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

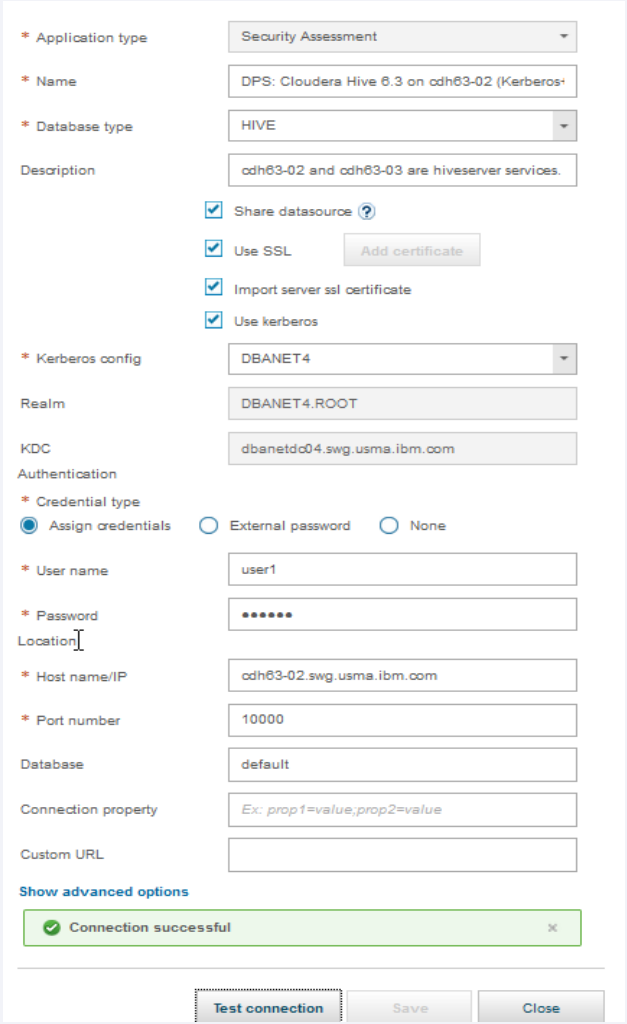
- New database release support for VA
- DPS upload validation and history reporting
- MySQL SSL and Sybase ASE SSL connection
- Custom upload datasource with role
- Datasource delete with cascade
- New Platform Support for Azure SQL
- SQL Server 2016 STIG VA Tests
- VA HALTED and resume
- DB2 special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



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.

DPS upload history

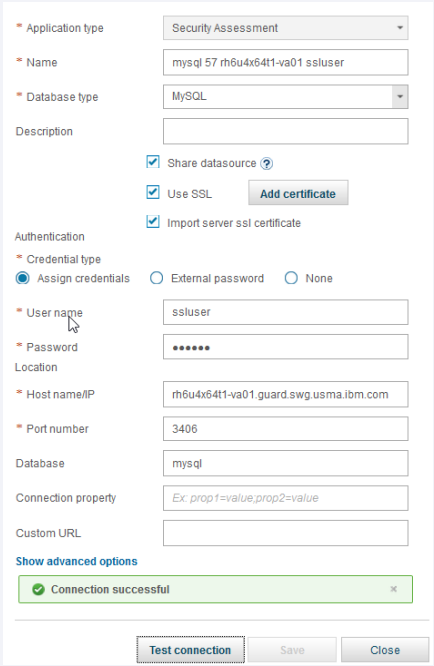
- Guardium v11.2 allows you to track the DPS upload history and see its status.
- In the Guardium CLI, run the following command: “show dps”

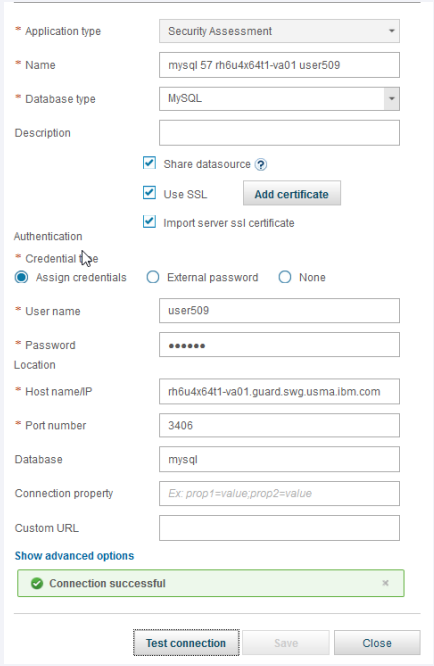
```
gva07.guard.swg.usma.ibm.com> show dps
DPS Upgrade History:
DPS File Name                                    DPS Type      Start Time           End Time             Status
-----------------------------------------------  --------      -------------------  -------------------  ------------------------------
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

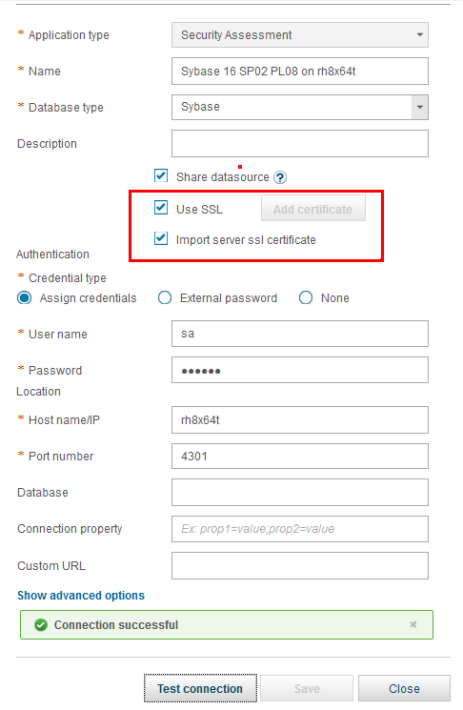
- Guardium v11.2 now supports SSL connections for MySQL 5.6, 5.7 and 8.0.
- You can connect without SSL, SSL server side or SSL x509 authentication.





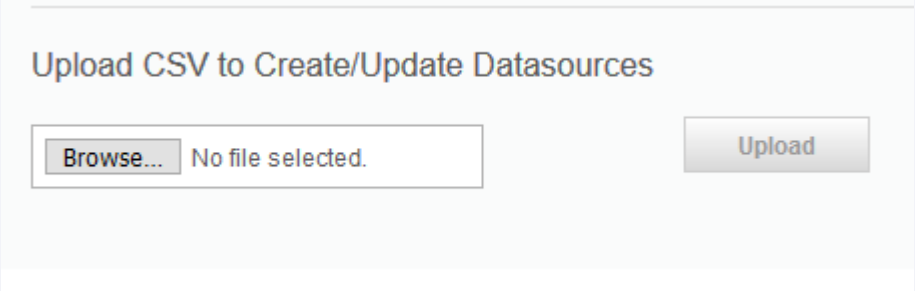
Sybase ASE datasource with SSL

- 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.



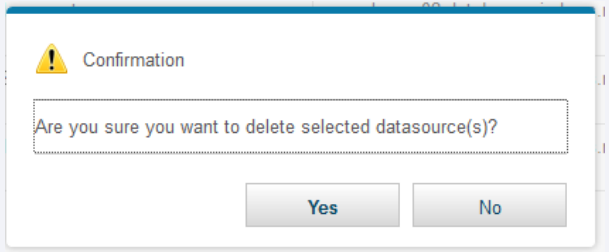
Upload CSV to Create/Update Datasources

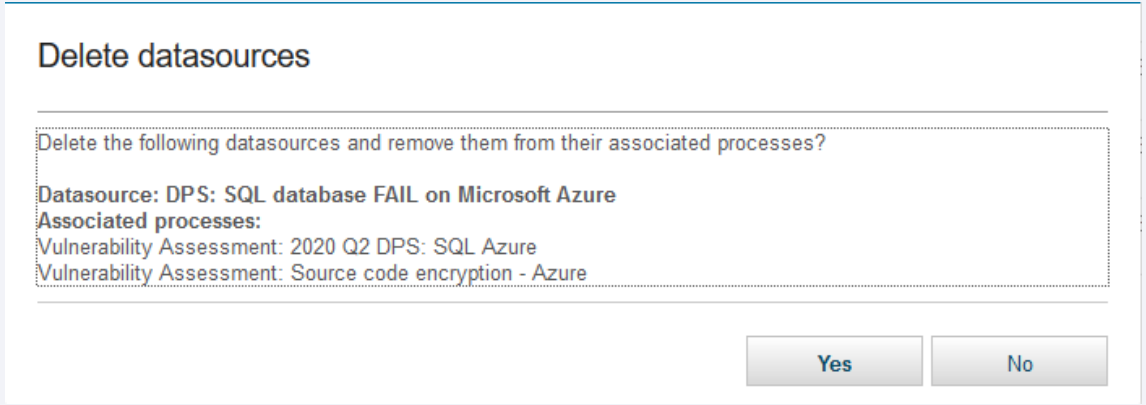
- Guardium v11.2 now supports adding and updating roles to datasources using the upload csv feature.
- You would add another column called “Role” to the csv file. You don’t need to provide a role if it is not required.
- You can add multiple roles per datasource separated by a semicolon.



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.

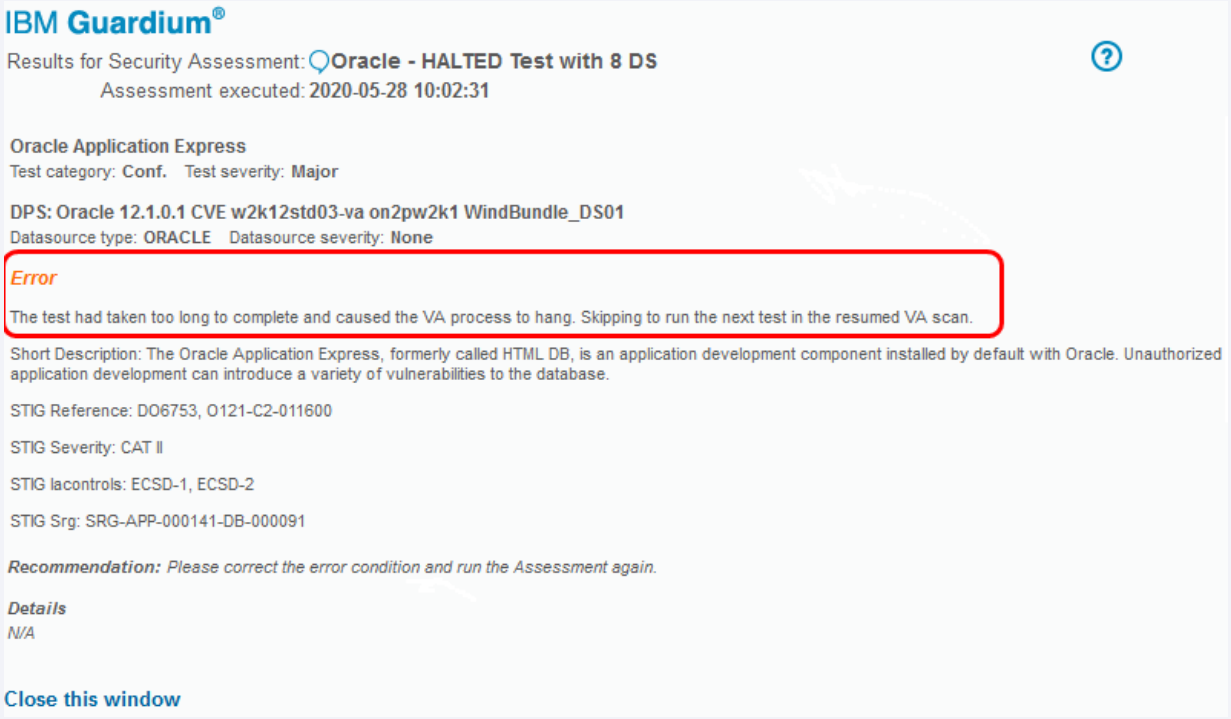
- We have created a new gdmmonitor script to support SQL DB Azure and enhanced the existing SQL Server gdmmonitor script to support the SQL Server 2016 STIG.

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.



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

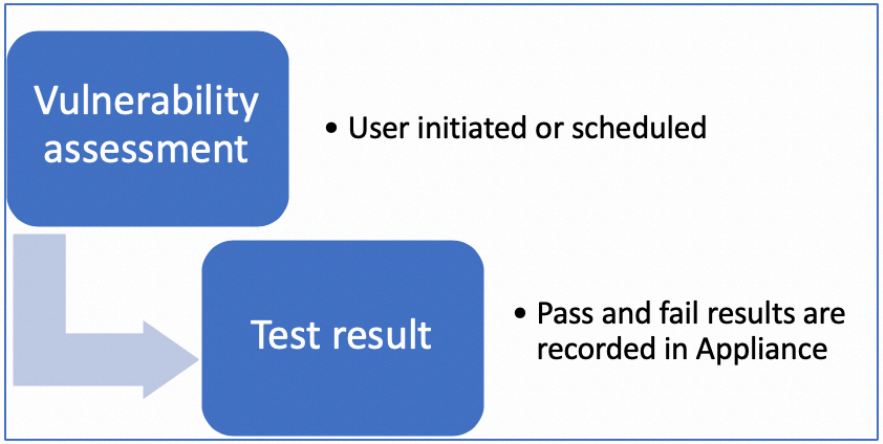
Q&A

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

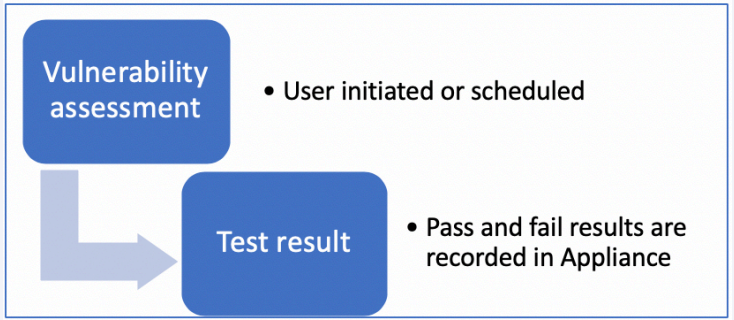
Benefits

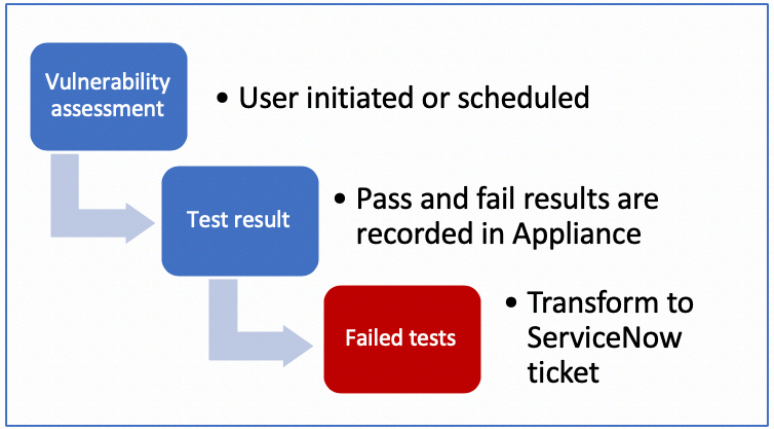
Before

- 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.





Integration features overview

VA integration with ServiceNow in Guardium v11.2

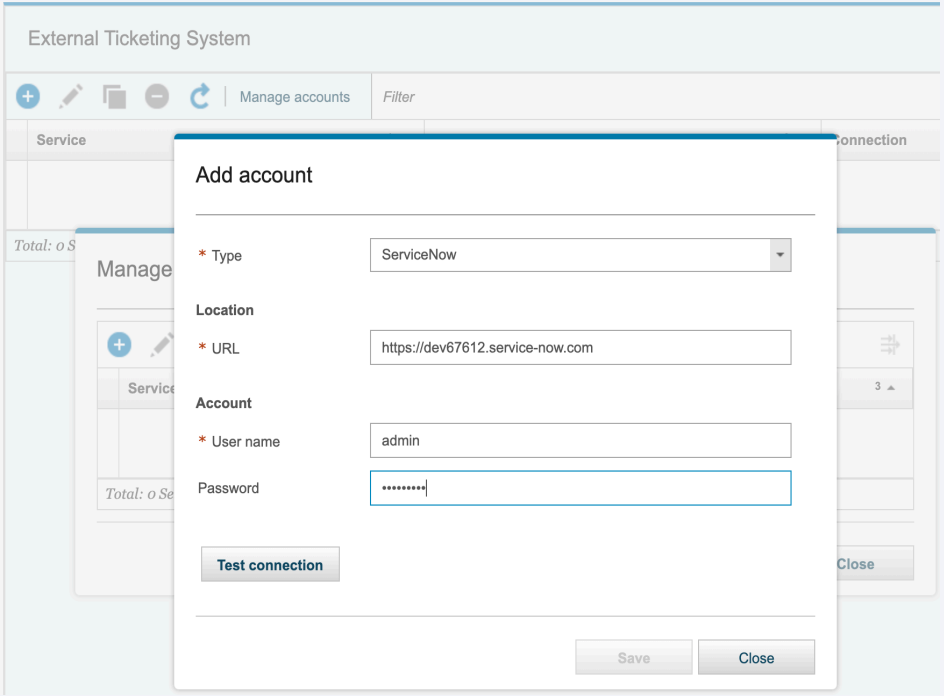
– Tickets are created in ServiceNow for failed VA tests in a few ways:

- 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:

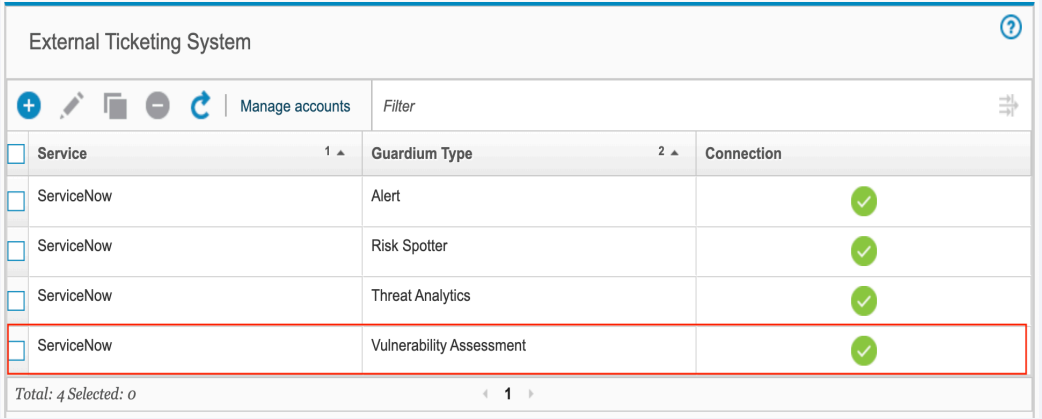
- Setup > Tools and Views > External Ticketing System
  - Add account
    - » URL: ServiceNow instance
    - » Account: user credential to access the ServiceNow instance
    - » Click “Test connection”
    - » When successful, save the account



External ticketing system configuration

Create an external ticketing configuration for Vulnerability Assessment:

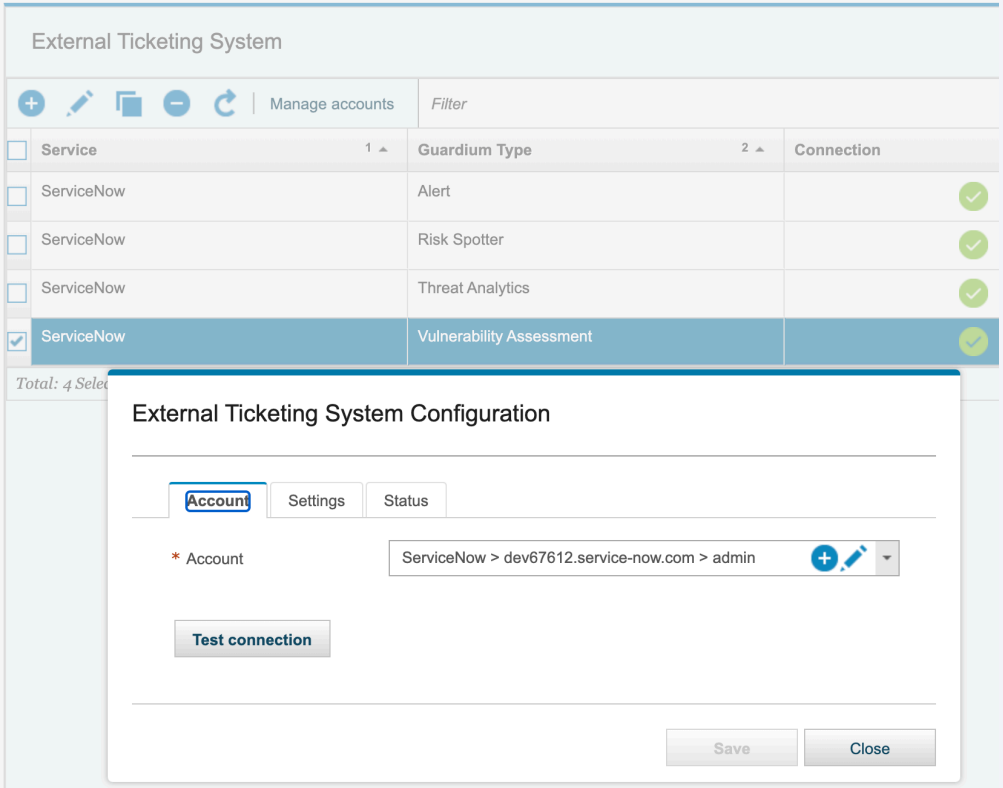
- NOTE: when we create the first external ticketing system account in Guardium, four external ticketing system configurations are created automatically. “VA Results” is one of them
- If any ticket operation failed, the "connection" will show a red X. The connection should be edited and tested again



External ticketing system configuration

The configuration dialog contains three tabs:

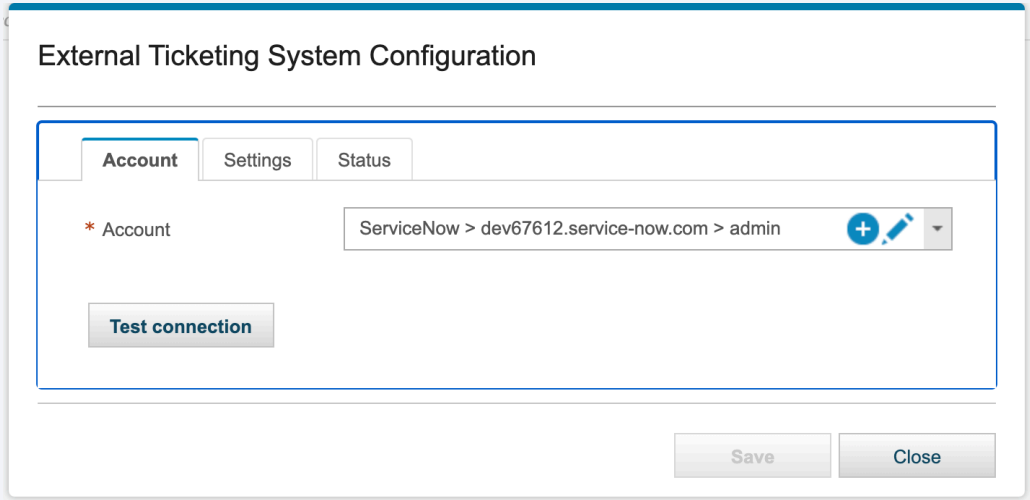
- Account
- Settings
- Status



External ticketing system configuration

Account tab

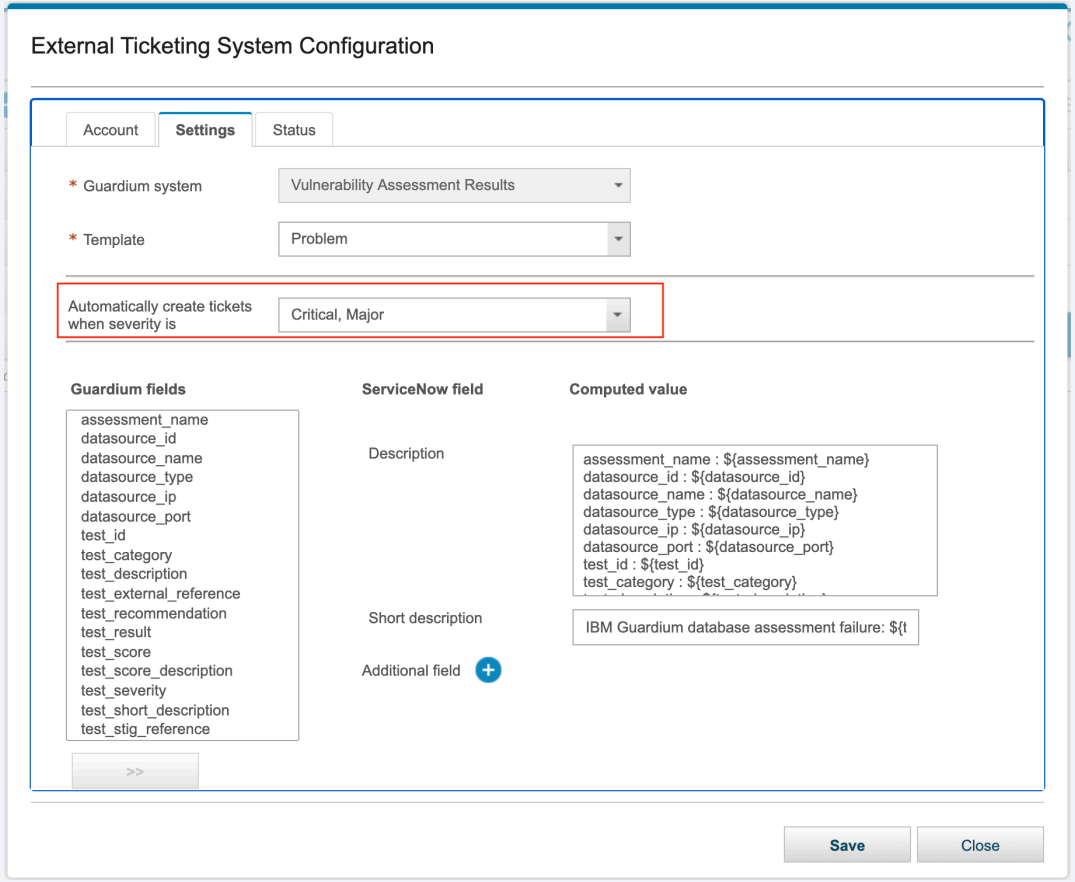
- Specifies the account created in previous step.
- Can add or edit account.



External ticketing system configuration

Settings tab

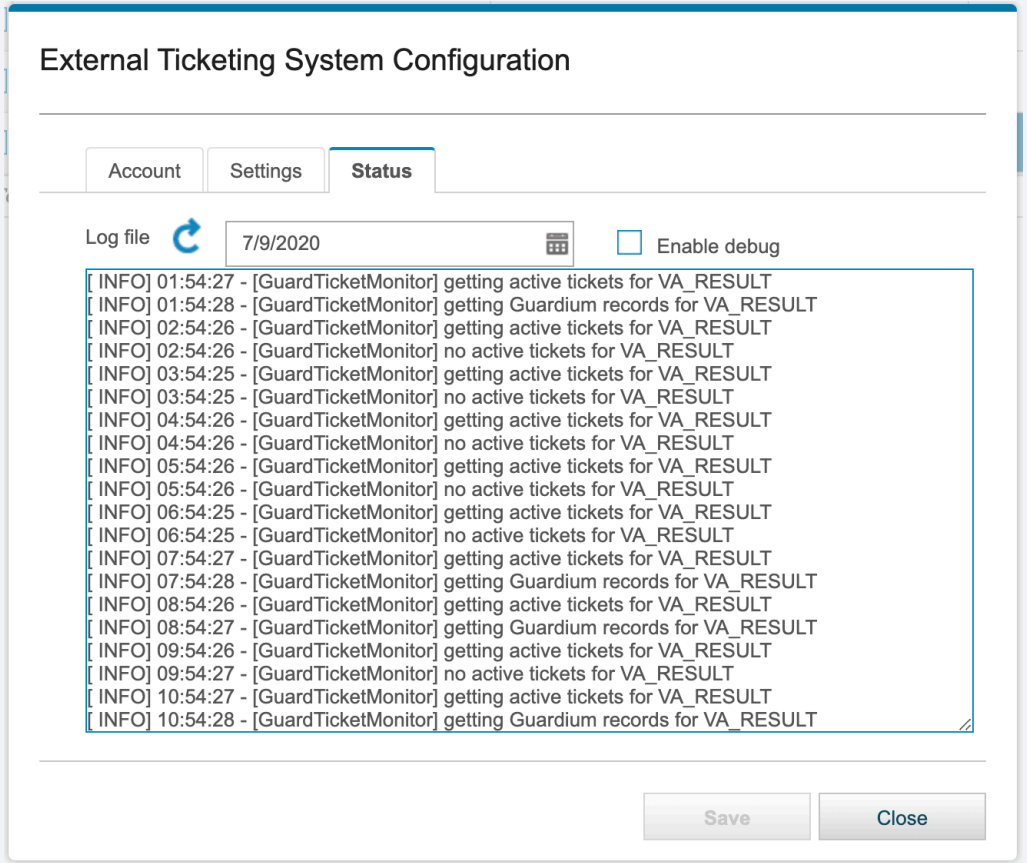
- Specifies the fields included in the tickets.
- Can specify severity options that tickets will be automatically created when the failed VA tests meet the severity criteria.



External ticketing system configuration

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.

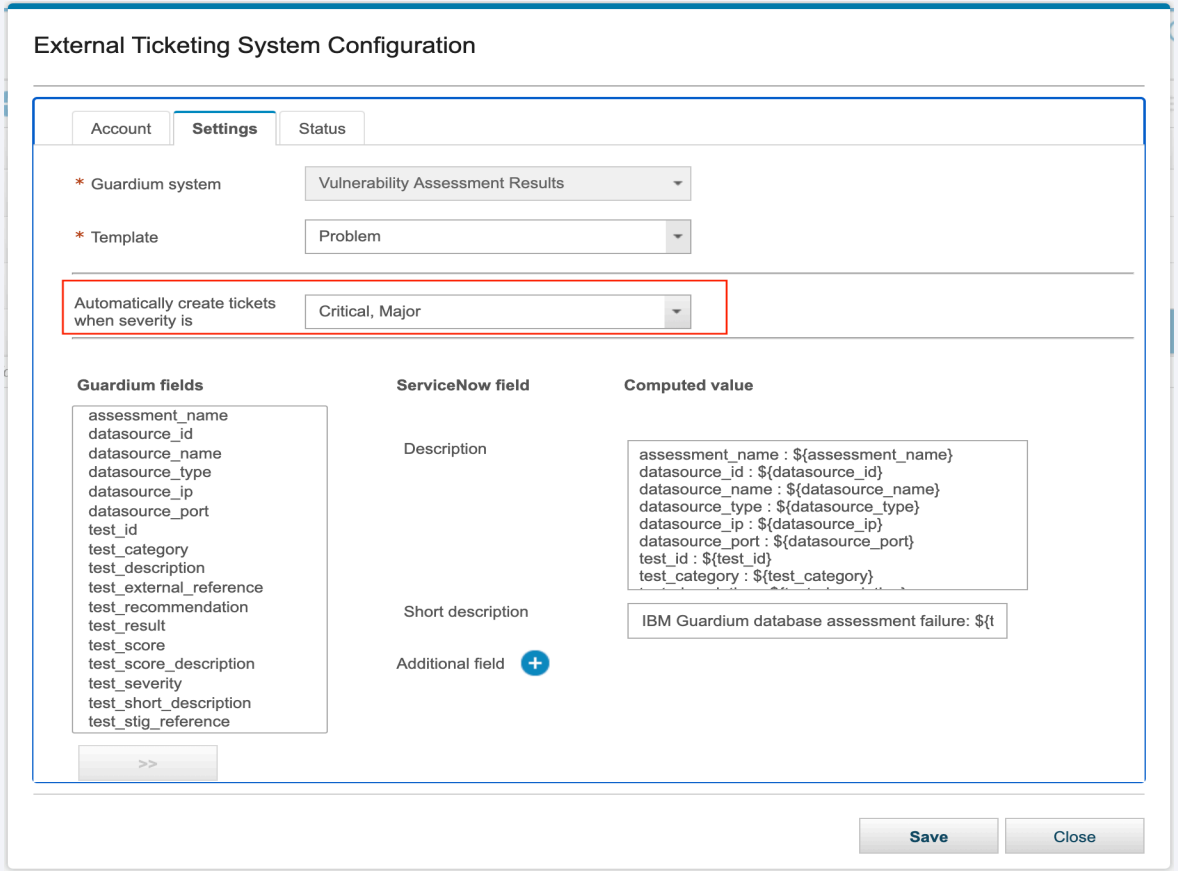


Creating tickets for VA failed tests

- 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

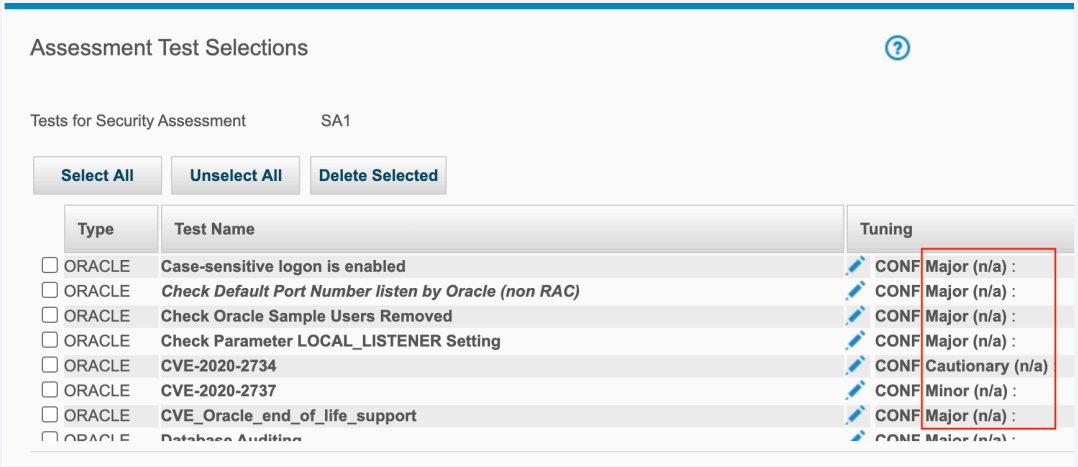
Creating tickets for VA failed tests

- 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



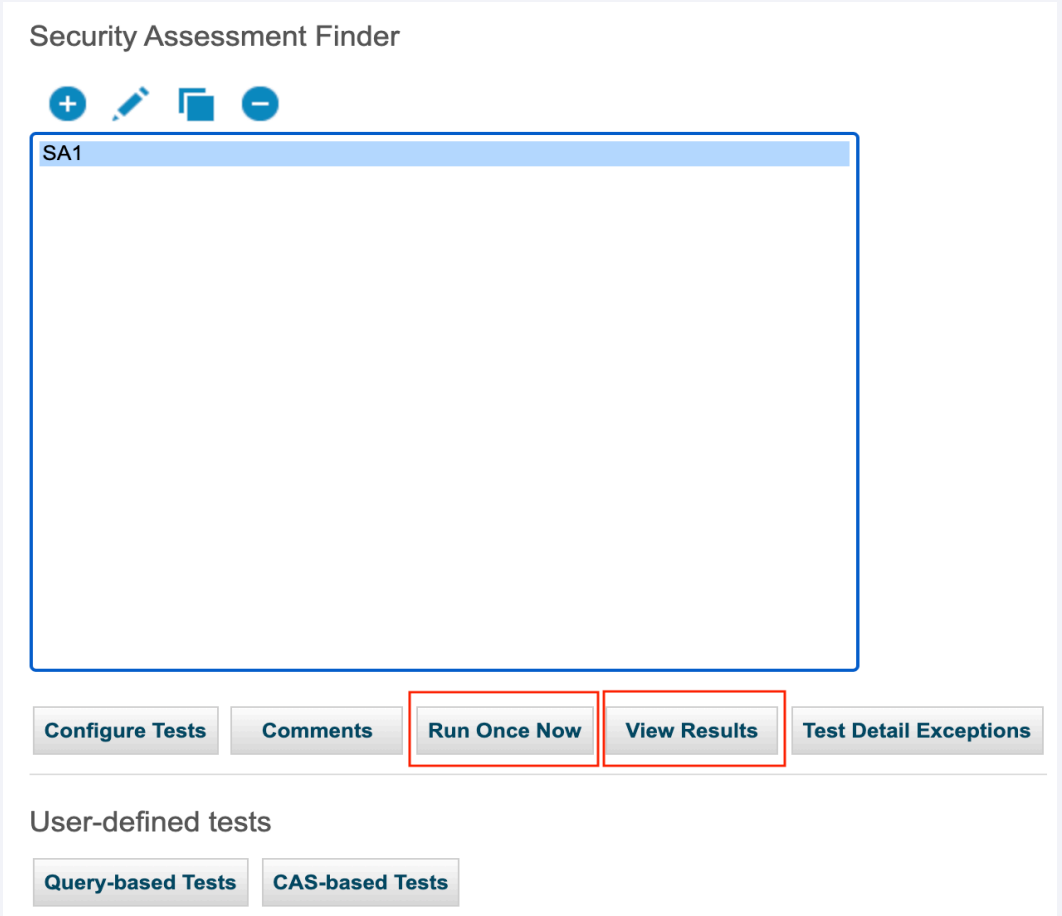
Creating tickets for VA failed tests

- 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



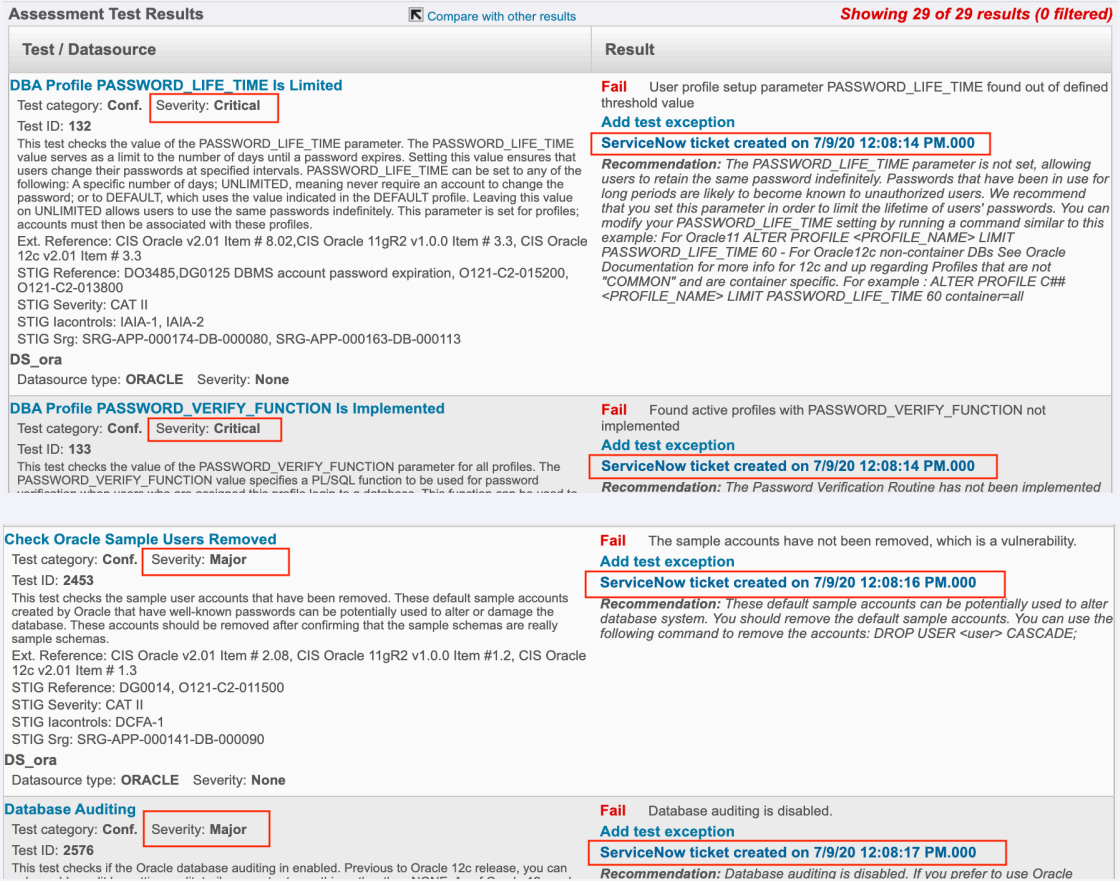
Creating tickets for VA failed tests

- 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”



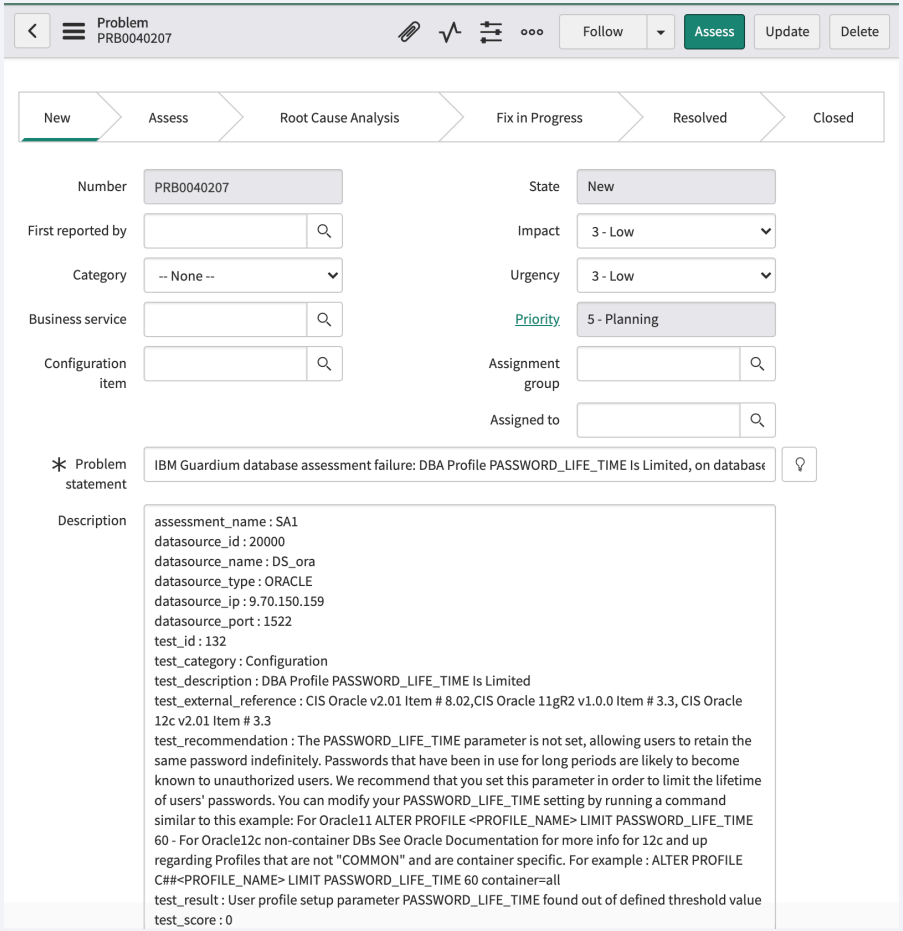
Creating tickets for VA failed tests

- 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



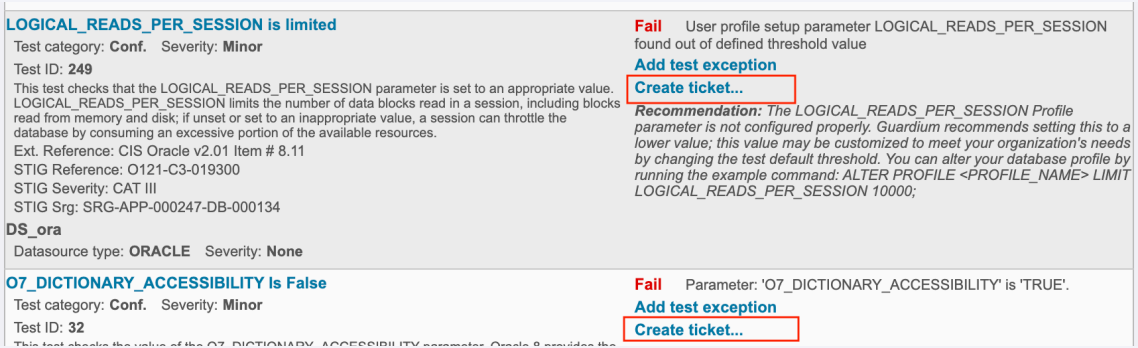
Creating tickets for VA failed tests

- 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



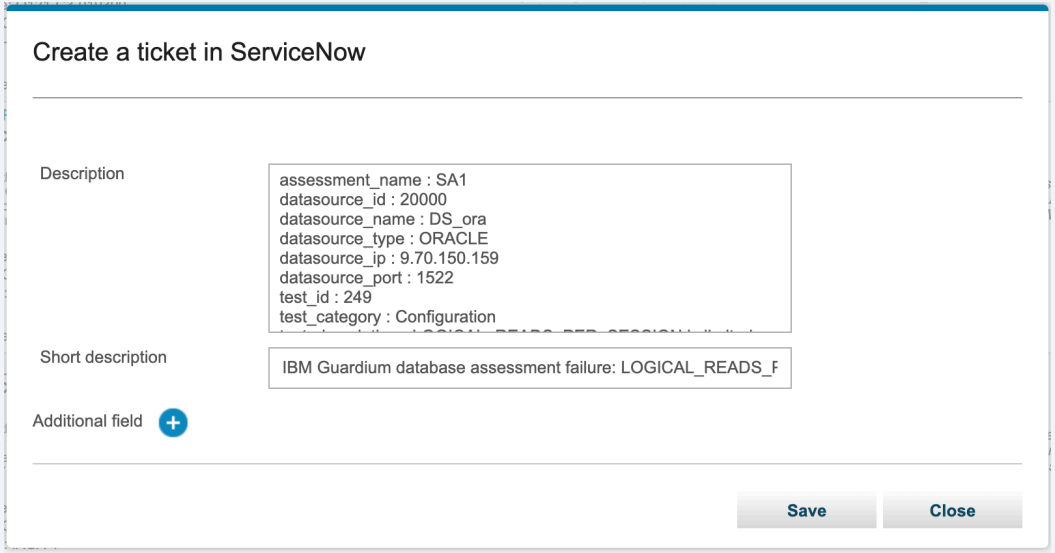
Creating tickets for VA failed tests

- Manually create tickets from VA test results page
  - On VA view results page, on a failed test, click “Create ticket…”



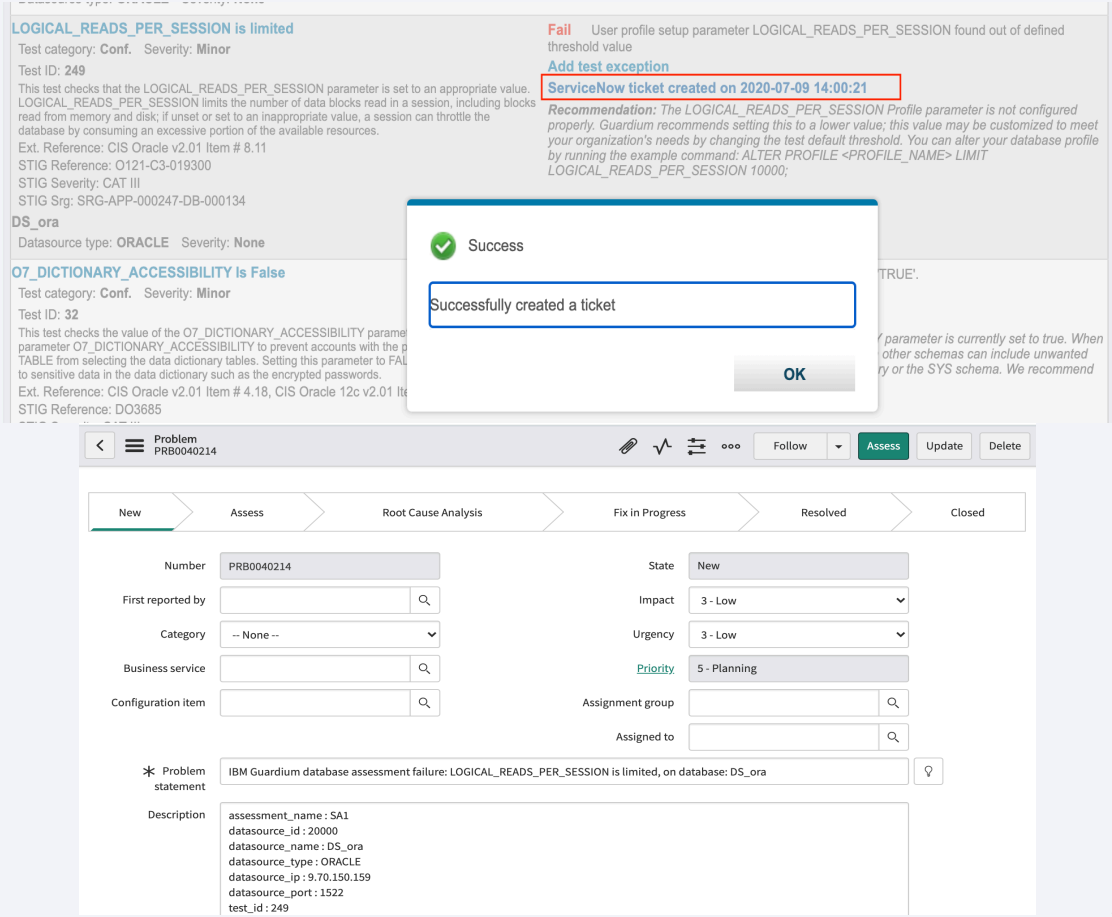
Creating tickets for VA failed tests

- 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



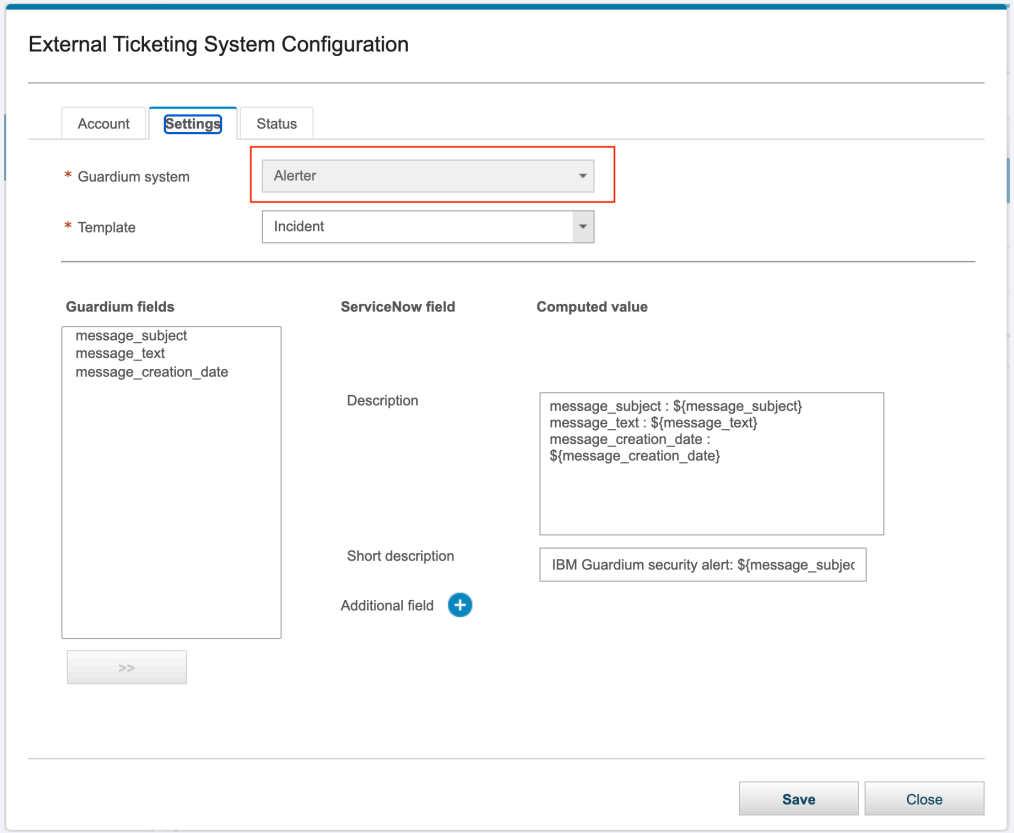
Creating tickets for VA failed tests

- 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



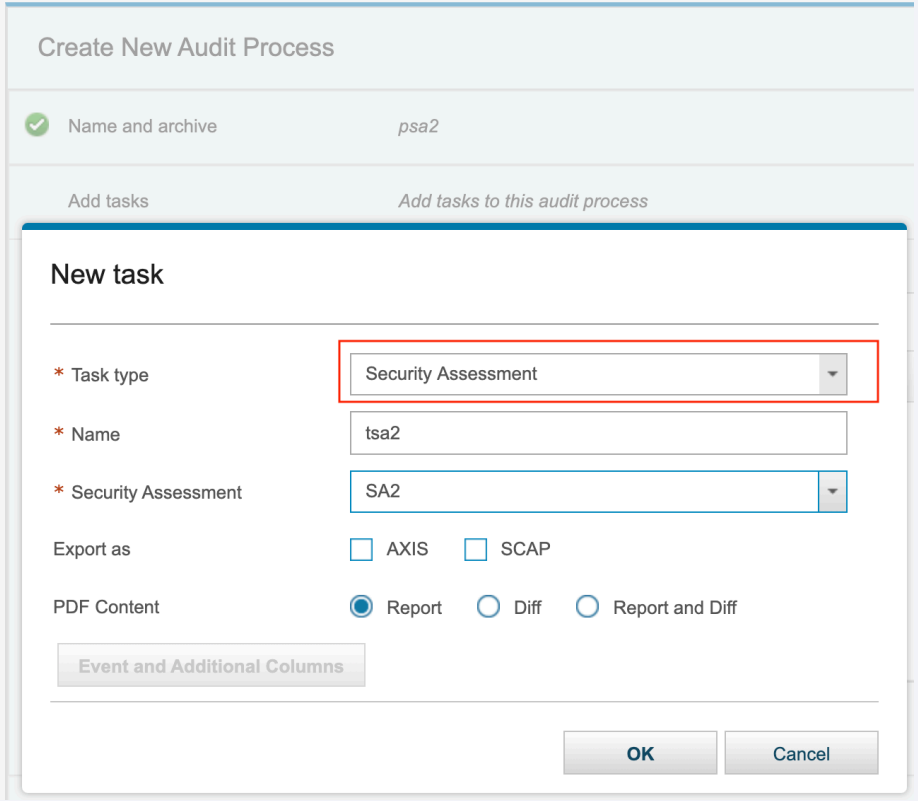
Creating tickets for VA failed tests

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



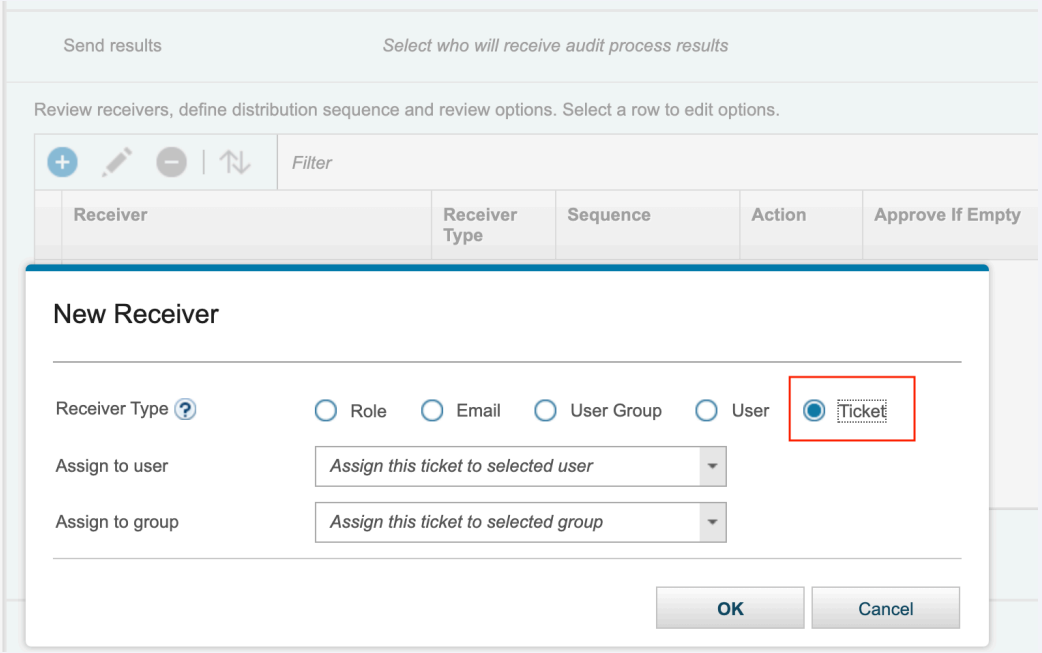
Creating tickets for VA failed tests

- 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



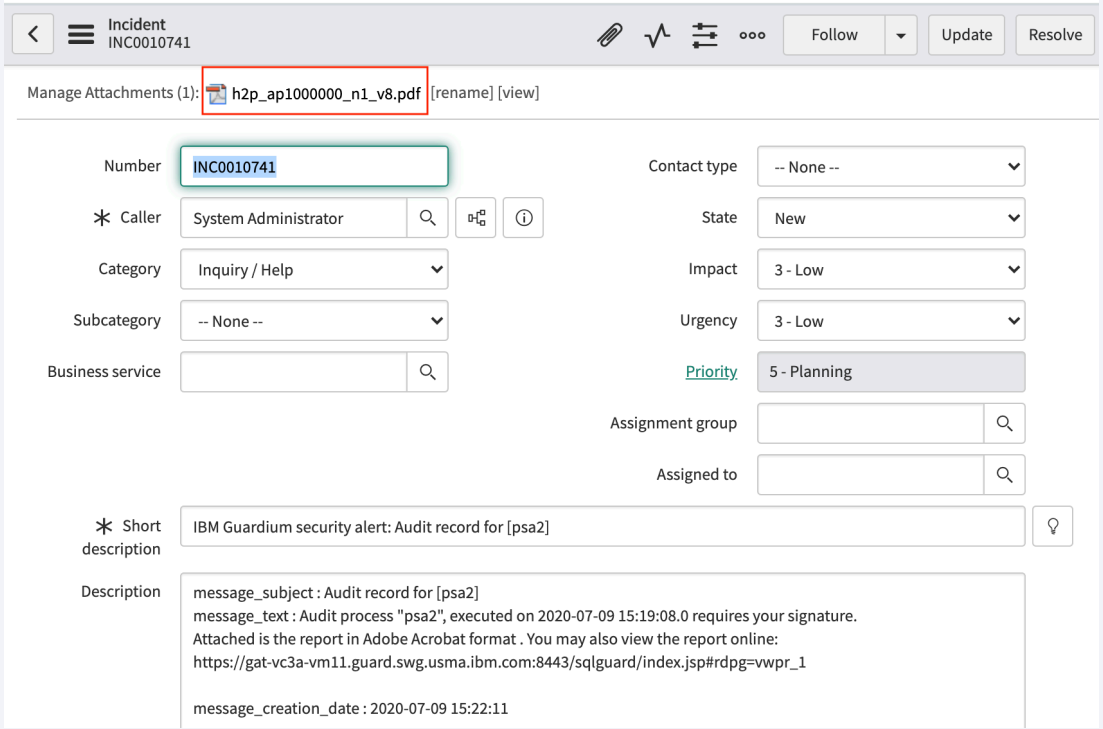
Creating tickets for VA failed tests

- 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



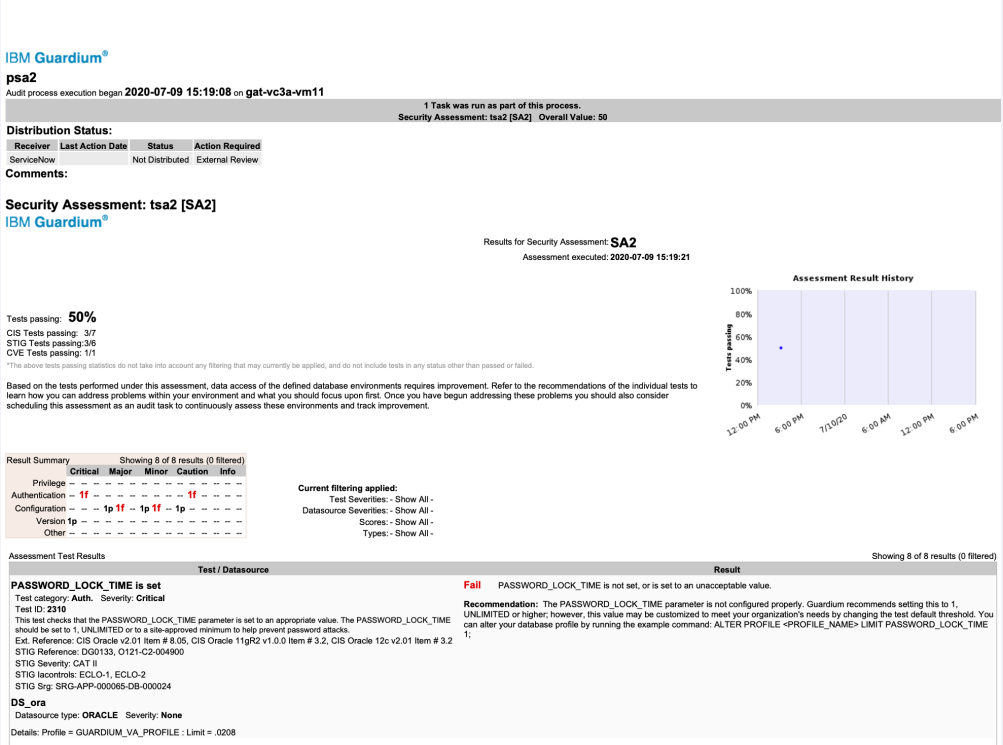
Creating tickets for VA failed tests

- 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



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: 50

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**

Assessment Result History

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.

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	--	--	--	--	--

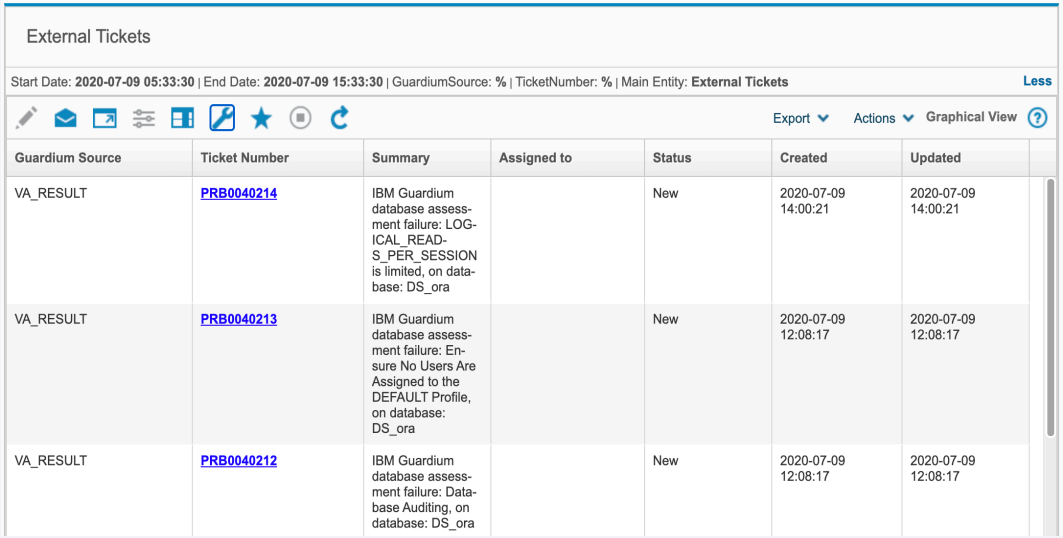
Current filtering applied:
Test Severities: - Show All -
Datasource Severities: - Show All -
Scores: - Show All -
Types: - Show All -

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: **2319** 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: DG0133, O121-C2-004900 STIG Severity: CAT II STIG Iacontrols: ECLO-1, ECLO-2 STIG Srg: SRG-APP-000065-DB-000024 **DS_ora** Datasource type: **ORACLE** Severity: **None** Details: Profile = GUARDIUM_VA_PROFILE : Limit = .0208	**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;

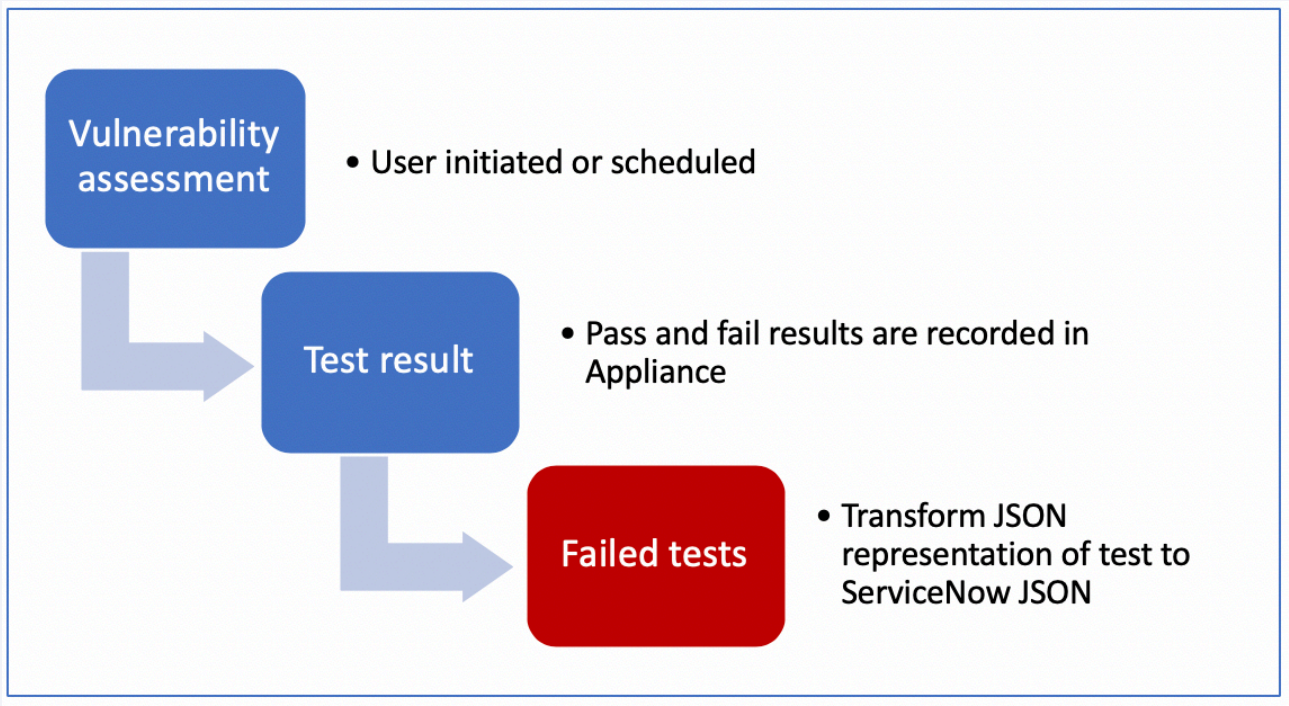
Viewing tickets

- “External Tickets” report on Gaurdium UI



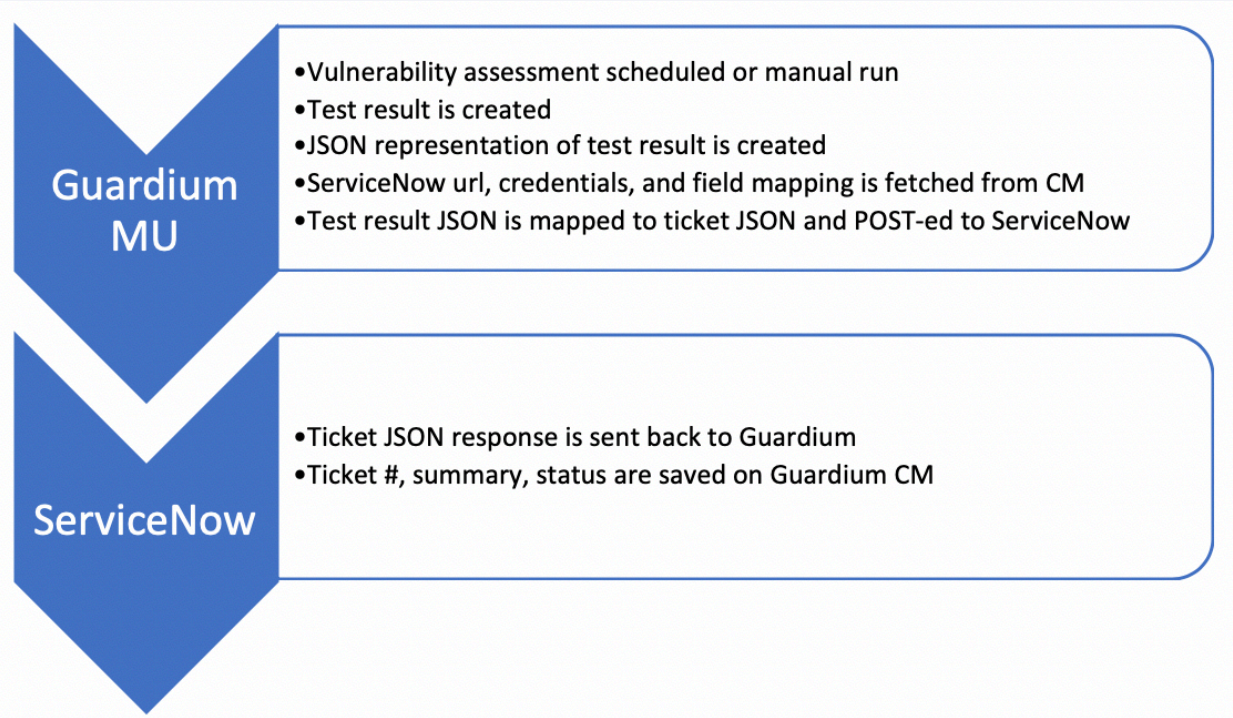
Integration design

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



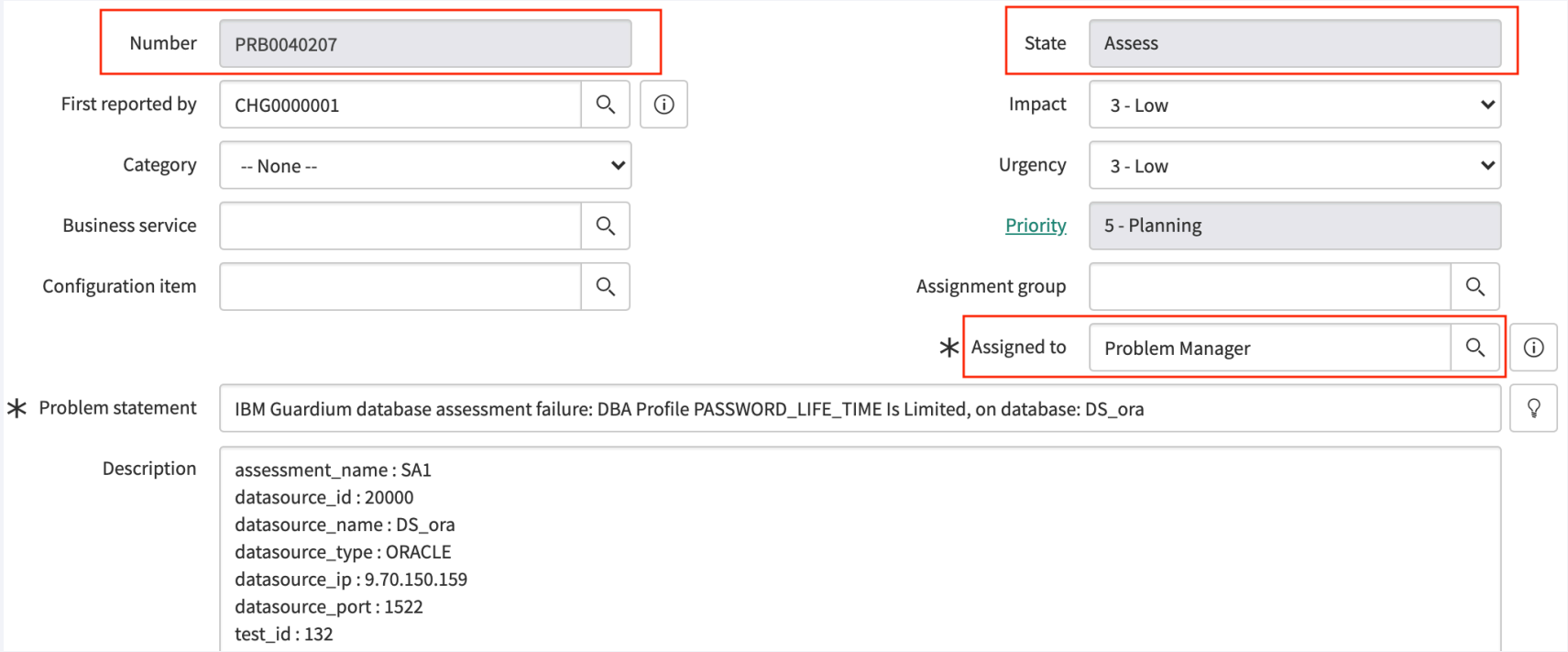
Updating tickets

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]

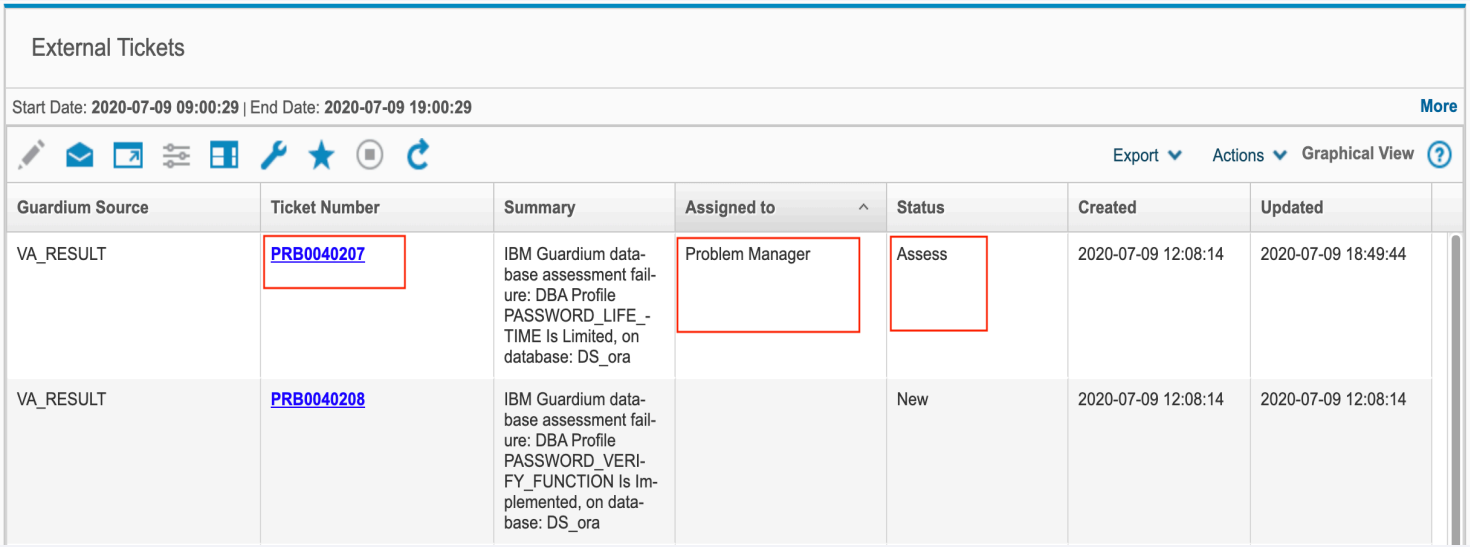
Updating tickets

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



Updating tickets

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



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

```
[redacted]> 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
```

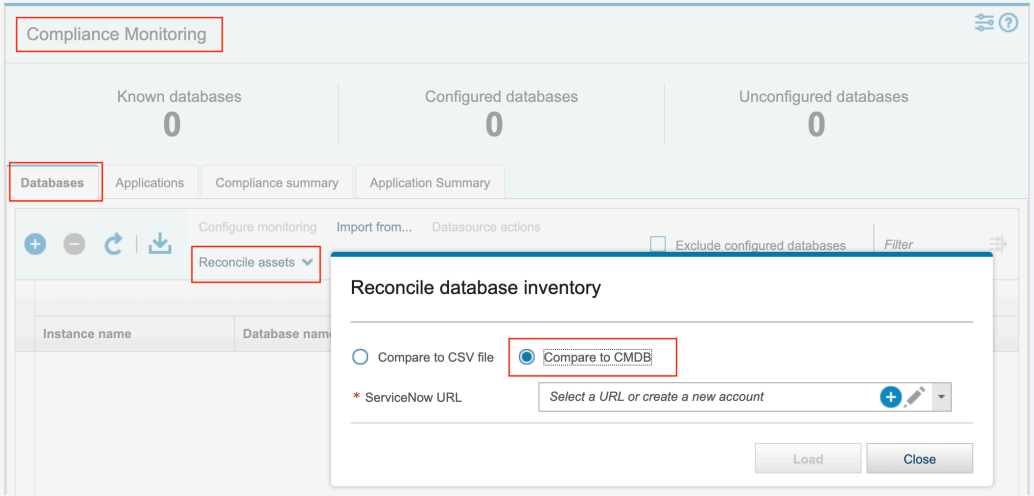
Purging tickets

- 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>

ServiceNow CMDB

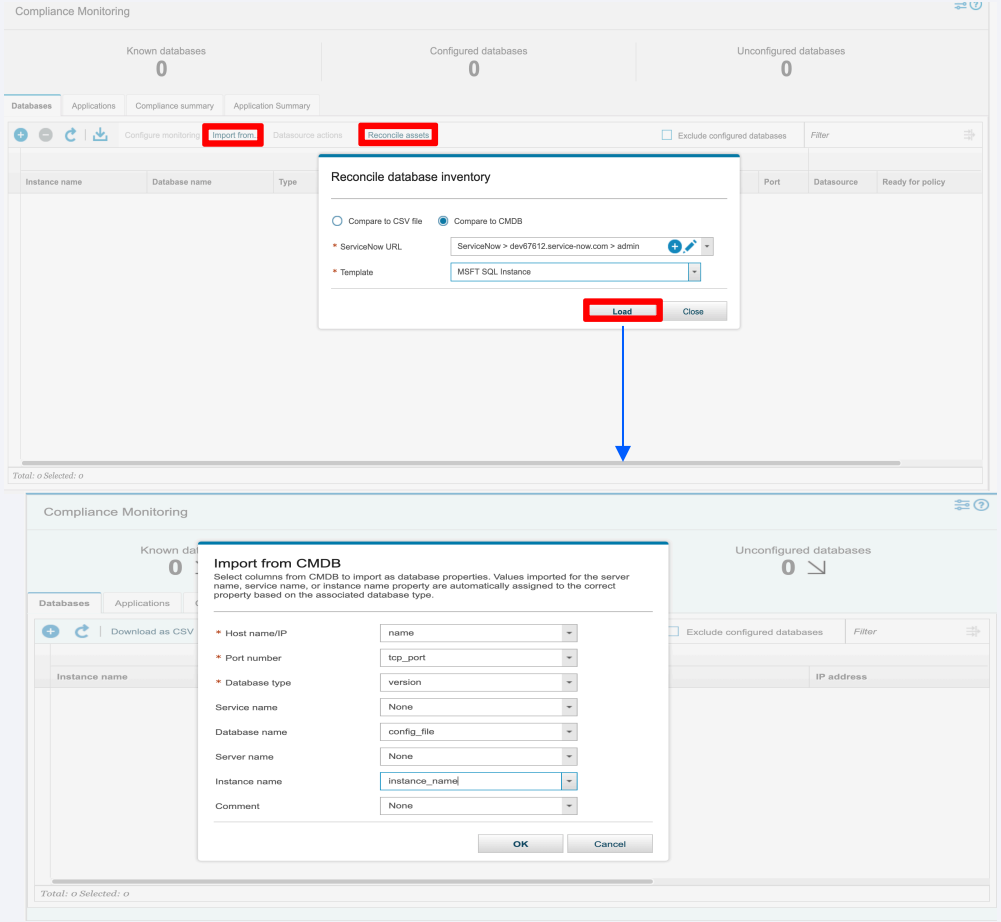
To reconcile database inventory between Guardium and ServiceNow:

- 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



Importing and reconciling CMDB assets

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



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

youtube/user/ibmsecuritysolutions