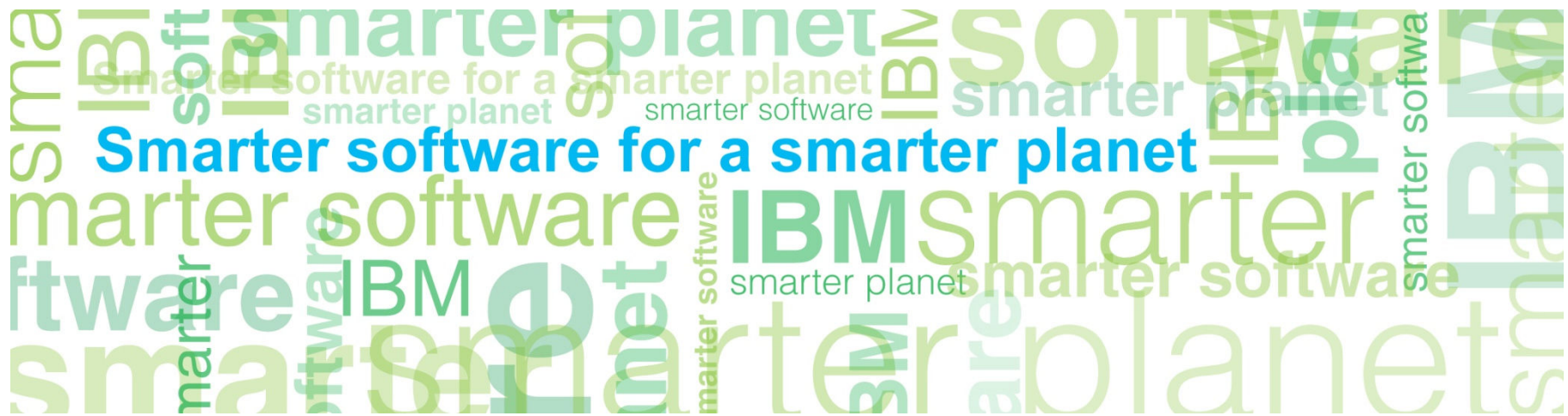


Guardium Roadmap



Disclaimer

© Copyright IBM Corporation 2009. All rights reserved.

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS AND/OR SOFTWARE.

IBM, the IBM logo, ibm.com, and DB2 are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

Addressing all aspects of database security



- Data access audit trails

- Very large estates
- Getting more and more heterogeneous
- Mainframe getting more attention in audits
- Big data starting to get attention – mostly in the US

- Fine grained access control and data protection

- 1/4-1/2 of deployments include a blocking element; differences mostly in geos
- Seeing jump into blocking as part of first implementation rather as follow on
- Asking for even more “fine grained” than blocking

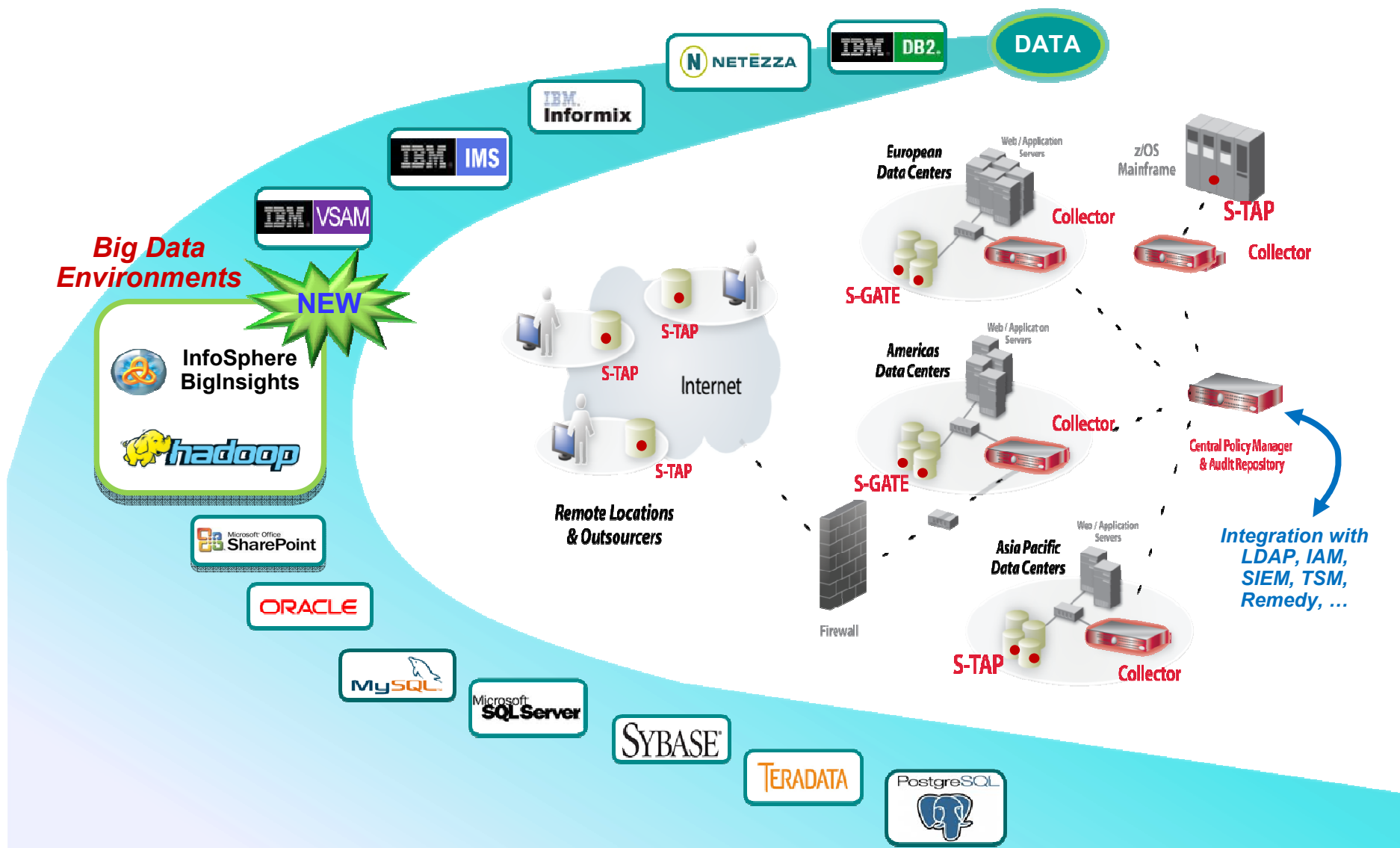
- Vulnerability assessment

- Also very heterogeneous, large estates
- Seeing more deployments that start with VA or do VA in parallel to DAP
- Very easy rollout

- Others

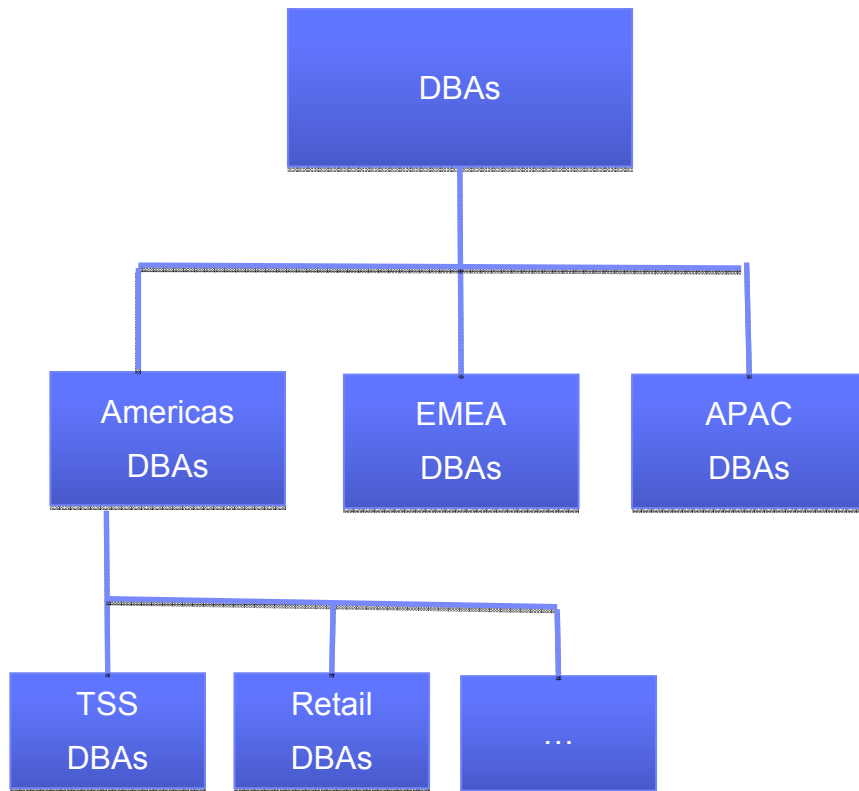
- Entitlement review/mgmt growing
- Discovery still mostly a supporting feature

RDBMS + Big Data + ...



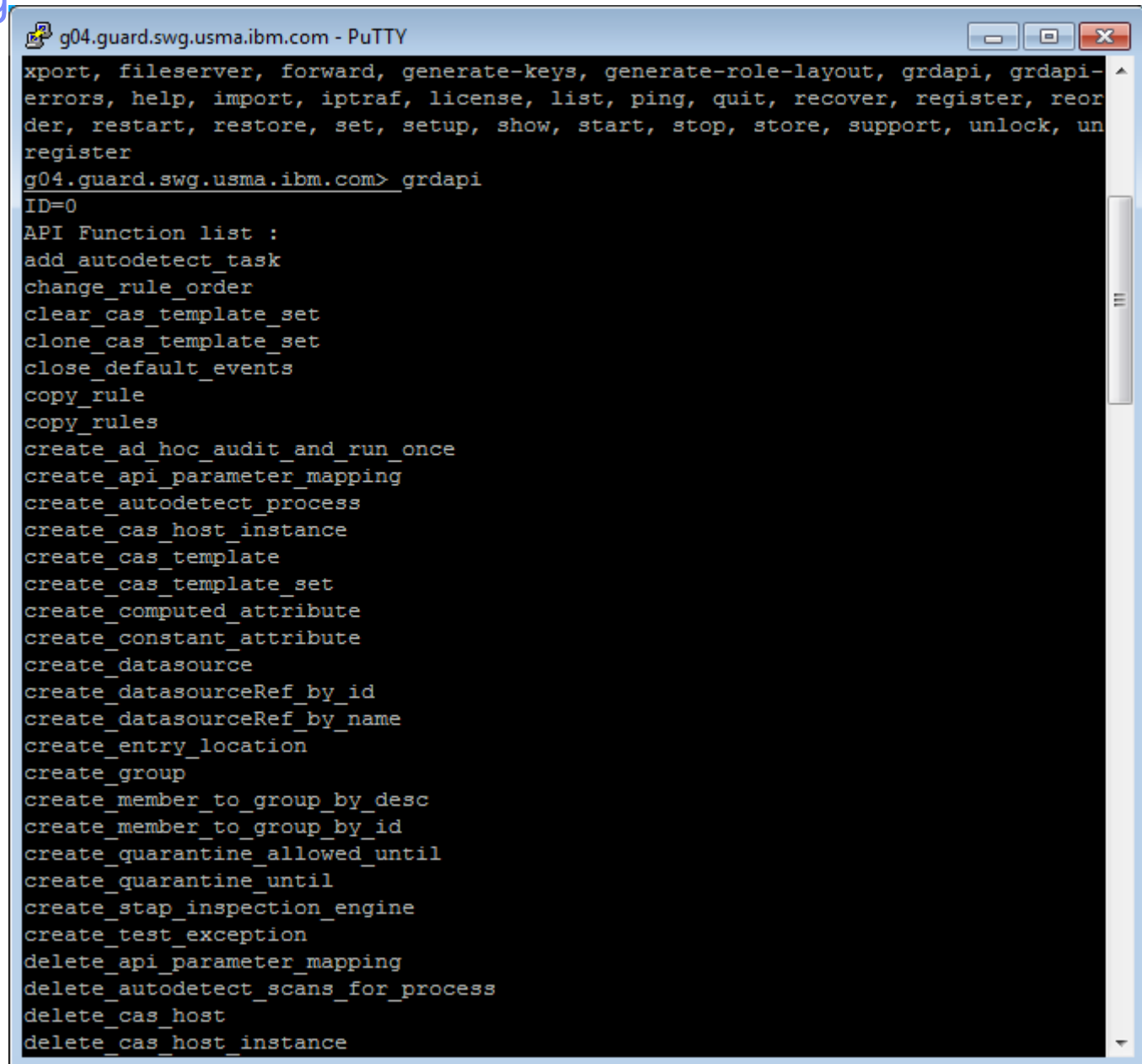
Some features/mechanisms to know about

- Fire-IDs and quarantining
- Hierarchical groups
- Grdapi
- Self-service and DLS
- Compliance workflow
- Diff reports



- Multiple policies at different levels/ownerships
 - Corporate wide, biz units, geo, ..
- Each level with full authorization and control
- All auditable and reportable
- All can affect multiple networks/servers/zones/..

Grdapi & Scripting



```
g04.guard.swg.usma.ibm.com - PuTTY
xport, fileserver, forward, generate-keys, generate-role-layout, grdapi, grdapi-
errors, help, import, iptraf, license, list, ping, quit, recover, register, reor
der, restart, restore, set, setup, show, start, stop, store, support, unlock, un
register
g04.guard.swg.usma.ibm.com> grdapi
ID=0
API Function list :
add_autodetect_task
change_rule_order
clear_cas_template_set
clone_cas_template_set
close_default_events
copy_rule
copy_rules
create_ad_hoc_audit_and_run_once
create_api_parameter_mapping
create_autodetect_process
create_cas_host_instance
create_cas_template
create_cas_template_set
create_computed_attribute
create_constant_attribute
create_datasource
create_datasourceRef_by_id
create_datasourceRef_by_name
create_entry_location
create_group
create_member_to_group_by_desc
create_member_to_group_by_id
create_quarantine_allowed_until
create_quarantine_until
create_stap_inspection_engine
create_test_exception
delete_api_parameter_mapping
delete_autodetect_scans_for_process
delete_cas_host
delete_cas_host_instance
```


- Three levels of user and role-based security – application, element, data
- DLS is key to efficient on-going maintenance
 - No need for multiple policies etc.
 - Dynamic and automated updates
- Allows for self-service and mixed deployments

Event Type	First Status	Allowed Status
DDL Review	OPEN	CLOSE, JUSTIFIED, OPEN

Edit Event Type Definition DDL Review

Description: DDL Review

First Status: OPEN

Allowed Status

Available Status: FOUND, OK, SUSPECT

Allowed Status: CLOSE, JUSTIFIED, OPEN

Defined Event Actions

Event Action Description	Prior Status	Next Status	Sign-off
JUSTIFY	OPEN	JUSTIFIED	<input checked="" type="checkbox"/>
APPROVE	JUSTIFIED	CLOSE	<input checked="" type="checkbox"/>
REJECT	JUSTIFIED	OPEN	<input checked="" type="checkbox"/>
REOPEN	CLOSE	OPEN	<input checked="" type="checkbox"/>

Roles

Roles have been assigned to this event type with status CLOSE

Roles have been assigned to this event type with status JUSTIFIED

Roles have been assigned to this event type with status OPEN

Buttons: Cancel, Apply, New...

Event Type	First Status	Allowed Status
SENSITIVE	FOUND	FOUND, OK, SUSPECT

Buttons: New Event Type, Event Status

Advanced Workflow – cont.



Events and Custom Fields

Filter Display Event: -- select -- Status: -- select --

For selected rows, add or update:

New Event: -- select -- Action: -- select --

TICKET: COMMAND: COMMENTS:

FCR: Sign

Report details: Compare with other results Show original values Use Aliases

<input type="checkbox"/>	Full SQL ID	Client IP	Server IP	Server Type	SQL Verb	Count of Object Name	Full Sql	Total access	TICKET	COMMAND	COMMENTS	FCR	Event/Status	Sign	By
<input type="checkbox"/>	163415	192.168.84.1	192.168.84.1	ORACLE	DROP TABLE	1	drop table t1	1					DDL Review/OPEN		Default Event
									4365456	ALTER INDEX	fgnhh	fhggh	DDL Review/JUSTIFIED	Signed	dba1(dba1 dba1)
													DDL Review/CLOSE	Signed	audit1(audit1 audit1)
															2011-02-18 21:35:48
															2011-03-20 03:33:00
															2011-03-20 05:21:08
<input type="checkbox"/>	163412	192.168.84.1	192.168.84.1	ORACLE	CREATE TABLE	1	create table t1(i int)	1					DDL Review/OPEN		Default Event
									4365456	ALTER INDEX	fgnhh	fhggh	DDL Review/JUSTIFIED	Signed	dba1(dba1 dba1)
													DDL Review/CLOSE	Signed	audit1(audit1 audit1)
															2011-02-18 21:35:48
															2011-03-20 03:33:00
															2011-03-20 05:21:08

Audit Process Builder

Audit Process Definition

Description: Weekly

Active: The

Archive Results:

Keep for a minimum of: 0

CSV/CEF File Label: weekly.

Email Subject:

Receiver Table

Receiver	Action
<input checked="" type="checkbox"/> poc (POC IBM)	<input type="radio"/> Rev
<input checked="" type="checkbox"/> admin (admin admin)	<input type="radio"/> Rev
<input checked="" type="checkbox"/> pot (pot training)	<input type="radio"/> Rev

Add Receiver

Receiver name: _____

Action Required: Review ()

To-Do List: Add

Email Notification: None ()

Continuous:

Approve if Empty Yes

Audit Tasks

- + Report: Failed Login Reports [Failed User Login Attempts] {now -1 month to now}
- + Report: Creates to the database [- SQL Trace] {now -1 month to now}
- + Security Assessment: Sybase Security Assessment [Sybase Assessment]
- + Security Assessment: Db2 Assessment [DB2 Assessment]
- + Security Assessment: SQL Server [SQL Server Assessment]
- + Security Assessment: Oracle Assessment [Oracle Product Assessment]
- + Report: Entitlement Review [ORA Roles Granted]

Report Configuration

Description: Entitlement Review

Task Type: Report Security Assessment Entity Audit Trail Privacy Set Classification Process

Report

Report: ORA Roles Granted

CSV/CEF File Label: Entitlement_Review

Export CSV file:

Export CEF file:

Export PDF file:

Write to Syslog:

Compress:

PDF Content: Report Diff Report and Diff

Task Parameters

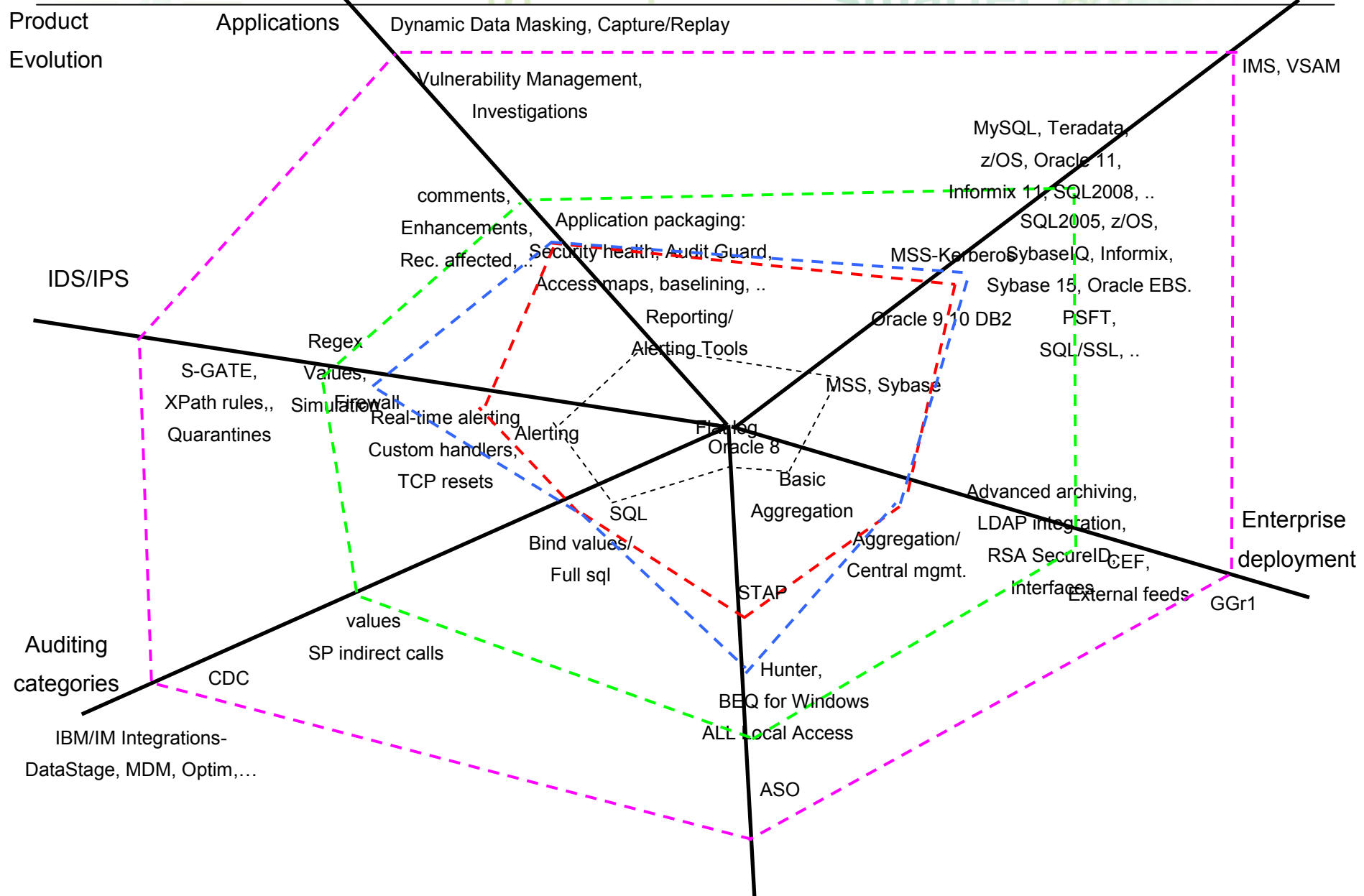
* On aggregators, only reports not exceeding the maximum merge period will be executed.

Enter Period From: now -1 week

Enter Period To: now

Show Aliases: On Off default

Remote Data Source: -- none --



- Operational dashboard
- Guardium for Hadoop – MapReduce, HDFS, HBASE (maybe more)
- STAP for system I
- Support for SQL Server 2012 (and other refreshes)
- Native integration with DB2 LUW
- Integration with Q1 for VA
- Various VA enhancements such as aging reports, more DB2/z, Sybase IQ, ...
- SCAP
- XACML
- Delivery platform for GA Capture/Replay
- ILM Interface – Table last reference & query types
- Significant throughput increase for full details logging
- STAP for Z:
 - Architectural simplification
 - Commit/rollback
 - Stage 1 -> Stage 0 filtering
 - Failed SQL capture
 - Spill file
 - Further zIIP enablement
 - VSAM Record-level audit
- Significant support-driven product enhancements
- Move to X-series appliances

V9x – June 2013

- **BigData and NoSQL:**
 - MongoDB
 - CouchDB
 - Cassandra
 - GreenplumDB
 - HortonWorks
- **Quick search**
- **Audit analytics – filtering, pivoting, delta reporting, ...**
- **Policy and audit process summaries**
- **64 bit & other performance improvements**
- **Change data capture**
- **CM active-passive**
- **Tablet UI**
- **Connection profiling application as built-in**
 - Including default policy
- **REST APIs**
- **Windows auto-discovery of MSSQL**
- **STAP upgrades in Linux OS upgrades**
- **Support Gathering**
- **Outliers Detection – shortly after v9x**

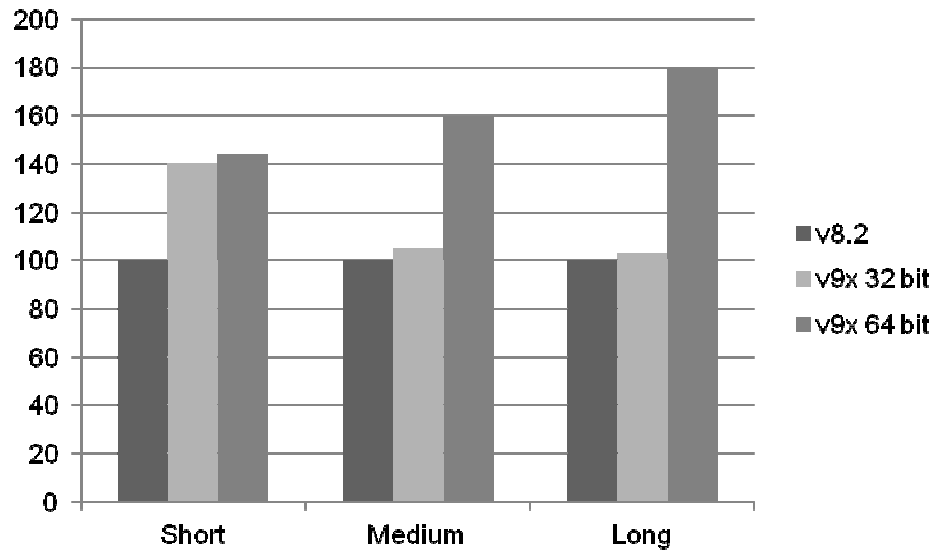
V9x Performance Improvements

- 64 bit option
- Faster database kernel
- Multi-line insert
- Faster parsing options
- Specific improvements for STAP/z

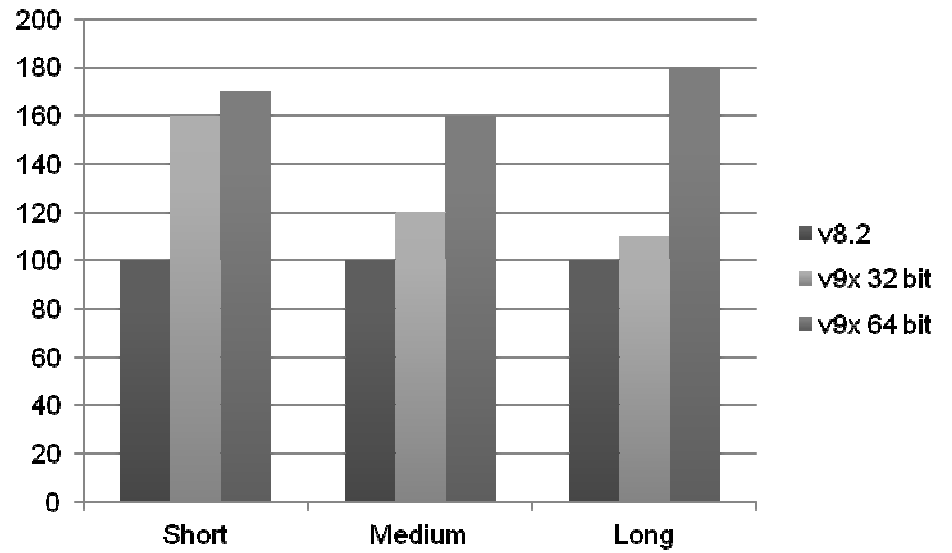
- Scaling to bigger machines

Write Speed Improvements (no change to parsing)

No Details



With Details

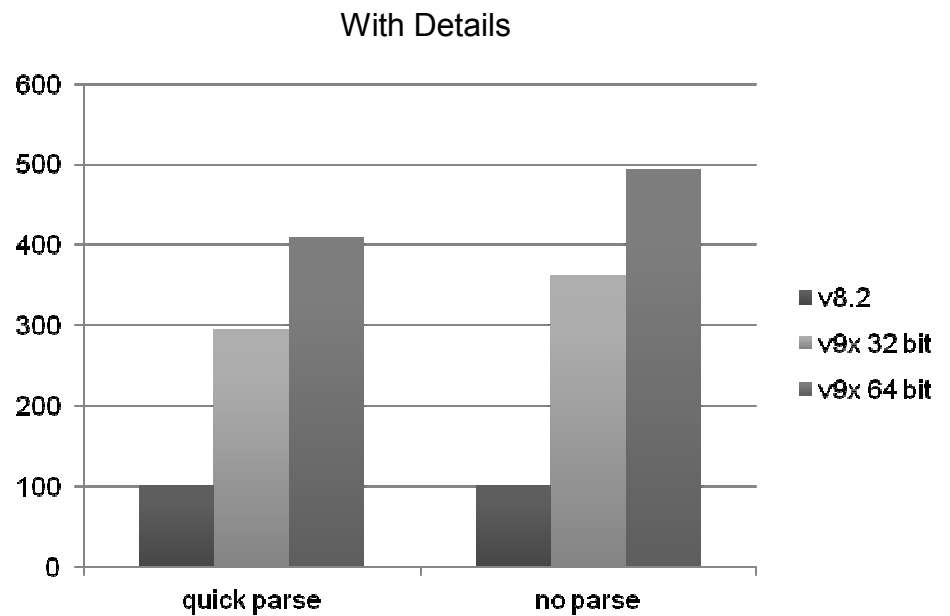
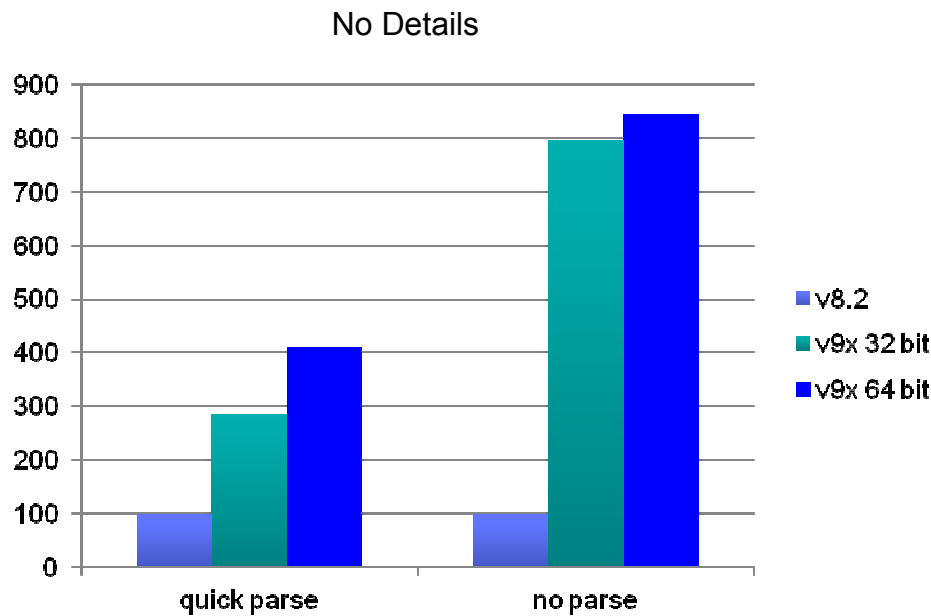


Specific - z

- ~400% throughput improvement (9x vs. 8.2 – both 32 and 64 bit)
- Results are from a real customer workload (big European bank)

With Logging and Parsing Improvements

- Average SQL size = 1500 bytes
- Tested using typical policies with and without details
- Percentage improvements:



Scaling to larger machines

- V9x 64 bit
- 2 socket machine vs. 4 socket machine (6 cores per socket)
 - Theoretical limit is 200%
- No Detail: 140% - 195% (depending on short/medium/long and database type)
- Full Detail: 140% - 160% (depending on short/medium/long and database type)
- With Extrusion Data: 140% - 190% (depending on short/medium/long and database type)

Pivoting – Data Marts

A Flat only

Start Date: End Date:

Aliases

Pivot table definition

Defined pivot tables:

new
p2-flat only
ron1

New Delete

*Name ron1

Sharing Private All

Display 100 rows in a page Sort Top rows Ascending Descending

Build a pivot table by clicking on the buttons from the headings on the right to the diagram on the left. Select at least one column, row, or field. You can change the order of buttons by drag and drop in the Row section. When dragging, wait for the green color before dropping.

Row: Maximum 10 fields
Bind Info

Column: Maximum 1 field
Timestamp Date

Data: Maximum 1 field
Records Affected

Sort: Maximum 1 field

Headings:
Succeeded
Timestamp
Timestamp Date
Timestamp Time
Records Affected
Bind Info

N1
N1
N1
N1
RV
RV
RV
RV
RV
RV
RV
RV
RV
RV

ron1

Bind Info	2010-09-15	2010-09-16	2011-01-11	2011-01-12	2011-05-28
PLAN=DSNUTIL	0	0	2975	0	2975
PLAN=N/A	286	0	0	0	286
PLAN=	335	0	2977	0	2342
PLAN=ADHPLAN1	614	0	0	0	553
PLAN=ADHPLAN3	1837	0	0	0	1837
PLAN=DSNTEP2	1058	1841	2975	0	1915
PLAN=DISTSERV	133	0	2211	2221	263
PLAN=ADB	0	1843	0	0	1843
PLAN=DSNTIAD	1555	0	3049	0	1934

1 to 20

1 to 9 of 9

V10

- SAP HANA
- Web application redaction – **Beta-level now**
- Dynamic Data Masking – **Completed first pilot with large financial services / cards brand**
- Versioning
- Smart entitlements & recursive collapse – including historical deltas and pivots
- Smart scheduling & dependencies
- **Policies, filtering etc.** using additional parameters including hostnames.
- File system monitoring and controls – **Beta-level now & completed pilot within IBM**
- Selective purge and archiving
- New architecture options – hypervisor interception, streams, ...
- Extension of V9x search into Big Data for Guardium
- Everything as RPMs
- Close gaps on DB2/Z – prevention, extrusion, DDM, ..

Row and column level filtering

- Policy says I can only see salary data for dept 20 – instead of removing columns, redact them

```
SQL> select * from emp;
```

EMPNO	ENAME	JOB	MGR	HIREDATE	SAL	COMM	DEPTNO
7499	ALLEN	SALESMAN	7698	21-FEB-81	*****	300	30
7521	WARD	SALESMAN	7698	23-FEB-81	*****	500	30
7566	JONES	MANAGER	7839	03-APR-81	3599.75		20
7788	SCOTT	ANALYST	7566	20-APR-87	3630		20
7839	KING	PRESIDENT		18-NOV-81	*****		10
7844	TURNER	SALESMAN	7698	09-SEP-81	*****	0	30
7876	ADAMS	CLERK	7788	24-MAY-87	1331		20
7900	JAMES	CLERK	7698	04-DEC-81	*****		30
7902	FORD	ANALYST	7566	04-DEC-81	3630		20
7934	MILLER	CLERK	7782	24-JAN-82	*****		10
4444	RON	DEV	7902	02-NOV-02	2000	100	20

14 rows selected.

QR GUI

The screenshot shows the IBM InfoSphere Guardium Query Rewrite GUI. The browser window title is "IBM InfoSphere Guardium (guard)". The sidebar on the left lists various configuration tools, with "Query Rewrite" selected. The main area displays a table of "Query Rewrite Definitions":

Name	Description	Negate	Sample Sql
<input type="checkbox"/> Maggie's	s	<input checked="" type="checkbox"/>	select * from d
<input checked="" type="checkbox"/> Steve's query		<input type="checkbox"/>	select * from foo where a in (select b from c)

Below the table are buttons for "New", "Delete", and "Search by name". A central area prompts the user to "Enter a sample query and then click on Parse" with a text area containing "select * from foo where a in (select b from c)" and a "Parse" button. Below this, it says "Click on the links to define rewrite rules" and shows a preview of the query with links for editing. A "Change query" dialog box is open, showing "Change from" as "foo" and "To" as an empty field. The dialog also has radio buttons for "All levels" and "Use regex", and "OK" and "Cancel" buttons. At the bottom right of the dialog is an "Apply" button. A "Preview" section on the right shows the current query and a "Test" button. At the bottom of the main window, there are two summary sections: "Changes you have made" (Select/Verb Change => from:select to:s depth:0) and "Existing query rewrite" (verb change=> From:select To:delete Use regex:false For all rule elements:false verb change=> From:select To:insert Use regex:false For all rule elements:false Add where clauses: whereText:c=1).