Informix Technology Days 2026

Security & Informix



Manuel Müller
manuel.mueller@de.ibm.com

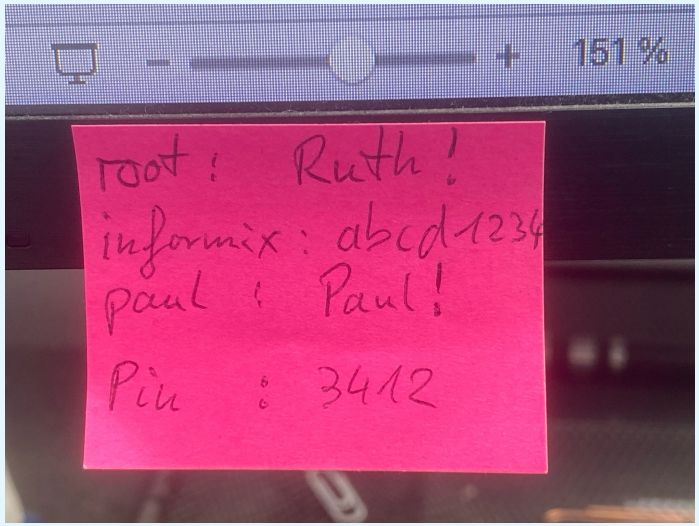
Gerd Kaluzinski
gerd.kaluzinski@de.ibm.com

Die Basis für Sicherheit …

- Sichere Passworte (complex und im PasswordSafe)
- Verbindungen zur Datenenbank immer als individual User
- Rechteverwaltung auf Tabellen und Prozeduren (ggf. Roles)
- Encryption at Rest (Daten auf Platte verschlüsselt abgelegt)
- Datenübertragung über SSL-Verbindungen
- Sicherungen verschlüsseln
- Sensitive Daten verschlüsseln (encrypt)
- …

Die Realität …

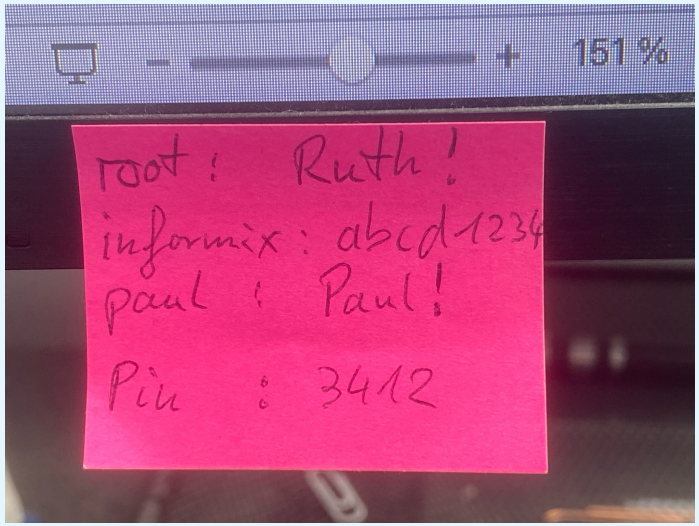
- Passworte finden sich oft am Bildschirmrand als POSTIT
- User “Informix” für alle Zugriffe
- “grant all to public” als Default
- Keine Verschlüsselung bei Transfer
- Sicherungen unverschlüsselt abgelegt
- Sensible Informationen im Klartext
- …



Die Realität …

- Passworte finden sich oft am Bildschirmrand als POSTIT
- User “Informix” für alle Zugriffe
- “grant all to public” als Default
- Keine Verschlüsselung bei Transfer
- …

STOP !!!



Wer sein System hier erkennt …

… IBM Expert Labs und unsere Partner können Ihnen helfen.

Sicherheit was können wir tun …

- Benutzerzugriffe ?
- Datenablage ?
- Datentransfer ?
- Sicherung ?
- Sensible Einträge verschlüsseln ?

Zugriffe überwachen

- Die POSTITs verschwinden >>> Password Safe nutzen
- User “Informix” nur für administrative Zugriffe erlauben
- Technische User nur für automatisierte Jobs
- Alle anderen Datenzugriffe nur mit individuellem User erlauben

Berechtigungen

- Als Umgebungsvariable NODEFDAC=yes setzen

  NODEFDAC = NoDefaultDistributAccess

- Bei bestehenden Datenbanken die Rechte für “public” entziehen
- Zugriffsrechte an “Rollen” (Tech, Sales, Finance, …) erteilen
- Die “Rollen” den Nutzern als “Default Role” zuordnen

>>> Nur noch bekannte User sind berechtigt

>>> Rechte werden zentral über Rollen und deren Zuordnung erteilt

Zugriffe überwachen

- AUDIT - Protokollieren der Aktivitäten durch onaudit
- GUARDIUM (IBM Guardium – Informix Connector)
  - Revisionssichere Protokollierung der Zugriffe
  - Rückverfolgung von Username zu LogName
  - Alarmierung bei Auffälligkeiten
  - Graphische Auswertung der Zugriffe und Datenflüsse
- Infosphere CDC (Change Data Capture)
  - Protokollierung aller Änderungen in einer externen

    “Audit Datenbank” mit Timestamp, User, Logname, …

Sicherheit im Überblick

- Benutzerzugriffe ✅
- Datenablage ❓
- Datentransfer ❓
- Sicherung ❓
- Sensible Einträge verschlüsseln ❓

Daten in DBSpaces auf Platte verschlüsseln

Die Daten der DBSpaces sind (mit etwas Geschick) lesbar.

```
1023104020 001  \0 220   F   8  \0  \0  \0 274  \a  \0  \0  \0  \0  \0  \0
1023104040  \0  \0  \0   *   K   a   l   u   z   i   n   s   k   i
1023104060                                  \0  \0  \0  \0  \0  \0  \0  \0
```

>>> Die Lösung: DISK_ENCRYPTION

Daten in DBSpaces verschlüsselt auf Platte

Dafür wird ein Keystore benötigt:

```
onkstore -create -file enc_test -type local -cipher aes256 -pw /DEMO/ENC/password_file


Creating a 'local' type keystore.
      Keystore file /opt/informix/etc/enc_test.p12 successfully created.
      Stash file /opt/informix/etc/enc_test.sth successfully created.
```

Zudem muss in der $ONCONFIG der Parameter gesetzt werden:

```
DISK_ENCRYPTION keystore=enc_test,cipher=aes256,rollfwd_create_dbs=encrypt
```

Daten auf Platte verschlüsseln

In der $ONCONFIG DISK_ENCRYPTION setzen

Neuanlage: oninit -ivy

Bestehende Instanzen mittels Restore:

ontape -r -encrypt

onbar -r -encrypt

Daten in DBSpaces verschlüsselt auf Platte

Die Daten sind nun sicher gegen unberechtigte Zugriffe:

```
1023000   Y   %   h   I  \n 205 246   4   s 031   " 313 340 300  \v 376
1023020 223 266   P 337   |   : 030 025   b 030 201   -   8 233 227 242
1023040   c 344 217 036 231 346   %   0 017 342   9 257   M 353   u   A
1023060 321 331  \b   8   +  \b   _  \0 246 201 346   b 306 344   2   _
```

onstat –d zeigt in den Flags (Flag E), ob ein DBSpace **E**ncryptet ist:

```
Dbspaces
address           number    flags      fchunk    nchunks   pgsize    flags    owner     name
45c3c030          1         0x10000001 1         1         2048      N  BAE   informix  rootdbs

    zum Vergleich unverschlüsselt:
address           number    flags      fchunk    nchunks   pgsize    flags    owner     name
45c3c030          1         0x1        1         1         2048      N  BA    informix  rootdbs
```

Sicherheit im Überblick

- Benutzerzugriffe ✅
- Datenablage ✅
- Datentransfer ❓
- Sicherung ❓
- Sensible Einträge verschlüsseln ❓

Client Server Datenaustausch verschlüsseln

Umstellung der Kommunikation auf SSL Verschlüsselung

Optionen: GsKit
OpenSSL (aber Version 14.10)

Voraussetzung:
Keystore erstellelle
SSL_KEYSTORE_LABEL in $ONCONFIG eintragen

Client Server Datenaustausch verschlüsseln

Sind diese Schritte erfolgt, so kann in der Datei $INFORMIXDIR/etc/sqlhosts eine ssl Verbindung eingetragen werden.

Beispiel:

```
ifx_ssl  onsocssl    kalu_test.ibm.com      9089
```

Zur Kontrolle kann der „onstat –g ntt“ verwendet werden:

```
onstat -g ntt | grep soc
47d60ca0 socssllst     7 10:43:29          kalu_test |9089|socssl
477cf590 soctcplst     6 10:43:29          kalu_test|9088|soctcp
```

Client Server Datenaustausch verschlüsseln

Für lokale Clients:

conssl.cfg in $INFORMIXDIR/etc mit Informationen zum

KeyStore (.p12)

Stash File (.sth)

Für Remote Clients:

client.p12 und client.sth in $INFORMIXDIR/ssl erstellen mit Informationen zum Zertifikat des Servers

Replikation verschlüsseln

Nutzung eines separaten Ports für die Replikation mit Option **s=6** (in sqlhosts) der nur Replikations Kommandos für CDR, HDR und RSS erlaubt .

Nutzung von **onpassword** für den Zugriff über den **Connection Managers** mittels verschlüsseltem Password.

Sicherheit im Überblick

- Benutzerzugriffe ✅
- Datenablage ✅
- Datentransfer ✅
- Sicherung ❓
- Sensible Einträge verschlüsseln ❓

Daten im Backup verschlüsseln

Auch wenn die Daten auf Disk verschlüsselt abgelegt sind, enthält eine Sicherung (ontape oder onbar) die Daten im Klartext:

```
117640140 001  \0 325 244   t  \0  \0  \0 200  \a  \0  \0  \0  \0  \0  \0
117640160  \0  \0  \0   *   K   a   l   u   z   i   n   s   k   i
117640200                                   I   B   M
117640220                                                   M 303 274   n
117640240   c   h   e   n
```

Daher sollte die Sicherung verschlüsselt erstellt werden.

ONCONFIG Parameter (für onbar und ontape):

BAR_ENCRYPTION keystore=enc_test,cipher=aes256

BACKUP_FILTER und **RESTORE_FILTER**

Sicherheit im Überblick

- Benutzerzugriffe ✅
- Datenablage ✅
- Datentransfer ✅
- Sicherung ✅
- Sensible Einträge verschlüsseln ❓

Sensible Daten verschlüsseln

Informix bietet die Funktionen encrypt() und decrypt() um Daten zu verschlüsseln.

```
set encryption password "Kalu knows the solution";
Encryption password set.

insert into encryption
select tabid, tabname, encrypt_aes(tabname)
from systables;

select *
from encryption order by 1;

          f1       f2          f3
          1  systables   0xDv/AAAAEAZNgwqJRJo2ol+bgHfrM+GCmgmiYI4Qyc
          2  syscolumns  04h3/AAAAEA0DDTpfzoouc4HbbhDryN6XTzjHn+eTmK
          3  sysindices  0zjH/AAAAEAb3CuqBeUpshoNy2JQDKDehH2+ydNTXbz

select f1, f2, decrypt_char(f3)
from encryption order by 1;

          f1 f2          (expression)
          1  systables   systables
          2  syscolumns  syscolumns
          3  sysindices  sysindices
```

Nur mit korrektem „encryption password“ wird der Inhalt angezeigt.

Individuellen Zugriff steuern

LBAC – Lable Based Access Control

Mittels LBAC kann der Zugriff sowohl auf Spalten, als auch Zeilen über individuelle Freigaben gesteuert werden.

Hierfür werden von einem SECADM die entsprechenden Label vergeben und die Zugriffe der User über Label gesteuert.

Sicherheit im Überblick

- Benutzerzugriffe ✅
- Datenablage ✅
- Datentransfer ✅
- Sicherung ✅
- Sensible Einträge verschlüsseln ✅

Fragen ?

?

Wieso ?

Weshalb ?

Warum ?

?

Damit ist es Zeit …



… dass der Alte Mann seinen Hut nimmt und Platz macht für die nächste Generation.

Vielen Dank!
Thanks a lot!

Manuel Müller
manuel.mueller@de.ibm.com

Gerd Kaluzinski
gerd.kaluzinski@de.ibm.com

