

Guardium Vulnerability Assessment V11.2: New Features Overview

and

VA + ServiceNow Integration

Vikalp Paliwal
Offering Manager
IBM Security Guardium VA

Mei Thom
Software Engineer
IBM Security Guardium

Contents

New Features

- New database release support for VA
- DPS upload validation and history reporting
- MySQL SSL and Sybase ASE SSL connection
- Custom upload datasource with role
- Datasource delete with cascade
- New Platform Support for Azure SQL
- SQL Server 2016 STIG VA Tests
- VA HALTED and resume
- DB2 special patch for CVE tests

Integration demo

- Vulnerability Assessments and External Ticketing Service Integration in Guardium v11.2

New database release support by VA

- DB2 LUW 11.5
- Informix 14.1
- SQL Server 2019
- Cloudera 6.x
 - Cloudera Certified solution
 - Hive datasource now supports TLS when using Kerberos authentication.

* Application type: Security Assessment

* Name: DPS: Cloudera Hive 6.3 on cdh63-02 (Kerberos)

* Database type: HIVE

Description: cdh63-02 and cdh63-03 are hiveserver services.

Share datasource ?

Use SSL Add certificate

Import server ssl certificate

Use kerberos

* Kerberos config: DBANET4

Realm: DBANET4.ROOT

KDC: dbanetdc04.swg.usma.ibm.com

Authentication

* Credential type

Assign credentials External password None

* User name: user1

* Password: *****

Location:

* Host name/IP: cdh63-02.swg.usma.ibm.com

* Port number: 10000

Database: default

Connection property: Ex: prop1=value;prop2=value

Custom URL:

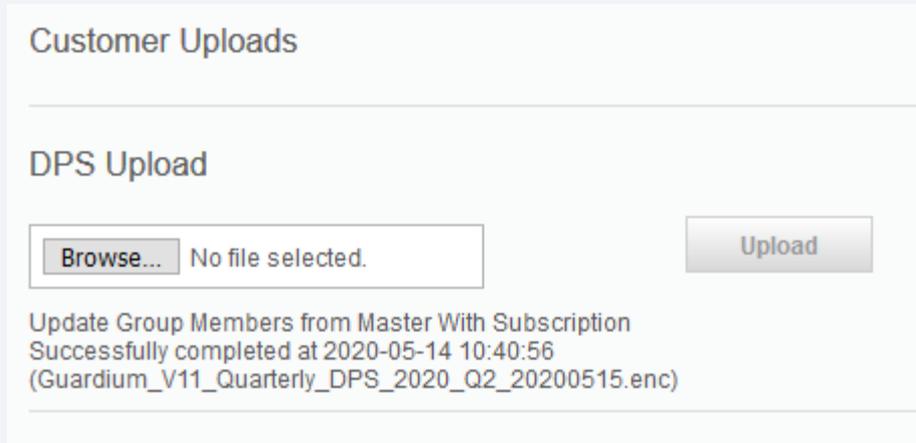
[Show advanced options](#)

Connection successful ✕

Test connection Save Close

DPS validation

- Guardium v11.2 now validates the DPS upload.
 - You cannot upload a DPS from another version.
 - You cannot upload an older DPS than what you already have.
 - You can upload the same DPS again.



The screenshot shows a web interface titled "Customer Uploads". Below the title is a horizontal line. Underneath, the section "DPS Upload" is displayed. There is a file selection area containing a "Browse..." button and the text "No file selected.". To the right of this area is an "Upload" button. Below the file selection area, there is a message: "Update Group Members from Master With Subscription Successfully completed at 2020-05-14 10:40:56 (Guardium_V11_Quarterly_DPS_2020_Q2_20200515.enc)".

DPS upload history

- Guardium v11.2 allows you to track the DPS upload history and see its status.
- In the Guardium CLI, run the following command: “show dps”

```
gva07.guard.swg.usma.ibm.com> show dps
DPS Upgrade History:
DPS File Name                               DPS Type   Start Time           End Time             Status
-----
Guardium_V11_Quarterly_DPS_2020_Q1_20200217.enc  QUARTER    2020-03-30 18:12:27  2020-03-30 19:56:38  DPS upgrade completed
Guardium_V11_Quarterly_DPS_2020_Q1_20200217.enc  QUARTER    2020-04-02 18:00:56  2020-04-02 18:01:36  DPS upgrade completed
Guardium_V11_Rapid_Response_DPS_For_2020_Q1_202004  RAPID      2020-04-07 10:21:51  2020-04-07 10:21:52  DPS upgrade completed
Guardium_V11_Rapid_Response_DPS_For_2020_Q1_202004  RAPID      2020-04-08 17:04:50  2020-04-08 17:04:50  DPS upgrade completed
Guardium_V11_Quarterly_DPS_2020_Q1_20200420.enc  QUARTER    2020-04-20 17:36:34  2020-04-20 17:38:04  DPS upgrade completed
Guardium_V11_Quarterly_DPS_2020_Q1_20200422.enc  QUARTER    2020-04-22 19:24:40  2020-04-22 19:25:19  DPS upgrade completed
Guardium_V11_Quarterly_DPS_2020_Q2_20200515.enc  QUARTER    2020-04-28 17:15:02  2020-04-28 17:15:55  DPS upgrade completed
Guardium_V11_Quarterly_DPS_2020_Q2_20200515.enc  QUARTER    2020-05-01 15:44:08  2020-05-01 15:44:50  DPS upgrade completed
Guardium_V11_Quarterly_DPS_2020_Q2_20200515.enc  QUARTER    2020-05-14 10:40:17  2020-05-14 10:40:56  DPS upgrade completed

DPS Upgrade Parameter Status:
Update Group Members from Master With Subscription Successfully completed at 2020-05-14 10:40:56 (Guardium_V11_Quarterly_DPS_2020_Q2_20200515.enc)
ok
gva07.guard.swg.usma.ibm.com>
```

MySQL datasource with SSL

- Guardium v11.2 now supports SSL connections for MySQL 5.6, 5.7 and 8.0.
- You can connect without SSL, SSL server side or SSL x509 authentication.

Application type: Security Assessment

Name: mysql 57 rh6u4x64t1-va01 ssluser

Database type: MySQL

Description:

Share datasource ?

Use SSL [Add certificate](#)

Import server ssl certificate

Authentication

Credential type: Assign credentials External password None

User name: ssluser

Password: *****

Location

Host name/IP: rh6u4x64t1-va01.guard.swg.usma.ibm.com

Port number: 3406

Database: mysql

Connection property: Ex: prop1=value,prop2=value

Custom URL:

[Show advanced options](#)

Connection successful

[Test connection](#) [Save](#) [Close](#)

Application type: Security Assessment

Name: mysql 57 rh6u4x64t1-va01 user509

Database type: MySQL

Description:

Share datasource ?

Use SSL [Add certificate](#)

Import server ssl certificate

Authentication

Credential type: Assign credentials External password None

User name: user509

Password: *****

Location

Host name/IP: rh6u4x64t1-va01.guard.swg.usma.ibm.com

Port number: 3406

Database: mysql

Connection property: Ex: prop1=value,prop2=value

Custom URL:

[Show advanced options](#)

Connection successful

[Test connection](#) [Save](#) [Close](#)

Sybase ASE datasource with SSL

- Guardium v11.2 now supports SSL connections for Sybase ASE v15.7 and 16.x.
- SSL is for server side only. No pem file is required.

The screenshot shows the configuration window for a Sybase ASE datasource. The 'Application type' is set to 'Security Assessment'. The 'Name' is 'Sybase 16 SP02 PL08 on rh8x64t'. The 'Database type' is 'Sybase'. The 'Share datasource' checkbox is checked. The 'Use SSL' checkbox is checked and highlighted with a red box, with an 'Add certificate' button next to it. The 'Import server ssl certificate' checkbox is also checked. The 'Authentication' section has 'Assign credentials' selected. The 'User name' is 'sa', the 'Password' is masked with dots, and the 'Host name/IP' is 'rh8x64t'. The 'Port number' is '4301'. A green notification bar at the bottom indicates 'Connection successful'. Buttons for 'Test connection', 'Save', and 'Close' are at the bottom.

Application type: Security Assessment

Name: Sybase 16 SP02 PL08 on rh8x64t

Database type: Sybase

Description:

Share datasource ?

Use SSL

Import server ssl certificate

Authentication

Credential type: Assign credentials External password None

User name: sa

Password:

Location

Host name/IP: rh8x64t

Port number: 4301

Database:

Connection property: Ex: prop1=value,prop2=value

Custom URL:

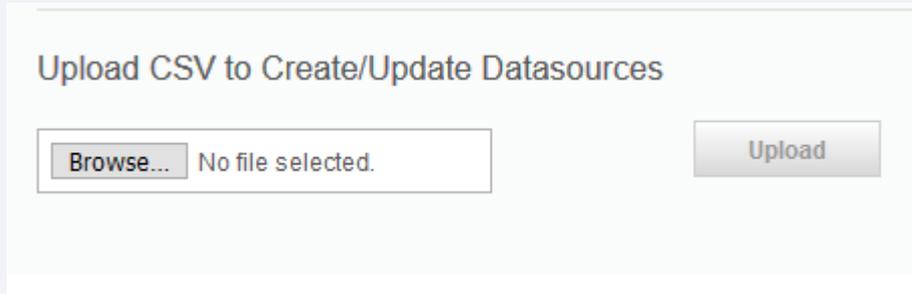
Show advanced options

Connection successful

Test connection Save Close

Upload CSV to Create/Update Datasources

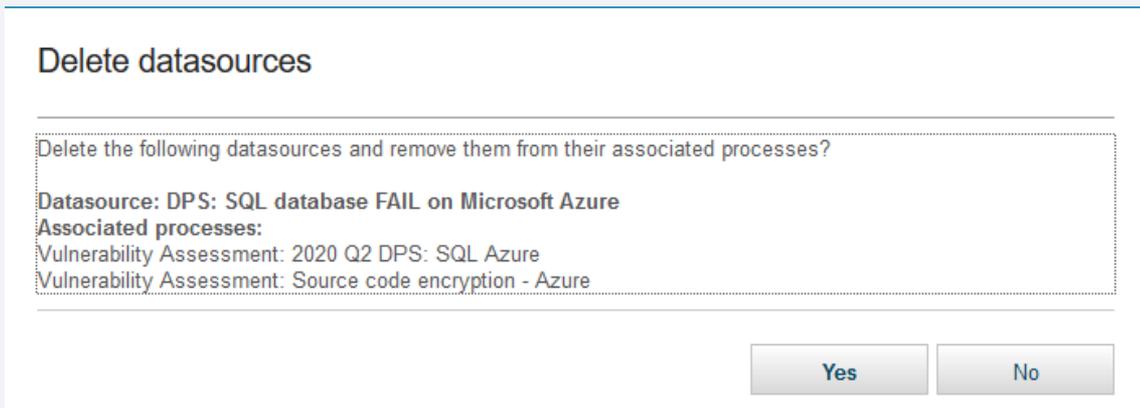
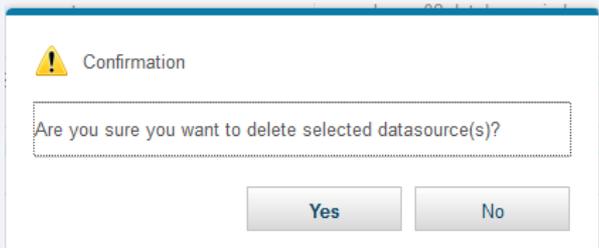
- Guardium v11.2 now supports adding and updating roles to datasources using the upload csv feature.
- You would add another column called “Role” to the csv file. You don’t need to provide a role if it is not required.
- You can add multiple roles per datasource separated by a semicolon.



The screenshot shows a web interface for uploading a CSV file. At the top, the title "Upload CSV to Create/Update Datasources" is displayed. Below the title, there is a file selection area containing a "Browse..." button and the text "No file selected.". To the right of this area is an "Upload" button.

Datasource deletion with CASCADE option

- When you delete a datasource and if that datasource is used by an application, it will prompt you if you want to continue. If so, it will remove the datasource and the datasource from VA, Classification, datasource group and others.



New Platform support:

What's New

- **SQL DB** on Microsoft Azure
 - We are introducing 33 new SQL DB Azure tests

Benefits

- We are supporting one of the popular DBs on Microsoft's Azure Cloud platform.

New Updates

What's New

- **SQL Server 2016 STIG Benchmark**
 - 41 new SQL Server 2016 STIG tests.

Benefits

- We've updated our support for SQL Server with new applicable tests and updated references.

- We have created a new gdmmonitor script to support SQL DB Azure and enhanced the existing SQL Server gdmmonitor script to support the SQL Server 2016 STIG.

VA resume after HALTED

- HALTED assessments happen after a test takes more than 30 minutes to execute, system reboot, UI restart or Classifier restart.
- Before 11.2, when an assessment is HALTED, it is usually killed by the nanny OS process due to a test taking longer than 30 minutes to execute. Users would have to re-run the entire assessment again.
- In Guardium 11.2, if an assessment is HALTED regardless of the cause, it will resume as soon as the classifier process comes back online.
- If a HALTED is caused by a test taking over 30 minutes to execute, it will skip over that test and continue to the next one in the same datasource.
- If a HALTED is caused due to OS, UI, classifier reboot or HALTED due to another multi-thread assessment causing the HALTED, it will resume where it left off without skipping any tests.

VA test HALTED result

- The test that caused the HALTED condition and was skipped, gets an Error test score.

IBM Guardium®

Results for Security Assessment:  Oracle - HALTED Test with 8 DS 

Assessment executed: 2020-05-28 10:02:31

Oracle Application Express

Test category: Conf. Test severity: Major

DPS: Oracle 12.1.0.1 CVE w2k12std03-va on2pw2k1 WindBundle_DS01

Datasource type: ORACLE Datasource severity: None

Error

The test had taken too long to complete and caused the VA process to hang. Skipping to run the next test in the resumed VA scan.

Short Description: The Oracle Application Express, formerly called HTML DB, is an application development component installed by default with Oracle. Unauthorized application development can introduce a variety of vulnerabilities to the database.

STIG Reference: DO6753, O121-C2-011600

STIG Severity: CAT II

STIG Iacontrols: ECSD-1, ECSD-2

STIG Srg: SRG-APP-000141-DB-000091

Recommendation: Please correct the error condition and run the Assessment again.

Details

N/A

[Close this window](#)

DB2 LUW special patch for CVE

- Before Guardium 11.2, the DB2 LUW CVE test mechanism recognized DB2 fixes in the form of database version and fix pack number. If there is a special fix within the fix pack, we would only credit that in the next fix pack numbering.
- In Guardium 11.2 for DB2 LUW 11.1 and lower release, we can recognize the special build.
 - Special builds are not cumulative, a higher special build number does not guarantee a security fix that a lower number has.
 - When a customer's DB2 has a special build higher than the CVE's test requirement, it does not mean they pass the test. The mechanism then does additional checks against the Guardium group "DB2 LUW Database Special Security Fixes" to see if the customer's special fix is in this group. If it is, then the test passes. If not, the test fails.
 - The "DB2 LUW Database Special Security Fixes" group will be maintained and updated by the quarterly DPS going forward. We will continue to add new special fixes as we see them. The customer also has the ability to add their special fix into this group, if they have a DB2 fix they know that addresses the security fixes.
 - New DB2 LUW CVE tests that use this mechanism, will be released in the Q3 2020 DPS and moving forward. We do not change older CVE tests logic or metadata. DB2 LUW Database Special Security Fixes.
 - Guardium v10.6 patch 650 includes DB2 LUW Special fix build feature.

Vulnerability Assessments and External Ticketing Service Integration in Guardium v11.2

Mei Thom
Software Engineer

Agenda

Presentation

Integration features overview

External ticketing system account

External ticketing system configuration

Creating tickets for VA failed tests

Viewing tickets

Updating tickets

Purging tickets

ServiceNow CMDB

Live Demo

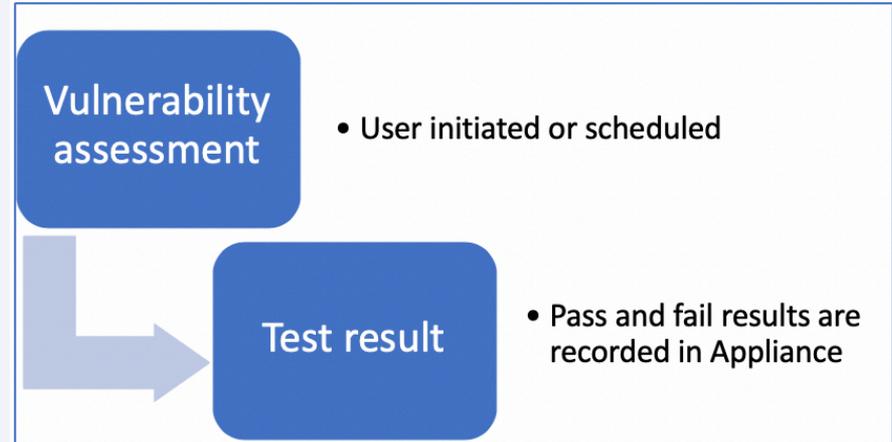
Q&A

Integration features overview

Benefits

Before

- VA test results were recorded in Appliance only.
- Users have to access Guardium system to review test results.



Integration features overview

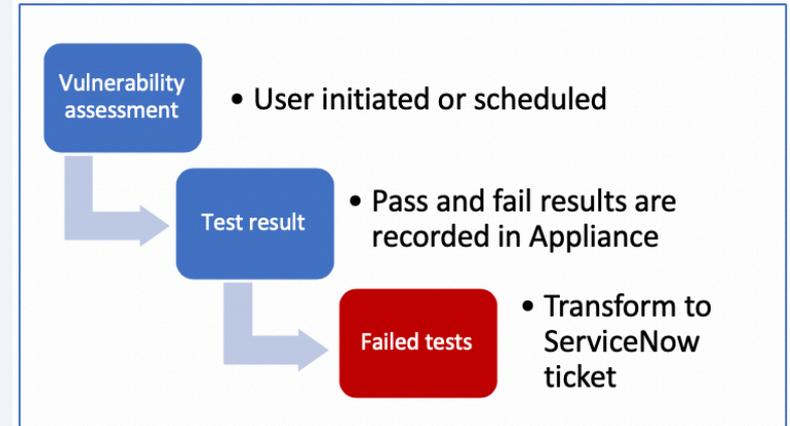
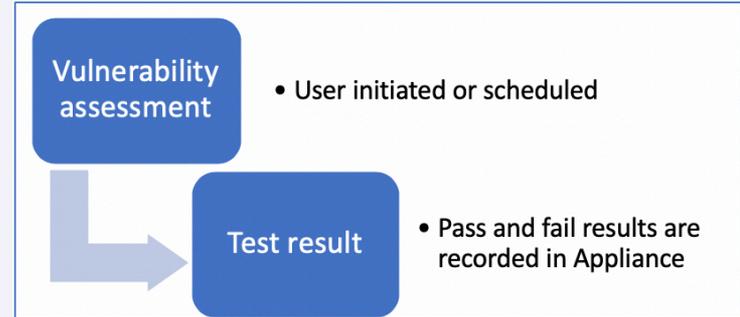
Benefits

Before

- VA test results were recorded in Appliance only.
- Users have to access Guardium system to review test results.

After

- For failed VA test results, a ticket is created on the external ticketing system.
- The external ticketing systems, known as incident tracking systems, usually have workflow, charts, notification and other services to help the customers manage tasks.



VA integration with ServiceNow in Guardium v11.2

- Tickets are created in ServiceNow for failed VA tests in a few ways:
 - Automatically create tickets during VA job run
 - Manually create tickets from VA test results page
 - Automatically create tickets when VA task is executed in an audit process

External ticketing system account

Add external ticketing account information to Guardium central manager:

- Setup > Tools and Views > External Ticketing System
 - Add account
 - » URL: ServiceNow instance
 - » Account: user credential to access the ServiceNow instance
 - » Click “Test connection”
 - » When successful, save the account

The screenshot shows the 'External Ticketing System' interface with an 'Add account' dialog box open. The dialog box contains the following fields and options:

- Type:** A dropdown menu with 'ServiceNow' selected.
- Location:** A text input field.
- URL:** A text input field containing 'https://dev67612.service-now.com'.
- Account:** A text input field.
- User name:** A text input field containing 'admin'.
- Password:** A text input field with masked characters '.....'.

At the bottom of the dialog box, there is a 'Test connection' button. Below the dialog box, there are 'Save' and 'Close' buttons.

External ticketing system configuration

Create an external ticketing configuration for Vulnerability Assessment:

- NOTE: when we create the first external ticketing system account in Guardium, four external ticketing system configurations are created automatically. "VA Results" is one of them
- If any ticket operation failed, the "connection" will show a red X. The connection should be edited and tested again

External Ticketing System		
Service	Guardium Type	Connection
<input type="checkbox"/> ServiceNow	Alert	
<input type="checkbox"/> ServiceNow	Risk Spotter	
<input type="checkbox"/> ServiceNow	Threat Analytics	
<input type="checkbox"/> ServiceNow	Vulnerability Assessment	

Total: 4 Selected: 0

External ticketing system configuration

The configuration dialog contains three tabs:

- Account
- Settings
- Status

External Ticketing System

Service	Guardium Type	Connection
<input type="checkbox"/> ServiceNow	Alert	<input checked="" type="checkbox"/>
<input type="checkbox"/> ServiceNow	Risk Spotter	<input checked="" type="checkbox"/>
<input type="checkbox"/> ServiceNow	Threat Analytics	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> ServiceNow	Vulnerability Assessment	<input checked="" type="checkbox"/>

Total: 4 Selected

External Ticketing System Configuration

Account Settings Status

* Account ServiceNow > dev67612.service-now.com > admin

Test connection

Save Close

External ticketing system configuration

Account tab

- Specifies the account created in previous step.
- Can add or edit account.

External Ticketing System Configuration

Account Settings Status

* Account 

External ticketing system configuration

Settings tab

- Specifies the fields included in the tickets.
- Can specify severity options that tickets will be automatically created when the failed VA tests meet the severity criteria.

External Ticketing System Configuration

Account Settings Status

* Guardium system Vulnerability Assessment Results

* Template Problem

Automatically create tickets when severity is Critical, Major

Guardium fields	ServiceNow field	Computed value
assessment_name datasource_id datasource_name datasource_type datasource_ip datasource_port test_id test_category test_description test_external_reference test_recommendation test_result test_score test_score_description test_severity test_short_description test_stig_reference	Description	assessment_name : \${assessment_name} datasource_id : \${datasource_id} datasource_name : \${datasource_name} datasource_type : \${datasource_type} datasource_ip : \${datasource_ip} datasource_port : \${datasource_port} test_id : \${test_id} test_category : \${test_category}
	Short description	IBM Guardium database assessment failure: \${t
	Additional field +	

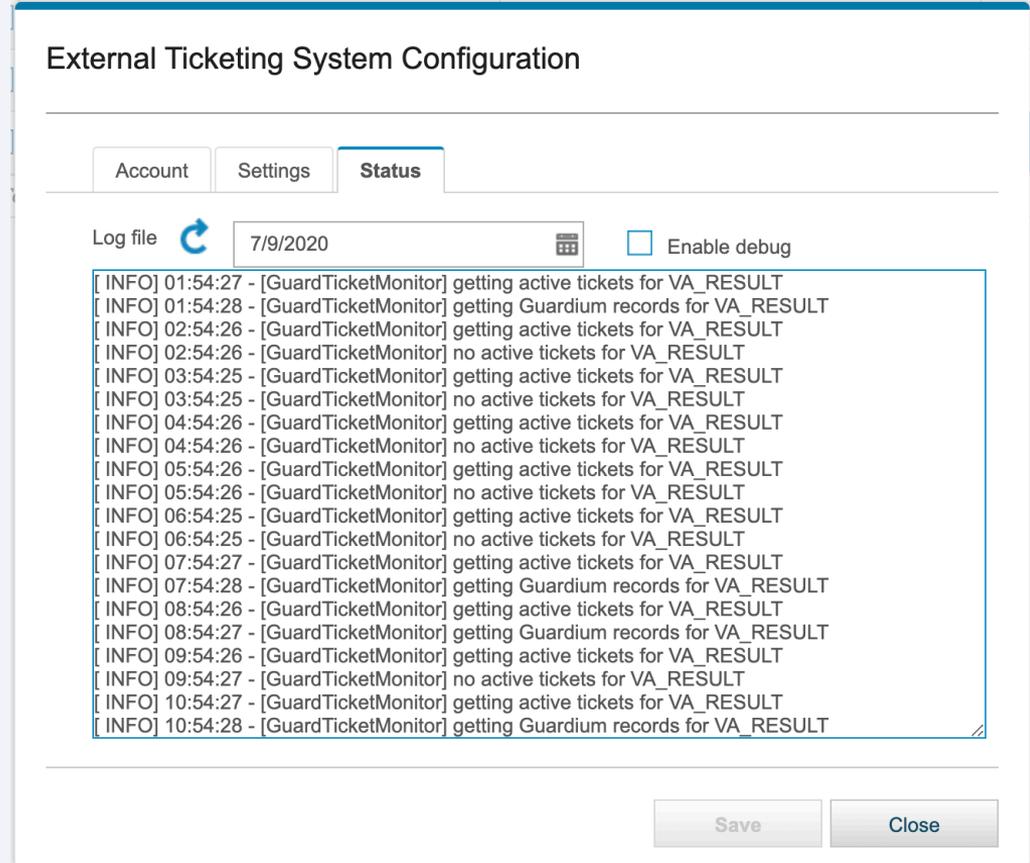
>>

Save Close

External ticketing system configuration

Status tab

- Lets user enable debug logging level on VA results ticketing activities.
 - Default logging level logs for INFO, WARN, ERROR, FATAL levels
- Lets user view the VA results ticketing logs.



The screenshot displays the 'External Ticketing System Configuration' interface, specifically the 'Status' tab. At the top, there are three tabs: 'Account', 'Settings', and 'Status'. Below the tabs, there is a 'Log file' section with a refresh icon, a date input field set to '7/9/2020', and an 'Enable debug' checkbox. The main area shows a log of system events from 01:54:27 to 10:54:28. The logs alternate between 'getting active tickets for VA_RESULT' and 'getting Guardium records for VA_RESULT', with some entries indicating 'no active tickets for VA_RESULT'. At the bottom right, there are 'Save' and 'Close' buttons.

```
[ INFO] 01:54:27 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 01:54:28 - [GuardTicketMonitor] getting Guardium records for VA_RESULT
[ INFO] 02:54:26 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 02:54:26 - [GuardTicketMonitor] no active tickets for VA_RESULT
[ INFO] 03:54:25 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 03:54:25 - [GuardTicketMonitor] no active tickets for VA_RESULT
[ INFO] 04:54:26 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 04:54:26 - [GuardTicketMonitor] no active tickets for VA_RESULT
[ INFO] 05:54:26 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 05:54:26 - [GuardTicketMonitor] no active tickets for VA_RESULT
[ INFO] 06:54:25 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 06:54:25 - [GuardTicketMonitor] no active tickets for VA_RESULT
[ INFO] 07:54:27 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 07:54:28 - [GuardTicketMonitor] getting Guardium records for VA_RESULT
[ INFO] 08:54:26 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 08:54:27 - [GuardTicketMonitor] getting Guardium records for VA_RESULT
[ INFO] 09:54:26 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 09:54:27 - [GuardTicketMonitor] no active tickets for VA_RESULT
[ INFO] 10:54:27 - [GuardTicketMonitor] getting active tickets for VA_RESULT
[ INFO] 10:54:28 - [GuardTicketMonitor] getting Guardium records for VA_RESULT
```

Creating tickets for VA failed tests

- Tickets are created on ServiceNow for failed VA tests in a few ways:
 - Automatically create tickets during VA job run
 - Manually create tickets from VA test results page
 - Automatically create tickets when VA task is executed in an audit process

Creating tickets for VA failed tests

- Automatically create tickets during VA job run
 - In External Ticketing Configuration for VA Results, set “Critical, Major” severity levels to get tickets automatically created if the test fails

External Ticketing System Configuration

Account Settings Status

* Guardium system Vulnerability Assessment Results

* Template Problem

Automatically create tickets when severity is Critical, Major

Guardium fields	ServiceNow field	Computed value
assessment_name datasource_id datasource_name datasource_type datasource_ip datasource_port test_id test_category test_description test_external_reference test_recommendation test_result test_score test_score_description test_severity test_short_description test_stig_reference	Description	assessment_name : \${assessment_name} datasource_id : \${datasource_id} datasource_name : \${datasource_name} datasource_type : \${datasource_type} datasource_ip : \${datasource_ip} datasource_port : \${datasource_port} test_id : \${test_id} test_category : \${test_category}
	Short description	IBM Guardium database assessment failure: \${t
	Additional field +	

>>

Save Close

Creating tickets for VA failed tests

- Automatically create tickets during VA job run
 - In External Ticketing Configuration for VA Results, set “Critical, Major” severity levels to get tickets automatically created if the test fails
 - Create a vulnerability assessment with various severity levels

Assessment Test Selections ?

Tests for Security Assessment SA1

Select All Unselect All Delete Selected

Type	Test Name	Tuning
<input type="checkbox"/>	ORACLE Case-sensitive logon is enabled	CONF Major (n/a) :
<input type="checkbox"/>	ORACLE Check Default Port Number listen by Oracle (non RAC)	CONF Major (n/a) :
<input type="checkbox"/>	ORACLE Check Oracle Sample Users Removed	CONF Major (n/a) :
<input type="checkbox"/>	ORACLE Check Parameter LOCAL_LISTENER Setting	CONF Major (n/a) :
<input type="checkbox"/>	ORACLE CVE-2020-2734	CONF Cautionary (n/a)
<input type="checkbox"/>	ORACLE CVE-2020-2737	CONF Minor (n/a) :
<input type="checkbox"/>	ORACLE CVE_Oracle_end_of_life_support	CONF Major (n/a) :
<input type="checkbox"/>	ORACLE Database Auditing	CONF Major (n/a) :

Creating tickets for VA failed tests

- **Automatically create tickets during VA job run**
 - In External Ticketing Configuration for VA Results, set “Critical, Major” severity levels to get tickets automatically created if the test fails
 - Create a vulnerability assessment with various severity levels
 - Run the vulnerability assessment
 - After job run completed, click “View Results”

The screenshot displays the 'Security Assessment Finder' interface. At the top, there are four icons: a plus sign, a pencil, a square, and a minus sign. Below these is a list box containing the entry 'SA1'. At the bottom of the interface, there are five buttons: 'Configure Tests', 'Comments', 'Run Once Now', 'View Results', and 'Test Detail Exceptions'. The 'Run Once Now' and 'View Results' buttons are highlighted with red boxes. Below the buttons, there is a section titled 'User-defined tests' with two sub-buttons: 'Query-based Tests' and 'CAS-based Tests'.

Creating tickets for VA failed tests

– Automatically create tickets during VA job run

- In External Ticketing Configuration for VA Results, set “Critical, Major” severity levels to get tickets automatically created if the test fails
- Create a vulnerability assessment with various severity levels
- Run the vulnerability assessment
- After job run completed, click “View Results”
- Failed tests with “Critical” and “Major” severity levels have tickets created on ServiceNow during job run

Assessment Test Results		Compare with other results	Showing 29 of 29 results (0 filtered)
Test / Datasource	Result		
DBA Profile PASSWORD_LIFE_TIME Is Limited Test category: Conf. Severity: Critical Test ID: 132 This test checks the value of the PASSWORD_LIFE_TIME parameter. The PASSWORD_LIFE_TIME value serves as a limit to the number of days until a password expires. Setting this value ensures that users change their passwords at specified intervals. PASSWORD_LIFE_TIME can be set to any of the following: A specific number of days; UNLIMITED, meaning never require an account to change the password; or to DEFAULT, which uses the value indicated in the DEFAULT profile. Leaving this value on UNLIMITED allows users to use the same passwords indefinitely. This parameter is set for profiles; accounts must then be associated with these profiles. Ext. Reference: CIS Oracle v2.01 Item # 8.02, CIS Oracle 11gR2 v1.0.0 Item # 3.3, CIS Oracle 12c v2.01 Item # 3.3 STIG Reference: DO3485, DG0125 DBMS account password expiration, O121-C2-015200, O121-C2-013800 STIG Severity: CAT II STIG Iacontrols: IAIA-1, IAIA-2 STIG Srg: SRG-APP-000174-DB-000080, SRG-APP-000163-DB-000113 DS_ora Datasource type: ORACLE Severity: None	Fail User profile setup parameter PASSWORD_LIFE_TIME found out of defined threshold value Add test exception ServiceNow ticket created on 7/9/20 12:08:14 PM.000 <i>Recommendation: The PASSWORD_LIFE_TIME parameter is not set, allowing users to retain the same password indefinitely. Passwords that have been in use for long periods are likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords. You can modify your PASSWORD_LIFE_TIME setting by running a command similar to this example: For Oracle11 ALTER PROFILE <PROFILE_NAME> LIMIT PASSWORD_LIFE_TIME 60 - For Oracle12c non-container DBs See Oracle Documentation for more info for 12c and up regarding Profiles that are not "COMMON" and are container specific. For example : ALTER PROFILE C##<PROFILE_NAME> LIMIT PASSWORD_LIFE_TIME 60 container=all</i>		
DBA Profile PASSWORD_VERIFY_FUNCTION Is Implemented Test category: Conf. Severity: Critical Test ID: 133 This test checks the value of the PASSWORD_VERIFY_FUNCTION parameter for all profiles. The PASSWORD_VERIFY_FUNCTION value specifies a PL/SQL function to be used for password verification when users are creating this profile in a database. This function can be used to	Fail Found active profiles with PASSWORD_VERIFY_FUNCTION not implemented Add test exception ServiceNow ticket created on 7/9/20 12:08:14 PM.000 <i>Recommendation: The Password Verification Routine has not been implemented</i>		
Check Oracle Sample Users Removed Test category: Conf. Severity: Major Test ID: 2453 This test checks the sample user accounts that have been removed. These default sample accounts created by Oracle that have well-known passwords can be potentially used to alter or damage the database. These accounts should be removed after confirming that the sample schemas are really sample schemas. Ext. Reference: CIS Oracle v2.01 Item # 2.08, CIS Oracle 11gR2 v1.0.0 Item #1.2, CIS Oracle 12c v2.01 Item # 1.3 STIG Reference: DG0014, O121-C2-011500 STIG Severity: CAT II STIG Iacontrols: DCFA-1 STIG Srg: SRG-APP-000141-DB-000090 DS_ora Datasource type: ORACLE Severity: None	Fail The sample accounts have not been removed, which is a vulnerability. Add test exception ServiceNow ticket created on 7/9/20 12:08:16 PM.000 <i>Recommendation: These default sample accounts can be potentially used to alter database system. You should remove the default sample accounts. You can use the following command to remove the accounts: DROP USER <user> CASCADE;</i>		
Database Auditing Test category: Conf. Severity: Major Test ID: 2576 This test checks if the Oracle database auditing is enabled. Previous to Oracle 12c release, you can	Fail Database auditing is disabled. Add test exception ServiceNow ticket created on 7/9/20 12:08:17 PM.000 <i>Recommendation: Database auditing is disabled. If you prefer to use Oracle</i>		

Creating tickets for VA failed tests

– Automatically create tickets during VA job run

- In External Ticketing Configuration for VA Results, set “Critical, Major” severity levels to get tickets automatically created if the test fails
- Create a vulnerability assessment with various severity levels
- Run the vulnerability assessment
- After job run completed, click “View Results”
- Failed tests with “critical” and “major” severity levels have tickets created on ServiceNow during job run
- Click on the blue hypertext link to open the ticket in ServiceNow

The screenshot shows a ServiceNow ticket creation interface. At the top, there is a navigation bar with a back arrow, a menu icon, the problem ID 'PRB0040207', and icons for edit, view, and share. On the right of the navigation bar are buttons for 'Follow', 'Assess', 'Update', and 'Delete'. Below the navigation bar is a progress bar with stages: 'New' (active), 'Assess', 'Root Cause Analysis', 'Fix in Progress', 'Resolved', and 'Closed'. The main form contains several fields: 'Number' (PRB0040207), 'State' (New), 'First reported by' (empty), 'Impact' (3 - Low), 'Category' (-- None --), 'Urgency' (3 - Low), 'Business service' (empty), 'Priority' (5 - Planning), 'Configuration item' (empty), 'Assignment group' (empty), and 'Assigned to' (empty). A 'Problem statement' field contains the text: 'IBM Guardium database assessment failure: DBA Profile PASSWORD_LIFE_TIME Is Limited, on database'. A 'Description' field contains a detailed assessment report: 'assessment_name : SA1, datasource_id : 20000, datasource_name : DS_ora, datasource_type : ORACLE, datasource_ip : 9.70.150.159, datasource_port : 1522, test_id : 132, test_category : Configuration, test_description : DBA Profile PASSWORD_LIFE_TIME Is Limited, test_external_reference : CIS Oracle v2.01 Item # 8.02,CIS Oracle 11gR2 v1.0.0 Item # 3.3, CIS Oracle 12c v2.01 Item # 3.3, test_recommendation : The PASSWORD_LIFE_TIME parameter is not set, allowing users to retain the same password indefinitely. Passwords that have been in use for long periods are likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords. You can modify your PASSWORD_LIFE_TIME setting by running a command similar to this example: For Oracle11 ALTER PROFILE <PROFILE_NAME> LIMIT PASSWORD_LIFE_TIME 60 - For Oracle12c non-container DBs See Oracle Documentation for more info for 12c and up regarding Profiles that are not "COMMON" and are container specific. For example: ALTER PROFILE C#<PROFILE_NAME> LIMIT PASSWORD_LIFE_TIME 60 container=all, test_result : User profile setup parameter PASSWORD_LIFE_TIME found out of defined threshold value, test_score : 0'. A blue link is visible next to the problem statement.

Creating tickets for VA failed tests

- Manually create tickets from VA test results page

- On VA view results page, on a failed test, click “Create ticket...”

<p>LOGICAL_READS_PER_SESSION is limited</p> <p>Test category: Conf. Severity: Minor</p> <p>Test ID: 249</p> <p>This test checks that the LOGICAL_READS_PER_SESSION parameter is set to an appropriate value. LOGICAL_READS_PER_SESSION limits the number of data blocks read in a session, including blocks read from memory and disk; if unset or set to an inappropriate value, a session can throttle the database by consuming an excessive portion of the available resources.</p> <p>Ext. Reference: CIS Oracle v2.01 Item # 8.11</p> <p>STIG Reference: O121-C3-019300</p> <p>STIG Severity: CAT III</p> <p>STIG Srg: SRG-APP-000247-DB-000134</p> <p>DS_ora</p> <p>Datasource type: ORACLE Severity: None</p>	<p>Fail User profile setup parameter LOGICAL_READS_PER_SESSION found out of defined threshold value</p> <p>Add test exception</p> <p>Create ticket...</p> <p><i>Recommendation: The LOGICAL_READS_PER_SESSION Profile parameter is not configured properly. Guardium recommends setting this to a lower value; this value may be customized to meet your organization's needs by changing the test default threshold. You can alter your database profile by running the example command: ALTER PROFILE <PROFILE_NAME> LIMIT LOGICAL_READS_PER_SESSION 10000;</i></p>
<p>O7_DICTIONARY_ACCESSIBILITY Is False</p> <p>Test category: Conf. Severity: Minor</p> <p>Test ID: 32</p> <p>This test checks the value of the O7_DICTIONARY_ACCESSIBILITY parameter. Oracle 9i provides the</p>	<p>Fail Parameter: 'O7_DICTIONARY_ACCESSIBILITY' is 'TRUE'.</p> <p>Add test exception</p> <p>Create ticket...</p>

Creating tickets for VA failed tests

- Manually create tickets from VA test results page
 - On VA view results page, on a failed test, click “Create ticket...”
 - On “Create a ticket in ServiceNow” dialog, edit as needed and click “Save” button to create the ticket in ServiceNow for this failed test result

Create a ticket in ServiceNow

Description

```
assessment_name : SA1
datasource_id : 20000
datasource_name : DS_ora
datasource_type : ORACLE
datasource_ip : 9.70.150.159
datasource_port : 1522
test_id : 249
test_category : Configuration
```

Short description

IBM Guardium database assessment failure: LOGICAL_READS_F

Additional field 

Creating tickets for VA failed tests

– Manually create tickets from VA test results page

- On VA view results page, on a failed test, click “Create ticket...”
- On “Create a ticket in ServiceNow” dialog, edit as needed and click “Save” button to create the ticket in ServiceNow for this failed test result
- Back to VA test results page, click on the ticket link to open the ticket in ServiceNow

The screenshot displays the VA test results page for a failed test. The test is titled "LOGICAL_READS_PER_SESSION is limited" and is categorized as "Conf." with a severity of "Minor". The test ID is 249. The description states: "This test checks that the LOGICAL_READS_PER_SESSION parameter is set to an appropriate value. LOGICAL_READS_PER_SESSION limits the number of data blocks read in a session, including blocks read from memory and disk; if unset or set to an inappropriate value, a session can throttle the database by consuming an excessive portion of the available resources." The test is associated with the database "DS_ora" and the data source type "ORACLE".

A "Success" dialog box is overlaid on the page, indicating that a ticket was successfully created in ServiceNow. The dialog text reads: "Successfully created a ticket".

The ServiceNow ticket details are shown below the dialog. The ticket number is PRB0040214. The state is "New". The impact is "3 - Low", the urgency is "3 - Low", and the priority is "5 - Planning". The problem statement is "IBM Guardium database assessment failure: LOGICAL_READS_PER_SESSION is limited, on database: DS_ora". The description includes the following details: "assessment_name : SA1", "datasource_id : 20000", "datasource_name : DS_ora", "datasource_type : ORACLE", "datasource_ip : 9.70.150.159", "datasource_port : 1522", and "test_id : 249".

Creating tickets for VA failed tests

- Automatically create tickets when VA task is executed in an audit process
 - The audit process ticketing system uses the Alerter configuration

External Ticketing System Configuration

Account **Settings** Status

* Guardium system Alerter

* Template Incident

Guardium fields	ServiceNow field	Computed value
message_subject message_text message_creation_date	Description	message_subject : \${message_subject} message_text : \${message_text} message_creation_date : \${message_creation_date}
	Short description	IBM Guardium security alert: \${message_subjec
	Additional field +	

Save Close

Creating tickets for VA failed tests

- Automatically create tickets when VA task is executed in an audit process
 - The audit process ticketing system uses the Alerter configuration
 - Create an audit process with a vulnerability assessment task

Create New Audit Process

✓ Name and archive *psa2*

Add tasks *Add tasks to this audit process*

New task

* Task type

* Name

* Security Assessment

Export as AXIS SCAP

PDF Content Report Diff Report and Diff

Creating tickets for VA failed tests

- Automatically create tickets when VA task is executed in an audit process
 - The audit process ticketing system uses the Alerter configuration
 - Create an audit process with a vulnerability assessment task
 - Add TICKET receiver for the audit process

Send results Select who will receive audit process results

Review receivers, define distribution sequence and review options. Select a row to edit options.

+ ✎ - | ↕ Filter

Receiver	Receiver Type	Sequence	Action	Approve If Empty
<div><h3>New Receiver</h3><p>Receiver Type ? <input type="radio"/> Role <input type="radio"/> Email <input type="radio"/> User Group <input type="radio"/> User <input checked="" type="radio"/> Ticket</p><p>Assign to user <input type="text" value="Assign this ticket to selected user"/></p><p>Assign to group <input type="text" value="Assign this ticket to selected group"/></p><p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p></div>				

Creating tickets for VA failed tests

- Automatically create tickets when VA task is executed in an audit process
 - The audit process ticketing system uses the Alerter configuration
 - Create an audit process with a vulnerability assessment task
 - Add TICKET receiver for the audit process
 - At the end of the audit process job, the audit process result PDF is attached to a new ServiceNow ticket

Incident INC0010741

Manage Attachments (1): h2p_ap1000000_n1_v8.pdf [rename] [view]

Number: INC0010741

Caller: System Administrator

Category: Inquiry / Help

Subcategory: -- None --

Business service: [Search]

Contact type: -- None --

State: New

Impact: 3 - Low

Urgency: 3 - Low

Priority: 5 - Planning

Assignment group: [Search]

Assigned to: [Search]

* Short description: IBM Guardium security alert: Audit record for [psa2]

Description: message_subject : Audit record for [psa2]
message_text : Audit process "psa2", executed on 2020-07-09 15:19:08.0 requires your signature. Attached is the report in Adobe Acrobat format . You may also view the report online: https://gat-vc3a-vm11.guard.swg.usma.ibm.com:8443/sqlguard/index.jsp#rdpg=vwpr_1
message_creation_date : 2020-07-09 15:22:11

Creating tickets for VA failed tests

– Automatically create tickets when VA task is executed in an audit process

- The audit process ticketing system uses the Alerter configuration
- Create an audit process with a vulnerability assessment task
- Add TICKET receiver for the audit process
- At the end of the audit process job, the audit process result PDF is attached to a new ServiceNow ticket
- Download attachment to review audit process result

IBM Guardium®
psa2
Audit process execution began 2020-07-09 15:19:08 on gat-vc3a-vm11

1 Task was run as part of this process.
Security Assessment: tsa2 [SA2] Overall Value: 90

Distribution Status:

Receiver	Last Action Date	Status	Action Required
ServiceNow		Not Distributed	External Review

Comments:

Security Assessment: tsa2 [SA2]
IBM Guardium®

Results for Security Assessment: **SA2**
Assessment executed: 2020-07-09 15:19:21

Tests passing: **50%**
CIS Tests passing: 3/7
STIG Tests passing: 3/6
CVE Tests passing: 1/1

*The above tests passing statistics do not take into account any filtering that may currently be applied, and do not include tests in any status other than passed or failed.

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

Assessment Result History

Time	Tests passing
12:00 PM	0%
6:00 PM	50%
7/9/20	0%
6:00 AM	0%
12:00 PM	0%
6:00 PM	0%

Result Summary Showing 8 of 8 results (0 filtered)

Critical	Major	Minor	Caution	Info
Privilege	--	--	--	--
Authentication	-- 1F	--	--	-- 1F
Configuration	--	1p 1f	1p 1f	1p
Version	1p	--	--	--
Other	--	--	--	--

Current filtering applied:
Test Severities: Show All -
Datasource Severities: Show All -
Scores: Show All -
Types: Show All -

Assessment Test Results Showing 8 of 8 results (0 filtered)

Test / Datasource	Result
PASSWORD_LOCK_TIME is set Test category: Auth. Severity: Critical Test ID: 2310 This test checks that the PASSWORD_LOCK_TIME parameter is set to an appropriate value. The PASSWORD_LOCK_TIME should be set to 1, UNLIMITED or to a site-approved minimum to help prevent password attacks. Ext. Reference: CIS Oracle v2.01 Item # 8.05, CIS Oracle 11gR2 v1.0.0 Item # 3.2, CIS Oracle 12c v2.01 Item # 3.2 STIG Reference: DGI9133, O121-C2-004900 STIG Severity: CAT II STIG Iacontrols: ECL0-1, ECL0-2 STIG Srg: SRG-APP-000065-08-000024	Fail PASSWORD_LOCK_TIME is not set, or is set to an unacceptable value. Recommendation: The PASSWORD_LOCK_TIME parameter is not configured properly. Guardium recommends setting this to 1, UNLIMITED or higher; however, this value may be customized to meet your organization's needs by changing the test default threshold. You can alter your database profile by running the example command: ALTER PROFILE <PROFILE_NAME> LIMIT PASSWORD_LOCK_TIME 1;
DS_orc Datasource type: ORACLE Severity: None Details: Profile = GUARDIUM_VA_PROFILE : Limit = .0208	

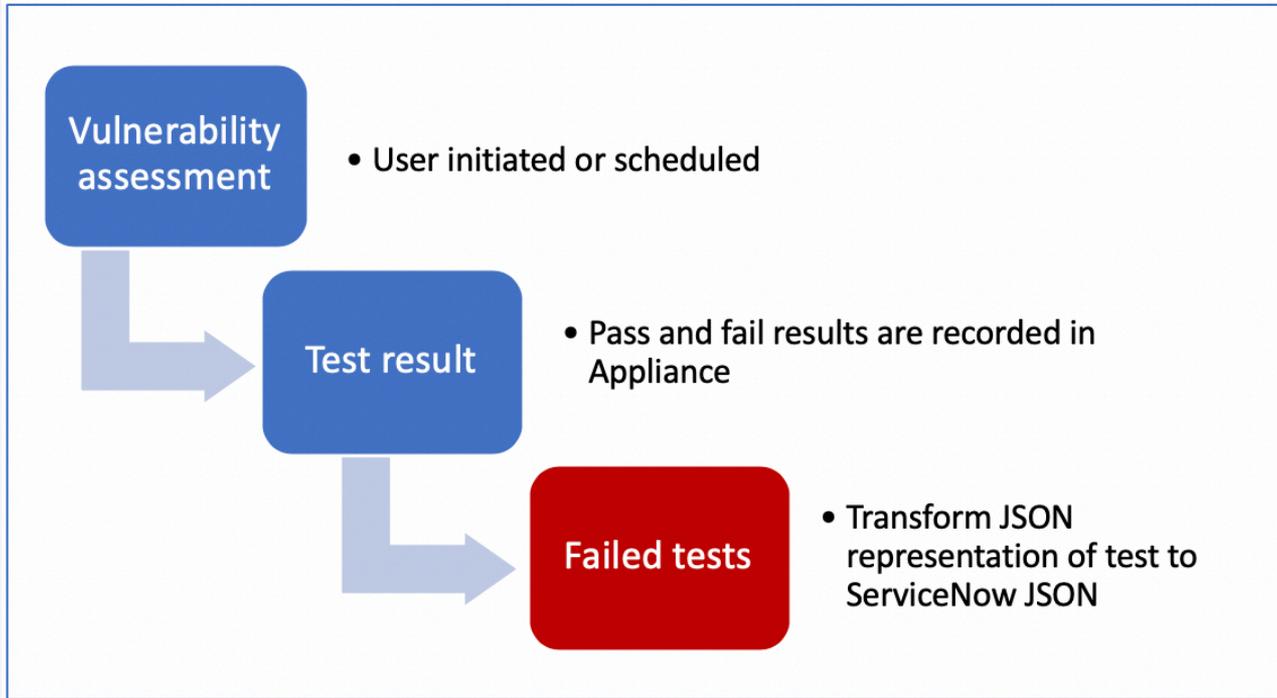
Viewing tickets

- “External Tickets” report on Gaurdium UI

External Tickets						
Start Date: 2020-07-09 05:33:30 End Date: 2020-07-09 15:33:30 GuardiumSource: % TicketNumber: % Main Entity: External Tickets Less						
 Export ▾ Actions ▾ Graphical View ?						
Guardium Source	Ticket Number	Summary	Assigned to	Status	Created	Updated
VA_RESULT	PRB0040214	IBM Guardium database assessment failure: LOGICAL_READS_PER_SESSION is limited, on database: DS_ora		New	2020-07-09 14:00:21	2020-07-09 14:00:21
VA_RESULT	PRB0040213	IBM Guardium database assessment failure: Ensure No Users Are Assigned to the DEFAULT Profile, on database: DS_ora		New	2020-07-09 12:08:17	2020-07-09 12:08:17
VA_RESULT	PRB0040212	IBM Guardium database assessment failure: Database Auditing, on database: DS_ora		New	2020-07-09 12:08:17	2020-07-09 12:08:17

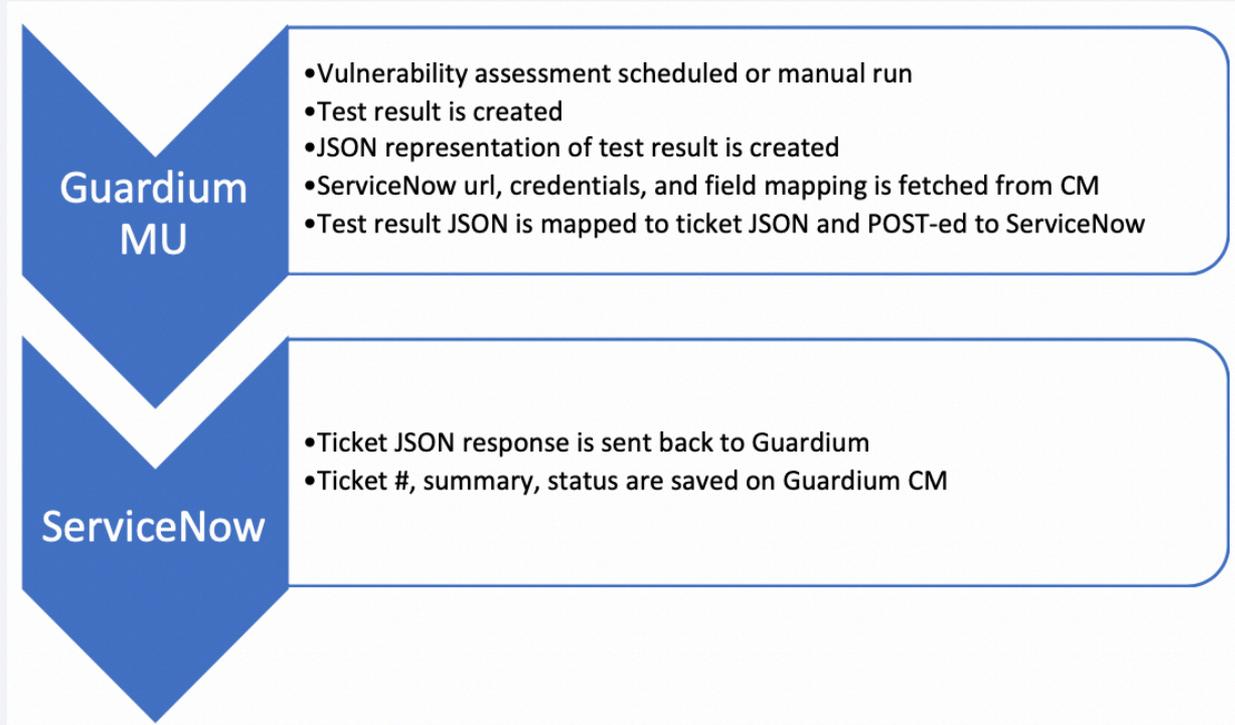
Integration design

VA failed tests are transformed to JSON that ServiceNow REST API can process to create tickets



Integration design

All ticket operations with ServiceNow are through ServiceNow REST-API



Updating tickets

Guardium ticket monitor

- Gets the latest status of all active tickets from ServiceNow created by Guardium
- Updates the matching ticket records in Guardium
- Sets “status” to closed for ticket records not in ServiceNow active ticket list
- Runs every 60 minutes by default
- Use CLI to modify the ticket monitor interval:
 - store ticket update interval <arg> [where arg represent a numeric of Minutes! ≥ 60 and ≤ 1440]

Updating tickets

On ServiceNow, add “Assigned to” and change “State” from “New” to “Assess”

Number	PRB0040207	State	Assess
First reported by	CHG0000001	Impact	3 - Low
Category	-- None --	Urgency	3 - Low
Business service		Priority	5 - Planning
Configuration item		Assignment group	
* Problem statement	IBM Guardium database assessment failure: DBA Profile PASSWORD_LIFE_TIME Is Limited, on database: DS_ora		
Description	assessment_name : SA1 datasource_id : 20000 datasource_name : DS_ora datasource_type : ORACLE datasource_ip : 9.70.150.159 datasource_port : 1522 test_id : 132		

Updating tickets

After Guardium ticket monitor runs, the ticket is updated in the Guardium External Tickets screen

External Tickets							
Start Date: 2020-07-09 09:00:29 End Date: 2020-07-09 19:00:29							More
				Export ▼ Actions ▼ Graphical View ?			
Guardium Source	Ticket Number	Summary	Assigned to ^	Status	Created	Updated	
VA_RESULT	PRB0040207	IBM Guardium database assessment failure: DBA Profile PASSWORD_LIFE_TIME Is Limited, on database: DS_ora	Problem Manager	Assess	2020-07-09 12:08:14	2020-07-09 18:49:44	
VA_RESULT	PRB0040208	IBM Guardium database assessment failure: DBA Profile PASSWORD_VERIFY_FUNCTION Is Implemented, on database: DS_ora		New	2020-07-09 12:08:14	2020-07-09 12:08:14	

Purging tickets

- In Guardium, for the tickets with a “Closed” status and not updated in 30 days, they will be purged by Guardium daily purging process.
- CLI command:
 - Show purge object age

```
guardium> show purge object age
```

ID	Age	Unit	Description
90	30	DAY	Active Risk Spotter iterations
95	90	DAY	Active Risk Spotter Score for old users
94	90	DAY	Active Risk Spotter Score per feature
75	7	DAY	Additional info for real time alerts
32	14	DAY	Aggregation Debug Log
43	7	DAY	Aggregation/Archive Log - Distributed
71	14	DAY	Alert Log
27	20	DAY	AME Files Purge
37	7	DAY	Analytic (outliers detection) log
79	90	DAY	Analytic Case
33	14	DAY	Analytic Data Debug Log
38	60	DAY	Analytic Outlier Details
39	60	DAY	Analytic Outliers Summary
46	60	DAY	Analytic User Feedback
4	7	DAY	Assessment Tests
22	14	DAY	Audit Process Log.
17	30	DAY	Baseline entries referred to user
10	90	DAY	Call Graph History
25	60	DAY	CAS AUdit State and State Datum
11	7	DAY	CAS Host Event History
96	30	DAY	Central Management External Tickets
1	7	DAY	Central Management Persistent Operations

Purging tickets

- In Guardium, for the tickets with a “Closed” status and not updated in 30 days, they will be purged by Guardium daily purging process.
- CLI command:
 - show purge object age
 - store purge object age 96 <day>



```
ok store purge object age 96 15
```

ServiceNow CMDB

To reconcile database inventory between Guardium and ServiceNow:

- Setup > Smart Assistant > Compliance Monitoring
 - Select the “Databases” tab
 - Click “Reconcile assets” and select “Reconcile” to open “Reconcile database inventory” dialog.
 - » Select “Compare to CMDB” radio button

The screenshot displays the ServiceNow Compliance Monitoring interface. At the top, the 'Compliance Monitoring' header is visible. Below it, three summary cards show 'Known databases', 'Configured databases', and 'Unconfigured databases', each with a count of 0. The 'Databases' tab is selected and highlighted with a red box. Below the tabs, the 'Reconcile assets' dropdown menu is also highlighted with a red box. The 'Reconcile database inventory' dialog box is open, showing two radio button options: 'Compare to CSV file' and 'Compare to CMDB'. The 'Compare to CMDB' option is selected and highlighted with a red box. Below the radio buttons, there is a text input field for the 'ServiceNow URL' with a placeholder text 'Select a URL or create a new account' and a dropdown arrow. At the bottom of the dialog, there are 'Load' and 'Close' buttons.

Importing and reconciling CMDB assets

- Select the ServiceNow account and template
- Map datasource fields → template's fields
- Click OK

The image displays two screenshots of the IBM Security Compliance Monitoring interface, illustrating the process of importing and reconciling CMDB assets.

Top Screenshot: Reconcile database inventory

The interface shows a dashboard with three tabs: "Known databases" (0), "Configured databases" (0), and "Unconfigured databases" (0). Below the dashboard, there are tabs for "Databases", "Applications", "Compliance summary", and "Application Summary". A table with columns "Instance name", "Database name", and "Type" is visible. A modal window titled "Reconcile database inventory" is open, showing two radio buttons: "Compare to CSV file" (unselected) and "Compare to CMDB" (selected). The "ServiceNow URL" field contains "ServiceNow > dev67812.service-now.com > admin". The "Template" dropdown is set to "MSFT SQL Instance". A red box highlights the "Load" button, with a blue arrow pointing down to the next screenshot.

Bottom Screenshot: Import from CMDB

The interface shows the same dashboard. A modal window titled "Import from CMDB" is open, with the instruction: "Select columns from CMDB to import as database properties. Values imported for the server name, service name, or instance name property are automatically assigned to the correct property based on the associated database type." The form contains several fields with dropdown menus:

- * Host name/IP: name
- * Port number: tcp_port
- * Database type: version
- Service name: None
- Database name: config_file
- Server name: None
- Instance name: instance_name
- Comment: None

Buttons for "OK" and "Cancel" are at the bottom of the modal.

SQL DB Azure – GDMMONITOR Script

- The gdmmonitor-azure.sql is used to apply the minimum required privileges to run our tests on the SQL DB Azure instance. The customer can open the file after downloading and see detailed instructions on how to run the script.
- With gdmmonitor-azure.sql, you can run this script using SSMS (Sql Server Management Studio) for EACH database that is part of your Azure instance. Meaning, you need to connect to EACH database and run this script due to limitations of connecting to another database from the MASTER database.
- In addition, you can use gdmmonitor-azure-connect.ps1 to run the gdmmonitor-azure.sql script using Powershell. The key difference to using this Powershell script versus running the gdmmonitor-azure.sql script itself, is that the Powershell script will LOOP through EACH database for you.

Important Note: The following 3 tests must be executed as the "Server Admin" or "Active Directory Admin". Credentials from these logins allow us to accurately see all the records in the system catalog view from the MASTER database. This is required in order to keep the test findings to be accurate.

1. Check for dbmanager role members
2. Check for loginmanager role members
3. Database Ownership - Azure

SQL Server – GDMMONITOR Script

- The gdmmonitor-mss.sql is used to apply the minimum required privileges to run our tests on the SQL Server instance. The customer can open the file after downloading and see detailed instructions on how to run the script.
- With gdmmonitor-mss.sql, you can run this script using SSMS (Sql Server Management Studio) or similar database client tools. In this case, the script will loop through the databases for you.
- We have added additional notes to these gdmmonitor scripts based on customer requests that will mention what changes have occurred to the script along with the date the changes took place. For example:

-- 20190911: grant select to SELECT ON sys.dm_exec_connections to gdmmonitor in master, make some comment changes

-- 20200228: add permissions related stig 2016 benchmark

APIs References

Delete datasource API References

- To support cascade delete datasource, we added 2 new parameters to delete_datasource_by_id and delete_datasource_by_name grdapi commands:
 - 1) cascade (not required – cascade is Boolean - with default value of 0 or false)
 - 2) confirmationNumber (not required – confirmation number is Integer with default value of 0)
- Executing these grdapi commands without the cascade parameters behaves as they have before. Which means, if the datasource is used by any application, it will not delete the datasource.
- Executing these grdapi commands with cascade = true performs a check. If the datasource is not used, it will delete the datasource.
- Otherwise, a message indicating where the datasource is being used along with a confirmation number which expires in 5 minutes, will be displayed.
- Executing these grdapi commands with cascade = true and that confirmation number, will delete the datasource and all of its references. (either have deleted or updated to be -1)
- Executing these grdapi commands with cascade=true and an expired confirmation number, performs a new check. If it is not used, it will delete the datasource.
- Otherwise, it will regenerate a new confirmation number and a message indicating where the datasource is being used, along with the new confirmation number will be displayed!

Delete datasource API References

- Test: Test1 - Delete a datasource that is used by VA, custom Table, and classification process - no cascade

```
grdapi delete_datasource_by_name name="A MMS demo DB2 10.5 FAIL on su11x64t3-va"
```

```
frank-vm02.guard.swg.usma.ibm.com> grdapi delete_datasource_by_name name="A MMS demo DB2 10.5 FAIL on su11x64t3-va"
```

```
delete_datasource_by_name:
```

```
ERR=126
```

```
In use by:
```

```
Classification Process: A mms demo discovery
```

```
Custom Table: DEMO_TABLE
```

```
Datasource group - A demo Datasource group
```

```
Vulnerability Assessment: A mms demo VA
```

```
Could not delete datasource. Error while checking usage.
```

```
ok
```

```
frank-vm02.guard.swg.usma.ibm.com>
```

Delete datasource API References

- Test: Test2 - Delete a datasource that is used by VA, datasource group, custom Table, and classification process - use cascade, no confirmation number

```
grdapi delete_datasource_by_name name="A MMS demo DB2 10.5 FAIL on su11x64t3-va" cascade=true
```

Result:

```
frank-vm02.guard.swg.usma.ibm.com> grdapi delete_datasource_by_name name="A MMS demo DB2 10.5 FAIL on su11x64t3-va" cascade=true
```

In use by:

Classification Process: A mms demo discovery

Custom Table: DEMO_TABLE

Datasource group - A demo Datasource group

Vulnerability Assessment: A mms demo VA

To delete cascade datasource A MMS demo DB2 10.5 FAIL on su11x64t3-va, please use cascade of true along with confirmation number 418619

ok

Delete datasource API References

- Test: Test3 - Delete a datasource that is used by VA, custom Table, and classification process - use cascade, use wrong confirmation number-

```
grdapi delete_datasource_by_name name="A MMS demo DB2 10.5 FAIL on su11x64t3-va" cascade=true  
confirmationNumber=650948
```

Result:

```
frank-vm02.guard.swg.usma.ibm.com> grdapi delete_datasource_by_name name="A MMS demo DB2 10.5 FAIL on su11x64t3-  
va" cascade=true confirmationNumber=650948
```

In use by:

Classification Process: A mms demo discovery

Custom Table: DEMO_TABLE

Datasource group - A demo Datasource group

Vulnerability Assessment: A mms demo VA

Wrong confirmation number, to delete this datasource please enter confirmation number 418619

ok

Delete datasource API References

- Test: Test4 - Delete a datasource that is used by VA, custom Table, and classification process - use cascade, use expired confirmation number-

```
grdapi delete_datasource_by_name name="A MMS demo DB2 10.5 FAIL on su11x64t3-va" cascade=true  
confirmationNumber=650948
```

Result:

```
frank-vm02.guard.swg.usma.ibm.com> grdapi delete_datasource_by_name name="A MMS demo DB2 10.5 FAIL on su11x64t3-  
va" cascade=true confirmationNumber=418619
```

In use by:

Classification Process: A mms demo discovery

Custom Table: DEMO_TABLE

Datasource group - A demo Datasource group

Vulnerability Assessment: A mms demo VA

Confirmation number has been expired, to delete this datasource please enter new confirmation number 834089

ok

Delete datasource API References

- Test: Test5 - Delete a datasource that is used by VA, custom Table, and classification process - use cascade, confirmation number-

```
frank-vm02.guard.swg.usma.ibm.com> grdapi delete_datasource_by_name name="A MMS demo DB2 10.5 FAIL on su11x64t3-va" cascade=true confirmationNumber=834089  
ID=20000  
ok  
frank-vm02.guard.swg.usma.ibm.com>
```

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM Security



IBM