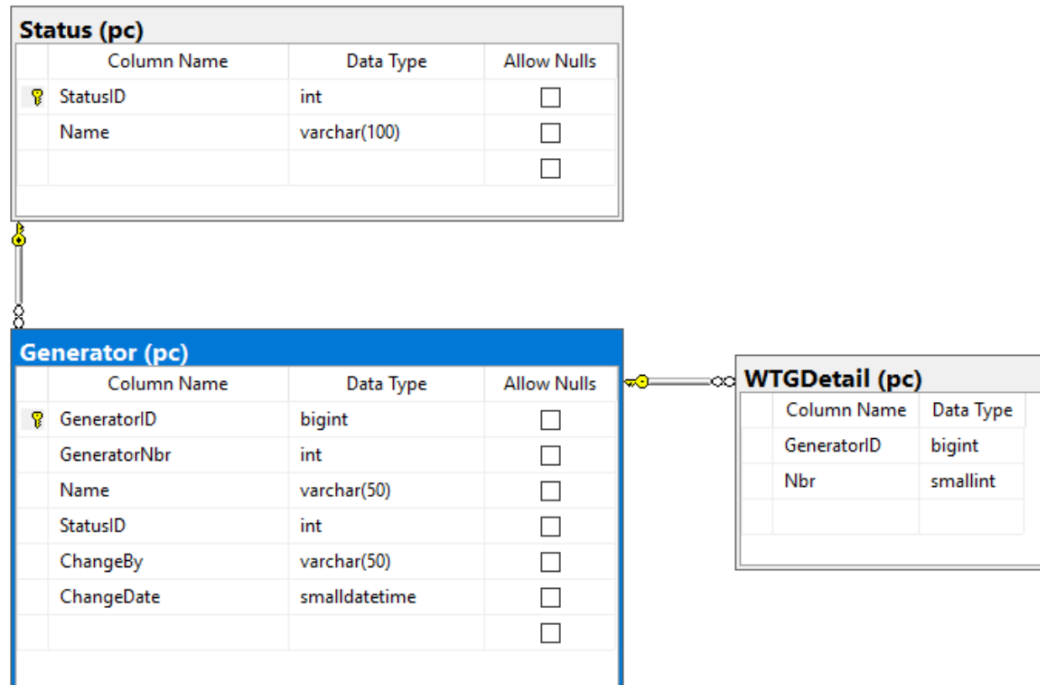
“At least one of you will not leave empty-handed!”

Proc CheckRLS



Check

- rowcount
- "key" table (pc.Status)
- tables with foreign key to pc.Status
- tables indirectly related to pc.Status
- Cache non-empty



Demo steps



- How to cache AD role membership
 - A. ADInfo view
 - B. Membership table
 - C. Membership view
 - D. CacheADmembership procedure
 - E. Job for synchronization
 - F. Check membership (select)
- How to write tests to check TVF's working correctly
 - CheckRLS
 - CheckAccess

Row Level Security – A real world example

You don't like the idea to change the data model to create kind of virtual private database?

- Why does it matter?
- SQL login vs Integrated security
- How foreign key relationships can be used
- Why to avoid is_member
- How to cache AD-role membership
- How to write tests to check TVF's working correctly
- Role split – “sysadmin” being admin without data access
- Q & A



Promise:

*"At least one of you
will not leave empty-
handed!"*

Split responsibility



```
ALTER SERVER ROLE [sysadmin]
  ADD MEMBER [Domainname\ADgroupSuperAdmin];
```

```
GRANT CONTROL SERVER          TO [DomainName\ADgroupNormalAdmin];
DENY IMPERSONATE ANY LOGIN    TO [DomainName\ADgroupNormalAdmin];
DENY CONTROL ON SCHEMA::secu TO [DomainName\ADgroupNormalAdmin];
```

Audit

Use Kenneth Fisher's stored procedures to get overview of authentication and authorization

[sp_SrvPermissions](#)

[sp_DBPermissions](#)

SQLBits - It's all about the community...

Please visit Community Corner, we are trying this year to get more people to learn about the SQL Community, equally if you would be happy to visit the community corner we'd really appreciate it.



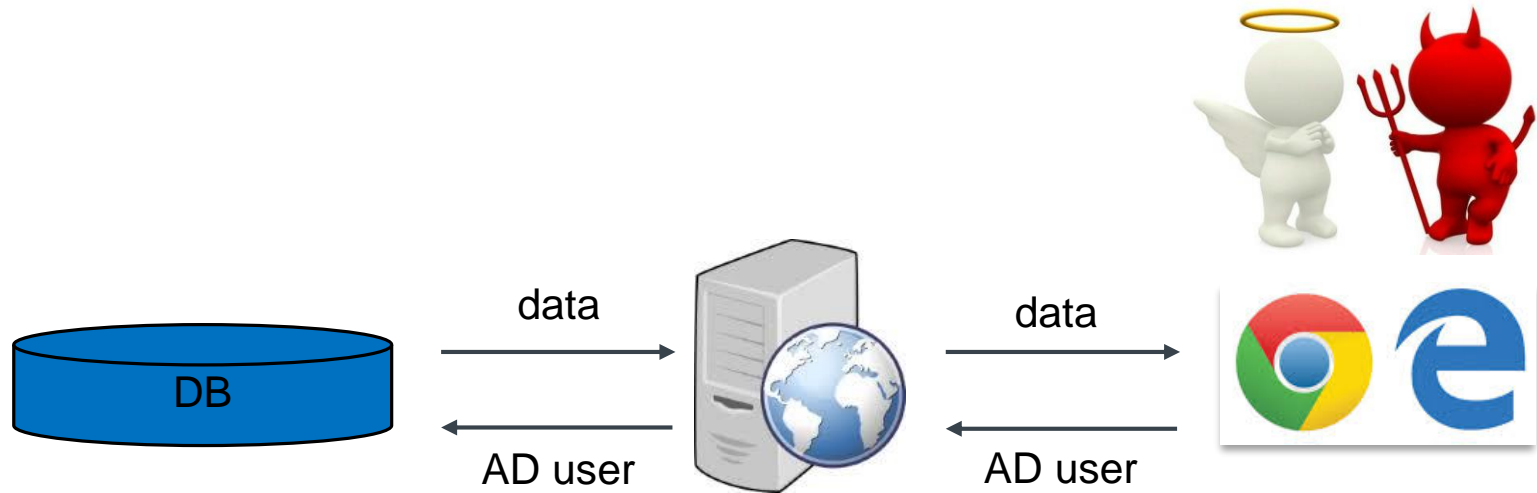


Promise:
*"At least one of you
will not leave empty-
handed!"*

Thank you for your attention!

bjdje@vestas.com
Bjorn.D.Jensen@gmail.com

Impersonation



- ASP .Net Impersonation / Windows Authentication: Enable
- Kerberos
- AppPoolCredentials / UseKernelMode: true
- Application binding
- Register domain name as A-record
- Svc account running web server: *Trust this user for delegation to specified services only*
- Register SPN (setspn)
- Client web browser: allow forwardable tickets
- Debugging: sniff Kerberos tickets (Wireshark)
- Good relations to IT-department