Security!
Ja, sicher…

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-/Entwicklungteam von Adabas-D
- Migrationen von verschiedenen DB-Herstellern nach Oracle
- Sehr viel Spaß an Oracle Herausforderungen
- www.cirone.de
- Email: Bruno@Cirone.de

Anmerkungen

Dieser Vortrag ist kein Ersatz für eine Security-Schulung!

Probieren Sie alles zuerst auf einer Testdatenbank aus.

Neue Versionen haben „Neue“ Defaults.

Dokumentieren Sie Ihre Maßnahmen außerhalb der Datenbank.

Besuchen Sie regelmäßig Informationsveranstaltungen.

Umfassende Änderungen sollten von einem zweiten DBA geprüft werden.

Planen Sie auch die Rücknahme von Aktionen ein.

Thema

- Dieser Vortrag ist eine Auswahl an Securitythemen,
  - die nicht extra lizenziert werden müssen
  - die mit vertretbarem (wenig) Aufwand umgesetzt werden können
  - die in allen Editionen vorhanden sind
  - die Änderungen/Ersatz von Rollen beinhalten

- Nicht betrachtet werden
  - Transparent Data Encryption
  - Fine Grained Auditing
  - Database Vault
  - Data Redaction
  - Data Masking
  - Invokers Rights
  - Locked-Down Profiles
  - usw.

Themen

Gibt es noch Default-Passwörter?

Welche Konfigurationseinstellungen sollten vorgenommen werden?

Wie richte ich eine Verschlüsselung zwischen Client/Server ein?

Wo finde ich Security-Empfehlungen?

Was ist ein Smoke-Test (BSI-Grundschutz)?

Was mache ich mit den Audit-Informationen?

Wie richte ich eine Passwortvaldierung ein?

Gibt es noch Default Passwörter?

- Welcher Oracle-User hat ein Standard Passwort?

```
select *
from dba_users_with_defpwd ;

USERNAME
--------
DIP
MDSYS
SYSTEM
SCOTT
usw.
```

- Ein kleines Problem:

SYS and SYSTEM accounts are incorrectly listed in DBA_USERS_WITH_DEFPWD in 12c (Doc ID 2173962.1)

Gibt es noch Default Passwörter?

- 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    03.04.19
Standard Oracle DBSNMP     EXPIRED & LOCKED    03.04.19
Standard Oracle SYS        OPEN
Standard Oracle SYSTEM     OPEN
User            BC         OPEN
User            WILLI      EXPIRED & LOCKED    11.04.19
```

Weniger Rechte braucht die Datenbank!

- Standarduser sollten gesperrt und expired werden.

```
ALTER USER WMSYS PASSWORD EXPIRE ACCOUNT LOCK;
```

- Passwörter sollten geändert werden!
  - Eine Liste z.B. http://www.petefinnigan.com/default/default_password_list.htm
  - Einige Standarduser sind hoch privilegiert (z.B. create User, Create any table)

Beispiel

Der User WMSYS hat ein Standardpasswort bei der Installation.

Bei einem nicht gesperrten User WMSYS erhalten wir u.a. folgende Rechte.

```
PRIVILEGE
-------------------------
 ADMINISTER DATABASE TRIGGER
 ALTER ANY INDEX
 ALTER ANY PROCEDURE
 ALTER ANY TABLE
 ALTER ANY TRIGGER
 ALTER USER
 CREATE ANY INDEX
 CREATE ANY PROCEDURE
 CREATE ANY TABLE
 CREATE ANY TRIGGER
 CREATE ANY VIEW
 CREATE USER
 DELETE ANY TABLE
```

SYS oder SYSTEM

```
CREATE USER bcc_sys IDENTIFIED BY Willi_Wutz123;
GRANT DBA TO bcc_sys;

ALTER USER sys ACCOUNT LOCK;
ALTER USER system ACCOUNT LOCK;
```

Ein gesperrter User SYS kann sich immer noch mit "`/ as sysdba`" auf dem Server einloggen.

User/Rollen

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

Rollen/Rechte

- Das Privileg "`SELECT ANY DICTIONARY`" erlaubt keine Zugriffe mehr auf folgende Objekte

  - DEFAULT_PWD$
  - ENC$
  - LINK$
  - USER$
  - USER_HISTORY$
  - XS$VERIFIERS

Restricted DBA (Anwendungsdba)

- Erstellen Sie eine eigene DBA-Rolle mit wesentlich weniger Rechten!

  Welcher Anwedungsdba benötigt z.B. „`Alter System, Alter Database`“.

- Rolle DBA hat ca. 500 Rechte

- Restricted_DBA Rolle hat typischer weise ca. 20 – 50 Rechte

Grant Read

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;
```

Leider geändert

- Ab der Version 12.01.02 kann kein “Unmögliches Passwort“ mehr 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 'ABACADAEA0A1A2A3';
User altered.
BCC>
```

Konfiguration init.ora (spfile)

- Was sollte mindestens eingestellt werden?

```
Alter system set SEC_MAX_FAILED_LOGIN_ATTEMPTS=10        scope=spfile;
Alter system set SEC_PROTOCOL_ERROR_TRACE_ACTION=LOG     scope=spfile;
Alter system set sec_protocol_error_further_action=DELAY scope=SPFILE;
Alter system set SEC_RETURN_SERVER_RELEASE_BANNER=FALSE  scope=spfile;
Alter system set AUDIT_TRAIL=DB                          scope=spfile; -- oder OS
Alter system set AUDIT_SYS_OPERATIONS=TRUE               scope=spfile;
Alter system set sec_case_sensitive_logon=TRUE           scope=SPFILE;
Alter system set sql92_security=TRUE                     scope=SPFILE;
Alter system set open_links=0                            scope=SPFILE; -- Optional
Alter system set os_authent_prefix=RUL$                  scope=SPFILE; -- Optional
Alter system set utl_file_dir = ''                       scope=SPFILE; -- Ab 18c Directory-Object
```

Verschlüsselung

- 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`
- `ORA-03134: Connections to this server version are no longer supported`

  - Default < 12.2
- `SQLNET.ALLOWED_LOGON_VERSION_SERVER=`**`8`** 10G (Oracle), 11G (SHA-1), und 12C (SHA-2)

  - Default => 12.2
- `SQLNET.ALLOWED_LOGON_VERSION_SERVER=`**`12`**

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`

Auditing

- 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.

Auditing I

- Erstellen einer neuen Policy.

```
CREATE AUDIT POLICY bc_audit_policy ACTIONS DELETE ON bcc.x10,
                                            INSERT ON bcc.x10,
                                            UPDATE ON bcc.x10,
                                            SELECT ON bcc.x10
                                       WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') = ''BCC'''
                                    EVALUATE PER SESSION;
```

- Kontrolle ob diese Policy angelegt worden ist.

```
SELECT *
  FROM audit_unified_policies
 WHERE policy_name = 'BC_AUDIT_POLICY';
```

- Enablen der Policy.

```
AUDIT POLICY BC_AUDIT_POLICY;
```

- Ist die Policy Enabled?

```
SELECT *
  FROM audit_unified_enabled_policies
 WHERE policy_name = 'BC_AUDIT_POLICY';
```

Auditing II

- Was kann geaudited werden?

```
SELECT name
  FROM auditable_system_actions
 WHERE component = 'Standard'
 ORDER BY name;
```

- Deaktivieren der Policy.

```
NOAUDIT POLICY BC_AUDIT_POLICY;
```

- Löschen der Policy.

```
DROP AUDIT POLICY BC_AUDIT_POLICY;
```

- Kontrolle ob diese Policy nicht mehr vorhanden ist.

```
SELECT *
  FROM audit_unified_policies
 WHERE policy_name = 'BC_AUDIT_POLICY';
```

Auditing III

- Anzeige der Audit-Trail Records.

```
SELECT event_timestamp,  dbusername,  action_name,
       object_schema, object_name,  os_username,
       client_program_name, return_code,  sql_text
  FROM unified_audit_trail
 WHERE DBUSERNAME = 'BCC'
ORDER BY event_timestamp DESC;
```

- Löschen einer Audit Aktion.

```
ALTER AUDIT POLICY bc_audit_policy
      DROP ACTIONS
               SELECT ON bcc.x10;
```

- Hinzufügen einer Audit Aktion.

```
ALTER AUDIT POLICY bc_audit_policy
     ADD ACTIONS
               SELECT ON bcc.x10;
```

Login Trigger

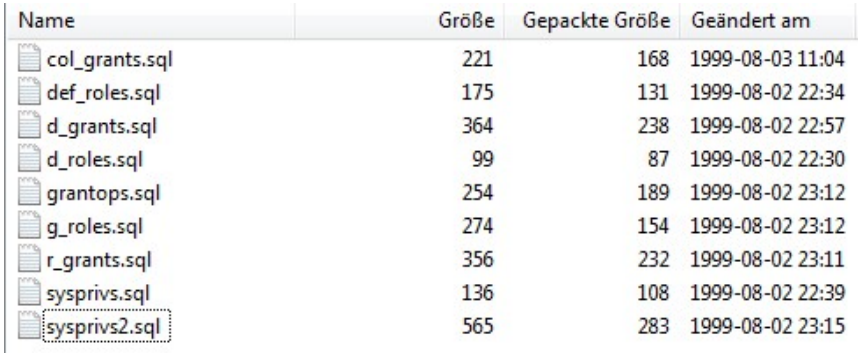
- Genauere Prüfung beim Login
  - Nur von 22:00 bis 6:00 Uhr
  - Nur von Montag bis Freitag
  - Nur von Programmen oder Modulen, die nicht sqlplus im Namen haben.
  - Und alle User außer WILLI

```
CREATE OR REPLACE TRIGGER SYSTEM.logon_trigger
    AFTER LOGON
    ON DATABASE
BEGIN
    IF    TO_NUMBER (TO_CHAR (SYSDATE, 'HH24')) BETWEEN 7 AND 21
       OR TO_CHAR (SYSDATE, 'D') IN (6, 7)
       OR UPPER (SYS_CONTEXT ('USERENV', 'CLIENT_PROGRAM_NAME')) LIKE  '%SQLPLUS%'
       OR UPPER (SYS_CONTEXT ('USERENV', 'MODULE')) LIKE '%SQLPLUS%'
       OR UPPER (SYS.LOGIN_USER) = 'WILLI'
    THEN
        RAISE_APPLICATION_ERROR (-20001, 'Nicht zu dieser Zeit, nicht zu diesem Tag, nicht mit sqlplus und Willi erst recht nicht');
    END IF;
END;
/
```

Smoke Test (BSI-Grundschutz)

Checkliste

Autor:	Carsten Mützlitz
Erstelldatum:	03.02.98
Letzte Änderung:	30.09.99
Kontrollnummer:	CHECK/IT-Grundschutz/001
Version:	1



Name	Größe	Gepackte Größe	Geändert am
col_grants.sql	221	168	1999-08-03 11:04
def_roles.sql	175	131	1999-08-02 22:34
d_grants.sql	364	238	1999-08-02 22:57
d_roles.sql	99	87	1999-08-02 22:30
grantops.sql	254	189	1999-08-02 23:12
g_roles.sql	274	154	1999-08-02 23:12
r_grants.sql	356	232	1999-08-02 23:11
sysprivs.sql	136	108	1999-08-02 22:39
sysprivs2.sql	565	283	1999-08-02 23:15

Pdf-Dokument:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Archiv/24_orcl_pdf.html

Scripte:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/SQL-Scripts-Oracle-Datenbanken.html

Smoke Test

- Dieser Security Check ist von einem Oracle Mitarbeiter (Carsten Mützlitz) erstellt worden.
  - Weiterführende Informationen sind in seinem Buch „*Oracle Security in der Praxis: Vollständige Sicherheitsüberprüfung für Ihre Oracle-Datenbank*“ enthalten.
- Es besteht hierfür kein Support und laufen „as it is“.
- Eine wesentlich erweiterte Version (dbsecrevunix.zip) ist mir von Oracle zur Verfügung gestellt worden.
- Im Gegensatz zu dem Toool DBSAT werden nur Daten gesammelt.
- Die entsprechenden Bewertungen müssen von den Administratoren vorgenommen werden.

DBSAT

Wird von Oracle kostenlos für Wartungskunden zur Verfügung gestellt.

Verschiedene Sprachen werden unterstützt.

Konfiguration kann geändert/erweitert werden.

Download / Data Sheet / FAQ:

https://www.oracle.com/de/database/technologies/security/dbsat.html

Beispiel:

https://apex.oracle.com/pls/apex/germancommunities/dbacommunity/tipp/6302/dbsat_pdb1_cdb3.html

CIS Center of Internet Security

- Sehr ausführliche Beschreibung (ca. 300 Seiten).

- Es beinhaltet:
  - Beschreibung des Parameters/Wertes etc.
  - Warum es ein Problem sein könnte?
  - Welche Einstellung sollte vorgenommen werden.
  - Welcher Befehl wird benötigt?
  - Die Referenzinformation zu diesem Sachverhalt.

- Download: https://learn.cisecurity.org/benchmarks

Invisible Column

- Hinzunehmen der Invisible Column mit Default Sysdate

```
ALTER TABLE SDGSTATUS  ADD (date_time  DATE INVISIBLE  DEFAULT sysdate) ;
```

- Erstellen des Update-Triggers

```
CREATE OR REPLACE TRIGGER SDGSTATUS_date_time
BEFORE UPDATE ON SDGSTATUS
FOR EACH ROW
BEGIN
    :new.date_time := sysdate;
END;
/
```

- Einen Update Faken

```
update SDGSTATUS     set funktion=funktion where sdgnr = '1234567890‘;
```

- Erstellen des jeweiligen Indexes

```
create index SDGSTATUS_BCI01     on SDGSTATUS(date_time)     tablespace TSTRNINDX;
```

- Abfrage aller Sätze, die vom Datum her größer ist als das Default Date.

```
select a.*, a.date_time from SDGSTATUS a where date_time > ( select min(date_time) from SDGSTATUS);
```

- Die Spalte date_time wird nur dann angesprochen und angezeigt, wenn Sie explizit angegeben wird.

Passwortprüfung

- 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
INACTIVE_ACCOUNT_TIME UNLIMITED
PASSWORD_VERIFY_FUNCTION ora12c_verify_function;
```

Passwortprüfung

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

DEMO

Differenz von alten und neuen Passwörtern

Verschlüsselte Passwörter können nicht verglichen werden.

Daher muss das alte Passwort eingegeben werden.

```
Alter user willi identified by Neupwd_123 replace Altpwd_124;
```

MOS-Note:

Password Verify Function Not Enforcing Difference Between Old

and New Passwords (Doc ID 816932.1)

Fragen und Antworten