Audit per sistemin PER

1. Auditi i Kuadrit Ligjor dhe Rregullator

Kontroll i kufizimeve të aksesit dhe kushteve për përditësimin e bazës së të dhënave.

1. Listim i të gjithë përdoruesve të bazës së të dhënave dhe të drejtat e tyre.

- ss-user: super user – Të gjitha privilegjet
- app-user: select, insert, update, execute procedurë
- replicator: userepl
- wow: read only
- monitor: read only
- Audit user: read only

2. Autentikimi i sistemit me databazen(connection string)

- Authentikimi realizohet me user environment variable
- [redacted]
- user: [redacted]
- Aksesin mbi kete user e ka Folio backend support team.

2. Auditimi i Arkitekturës së Sistemit dhe Bazës së të Dhënave

Shqyrtim i strukturës së bazës te të dhënave për të siguruar që të dhënat e votuesve të jenë të ndara dhe të mbrojtura.

1. Aksesi që kanë users në tabelën ku ruhen imazhet e skanuara apo të upload te dokumenteve

- ss-user: super user - Te gjitha privilegjet
- app-user: select, insert, update
- replicator: read only
- monitor: read only
- Audit: read only

2. Formati i ruajtjes në databazë të imazheve dhe algoritmi i enkriptimit.

- Formati i ruajtjes së imazheve PDF, WEBP, JPEG
- Algoritmi i enkriptimit: EC or RSA

3. Cfare Database Auditing Action types janë bëre enabled për të monitoruar këto të dhëna
- Aktualisht, auditimi i bazes së të dhënave në nivel serveri nuk është i zbatuar.

4. Procedurat e Backup
- Daily backup i te dhenave kryhet çdo dite ne oren 11:00 PM dhe ruhet ne serveret e bazes se te dhenave. Gjithashtu, eshte zbatuar replikimin i transmetimit PostgreSQL, i cili siguron disponueshmeri te larte sipas nje skeme aktive-pasive.

5. Testimi i restore i backup-it
- Po, per konfigurimin e procesit te PostgreSQL Streaming Replication, ishte e nevojshme te merrej nje kopje rezerve e bazes se te dhenave kryesore dhe te rikthehej ne bazen e te dhenave replike, gje qe na lejoi te verifikonim efektivitetin e kopjeve rezerve gjate ketij procesi. Eshte e rendesishme te theksohet se me konfigurimin e PostgreSQL Streaming Replication kemi dy servere—nje aktiv dhe nje rezerve—qe permbajne saktesisht te njejtat te dhena, pasi replikimi ndodh ne kohe reale.

6. Ku ruhet backup dhe a eshte i encriptuar
- Aktualisht, kopjet rezerve te bazes se te dhenave ruhen ne te njejtin server te bazes se te dhenave, me nje replike shtese ne nje server tjeter ne gjendje pritjeje. Eshte e rendesishme te theksohet se keto kopje rezerve nuk jane te enkriptuara. Nese kerkohet enkriptimi i kopjeve rezerve, ai duhet te zbatohet gjate nje periudhe te planifikuar mirembajtjeje.

3. Auditi i Procesit të Regjistrimit dhe Identifikimit të Votuesve

1. Procedurat e regjistrimit te votuesve

- Procedurat e regjistrimit të votuesve janë në përpushshmeri me kërkesat e dakordesuar mes palëve.

4. Krahasimi i Imazheve të Ruajtura në Sistem

1. Funksionaliteti që po përdoret për face recognition dhe rezolucioni i të dhënave që ruhen
   - Të dhënat nuk ruhen, ato perdoren vetem per perpunim dhe dergohen ne bazen lokale te te dhenave (ku ruhen me nje rezolucion prej 800x800). Perdoren motore te ndryshem per krahasimin e fytyrave, ku AWS Recognition eshte kryesori
2. Limiti i poshtem per te bere skanimin e fytyres se qytetarit(Minimumi i MP te front camera sa duhet te jene)
   - Nuk ka minimum, por rekomandohet Full HD me fokus automatik.

5. Siguria e Aksesit në Sistemin dhe Baza e të Dhënave

1. Loji i algoritmit te enkriptimit per imazhet që ruhet ne databazen lokale.

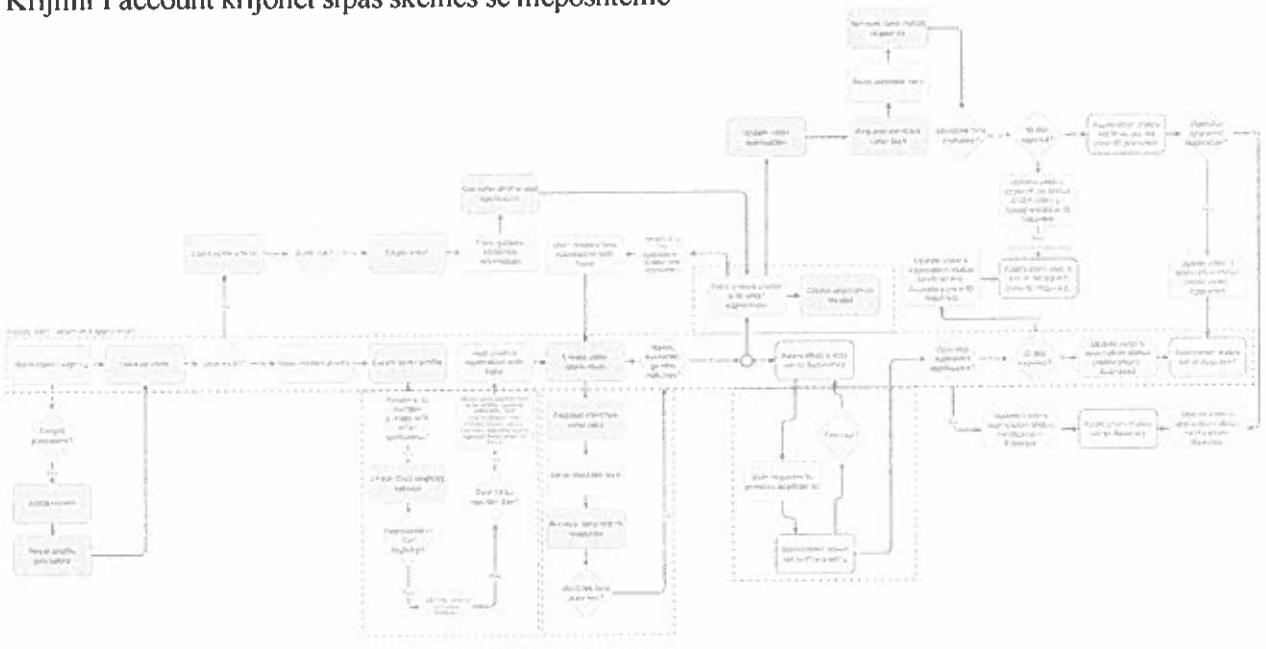
- Imazhet ruhen ne sistemin e skedareve. Paketa e plote eshte e enkriptuar me EC ose RSA, por imazhet nuk jane te enkriptuara.

2. Audit action types

- Aktualisht, auditimi i bazes se te dhenave ne nivel serveri nuk eshte i zbatuar.

3. Procedura e autentikimit me dy faktorë (2FA) për administratën dhe votuesit.

- Krijimi I account krijohet sipas skemes se meposhteme



6. Roli i Operatorëve dhe Trajnimi i Stafit

1. Vleresimet per trajnimin e stafit përgjegjës për regjistrimin e votuesve dhe kredencialet qe disponojne.

- Operatoret kane trajnimin e nevojshem per te realizuar detyrat, nisur dhe nga procesimi i aplikimeve ne menyre te shpejte. Sa i perket perpunimit te te dhenave operatoret kane te drejta te limituara vetem per rolin e tyre.

7. Testimi i Integritetit të Sistemit

1. Tools monitorues per sulmet ndaj sistemit

- Nje sistem gjitheperfshires monitorimi per CPU, disk, RAM dhe SWAP eshte zbatuar duke perdorur agjentin e monitorimit Telegraf. Ky agjent mbledh dhe dergon te dhena ne kohe reale ne nje server Grafana, i cili lejon vizualizimin dhe analizen e te dhenave. Perveç kesaj, serveri Grafana eshte konfiguruar per te gjeneruar njoftime automatike ne rast se zbulohen alarme per burimet.

8. Verifikimi i Performancës së Sistemit

1. Rezultatet e performances se sistemit
    - Ne dokumentin attached do te gjeni rezultatet e performaces se sistemit te kryer nga kompania zhvilluese

PER-Service-API-perf
ormance-report-29.pt

9. Gjurmimi dhe Auditimi i Ndryshimeve në të Dhëna

1. Sistemi nuk ka audit action types të bëra enabled për këtë arsy nuk mund te trakohen ndryshimet ne audit logs.

10. Raportime dhe Sygjerime

Sygjerime per backup process

1. Full backup (ditor):
- Kap të gjithë gjendjen e bazës së të dhënave.
- Zakonisht bëhet çdo ditë për bazat e të dhënave të vogla dhe çdo javë për bazat e të dhënave të mëdha.
2. Diferencial backup (çdo 4 orë):

- Regjistron ndryshimet që nga rezervimi i fundit i plotë.
- Redukton kohën e rikuperimit në krahasim me përdorimin vetëm të regjistrave të transaksioneve.

3. Transaction Backup (çdo 15 minuta për disponueshmëri të lartë):
- Regjistron ndryshimet që nga rezervimi i fundit i regjistrit të transaksioneve.
- Kritike për bazat e të dhënave duke përdorur modelin e rikuperimit të plotë.

Sygjerim per ruajtjen e backup

1. Backup duhet te ruhet me një server tjetër i ndryshëm nga server i sistemit dhe të jetë i enkriptuar

Sygjerim per ruajtjen e imazheve sensitive

1. Imazhet duhet të ruhen të enkriptuara në bazën e të dhënave

Sygjerim lidhur me auditim te te dhenave

1. Sygjerohet te behen enable audit action types ne tabelat sensitive te sistemit. Me poshte do te listohen audit action types qe sygjerohen te behen enable

- ADD (INSERT, UPDATE, DELETE ON DATABASE)
- ADD (SCHEMA_OBJECT_CHANGE_GROUP)
- ADD (SELECT ON DATABASE)
- ADD (DATABASE_PERMISSION_CHANGE_GROUP)

Auditues

Ervin Bana

Performance Test Report - Dec 26, 2024 (#29)

Open in Postman

Postman collection: ERP Service API

Report exported on: Dec 26, 2024, 15:28:13 (GMT-3)

Test setup

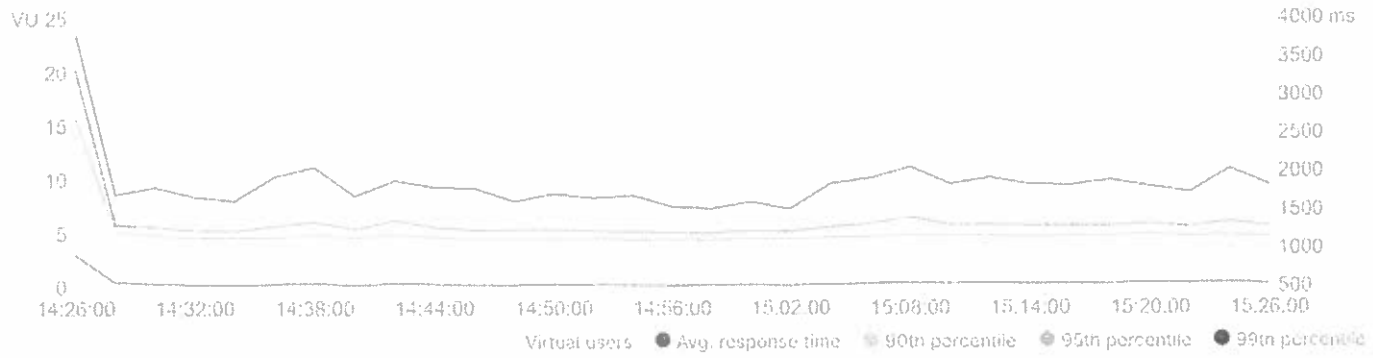
Virtual users	Start time	Load profile
25 VU	Dec 26, 14:27:26 (GMT-3)	Fixed
Duration	**End time**	**Environment**
60 minutes	Dec 26, 15:27:38 (GMT-3)	New Environment

1. Summary

Total requests sent	Throughput	Average response time	Error rate
112,124	31.04 requests/second	561 ms	4.25 %

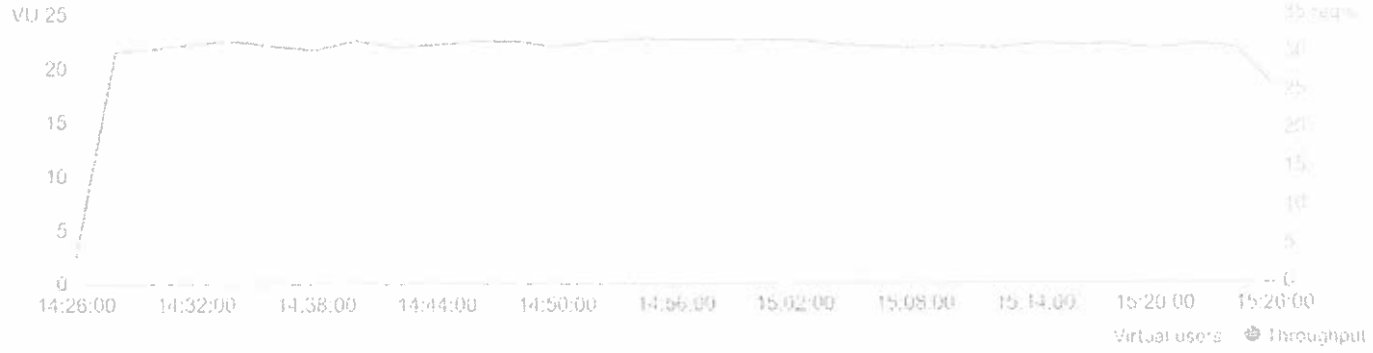
1.1 Response time

Response time trends during the test duration.



1.2 Throughput

Rate of requests sent per second during the test duration.



1.3 Requests with slowest response times

Top 5 slowest requests based on their average response times.

Request	Resp. time (Avg ms)	90th (ms)	95th (ms)	99th (ms)	Min (ms)	Max (ms)
POST Create voter profile Copy	1,154	1,297	1,465	2,017	970	20,777
[redacted]						
POST Create voter application Copy	976	1,400	1,650	2,561	234	11,310
[redacted]						
GET Get voter profile Copy	239	284	382	644	183	2,609
[redacted]						
POST Lookup voter Copy	218	246	287	639	177	1,911
[redacted]						
POST Login voter Copy	218	255	283	375	180	1,668
[redacted]						

1.4 Requests with most errors

Top 5 requests with the most errors, along with the most frequently occurring errors for each request.

Request	Total error count	Error 1	Error 2	Other errors
POST Create voter application Copy	4,765	403 Forbidden (4766)	-	0
[redacted]				

2. Metrics for each request

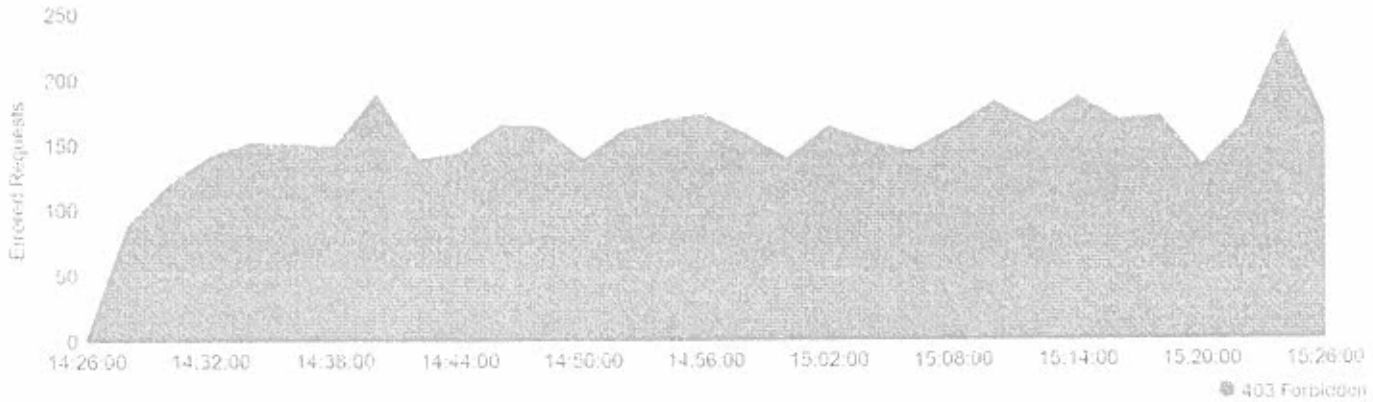
The requests are shown in the order they were sent by virtual users.

Request	Total requests	Requests/s	Min (ms)	Avg (ms)	90th (ms)	Max (ms)	Error %
POST Lookup voter Copy [redacted]	22,429	6.21	177	218	246	1,911	0
POST Create voter profile Copy [redacted]	22,428	6.21	970	1,154	1,297	20,777	0
POST Login voter Copy [redacted]	22,427	6.21	180	218	255	1,668	0
GET Get voter profile Copy [redacted]	22,425	6.21	183	239	284	2,609	0
POST Create voter application Copy [redacted]	22,415	6.21	234	976	1,400	11,310	21.26

3. Errors

3.1 Error distribution over time

Top 5 error classes observed during the test duration.



3.2 Error distribution for requests

Errored requests grouped by error class, along with the error count for each class.

Error class	Total counts
403 Forbidden	4766
POST Create voter application Copy	4,766

Testing API performance on Postman

Postman enables you to simulate user traffic and observe how your API behaves under load. It also helps you identify any issues or bottlenecks that affect performance.

Learn more about testing API performance.