

Top 10 reasons to protect your databases with Guardium VA

1. **You get even more tests** - to cover the full spectrum of database vulnerabilities.

Our full Guardium Vulnerability Assessment (VA) solution currently supports 11 database types offering more than 1600 tests. We continually add new database types and tests including NoSQL, to build a growing library of tests that you can put to good use.

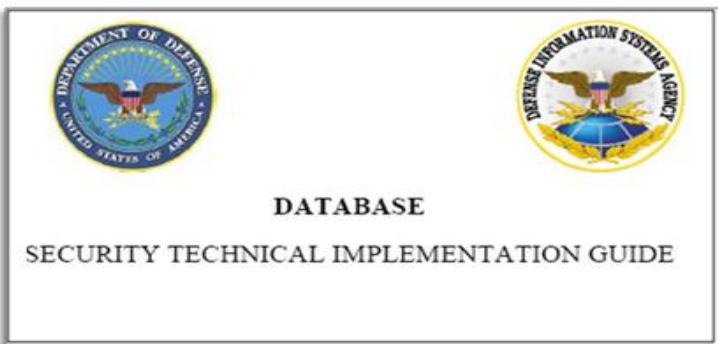
Database Type	Test counts	VA Evaluation counts
DB2	241	210
DB2 z/OS	208	0
INFORMIX	65	49
MS SQL SERVER	114	67
MYSQL	264	0
NETEZZA	21	9
ORACLE	462	392
POSTGRESQL	95	0
SYBASE	70	36
SYBASE IQ	39	36
TERADATA	39	23
TOTAL TESTS	1618	822

Note: Using the full product gives you access to even more configurations and privilege tests.

For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
where you can explore next steps and get closer to a secured database environment.

2. **Continuous updates** - to reflect new vulnerabilities and best-practice recommendations.

Stay ahead of potential vulnerabilities by receiving updates, including new tests from our library of CVE, STIG, CIS and best practice assessments. We leverage our close relationships with many database security architects and experts in the industry as well as the many database vendors themselves to bring these dynamic, hardened VA tests to our customers.



For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
where you can explore next steps and get closer to a secured database environment.

3. Personalize test parameters - to better reflect your requirements and priorities.

Our full Guardium VA solution allows you to tune individual tests including changing thresholds where applicable. Have a customized configuration? Create a truly personalized test. You can also create test exceptions to exclude certain authorized grantees with certain privileges. In our privilege tests, when Guardium finds a violation, it also reports on the individual grantee and privileges associated with it. This helps the DBA to understand what needs to be remediated.

Take a look at what you can do here to process a test exception:

The screenshot shows the 'Assessment Test Tuning' interface. At the top, it says 'Tuning for test on Assessment' with a note 'IDLE_TIME is limited oracle 12 c demo'. Below this is a 'Tuning' section with fields for 'Severity' (set to 'Cautionary') and 'Enter maximum allowed value' (set to '15'). There are also 'External Reference' and 'Exception group' fields. A red arrow points from the 'Save As Default' checkbox in the tuning section to a 'Change default threshold value' dialog box. This dialog has two 'Save As Default' checkboxes and a 'Cancel' button.

The screenshot shows the 'Administrative privilege assignment' interface. It indicates a 'Fail' status with a 'Detail violation' message. The violation details mention 'DPS: Oracle12c FAIL su11u1x64t1-va on2psu11 (gdm)' and 'External Reference: STIG DG0117 Administrative privilege'. A red arrow points from the violation message to an 'Add Selected Members To Group' dialog box. This dialog has a 'Group' dropdown, a 'Select All' checkbox, and a list of grants. One grant is checked: 'Grantee = GUARDIUM_DBA : Granted_Role = RESOURCE'. Another red arrow points from this checked grant to the text 'Excluding authorized grantee'.

For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
 where you can explore next steps and get closer to a secured database environment.

4. **Build your own customized tests** – to fine tune the scans to meet the specific needs of your environments.

Our full Guardium VA solution allows you to build your own individual tests leveraging the infrastructure and reporting system that is currently in place. For example, you can create your own tests to enforce security for your own applications or packaged applications like SAP, EBS, PeopleSoft, etc. Here is an example of our Test Builder:

Security Assessment Builder

Query-based Test Builder

Test Name	No PUBLIC access to critical packages
Database Type	ORACLE
Category	Privilege
Severity	Major
Short Description	This test checks for PUBLIC privilege to these packages: UTL_FILE, UTL_SMTP, UTL_TCP, UTL_HTTP, DBMS_RANDOM, DBMS_LOB, DBMS_SQL, DBMS_SYS_SQL, DBMS_JOB, DBMS_BACKUP_RESTORE and DBMS_OBFUSCATION_TOOLKIT. Access to critical packages should be restricted to authorized accounts only.
External Reference	STIG DO3475 No PUBLIC access to critical packages. CIS O
Result text for pass	Access to critical packages is restricted from PUBLIC, as recon
Result text for fail	PUBLIC access to one or more critical packages has been gra
Recommendation text for pass	No action required
Recommendation text for fail	You should revoke PUBLIC access to critical packages. You can use the following command to revoke the privilege: REVOKE EXECUTE ON <schema>. <package_name> FROM PUBLIC.
SQL statement	declare nval integer := 0;
SQL statement for detail	select DISTINCT TABLE_NAME from DBA_TAB_PRIVS where GRANTEE ='PUBLIC'
Pre test check SQL	

For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
 where you can explore next steps and get closer to a secured database environment.

5. Automated workflow to schedule scans & share results - to automate the assessment scans and review process.

You can save time and money by having the system do all the work in the background. It is easy to set up audit jobs that run on a scheduled basis, go to a distribution list, and then require receivers to review or comment on test results. Guardium allows you to easily do this and keep copies of the results for review and remediation.

The screenshot shows the Audit Process Builder interface with the following sections:

- Audit Process Definition:**
 - Description: (Demo) Oracle VA
 - Active: There's a schedule associated with this process
 - Archive Results:
 - Allow Result Purge before Reviewed:
 - Keep for a minimum of 0 days or 5 runs
 - CSV/CEF File Label: _Demo__Oracle_VA
 - Zip CSV for mail:
 - Email Subject: auditor@us.ibm.com
 - Buttons: View, Run Once Now, Modify Schedule...
- Receiver Table:**

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
admin (admin admin)	<input checked="" type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input type="checkbox"/>	<input type="checkbox"/>

Add Receiver:

Receiver name:

Action Required: Review Sign

To-Do List: Add

Email Notification: None Link Only Full Results

Continuous:

Approve if Empty: Yes

Add button
- Audit Tasks:**
 - Security Assessment: Oracle VA [(Demo) Oracle VA]**
 - Description: Oracle VA
 - Task Type: Report Security Assessment Entity Audit Trail Privacy Set Classification Process
 External Feed
 - Security Assessment** (Demo) Oracle VA
 - Export AXIS xml:
 - Export SCAP xml:
 - PDF Content: Report Diff Report and Diff
 - Event and Additional Columns button
 - Apply button
 - Add Audit Task button
- Roles:**

No roles have been assigned to this Process

Roles... button

For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
 where you can explore next steps and get closer to a secured database environment.

6. Entitlements reporting - to identify data exposure and dormant entitlements

Guardium's entitlement reporting helps you identify the relationship of objects and roles – what objects are granted to what users. Our set of predefined reports show comprehensive privileges in your database. You can schedule these reports to run on a regular basis and compare the results to a previously executed report. Look at how easy it is to see at-a-glance your permissions for SQL Server:

Schema	Owner	Object Name	Object Type	Permission	Grant Type	SqlGuard Timestamp	Datasource Details	DB Name
sys		parameter_type_usages	VIEW	SELECT	GRANT	2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
sys		partition_range_values	VIEW	SELECT	GRANT	2014-10-15 10:28:24.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	pubs
sys		remote_logins	VIEW	SELECT	GRANT	2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
sys		server_event_session_fields	VIEW	SELECT	GRANT	2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
sys		service_message_types	VIEW	SELECT	GRANT	2014-10-15 10:28:23.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	msdb
sys		sp_adddynamicsnapshot_job	SQL_STORED_PROCEDURE	EXECUTE	GRANT	2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
sys		sp_availability_group_command_internalEXTENDED_STORED_PROCEDUREEXECUTE	GRANT			2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
sys		sp_change_subscription_properties	SQL_STORED_PROCEDURE	EXECUTE	GRANT	2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
sys		sp_cursorprepexec	EXTENDED_STORED_PROCEDUREEXECUTE	GRANT		2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
sys		sp_droporphans	EXTENDED_STORED_PROCEDUREEXECUTE	GRANT		2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
sys		sp_getpublisherlink	SQL_STORED_PROCEDURE	EXECUTE	GRANT	2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
sys		sp_helprepfailovermode	SQL_STORED_PROCEDURE	EXECUTE	GRANT	2014-10-15 10:28:22.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	master
dbo		sp_add_job	SQL_STORED_PROCEDURE	EXECUTE	GRANT	2014-10-15 10:28:23.0	DPS: MSSQL2012 FAIL on wi8ku2x64l2-va Datadirec(S : MS SQL SERVER : 9.70.144.223 :: 1433 :	msdb

For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
where you can explore next steps and get closer to a secured database environment.

7. Scale, Organization & Speed - to expand scope and build your own clusters of tests.

Our full Guardium VA solution allows you to easily create various security assessments. You can group them based on database functions, classifications or database types then choosing specific tests that you want to execute only. You can easily set your security assessments to run against thousands of database servers in a short period of time. In large, complex environments this is a great feature to organize and streamline your assessment library. Take a look at what you can do here:

Configuring your VA Test

The screenshot shows the 'Assessment Test Selections' section of the Security Assessment Builder. It includes a table of selected tests, a tuning panel, and various configuration filters.

- Type of test:** A red box highlights the 'Test Type' filter section, which includes Predefined, Query based, CVE, APAR, All, Critical, Major, Minor, Caution, Info, and Other options. The 'Include CAS' checkbox is also shown.
- Database types:** A red box highlights the 'Tests available for addition' section, which lists various database engines: [Observed] DB2 DB2 z/OS INFORMIX MS SQL SERVER MYSQL Netezza ORACLE POSTGRESQL SYBASE SYBASE IQ TERADATA.
- Fine tune selected tests:** A red box highlights the 'Tuning' column in the main table, which contains checkboxes for various configuration items like 'PRIV Major (n/a)' and 'CONF Cautionary 5,000,000'.
- Tests Available:** A red box highlights the list of available tests in the bottom panel, such as 'CONF(Major): ADMIN_RESTRICTIONS Is On *' and 'CONF(Major): EXTPROC Parameter NOT Defined in the Configuration File *'.

For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
 where you can explore next steps and get closer to a secured database environment.

8. History & Progression - to compare with previous results and show overtime improvement.

If your memory fails you, you can easily compare previous runs of an assessment right on-line to see if you are getting better or worse over time. Our full Guardium VA solution allows you to save previously executed results and call them up at any time. You can also filter results based on what you want to review. There is a chart for the summary as well as test details to demonstrate progress over time. The report cover sheet is further expanded to show progress over time with an overall score result – allowing you to focus on improving your security position.

Anatomy of a VA test results report

Summary Test Results: This section includes the overall score (51%), detailed scoring matrix, and a result history chart showing trends over time.

Overall Score: Displays the overall test passing percentage (51%).

Detailed Scoring Matrix: A grid showing the number of tests passed (p), failed (f), and other (o) for various categories like Privilege, Authentication, Configuration, Version, and Other.

Result History Shows Trends: A line graph titled "Assessment Result History" showing the percentage of tests passing over time from 12:00 PM on 5/30/14 to 6:00 PM on 5/30/14.

Filter/Sort controls for easy use: Buttons for "Reset Filtering" and "Filter / Sort Controls".

Detailed Remediation Suggestions: A section titled "Assessment Test Results" listing specific findings and recommendations, such as profiles not compliant with QPWDEXPITV and profiles with *ALLOBJ special authority.

For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
 where you can explore next steps and get closer to a secured database environment.

9. Custom report formatting - produce and customize reports to be shared with different stakeholders.

You can customize the look and feel of the reports. Some people like just a summary while others need detailed reports to get the remediation started. These different report formats can be automatically distributed to various parties, reducing the time to provide customized details to different teams. You get the right format to the right people at the right time.

Create your own custom VA reports to filter on columns, database and condition that you want to see																
Name	Type	DB Name	Version	Patch Level	Full Version Info	Description	Host	Test Description	Test Score	Score Description	Result Text	Recommendation	Severity	Category	Execution Date	Assessment Description
DPS: Oracle 11 FAL on w3ku2x322	ORACLE	11.1.0.6.0	NO Patch	11.1.0.6.0	w3ku2x322.guard.swg.usma.ibm.com	Version: Oracle	Version: ORACLE '11.1.0.6.0'	0	Fail	Version: ORACLE '11.1.0.6.0'.	The Oracle version installed is not one of your standard Oracle versions; it is recommended that you upgrade this Oracle instance to an acceptable version.	MAJOR	VER	2014-10-17 (Demo) Oracle	VA	
DPS: Oracle 11 FAL on w3ku2x322	ORACLE	11.1.0.6.0	NO Patch	11.1.0.6.0	w3ku2x322.guard.swg.usma.ibm.com	Access To The Selected Packages is restricted	Access to the selected packages has been granted to PUBLIC. You should revoke these PUBLIC grants and restricted it according to the needs of your organization. You can use the following command to revoke the privilege:	0	Fail	Access to the selected packages has been granted to PUBLIC.	REVOKE EXECUTE ON schema_name.package_name FROM PUBLIC;	MAJOR	PRIV	2014-10-17 (Demo) Oracle	VA	
DPS: Oracle 11 FAL on w3ku2x322	ORACLE	11.1.0.6.0	NO Patch	11.1.0.6.0	w3ku2x322.guard.swg.usma.ibm.com	OS_AUTHENT_PREFIX Is Not OPS\$	Parameter: 'OS_AUTHENT_PREFIX' is OPS\$.	0	Fail	Parameter: 'OS_AUTHENT_PREFIX' is OPS\$.	Parameter: 'OS_AUTHENT_PREFIX' is set to the default value. We recommend changing this parameter to a value different than the default value. Leaving the default value compromises the security of your system.	MINOR	CONF	2014-10-17 (Demo) Oracle	VA	
DPS: Oracle 11 FAL on w3ku2x322	ORACLE	11.1.0.6.0	NO Patch	11.1.0.6.0	w3ku2x322.guard.swg.usma.ibm.com	SQL92_SECURITY Is True	Parameter: 'SQL92_SECURITY' is TRUE	0	Fail	Parameter: 'SQL92_SECURITY' is TRUE.	Parameter: 'SQL92_SECURITY' is set to the default value. We recommend setting this parameter to true to ensure table-level SELECT privileges are required to execute updates. If this option is not enabled the UPDATE privilege can be used to determine values that should require SELECT privileges.	MAJOR	CONF	2014-10-17 (Demo) Oracle	VA	
DPS: Oracle 11 FAL on w3ku2x322	ORACLE	11.1.0.6.0	NO Patch	11.1.0.6.0	w3ku2x322.guard.swg.usma.ibm.com	UTL_FILE_DIR Should Not Point To Sensitive Directories	UTL_FILE_DIR Should Not Point To Sensitive Directories	0	Fail	Parameter: 'UTL_FILE_DIR' is ''.	The UTL_FILE_DIR parameter is set too broadly - e.g. to the server's root directory. This parameter defines the directory where procedures and functions can read and write files. We recommend that you set this parameter only if it is required by applications, and then to as small a range of directories as possible (e.g. '/home/oracle/output/report_listings/MyParticularApp').	MAJOR	CONF	2014-10-17 (Demo) Oracle	VA	

VA Summary report allows you to track the history of tests when it passed and failed.

Test Description	Db Host	Service Name	Port	First Execution Datetime	Last Execution Datetime	First FailDatetime	Last FailDatetime	First PassDatetime	Last PassDatetime	Current Score	Current Score Since	Cumulative Fail Age	Cumulative Pass Age
DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited	su11u1x64t1-va.guard.swg.usma.ibm.com	on2psu11	1521	2014-10-06 14:25:58.0	2014-10-08 09:59:51.0	2014-10-07 16:36:55.0	2014-10-07 16:39:35.0	2014-10-06 14:25:58.0	2014-10-08 09:59:51.0	Pass	2014-10-08 09:59:51.0	2	3
DBA Profile PASSWORD_VERIFY_FUNCTION Is Implemented	su11u1x64t1-va.guard.swg.usma.ibm.com	on2psu11	1521	2014-10-06 14:25:58.0	2014-10-08 09:59:51.0	2014-10-07 16:39:35.0	2014-10-07 16:39:35.0	2014-10-06 14:25:58.0	2014-10-08 09:59:51.0	Pass	2014-10-08 09:59:51.0	2	3
IDLE_TIME is limited	su11u1x64t1-va.guard.swg.usma.ibm.com	on2psu11	1521	2014-10-06 14:25:58.0	2014-10-08 09:59:52.0	2014-10-07 16:38:15.0	2014-10-07 16:39:35.0	2014-10-06 14:25:58.0	2014-10-08 09:59:52.0	Fail	2014-10-07 16:38:15.0	2	2
No PUBLIC access to SYSCAT.DBAUTH and SYSIBM.SYSDBAUTH	rh6x64-va	sample	5000	2014-10-09 12:17:31.0	2014-10-09 15:07:25.0	2014-10-09 12:17:31.0	2014-10-09 15:07:25.0			Fail	2014-10-09 12:17:31.0	1	0
No PUBLIC access to SYSCAT.PACKAGEAUTH and SYSIBM.SYSPLANAUTH	rh6x64-va	sample	5000	2014-10-09 12:17:33.0	2014-10-09 12:28:43.0	2014-10-09 12:17:33.0	2014-10-09 12:28:43.0			Fail	2014-10-09 12:17:33.0	1	0
No PUBLIC access to SYSCAT.TABAUTH and SYSIBM.SYSTABAUTH	rh6x64-va	sample	5000	2014-10-09 12:17:33.0	2014-10-09 15:07:26.0	2014-10-09 12:17:33.0	2014-10-09 15:07:26.0			Fail	2014-10-09 12:17:33.0	1	0

For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
where you can explore next steps and get closer to a secured database environment.

10. OS-Level assessments - expand assessment to monitor files and folder permissions.

Our full Guardium VA solution allows you to not only monitor privileges in your database, but it can also monitor files and folder permission at the OS level for database binaries and datafiles. Guardium has predefined tests that enforce such privileges along with tests that monitor database specific configuration setting at the OS level, for example, your listener.ora and sqlnet.ora files. This is a must for many regulatory requirements – make sure that the database configuration files have not been tampered with and that there is no malware injected into the executables.

Short Description: This test checks OS-level permissions on Oracle parameter files. Parameter files control the functioning of your Oracle database, and even its ability to start. Access to these parameter files should be restricted to OS users with direct responsibility for database or system administration.

External Reference: CVE-2000-0206, CVE-2001-0300, CVE-2002-0857, CVE-2004-1366

Recommendation: Some of the files checked have permissions above the required. We recommend to restrict access to these files.

Details: Add Selected Members To Group

```
-rw-r--r-- /home/oracle12/product/12.0/db_1/dbs/init.ora (Expected: < rwxr-x--)
-rw-r--r-- /home/oracle12/product/12.0/db_1/network/admin/sqlNet.ora (Expected: < rwxr-x--)
drwxrwxrwx /home/oracle12/product/12.0/db_1/network/admin/samples (Expected: < rwxr-x--)
-rwxrwxrwx /home/oracle12/product/12.0/db_1/network/admin/samples/sqlNet.ora (Expected: < rwxr-x--)
-rwxrwxrwx /home/oracle12/product/12.0/db_1/network/admin/samples/listener.ora (Expected: < rwxr-x--)
-rw-r--r-- /home/oracle12/product/12.0/db_1/network/admin/shrept.lst (Expected: < rwxr-x--)
-rw-r--r-- /home/oracle12/product/12.0/db_1/dbs/initon2csu11.ora (Expected: < rwxr-x--)
-rw-r--r-- /home/oracle12/product/12.0/db_1/srvm/admin/init.ora (Expected: < rwxr-x--)
-rw-r--r-- /home/oracle12/product/12.0/db_1/hs/admin/initdg4odbc.ora (Expected: < rwxr-x--)
```

2014 October 31

IBM InfoSphere Guardium Licensed Materials - Property of IBM. © Copyright IBM Corp. 2014. U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" (www.ibm.com/legal/copytrade.shtml)

For complete information on the full Guardium Vulnerability Assessment product, go to:
<http://www-03.ibm.com/software/products/en/infoguarvulnasse>
where you can explore next steps and get closer to a secured database environment.