

Neues, Altbewährtes und
Wissenswertes in der Version
12c



Bruno Cirone

Themenverantwortlicher Security

Wer ist Bruno Cirone?

- Oracle Erfahrung seit 1986
- Selbständig seit 1989
- Projekte im In- und Ausland.
- Oracle, Adabas-D (MAXDB), Unix, Linux
- Mitglied im Planungs-/Entwicklungsteam von Adabas-D
- Migrationen von verschiedenen DB-Herstellern nach Oracle
- Sehr viel Spaß an Oracle Herausforderungen
- www.cirone.de
- [Email: Bruno@Cirone.de](mailto: Bruno@Cirone.de)

Neues

- Auswahl der Neuerungen
 - Nur Neuerungen, die nicht extra lizenziert werden müssen
 - Mit vertretbarem (wenig) Aufwand umzusetzen
 - Neuerungen, die in allen Editionen vorhanden sind
 - Änderungen bei Rollen
- Nicht betrachtet werden
 - Transparent Data Encryption
 - Fine Grained Auditing
 - Database Vault
 - Data Redaction
 - Data Masking
 - Invokers Rights
 - usw.

Neues

- **SHA-2**

- Auch nutzbar mit `DBMS_CRYPTO`

- `SQLNET.ALLOWED_LOGON_VERSION_SERVER=11` 10G (Oracle), 11G (SHA-1), und 12C (SHA-2)
- `SQLNET.ALLOWED_LOGON_VERSION_SERVER=12` 11G (SHA-1) und 12C (SHA-2)
- `SQLNET.ALLOWED_LOGON_VERSION_SERVER=12a` 12C (SHA-2)

- `ORA-28040: No matching authentication protocol`

- **Der Default ist**

- `SQLNET.ALLOWED_LOGON_VERSION_SERVER=8` 10G (Oracle), 11G (SHA-1), und 12C (SHA-2)

Neues

- Das Privileg "SELECT ANY DICTIONARY" erlaubt keine Zugriffe mehr auf folgende Objekte
 - DEFAULT_PWD\$
 - ENC\$
 - LINK\$
 - USER\$
 - USER_HISTORY\$
 - XS\$VERIFIERS

Neues

- Die Rolle "Resource" hat kein Unlimited Tablespace Privileg mehr
- Letztes erfolgreiches Login
 - In der Tabelle USER\$ in der Spalte SPARE6
- Separation of Duty (SYSDBA, SYSOPER, SYSBACKUP, SYSDG, SYSKM)

Neues

- Neue Password Verify Function

- `$ORACLE_HOME/rdbms/admin/utlpwdmg.sql`
 - `verify_function_11G`
 - `ora12c_verify_function`
 - `ora12c_strong_verify_function`

- **Achtung !!!!** In dem Script wird am Ende folgender Befehl ausgeführt:

```
ALTER PROFILE DEFAULT LIMIT
PASSWORD_LIFE_TIME 180
PASSWORD_GRACE_TIME 7
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX UNLIMITED
FAILED_LOGIN_ATTEMPTS 10
PASSWORD_LOCK_TIME 1
PASSWORD_VERIFY_FUNCTION verify_function_11G;
```


Neues

Unterschiede der einzelnen Funktionen:

verify_function_11G

Passwordlänge von 8 bis 30 Zeichen

Unterscheidung zum vorherigen Password mindestens 3 Character

ora12c_verify_function

Passwordlänge von 8 bis 255 Zeichen

Unterscheidung zum vorherigen Password mindestens 3 Character

ora12c_strong_verify_function

Passwordlänge von 9 bis 255 Zeichen

Unterscheidung zum vorherigen Password mindestens 4 Character

Mindestens 2 Großbuchstaben

Mindestens 2 Kleinbuchstaben

Mindestens 2 Ziffern

Mindestens 2 Sonderzeichen

Neues

Kennen Sie diesen Befehl?

```
Grant Read on scott.emp to user_willi;
```

Oder nur diesen?

```
Grant Select on scott.emp to user_willi;
```

Bei „Grant Read“ sind folgende Befehle nicht mehr möglich!

```
LOCK TABLE Tabellen_Name IN EXCLUSIVE MODE;  
SELECT ... FROM Tabellen_Name FOR UPDATE;
```

Es gibt auch!

```
Grant Read any table to user_willi;
```

Neues

- Ab der Version 12.01.02 kann kein “Unmögliches Passwort“ gesetzt werden.
- Das Passwort muss “ Formal“ korrekt sein. D.h. Länge und HEX-Zeichen.

```
BCC> alter user Willi identified by values 'Invalid Password';
alter user Willi identified by values 'Invalid Password';
*
ERROR at line 1:
ORA-02153: invalid VALUES password string
BCC> alter user Willi identified by values 'ABACADAEAOA1A2A3';
User altered.
BCC>
```

Neues

- Unified Auditing Einstellung

```
Select value  
  from v$option  
 Where parameter='Unified Auditing';
```

TRUE =Nur Unified Auditing

FALSE=Mixed Betrieb (Altes und Neues Auditing)

- Sichern von Unified Auditing Einträgen

```
Create table Save_audit_trail as Select * from unified_audit_trail where 1=2;  
Insert into Save_audit_trail Select * from unified_audit_trail;
```

- Administration von Unified Auditing

- Tabellen sind alle nur "READ ONLY"
- Owner der Tabellen ist der User AUDSYS
- Administration nur mit dem Package DBMS_AUDIT_MGMT möglich
- Initialisierungsparameter UNIFIED_AUDIT_SGA_QUEUE_SIZE kann von 1MB (Default) bis zu 30M gesetzt werden.

Altbewährtes

- Verschlüsselung der Client/Server Verbindungen
 - Auf dem Server
 - `SQLNET.ENCRYPTION_SERVER=required`
 - `SQLNET.ENCRYPTION_TYPES_SERVER=(rc4_256,de40,...)`
 - Auf dem Client
 - `SQLNET.ENCRYPTION_CLIENT=accepted`

Wissenwertes

- Welcher Oracle-User hat ein Standard Passwort?

```
select *  
from dba_users_with_defpwd ;
```

```
USERNAME
```

```
-----
```

```
DIP
```

```
MDSYS
```

```
SYSTEM
```

```
SCOTT
```

```
usw.
```

Wissenswertes

- Was kann man damit auch noch machen?

```
SELECT distinct
  decode(b.user_name, a.username, 'Standard Oracle ', 'User') User_type,
  a.USERNAME,
  a.ACCOUNT_STATUS,
  a.EXPIRY_DATE
FROM dba_users a, SYS.default_pwd$ b
WHERE a.username = b.user_name (+)
order by user_type, username;
```

USER_TYPE	USERNAME	ACCOUNT_STATUS	EXPIRY_DATE
Standard Oracle	CTXSYS	EXPIRED & LOCKED	03.04.13
Standard Oracle	DBSNMP	EXPIRED & LOCKED	03.04.13
Standard Oracle	SYS	OPEN	
Standard Oracle	SYSTEM	OPEN	
User	BC	OPEN	
User	WILLI	EXPIRED & LOCKED	11.04.15

Fragen und Antworten

Hinweise

- SIG – Database-Day 16.03.2016
- SIG – Security-Day 17.03.2016

- Nächstes Webinar 12.02.2016
Oracle 12c Standard Edition Two Single Tenant Database

- Das Call for Papers DOAG-2016 Datenbank ist bis einschl. 08.01.2016 bis 24:00 Uhr offen, wird aber um einige Tage verlängert!

- Interview mit Dr. Günter Unbescheid bei DOAG.TV