

GDPR

- HVORDAN FÅ JOBBEN GJORT?

Vidar Eidissen

Better Work AS

Vidar@better-work.no

@nicetheoryvidar

nicetheory.io

Freelancer

Database arkitekt/utvikler

Technical team mentor/coach

23 år fra Helse-IT

Oracle siden 1998

Oracle Database
SQL Certified Expert

Oracle Advanced PL/SQL
Developer Certified Professional

(DBA - OCP 8i)



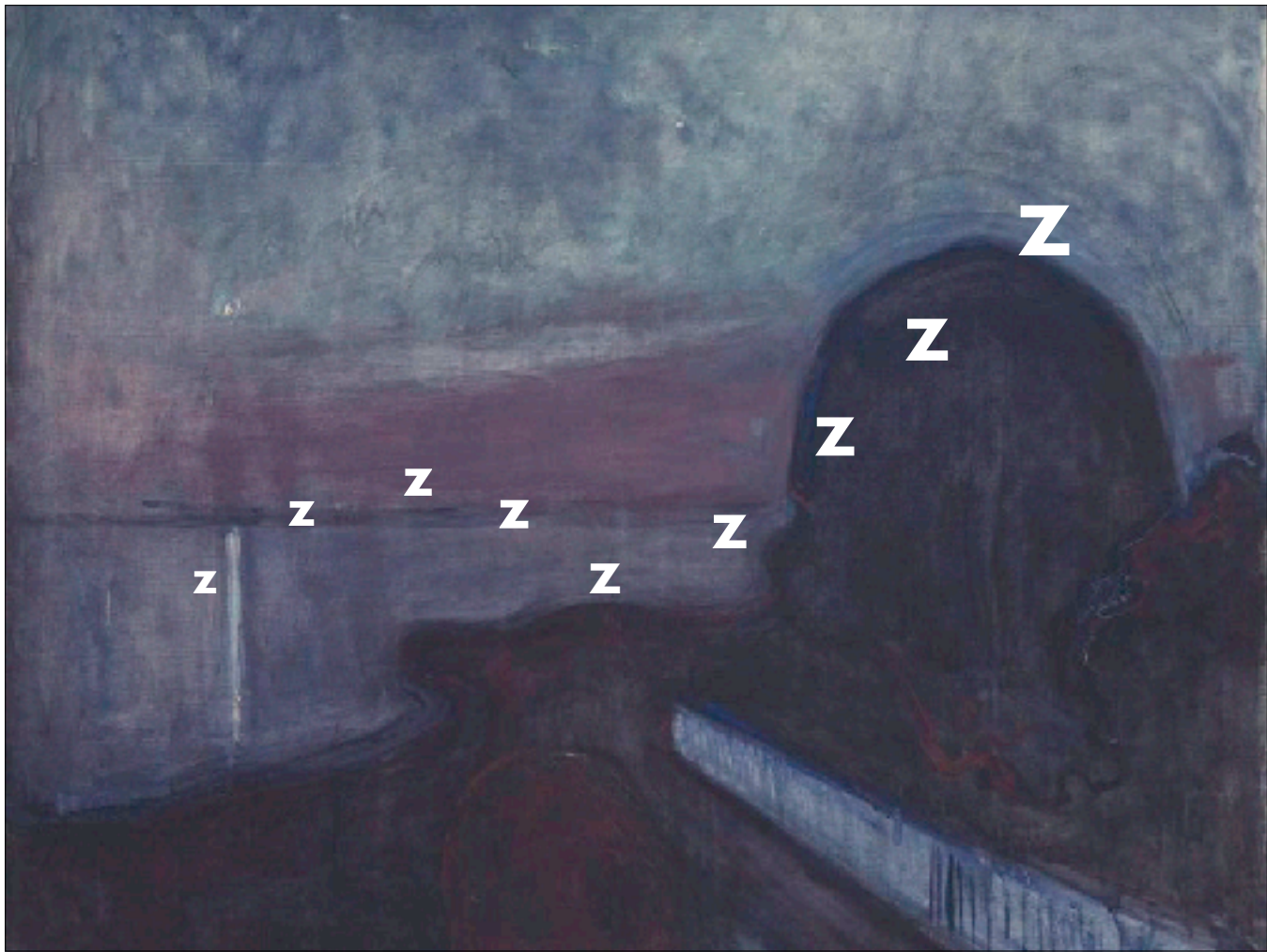
Alcatraz swim 2017

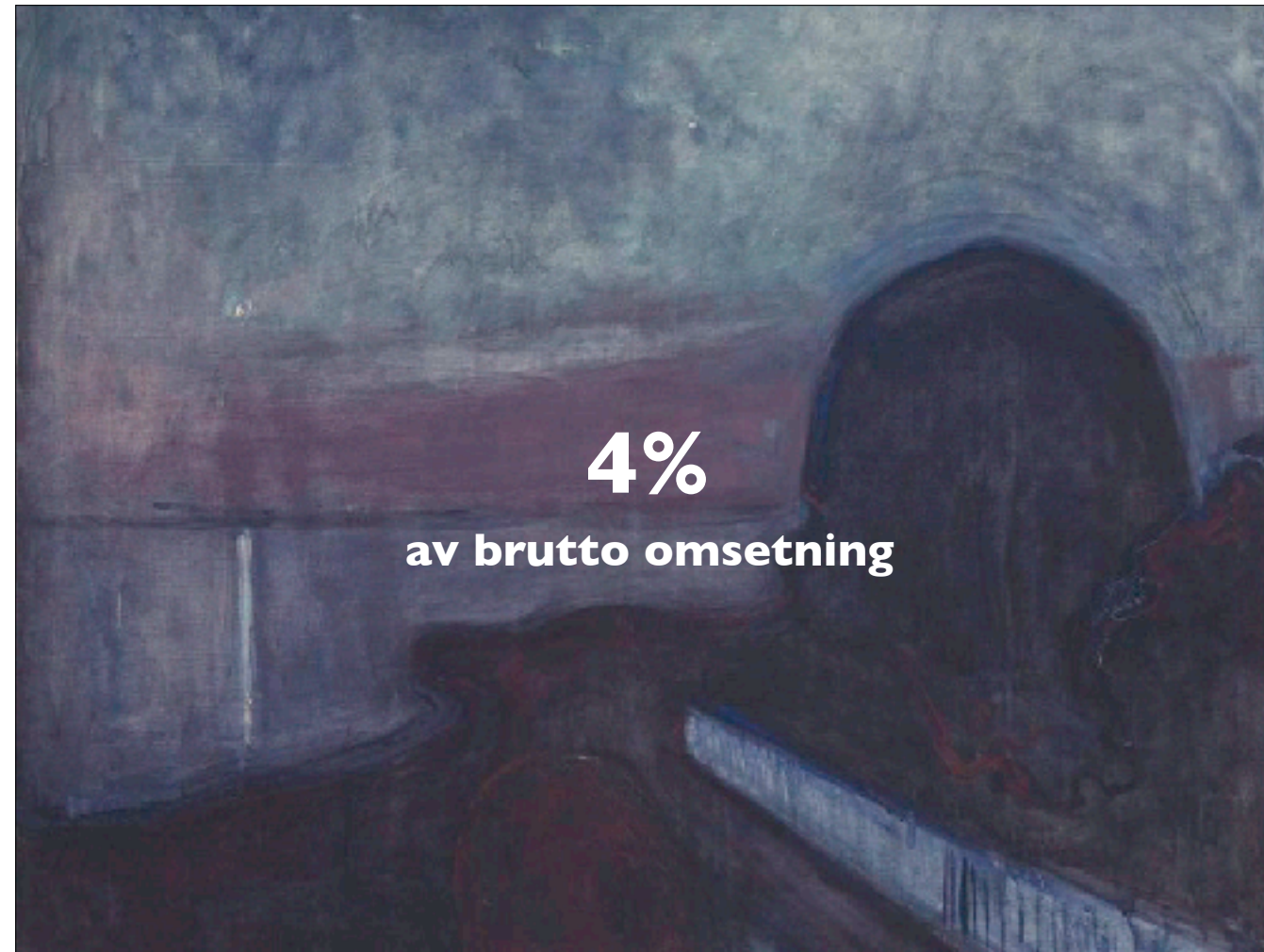
DAGENS TEMA

- Litt GDPR
- Utfordringer
 - Sikkerhet, sletting av data, sporbarhet
- En titt i Oracle-verktøykassa for litt inspirasjon

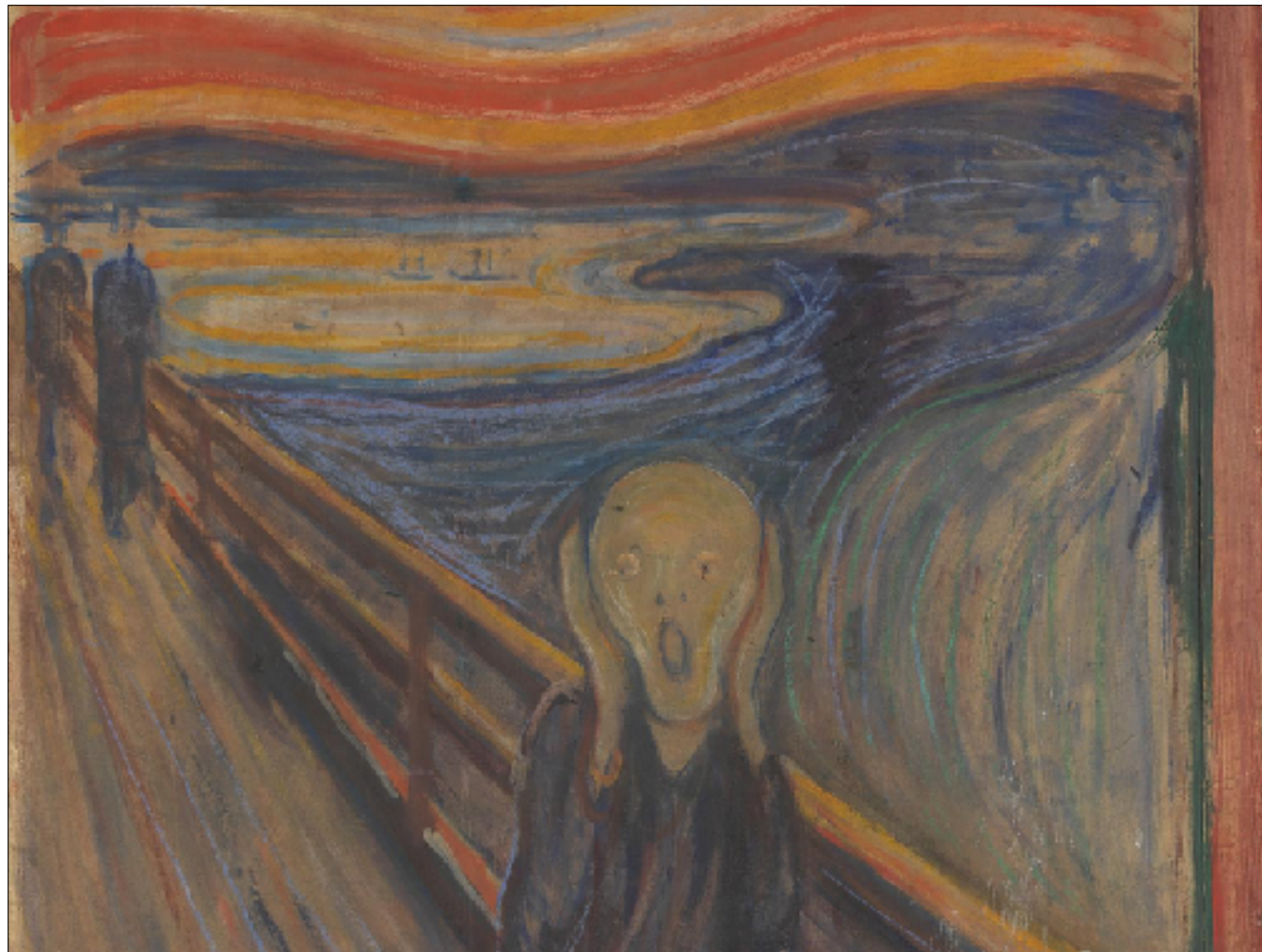


Dommedagsklokke: <http://www.eugdpr.org>





Omsetning på 1 mrd = 40 millioner



Munch - skriket

GDPR

- Går live 25. mai neste år
- Litt Y2K-stemning over det hele
- Men verden, slik vi kjenner den, kommer ikke til å opphøre
- Mange meninger rundt GDPR, effekter og tolkninger
- Det viktigste er nå en gang å være bevisst
- Du kan neppe la være å gjøre noe som helst
- Gjelder fra det øyeblikk du har en EU-borger på kundelista



GDPR - RETTIGHETER

- Consent
- Right of Access
- Right to Rectification
- Right to be Forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers
- Breach Notification
- Innen 72 timer

<http://www.eugdpr.org/key-changes.html>

Consent:

Explicit consent is required only for processing sensitive personal data - in this context, nothing short of “opt in” will suffice. However, for non-sensitive data, “unambiguous” consent will suffice.

Data Protection Officers:

DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37).



TAKK FOR DIN PÅMELDING

Du vil nå motta nyhetsbrev og **eksklusive tilbud** fra oss

Jeg takket kun ja
til å motta kvittering på
e-post...

TAKK FOR DIN PÅMELDING

Vi setter stor pris på at du ønsker å motta nyhetsbrev og kvitteringer på e-post. Som mottaker av vårt nyhetsbrev vil du blant annet motta ukens kampanje, eksklusive tilbud og informasjon om nye produkter.

Du kan melde deg av nederst i e-posten om du beklageligvis har blitt påmeldt ved en feiltakelse.

ALT DETTE INNEBÆRER AT DET MÅ
RYDDES I RUTINER, SYSTEMER OG
DATA

Compliance for å styrke varemerket - skape kundetrygghet

VURDERINGER

- Kan du lagre det du lagrer?
- Kan du bruke det til det du bruker det til?
- Kan du bruke det til det du har tenkt å bruke det til?
- Når må du kvitte deg med data?
- Og fra hvilke systemer?

Gjør klar for å tenke oppbevaringstiden på forskjellige kategorier av data.
Hvor lenge kan du beholde disse dataene og til hva kan du bruke dem?

DAGENS TIPS # I

OPPGRADER TIL I2C

HVORFOR?

Verktøykassa er bedre
Dessuten er Ilg (på vei) ut



SLETTE DATA

HVORFOR?

- Du kan beholde data om kunden for legitim utførelse av virksomheten/kontrakten
- Når du ikke lengre har en legitim grunn og kunden ikke har gitt sitt samtykke må du gjøre noe
- Kunden krever sletting

Hvorfor man må slette data:

Når legitimate reasons ikke gjelder lengre

Right to be forgotten

Right to object

Revoke of consent

To delete or not to delete

– That is the query

STANDARD DELETE

- Sjekk hva fremmednøkler kan gjøre for deg
 - hvis du har dem
 - on cascade delete / on cascade null
- Genererer mye undo

PARTITIONING

- En svært nyttig opsjon
- En tabell blir delt inn i flere fysiske sub-tabeller
- Transparent
- Kan benyttes i mange forskjellige henseende
- Row movement

How do you update millions of rows?

You don't

Legg inn link til Tom Kyte

CTAS

- Create table as select
- Kan også angi attributter for tabellen, evt opprette den på forhånd
- Bruk /*+append*/ hint for å redusere undo/redo
- Enable parallel dml?
- Kan evt bruke compress basic for å spare plass
 - Trenger ikke egen lisens og funker bare ved direct path inserts
 - Kan redusere I/O hvis det passer med applikasjonen (lite updates)

Compress basic eksempel

PARALLEL DML

- Kommer ikke av seg selv...
- When parallel DML is disabled, no DML is executed in parallel even if the PARALLEL hint is used.
- ALTER SESSION ENABLE PARALLEL DML;
- i 12c også som hint:
- INSERT /*+ ENABLE_PARALLEL_DML */ ...
- "The DML operation may still execute serially if there are no parallel hints or no tables with a parallel attribute or if restrictions on parallel operations are violated."

ALTSÅ...

- Alter table <table_name> parallel x
- Alter index <index_name> parallel x
- alter session enable parallel dml;
- INSERT /*+PARALLEL x APPEND */ INTO ...
- eller
- INSERT /*+ ENABLE_PARALLEL_DML PARALLEL x APPEND*/ ...

Make test-cases

DBMS_REDEFINITION

- Hvis du ikke har anledning til å ta mye nedetid
- Denne fikser også indekser, constraints, trigger, grants... Nice!
- Online redefinering av tabeller kan benyttes til å også droppe / modifisere data via **col_mapping**-parameteren (psevdo-/anonymisering)
- Kan fysisk reorganisere data via **orderby**-parameteren (sortering)
- Kan evt sette parallellitet på tabellen og indeksene før du setter i gang.
- Potensiale for compress og append her også

Kan man endre spørringen som benyttes for å populere den nye tabellen?

Kan sortere på statusfelt, slik at rader som skal slettes ligger samlet til slutt. Deretter delete og deallocate unused?

Hva skjer om man kombinerer dbms_redefinition med VPD? Vil man få med VPD-predikater?

HVA OM DU IKKE HELT TØR Å
SLETTE?

DU HAR VEL ET TEST-SYSTEM?

MEN NOEN GANGER SKAL DET
BARE VÆRE SLETTET FOR NOEN
BRUKERE/SYSTEMER

FORSKJELLIGE BEHOV

- Man har forskjellige interne krav
- Kunden bør slettes fra systemet og har bedt seg slettet
- Men må beholde data pga juridiske forpliktelser

IN-DATABASE ARCHIVING

- 12.1-funksjonalitet
- Ingen ekstra lisens
- alter table xxx row archival
- Legger til en ekstra kolonne for "soft-delete"
- Delete gjøres ved update av ORA_ARCHIVE_STATE
 - Kan godt kombineres med partisjonering og row movement
- Transparent for applikasjoner

Tim Hall: <https://oracle-base.com/articles/12c/in-database-archiving-12cr1>

Oracle ILM støtter kun verdiene 0 og 1 for automatikk

Transparent så lenge man ser bort fra at deletes i en del tilfeller må skrives om til update.

```
SQL> create table ida (  
2     id number primary key,  
3     text varchar2(10)  
4 )  
5 tablespace users  
6 row archival;
```

Table IDA created.

```
SQL> begin  
2     insert into ida  
3     values (1, 'Linje 1');  
4     insert into ida  
5     values (2, 'Linje 2');  
6     insert into ida  
7     values (3, 'Linje 3');  
8     commit;  
9 end;  
10 /
```

```
SQL> select id, text, ora_archive_state from  
ida;
```

ID	TEXT	ORA_ARCHIVE_STATE
1	Linje 1	0
2	Linje 2	0
3	Linje 3	0

```
3 rows selected.
```

```
SQL> -- Obs - user_tab_columns viser ikke hidden columns
SQL> select column_name, data_type, data_length
  2   from user_tab_columns
  3  where table_name = 'IDA';
```

COLUMN_NAME	DATA_TYPE	DATA_LENGTH
ID	NUMBER	22
TEXT	VARCHAR2	10

2 rows selected.

```
SQL> -- Men det gjør user_tab_cols:
SQL> select column_name, data_type, data_length, hidden_column
  2   from user_tab_cols
  3  where table_name = 'IDA';
```

COLUMN_NAME	DATA_TYPE	DATA_LENGTH	HID
ORA_ARCHIVE_STATE	VARCHAR2	4000	YES
ID	NUMBER	22	NO
TEXT	VARCHAR2	10	NO

3 rows selected.

```
SQL> update ida
      2  set ora_archive_state = 1
      3  where id = 2;
```

1 row updated.

```
SQL>
```

```
SQL> select id, text, ora_archive_state from ida;
```

ID	TEXT	ORA_ARCHIVE_STATE
1	Linje 1	0
3	Linje 3	0

2 rows selected.


```
SQL> update ida
      2  set ora_archive_state = 'Slettes 25.05.2018'
      3  where id = 3;
```

1 row updated.

```
SQL>
```

```
SQL> select id, text, ora_archive_state from ida;
```

ID	TEXT	ORA_ARCHIVE_STATE
1	Linje 1	0

1 row selected.

```
SQL> alter session set row archival visibility = all;
```

```
Session altered.
```

```
SQL>
```

```
SQL> select id, text, ora_archive_state from ida;
```

ID	TEXT	ORA_ARCHIVE_STATE
1	Linje 1	0
2	Linje 2	1
3	Linje 3	Slettes 25.05.2018

```
3 rows selected.
```

```
SQL> alter session set row archival visibility = active;
```

```
Session altered.
```

```
SQL>
```

```
SQL> select id, text, ora_archive_state from ida;
```

ID	TEXT	ORA_ARCHIVE_STATE
1	Linje 1	0

```
1 row selected.
```

```
SQL> declare
  2     l_ida_row ida%rowtype;
  3  begin
  4     select *
  5     into l_ida_row
  6     from ida
  7     where id = 1;
  8
dbms_output.put_line(l_ida_row.ora_archive_state);
  9  end;
10  /
```

Error report -

ORA-06550: linje 8, kolonne 34:

PLS-00302: komponenten ORA_ARCHIVE_STATE må deklarereres

ORA-06550: linje 8, kolonne 3:

PL/SQL: Statement ignored

06550. 00000 - "line %s, column %s:\n%s"

*Cause: Usually a PL/SQL compilation error.

*Action:

```
SQL> -- alter table får radene frem igjen
SQL> select * from ida;
```

ID	TEXT
1	Linje 1

1 row selected.

```
SQL> alter table ida no row archival;
```

Table IDA altered.

```
SQL> select * from ida;
```

ID	TEXT
1	Linje 1
2	Linje 2
3	Linje 3

3 rows selected.

```
SQL> -- Når man gjør alter ... row archival:  
SQL> alter table ida row archival;
```

Table IDA altered.

```
SQL>  
SQL> -- Får man en ekstra kolonne...  
SQL> select column_name, data_type, data_length, hidden_column  
2   from user_tab_cols  
3   where table_name = 'IDA';
```

COLUMN_NAME	DATA_TYPE	DATA_LENGTH	HID
SYS_NC00003\$	RAW	126	YES
ID	NUMBER	22	NO
TEXT	VARCHAR2	10	NO
ORA_ARCHIVE_STATE	VARCHAR2	4000	YES

4 rows selected.

PASS PÅ...

- Variabler forankret i tabell-definisjonen
 - %rowtype
- Vil ikke få med seg skjulte kolonner
- Må kanskje endre delete til update i noen tilfeller
- Du har fremdeles dataene - de er ikke slettet

ANDRE VARIANTER

- Oracle ILM: Information Lifecycle Management
- Temporal Validity
- Ikke glem å rydde i logger også

<https://docs.oracle.com/database/122/VLDBG/control-validity-visibility-data.htm#VLDBG14153>

MEN - VI KAN IKKE OMSKRIVE EN
HAUG MED SPØRRINGER

FORSKJELLIGE APPLIKASJONER
=
FORSKJELLIGE APPLIKASJONSBRUKERE

VPD

- Virtual Private Database
- Ingen ekstra lisens (gitt Enterprise Edition)
- Fungerer ved at det, transparent, legges til ekstra predikater på SQL-statements
- Forbedret i 12c....:

RAS

- Real Application Security
- Ingen ekstra lisens
- Forbedret versjon av VPD
- Deklarativt oppsett og påstått bedre skalerbarhet

Link til whitepaper: <http://www.oracle.com/technetwork/database/database-technologies/real-application-security/overview/index.html>

RAS SECURITY COMPONENTS



DATA REALMS

		ViewSSN	ViewSalary		
Name	ID	SSN	Salary	Manager	Phone Num
Steven	SKING			*	515.123.4557
Neena	NKODHAR			Steven	515.123.4558
Nancy	NGREENBE	105.81.4560	12008	Neena	515.124.4569
John	JCHEN		8200	Nancy	515.124.4289
Luis	LPORP		6900	Nancy	515.126.1111

ACL: Employee can view own SSN, Salary

ACL: Manager can view Salary

ACL: All Employees can view cells of remaining columns

RAS/VPD - POTENSIELLE SEGMENTERINGSNØKLER

- Logon Schema
- Rolle
- Applikasjonskode
- Logon-trigger
- Service
- m.m.

**Må kunne identifisere
sluttbrukere og
applikasjoner/moduler**

Nøkkelen til å få dette til å fungere er å klare å identifisere slutt-brukere, roller, m.m.

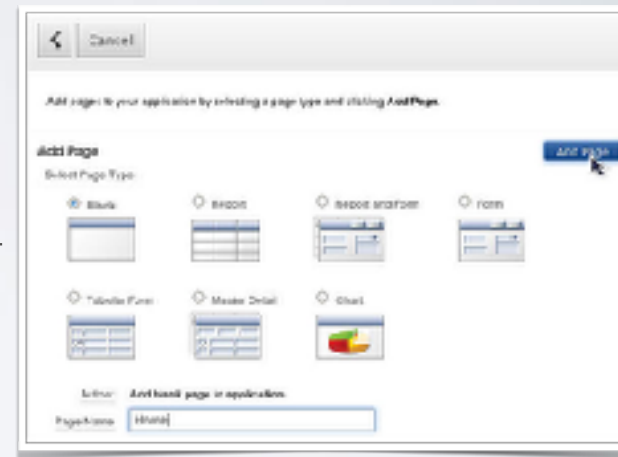
WHITE LISTS VS BLACK LISTS

- White list = Alle disse er lov
- Black list = Alle unntatt disse er lov
- Viktig å finne en effektiv måte å filtrere data på
- Komplekse regler med tunge oppslag vil kunne ha store negative konsekvenser for ytelsen
- Ideelt sett filtrerer du basert på context-verdier

Application context = key/value i memory

RYDDING I DATA

- Apex to the rescue!
- Ligger i databasen
- Test det ut på apex.oracle.com
- Ypperlig til å
 - Erstatte regneark
 - Lage apper for rydding i datagrunnlag



HAR DU EN HJEMMELAGET
APPLIKASJON?

ALT KAN REPARERES?

MEN DET ER JO GREIT Å TESTE LITT
FØRST?

TESTDATA

- Produksjonsdata er ikke nødvendigvis manna for å få testet nyutviklet kode - ofte tvert i mot
- Mange testprosedyrer lider under tilfeldigheter
 - I hva som egentlig testes
 - I hvilke data som brukes
- Vurdere å innføre automatisert testing med kjente data
- Vurdere å benytte TDD metodikk (Test Driven Development)

Mange gjøre en serie av manuelle steg med å legge inn data og så sjekke manuelt.
Disse stegene kan programmeres og automatiseres.

PRODUKSJONSDATA I TEST

- Tar mye plass
- Tar tid å få på plass
- Er mest aktuell for test av oppgradering og kanskje volumtest
 - Ikke utvikling
- Viktig å beskytte disse - tidlig i prosessen
- Anonymisering/Pseudonymisering/Aidentifisering

Kan gjerne lage en utviklingsbase basert på prod, men uten personidentifiserbare data.

<http://www.hioa.no/Om-HiOA/Interne-ressurser-og-rutinebeskrivelser/FoU-haandbok/Definisjoner-og-forkortelser>

PROVISJONERING

HVORDAN SKAFFE GODE TESTMILJØ

- Gjør dem "lettere": Å få på plass, bruke og bytte ut
- Virtual Box / andre typer VM
- Container-teknologi: Docker, ...
- Clone DB
- Men pass nå på hvor du kopierer de sensitive dataene dine...

Tidlig rensking.

Clone DB article by Martin Bach: <https://martincarstenbach.wordpress.com/2015/08/04/clonedb-in-oracle-12-1-0-2/>

Tim Hall: <https://oracle-base.com/articles/11g/clonedb-11gr2>

CLONE DB

- Thin provisioning
- Flere instanser kan benytte samme datafilsett over dNFS
- Endringer skrives til "lokalt" delta
- Instansene kan selvsagt påvirke hverandre ytelsesmessig
- Kan redusere plassbehovet betraktelig ved flere instanser

Clone DB article by Martin Bach: <https://martincarstenbach.wordpress.com/2015/08/04/clonedb-in-oracle-12-1-0-2/>

Tim Hall: <https://oracle-base.com/articles/11g/clonedb-11gr2>

Read-only tablespace kan deles mellom flere instanser - det gjorde jeg ved et uhell en gang.

OBS!

Test og utvikling er ikke det samme

EBR

- Edition Based Redefinition
- Tryggere utrulling av endringer i kode
- Sikrer utfasing av død kode = du forblir compliant

Seminar i Bergen i slutten av november

DATA BREACH

SIKKERHET

- Fryktelig pinlig og dårlig for omdømmet å måtte melde til kundene at man har hatt et innbrudd
- God motivasjon for å passe på hva man lagrer
- Gå gjennom systemene fra A til Å og gjør det jevnlig

Trigger points:

Config-endringer

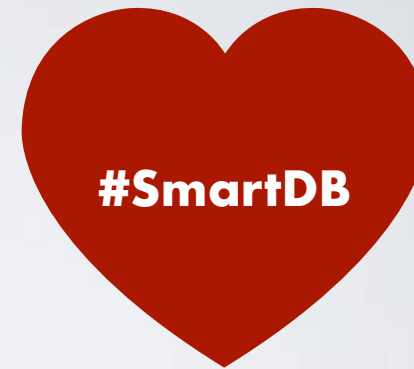
Nye systemer (datavarehus/BI)

Nye tabeller

Hente data til testing

Eksempel: Amedia sendte mail med brukernavn OG passord som kvittering på at man hadde registrert seg.

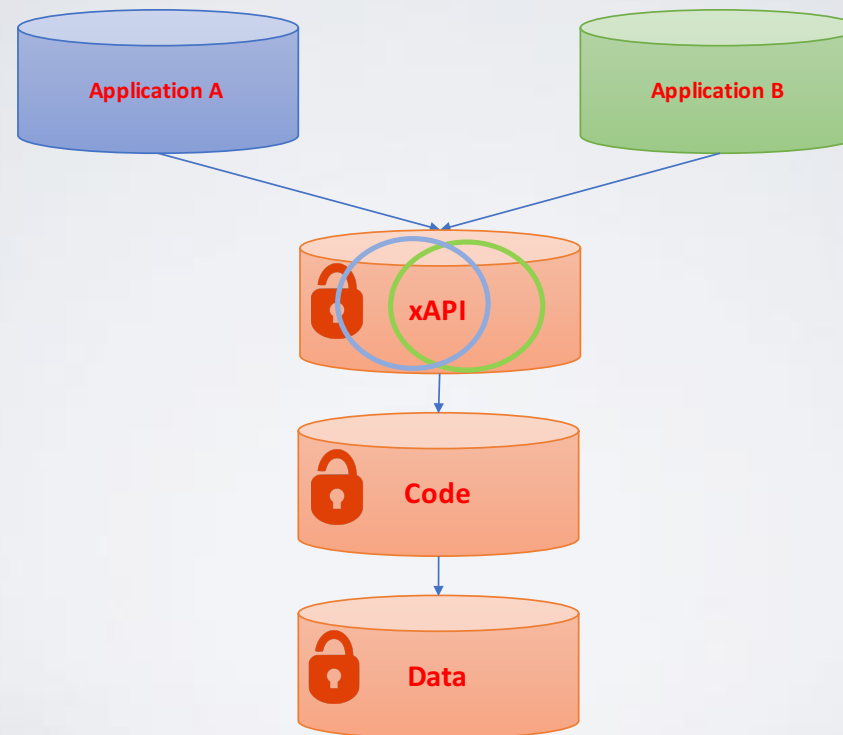
"GULLSTANDARDEN"



- 3-4 schema:
- Aksess: (web-/applikasjonsserver)
- API: Kun de metodene som skal være eksternt tilgjengelig
- Kode: Forretningslogikk
- Data: Kun tabeller

Riktig observert: Dette er #SmartDB

COMPARTMENTALIZATION



Least privileges hele veien

LEAST PRIVILEGES PRINCIPLE!

Oracle Database Security Guide: Oracle Database Security Guide: <https://docs.oracle.com/database/122/DBSEG/title.htm>


```
ALTER USER ... ACCOUNT LOCK;
```

REVOKE ... ANY ... FROM ...

Dette er ikke en komplett liste...

Kamil Stawiarski demonstrerte hvordan han kunne lese fra datafilene etter å ha jobbet videre fra et create any index-privilegie.
Et godt case for tablespace encryption?

SECURITY BY DESIGN

- SQL hører hjemme, innelåst i databasen, bak definerte PL/SQL-grensesnitt
- Unngå dynamisk SQL
 - Hvis dynamisk er et must, bruk `dbms_assert`
- Logging!

Logger: <https://github.com/OraOpenSource/Logger>

Log4PLSQL: <http://log4plsql.sourceforge.net>

HVA VI IKKE HAR SNAKKET OM

- Encryption
- Auditing
- Label security
- PL/Scope
- Alt det andre dere har: DW/BI, Splunk, Elasticsearch

BRUK GDPR

- Til å få tatt en grundig gjennomgang av systemene
- Rydd og kast
- Stram inn sikkerheten
- Endre adferd og prosedyrer
- Hev nivået!

HVA SKJER 25. MAI 2018?

Noen av disse vil neppe holde munnen lukket om de ikke får ut dataene sine.

KANSKJE IKKE SÅ MYE, MEN...

- Noen vil nok teste ut Right of Access og Right of Portability
- De vil ha dataene sine og kan finne på å si fra - høyt
- Tenk deg om når du utvikler funksjoner og formater for disse
- Tenk på hva du leverer ut av data
- Tenk på hvordan du leverer ut data
- Kan det misbrukes til å finne ut av interne strukturer?

Husk!

Jobben er ikke over 25. mai (eller 25. juni)

Husk at dette er et personverndirektiv: Én ting er å rydde opp, en annen er å sikre data mot fremtidige innbrudd.

Stay compliant!

or

stay trygda!

I'd like to do

Better Work

vidar@better-work.no

@nicetheoryvidar

nicetheory.io