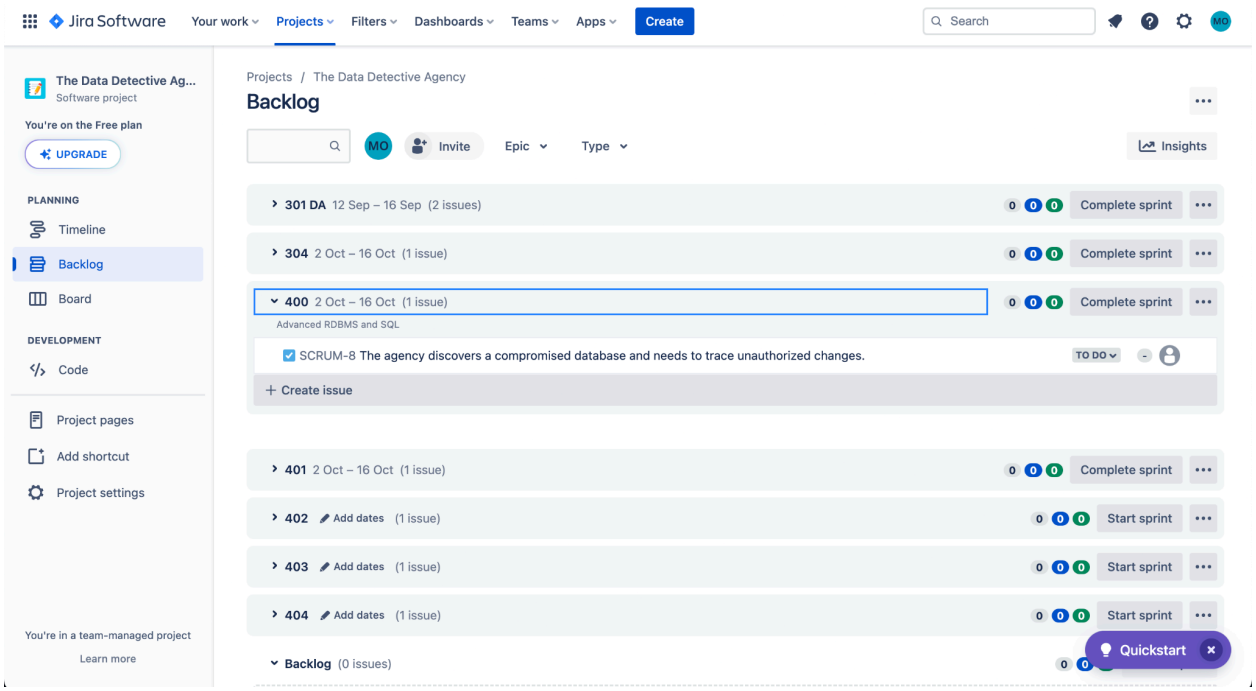
ACT 400 - The Data Detective Agency (continued)

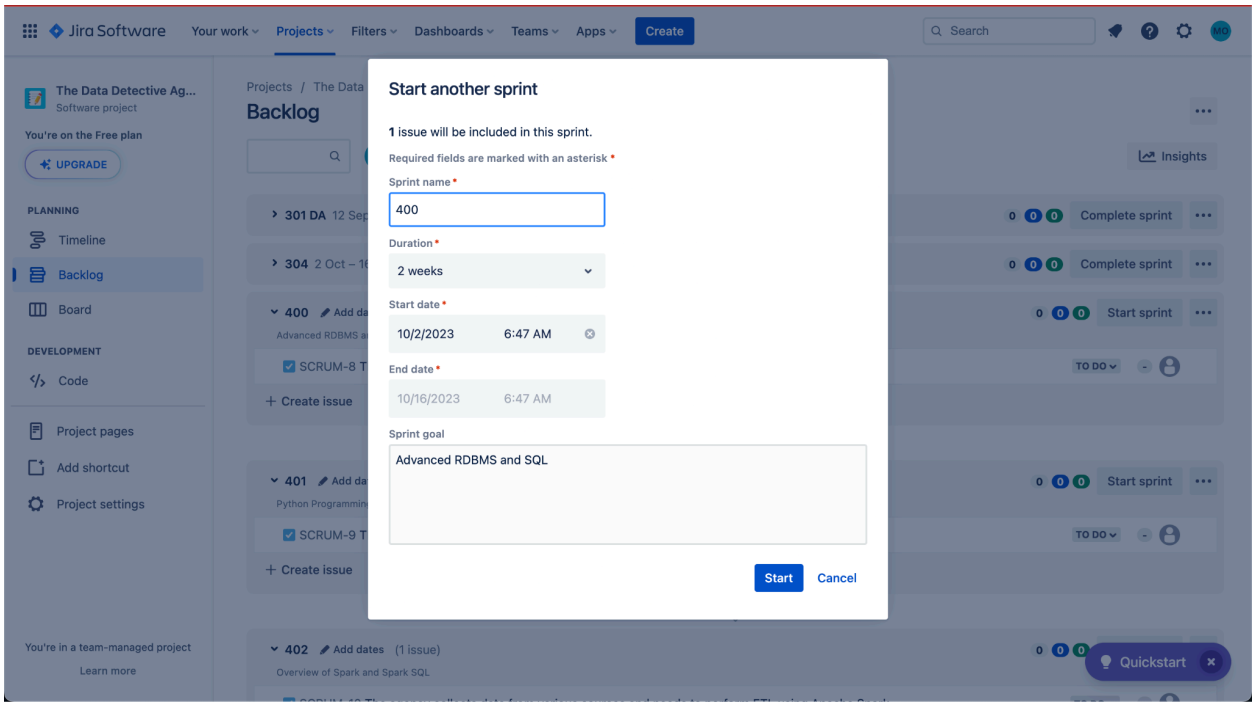
Version 1, 9/13/2023

Scenario and Instructions

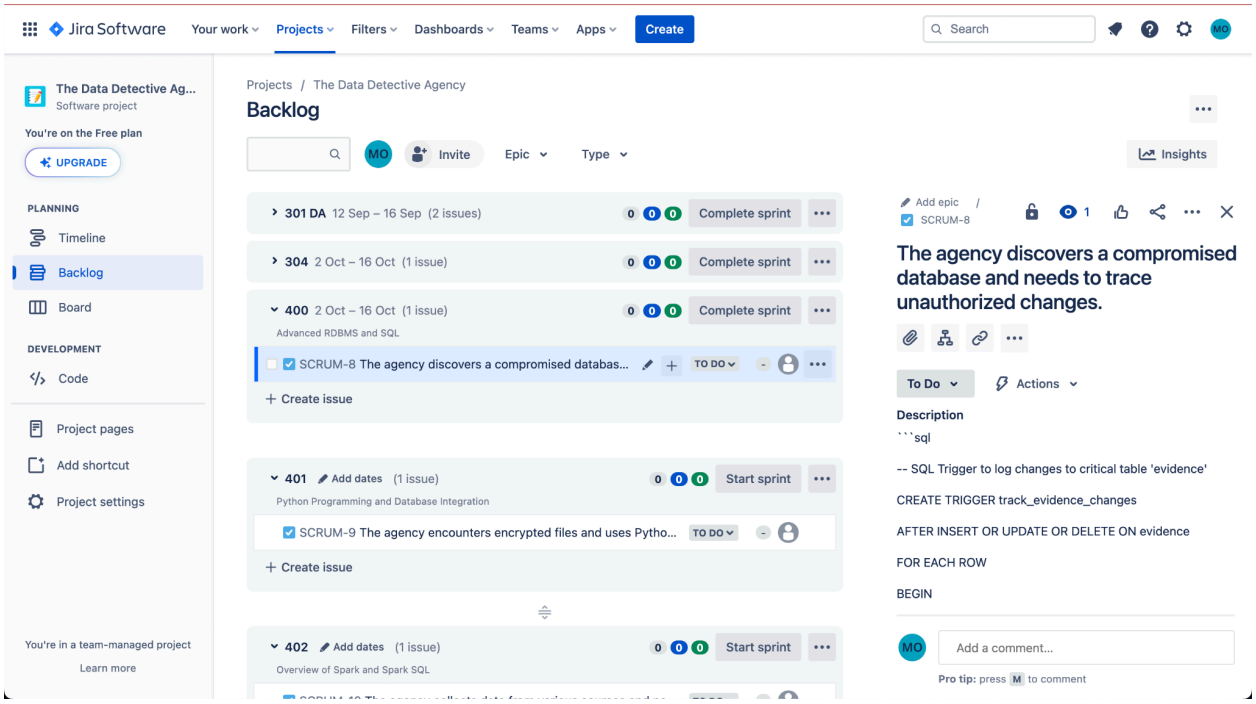
Step 1: In order to start the project, you should first sign up to the Jira.
Step 2: You should look for “The Data Detective Agency” project.
Step 3: After selecting the mentioned project, you will have to look under the “Planning” menu on the left sidebar, and select the “Backlog” tab. Go to Sprint 400 and click on the Start Sprint button.



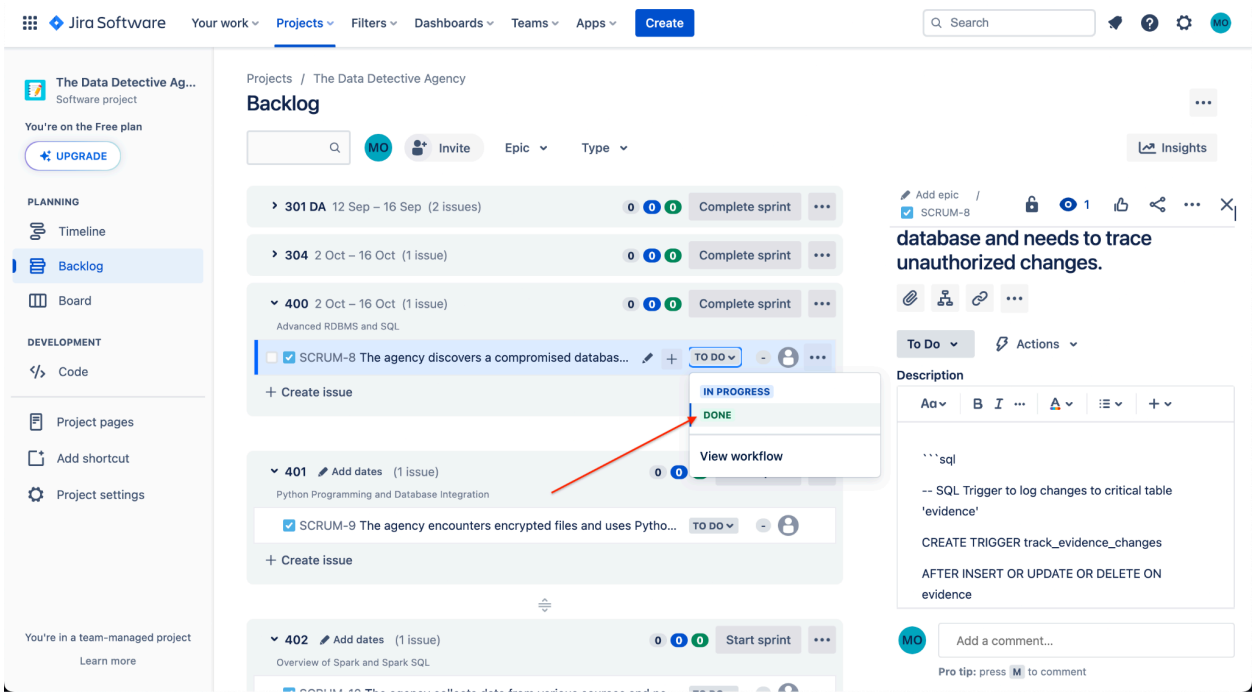
Step 4: Select the duration of the Sprint for each module, as mentioned in the course outline. Start the Sprint after selecting the duration.



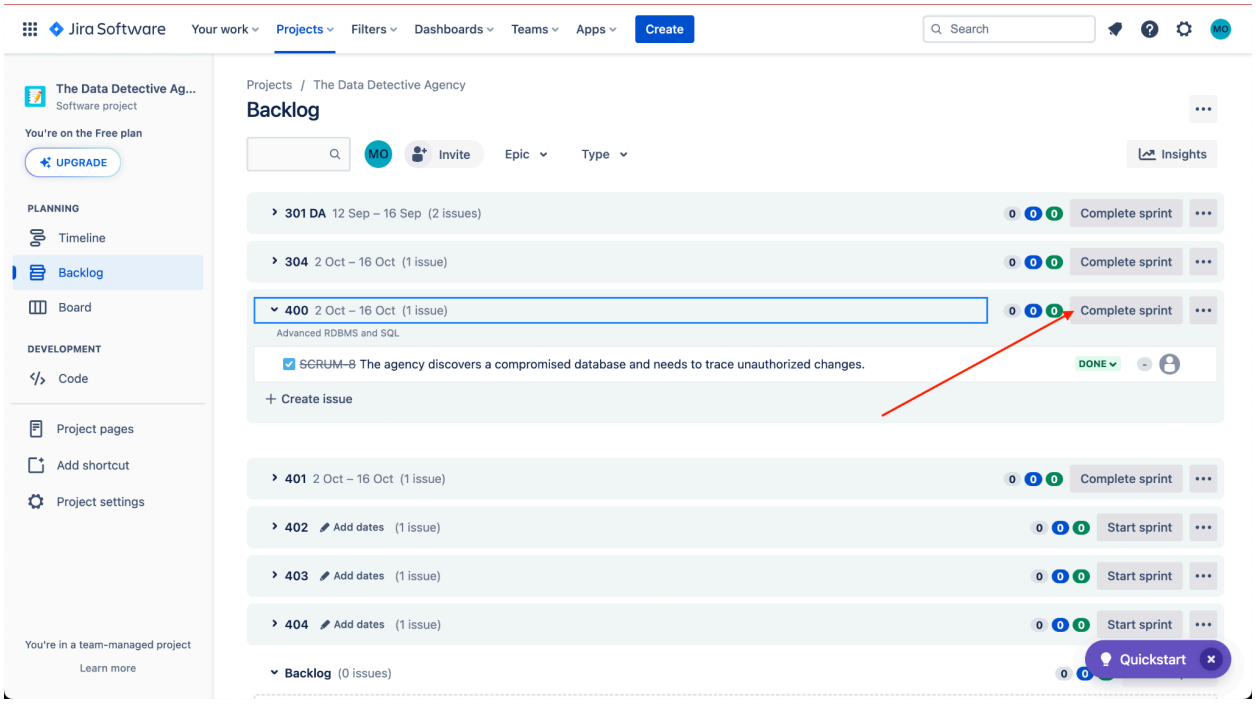
Step 5: Select the “SCRUM-8” under 400 Sprint to check the description. Now, execute the query to trigger the log changes to critical table 'evidence' as given in the description.

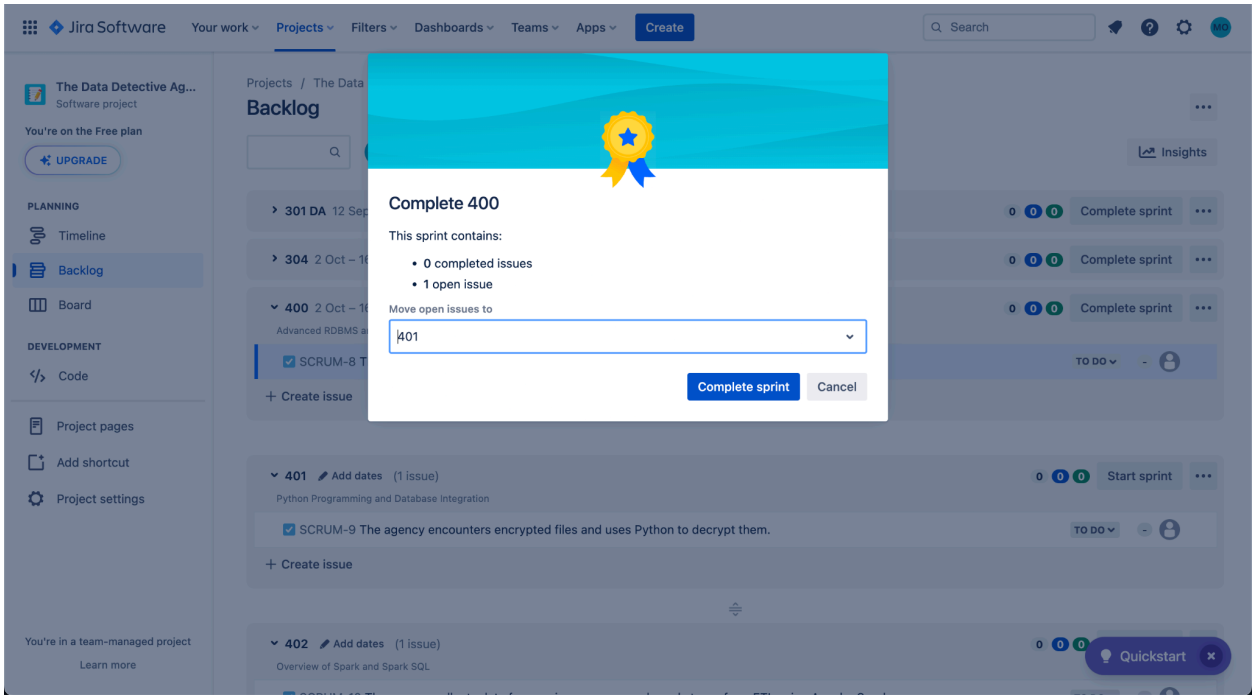


Step 6: After the task in Scrum 8 is completed, update the “To Do” and select the “Done” option as given in the picture below.



Step 7: After Scrum 8 is completed, click on the “Complete Sprint” button on Sprint 400, as shown below.


Jira Software
Your work
Projects
Filters
Dashboards
Teams
Apps
Create
Search
The Data Detective Ag...
Software project
You're on the Free plan
UPGRADE
PLANNING
Timeline
Backlog
Board
DEVELOPMENT
Code
Project pages
Add shortcut
Project settings
You're in a team-managed project
Learn more
Projects / The Data Detective Agency
Backlog
Invite
Epic
Type
Insights
301 DA 12 Sep – 16 Sep (2 issues)
304 2 Oct – 16 Oct (1 issue)
400 2 Oct – 16 Oct (1 issue)
Advanced RDBMS and SQL
SCRUM-8 The agency discovers a compromised database and needs to trace unauthorized changes.
DONE
Create issue
401 2 Oct – 16 Oct (1 issue)
402 Add dates (1 issue)
403 Add dates (1 issue)
404 Add dates (1 issue)
Backlog (0 issues)
Complete sprint
Start sprint
Quickstart


Jira Software
Your work
Projects
Filters
Dashboards
Teams
Apps
Create
Search
Backlog
Complete 400
This sprint contains:
0 completed issues
1 open issue
Move open issues to
401
Complete sprint
Cancel
401 Add dates (1 issue)
Python Programming and Database Integration
SCRUM-9 The agency encounters encrypted files and uses Python to decrypt them.
TO DO
Create issue
402 Add dates (1 issue)
Overview of Spark and Spark SQL
Quickstart

The agency discovers a compromised database and needs to trace unauthorized changes.

The task involves responding to a compromised database by implementing a trigger, track_evidence_changes. This trigger is designed to trace unauthorized changes, activating after each insert, update, or delete operation on the "evidence" table.

For each affected row, it logs details such as evidence ID, the action type ('INSERT'), and the timestamp of the change in the "evidence_changes" table. This measure aims to enhance the agency's ability to monitor and trace unauthorized modifications in the event of a security breach.

Step 1: You will be needing a data set to continue with scrum - 8. You can directly download the dataset and import it in your SQL workbench from the link below.
https://drive.google.com/file/d/1ztS_3eZYS1vf1de8pbpE8u-bSUHtxFXw/view?usp=drive_link

Step 2: You can also create the database named “cap_evidence” and use the SQL queries given below to create the tables and insert values in the tables.

Step 2.1: Create evidence table:

```
CREATE TABLE evidence (
    evidence_id INTEGER PRIMARY KEY,
    description TEXT
    -- Add other relevant columns as needed
);
```

Step 2.2: Create evidence_changes table:

```
CREATE TABLE evidence_changes (
    change_id INTEGER PRIMARY KEY AUTO_INCREMENT,
    evidence_id INTEGER,
    action VARCHAR(10),
    change_date TIMESTAMP,
    FOREIGN KEY (evidence_id) REFERENCES evidence (evidence_id)
);
```

Step 2.3: Insert dummy data into evidence table:

```
INSERT INTO evidence (evidence_id, description) VALUES
    (1, 'Document A'),
    (2, 'Photograph B'),
    (3, 'Audio Recording C');
```

Step 2.4: Insert an example change to trigger the track_evidence_changes trigger:

```
INSERT INTO evidence (evidence_id, description) VALUES
    (4, 'Video Footage D');
```

Step 3: Once the database is created or the SQL is imported you can execute the query that is included in the Scrum-8's description in the Jira. The code to be executed is:

```
DELIMITER //

CREATE TRIGGER track_evidence_changes
AFTER INSERT ON evidence
FOR EACH ROW
BEGIN
    INSERT INTO evidence_changes (evidence_id, action, change_date)
    VALUES (NEW.evidence_id, 'INSERT', NOW());
END;
//

-- Reset the delimiter
DELIMITER ;
```

Step 4: Capture the output and post it in the jira before closing out the sprint.