

Wie lange dauert Sicherheit?

Ernst Leber, MT AG

Oracle Virtual Private Database (VPD) und Transparent Data Encryption (TDE) sind Bestandteile der Oracle Enterprise Edition. In diesem Artikel wird untersucht, wie sich die Zugriffszeiten auf Daten in einer Oracle Datenbank bei Verwendung von VPD und TDE verändern.

Die Frage nach der Sicherheit von gespeicherten Daten wird immer häufiger diskutiert. Oracle stellt mit Transparent Data Encryption (TDE) und Virtual Private Database (VPD) Mechanismen bereit, um Daten vor nicht erlaubten Zugriffen zu schützen. Nachfolgend wird die Verlängerung der Zugriffszeiten auf die Daten in einer Oracle Datenbank bei Verwendung von VPD und TDE gemessen. Ein weiterer Aspekt ist die Frage, inwieweit sich die Ausführungszeit durch native Compilierung verkürzt.

Umsetzung

Für die Messung der Zugriffszeiten wird eine einfache Tabelle KONTO mit Kontodaten und einem künstlichen Schlüssel als Primary Key genutzt. Während der Messungen wird auf die Daten nicht nur über den Primary Key zugegriffen, sondern auch über die Kontonummer. Für diesen Zugriff wird der Index KONTO_IDX_2 (siehe Abbildung 1) erstellt.

Die Ergebnisse der Messungen werden in der Tabelle KONTO_RESULT gespeichert. Die Bedeutung der Tabellenattribute ist in der folgenden Tabelle aufgelistet.

Für das Schreiben und Lesen der Daten in die Tabelle KONTO wird eine einfache Prozedur erstellt, die in mehreren Durchläufen Zufallszahlen schreibt, liest, verändert und löscht. Für die vorliegenden Messungen wurden 1.000.000 Durchläufe gewählt.

Diese Prozedur besteht aus mehreren Schleifen, die nach dem gleichen Prinzip aufgebaut sind und sich nur durch die Aktion Insert, Update, Select oder Delete unterscheiden. Abbildung 2 zeigt einen Auszug aus der Prozedur am Beispiel eines Updates.

KONTO		
P	N	KONTO_ID NUMBER
A		KONTO_NUMMER VARCHAR2 (30 BYTE)
A		BLZ VARCHAR2 (30 BYTE)
KONTO_PK		
KONTO_IDX_2		

KONTO_RESULT		
P	N	RUN_ID NUMBER
P	N	AKTION VARCHAR2 (20 BYTE)
A		DELTA_100 NUMBER
A		ANZAHL NUMBER
A		CRYPT VARCHAR2 (5 BYTE)
A		VPD VARCHAR2 (5 BYTE)
A		COMP VARCHAR2 (5 BYTE)
KONTO_RESULT_PK		

Abbildung 1: Die Tabellen für die Messung und Speicherung der Messergebnisse

```

start_100 := sys.dbms_utility.get_time;

for i in tab_konto.first .. tab_konto.last loop
  update konto
  set blz = tab_konto(i).blz
  where konto_id = tab_konto(i).konto_id;

end loop;
commit;

stop_100 := sys.dbms_utility.get_time;

-- daten merken
insert into konto_result
values (l_run_id
       , 'update'
       , stop_100 - start_100
       , l_crypt
       , l_vpd
       , l_comp
       , pi_count);

Commit;
    
```

Abbildung 2: Auszug aus der Prozedur zum Messen der Laufzeiten

Attribut	Wert	Bedeutung
RUN_ID		Fortlaufende Nummer während der Messung
AKTION		Kurztext der Datenbankaktion (Select, Insert etc.)
DELTA_100		Zeit zwischen den Operationen in Millisekunden
ANZAHL		Anzahl der Durchläufe der Messung
TDE	TRUE / FALSE	Spalten KONTO_NUMMER und BLZ verschlüsselt oder nicht
VPD	TRUE / FALSE	Virtual Private Database (VPD) aktiviert Ja / Nein
COMP	TRUE / FALSE	Status des VPD Packages und der Prozedur NATIVE / INTERPRETED

Tabelle 1: Erläuterung der Spalten in der Tabelle KONTO_RESULT

Als Basis für die Zugriffsbeschränkungen mit VPD werden die im Artikel „Absicherung einer bestehenden Applikation mit Oracle Virtual Private Database VPD“ [1] beschriebenen Tabellen und Prozeduren verwendet und die Policy entsprechend angepasst (siehe Abbildung 3).

Bei der Zeitmessung für den Select werden zwei Statements ausgeführt, um die unterschiedlichen Zeiten beim Zugriff über den künstlichen Schlüssel beziehungsweise über die verschlüsselte Kontonummer zu messen.

Den kompletten Sourcecode für die Prozedur und die verwendeten Skripte finden Sie unter http://www.mt-ag.com/web/download/experts_library in der Rubrik „Special-Interest-Artikel“. Die Messungen wurden auf einem Notebook mit folgender Konfiguration durchgeführt:

Hardware:

- Intel Dual Core 1,66 GHz CPU und 2 GB RAM

Software:

- Windows XP Professional
- Service Pack 3
- Oracle Database 11g Enterprise Edition Release 11.1.0.6.0 – Production With the Partitioning, OLAP, Data Mining and Real Application Testing options

Messung

Beim Start der Messung sind VPD und die Verschlüsselung mit TDE deaktiviert. Die Prozeduren und Packages sind normal, das heißt, interpretativ kompiliert. Zwischen den Zeitmessungen werden TDE, VPD und die Compilierung manuell über Skripte geändert

TDE	VPD	COMP
False	False	False
True	False	False
True	True	False
True	True	True
False	True	False
False	True	True
False	False	True

Tabelle 2: Ablauf der Zeitmessung

```

begin
  dbms_rls.add_policy(
    object_schema => 'APP_ADMIN',
    object_name => 'KONTO',
    policy_name => 'APP_BLOCK',
    function_schema => 'APP_ADMIN',
    policy_function => 'SEC_APPLIK.SET_APPLIK',
    statement_types => 'select, insert, update, delete',
    update_check => TRUE,
    enable => TRUE,
    static_policy => FALSE
  );
end;

```

Abbildung 3: Listing der Policy

ID	AKTION	EINSELZEIT	TDE	VPD	COMP	Verlängerung
1	insert	0,01072	FALSE	FALSE	FALSE	1
2	insert	0,02449	TRUE	FALSE	FALSE	2,28
3	insert	0,03695	FALSE	TRUE	FALSE	3,45
4	insert	0,01415	FALSE	FALSE	TRUE	1,32
5	insert	0,05602	TRUE	TRUE	FALSE	5,23
6	insert	0,05219	TRUE	TRUE	TRUE	4,87
7	insert	0,03115	FALSE	TRUE	TRUE	2,91
8	update	0,00746	FALSE	FALSE	FALSE	1
9	update	0,02200	TRUE	FALSE	FALSE	2,95
10	update	0,02813	FALSE	TRUE	FALSE	3,77
11	update	0,00759	FALSE	FALSE	TRUE	1,02
12	update	0,04569	TRUE	TRUE	FALSE	6,12
13	update	0,04632	TRUE	TRUE	TRUE	6,21
14	update	0,02783	FALSE	TRUE	TRUE	3,73
15	select konto_id	0,00520	FALSE	FALSE	FALSE	1
16	select konto_id	0,01886	TRUE	FALSE	FALSE	3,63
17	select konto_id	0,02603	FALSE	TRUE	FALSE	5,01
18	select konto_id	0,00539	FALSE	FALSE	TRUE	1,04
19	select konto_id	0,04115	TRUE	TRUE	FALSE	7,91
20	select konto_id	0,04112	TRUE	TRUE	TRUE	7,91
21	select konto_id	0,02583	FALSE	TRUE	TRUE	4,97
22	select Konto_Nummer	0,00587	FALSE	FALSE	FALSE	1
23	select Konto_Nummer	0,02487	TRUE	FALSE	FALSE	4,24
24	select Konto_Nummer	0,02940	FALSE	TRUE	FALSE	5,01
25	select Konto_Nummer	0,00787	FALSE	FALSE	TRUE	1,34
26	select Konto_Nummer	0,04839	TRUE	TRUE	FALSE	8,24
27	select Konto_Nummer	0,04741	TRUE	TRUE	TRUE	8,08
28	select Konto_Nummer	0,02802	FALSE	TRUE	TRUE	4,77
29	delete	0,01444	FALSE	FALSE	FALSE	1
30	delete	0,03105	TRUE	FALSE	FALSE	2,15
31	delete	0,03286	FALSE	TRUE	FALSE	2,28
32	delete	0,01562	FALSE	FALSE	TRUE	1,08
33	delete	0,04569	TRUE	TRUE	FALSE	3,16
34	delete	0,04523	TRUE	TRUE	TRUE	3,13
35	delete	0,03200	FALSE	TRUE	TRUE	2,22

Tabelle 3: Messergebnisse

Die Messreihe ist nach den vier Schritten ungesichert, mit Verschlüsselung, VPD und nativer Compilierung eigentlich beendet, da eine transparente Verschlüsselung der Daten mit TDE ohne Einschränkung der Zugriffe über VPD sicherheitstechnisch sinnlos ist. Die Messreihe wurde dennoch fortgeführt, um die Zeitdifferenzen beim Einsatz von VPD mit und ohne TDE beziehungsweise nativer Compilierung zu ermitteln.

Bei der Betrachtung der Messergebnisse zeigt sich, dass die Zugriffszeiten – wie erwartet – durch die Aktivierung von TDE und VPD länger werden. Die Verlängerung schwankt, je nach Aktion, zwischen dem 5- bis 8-fachen der normalen Ausführungszeit.

Bei der nativen Compilierung wird die Ausführungszeit ebenfalls länger! Diese Verlängerung liegt daran, dass die verwendete Prozedur beziehungsweise das Package nicht so komplex ist, dass sich eine native Compilierung wesentlich auswirken kann, sondern

der Overhead für den Aufruf der nativ compilierten Programme größer als der Nutzen ist. Ein weiteres Indiz dafür sind die geringfügigen Verkürzungen der Laufzeiten beim Insert und Select, siehe die Mess IDs 5 und 6 sowie 26 und 27 und die Verlängerung beim Update (IDs 12 und 13).

Die Laufzeitunterschiede beim Select der Daten über den künstlichen Schlüssel beziehungsweise die verschlüsselte Kontonummer fallen gering aus. Der Verlängerungsfaktor bei der Ausführung schwankt zwischen 7,91 und 8,08 (ID 20 / ID 15 beziehungsweise ID 27 / 22). Diese Schwankung dürfte auf die Mess-Ungenauigkeiten zurückzuführen sein.

Fazit

Beim Einsatz von TDE und VPD verlängern sich die Ausführungszeiten der Statements. Je nach Art der Daten und den damit verbundenen Sicherheitsanforderungen sollten jedoch unbedingt

die Kombination von VPD und TDE oder ähnliche Werkzeuge für die Absicherung von Daten in Datenbanken eingesetzt werden.

Die Laufzeitverlängerung der Statements und der damit verbundene höhere Ressourcen-Einsatz sollte beim Design und der Realisierung der Applikation berücksichtigt werden, da die Kosten für die nachträgliche Verbesserung der Datensicherheit und der Imageschaden bei einem Datendiebstahl um ein Vielfaches höher sind.

Literatur

Ernst Leber MT AG: 'Absicherung einer bestehenden Applikation mit Oracle Virtual Private Database VPD'. http://www.mt-ag.com/web/download/experts_library/special_interest_artikel/2008_August_Oracle_VPD_Ernst_Leber.pdf

Kontakt:

Ernst Leber
ernst.leber@mt-ag.com



Save the Date

DOAG Logistik & SCM 2009

Am 12. Mai 2009 veranstalten die DOAG und Oracle gemeinsam die DOAG Logistik & SCM 2009 und knüpfen damit an die erfolgreiche Veranstaltung des Vorjahres an.

In diesem Jahr findet die Tagung im DHL Innovation-Center, Troisdorf statt. Dabei soll die Bandbreite der Praxisbeispiele deutlich erweitert und der Teilnehmerkreis noch stärker in Richtung Fachbereichsentscheider weiterentwickelt werden.



Dies ist eine ausgezeichnete Gelegenheit, um ...

- ▶ in „lebendiger Form“ die neuesten Innovationen und globale Logistiklösungen im Rahmen eines Rundgangs durch den Showroom des DHL Innovation Centers zu erleben
- ▶ sich mit Praktikern aus unterschiedlichen Branchen über aktuelle Best Practices auszutauschen
- ▶ sich über die neuesten Strategien und Produktentwicklungen zu informieren
- ▶ mit Oracle Experten und Führungskräften über neue und innovative Ideen für Ihre Projekte zu diskutieren