Vodnje revizijskih sledi

brez posegov v aplikacije

Ivan Stojsavljević

univ. dipl. ing. računalništva in informatike

Univerza v Mariboru

Fakulteta za varnostne vede

ISACA Slovenski odsek

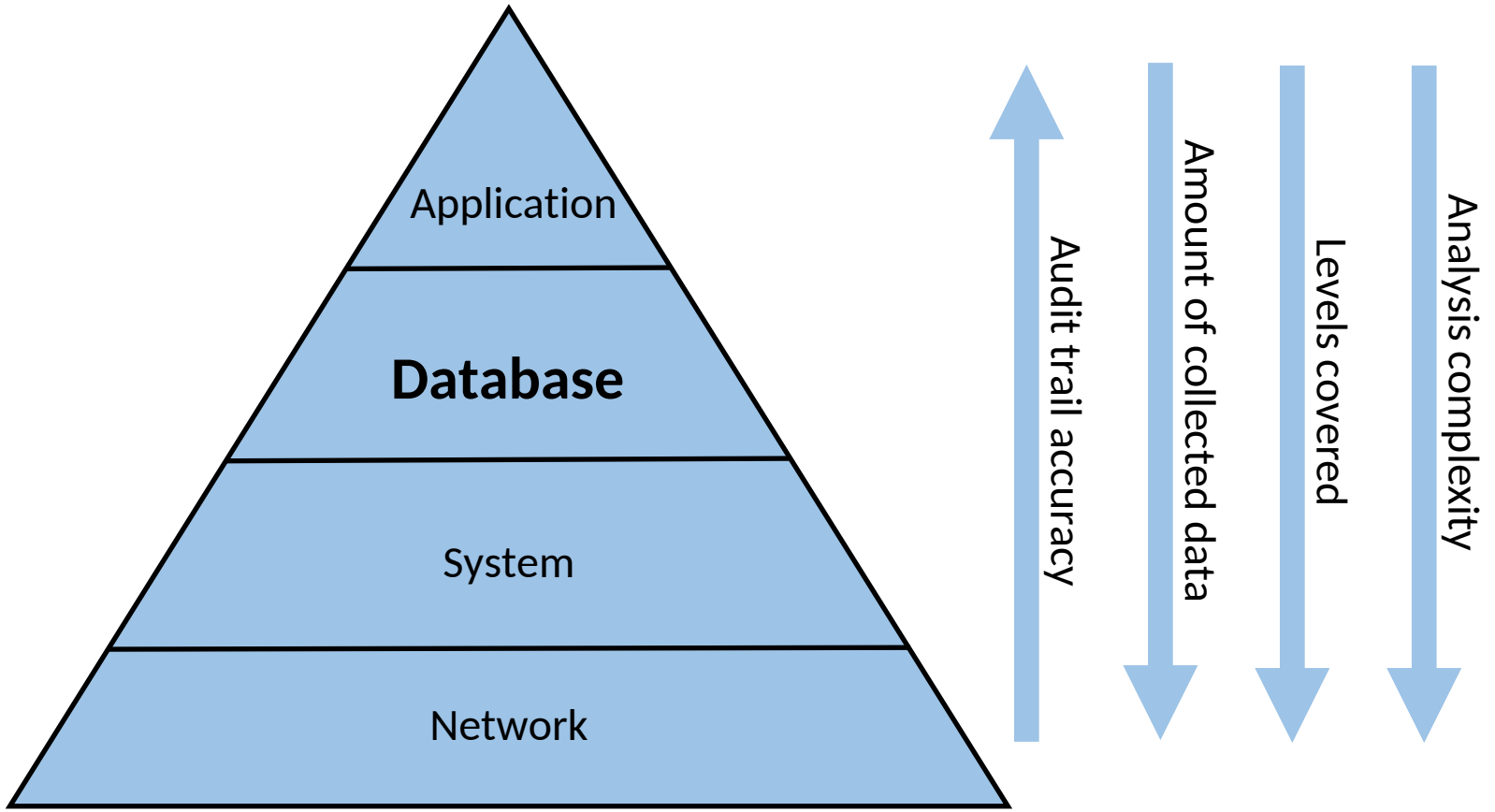
Abakus Plus d.o.o.

- Infrastructure Team
  - Services
    - OS & NET admin
    - DBA, Programming
  - Applications
    - Deja Vu
    - APPM
    - Arbiter
- Development Team
  - Enterprise Applications
  - Document Management
  - Newspaper Distribution
  - Flight Information System

Audit Trails in IT

- An **audit trail** (also called **audit log**) is a security-relevant chronological record, set of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.
- IT environments provide tools for employees to run core business processes. Those tools are in most cases **applications**.
- Modern business applications use **databases** to record data into and read data from.
- Databases contain sensitive, personal and classified information which has to be audited because of its nature.

Audit Trail Collection Level



Audit trail collection mechanism should be **independent** from the system generating audit trail.

Application Level Implementation Costs

- Many applications
  - can be costly
  - hard to manage projects
- Different vendors
  - different implementations
  - inconsistency => confused users
- Most of them are using a small number of databases
- What if audit trail was implemented **at database level**?
  - Oracle, MS SQL Server

Relational Databases

- Enterprise applications
- Data is valuable
  - Availability
  - Safety
  - Protection
  - **Changes**
  - **Intrusions**
  - **Views (GDPR)**

Definition

- Database
  - Collection of persistent data

- Database Management System (DBMS):
  - Software that supports creation, population and querying of a database.

Relational Database

Consists of **tables**.

DEPT_ID	DEPARTMENT_NAME
1	Finance
2	Marketing
3	Sales

EMP_ID	DEPT_ID	FIRST_NAME	LAST_NAME	SALARY
101	3	Steven	King	1500
102	3	Diana	Rogers	1200
103	1	Bruce	Matos	1400
107	2	David	Russell	1200
112	2	Luis	Kaufling	1250
113	3	Nancy	Olson	2000
123	3	John	Atkinson	1000

Client / Server Architecture

SQL – Data Selection

Structured Query Language

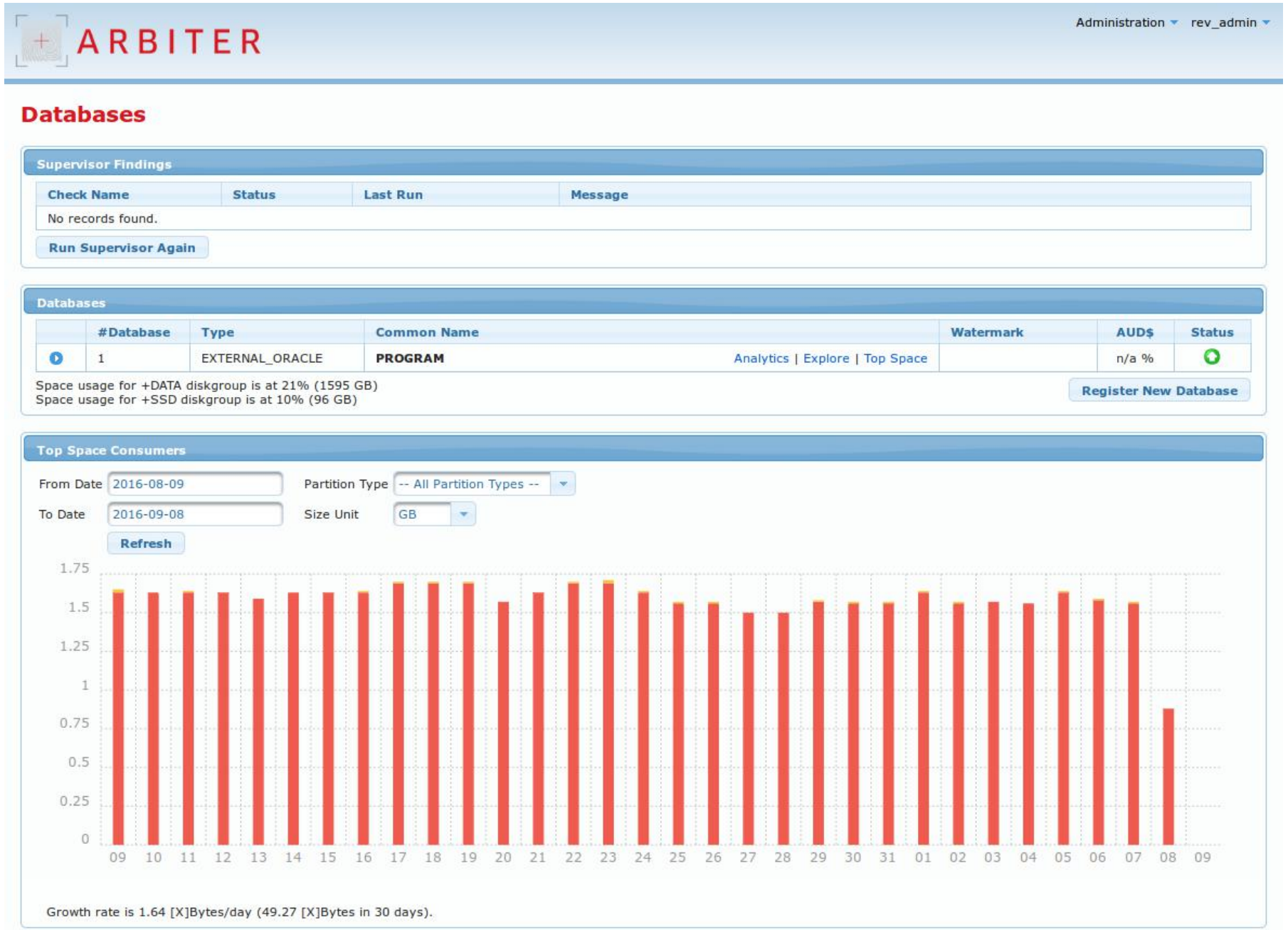
```
SELECT last_name, first_name, salary
    FROM employees
    WHERE salary > 1500
    ORDER BY last_name, first_name;
```

SQL - Data Modification

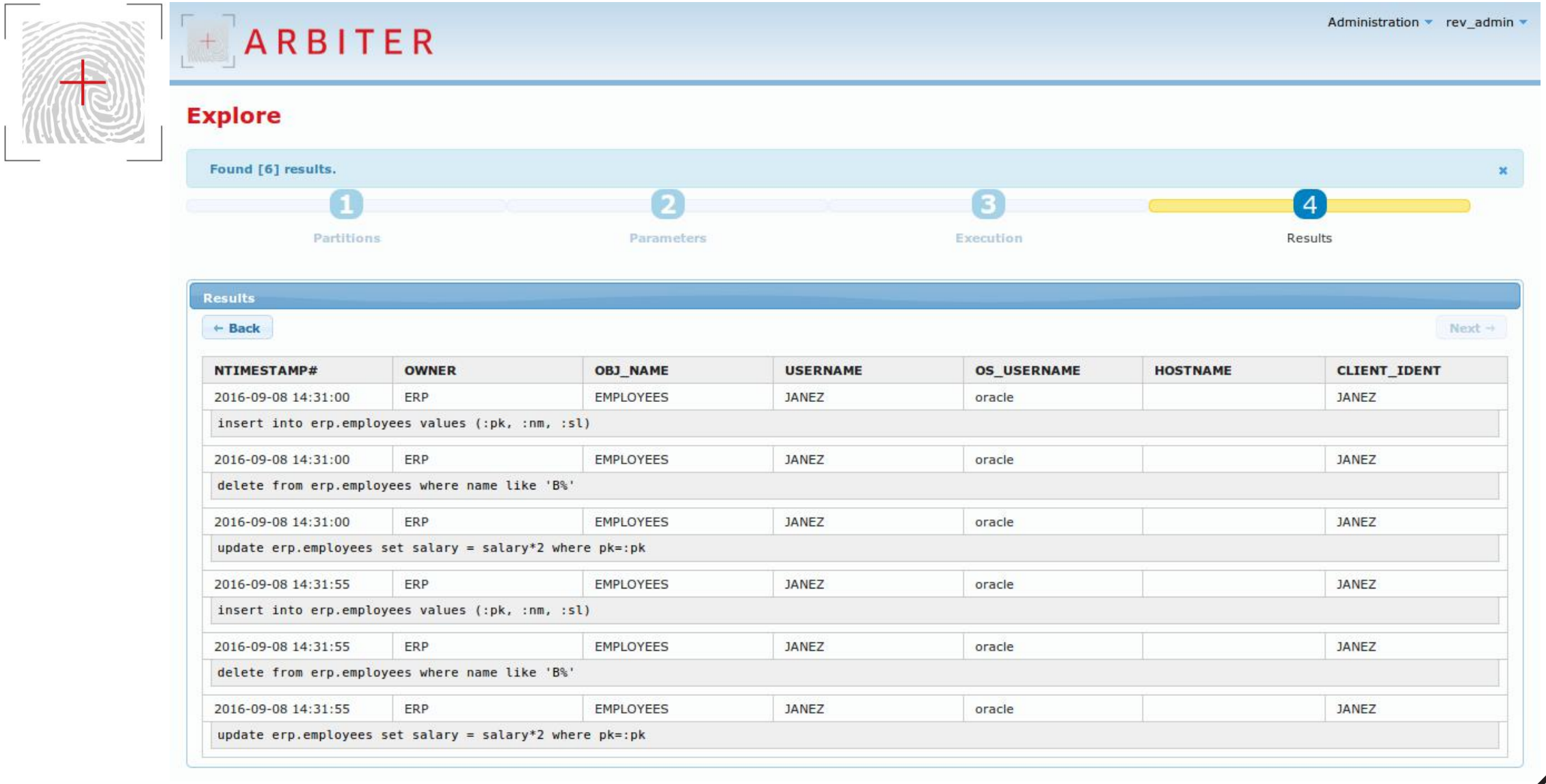
```
INSERT INTO employees (emp_id, dept_id,  first_name, last_name, salary)
   VALUES (150, 3, 'Johnny', 'Bravo', 3000);

DELETE FROM employees
     WHERE first_name='Lisa';

UPDATE employees
     SET salary=2900
     WHERE first_name='Ben';
```

Database Level Audit Trail

- Every SQL statement received & executed by RDBMS.
- Old and new values of changed data.
- Sessions (logoff & logoff)
  - Transactions (commit/rollback)

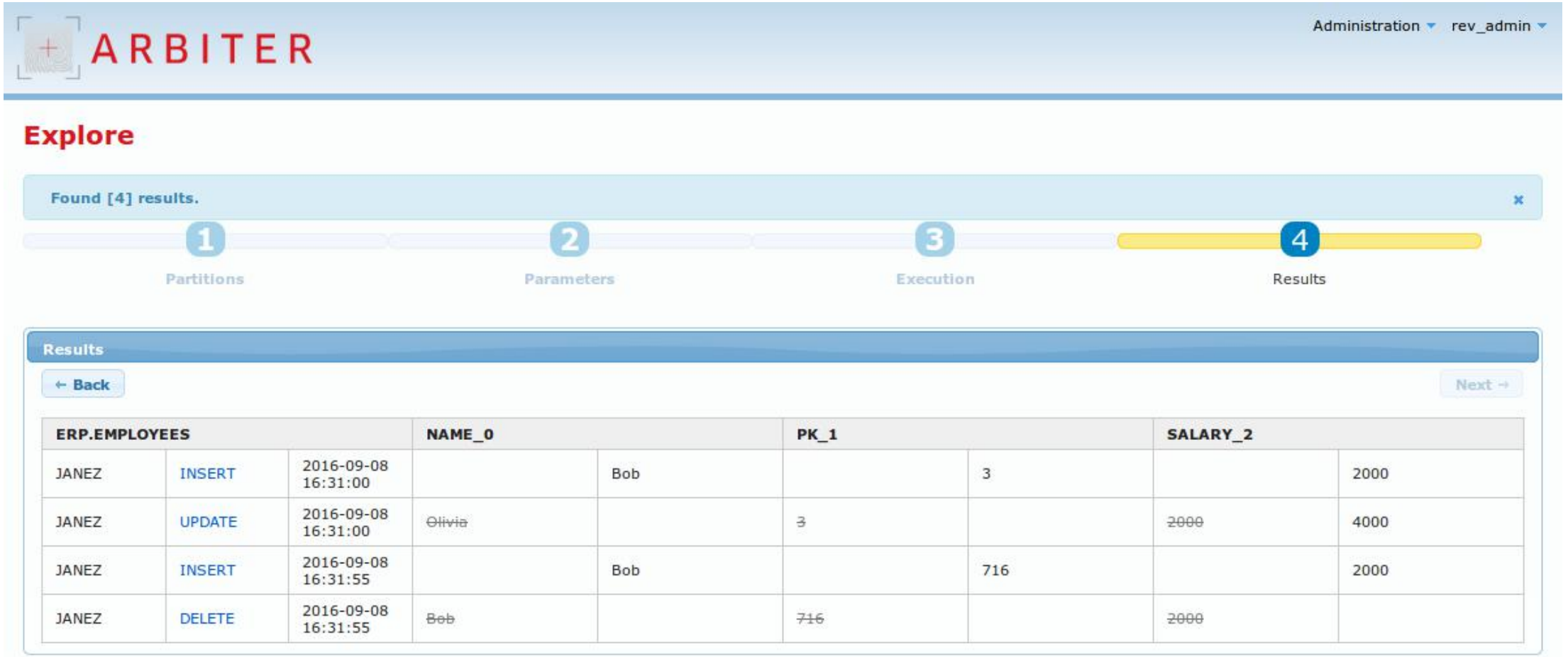


Arbter's license allows monitoring of an **unlimited number of resources**.



Which **user** ran what **SQL statement** against what **table** at a certain point in **time**.

Abakus
As na disku.



ERP.EMPLOYEES			NAME_0		PK_1		SALARY_2	
JANEZ	INSERT	2016-09-08 16:31:00		Bob		3		2000
JANEZ	UPDATE	2016-09-08 16:31:00	~~Olivia~~		~~3~~		~~2000~~	4000
JANEZ	INSERT	2016-09-08 16:31:55		Bob		716		2000
JANEZ	DELETE	2016-09-08 16:31:55	~~Bob~~		~~716~~		~~2000~~	

Arbiter displays data **old** and **new** values.

Arbiter users

Ljubljana Airport

Gorenjska Banka

LON

NLB Skladi

NLB Vita
Življenjska zavarovalnica

SAVARe

PH Primorska hranilnica

PRONET
CHOOSE THE FUTURE

LASERLINE

Abakus
As na disku.

Gospodarska zbornica Slovenije

Območna zbornica za Gorenjsko

Srebrno priznanje

Za inovacijo

Program za vodenje revizijskih sledi brez posegov v aplikacije - Arbiter

prejmejo

Boris Oblak
Jure Kajzer
Luka Čučnik

Abakus plus d.o.o.

Kranj, junij 2011

Predsednik komisije za inovacije
Avguštin Novšak

Predsednik UO območne zbornice
Miro Pinterič

Perfect Audit Trail Implementation?

- Should be independent.
- Must record events that happened beyond the application.
- **Can be done at database level alone.**
- Is a combination of application and database levels