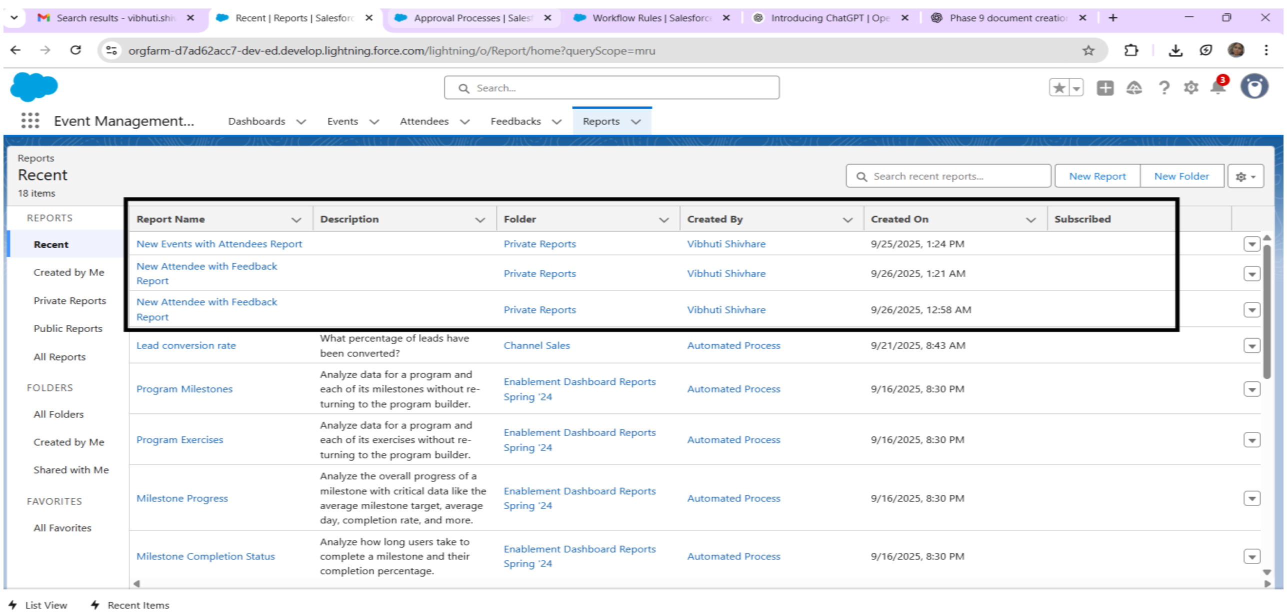
Phase 9 – Reporting, Dashboards

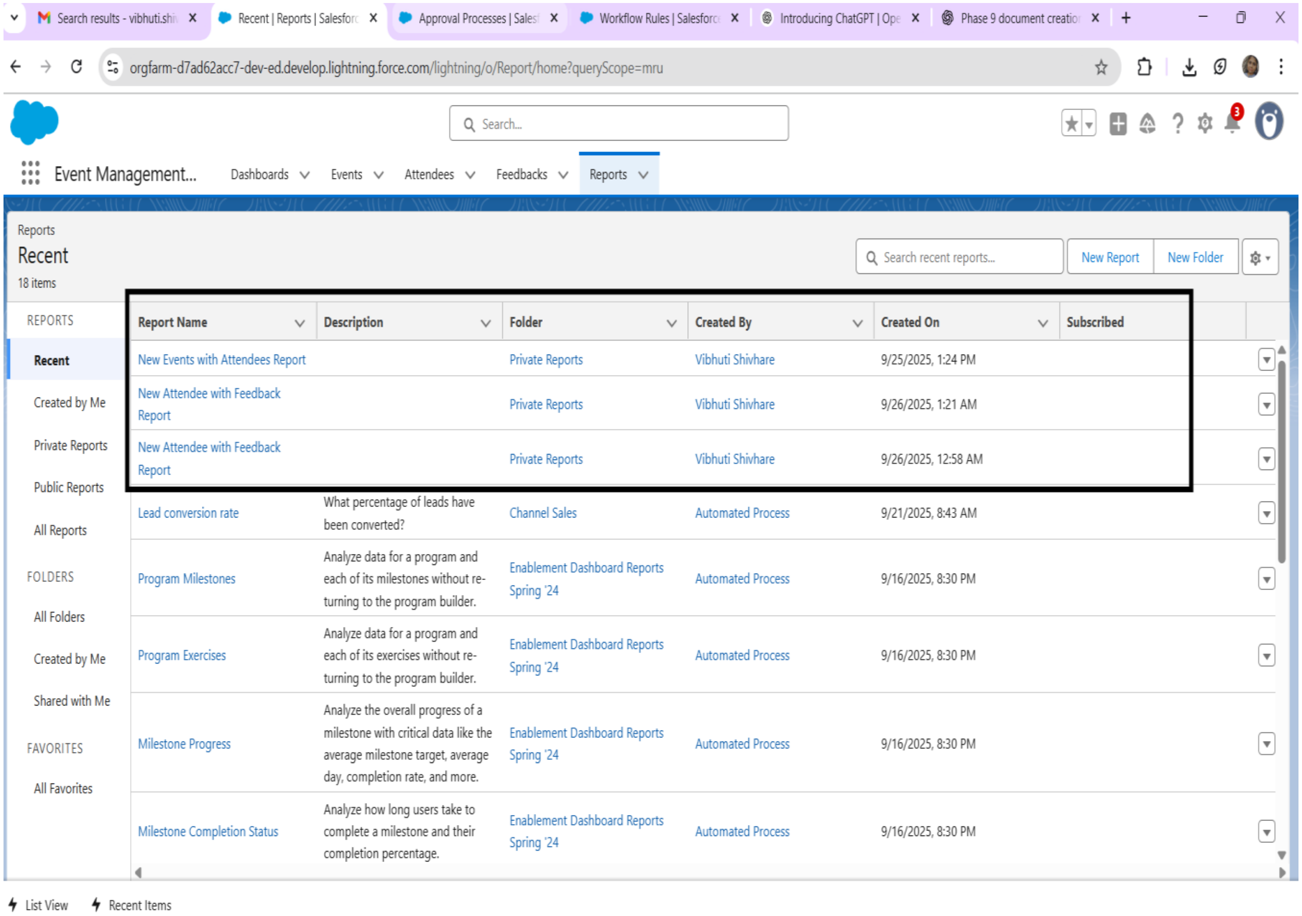
Step 1: Create a Report

- Go to App Launcher (grid icon) → Search "Reports".
- Click "New Report".
- Select the report type (example: Opportunities, Leads, or your custom object).
- Choose report format: Tabular, Summary, Matrix, or Joined.
- Add filters, fields, and grouping as needed.
- Save & Run the report.



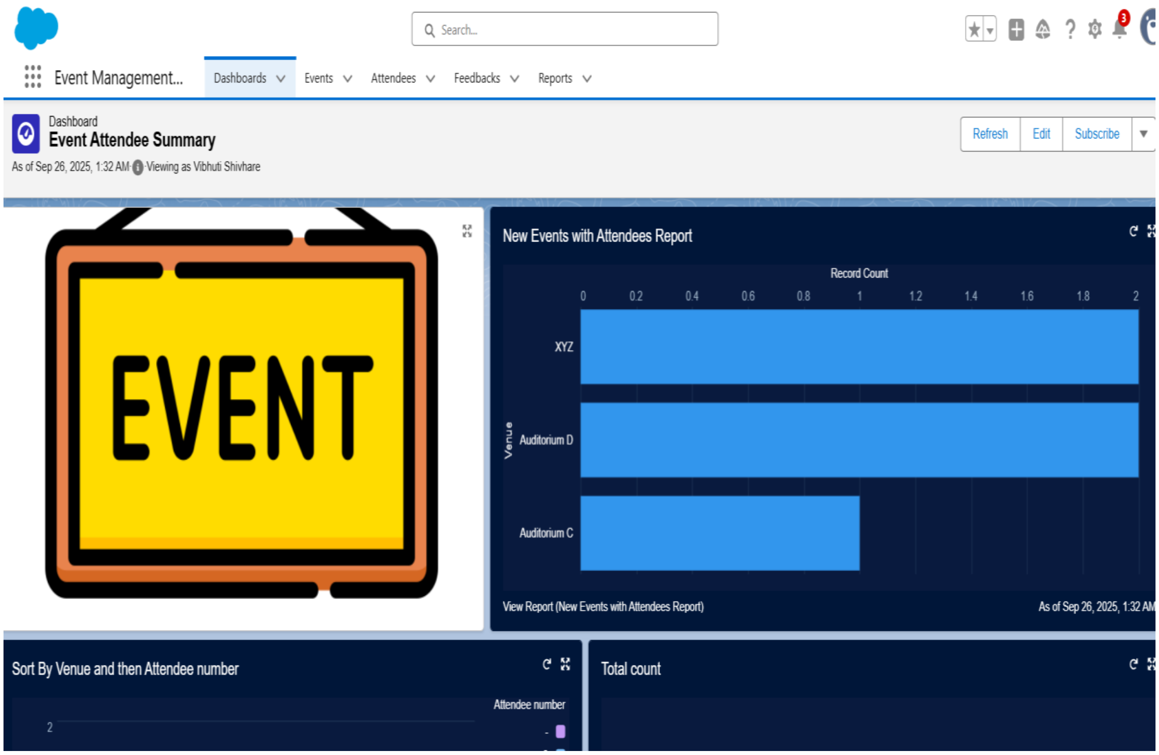
Step 2: Create a Custom Report Type (if needed)

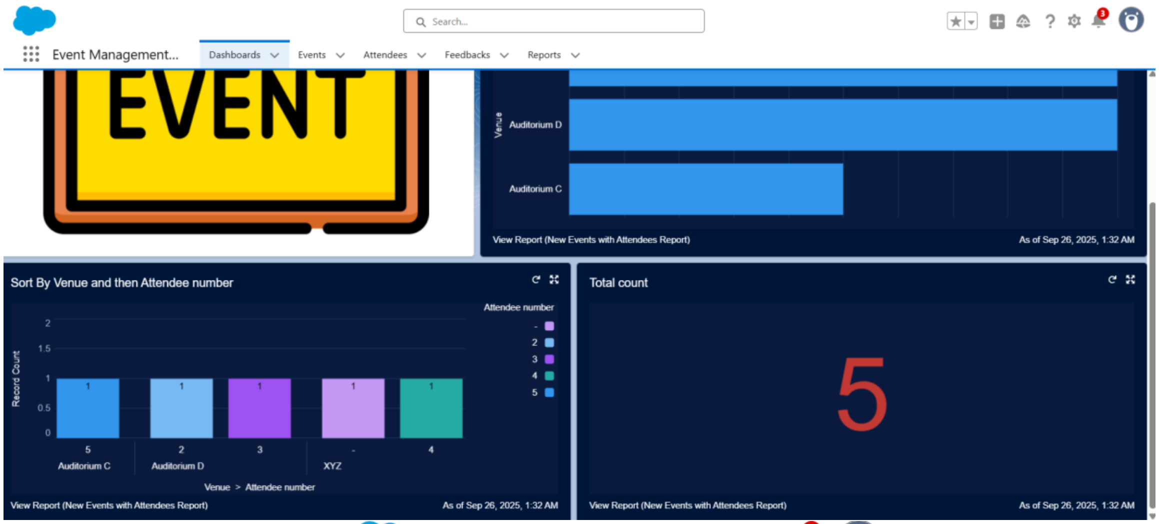
- Go to Setup → "Report Types" in Quick Find.
- Click "New Custom Report Type".
- Select the primary object.
- Define related objects and field relationships.
- Save and deploy.

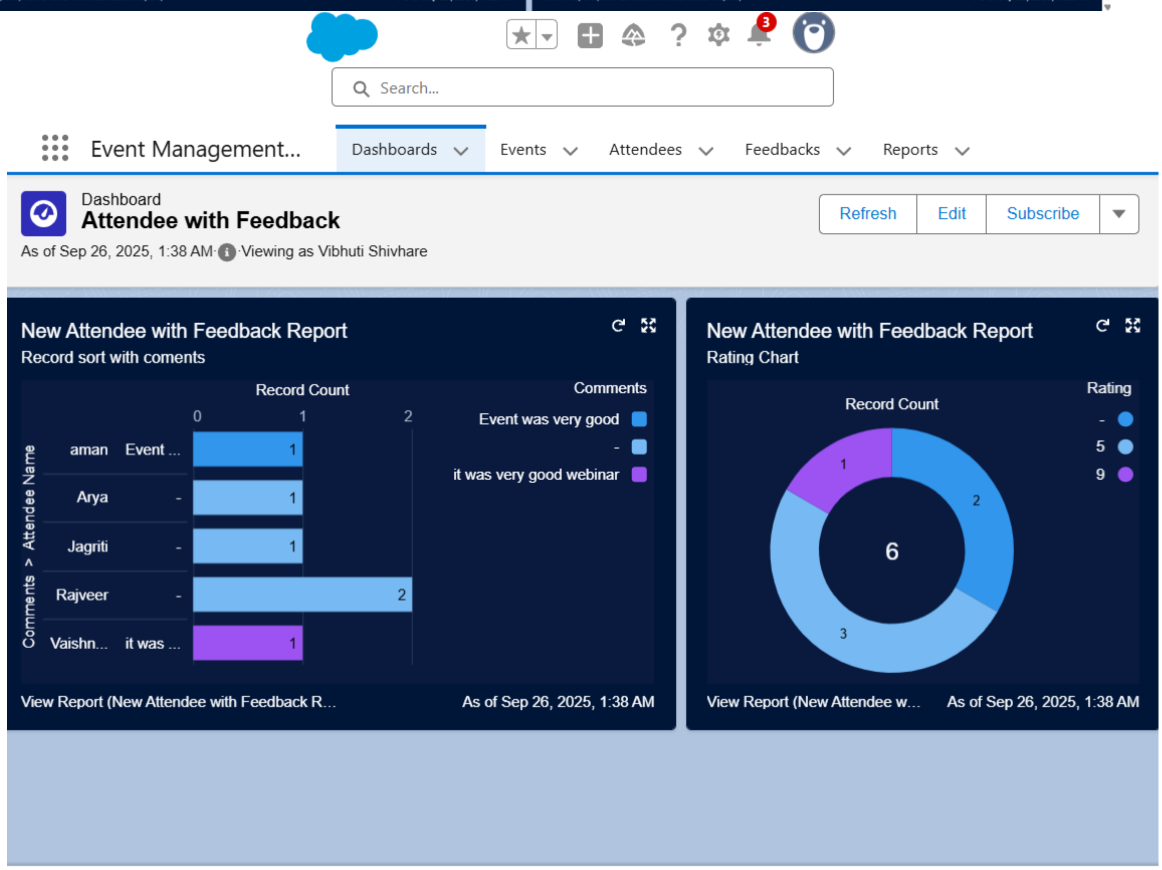
- 

Step 3: Create a Dashboard

- Go to App Launcher → Search “Dashboards”.
- Click “New Dashboard”.
- Enter Name, Folder, Description.
- Add a new component (Chart, Table, Metric, Gauge).
- Select the source report for each component.
- Adjust layout and size.
- Save and view dashboard.


Search...
Event Management...
Dashboards
Events
Attendees
Feedbacks
Reports
Dashboard
Event Attendee Summary
As of Sep 26, 2025, 1:32 AM · Viewing as Vibhuti Shivhare
Refresh
Edit
Subscribe
EVENT
New Events with Attendees Report
Record Count
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2
Venue
XYZ
Auditorium D
Auditorium C
View Report (New Events with Attendees Report)
As of Sep 26, 2025, 1:32 AM
Sort By Venue and then Attendee number
Attendee number
2
Total count





Step 4: Enable Dynamic Dashboards

- Open the dashboard you created.
- Click “Edit”.
- Under “View Dashboard As” select “Run as Logged-In User” (Dynamic) or choose a specific user (Static).
- Save.

Step 5: Configure Sharing Settings

- Go to Setup → "Sharing Settings".
- Set Organization-Wide Defaults (OWD) for each object.
- Configure Role Hierarchy (Setup → "Roles") to allow upward data access.
- Create Sharing Rules for wider access beyond OWD.
- Use Manual Sharing for individual records if needed.

Step 6: Apply Field-Level Security (FLS)

- Go to Setup → Object Manager → Select Object → Fields & Relationships.
- Click the field you want to secure.
- Click "Set Field-Level Security".
- Select which profiles/permission sets can see or edit the field.
- Save.

Step 7: Adjust Session Settings

- Go to Setup → "Session Settings".
- Set Session Timeout (e.g. 30 minutes).
- Enable/disable "Force Logout on Session Timeout".
- Save.

Step 8: Configure Login IP Ranges

- Go to Setup → "Profiles".
- Select the profile you want to secure.
- Scroll to "Login IP Ranges" → Click "New".
- Enter allowed IP ranges.
- Save.

Step 9: Review Audit Trail

- Go to Setup → "View Setup Audit Trail" in Quick Find.
- Review who made changes, what was changed, and when.
- Export if needed for compliance/security reviews.

Purpose of Phase 9

- Gain accurate insights with Reports and Dashboards.
- Provide role-based and user-based visibility with Dynamic Dashboards and Sharing Settings.
- Protect sensitive data with Field-Level Security and IP restrictions.

- Monitor configuration changes with Audit Trail.