20. Strokovno srečanje SIOUG

SIOUG 2015

12.-13. oktober 2015

Zaščita podatkov

pred vdori, naravnimi katastrofami in aplikativnimi napakami

Predavatelj:

Urh Srečnik <urh.srecnik@abakus.si>

DBA & Software Architect @ Abakus Plus d.o.o.

ORACLE

Certified Associate

Oracle Database 11*g*
Administrator

AS
Abakus
As na disku.

ORACLE **Gold Partner**

Specialized
Oracle Database

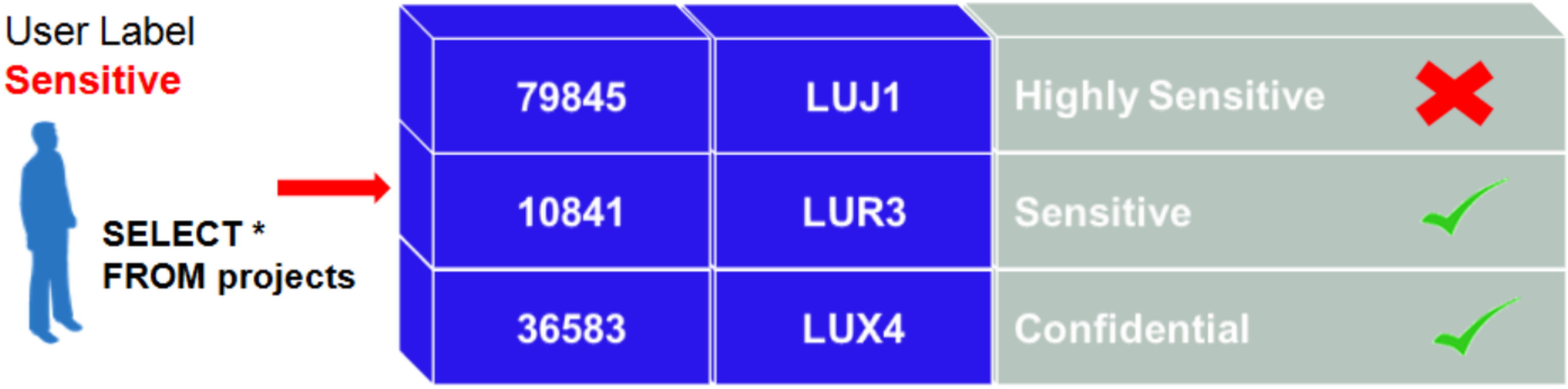
Grožnje

- Nepooblaščeni dostopi
- Odpoved programske ali strojne opreme
- Aplikativne napake

Rešitve

- Nepooblaščeni dostopi
  - Dodelava aplikacije
    - Zahteva izkušene programerje.
  - Nakup dodatnih [Oracle] produktov
    - Vnaprej definirane standardne prakse.

Oracle Label Security

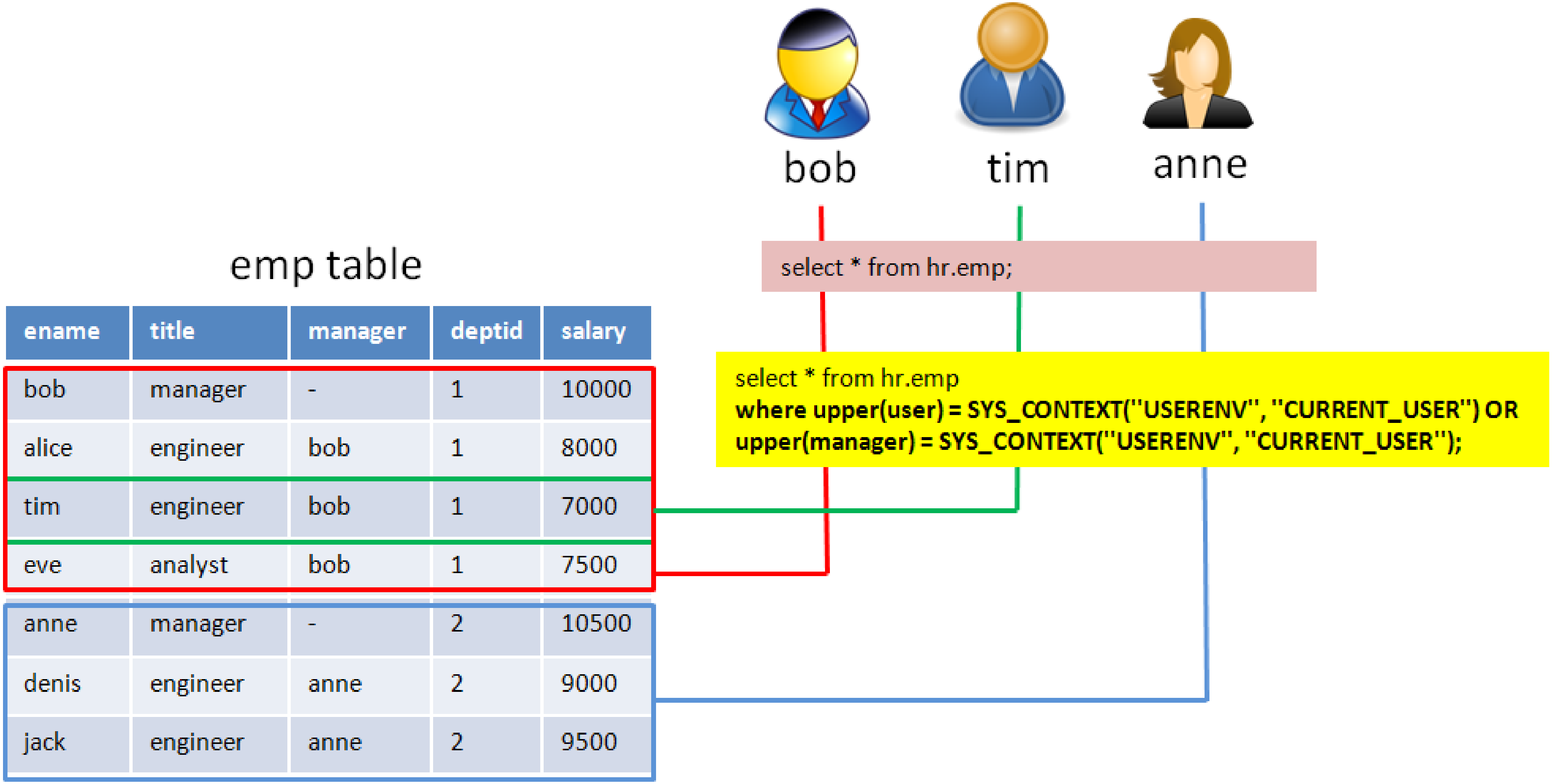


User Label
Sensitive

```
SELECT *
FROM projects
```

79845	LUJ1	Highly Sensitive	✗
10841	LUR3	Sensitive	✓
36583	LUX4	Confidential	✓

Oracle Virtual Private Database



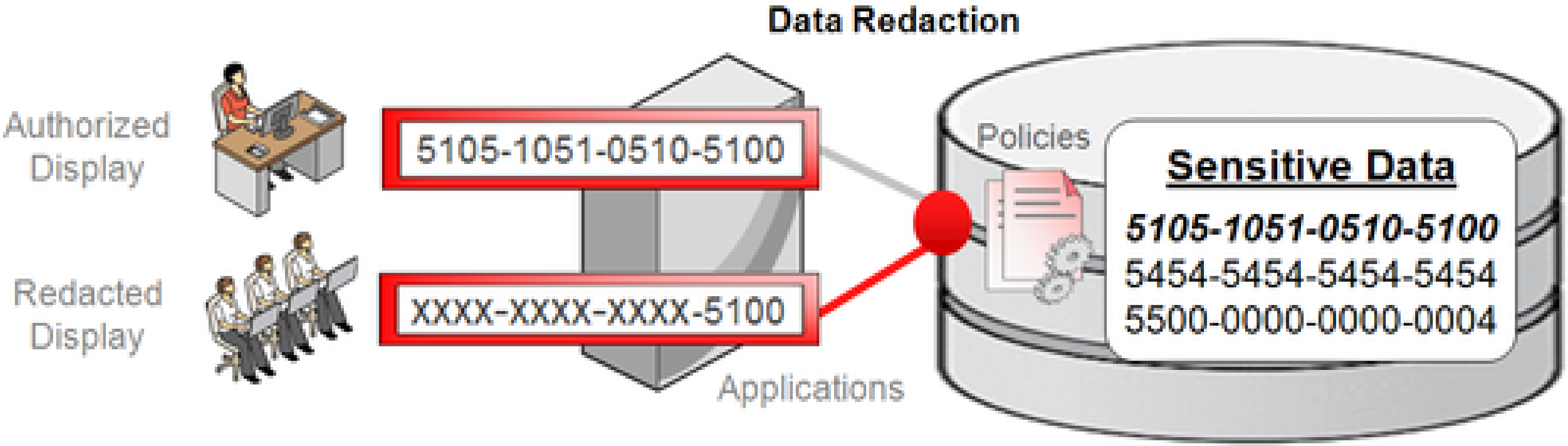
emp table

ename	title	manager	deptid	salary
bob	manager	-	1	10000
alice	engineer	bob	1	8000
tim	engineer	bob	1	7000
eve	analyst	bob	1	7500
anne	manager	-	2	10500
denis	engineer	anne	2	9000
jack	engineer	anne	2	9500

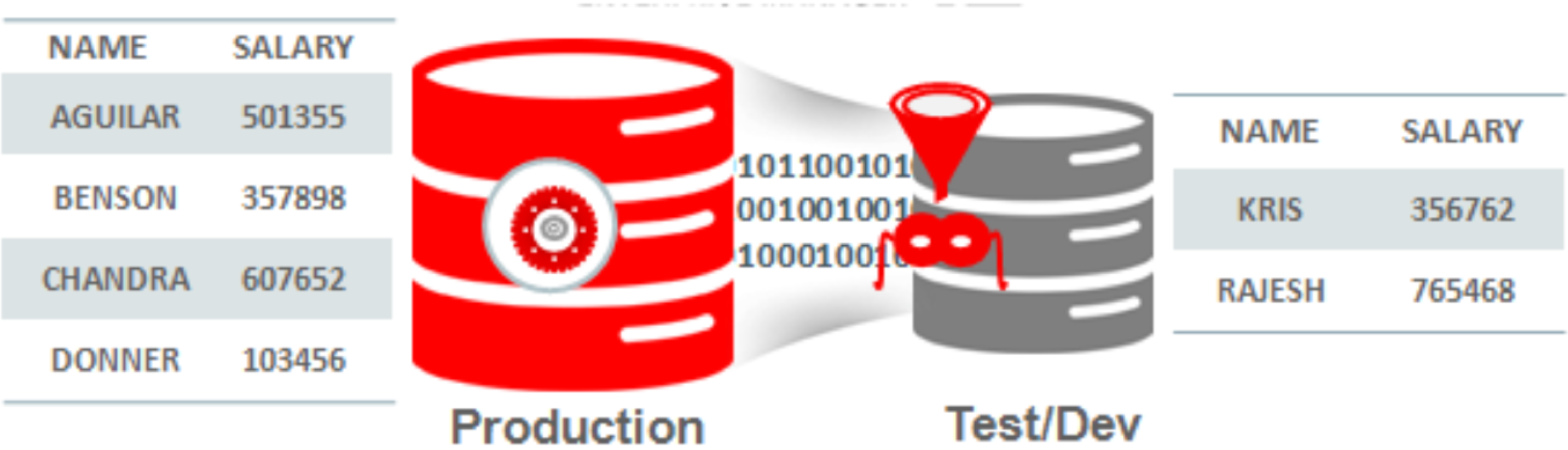
```
select * from hr.emp;
```

```
select * from hr.emp
where upper(user) = SYS_CONTEXT("USERENV", "CURRENT_USER") OR
upper(manager) = SYS_CONTEXT("USERENV", "CURRENT_USER");
```

Oracle Data Redaction



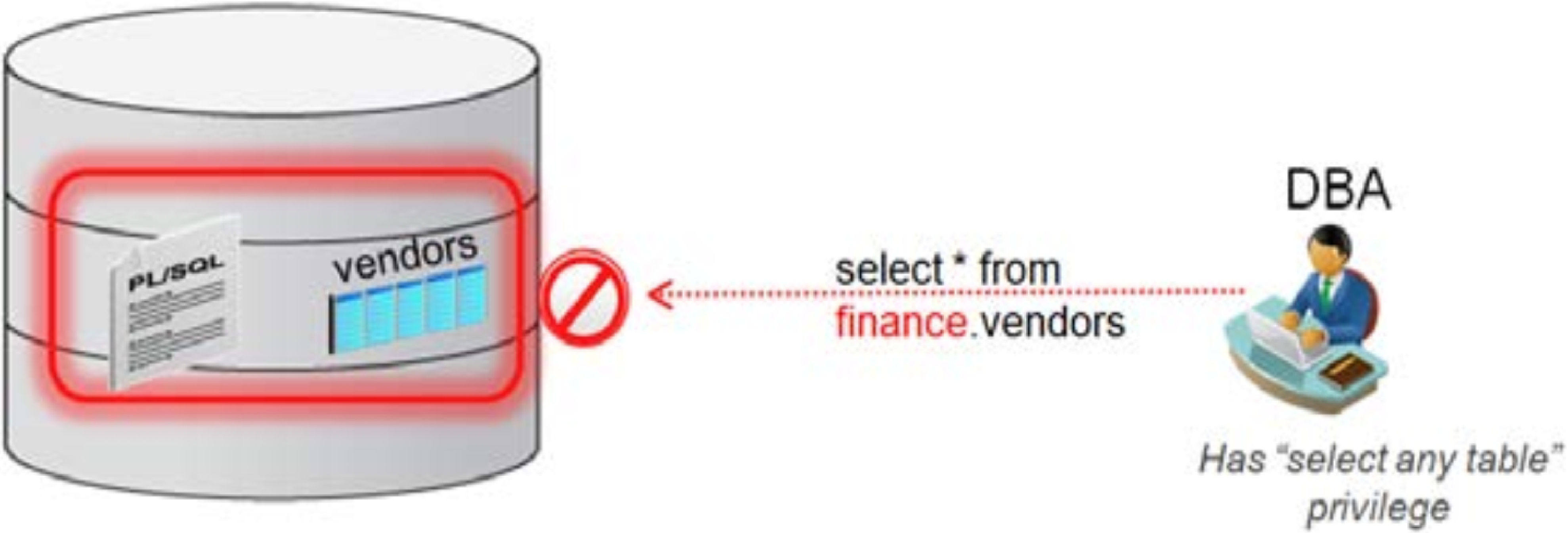
Oracle Data Masking



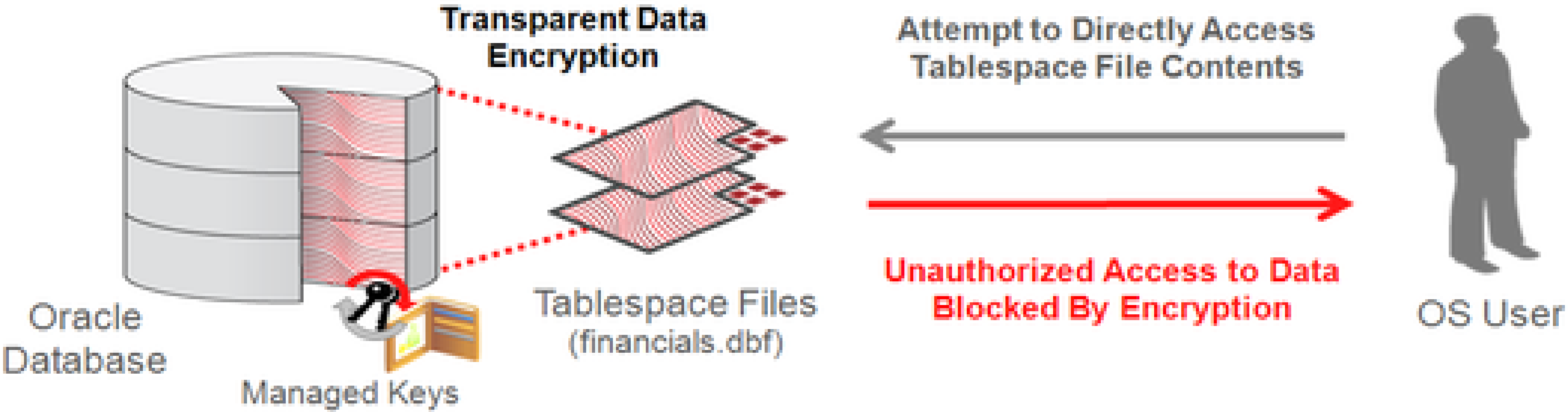
NAME	SALARY
AGUILAR	501355
BENSON	357898
CHANDRA	607652
DONNER	103456

NAME	SALARY
KRIS	356762
RAJESH	765468

Oracle Database Vault

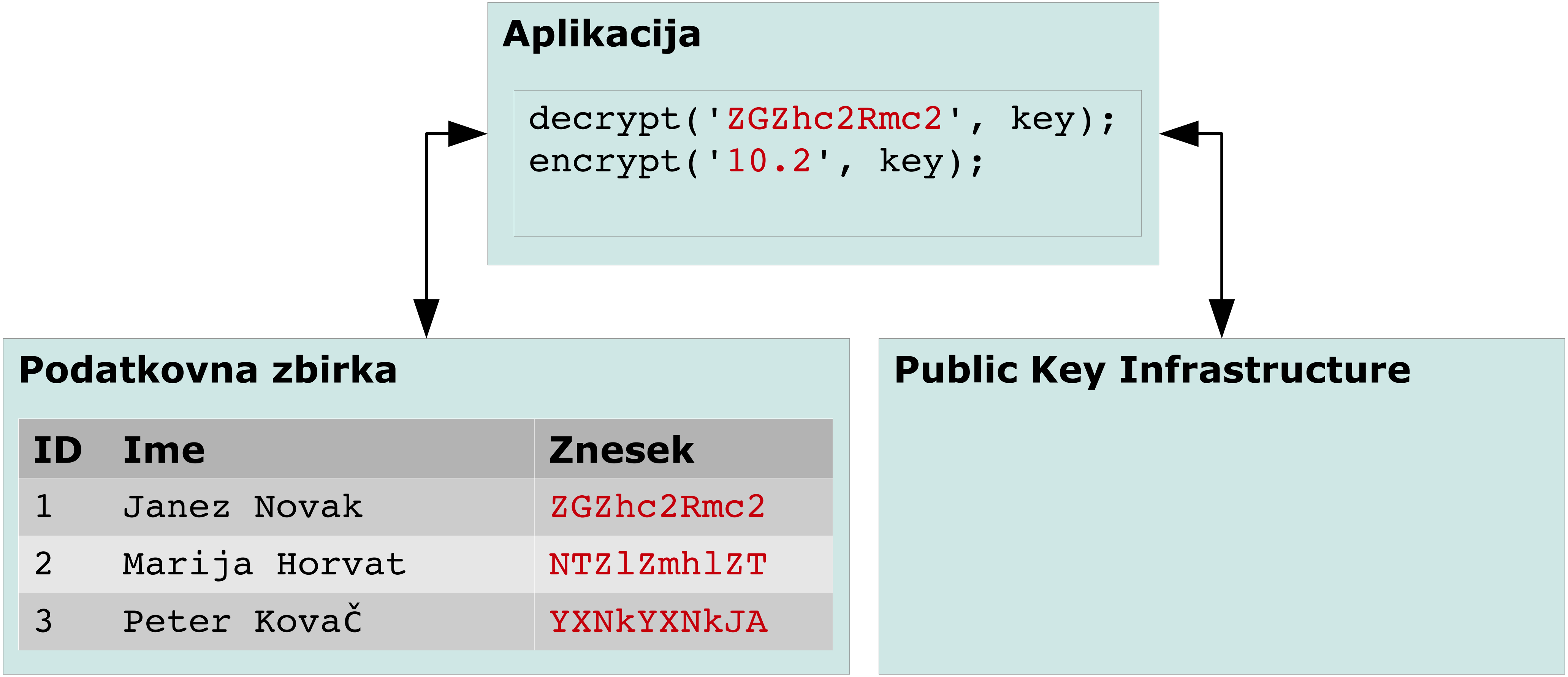


Transparent Data Encryption


Transparent Data Encryption
Attempt to Directly Access Tablespace File Contents
Oracle Database
Managed Keys
Tablespace Files (financials.dbf)
Unauthorized Access to Data Blocked By Encryption
OS User

Primeri aplikativnih rešitev

- CREATE VIEW :)
- PKI, za enkripcijo kolone skrbi aplikacija



Aplikacija

```
decrypt('ZGZhc2Rmc2', key);
encrypt('10.2', key);
```

Podatkovna zbirka

ID	Ime	Znesek
1	Janez Novak	ZGZhc2Rmc2
2	Marija Horvat	NTZlZmhlZT
3	Peter Kovač	YXNkYXNkJA

Public Key Infrastructure

Revizijske sledi

- Višji nivoji ponujajo več aplikativnih podatkov
- Nižji nivoji ponujajo bolj generične podatke

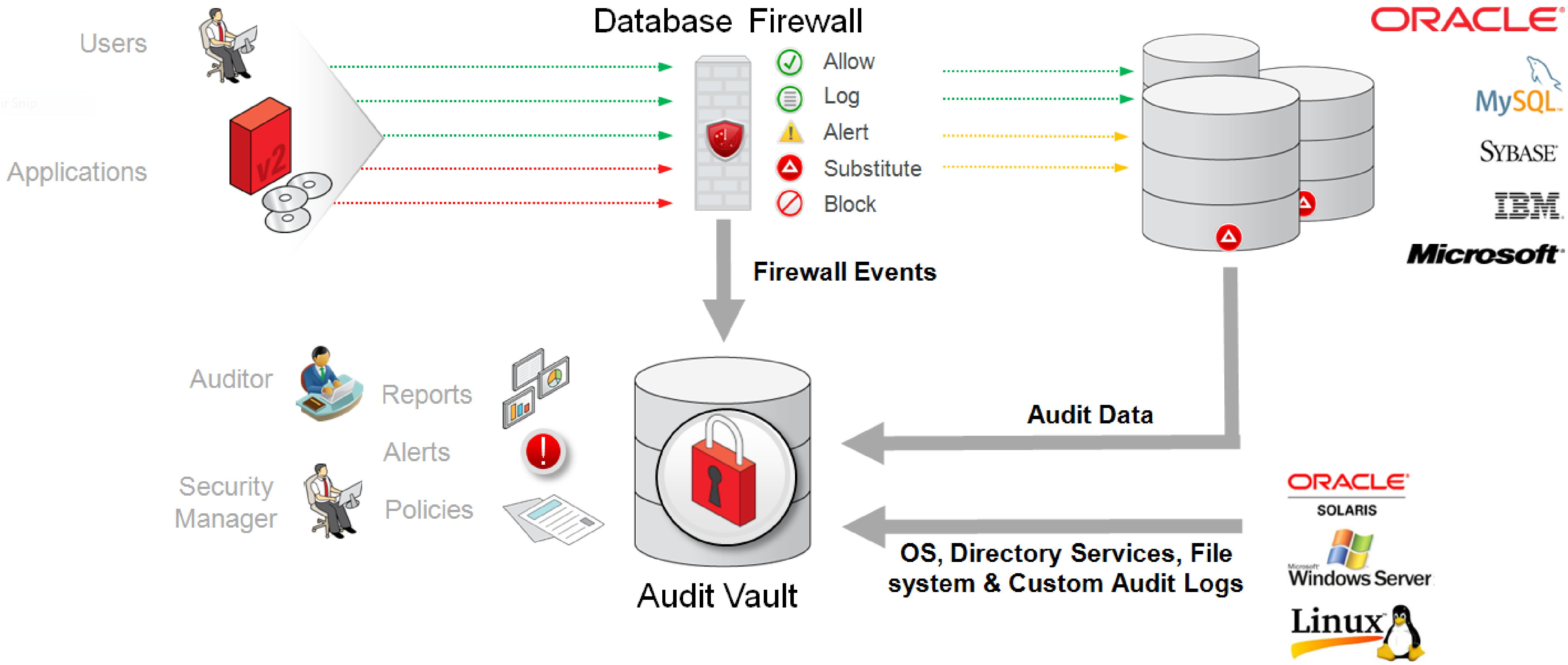
- Nivoji rev. sledi:
  - Aplikacija
  - Podatkovna zbirka
  - Operacijski sistem
  - Omrežje

Rešitve

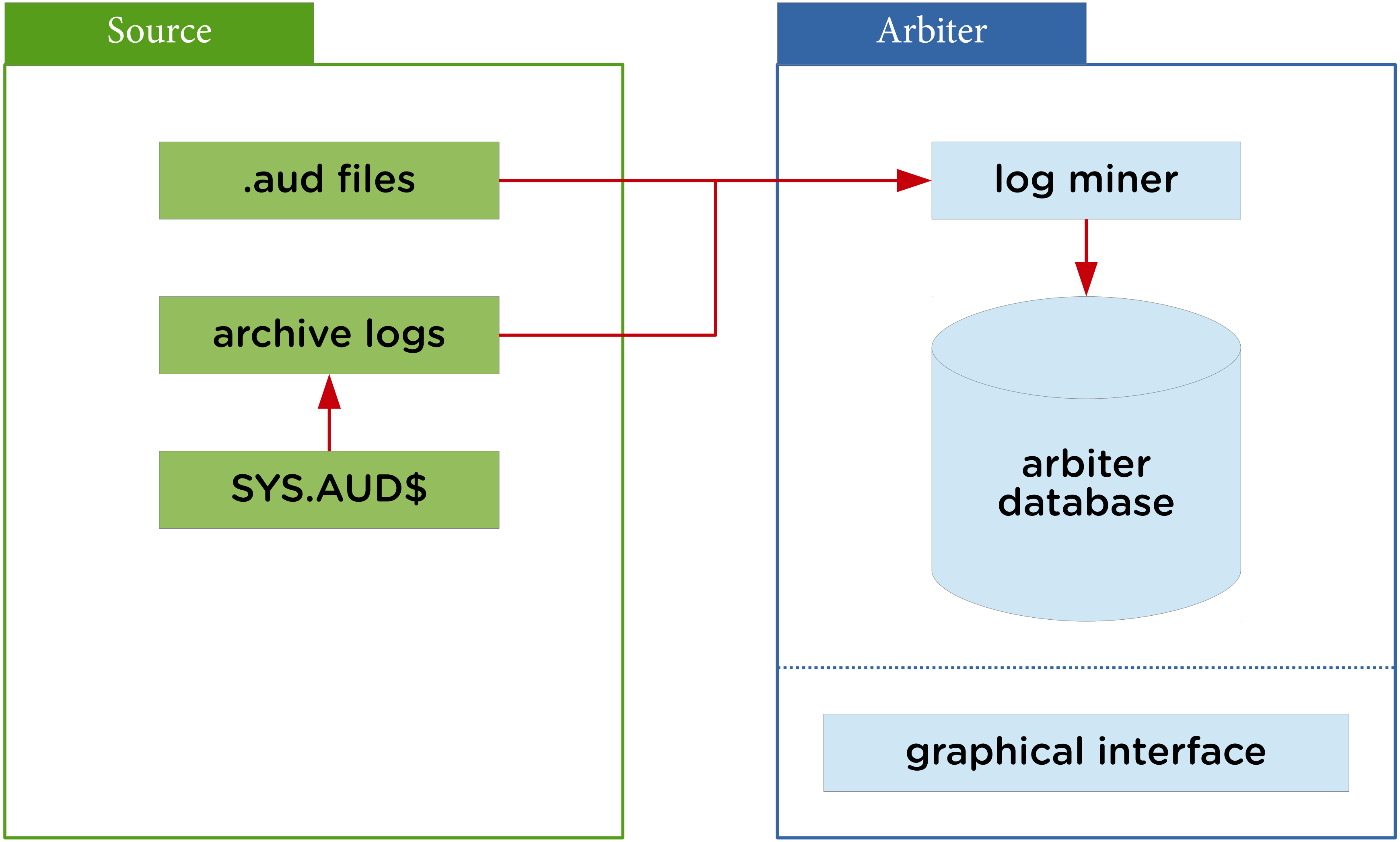
- Oracle Audit Vault
- Abakus Arbiter

- Splunk
- ELK (Elastic Search, Logstash, Kibana)

Oracle Audit Vault



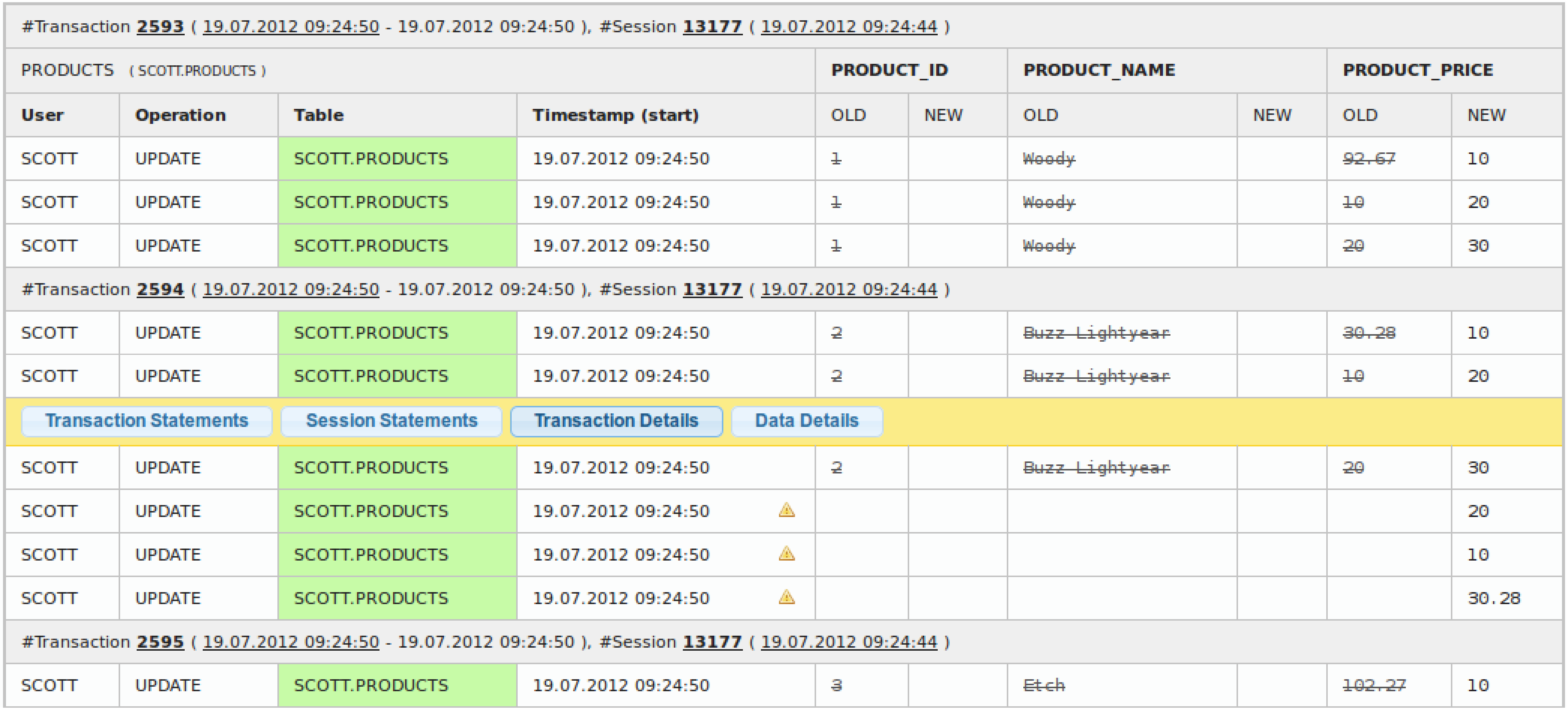
Abakus Arbiter



Abakus Arbiter

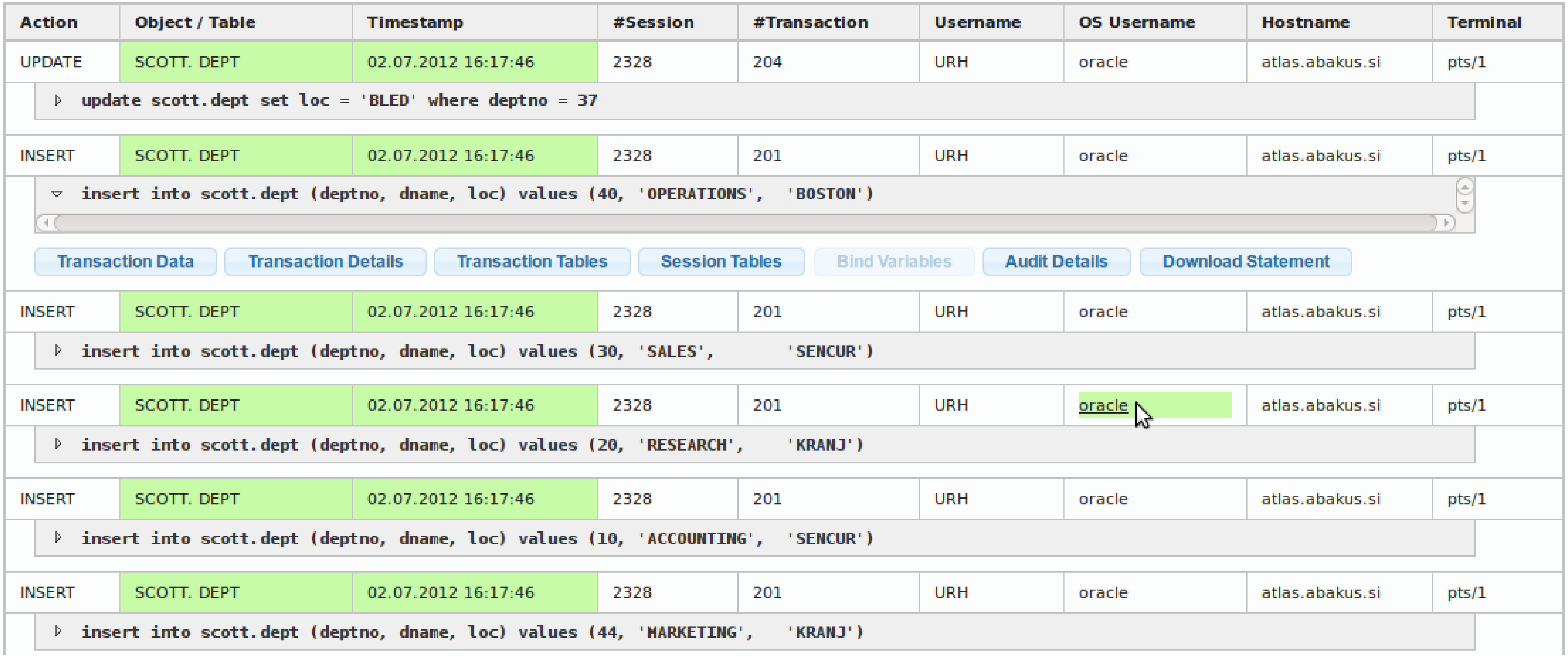
- Arbiter ALP
- Query Analytics
  - SELECT Parser
  - PLAN Analyzer
  - Remote Query Test

Arbiter – Screenshot 1



#Transaction **2593** (19.07.2012 09:24:50 - 19.07.2012 09:24:50), #Session **13177** (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~~		~~Woody~~		~~92.67~~	10
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	~~1~~		~~Woody~~		~~10~~	20
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	~~1~~		~~Woody~~		~~20~~	30
#Transaction **2594** (19.07.2012 09:24:50 - 19.07.2012 09:24:50), #Session **13177** (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
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 **2595** (19.07.2012 09:24:50 - 19.07.2012 09:24:50), #Session **13177** (19.07.2012 09:24:44)									
SCOTT	UPDATE	SCOTT.PRODUCTS	19.07.2012 09:24:50	~~3~~		~~Etch~~		~~102.27~~	10

Arbiter – Screenshot 2

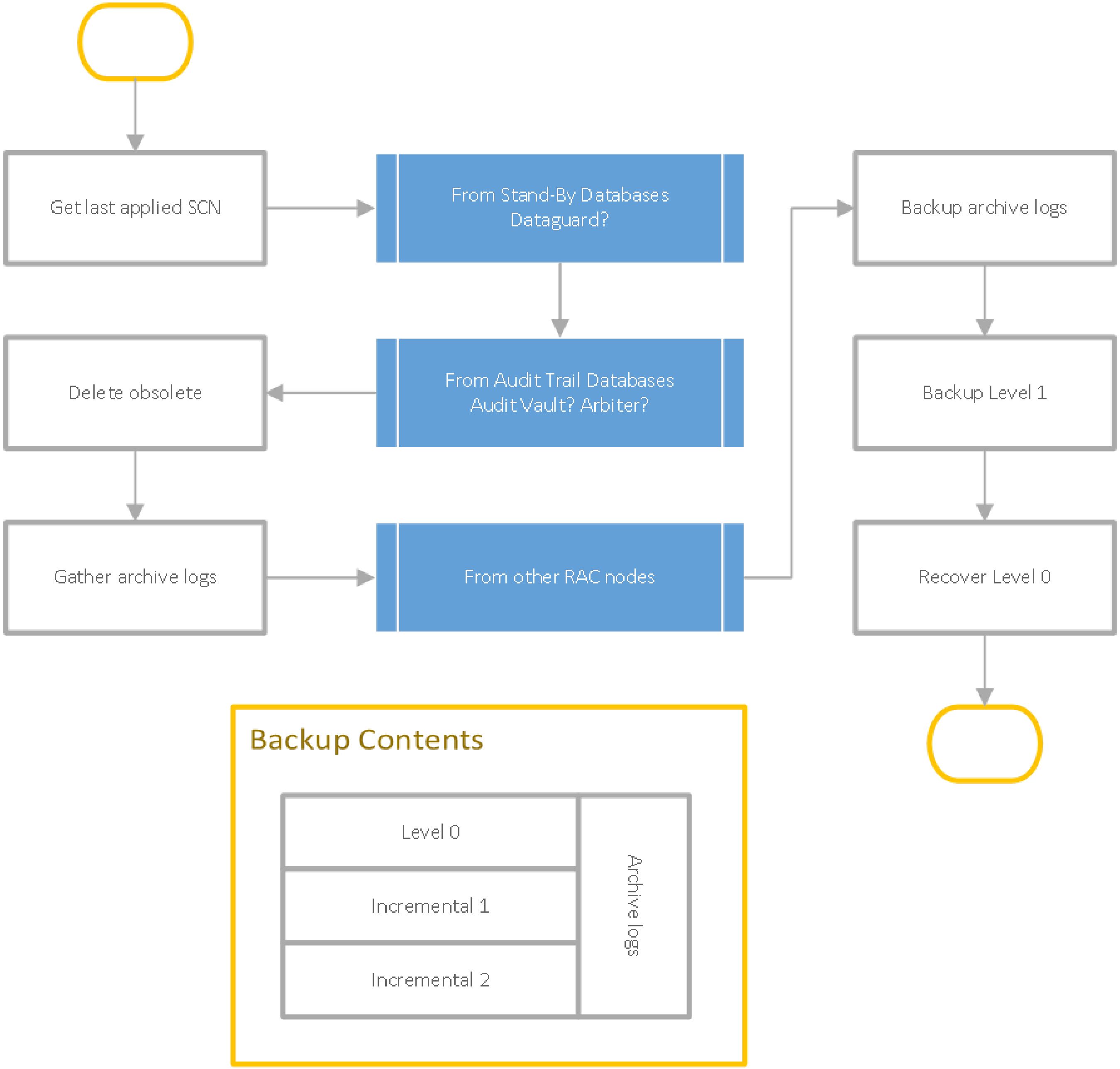


<table>
<tr><th>Action</th><th>Object / Table</th><th>Timestamp</th><th>#Session</th><th>#Transaction</th><th>Username</th><th>OS Username</th><th>Hostname</th><th>Terminal</th></tr>
<tr><td>UPDATE</td><td>SCOTT. DEPT</td><td>02.07.2012 16:17:46</td><td>2328</td><td>204</td><td>URH</td><td>oracle</td><td>atlas.abakus.si</td><td>pts/1</td></tr>
<tr><td colspan="9">▷ update scott.dept set loc = 'BLED' where deptno = 37</td></tr>
<tr><td>INSERT</td><td>SCOTT. DEPT</td><td>02.07.2012 16:17:46</td><td>2328</td><td>201</td><td>URH</td><td>oracle</td><td>atlas.abakus.si</td><td>pts/1</td></tr>
<tr><td colspan="9">▽ insert into scott.dept (deptno, dname, loc) values (40, 'OPERATIONS', 'BOSTON')</td></tr>
<tr><td colspan="9">Transaction Data | Transaction Details | Transaction Tables | Session Tables | Bind Variables | Audit Details | Download Statement</td></tr>
<tr><td>INSERT</td><td>SCOTT. DEPT</td><td>02.07.2012 16:17:46</td><td>2328</td><td>201</td><td>URH</td><td>oracle</td><td>atlas.abakus.si</td><td>pts/1</td></tr>
<tr><td colspan="9">▷ insert into scott.dept (deptno, dname, loc) values (30, 'SALES', 'SENCUR')</td></tr>
<tr><td>INSERT</td><td>SCOTT. DEPT</td><td>02.07.2012 16:17:46</td><td>2328</td><td>201</td><td>URH</td><td>oracle</td><td>atlas.abakus.si</td><td>pts/1</td></tr>
<tr><td colspan="9">▷ insert into scott.dept (deptno, dname, loc) values (20, 'RESEARCH', 'KRANJ')</td></tr>
<tr><td>INSERT</td><td>SCOTT. DEPT</td><td>02.07.2012 16:17:46</td><td>2328</td><td>201</td><td>URH</td><td>oracle</td><td>atlas.abakus.si</td><td>pts/1</td></tr>
<tr><td colspan="9">▷ insert into scott.dept (deptno, dname, loc) values (10, 'ACCOUNTING', 'SENCUR')</td></tr>
<tr><td>INSERT</td><td>SCOTT. DEPT</td><td>02.07.2012 16:17:46</td><td>2328</td><td>201</td><td>URH</td><td>oracle</td><td>atlas.abakus.si</td><td>pts/1</td></tr>
<tr><td colspan="9">▷ insert into scott.dept (deptno, dname, loc) values (44, 'MARKETING', 'KRANJ')</td></tr>
</table>

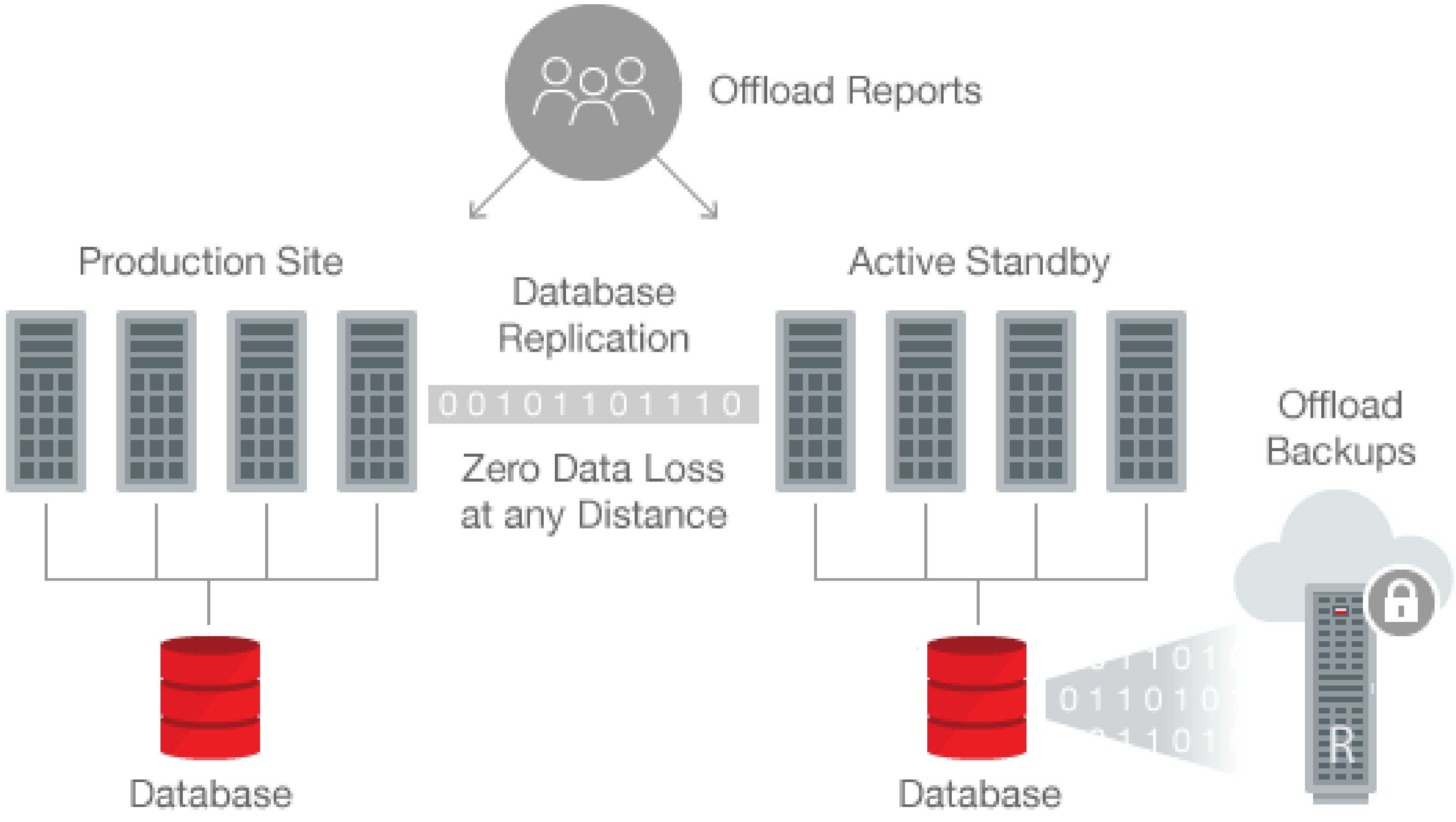
Odpoved strojne ali programske opreme

- Redundanca
  - Backup
  - Fizični standby
  - Real Application Clusters
  - Abakus(r) Active Backup Server

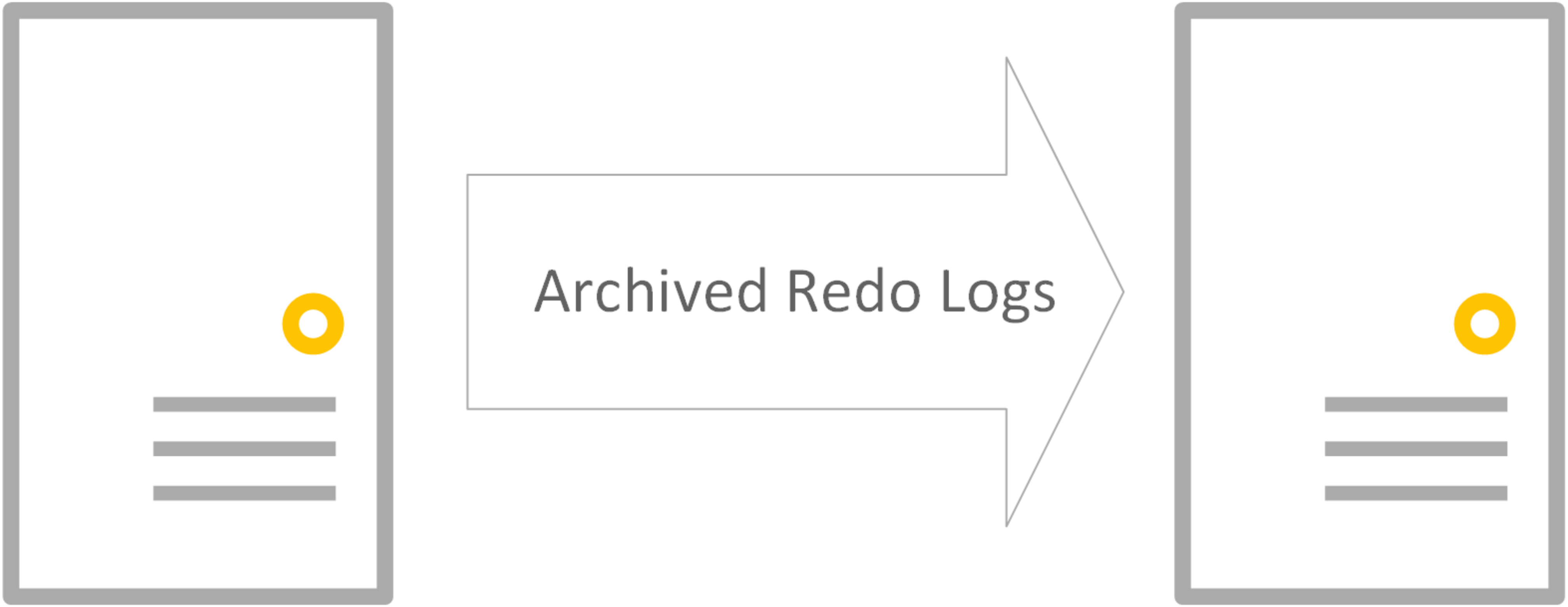
Abakus Amon - Backup Script



Oracle Data Guard – fizični standby

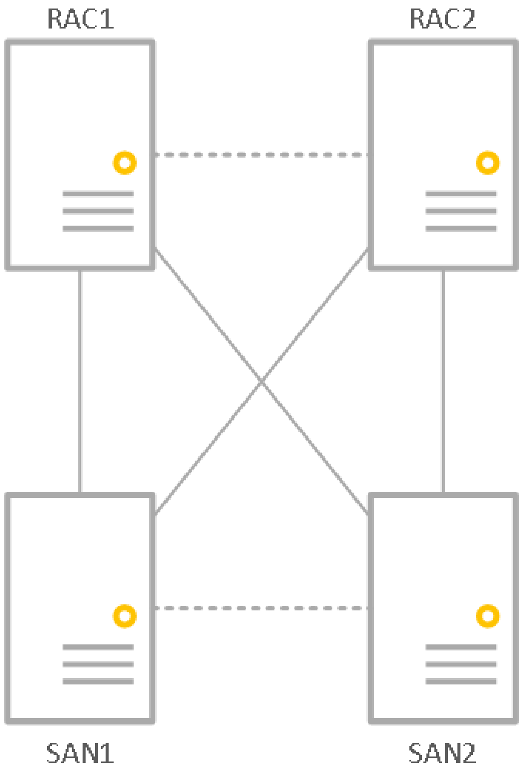


Abakus Amon - fizični standby



Oracle Real Application Clusters

- Ščiti ***samo*** pred odpovedjo strojne opreme
- ***Ne ščiti pa*** pred aplikacijskimi napakami.
- V nekaterih primerih se mora aplikacija zavedat, da teče v RAC okolju:
  - gv$view vs v$view
  - dbms_pipe, dbms_service, …

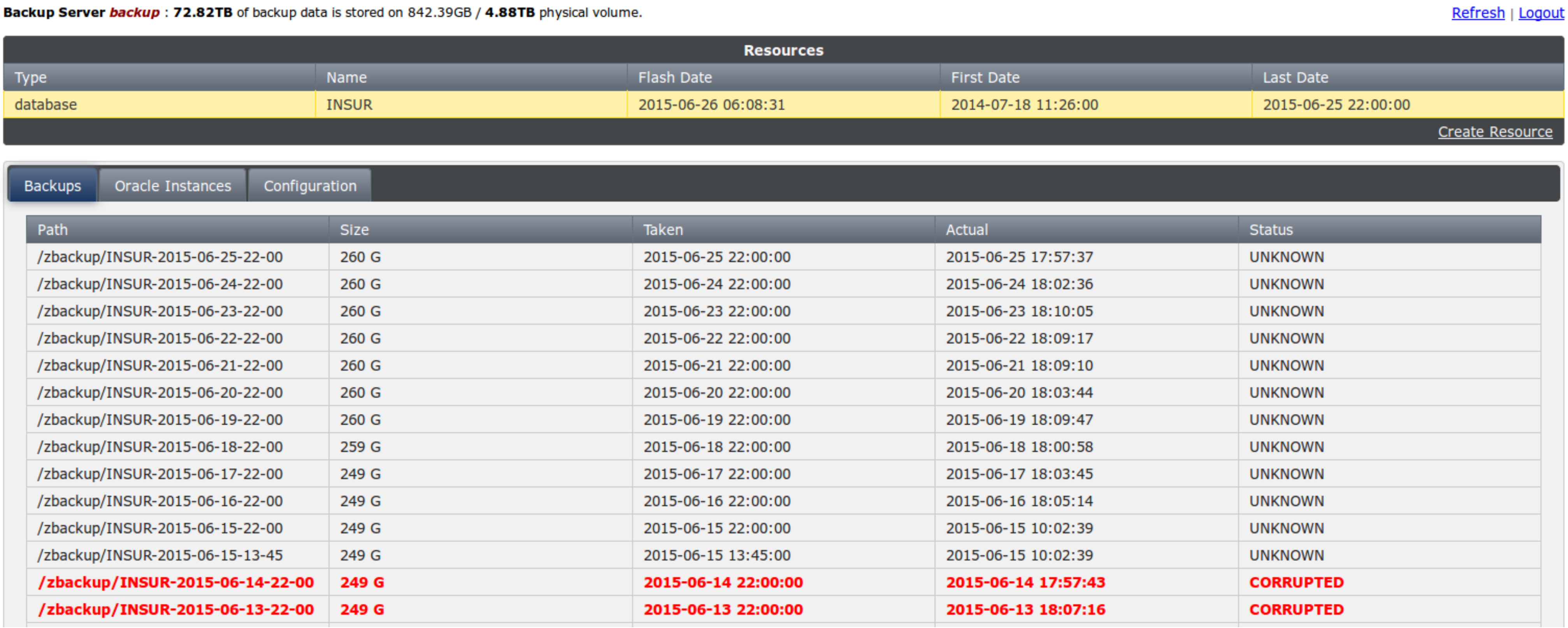


Abakus Backup Server

- “Stand-By” prostor
  - Na njem teče trenutna kopija fizičnega standby.
- Kompresirani prostor
  - Za shranjevanje arhivskih dnevniških datotek.
- Deduplicirani prostor
  - Vsebuje dnevne varnostne kopije podatkovnih zbirk.

- ***431,98TB*** *of backup data is stored on 17,53TB / 20,00TB physical volume.*

Abakus Backup Server



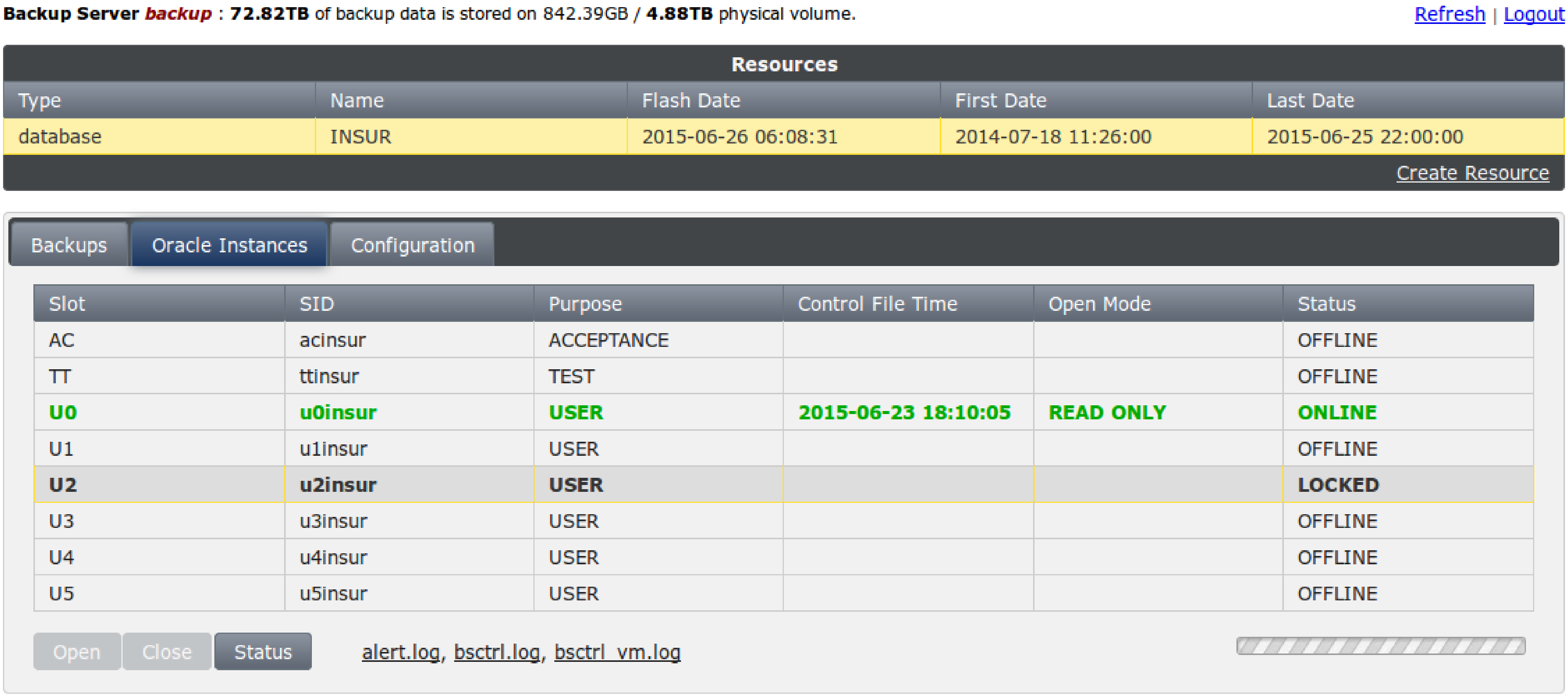
Backup Server ***backup*** : **72.82TB** of backup data is stored on 842.39GB / **4.88TB** physical volume.

Resources

Type	Name	Flash Date	First Date	Last Date
database	INSUR	2015-06-26 06:08:31	2014-07-18 11:26:00	2015-06-25 22:00:00

Path	Size	Taken	Actual	Status
/zbackup/INSUR-2015-06-25-22-00	260 G	2015-06-25 22:00:00	2015-06-25 17:57:37	UNKNOWN
/zbackup/INSUR-2015-06-24-22-00	260 G	2015-06-24 22:00:00	2015-06-24 18:02:36	UNKNOWN
/zbackup/INSUR-2015-06-23-22-00	260 G	2015-06-23 22:00:00	2015-06-23 18:10:05	UNKNOWN
/zbackup/INSUR-2015-06-22-22-00	260 G	2015-06-22 22:00:00	2015-06-22 18:09:17	UNKNOWN
/zbackup/INSUR-2015-06-21-22-00	260 G	2015-06-21 22:00:00	2015-06-21 18:09:10	UNKNOWN
/zbackup/INSUR-2015-06-20-22-00	260 G	2015-06-20 22:00:00	2015-06-20 18:03:44	UNKNOWN
/zbackup/INSUR-2015-06-19-22-00	260 G	2015-06-19 22:00:00	2015-06-19 18:09:47	UNKNOWN
/zbackup/INSUR-2015-06-18-22-00	259 G	2015-06-18 22:00:00	2015-06-18 18:00:58	UNKNOWN
/zbackup/INSUR-2015-06-17-22-00	249 G	2015-06-17 22:00:00	2015-06-17 18:03:45	UNKNOWN
/zbackup/INSUR-2015-06-16-22-00	249 G	2015-06-16 22:00:00	2015-06-16 18:05:14	UNKNOWN
/zbackup/INSUR-2015-06-15-22-00	249 G	2015-06-15 22:00:00	2015-06-15 10:02:39	UNKNOWN
/zbackup/INSUR-2015-06-15-13-45	249 G	2015-06-15 13:45:00	2015-06-15 10:02:39	UNKNOWN
/zbackup/INSUR-2015-06-14-22-00	**249 G**	**2015-06-14 22:00:00**	**2015-06-14 17:57:43**	**CORRUPTED**
/zbackup/INSUR-2015-06-13-22-00	**249 G**	**2015-06-13 22:00:00**	**2015-06-13 18:07:16**	**CORRUPTED**

Abakus Backup Server



Backup Server ***backup*** : **72.82TB** of backup data is stored on 842.39GB / **4.88TB** physical volume.

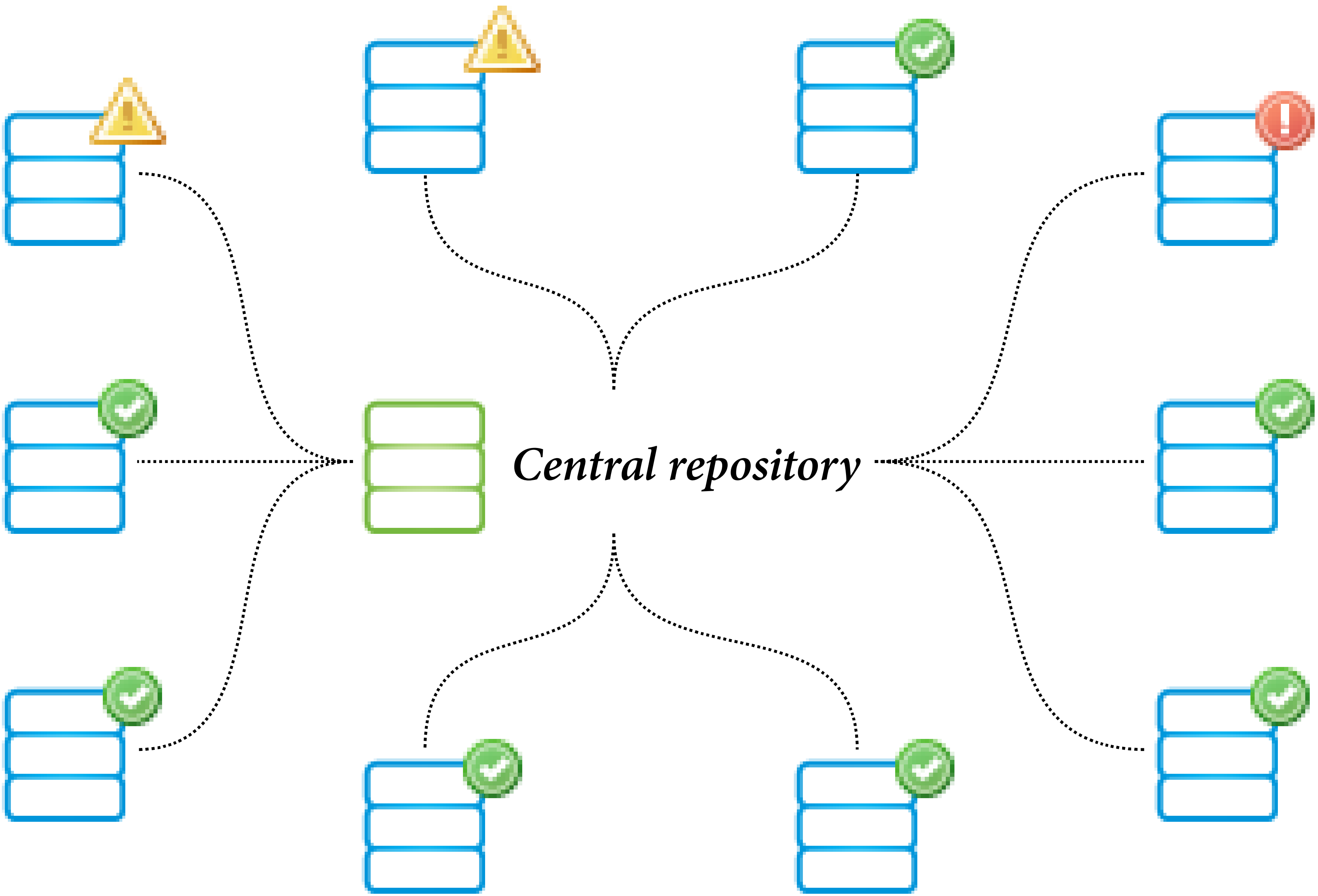
Resources

Type	Name	Flash Date	First Date	Last Date
database	INSUR	2015-06-26 06:08:31	2014-07-18 11:26:00	2015-06-25 22:00:00

Slot	SID	Purpose	Control File Time	Open Mode	Status
AC	acinsur	ACCEPTANCE			OFFLINE
TT	ttinsur	TEST			OFFLINE
U0	**u0insur**	**USER**	**2015-06-23 18:10:05**	**READ ONLY**	**ONLINE**
U1	u1insur	USER			OFFLINE
U2	**u2insur**	**USER**			**LOCKED**
U3	u3insur	USER			OFFLINE
U4	u4insur	USER			OFFLINE
U5	u5insur	USER			OFFLINE

alert.log, bsctrl.log, bsctrl_vm.log

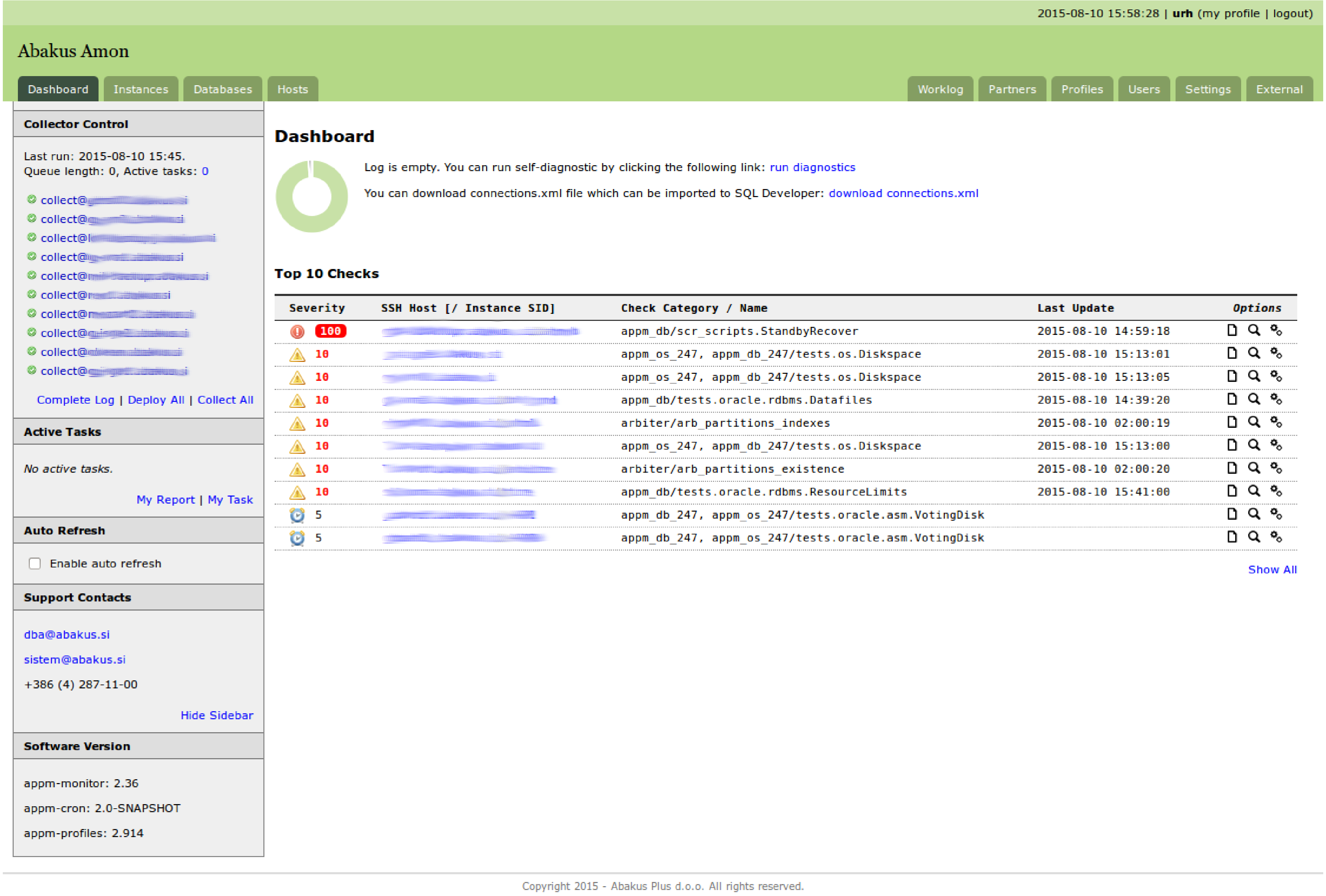
Central IT Monitoring



Central IT Monitoring – Solutions

- Microsoft Operations Manager
- Oracle Enterprise Manager
- Nagios
- **Abakus AMON**

AMON Screenshot 1



Collector Control

Last run: 2015-08-10 15:45.
Queue length: 0, Active tasks: 0

- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]

Complete Log | Deploy All | Collect All

Active Tasks

No active tasks.

My Report | My Task

Auto Refresh

□ Enable auto refresh

Support Contacts

dba@abakus.si

sistem@abakus.si

+386 (4) 287-11-00

Hide Sidebar

Software Version

appm-monitor: 2.36

appm-cron: 2.0-SNAPSHOT

appm-profiles: 2.914

Dashboard

Log is empty. You can run self-diagnostic by clicking the following link: run diagnostics

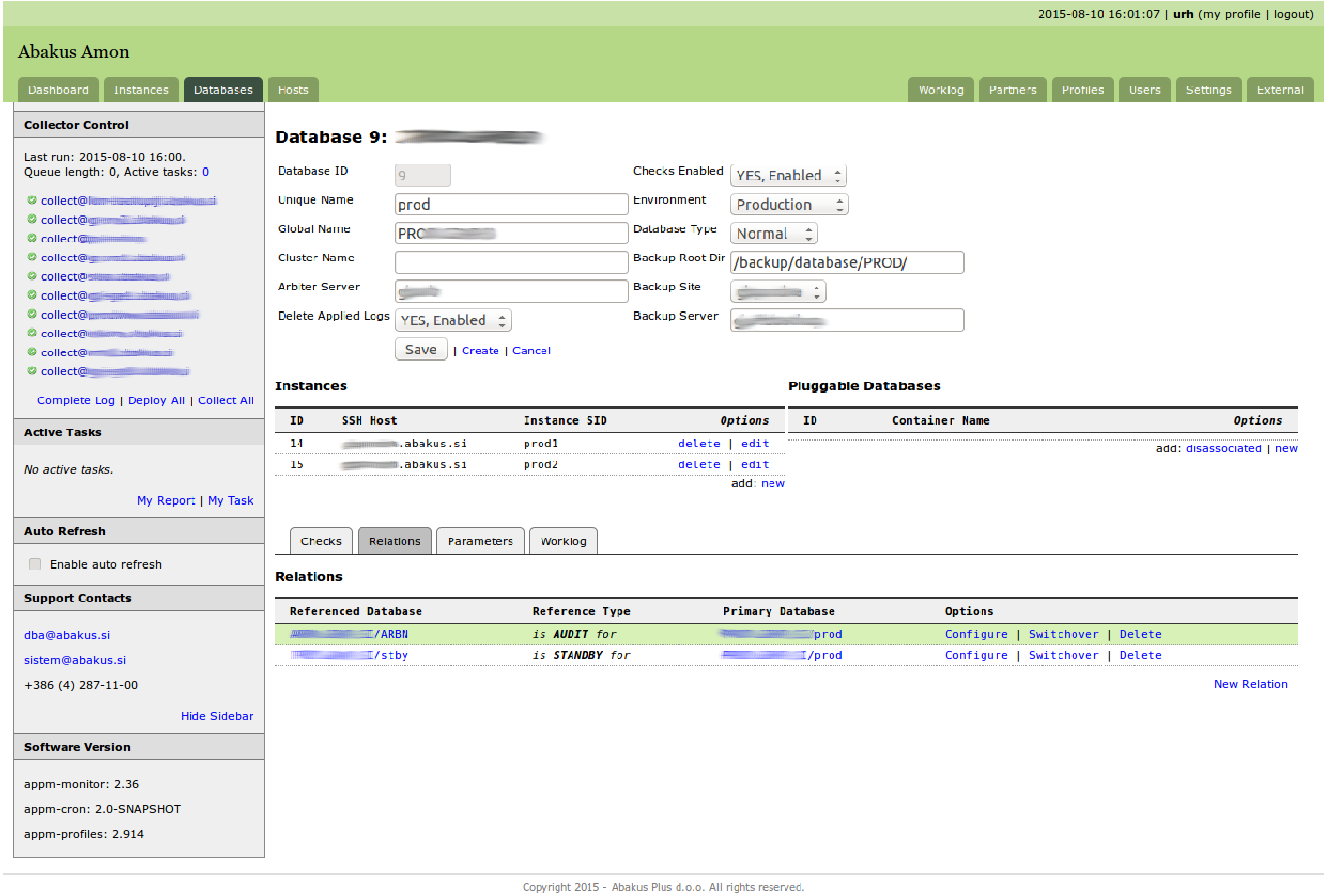
You can download connections.xml file which can be imported to SQL Developer: download connections.xml

Top 10 Checks

Severity	SSH Host [/ Instance SID]	Check Category / Name	Last Update	*Options*
! 100	[redacted]	appm_db/scr_scripts.StandbyRecover	2015-08-10 14:59:18	🗋 🔍 ⚙
⚠ 10	[redacted]	appm_os_247, appm_db_247/tests.os.Diskspace	2015-08-10 15:13:01	🗋 🔍 ⚙
⚠ 10	[redacted]	appm_os_247, appm_db_247/tests.os.Diskspace	2015-08-10 15:13:05	🗋 🔍 ⚙
⚠ 10	[redacted]	appm_db/tests.oracle.rdbms.Datafiles	2015-08-10 14:39:20	🗋 🔍 ⚙
⚠ 10	[redacted]	arbiter/arb_partitions_indexes	2015-08-10 02:00:19	🗋 🔍 ⚙
⚠ 10	[redacted]	appm_os_247, appm_db_247/tests.os.Diskspace	2015-08-10 15:13:00	🗋 🔍 ⚙
⚠ 10	[redacted]	arbiter/arb_partitions_existence	2015-08-10 02:00:20	🗋 🔍 ⚙
⚠ 10	[redacted]	appm_db/tests.oracle.rdbms.ResourceLimits	2015-08-10 15:41:00	🗋 🔍 ⚙
⏰ 5	[redacted]	appm_db_247, appm_os_247/tests.oracle.asm.VotingDisk		🗋 🔍 ⚙
⏰ 5	[redacted]	appm_db_247, appm_os_247/tests.oracle.asm.VotingDisk		🗋 🔍 ⚙

Show All

Amon Screenshot 2



2015-08-10 16:01:07 | **urh** (my profile | logout)

Abakus Amon

Collector Control

Last run: 2015-08-10 16:00.
Queue length: 0, Active tasks: 0

- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]
- collect@[redacted]

Complete Log | Deploy All | Collect All

Active Tasks

No active tasks.

My Report | My Task

Auto Refresh

□ Enable auto refresh

Support Contacts

dba@abakus.si

sistem@abakus.si

+386 (4) 287-11-00

Hide Sidebar

Software Version

appm-monitor: 2.36

appm-cron: 2.0-SNAPSHOT

appm-profiles: 2.914

Database 9: [redacted]

Database ID	9	Checks Enabled	YES, Enabled
Unique Name	prod	Environment	Production
Global Name	PRO[redacted]	Database Type	Normal
Cluster Name		Backup Root Dir	/backup/database/PROD/
Arbiter Server	[redacted]	Backup Site	[redacted]
Delete Applied Logs	YES, Enabled	Backup Server	[redacted]

Save | Create | Cancel

Instances

ID	SSH Host	Instance SID	*Options*
14	[redacted].abakus.si	prod1	delete | edit
15	[redacted].abakus.si	prod2	delete | edit

add: new

Pluggable Databases

ID	Container Name	*Options*

add: disassociated | new

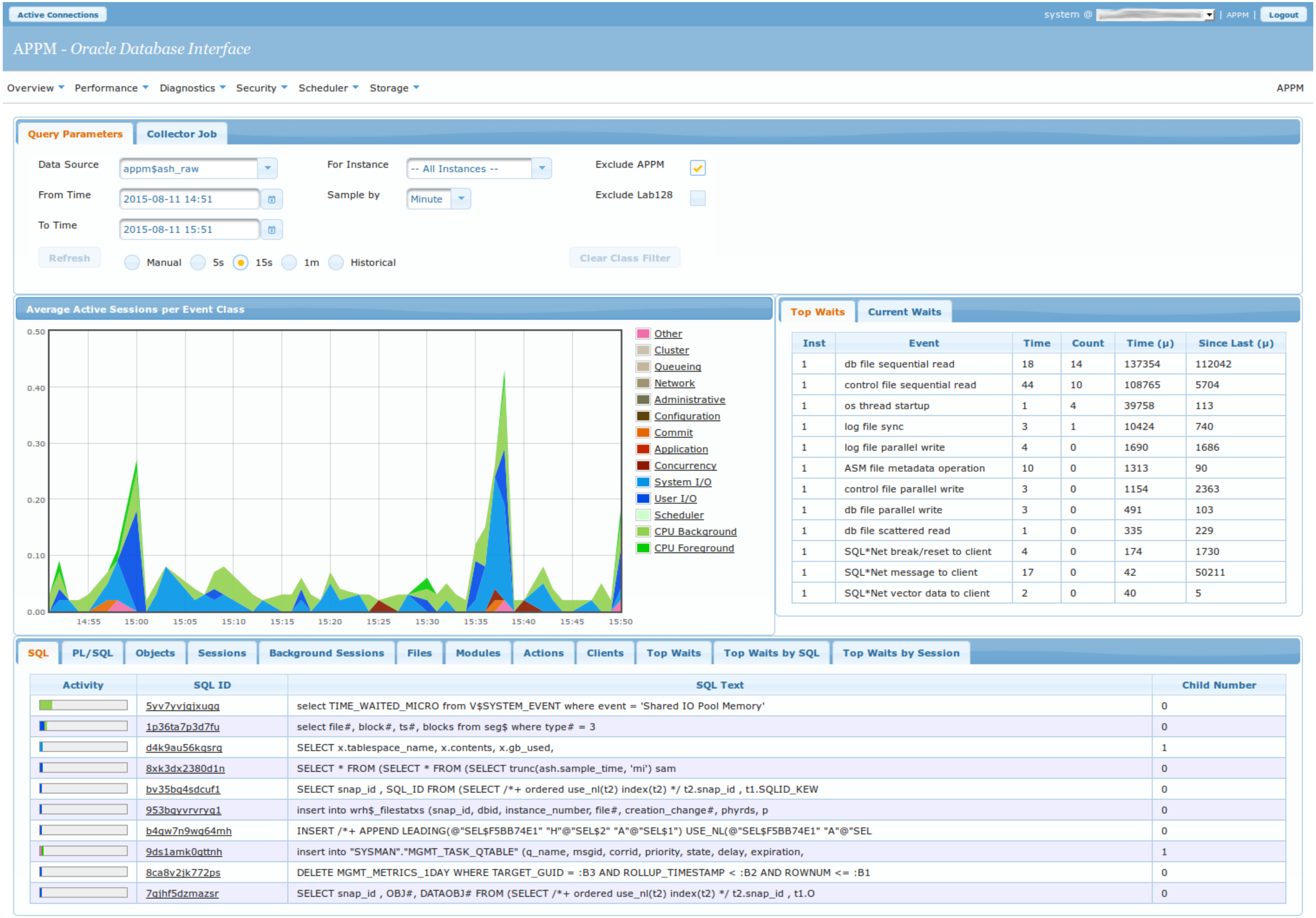
Relations

Referenced Database	Reference Type	Primary Database	Options
[redacted]/ARBN	*is **AUDIT** for*	[redacted]/prod	Configure | Switchover | Delete
[redacted]/stby	*is **STANDBY** for*	[redacted]/prod	Configure | Switchover | Delete

New Relation

Copyright 2015 - Abakus Plus d.o.o. All rights reserved.

APPM Screenshot



Data Source: appm$ash_raw

For Instance: -- All Instances --

Exclude APPM ☑

From Time: 2015-08-11 14:51

Sample by: Minute

Exclude Lab128 □

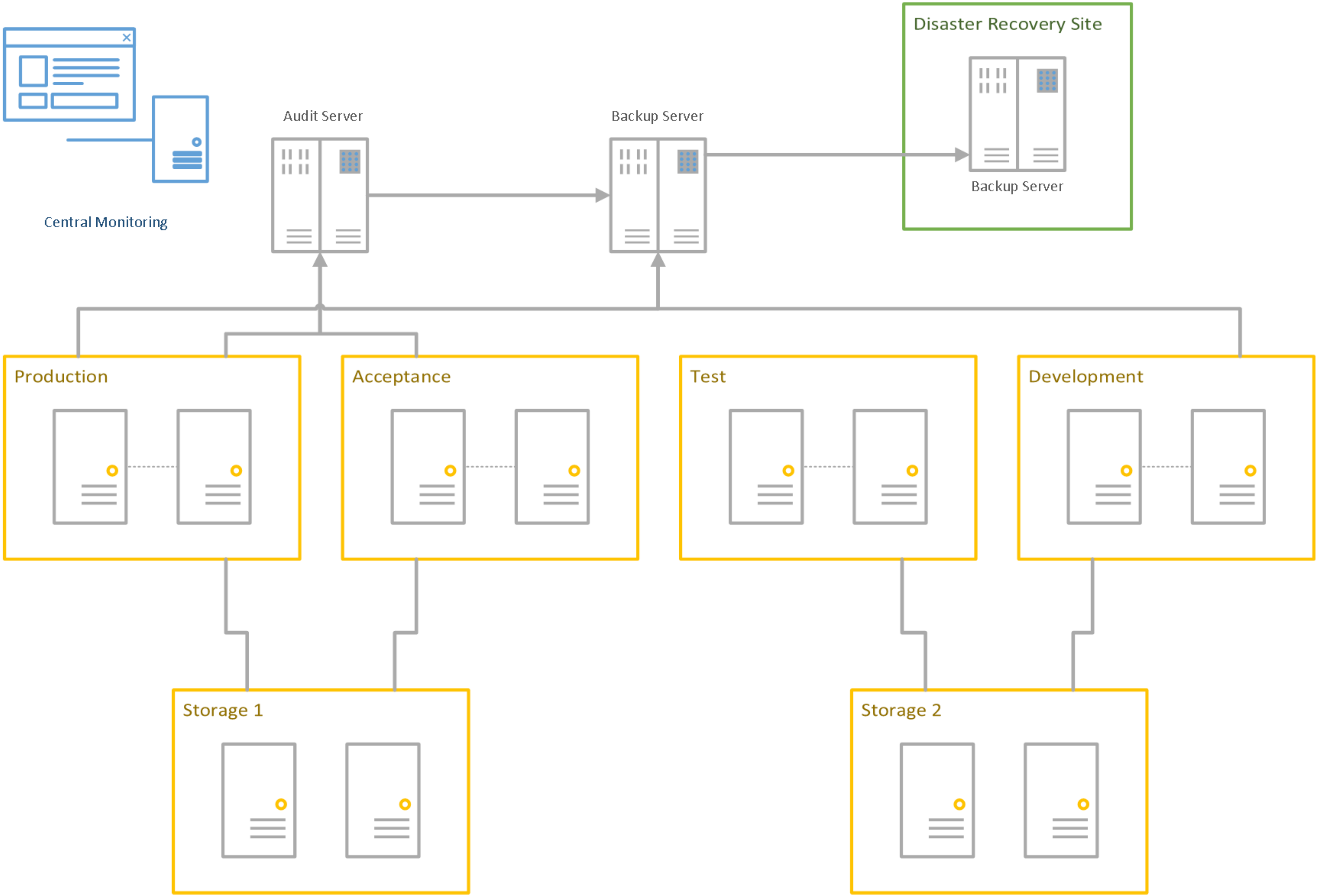
To Time: 2015-08-11 15:51

○ Manual ○ 5s ● 15s ○ 1m ○ Historical

Inst	Event	Time	Count	Time (μ)	Since Last (μ)
1	db file sequential read	18	14	137354	112042
1	control file sequential read	44	10	108765	5704
1	os thread startup	1	4	39758	113
1	log file sync	3	1	10424	740
1	log file parallel write	4	0	1690	1686
1	ASM file metadata operation	10	0	1313	90
1	control file parallel write	3	0	1154	2363
1	db file parallel write	3	0	491	103
1	db file scattered read	1	0	335	229
1	SQL*Net break/reset to client	4	0	174	1730
1	SQL*Net message to client	17	0	42	50211
1	SQL*Net vector data to client	2	0	40	5

Activity	SQL ID	SQL Text	Child Number
	5yv7yvjqjxuqg	select TIME_WAITED_MICRO from V$SYSTEM_EVENT where event = 'Shared IO Pool Memory'	0
	1p36ta7p3d7fu	select file#, block#, ts#, blocks from seg$ where type# = 3	0
	d4k9au56kqsrq	SELECT x.tablespace_name, x.contents, x.gb_used,	1
	8xk3dx2380d1n	SELECT * FROM (SELECT * FROM (SELECT trunc(ash.sample_time, 'mi') sam	0
	bv35bq4sdcuf1	SELECT snap_id , SQL_ID FROM (SELECT /*+ ordered use_nl(t2) index(t2) */ t2.snap_id , t1.SQLID_KEW	0
	953bqyvrvryq1	insert into wrh$_filestatxs (snap_id, dbid, instance_number, file#, creation_change#, phyrds, p	0
	b4qw7n9wq64mh	INSERT /*+ APPEND LEADING(@"SEL$F5BB74E1" "H"@"SEL$2" "A"@"SEL$1") USE_NL(@"SEL$F5BB74E1" "A"@"SEL	0
	9ds1amk0qttnh	insert into "SYSMAN"."MGMT_TASK_QTABLE" (q_name, msgid, corrid, priority, state, delay, expiration,	1
	8ca8v2jk772ps	DELETE MGMT_METRICS_1DAY WHERE TARGET_GUID = :B3 AND ROLLUP_TIMESTAMP < :B2 AND ROWNUM <= :B1	0
	7qjhf5dzmazsr	SELECT snap_id , OBJ#, DATAOBJ# FROM (SELECT /*+ ordered use_nl(t2) index(t2) */ t2.snap_id , t1.O	0

The Big Picture?

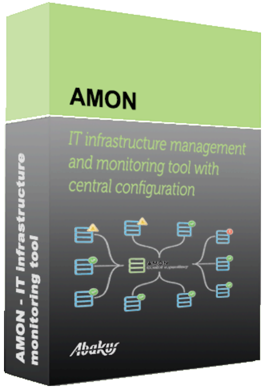


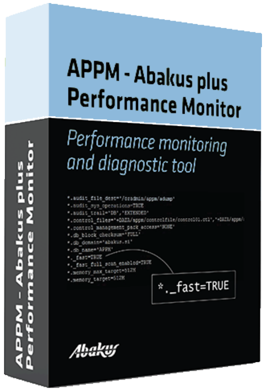
AS

Abakus

As na disku.

Arbiter
Celovita rešitev za upravljanje revizijskih sledi
Zaupanja vredne sledi
Arbiter - celovita rešitev za upravljanje revizijskih sledi
Abakus


AMON
IT infrastructure management and monitoring tool with central configuration
AMON - IT infrastructure monitoring tool
Abakus


APPM - Abakus plus Performance Monitor
Performance monitoring and diagnostic tool
*._fast=TRUE
APPM - Abakus plus Performance Monitor
Abakus

```
*.audit_file_dest='/oradmin/appm/adump'
*.audit_sys_operations=TRUE
*.audit_trail='DB','EXTENDED'
*.control_files='+DATA/appm/controlfile/control01.ctl','+DATA/appm/
*.control_management_pack_access='NONE'
*.db_block_checksum='FULL'
*.db_domain='abakus.si'
*.db_name='APPM'
*._fast=TRUE
*._fast_full_scan_enabled=TRUE
*.memory_max_target=512M
*.memory_target=512M
```

http://www.abakus.si/