

## Willkommen zum „IBM Informix Newsletter“

### Inhaltsverzeichnis

Aktuelles.....	1
TechTipp: Neue Features in Version 12.10.xC8.....	2
TechTipp: DBSpace Encryption on Disk.....	3
TechTipp: ONCONFIG - DISK_ENCRYPTION.....	4
TechTipp: Aufbau einer Instanz mit Disk Encryption.....	5
TechTipp: onstat -d (Encryption Flag).....	7
TechTipp: Backup/Restore verschlüsselter DBSpaces.....	8
TechTipp: Backup encryption.....	10
TechTipp: Historie bei Aufrufen im „dbaccess“.....	11
TechTipp: Rename automatisch erstellter Indexe.....	12
TechTipp: oninit -S (Start der Instanz in Standard Mode).....	12
TechTipp: oninit -D (Start der Instanz ohne HDR und ER).....	12
TechTipp: oninit -t (Test).....	13
TechTipp: oninit -FILE (Datei mit Umgebungsvariablen zum Start).....	13
TechTipp: TimeSeries – InsSet() - Insert von MultiSet in TimeSeries.....	14
Hinweis: Einweihung Watson IoT Center München.....	16
Hinweis: INFORMIX auf der CeBIT (20.-24.März 2017).....	16
Hinweis: INFORMIX auf der Hannover Messe (24.-28.April 2017).....	17
Hinweis: INFORMIX Technologie Tag in München (16.Mai 2017).....	17
Versionsinfo: 12.10.xC8 / 12.10.xC8W1 ist verfügbar.....	17
Anmeldung / Abmeldung / Anmerkung.....	18
Die Autoren dieser Ausgabe.....	18

### Aktuelles

Liebe Leserinnen und Leser,

seit der letzten Ausgabe ist viel passiert. Mit Version 12.10.xC8 wurde die Verschlüsselung der abgelegten Daten auf Platte eingeführt. Das Sharding von Daten erhielt neue Optionen und viele weitere Features kamen hinzu.

Das „**IBM Watson IoT Center**“ in München wurde feierlich eröffnet und zeigt, dass Informix mit TimeSeries, JSON und Sharding auf dem richtigen Weg ist, sich als Datenbank für IoT zu etablieren.



Wie immer haben wir für Sie eine Reihe an Tipps und Tricks zusammengestellt.

Viel Spaß mit den Tipps der aktuellen Ausgabe.

Ihr TechTeam

## TechTipp: Neue Features in Version 12.10.xC8

Seit der letzten Ausgabe des Informix Newsletters wurde ein neues Release bereitgestellt, das eine Reihe interessanter Features enthält. Eine Auswahl dieser Features werden wir in dieser und den folgenden Ausgaben des Informix Newsletters näher vorstellen. Hier vorab schon einmal eine Zusammenfassung, was an Neuerungen auf Sie zukommt:

### Änderungen in der Datenablage, bzw. den Zugriffen

- **DISK\_ENCRYPTION** – Die verschlüsselte Ablage der Daten auf Platte
- **USE\_SHARDING** – Zugriff auf verteilte Daten ausführen
- **IFX\_LO\_READONLY** – Zugriff als „Read-Only“ über JDBC auf Large Objects

### Administration

- History Funktion in dbaccess um Aufrufe zu wiederholen

### JSON Kompatibilität

- Konsistente Ausführung bei sharded insert, update, und delete
- Komplexe Textsuche mit regulären Ausdrücken
- JSON Erweiterungen zur Kompatibilität

### Enterprise Replikation

- Konsistente Ausführung von sharded insert, update, und delete
- List Enterprise Replication definition commands

### Application development

- Umbenennung system-generierter Indices (z.B. Index eines Primary Keys)
- Informationen zur Nutzung von Temporären DBSpaces
- Suspendieren der Validierung bei Check Constraints
- JDBC 4.0 compliance
- JDBC-Query auf Smart Large Objects mit Read-Only Zugriff

### Sicherheit

- Encrypt storage spaces

### Time series

- Advanced analytics für Time Series Data
- Zusätzliche Time Series Funktionen

### Embeddability

- Einfachere Handhabung des ifxdeploy

## TechTipp: DBSpace Encryption on Disk

Der Datensicherheit wird mehr und mehr Aufmerksamkeit zuteil. Der Zugriff auf die Datenbanken mittels SQL lässt sich mit einer Reihe an Massnahmen einschränken. In früheren Ausgaben des Newsletters hatten wir ein Berechtigungsmanagement vorgestellt, das auf Benutzerrechten, Rollen und Default-Rollen basiert. Dies wird in vielen Fällen strikt gehandhabt und sichert das System gegen unerlaubten Zugriff im laufenden Betrieb.

Was bei den Betrachtungen oft vernachlässigt wird, ist der Umstand, dass die Daten unverschlüsselt auf der Platte liegen und hier ein unerlaubter Zugriff erfolgen könnte. Zwar sind die Chunks immer mit den Rechten 660 nur für den Benutzer „informix“ und die Gruppe „informix“ zugreifbar, aber dies ist keine absolute Sicherheit.

Ab Version 12.10.xC8 wurde als neues Feature die „Encryption on Disk“ eingeführt. Hierbei werden die Daten der DBSpaces auf der Platte verschlüsselt abgelegt. Bei der Implementierung wurde Wert auf die Benutzerfreundlichkeit gelegt, so dass es möglich ist, wahlweise einzelne DBSpaces zu verschlüsseln, oder alle DBSpaces verschlüsselt abzulegen. Mittels Backup und Restore lassen sich die bestehenden DBSpaces verschlüsseln und auch wieder entschlüsseln. Der benötigte Platz wird durch die Verschlüsselung nicht grösser, da die Daten-Pages in sich verschlüsselt werden.

In den folgenden Tipps wird gezeigt, wie eine Instanz mit Disk Encryption aufgebaut wird, wie eine bestehende Instanz verschlüsselt oder wieder entschlüsselt werden kann.

Wird eine Instanz mit Disk Encryption erstellt, so wird gleichzeitig im Verzeichnis \$INFORMIXDIR/etc die KeystoreDB mit dem gewählten Namen erstellt.

Werden mehrere Instanzen betrieben, so muss für jede Instanz ein anderer KeyStore mit unterschiedlichem Namen gewählt werden, damit sich diese nicht gegenseitig beeinflussen. Eine gemeinsame Nutzung ist nicht möglich. Sollen SDS Server eingesetzt werden, muss der KeyStore auf alle beteiligten Server kopiert werden.

Da auch Logical Log und Physical Log geänderte Daten enthalten, sollte bei der Entscheidung nur die DatenDBSpaces zu verschlüsseln auch dieser Bereich mit berücksichtigt werden.

## TechTipp: ONCONFIG - DISK\_ENCRYPTION

Um das Feature der Disk Encryption zu nutzen, muss in der ONCONFIG der Instanz der zusätzliche Parameter DISK\_ENCRYPTION eingetragen werden. Dieser ist nicht in der onconfig.std enthalten. Als Wert wird der Name der KeyStoreDB gesetzt, die genutzt werden soll. In unserem Fall ist dies „ifx“. Als Verschlüsselung stehen folgende „cipher“ zur Auswahl:

- aes128 = Default. Advanced Encryption Standard cipher with 128-bit keys.
- aes192 = Advanced Encryption Standard cipher with 192-bit keys.
- aes256 = Advanced Encryption Standard cipher with 256-bit keys.

Für DBSpaces, die während des Recovery (z.B. beim Einspielen eines Level-1-Archiv oder von Logs) erstellt werden, kann mittels „rollfwd\_create\_dbs“ bestimmt werden, ob diese verschlüsselt angelegt werden sollen oder nicht (Der Default ist die Verschlüsselung des Rootdbs):

- encrypt = Encrypt the newly created storage space
- decrypt = Do not encrypt the newly created storage space

Für unser Beispiel (mit KeyStoreDB ifx) setzen wir den Parameter auf:

**DISK\_ENCRYPTION ifx,cipher=aes256,rollfwd\_create\_dbs=encrypt**

Der Parameter ist nicht dynamisch änderbar, so dass ein Neustart der Instanz zum Ändern notwendig ist.

### WICHTIG:

Die Datei der KeyStoreDB muss separat gesichert werden und ist weder in einer Vollsicherung, noch in der Sicherung der „critical files“ des „onbar“ enthalten. Da mit Hilfe dieses KeyStore die Datenbank jederzeit entschlüsselt werden kann, empfiehlt es sich, \$INFORMIXDIR und die DBSpaces nicht auf der selben Platte zu speichern.

Geht die KeyStoreDB verloren, ist ein Zugriff auf den Datenbestand nicht mehr möglich.

## TechTipp: Aufbau einer Instanz mit Disk Encryption

Ist vor der Initialisierung der Instanz der Parameter DISK\_ENCRYPTION in der ONCONFIG gesetzt, so kann die Instanz verschlüsselt initialisiert werden. Dies geschieht mit dem bekannten Befehl

„**oninit -ivy**“, der voraussetzt, dass in der \$ONCONFIG der Parameter FULL\_DISK\_INIT auf 1 steht.

Die Ausgabe und das „online.log“ enthält dann zusätzliche Informationen zur Verschlüsselung:

```
¼
Initializing Dictionary Cache and SPL Routine Cache...succeeded
Initializing encryption-at-rest if necessary...succeeded
Initializing encryption-at-rest structures (part 1)...succeeded
Bringing up ADM VP...succeeded
  Creating VP classes...succeeded
Forking main_loop thread...succeeded
Initializing DR structures...succeeded
Forking 1 @soctcp@ listener threads...succeeded
Starting tracing...succeeded
Initializing 8 flushers...succeeded
Clearing encrypted root chunk 1 before initialization...
25% done.
50% done.
75% done.
100% done.
Initializing encryption-at-rest structures (part 2)...succeeded
Initializing log/checkpoint information...succeeded
¼
```

Da es sich bei dem verwendeten Bereich des DBSpaces um einen bereits zuvor beschriebenen Sektor handeln könnte, wird vor der Erstellung zuerst der gesamte Bereich gelöscht (clearing).

In den reservierten Seiten des Rootdbs stehen Details zur Verschlüsselung:

```
Database system flags          0x39
Encryption-at-rest is enabled using cipher @aes256@
64-bit server
BigChunk page flags are not in use
The ROOT Dbspace is encrypted
```

Eine Instanz mit verschlüsselten DBSpaces kann nur gestartet werden, wenn die KeyStoreDB für die Entschlüsselung vorhanden ist.

Wird eine Instanz mit verschlüsselten DBSpaces ohne den ONCONFIG-Parameter DISK\_ENCRYPTION gestartet (und ist kein Keystore mit dem Default Namen „ifx\_keystore“ in \$INFORMIXDIR/etc vorhanden), so wird folgende Fehlermeldung ausgegeben und der Start schlägt fehl:

**11:26:14 Unable to open the Encryption Key Database, errno GSKKM\_ERR\_NULL\_PARAMETER.**

**(/opt/informix\_12.10.FC8AEE/etc/ifx\_keystore.p12)**

**11:26:14 Initialization of encryption subsystem failed with error 21548.**

**11:26:14 oninit: Fatal error in shared memory initialization**

**11:26:14 IBM Informix Dynamic Server Stopped.**

Ist die KeyStoreDB abhanden gekommen, hilft auch kein Support weiter. Dann bleibt nur der Restore aus einem Backup, zu dem der Zugang vorhanden ist. Da das Backup unabhängig von der KeyStoreDB ist, benötigt man hier nur die Information ob und wie ggf. das Backup verschlüsselt wurde.

Hinweis:

Die Daten im Memory sind auch bei einer Instanz mit Disk Encryption nicht verschlüsselt. Ein Memory Dump könnte daher Daten im Klartext preisgeben.

## TechTipp: onstat -d (Encryption Flag)

Die Ausgabe des „onstat -d“ zeigt, ob ein DBSpace verschlüsselt angelegt wurde oder nicht. Eine Verschlüsselung wird im sechsten Parameter als „E“ angezeigt.

Im folgenden Beispiel wurden die DBSpaces „datadbs2“ und „tmp2dbs“ unverschlüsselt erstellt, wohingegen die anderen DBSpaces verschlüsselt sind. Am Beispiel ist zu sehen, dass sich die Verschlüsselung auf alle Arten von DBSpaces anwenden lässt.

```
onstat -d
IBM Informix Dynamic Server Version 12.10.FC8W1 -- On-Line -- Up ¼
  Dbspaces
address      number flags      fchunk nchunks  pgsize  flags      owner      name
4648e028     1      0x10020001 1        1      2048     N BAE      informix  rootdbs
46619c50     2      0x10028001 2        1      2048     N SBAE     informix  sbdbs
63e76b80     3      0x10020001 3        1      2048     N BAE      informix  datadbs
6364bb90     4      0x20001    4        1      2048     N BA       informix  datadbs2
63854b90     5      0x10002001 5        1      2048     N TBAE     informix  tmpdbs
63854dd0     6      0x2001    6        1      2048     N TBA      informix  tmp2dbs
```

Nun können wir testen, was die Verschlüsselung auf Plattenebene bewirkt:

In den DBSpaces „datadbs“ und „datadbs2“ wird jeweils eine einfache Tabelle mit einer Spalte vom Typ Char(18) angelegt und mit den Werten "**Carmen**", "**Carina**" und "**Inja**" gefüllt.

Die Suche im verschlüsselten „datadbs“ auf Platte ergibt:

```
$ od -c datadbs
      # Hier sind keine verwertbaren Informationen zu finden.
      # Auch leere Bereiche werden mit nicht wiederholenden Mustern gefüllt
0010520 321 220 . 224 300 213 026 004 034 177 J 240 $ 322 234 202
0010540 211 8 017 025 L 267 316 205 b Y 003 , 207 312 266 277
0010560 + 016 346 w 326 374 375 371 F \t 245 ( 002 3 z r
0010600 220 ; 266 240 X = ( 350 036 \r \0 274 : x 003 016
0010620 370 : \t U 226 s 003 V 016 304 024 213 034 X 325 y
```

Wird die selbe Suche auf dem unverschlüsselten „datadbs2“ ausgeführt, so sind die Einträge schnell aufzufinden:

```
$ od -c datadbs2
      # Die suche nach den Namen ist erfolgreich:
...
16040020 \0 \0 \0 \0 \0 \0 \0 \0 C a r m e n
16040040      C a r i n a      I n j a
16040060      \0 \0 \0 \0 \0 \0 \0 \0 \0 \0
```

Im verschlüsselten DBSpace sind auf Platte keine wiederkehrenden Muster erkennbar, so dass ein Auslesen von Daten von Platte nicht mehr möglich ist.

## TechTipp: Backup/Restore verschlüsselter DBSpaces

Das Backup einer Datenbankinstanz ist immer unverschlüsselt. Soll auch diese externe Sicherung verschlüsselt erfolgen, so kann dies z.B. mit Hilfe des BACKUP\_FILTERS implementiert werden (siehe folgenden Artikel „Backup encryption“).

Bei einem Restore ist entscheidend, ob der Parameter DISK\_ENCRYPTION in der \$ONCONFIG gesetzt ist, und auf einen existierenden Keystore verweist. Ist dies der Fall, so werden als Default alle DBSpaces verschlüsselt angelegt. Ist kein Keystore angegeben, so erfolgt der Restore unverschlüsselt.

Mit dem Parameter „-encrypt“ bzw. „-decrypt“ kann das Defaultverhalten übersteuert werden.

Während des Restore versucht der Server die Dateien <keystore>.p12 und <keystore>.sth im Verzeichnis \$INFORMIXDIR/etc zu erstellen. Sind diese bereits vorhanden, so müssen diese vor einem verschlüsselten Restore explizit gelöscht werden.

Das folgende Beispiel zeigt die Ausgaben in einer derartigen Fehlersituation:

```
ontape -r -encrypt
Continue restore? (y/n)y
Do you want to back up the logs? (y/n)n
One or both of the Encryption Key Database
    (/opt/informix_12.10.FC8AEE/etc/ifx.p12)
or Encryption Key Stashfile
    (/opt/informix_12.10.FC8AEE/etc/ifx.sth)
already exists. Because this is a complete
initialization of
the IBM Informix server they must not already exist.
Remove the file(s) manually or set the FULL_DISK_INIT
onconfig
Physical restore failed - InitKeystore failed
    parameter to remove the files automatically.Creation of
encryption key database failed: GSKKM_ERR_DATABASE_ALREADY_EXISTS
(/opt/informix_12.10.FC8AEE/etc/ifx.p12)
Program over.
```

Bei einem erfolgreichen Restore mit Verschlüsselung werden alle DBSpaces (auch TempSpaces) vor dem Restore geleert, damit keinerlei lesbare „Altdateien“ in den Plattenbereichen zu finden sind. Daher kann ein verschlüsselter Restore einer grossen Instanz einige Zeit länger dauern als ohne Verschlüsselung.

Im folgenden Beispiel sind die Ausgaben zu sehen, die bei einem verschlüsselten Restore in das Message Log geschrieben werden:

```
14:40:15 IBM Informix Dynamic Server Version 12.10.FC8W1 Software
Serial Number AAA#B000000
14:40:17 IBM Informix Dynamic Server Initialized -- Shared Memory
Initialized.
...
14:40:17 Encryption-at-rest is enabled using cipher @aes128@
...
14:40:18 Physical Restore of rootdbs, enc_test1, datadbs,
datadbs2, datadbs1, ten1data, ten2data, log1dbs, enc_not_test2,
sdbdbs, ten1sb, ten2sb started.
...
14:40:18 Clearing encrypted chunk 14 before restoring log
pages...
14:40:20 Clearing encrypted chunk 2 before restore...
14:40:21 Clearing encrypted chunk 3 before restore...
14:40:44 Clearing encrypted chunk 6 before restore...
14:40:53 Clearing encrypted chunk 7 before restore...
14:41:04 Clearing encrypted chunk 8 before restore...
...
14:41:22 Physical Restore of rootdbs, enc_test1, datadbs,
datadbs2, datadbs1, ten1data, ten2data, log1dbs, enc_not_test2,
sdbdbs, ten1sb, ten2sb Completed.
14:44:09 No logical log restore will be performed.
14:44:09 Clearing the physical and logical logs has started
14:44:12 Cleared 124 MB of the physical and logical logs in 2
seconds
14:44:12 Physical Recovery Started at Page (1:10031).
14:44:12 Physical Recovery Complete: 0 Pages Examined, 0 Pages
Restored.
14:44:12 Clearing encrypted primary chunk 5 before
initialization...
14:44:13 Clearing encrypted primary chunk 10 before
initialization...
14:44:15 Logical Recovery Started.
14:44:15 10 recovery worker threads will be started.
14:44:16 Logical Recovery has reached the transaction cleanup
phase.
14:44:16 Logical Recovery Complete.
0 Committed, 0 Rolled Back, 0 Open, 0 Bad Locks
```

Die DBSpaces mit Chunk 5 und Chunk 10 sind TempSpaces und werden daher nach dem Recovery initialisiert.

## TechTipp: Backup encryption

Nachdem wir im vorhergehenden Artikel gesehen haben, wie die Daten auf Platte verschlüsselt abgelegt werden können, ist das Backup der nächste logische Schritt, bei dem eine sichere Verschlüsselung gegen fremde Zugriffe sinnvoll ist.

Hierzu gibt es zwei unterschiedliche Ansätze:

- Using Pipe mit externer Verschlüsselung (nur bei ontape)
- Using Filters mit Verschlüsselung durch die Instanz (ontape und onbar)

Die externe Verschlüsselung mittels Backup nach Standard Out und anschließender Verschlüsselung kann z.B. mittels folgendem Befehl erfolgen:

```
$ ontape -s -L 0 -t STDIO | openssl enc -e -des3 -salt -out backup.enc
```

Der Restore benötigt dann eine Entschlüsselung der Daten und erfolgt dementsprechend über die Schnittstelle von Standard In.

```
$ openssl enc -d -des3 -salt -in backup.enc | ontape -r -t STDIO
```

Die Verschlüsselung mittels BACKUP\_FILTER wird weit häufiger genutzt. Hierbei muss zuerst ein Schlüsselpaar aus Public und Private Key angelegt werden:

```
$ openssl req -x509 -nodes -days 1461 -newkey rsa:2048 -keyout backup.pem  
-subj "/C=BY /L=Lindau/O=IT/CN=www.example.com" -out backup.pem.pub
```

Anschließend werden in der Datei \$ONCONFIG die Werte für die Verschlüsselung als Parameter der Filter eingetragen:

```
BACKUP_FILTER "/usr/bin/openssl smime -encrypt -des3 -binary -outform DEM  
/home/informix/ids1210fc8/ssl/backup.pem.pub"
```

```
RESTORE_FILTER "/usr/bin/openssl smime -decrypt -des3-binary -inform DEM -inkey  
/home/informix/ids1210fc8/ssl/backup.pem"
```

Nach einem Neustart sind alle Sicherungen, die mittels „ontape“ oder „onbar“ erstellt werden, verschlüsselt.

## TechTipp: Historie bei Aufrufen im „dbaccess“

Der „dbaccess“ ist weiterhin eines der meist genutzten Interfaces für die Administration der Informix Datenbank. Benutzer anderer Datenbanken lächeln oft über dieses Tool, da es weder „bunt“ noch mit der Maus zu steuern ist. Was für den „dbaccess“ spricht, ist die Nähe zum Datenbank Server und die einfache Handhabung um SQL-Skripts auszuführen.

Dass der „dbaccess“ auch bei den Entwicklern nicht abgeschrieben ist, zeigt dieses neue Feature, das eine History Funktion für bisher abgesetzte Befehle bietet. Da ein Beispiel die Funktion besser erklärt als viele Worte, stellen wir die Nutzung hier vor:

**dbaccess -history - -**

Der Befehl „-history“ aktiviert die Historisierung von Aufrufen  
Befehle müssen mit dem Semikolon abgeschlossen werden

**1> database stores;**

Jedes Kommando erhält eine eindeutige Befehlsnummer

**Database selected.**

**2> select count(\*) from systables;**

**(count(\*))**

**73**

**1 row(s) retrieved.**

**3> select first 1 \* from systables;**

<b>tabname</b>	<b>systables</b>
----------------	------------------

<b>owner</b>	<b>informix</b>
--------------	-----------------

**...**

**1 row(s) retrieved.**

**4> history;**

History listet die bisherigen Befehle mit Befehlsnummern auf

**1 database stores**

**2 select count(\*) from systables**

**3 select first 1 \* from systables**

**4> run 2;**

Um einen Befehl erneut aufzurufen, reicht die Angabe von „run <Befehlsnummer>“

**(count(\*))**

**73**

**1 row(s) retrieved.**

## TechTipp: Rename automatisch erstellter Indexe

Automatisch erstellte Indexe, die z.B. beim Erstellen eines Primary Key Constraints entstehen, haben als Namen ein führendes Leerzeichen, gefolgt von der Tabid, einem Underscore und der eindeutigen Constraint-ID. Ein Rename dieser Indexe war bisher sehr schwierig und konnte nur mit Hilfe der Einstellungen für „DELIMIDENT“ erfolgen.

Mit Version 12.10.xC8 können diese Indexe einfach umbenannt werden, und das System erkennt welcher Index gemeint war, auch wenn kein führendes Leerzeichen angegeben wurde.

Beispiel:

Der Index " 100\_1", der in der Datenbank Stores zum Primary Key der Tabelle „customer“ gehört, soll in „customer\_idx1“ umbenannt werden:

```
RENAME INDEX 100_1 TO customer_idx1;
```

Es ist auch möglich, den Owner mit anzugeben, wie das folgende Beispiel zeigt:

```
RENAME INDEX kalu.100_1 TO customer_idx1;
```

## TechTipp: oninit -S (Start der Instanz in Standard Mode)

Soll ein Datenbank Server, der vor dem Shutdown in einem HDR Verbund aktiv war, als „StandAlone“ im Standard-Mode gestartet werden, so kann dies mittels

```
„oninit -S“
```

erfolgen.

Die Replikation ist damit beendet und muss bei Bedarf neu aufgesetzt werden.

## TechTipp: oninit -D (Start der Instanz ohne HDR und ER)

Soll ein Datenbank Server ohne Replikation gestartet werden, so kann dies mittels

```
„oninit -D“
```

erfolgen.

Ist für den Server eine Enterprise Replikation definiert, so kann diese anschliessend mittels „cdr start“ aktiviert werden. Eine HDR Replikation kann nicht wieder gestartet werden.

## TechTipp: oninit -t (Test)

Diese Option des „oninit“ dient dazu, Fehler in der Konfiguration ohne expliziten Start zu erkennen und zu beheben. Dies ist z.B. dann sinnvoll, wenn nach einem Totalausfall die gesamte Installation neu erstellt und eine gesicherte Konfiguration eingespielt werden musste.

Die Ausgabe zeigt die erkannten Konfigurationsparameter:

### Configuration Parameter List

ID	name	current value
0	ROOTNAME	rootdbs
1	ROOTPATH	./rootdbs
2	ROOTOFFSET	0
3	ROOTSIZE	300000
4	MIRROR	0
5	MIRRORPATH	
6	MIRROROFFSET	0
7	DBSERVERNAME	test
8	DBSERVERALIASES	
9	SERVERNUM	100

¼

## TechTipp: oninit -FILE (Datei mit Umgebungsvariablen zum Start)

Mit dieser Option kann eine Informix Instanz mit Umgebungsvariablen aus einer Konfigurationsdatei gestartet werden. Die Umgebungsvariablen müssen dabei im Format

```
#$<variable> <wert>
```

in der Datei eingetragen sein.

Beispiel:

**envconfig.kalu**

```
# *** Start environment settings for kalu42
#
#$INFORMIXSERVER kalu42
#$DBDATE DMY4.
#$SERVER_LOCALE en_us.utf8
#
# *** End environment settings for kalu42
```

Aufruf:

```
oninit -FILE=envconfig.kalu
```

## TechTipp: TimeSeries – InsSet() - Insert von MultiSet in TimeSeries

Ein Leser hat uns gebeten zum Insert eines MultiSets in eine Zeitreihe Beispiele zu liefern. Dieser Anfrage kommen wir gerne nach.

Die TimeSeries Funktion InsSet erwartet als Argument eine TimeSeries, ein Multiset und ein Flag (Default 0). Das Flag stellen wir zum Test auf 256 (reduce log). Der Rückgabewert dieser Funktion ist wiederum eine TimeSeries.

Zuerst erstellen wir eine Datenbank für den Test:

```
create database if not exists test42 in datadbs with log;
```

Für die TimeSeries benötigen wir einen RowType:

```
create row type r_test42 (
    timestamp datetime year to fraction(5),
    value decimal(16,5),
    flag int
);
```

Um die Daten speichern zu können, benötigen wir noch einen Containerer:

```
execute procedure
TSContainerCreate("cont_test42","datadbs","vals_test42",40000,40000);
```

Nun können wir die Tabelle mit der TimeSeries erstellen:

```
create table if not exists tab_test42 (
    id int,
    vals_test42 timeseries(r_test42)
);
```

und die TimeSeries initialisieren:

```
insert into tab_test42 values (
    42,
    TSCreate(@ts_lmin@,@2017-01-01 00:00:00.00000@,
    10000,0,1000, @cont_test42@)
);
```

Nach diesen Vorbereitungen können Werte in die TimeSeries Tabelle eingetragen werden. Dies kann bei Einzelwerten über den Befehl PutElem() erfolgen:

```
UPDATE tab_test42 SET vals_test42 = PutElem (vals_test42,
    row(@2017-01-06 21:00:00.00000@,3.22570,0)::r_test42,256)
WHERE id = 42 ;
```

Liegen die Werte in Form eines MultiSet vor, so können diese über InsSet eingetragen werden:

```
UPDATE tab_test42 SET vals_test42 = InsSet(vals_test42,MULTISET{
    row("2017-01-06 21:00:00.00000",3.22570,0)::r_test42,
    row("2017-01-06 21:01:00.00000",3.22571,0)::r_test42,
    row("2017-01-06 21:02:00.00000",3.22572,0)::r_test42,
    row("2017-01-06 21:03:00.00000",3.22573,0)::r_test42,
    row("2017-01-06 21:04:00.00000",3.22574,0)::r_test42,
    row("2017-01-06 21:05:00.00000",3.22575,0)::r_test42,
    row("2017-01-06 21:06:00.00000",3.22576,0)::r_test42,
    row("2017-01-06 21:07:00.00000",3.22577,0)::r_test42,
    row("2017-01-06 21:08:00.00000",3.22578,0)::r_test42,
    row("2017-01-06 21:09:00.00000",3.22579,0)::r_test42,
    row("2017-01-06 21:10:00.00000",3.22580,0)::r_test42,
    row("2017-01-06 21:11:00.00000",3.22581,0)::r_test42},256)
WHERE id = 42 ;
```

Multisets können auch das Ergebnis der Abfrage einer Tabelle ohne Angabe der Spalten sein.

Beispiel:

```
select systables from systables
```

```
systables ROW(©systables©,©informix©,4195839,1 ,500,26,2,
139.0000000000,©01.07.2014©,65609, ©T©,©R©,12.0000000000,
16,16,0,NULL,NULL,0 ,0,2048,©2017-02-06 14:02:43.30461©,
0 ,© ©,NULL,© ©)
```

```
systables ROW(©syscolumns©,©informix©,4194338,2 ,157,10,2,
932.0000000000,©01.07.2014©,65609 ,©T©,©R©,21.0000000000,
16,16,0,NULL,NULL,0 ,0,2048,©2017-02-06 14:02:43.56406©,
0 ,© ©,NULL,© ©)
```

¼

## **Hinweis: Einweihung Watson IoT Center München**

Am 15. Februar wurde in München das IBM Watson IoT Center eingeweiht. Damit ist eine der weltweit führenden Forschungseinrichtungen für zukünftige Technologien in Bayern angesiedelt. Das Zusammenspiel von BigData, Internet of Things und Watson bringt eine Vielzahl an neuen Möglichkeiten. Mit seinen Stärken im Bereich IoT und BigData ist Informix ein wichtiger Teil, der zum Erfolg der neuen Technologien beiträgt. Erste Projekte sind bereits erfolgreich gestartet, viele weitere Neuerungen werden folgen.

Wer mehr wissen möchte, der sollte sich über die den folgenden Link mehr Informationen zu IBM Watson ansehen:

<http://www.ibm.com/de/watson/>

## **Hinweis: INFORMIX auf der CeBIT (20.-24.März 2017)**

Auf der diesjährigen CeBIT ist Informix in zahlreichen ShowCases eingebunden. Auch wenn im ersten Moment nicht INFORMIX als Beschriftung am Stand angebracht ist, besteht der Kern vieler der gezeigten Anwendungen aus einer Informix Datenbank, die über TimeSeries, JSON oder eines der anderen neuen Features zur Leistungsfähigkeit der Lösung beiträgt.

Sie finden INFORMIX auf der CeBIT z.B. an folgenden Ständen:

**Demopunkt Nr. 33: Creating Smart Buildings with IoT**

**Demopunkt Nr. 24: Greencom: Analytics at the Edge**

**Demopunkt Nr. 23: G&H Bankensoftware ("Bancos")**

**Genius Bar (Data Server)**

Kommen Sie bei uns vorbei und lassen Sie sich über die Möglichkeiten informieren, die Informix im IoT-Umfeld bietet.

Haben Sie spezielle Fragen ? Dann senden Sie uns diese vorab an

[ifmxnews@de.ibm.com](mailto:ifmxnews@de.ibm.com) mit dem Subject „CEBIT\_2017“ und einem Terminvorschlag, wann sie uns besuchen wollen.

## **Hinweis: INFORMIX auf der Hannover Messe (24.-28.April 2017)**

Auch auf der Hannover Messe international ist Informix im Rahmen von IoT, Cloud und Cognitive präsent. Besuchen Sie den Stand in Halle 7, der unter dem Motto

**"Where physical meets digital - Industry 4.0 with Watson!"**

steht. Gerne bieten wir Ihnen auch hier geführte Touren an und beantworten Ihre Fragen.

Bitte melden Sie sich für Touren an unter [ifmxnews@de.ibm.com](mailto:ifmxnews@de.ibm.com) mit dem Subject „HannoverMesse\_2017“ und lassen uns Ihre Fragen vorab zukommen.

## **Hinweis: INFORMIX Technologie Tag in München (16.Mai 2017)**

Nachdem die Informix Technologie Tage der letzten Jahre auf ein sehr positives Echo der Teilnehmer gestoßen sind, soll auch in diesem Jahr wieder ein Technologie Tag durchgeführt werden. Der Termin in diesem Jahr ist **Dienstag, der 16.05.2017**. Die Veranstaltung wird in München stattfinden. Anmeldungen werden ab Ende März möglich sein.

Wir planen eine Mischung aus einer Key-Note mit Informationen aus Entwicklung und Support sowie Vorträgen aus diesen Bereichen, würden uns aber freuen, wenn auch Kunden selbst sich zu Wort melden.

Wir bitten Sie deshalb, Themen und Präsentationen für den Informix Technologie Tag vorzuschlagen. Dabei genügt zunächst ein Titelvorschlag, eventuell mit einer Kurzbeschreibung des Inhalts.

Es können zwei Arten von Vorschlägen gemacht werden

- Themen zu Vorträgen, die Sie gerne selbst halten wollen
- Themen zu Vorträgen, die Sie gerne hören möchten.

Bitte schicken Sie Ihren Themen- oder Vortragswunsch bis zum 27.03.2017 an [elisabeth.bach@de.ibm.com](mailto:elisabeth.bach@de.ibm.com), und geben Sie auch ihre Kontaktdaten an.

Wir freuen uns auf ihre Rückmeldungen und hoffen, Sie ihm Mai zahlreich zu sehen!

## **Versionsinfo: 12.10.xC8 / 12.10.xC8W1 ist verfügbar**

Seit Dezember 2016 ist die Version 12.10.xC8, seit Februar 2017 zudem die Version 12.10.xC8W1 für alle unterstützten Plattformen und Editionen verfügbar. Hierin sind einige Patches enthalten, die Fehler beheben und neue Features verbessern.

## Anmeldung / Abmeldung / Anmerkung

Der Newsletter wird ausschließlich an angemeldete Adressen verschickt. Die Anmeldung erfolgt, indem Sie eine Email mit dem Betreff „**ANMELDUNG**“ an **ifmxnews@de.ibm.com** senden.

Im Falle einer Abmeldung senden Sie „**ABMELDUNG**“ an diese Adresse.

Das Archiv der bisherigen Ausgaben finden Sie zum Beispiel unter:

<http://www.iiug.org/intl/deu>

[http://www.iug.de/index.php?option=com\\_content&task=view&id=95&Itemid=149](http://www.iug.de/index.php?option=com_content&task=view&id=95&Itemid=149)

<http://www.informix-zone.com/informix-german-newsletter>

<http://www.drap.de/link/informix>

<http://www.nsi.de/informix/newsletter>

<http://www.cursor-distribution.de/index.php/aktuelles/informix-newsletter>

<http://www.listec.de/Newsletter/IBM-Informix-Newsletter/View-category.html>

<http://www.bereos.eu/software/informix/newsletter/>

Die hier veröffentlichten Tipps&Tricks erheben keinen Anspruch auf Vollständigkeit. Da uns weder Tippfehler noch Irrtümer fremd sind, bitten wir hier um Nachricht falls sich bei der Recherche einmal etwas eingeschlichen hat, was nicht wie beschrieben funktioniert.

## Die Autoren dieser Ausgabe

Gerd Kaluzinski                      IT-Specialist Informix, DB2, InfoSphere CDC, DataStage  
IBM Analytics  
[gerd.kaluzinski@de.ibm.com](mailto:gerd.kaluzinski@de.ibm.com)                      +49-175-228-1983

Martin Fuerderer                      IBM Informix Entwicklung, München  
IBM Software Group, Information Management  
[martinfu@de.ibm.com](mailto:martinfu@de.ibm.com)

Roger Schmitz                      FE Software Support Spezialist Informix,  
[Kelsterbach, Germany](http://www.kelsterbach.de)  
[schmitzr@de.ibm.com](mailto:schmitzr@de.ibm.com)

Die Versionsinfo stammt aus dem Versions-Newsletter der CURSOR Software AG  
<http://www.cursor-distribution.de/download/informix-vinfo>

Sowie unterstützende Teams im Hintergrund.

Fotonachweis: IBM Flyer zur Eröffnung Watson-IoT-Center München