COMMITTED TO ICT.
INVOLVED IN PEOPLE.

Wie ik ben

- Andre van Winssen
- >20 jaar aan het werk met oracle software
- Oracle database support, dba, security, OIAM
- Principal Consultant Amis, BC
- OCP from 7.3-11g, OCM 10g, 11g
- CISA (auditing), CISSP (security), CEH (ethical hacking)

TRAININGEN EN MASTERCLASSES

28 oktober 2011

Oracle Database 10g/11g Advanced Security door Andre van Winssen

Data veilig? Het kan beter….

Leer over de complete set aan security opties in Oracle databases

Advanced Security	Oracle Database Firewall	Applicatie Encryptie
Database Vault	Secure Application Roles	File encryptie (rman, DP)
Audit Vault	Oracle Label Security	Authenticatie en autorisatie
Data Masking	Virtual private databases	Auditing + FGA

Schrijf je in via www.amis.nl

It's all about

Context

OGH 4 oktober 2011

Context

De totale omgeving waarin iets zijn betekenis krijgt

"Dat is vet"

- jongeren onder elkaar
- op de diëetclub
- biologen en medici aan de snijtafel
- tijdens de afwas
- de chef-automonteur tegen zijn stagiair

Bron: wikipedia

In Oracle Context

- Applicatie Context, i.e. te gebruiken in applicaties
- Geheugen container met lees attributen
- Container is een “naamruimte” met benoemde attributen
- Attribuutnamen zijn uniek binnen naamruimte
- Verschillende attributen met dezelfde naam kunnen alleen bestaan in verschillende naamruimtes
- Naamruimte wordt gevuld middels een PLSQL package
  - of een policy functie
- Naamruimtes zijn onafhankelijk van elkaar

Oracle Context

```
create context mylocalcontext using mypackage;
```

- Naamruimte is mylocalcontext
- PLSQL package om naamruimte te vullen is mypackage
  - Hoeft niet te bestaan ten tijde van CREATE CONTEXT
- Elke poging buiten deze package om context attributen te zetten zal falen
  - `ORA-01031: insufficient privileges`

Mypackage heeft een procedure om context attributen te zetten.

Die procedure moet volgende aanroep doen:

```
dbms_session.set_context('<naamruimte>',<attr.naam>,<attr.waarde>)
```

Oracle Context

Gedefinieerde context bekijken:

select * from **dba_context** where namespace = 'MYLOCALCONTEXT' ;

```
NAMESPACE            SCHEMA          PACKAGE                    TYPE
-------------------- --------------- -------------------------- -----------------
MYLOCALCONTEXT       SYSTEM          MYPACKAGE                  ACCESSED LOCALLY
```

Oracle Context

Gezette context attributen in huidige sessie bekijken:

select * from session_context

```
NAMESPACE                      ATTRIBUTE                      VALUE
------------------------------ ------------------------------ -----------
MYLOCALCONTEXT                 MP                             Mark Rutte
```

Oracle Context
(toepassingen)

- Autoriseren van gebruikers vanuit connectie pool
- Beperken van toegang tot gegevens middels FGAC policies
  - Fine Grained Access Control
- Voor opzetten van FGA
  - Fine Grained Auditing
- Zetten van attribuutwaardes t.b.v. applicaties
  - Uitsparen van database lookups

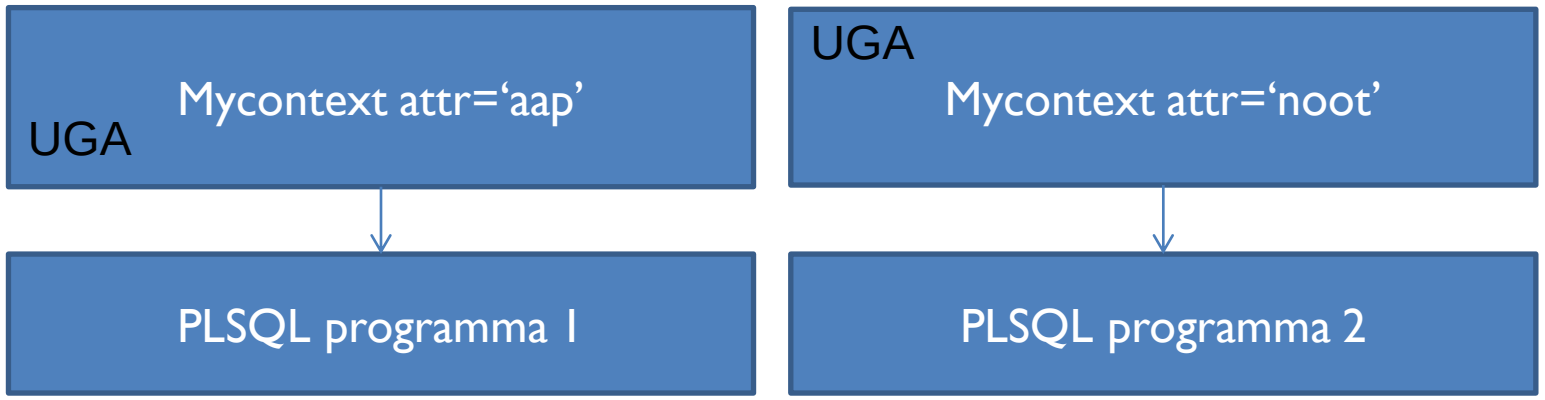
Oracle Context
(blikveld)

- Lokaal, alleen toegankelijk binnen sessie
  - State bewaard in UGA (niet afhankelijk van pga_aggregate_target)
  - Accessed locally

- Globaal, te gebruiken over sessies heen
  - State bewaard in SGA
  - Accessed globally

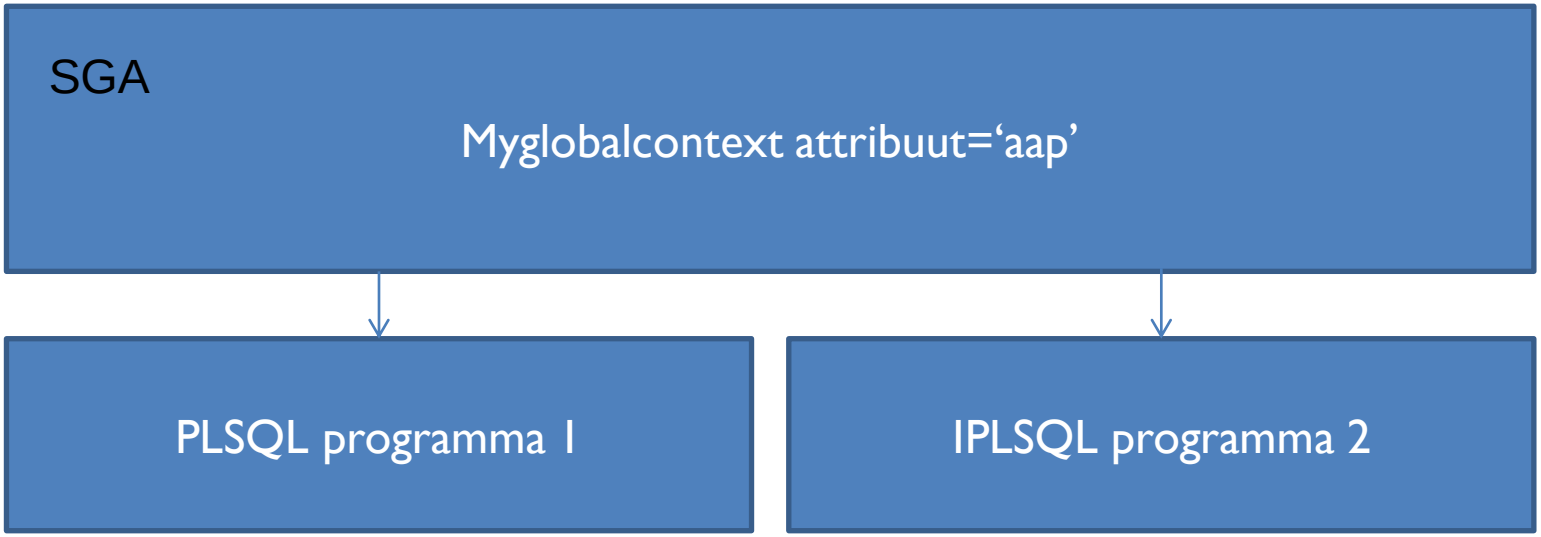
Oracle Context
(blikveld lokaal)

- `Create context mylocalcontext`
- P1: `dbms_session.set_context('mycontext','attr','aap')`
- P2: `dbms_session.set_context('mycontext','attr','noot')`
- fixed gedeelte van User Global Area (UGA)



Oracle Context
(blikveld globaal)

- `Create context myglobalcontext accessed globally`



Oracle Context
(blikveld globaal)

- Bewaren van globale applicatiewaardes
- Authenticeren (“herkennen”) van non-database gebruikers.
  - Connectie pool
  - Zelfde oracle login voor elke sessie
  - Individuele applicatiegebruiker onderscheiden dmv global context attribuut waarde


Oracle Context (initialisatie)

- Lokaal
  - Middels aanroepen naar dbms_session.set_context
- Extern
  - Vanuit OCI aanroep
  - Job queue
  - Database link (propageren van context attribuut waardes voor remote sessies)
- Globaal
  - Vanuit global context van een gebruiker's OID record
    - OracleDBAppContext object
    - SYS_LDAP_USER_DEFAULT namespace

Oracle Context
(opruimen)

- DBMS_SESSION

```
–  PROCEDURE CLEAR_CONTEXT
–   Argument Name                  Type                    In/Out Default?
–   ------------------------------ ----------------------- ------ --------
–   NAMESPACE                      VARCHAR2                IN
–   CLIENT_ID                      VARCHAR2                IN     DEFAULT
–   ATTRIBUTE                      VARCHAR2                IN     DEFAULT

–  PROCEDURE CLEAR_IDENTIFIER
```

- DEMO

Oracle Context
(meegeleverd)

- Ingebouwde context USERENV voor elke sessie te gebruiken
  - Bijna alle velden van [G]V$SESSION
    - 'authentication_method'
    - 'client_identifier'
    - 'current_schema'
    - 'host'
    - 'instance_name'
    - 'ip_address'
    - 'isdba'
    - 'os_user'
    - 'server_host'
    - 'session_user'
    - 'sid'

Oracle Context
(userenv)

```
select SYS_CONTEXT('USERENV','IP_ADDRESS') FROM DUAL;

SYS_CONTEXT('USERENV','IP_ADDRESS')
----------------------------------------------------------------
192.168.1.110
```

Oracle Context
(na installatie)

Hangt af van geinstalleerd subsysteem: OEM, CTX..

select * from dba_context;

NAMESPACE	SCHEMA	PACKAGE	TYPE
DR$APPCTX	CTXSYS	DRIXMD	ACCESSED LOCALLY
DBFS_CONTEXT	SYS	DBMS_DBFS_CONTENT_ADMIN	ACCESSED GLOBALLY
GLOBAL_AQCLNTDB_CTX	SYS	DBMS_AQJMS	ACCESSED GLOBALLY
REGISTRY$CTX	SYS	DBMS_REGISTRY_SYS	ACCESSED LOCALLY
EM_USER_CONTEXT	SYSMAN	SETEMUSERCONTEXT	ACCESSED LOCALLY
STORAGE_CONTEXT	SYSMAN	STORAGE_UI_UTIL_PKG	ACCESSED LOCALLY
LT_CTX	WMSYS	LT_CTX_PKG	ACCESSED LOCALLY

Secure application role
(analogie met application context)

- Gebruikt ook SYS_CONTEXT('USERENV',xxx) mechanisme
- Zet ook rol aan d.m.v. stored plsql procedure aanroep
- Database server controleert aanroep stack

Daarnaast:

- Voorwaarde voor aanzetten rol kan ook DBV rule set zijn
  - DBV=Database Vault

Secure application role
hoe werkt het

- Creeer de rol
  - `create role set_dba_role identified using beheer.set_secure_role_pkg`
  - Beheer.set_secure_role_pkg hoeft nog niet te bestaan t.t.v. create role
  - Database server controleert stack van aanroepen
- Creeer de package die de rol mag zetten
  - "create or replace procedure beheer.set_secure_role_pkg.."
- Geef execute privilege op deze procedure
  - `Grant execute on beheer.set_secure_role_pkg to eind / proxy gebruikers`
- Implementeer procedure beheer.set_secure_role_pkg
  - AUTHID CURRENT_USER is verplicht
  - In de procedure roep DBMS_SESSION.SET_ROLE aan

Voorbeeld procedure

```
CREATE OR REPLACE PROCEDURE beheer.set_secure_role_pkg
-- deze procedure controleert of aanroeper wel in het DBA VLAN
-- 10.240.250.0 zit tijdens de aanroep. Zo ja dan wordt de secure
-- application role DBA_ROLE aangezet voor de aanroeper, zo neen,
-- dan volgt slechts een entry in de audit trail voor deze poging
   AUTHID CURRENT_USER
 AS
  v_ipaddr varchar2(15);
BEGIN
  v_ipaddr := sys_context ('userenv','ip_address');
   IF v_ipaddr like '10.240.250.%'    -- bijvoorbeeld dba vlan
    THEN
     EXECUTE IMMEDIATE 'SET ROLE dba_role';
    ELSE
      paudit (..,v_ipaddr ,  sysdate,..);
END IF;
END;
```

Aanzetten Secure application role

- Geef de secure application role niet als default aan een user
  - Bijv: alter user andrevw default role all except sec_app_role
- Gebruik alleen de procedure genoemd in create role commando om rol te laten zetten
- Zorg voor auditing, je wilt misschien wel weten wie deze procedure onrechtmatig aanroept

View secure application roles

- Session roles
  - Roles die aan gezet zijn in huidige sessie
- Gedefinieerde rollen in Dba|all|user_application_roles
  - ROLE
  - SCHEMA
  - PACKAGE

```
SQL> create role set_dba_role identified using beheer.set_secure_role_pkg ;
Role created.
SQL> select * from dba_application_roles;
ROLE                 SCHEMA               PACKAGE
-------------------- -------------------- ------------------------------
SET_DBA_ROLE         BEHEER               SET_SECURE_ROLE_PKG
SQL>
```

Q&A

COMMITTED TO ICT.

INVOLVED IN PEOPLE.