



*Abakus*

# ARBITER

Sistem vodenja revizijskih sledi

hiter začetek uporabe za revizorje

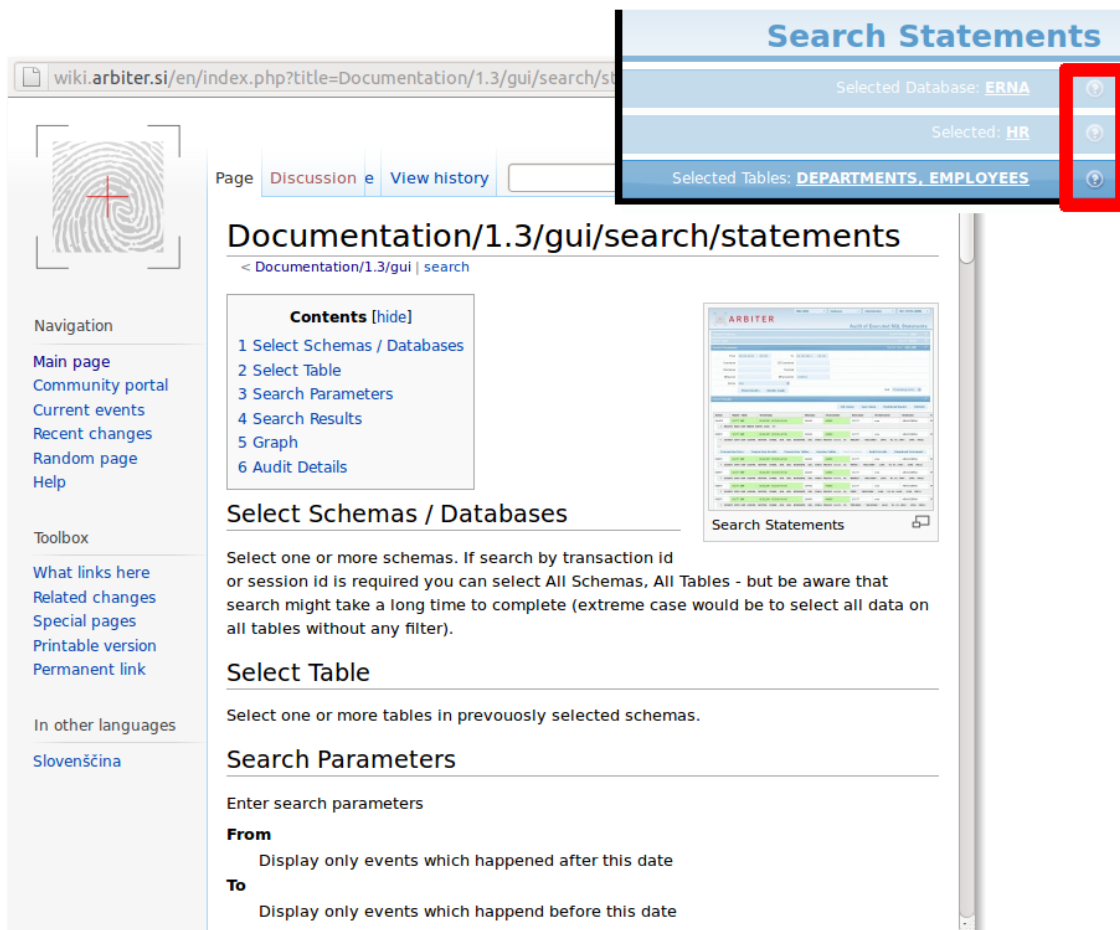
## Kazalo

Uradna dokumentacija.....	1
Opis osnovnih gradnikov.....	2
Gumbi.....	2
Tabele.....	2
Podatkovni model.....	4
SQL Stavki.....	5
Stare in nove vrednosti.....	5
Seje.....	5

Transakcije.....	6
Sprehod skozi uporabniški vmesnik.....	7
Prva stran.....	7
Seje.....	8
SQL Stavki.....	9
Stare in nove vrednosti.....	11
Kontakt in tehnična podpora.....	12

Na naslednjih straneh je opisana uporaba Arbitra za revizorje oz za končne uporabnike. Za področje administracije si lahko preberete dokument "Arbiter za administratorje".

# Uradna dokumentacija

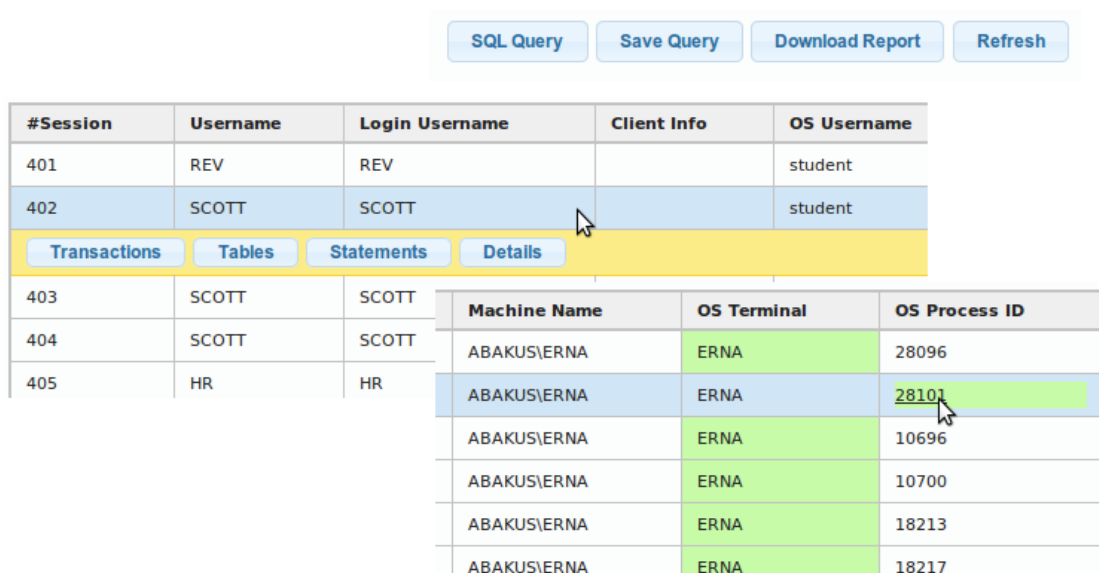


V tem vodiču so opisane glavne lastnosti grafičnega vmesnik. Vendar pa boste ob podrobnem pregledu najbrž potrebovali podrobno razlago posameznih vnosnih polj ali prikazanih kolon. Zato ima Arbiter **pomoč vgrajeno v uporabniški vmesnik**. Le-ta je dostopna s klikom na ikono v podobi vprašaja, ki se vedno nahaja na desni strani (kot prikazuje slika desno zgoraj). Ob kliku se odpre spletna stran wiki.arbiter.si na kateri se prikaže dokumentacija za trenutni zaslonski prikaz.

## Opozorila

- Za delovanje povezave do dokumentacije odjemalec potrebuje dostop do interneta, ki sicer za samo delovanje Arbitra in njegovega uporabniškega vmesnika ni potreben.
- Dokumentacija je napisana v angleščini in je precej podrobna. Zato smo za splošen pregled funkcionalnosti in uporabe so pripravili tale priročnik. Podoben priročnik obstaja tudi za administracijo.

# Opis osnovnih gradnikov



#Session	Username	Login Username	Client Info	OS Username
401	REV	REV		student
402	SCOTT	SCOTT		student

#Session	Username	Login Username	Machine Name	OS Terminal	OS Process ID
403	SCOTT	SCOTT			
404	SCOTT	SCOTT	ABAKUS\ERNA	ERNA	28096
405	HR	HR	ABAKUS\ERNA	ERNA	28101
			ABAKUS\ERNA	ERNA	10696
			ABAKUS\ERNA	ERNA	10700
			ABAKUS\ERNA	ERNA	18213
			ABAKUS\ERNA	ERNA	18217

Zgornji tabeli prikazujeta primer interaktivnega poročila. Arbiter podpira nekaj vrst različnih poročil, ki si jih bomo ogledali na naslednjih straneh, vendar pa je uporabniška izkušnja ne glede na vrsto poročila enaka. Na vsakem poročilo so omogočeni sledeče možnosti:

## Gumbi

- **SQL Query:** Izpiše SQL stavek z izvedbo katerega lahko pridete do enakih rezultatov ročno iz okolja kot je npr. SQL Developer ali SQL\*Plus.
- **Save Query:** Omogoča shranjevanje parametrov poizvedbe, tako da lahko v bodoče enostavno ponovite trenutno iskanje z enakimi parametri.
- **Download Report:** Omogoča prenos (oz. izvoz) rezultatov v oblikah PDF, HTML ali CSV.
- **Refresh:** Omogoča osvežitev rezultatov (ponovno požene poizvedbo z enakimi parametri).

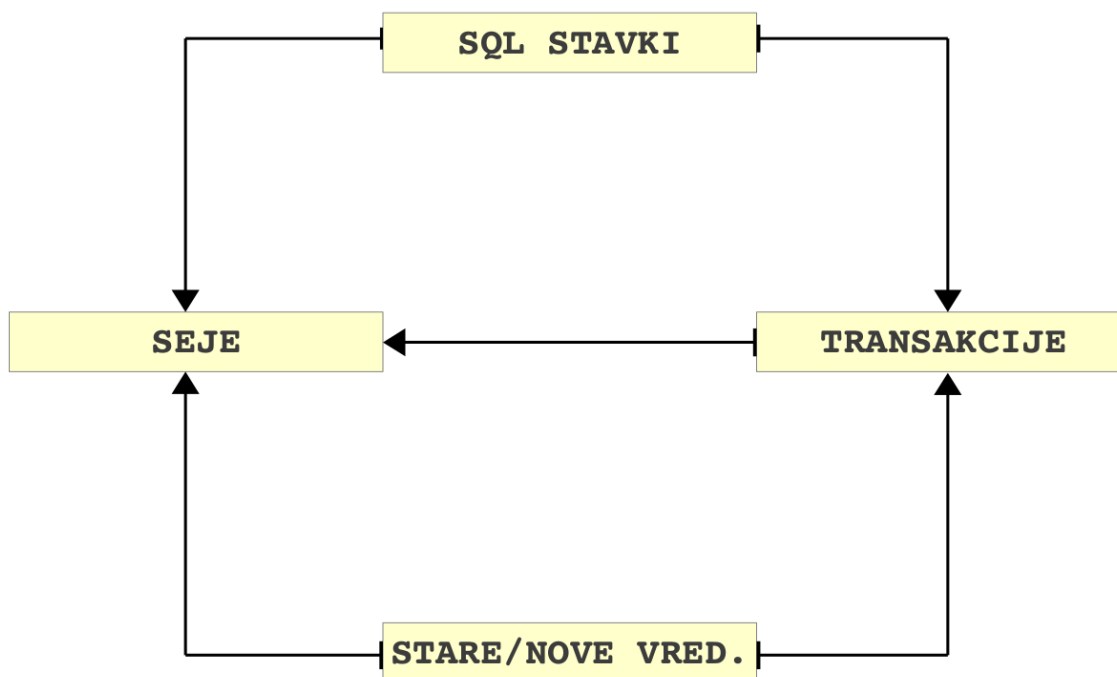
## Tabele

Tabele z rezultati so narejene tako, da se **ob kliku na vrstico prikaže nekaj dodatnih gumbov** – le ti so odvisni od vrste poročila. Na ta način lahko pridemo do podrobnejših podatkov o zapisu (ker včasih ekran enostavno ni dovolj širok, da bi lahko prikazali vse podatke, ki so na voljo, prikažemo le najpomembnejše, ostali pa so na voljo s klikom na gumb Details) ali pa povezave na druga poročila v povezavi s trenutnim.

**Zeleno obarvane kolone** pomenijo, da so to kolone na katere ste postavili filter. V zgornjem primeru je bil nastavljen filter, da naj prikaže vse zapise, ki so nastali za OS Terminal = 'ERNA'.

Nekateri rezultati pa se bodo obarvali zeleno, če se z miško zapeljemo čeznje – v zgornjem primeru je kazalec miške na vrstici kolone OS Process ID. To pomeni, da se bo ob kliku na to vrednost filter posodobil. Tako kot kaže slika, bi ob kliku na 28101 filter postal OS Terminal = 'ERNA' AND OS Process ID = '28101'.

## Podatkovni model



Na sliki je prikazan podatkovni model na osnovi katerega je zgrajena tudi navigacija in način dostop do poročil. Izhodišča za iskanje so torej lahko:

- **SQL Stavki** (dejanski ukazi, ki so jih uporabnik izvajali skupaj s podatki kdo jih je izvajal).
- **Stare in nove vrednosti podatkov** (ce je nekdo naprimer nekdo popravil kolono `placa`, je tukaj zapisano kdo je popravil vrednost, kakšna je bila višina plače pred spremembo in kakšna je bila po spremembi)
- **Seje** (vsaka prijava na podatkovno bazo ustvari sejo, Arbiter beleži kdaj se je nekdo prijavil in kdaj odjavil).

**Transakcije** niso možne kot izhodišče, saj so vezane na določeno sejo (transakcija brez seje ne more obstajati), zato je treba najprej najti sejo, nato pa lahko dobimo spisec transakcij, ki so se zgodile v tej seji.

Na sliki so na enem koncu povezave narisane črte na drugem pa trikotniki. Notacija predstavlja relacije. Primer za  $A \rightarrow B$ : "*B ima [lahko] določen A. V sklopu A lahko obstaja nič ali več B*".

## SQL Stavki

Vir podatkov je ponavadi AUDIT TRAIL (za Oracle, sicer odvisno od tipa podatkovne baze). Glavne stvari, ki se beležijo za vsak SQL stavek so:

- **Action:** Vrsta akcije, npr INSERT ali SELECT.
- **Object/Table:** Ime objekta nad katerim je bila akcija izvedena.
- **Timestamp:** Čas izvedebe akcije.
- **Username:** Uporabniško ime uporabnika, ki je izvede akcijo.
- **Hostname:** Naslov računalnika iz katerega je bil ukaz (sql stavek) prejet
- **SQL Text:** Točen SQL stavek.
- **Bind Variables:** Parametri s katerimi je bil stavek zagnan.

## Stare in nove vrednosti

Vir podatkov so ponavadi ARCHIVED REDO LOG datoteke (za Oracle, sicer odvisno od tipa podatkovne baze). Glavne stvari, ki jih beležimo:

- **Operation:** INSERT, UPDATE ali DELETE
- **Timestamp:** Čas spremembe
- **User:** Uporabnik, ki je spremembo naredil.
- **Stara in nova vrednost za vsako vrstico in vsako\* kolono.** (ne vedno vsako kolono – to je odvisno od konfiguracije, lahko se nastavi beleženje samo spremenjenih kolon namesto vseh)

## Seje

Seje se krirajo na podlagi iz enakega vira kot SQL Stavki, točneje, na podlagi zabeleženih LOGIN in LOGOFF dogodkov. Arbiter vodi sledeče podatke za vsako sejo:

- **#Session:** Unikatna številčna oznaka seje.
- **Username:** Uporabniško ime uporabnika, ki je sejo ustvaril (s tem da se je prijavil na sistem)
- **Logon & Logoff time:** Čas odjave in prijave. Iz tega sledi tudi trajanje seje.

- **Machine Name:** Ime računalnika iz katerega se je uporabnik prijavil.
- **OS Username:** Uporabniško ime s katerim je uporabnik lokalno prijavljen (npr. Windows Username)
- **OS Program name:** Ime programa, s katerim se je uporabnik povezal na sistem.

## Transakcije

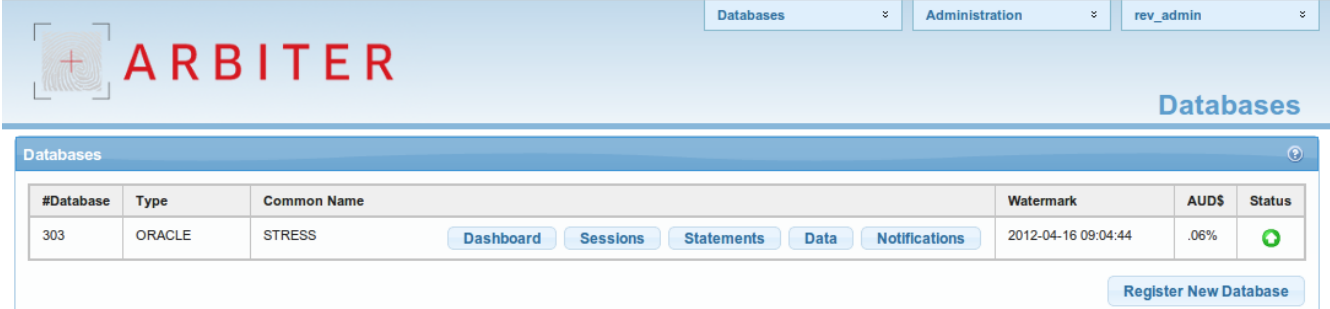
Transakcije se kreirajo na podlagi starih/novih podatkov in se zaključijo glede na COMMIT/ROLLBACK dogodke. Za vsako transakcijo se vodi:

- **#Transaction:** Unikatna številčna oznaka transakcije
- **Start & End time:** Čas začetka in konca transakcije.
- **Committed:** Ali je bila transakcija potrjena ali ne. Tudi `rollback to savepoint` postavi to vrednost na `TRUE`.



# Sprehod skozi uporabniški vmesnik

## Prva stran



The screenshot shows the ARBITER web interface. At the top, there is a navigation bar with the ARBITER logo on the left and three dropdown menus: 'Databases', 'Administration', and 'rev\_admin'. Below the navigation bar, the word 'Databases' is displayed in a large font. The main content area features a table with the following columns: '#Database', 'Type', 'Common Name', 'Watermark', 'AUD\$', and 'Status'. A single row is visible in the table, representing a database with ID 303, type ORACLE, and common name STRESS. Below the table, there are several buttons: 'Dashboard', 'Sessions', 'Statements', 'Data', and 'Notifications'. To the right of the table, the 'Watermark' column shows the date '2012-04-16 09:04:44', the 'AUD\$' column shows '.06%', and the 'Status' column shows a green plus icon. At the bottom right of the table area, there is a button labeled 'Register New Database'.

#Database	Type	Common Name	Watermark	AUD\$	Status
303	ORACLE	STRESS	2012-04-16 09:04:44	.06%	+

Na prvi strani so prikazane vse registrirane baze za katere ima uporabnik dovoljenje za brskanje po njenih revizijskih sledih. Na sliki vidimo, da je registrirana samo ena podatkovna baza (ime baze je STRESS, njena unikatna šifra pa je 303).

**Watermark** je čas, do katerega so podatki že sprocesirani in na voljo za prikaz preko grafičnega vmesnika. Podatki pred tem datumom so lahko prikazani nepopolno ali pa jih sploh še ni.

**AUD\$** prikazuje zasedenost prostora namenjena začasnemu shranjevanju revizijske sledi na izvorni bazi ("tablespace usage"). Številka je pomembna, ker v primeru 100% zasedenosti izvorna baza preneha delovati ker nima več prostora za beleženje novih akcij.

**Status** je zelene barve ko Arbiter vsa svoja opravila opravlja nemoteno. Lahko je rumene ali rdeče barve v primeru, da je pri kateremu od opravil (ki se izvajajo v ozadju) prišlo do napake in se ne izvaja pravilno. V takem primeru je potrebno obvestiti administratorja da preveri v čem je problem.

STRESS (303) ▾
Databases ▾
Administration ▾
rev\_admin ▾

## ARBITER

Search Sessions

Search Parameters

From  
To

#Session

Username 
Ignore rev\_src\_user

Login Username 
OS Username

Machine Name 
OS Terminal

OS Process ID 
OS Program name

Search Results

Enter search words to filter underlying contents.

#Session	Username	Login Username	Client Info	OS Username	Machine Name	OS Terminal	OS Process ID	OS Program name	Logon	Logoff	Return Code	No. S#
2646	BOB								03.07.2012 13:29:37	03.07.2012 13:29:37	28001: ORA-28001: the password has expired	0
2645	ALICE	ALICE		oracle	atlas.abakus.si	pts/0	23424		03.07.2012 13:29:11	03.07.2012 13:29:12	0: Authenticated by: DATABASE	1
2644	ERNA								03.07.2012 13:27:54	03.07.2012 13:27:54	1017: ORA-01017: invalid username/password; logon denied	0
2643	URH	URH		urh	urh	pts/3	23333		03.07.2012 13:27:42	03.07.2012 13:27:44	0: Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp) (HOST=193.138.47.205) (PORT=60539))	1
2636	SCOTT	SCOTT		oracle	atlas.abakus.si	UNKNOWN	23162		03.07.2012 13:25:03	03.07.2012 13:25:05	0	1
2618	SCOTT	SCOTT		oracle	atlas.abakus.si	UNKNOWN	19571		03.07.2012 12:25:03	03.07.2012 12:25:05	0	1
2605	SCOTT	SCOTT		oracle	atlas.abakus.si	UNKNOWN	14667		03.07.2012 11:25:03	03.07.2012 11:25:05	0	1
2593	SCOTT	SCOTT		oracle	atlas.abakus.si	UNKNOWN	11109		03.07.2012 10:25:03	03.07.2012 10:25:05	0	1


Na sliki so prikazane seje (spisek prijav na bazo) za obdobje 03.07.2012 med 7:00 in 16:00 uro.

**Ignore rev\_src\_user** opcija pomeni, da v izpisu ignorira (ne izpiše) sej, ki jih je kreiral uporabnik REV\_SRC\_USER. To je sistemski uporabnik na izvorni podatkovni bazi s katerim se na izvorno bazo prijavlja Arbitr, da lahko od tam prenaša podatke. Takih prijav je lahko (odvisno od konfiguracije) zelo veliko (reda nekaj 10 prijav na uro).

**#Session** je unikatna šifra seje. Če seja traja dlje kot pa dovoljuje Arbitr-ov pomnilnik (privzeto 14 dni, odvisno od konfiguracije), lahko Arbitr tako sejo zabeleži pod večimi šiframi kot več različnih sej.

Pomembno polje je še **Username**, ki prikazuje uporabniško ime s katerim se je uporabnik (poskušal) prijaviti na bazo. Ali je prijava uspela ali ne pa nakazuje kolona **Return Code**. **Machine name** prikazuje izvor (ime računalnika) od kod seja izvira.

## SQL Stavki

STRESS (303) Databases Administration rev\_admin

### Search Statements

Select Schemas Selected Database: **STRESS**

Select Table Selected: **SCOTT [.]**

Search Parameters Selected Tables: **EMPLOYEES, DEPT**

From **02.07.2012 00:00** To **02.07.2012 23:59**

Time between  and

Username  OS Username

Hostname  Terminal

#Session  #Transaction

Action **Any**

Show Results Render Graph Count By **Do NOT Count** Sort **Timestamp (Desc)**

#### Search Results

SQL Query Save Query Download Report Refresh

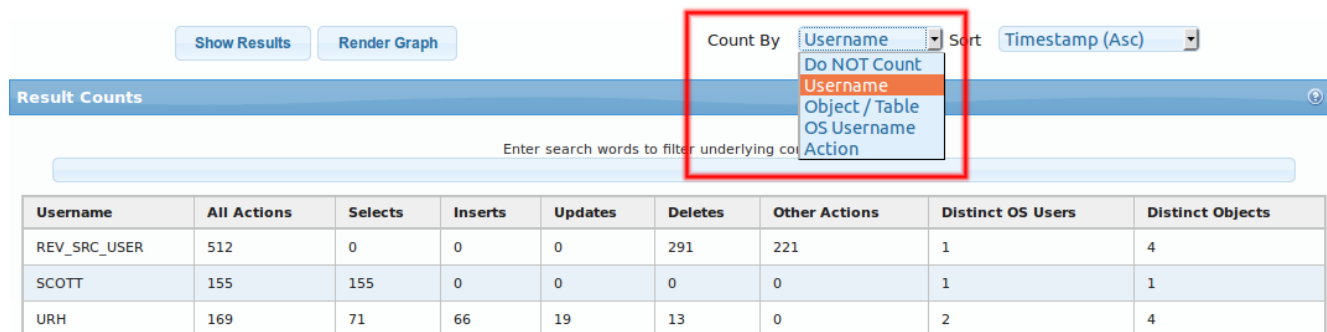
Action	Object / Table	Timestamp	#Session	#Transaction	Username	OS Username	Hostname	Terminal
UPDATE	SCOTT. DEPT	02.07.2012 16:17:46	2328	204	URH	oracle	atlas.abakus.si	pts/1
update scott.dept set loc = 'BLED' where deptno = 37								
INSERT	SCOTT. DEPT	02.07.2012 16:17:46	2328	201	URH	oracle	atlas.abakus.si	pts/1
insert into scott.dept (deptno, dname, loc) values (40, 'OPERATIONS', 'BOSTON')								
Transaction Data Transaction Details Transaction Tables Session Tables Bind Variables Audit Details Download Statement								
INSERT	SCOTT. DEPT	02.07.2012 16:17:46	2328	201	URH	oracle	atlas.abakus.si	pts/1
insert into scott.dept (deptno, dname, loc) values (30, 'SALES', 'SENCUR')								
INSERT	SCOTT. DEPT	02.07.2012 16:17:46	2328	201	URH	oracle	atlas.abakus.si	pts/1
insert into scott.dept (deptno, dname, loc) values (20, 'RESEARCH', 'KRANJ')								
INSERT	SCOTT. DEPT	02.07.2012 16:17:46	2328	201	URH	oracle	atlas.abakus.si	pts/1
insert into scott.dept (deptno, dname, loc) values (10, 'ACCOUNTING', 'SENCUR')								
INSERT	SCOTT. DEPT	02.07.2012 16:17:46	2328	201	URH	oracle	atlas.abakus.si	pts/1
insert into scott.dept (deptno, dname, loc) values (44, 'MARKETING', 'KRANJ')								

Od vrha navzdol: Najprej je prikazana izbrana baza STRESS, izbrana shema SCOTT ter dve izbrani tabeli EMPLOYEES in DEPT. Prikazani podatki so za dan 02.07.2012 (od 00:00 do 23:59).

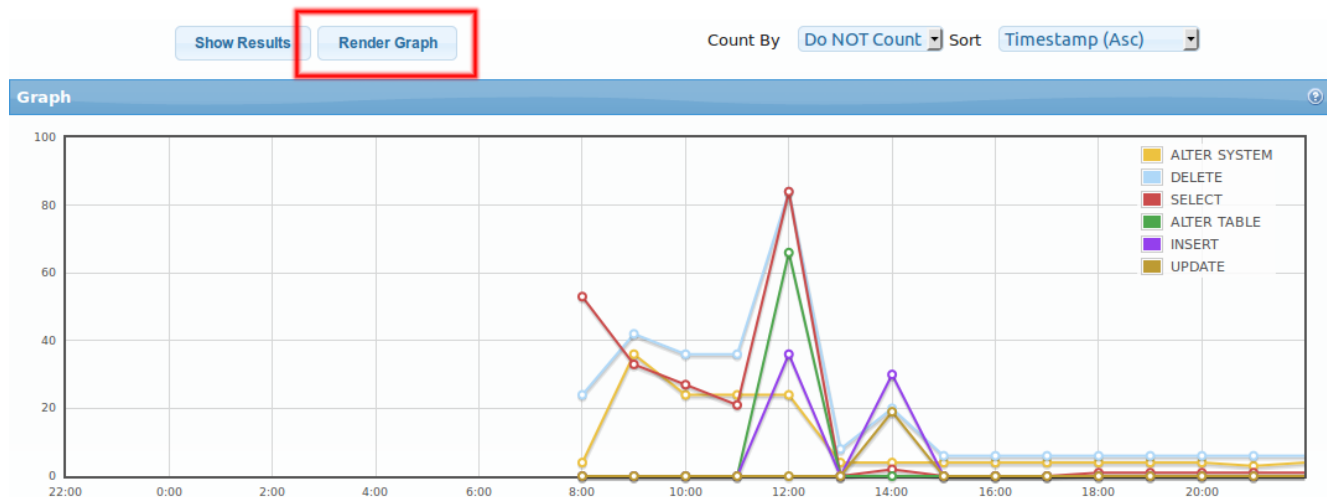
Razvidni so točni SQL ukazi ter podatki o uporabniku (username, OS username, hostname, ...), ki jih je izvedel. Gumb Audit Details prikaže še več podrobnosti o uporabniku.

Poleg točnih ukazov lahko pogledamo povzetek v obliki seštevka ali v obliki grafa, kot prikazujeta spodnji dve sliki.

Na sledeči sliki so razvidne možnosti štetja, lahko nas zanimajo akcije po uporabnikih, po objektih ali po sistemskih uporabnikih. Tako je glede na izbor prikazano število posameznih ukazov (kolone Selects, Inserts, Updates, Deletes prikazujejo število ukazov za branje, dodajanje, spreminjanje in brisanje podatkov).



Lahko pa podatke vidimo na še višjem nivoju in prikažemo graf glede na prej izbran kriterij. Graf sam po sebi sicer ni razdeljen na posamezne uporabnike/objekte, lahko pa ga na tak kriterij omejimo preden kliknemo gumb Render Graph.



## Stare in nove vrednosti

ARBITER

STRESS (303) ▾
Databases ▾
Administration ▾
rev\_admin ▾

Search Data Tables

Select Schemas
Selected Database: STRESS

Select Table
Selected: SCOTT [.]

Select Schemas
Selected Tables: PRODUCTS

From

To

Operation

#Transaction

Show Results
Transactions Sort 
Actions Sort

SQL Query
Save Query
Download Report
Refresh

Enter search words to filter underlying contents.

#Transaction <b>2593</b> ( 19.07.2012 09:24:50 - 19.07.2012 09:24:50 ), #Session <b>13177</b> ( 19.07.2012 09:24:44 )									
PRODUCTS ( SCOTT.PRODUCTS )				PRODUCT_ID		PRODUCT_NAME		PRODUCT_PRICE	
User	Operation	Table	Timestamp (start)	OLD	NEW	OLD	NEW	OLD	NEW
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	1		Weedy		92-67	10
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	1		Weedy		10	20
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	1		Weedy		20	30
#Transaction <b>2594</b> ( 19.07.2012 09:24:50 - 19.07.2012 09:24:50 ), #Session <b>13177</b> ( 19.07.2012 09:24:44 )									
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	2		Buzz-Lightyear		30-28	10
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	2		Buzz-Lightyear		10	20
Transaction Statements	Session Statements	Transaction Details	Data Details						
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	2		Buzz-Lightyear		20	30
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50						20
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50						10
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50						30, 28
#Transaction <b>2595</b> ( 19.07.2012 09:24:50 - 19.07.2012 09:24:50 ), #Session <b>13177</b> ( 19.07.2012 09:24:44 )									
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	3		Etch		102-27	10

Prikazan je potek spreminjanja podatkov za tabelo PRODUCTS v shemi STRESS.

V tabeli so s sivo barvo ozadja označene transakcije, znotraj katerih so vidne akcije. Za vsako akcijo vemo kdaj so se zgodile (kolona Timestamp), ter kdo je za to spremembo odgovoren (kolona User). Poleg tega so seveda vidne stare in nove vrednosti za vsako kolono izvirne tabele (OLD/NEW).

Nekatere vrstice imajo rumen trikotnik. To so vrstice ki so bile generirane kot posledica ROLLBACK operacije.

## Kontakt in tehnična podpora

Na voljo smo za vsakršna vprašanja:

- po e-pošti: [arbiter@abakus.si](mailto:arbiter@abakus.si)
- po telefonu: 04 287 11 00

**Spletne povezave:**

<http://www.arbiter.si/en/documentation>

<http://wiki.arbiter.si/>

<http://www.abakus.si/>

