UNİVERSİTET ◦ UNIVERSITY
ADA

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

CSCI6917: Guided Research Methods

Summer 2023

Stephen H. Kaisler, D.Sc. (GWU)
Jamaladdin Hasanov, Ph.D. (ADA)

Data Privacy and Security in Database System

Student: Gunay Maharramli

8 August 2023

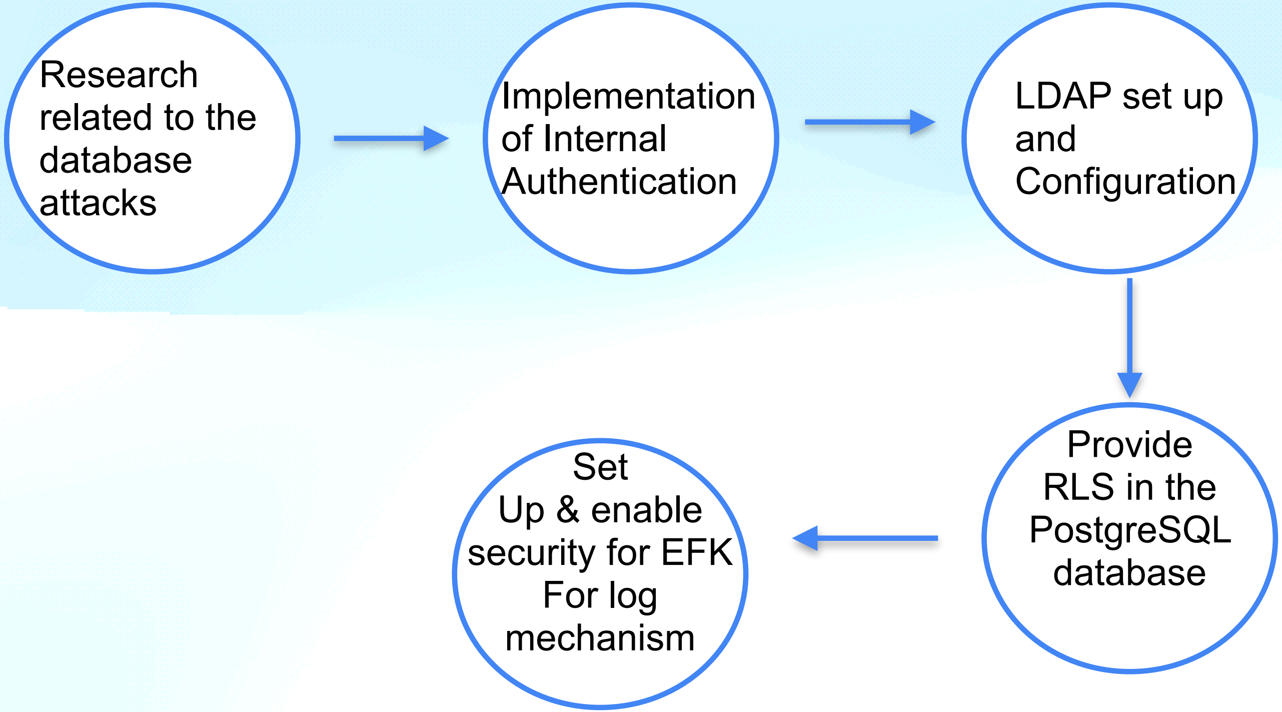
Heilmeier Questions

What are you going to do?	The aim of researching data privacy and security in database systems is to address the pressing concerns and challenges surrounding the protection of sensitive information in the digital age.
How is it done today? Current Limitations?	Access controls, encryption, and regular security audits Limitations persist, such as the potential for insider threats, evolving cybersecurity threats, and the challenge of balancing privacy with data usability.
What is new in your approach and why do you think it will be successful?	Implementing LDAP authentication can bolster data privacy and security in database systems by providing centralized user authentication and access control management. By leveraging LDAP, organizations can streamline user management, enforce strong password policies, and enable secure authentication across multiple systems.
Who will benefit from your work? Why?	The work on data privacy and security in database systems benefits a wide range of stakeholders. Organizations gain protection against data breaches and regulatory penalties, ensuring business continuity and customer trust.Database administrators (DBAs) can also reap several benefits from the work on data privacy and security in database systems
How long will it take?	2 months

Project Objectives

- Implement Authorization Mechanisms - Develop and integrate strong authentication methods
- Deploy Lightweight Directory Access Protocol (LDAP) or Active Directory: Integrate and configure the chosen directory service
- Establish Auditing and Monitoring Mechanisms: Implement auditing and monitoring features within the database system to track and log all user activities and access attempts, enabling real-time detection of suspicious or unauthorized actions and ensuring compliance with security policies.
- Regularly Review Logs and Reports: Conduct periodic reviews of audit logs and monitoring reports to analyze patterns

Key Steps



Research related to the database attacks

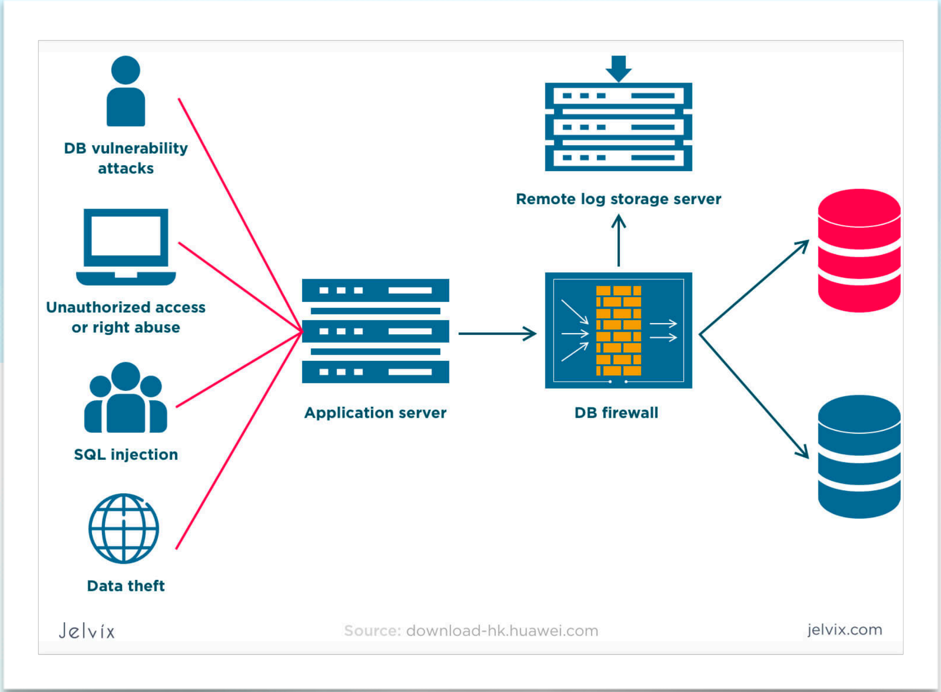
Implementation of Internal Authentication

LDAP set up and Configuration

Provide RLS in the PostgreSQL database

Set Up & enable security for EFK For log mechanism

Technical Approach

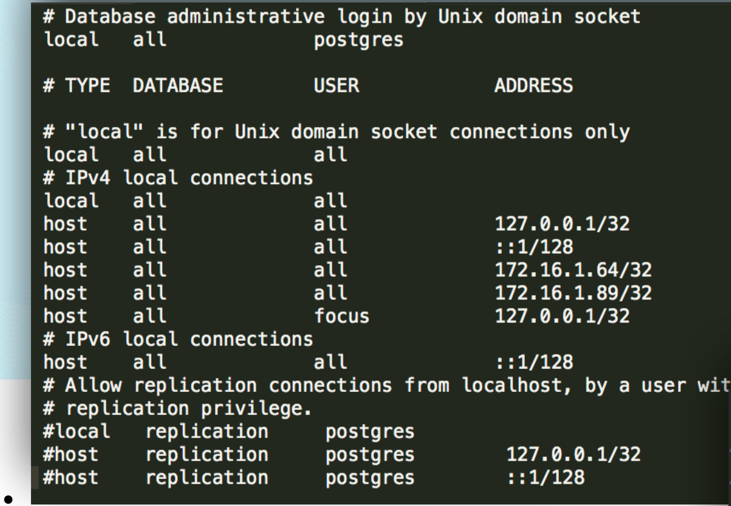


Source: download-hk.huawei.com

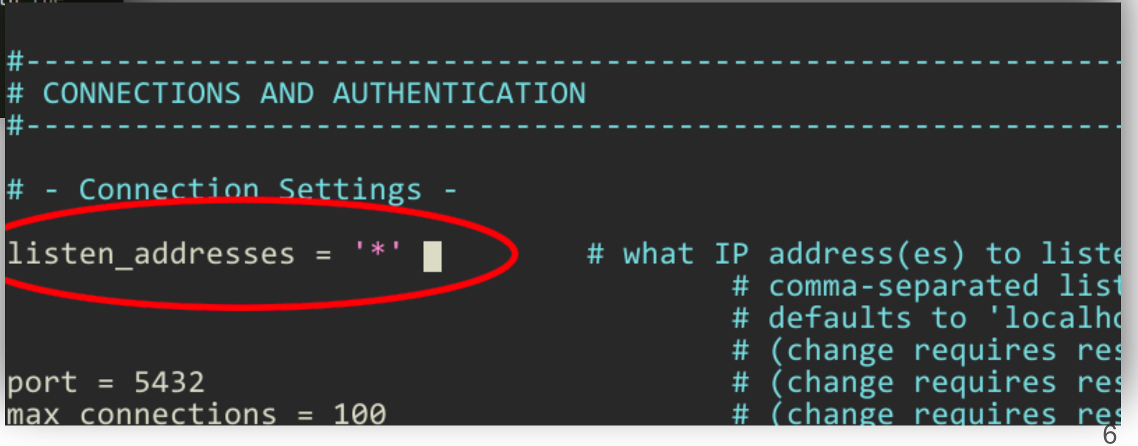
Attacks based on Confidentiality of Data and Privacy of Data

- Injection Attacks
- Concrete Attacks
- Snapshot Leaks
- Full System Compromise
- Identification Attacks

Technical Approach Internal Authentication - PostgreSQL

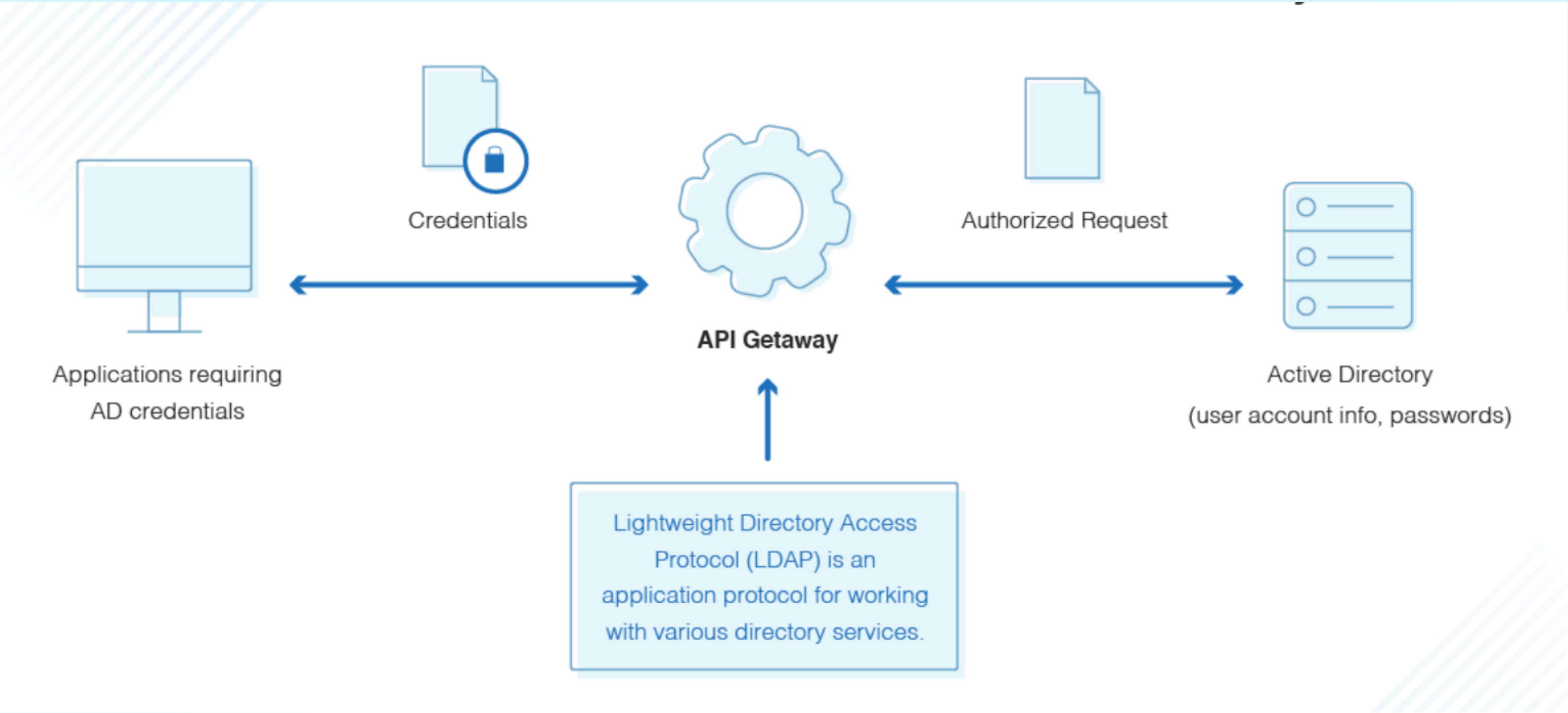


```
# Database administrative login by Unix domain socket
local   all             postgres                                peer

# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections
local   all             all                                     trust
host    all             all             127.0.0.1/32            trust
host    all             all             ::1/128                 trust
host    all             all             172.16.1.64/32          md5
host    all             all             172.16.1.89/32          md5
host    all             focus           127.0.0.1/32            trust
# IPv6 local connections
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
#local   replication     postgres
#host    replication     postgres        127.0.0.1/32
#host    replication     postgres        ::1/128
```



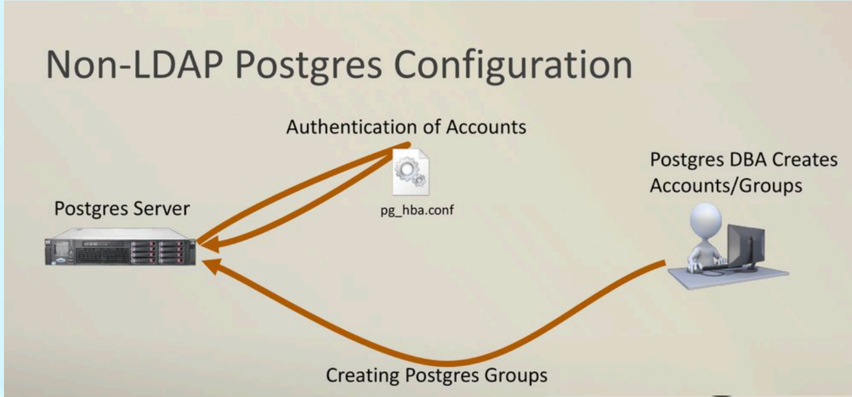
```
#------------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------

# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to liste
                                        # comma-separated list
                                        # defaults to 'localho
                                        # (change requires res
port = 5432                             # (change requires res
max_connections = 100                   # (change requires res
```

Technical Approach - LDAP


Credentials
Authorized Request
Applications requiring AD credentials
API Getaway
Active Directory
(user account info, passwords)

Lightweight Directory Access Protocol (LDAP) is an application protocol for working with various directory services.

LDAP - Difference



Non-LDAP Postgres Configuration

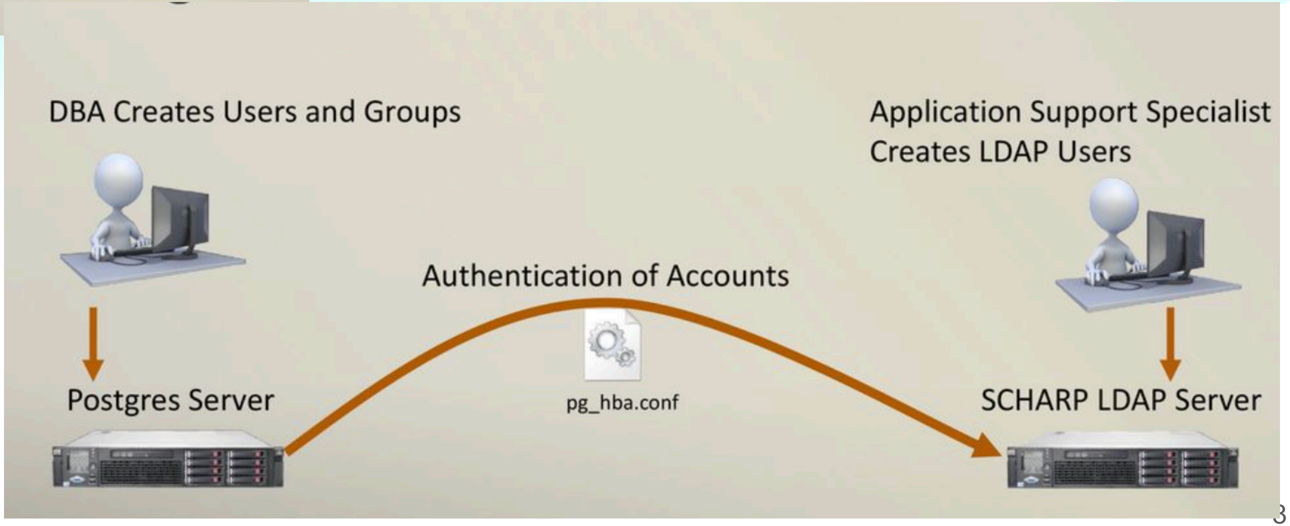
Postgres Server

Authentication of Accounts

pg_hba.conf

Postgres DBA Creates Accounts/Groups

Creating Postgres Groups



DBA Creates Users and Groups

Application Support Specialist Creates LDAP Users

Authentication of Accounts

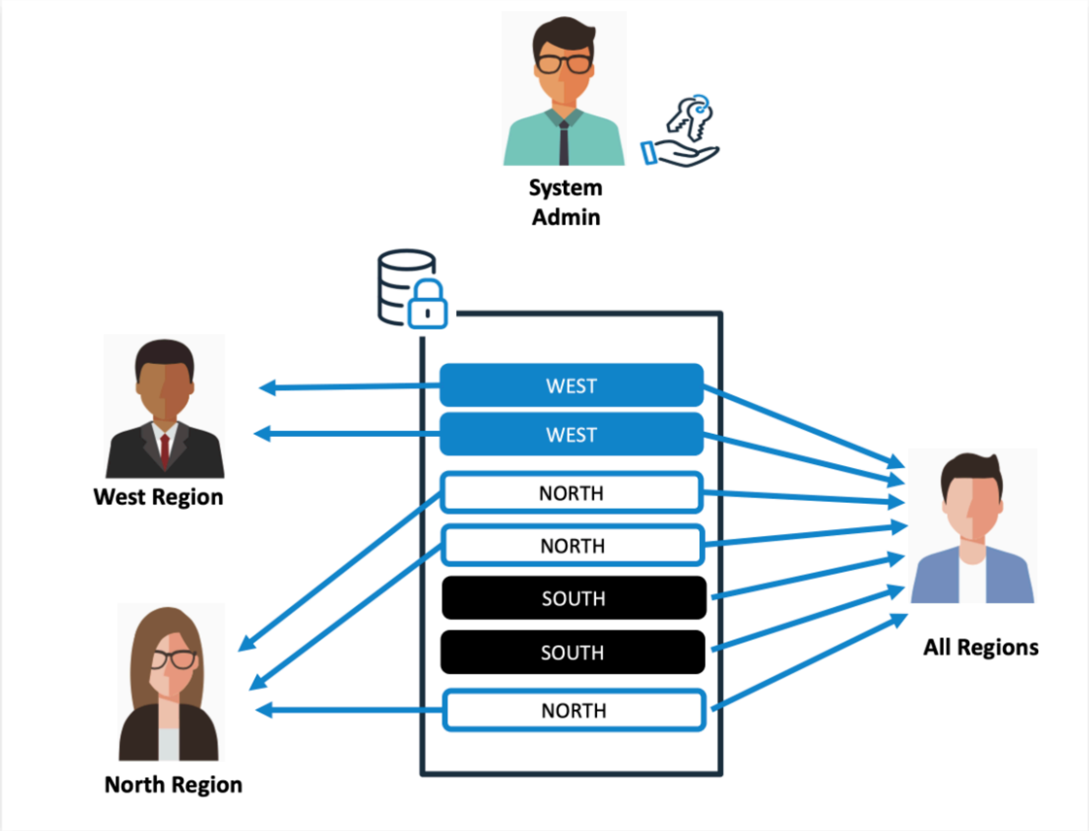
Postgres Server

pg_hba.conf

SCHARP LDAP Server

ROW Level Security

RLS is a technology available in Postgres that allows you to define policies that limit the visibility of rows in a table to certain roles.



Technical Approach - Auditing and Monitoring Mechanisms

1. Authentication and Access Control Auditing: Process of identifying the information of who accessed which systems and what components, including when and how.

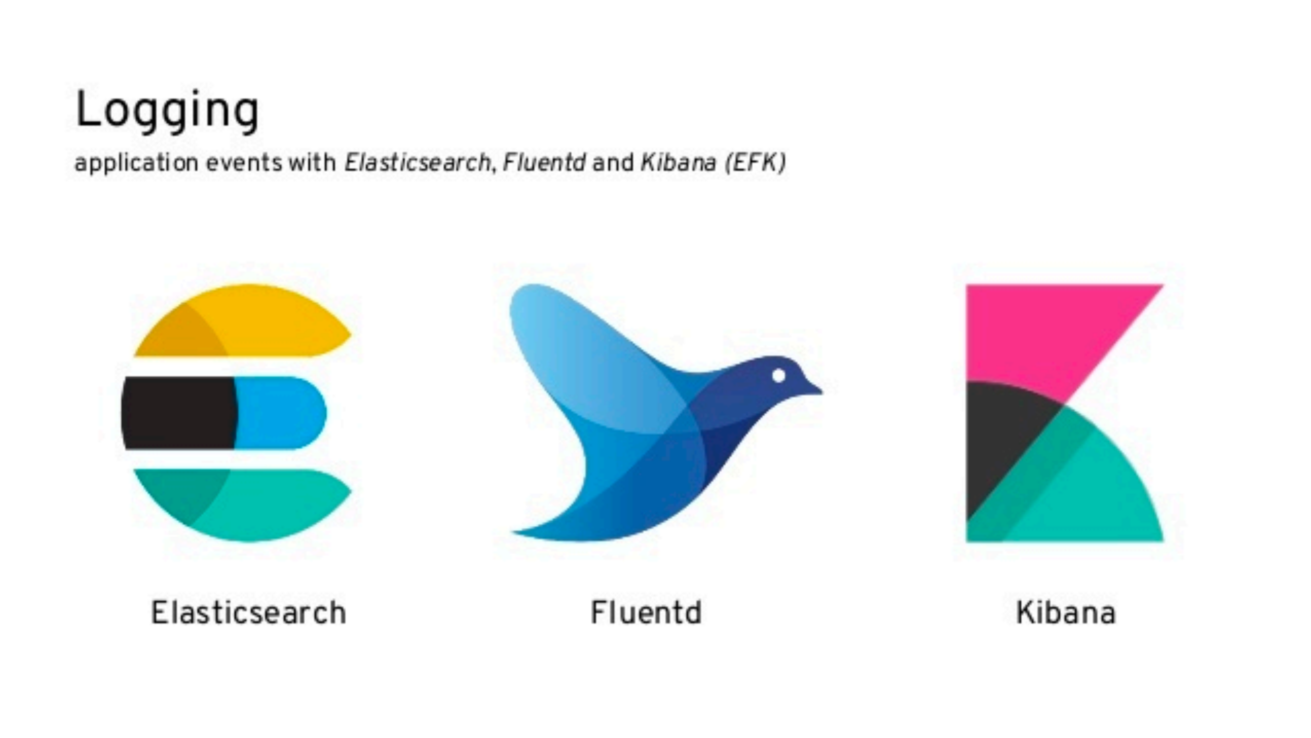
2. Subject/user Auditing: Process of identifying what activities (e.g., insert, update, delete etc.) have been performed by the users/administrators of the database system.

3. Security Activity Monitoring: Process of identifying and flagging any suspicious, abnormal or unusual activity/ access to sensitive data.

4. Vulnerability and Threat Auditing: Process of identifying the vulnerabilities in the database and monitor for users attempting to exploit them.

5. Change Auditing: Implementing baseline policy for different database objects, configurations, schemas, users and privileges and then track deviations from that baseline.

EFK configuration for logs



Logging

application events with *Elasticsearch*, *Fluentd* and *Kibana (EFK)*

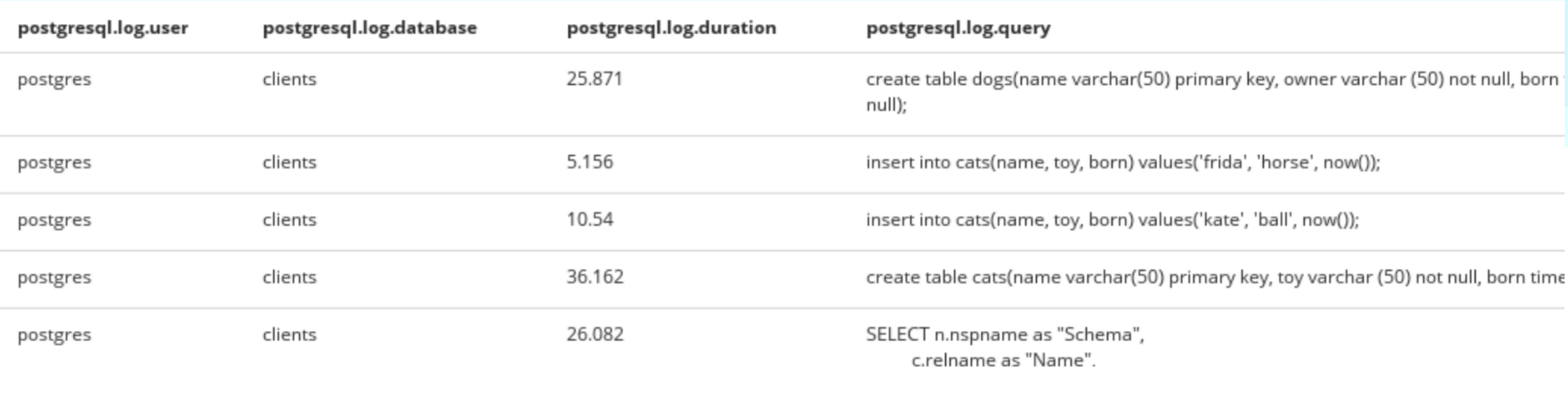
Elasticsearch

Fluentd

Kibana

-

Example logs



postgresql.log.user	postgresql.log.database	postgresql.log.duration	postgresql.log.query
postgres	clients	25.871	create table dogs(name varchar(50) primary key, owner varchar (50) not null, born null);
postgres	clients	5.156	insert into cats(name, toy, born) values('frida', 'horse', now());
postgres	clients	10.54	insert into cats(name, toy, born) values('kate', 'ball', now());
postgres	clients	36.162	create table cats(name varchar(50) primary key, toy varchar (50) not null, born time
postgres	clients	26.082	SELECT n.nspname as "Schema", c.relname as "Name".

Results

- Authorization mechanisms are functioning correctly, ensuring secure access control
- The security of the LDAP setup is validated against best practices and industry standards
- User access is restricted based on their roles, groups, or specific conditions defined in the security policies.
- EFK stack has been successfully installed and configured for log aggregation and analysis.

Conclusion

The implementation of LDAP authentication, row-level security, auditing, and monitoring in the database system ensures robust data privacy and security. LDAP authentication guarantees that only authorized users can access the database, while row-level security restricts access to sensitive information. Auditing and monitoring provide real-time insights and traceability, allowing proactive detection and response to potential security threats.

Future Work

- Configure alert rules and anomaly detection in Elasticsearch to swiftly detect and respond to security incidents and potential threats
- Set Up Kafka and Kafka Connect between Elasticsearch and Server
- Test other third party tools

Thank you for Attention!

Backup