Project Description: Reduced Power BI Data Security Risk

Table of Contents

Introduction

The Reduced Power BI Data Security Risk project addresses the challenge of synchronizing user access between Microsoft Entra (Azure Active Directory) and Salesforce for a Power BI dashboard, significantly enhancing data security and operational efficiency. By optimizing a Power Automate flow with advanced data operations, this solution reduces the synchronization time for over 10,000 users from 8 hours to just 15 minutes, ensuring that only authorized users, as defined in a specific Salesforce group, can access sensitive analytics data protected by Row-Level Security (RLS).

Project Overview

The Power BI dashboard leverages RLS, implemented using DAX, to restrict data access based on user roles. Access to the dashboard is controlled via an Azure AD security group, which must align with a corresponding user group in Salesforce CRM. Initially, a Power Automate flow using an "Apply to Each" action to compare user lists from Microsoft Entra and Salesforce took approximately 8 hours due to the high volume of users (over 10,000 in each list). This project introduces an optimized approach using Power Automate's data operations, drastically reducing runtime and improving the management of user additions and deletions across both platforms.

System Architecture

The solution integrates multiple components to achieve efficient user synchronization and secure data access:

Power BI Dashboard

- Employs RLS via DAX to enforce data-level security based on user roles.

Azure AD Security Group

- Controls access to the Power BI dashboard, with membership managed dynamically by the Power Automate flow.

Power Automate Flow

- Connects to Salesforce (via Salesforce connector) and Microsoft Entra (via Groups connector) to fetch user lists.
- Utilizes inbuilt data operations to process and compare large datasets efficiently.

Salesforce CRM

- Defines the authoritative user group that dictates dashboard access eligibility.

Optimized Workflow

The Power Automate flow follows an advanced process to synchronize user access:

Data Retrieval

- Fetches email IDs of users from the Azure AD security group and the Salesforce group using a single API call per connector.

Array Creation

- Constructs two arrays: one for Azure AD users and one for Salesforce users.

- Creates a third unique array for comparison, identifying differences between the two lists.

User Management

- Adds or removes users in the Azure AD security group based on the comparison.

- Identifies users to be added or removed in Salesforce for admin action.

Notification

- Sends an email to stakeholders with four lists: users added to Azure AD, users removed from Azure AD, users to be added to Salesforce, and users to be removed from Salesforce.

Data Logging

- Stores synchronization details in a SharePoint library for audit and reference purposes.

Key Features

The optimized flow introduces several critical enhancements:

Efficient Data Operations

- Replaces the slow "Apply to Each" action with array-based comparisons, minimizing API calls and processing time.

Bidirectional Synchronization

- Manages user updates not only for Azure AD but also identifies necessary changes in Salesforce, ensuring consistency across platforms.

Real-Time User Management

- Automates additions and deletions in the Azure AD security group, maintaining alignment with Salesforce group membership.

Stakeholder Communication

- Provides detailed email notifications to facilitate Salesforce admin actions and keep stakeholders informed.

Performance Improvements

The shift to data operations yields significant efficiency gains:

- Runtime Reduction: Cuts synchronization time from approximately 8 hours to just 15 minutes for over 10,000 users.

- Reduced API Load: Limits traffic to one API call per connector, avoiding the overhead of iterative requests in the original approach.

Security Benefits

This project strengthens Power BI data security by:

- Ensuring Authorized Access: Guarantees that only users currently defined in the Salesforce group can access the dashboard, enforced via the Azure AD security group.

- Minimizing Exposure Risk: Rapid synchronization reduces the window during which discrepancies between systems could allow unauthorized access.

Conclusion

The Reduced Power BI Data Security Risk project demonstrates the power of optimization in enhancing both security and performance. By leveraging Power Automate's advanced data operations, the solution slashes synchronization time from 8 hours to 15 minutes, ensuring that access to sensitive analytics data remains tightly controlled and aligned with Salesforce group membership. This improvement not only mitigates data security risks but also streamlines administrative processes, delivering a scalable and efficient framework for managing large-scale user access.