AppStack

An Open Source Cloud Native Platform for Running Digital Public Services

Dimitris Mitropoulos, Alex Kiousis

dimitro@grnet.gr, alexkiousis@grnet.gr

National Infrastructures for Research and Technology

grnet

Roadmap

1. GRNET Scope
2. Operating digital public services: challenges
3. AppStack
4. Tackling problems with different OSS components
5. Experiences from production

GRNET – National Infrastructures for Research and Technology

the Greek National Research and Education Network (NREN) established in 1998.
A specialized Internet service provider dedicated to support the needs of the research and education communities within a country

Scope

GRNET provides:

- Internet connectivity
- cloud computing
- high-performance computing
- advanced services

to the Greek academic and research community and to agencies of the public sector

340 PoPs

10K km optical fiber

connecting >150
universities,
research centers,
and more

10Gbps per
organization

50 cities

thousands
of users

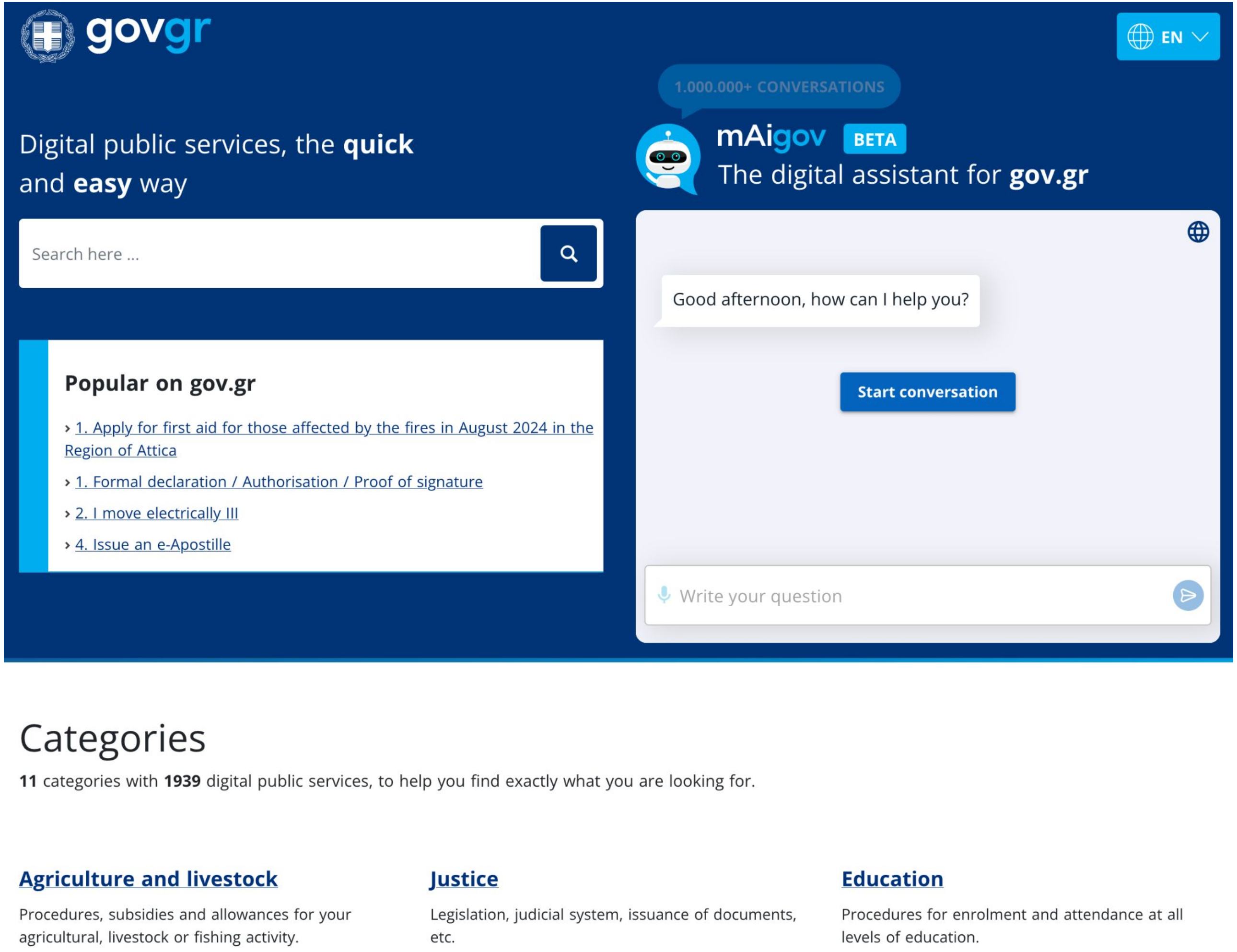
- 6 DCs
- >120 racks
- >2K servers
- >12K VMs

(up until 2019)

Copernicus BDR HARMONI Eudoxus Apella ~okeanos ~okeanos-global ~okeanos-knossos Diavlos Zeus Delos365 AcademicID HIDM ViMa Argo DNS Mail AaaS parltv Firewall-On-Demand Eduroam Phabricator Phabricator JIRA Piwik Wordpress Limesurvey Sympa Confluence Massmail TravelExpenses SecureNotes XMPP Chat Webdns4 Nextcloud OpenVPN LDAP FTP SnipeIT Netbox Syslog RADIUS Mon IDP Jenkins Puppet FAI Icinga Prometheus Elasticsearch Grafana Bacula PostgreSQL MariaDB Atlas GR-IX HPC-ARIS

gov.gr: portal and services

(summer ‘19)



Digital public services, the **quick** and **easy** way

The digital assistant for **gov.gr**

Good afternoon, how can I help you?

Popular on gov.gr

- 1. Apply for first aid for those affected by the fires in August 2024 in the Region of Attica
- 1. Formal declaration / Authorisation / Proof of signature
- 2. I move electrically III
- 4. Issue an e-Apostille

Categories

11 categories with **1939** digital public services, to help you find exactly what you are looking for.

Agriculture and livestock

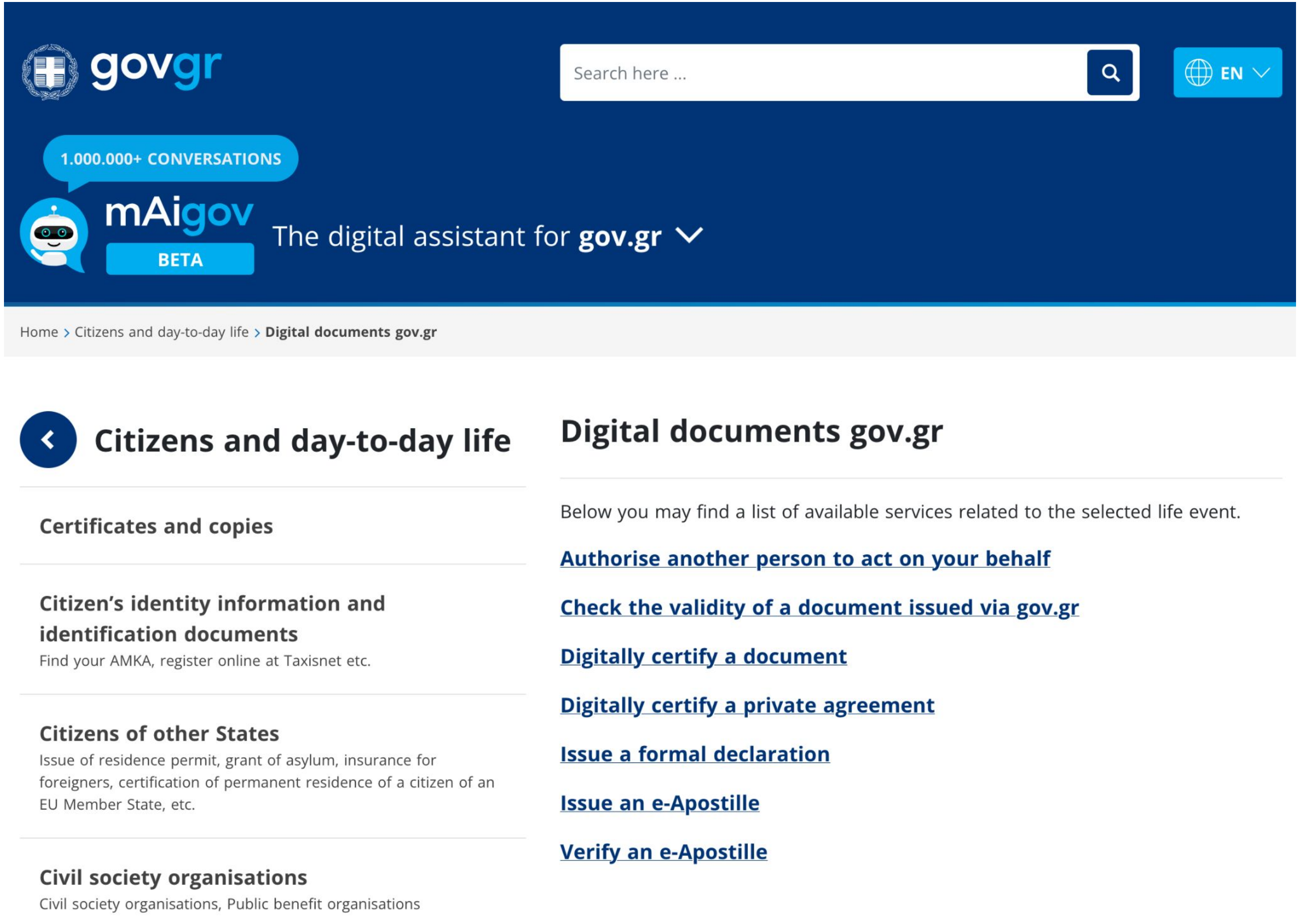
Procedures, subsidies and allowances for your agricultural, livestock or fishing activity.

Justice

Legislation, judicial system, issuance of documents, etc.

Education

Procedures for enrolment and attendance at all levels of education.


govgr
Search here ...
EN
1.000.000+ CONVERSATIONS
mAigov
BETA
The digital assistant for gov.gr
Home > Citizens and day-to-day life > Digital documents gov.gr

Citizens and day-to-day life

Certificates and copies

Citizen’s identity information and identification documents
Find your AMKA, register online at Taxisnet etc.

Citizens of other States
Issue of residence permit, grant of asylum, insurance for foreigners, certification of permanent residence of a citizen of an EU Member State, etc.

Civil society organisations
Civil society organisations, Public benefit organisations

Digital documents gov.gr

Below you may find a list of available services related to the selected life event.

Authorise another person to act on your behalf

Check the validity of a document issued via gov.gr

Digitally certify a document

Digitally certify a private agreement

Issue a formal declaration

Issue an e-Apostille

Verify an e-Apostille

challenges?

faster development and deployment cycles

scalability and resiliency

security

public perception and reputation

AppStack

a unified computing environment for gov.gr services

currently hosting:
dilosi, gov.gr, edupass, DGC, EIDAS, firstreg, gov wallet, auth, vouchers and more

Goals

Embrace new technologies:

- Containers
- CI/CD
- Self-service tools

Gain:

- Faster, hands-free deployments
- Proper service overview
- Fast scaling of resources

Decisions - I

Define an internal platform that the SRE team runs and developers and service operators can use to efficiently run services

Invest in a self-hosted Kubernetes setup as the basis for all service workloads

Decisions - II

Trust open source tools and our own experience to compose an agile and configurable solution for our needs

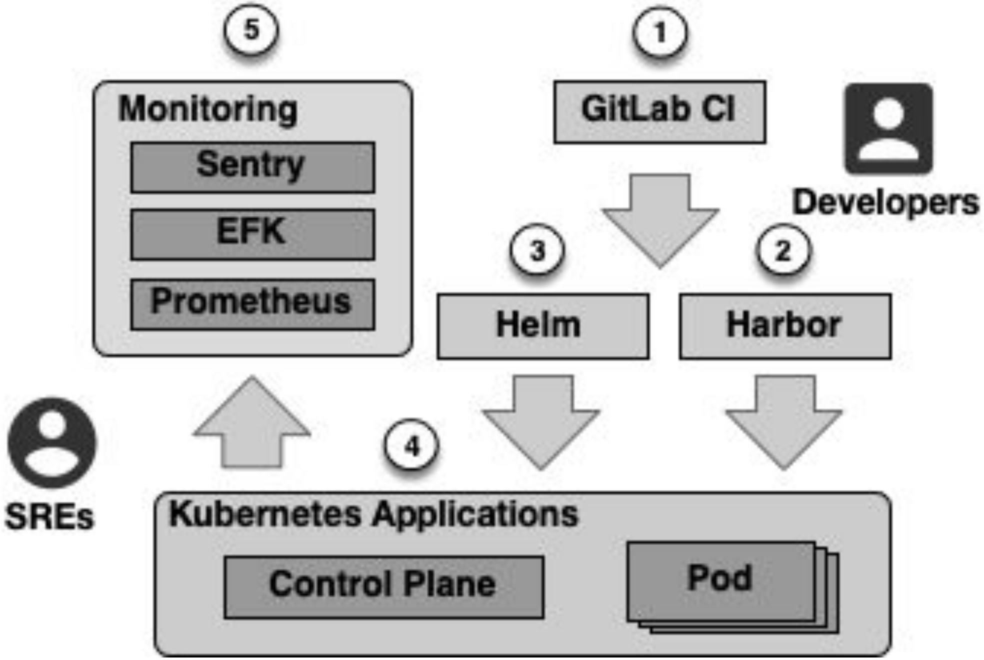
Decisions - III

Keep using what worked already (VM infrastructure, Puppet, backups,)

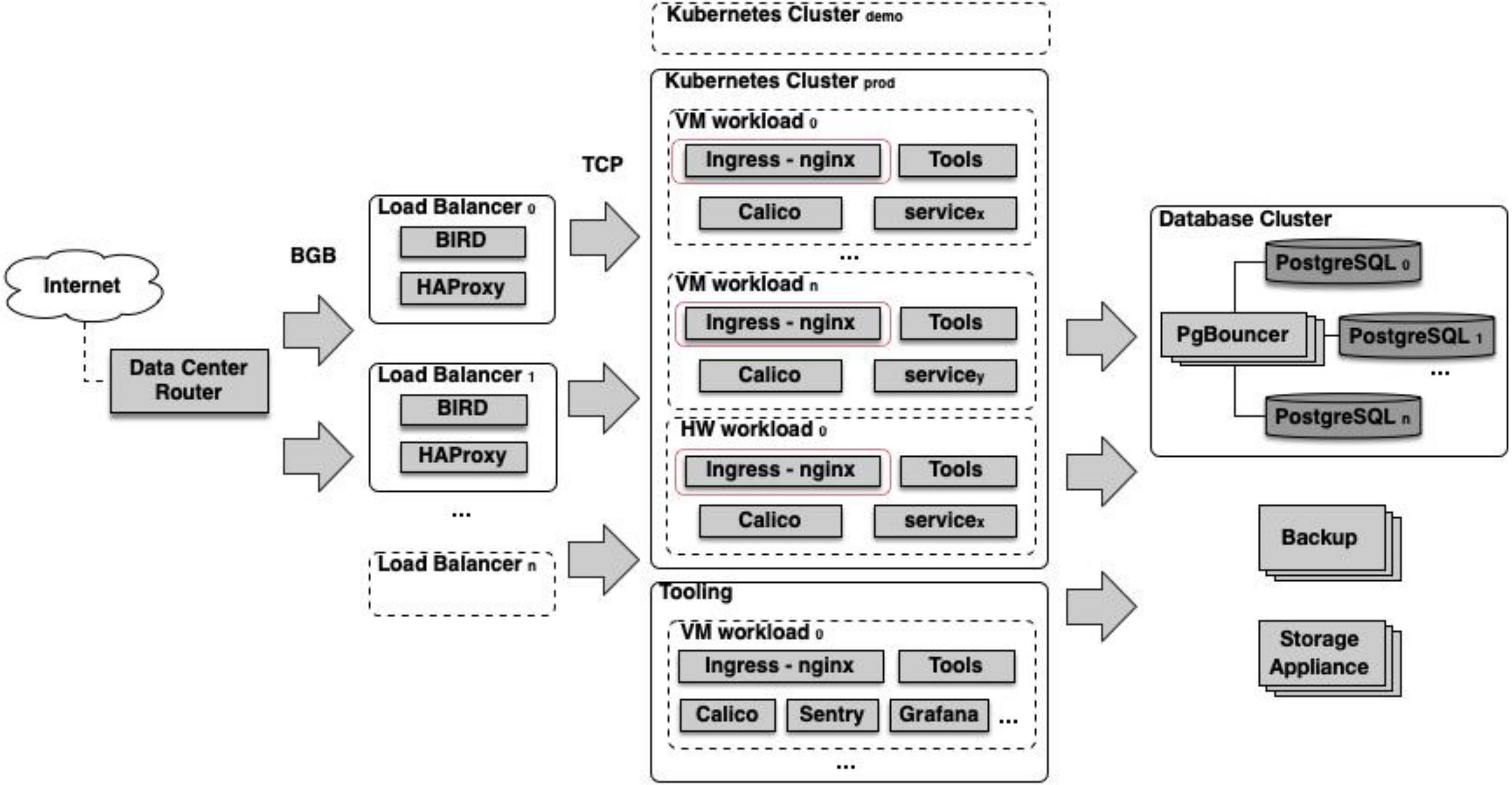
Keep databases and other stafefull components outside of Kubernetes

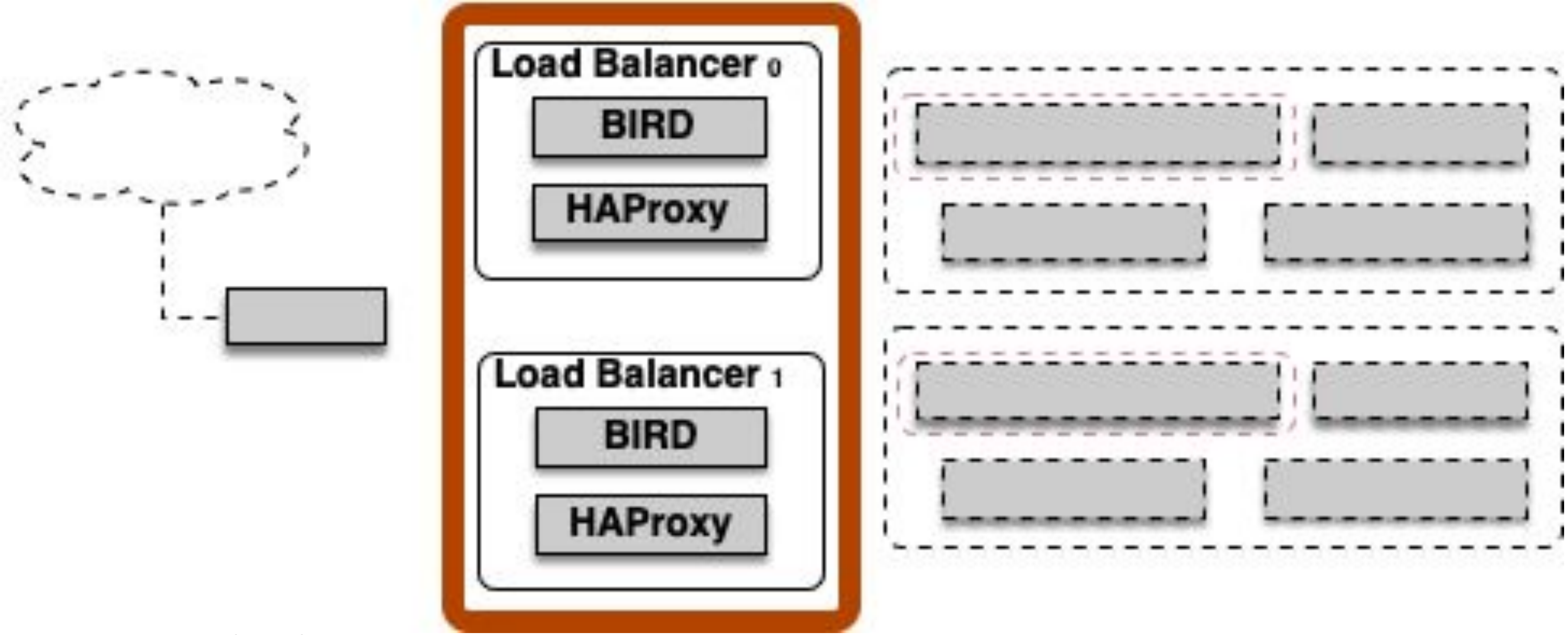
Utilise our existing hardware infrastructure to provide the base for the platform

Service Overview

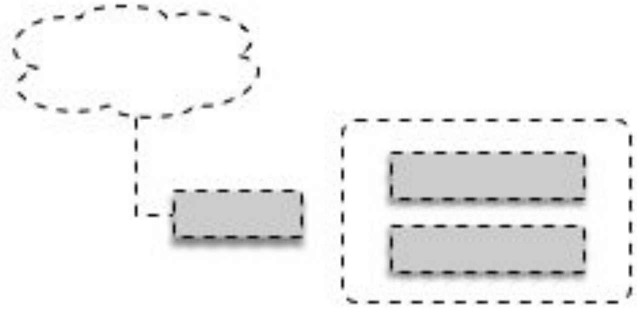


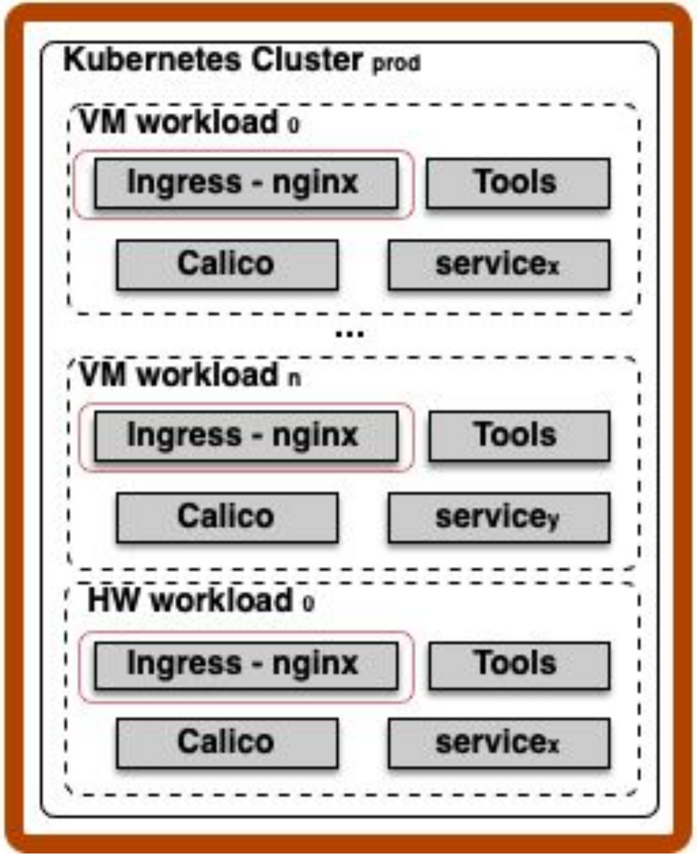
Infrastructure Overview

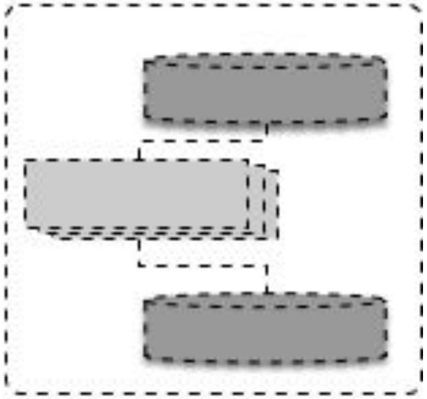




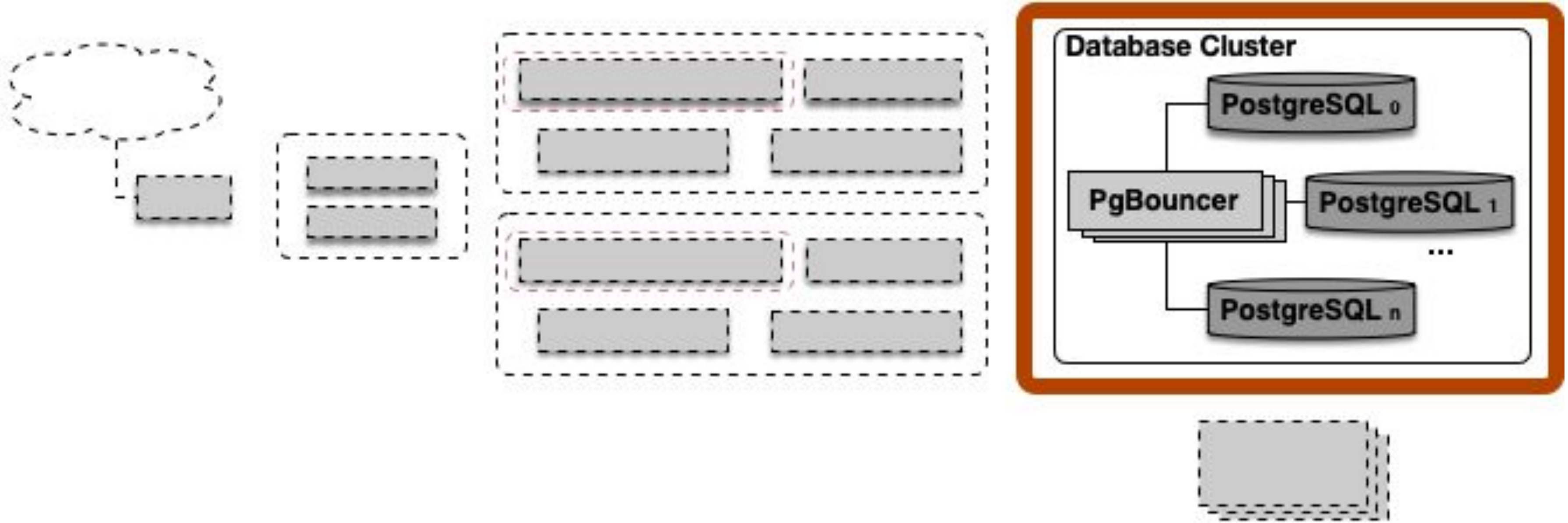
- BGP IP announcement (BIRD)
- TCP load balancing (HAProxy)
- Kubernetes nodeport for ingress-nginx service



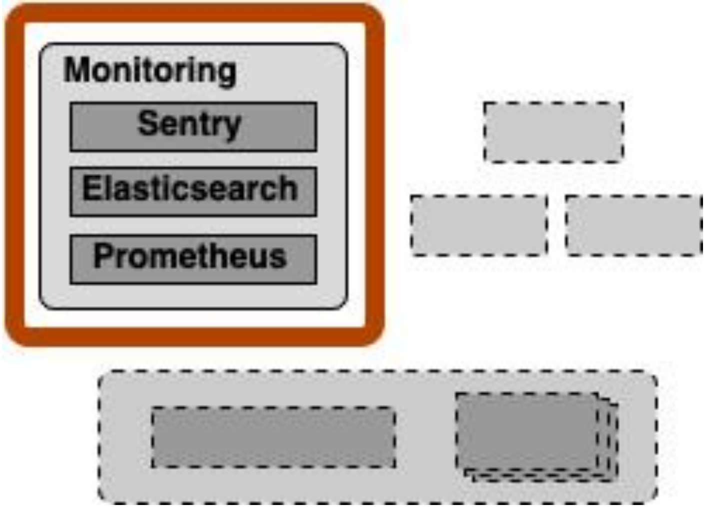




- Multiple clusters that support different groupings of services
- Also different clusters for different environments of the same service
- Each cluster has a series of infrastructure components that supports the services running on the clusters



- Postgresql cluster (1 leader, multiple replicas)
- Repmgr as cluster management tool
- Pgbouncer acts as as a lightweight connection pool

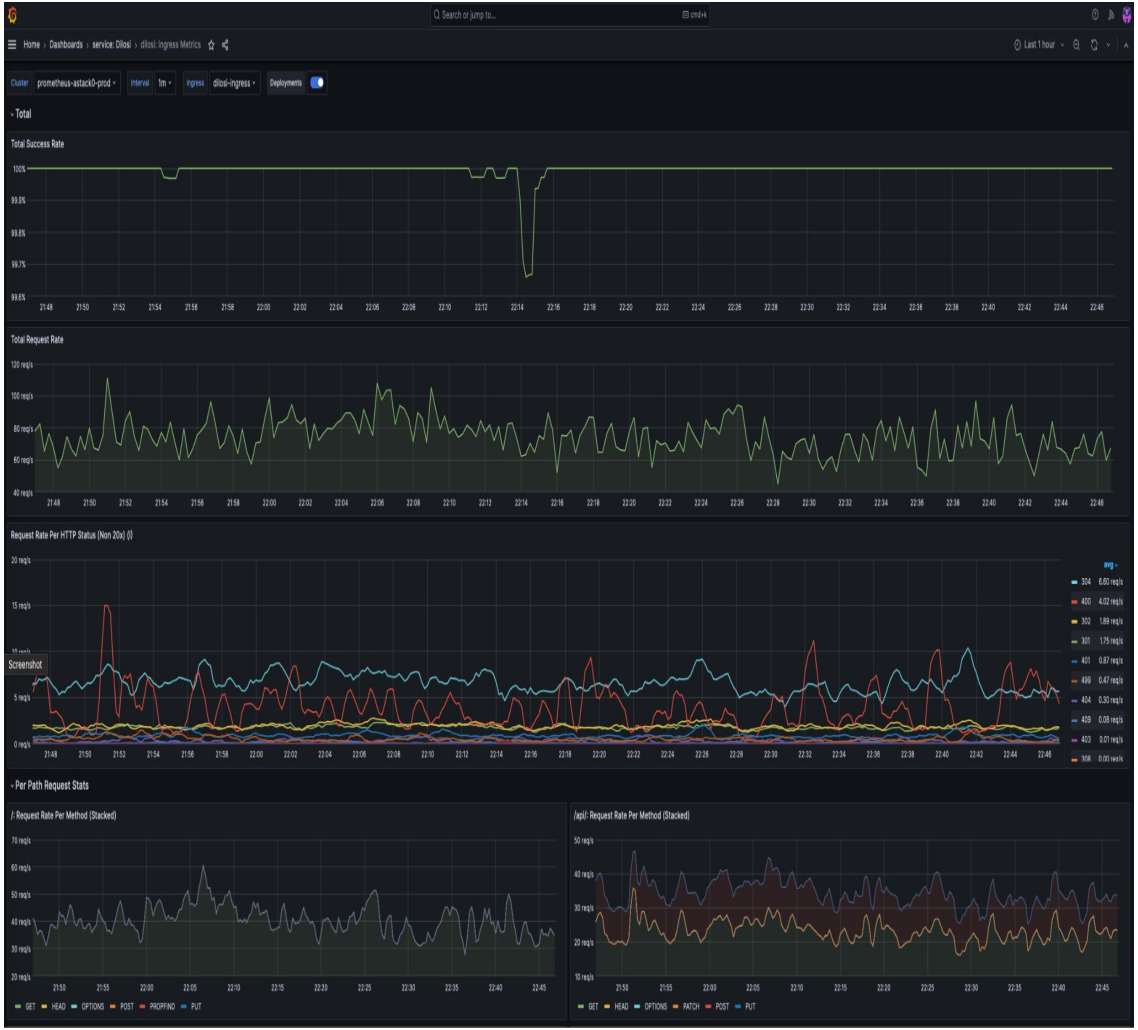


Monitoring

Sentry

Elasticsearch

Prometheus



Search or jump to... cmd+k

Home › Dashboards › service: Dilosi › dilosi: Ingress Metrics

Last 1 hour

Cluster: prometheus-astack0-prod

Interval: 1m

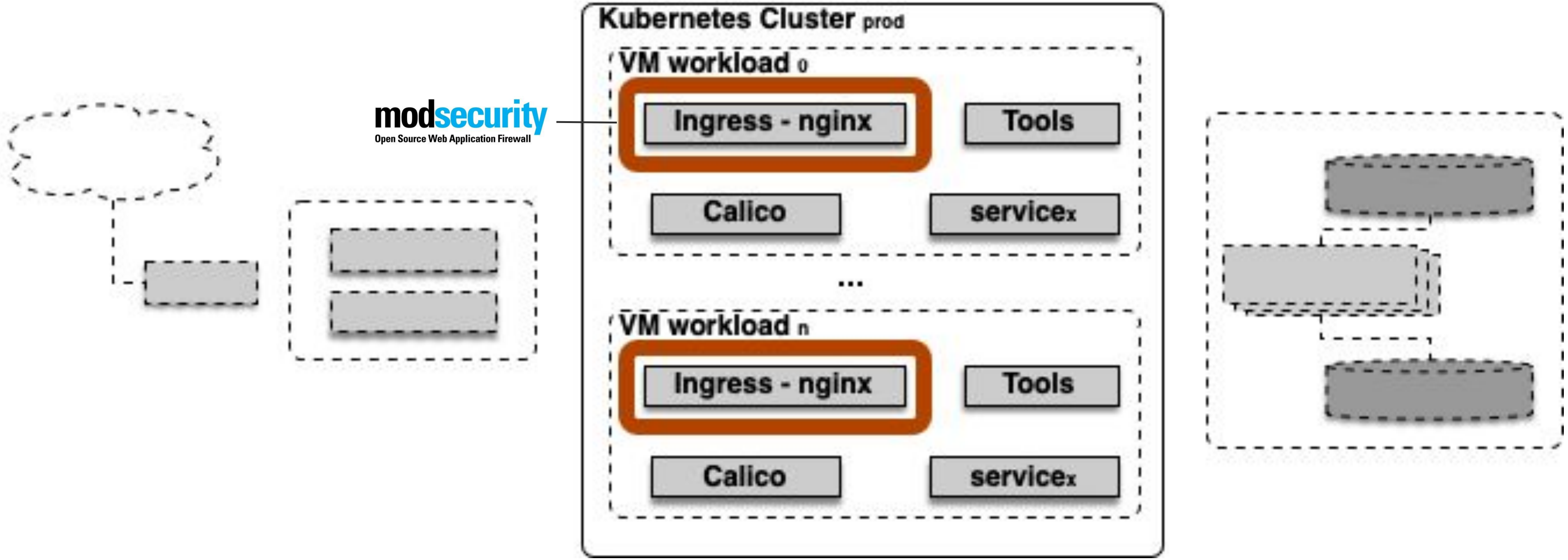
ingress: dilosi-ingress

Deployments

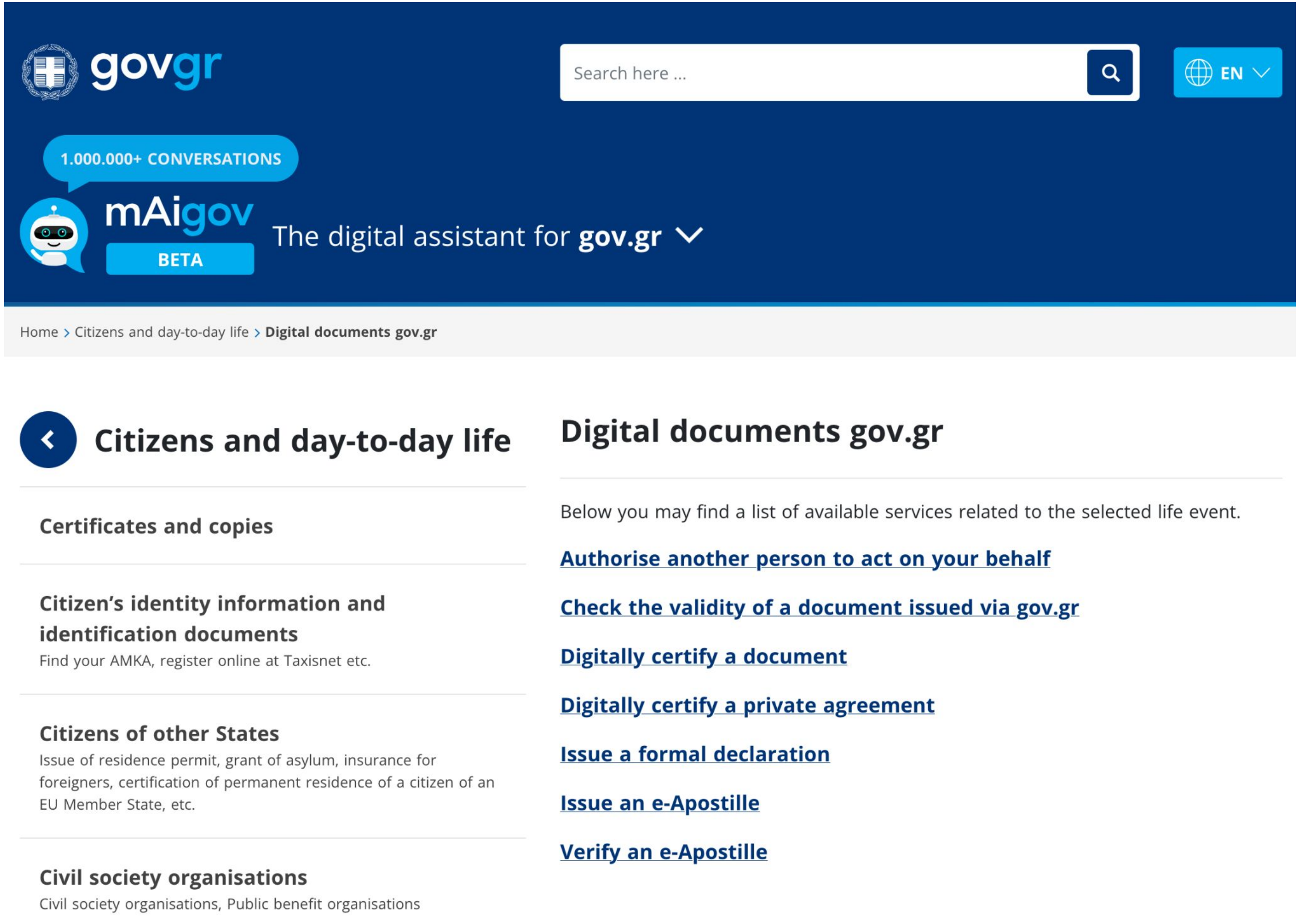
Total

	avg
304	6.60 req/s
400	4.02 req/s
302	1.89 req/s
301	1.75 req/s
401	0.87 req/s
499	0.47 req/s
404	0.30 req/s
409	0.08 req/s
403	0.01 req/s
308	0.00 req/s

Per Path Request Stats



- Use the well-established WAFI (WAF), modsecurity, supported in ingress-nginx
- Utilise the OWASP (Open Web Application Security Project) Core Rule Set
- Library for including for a service-specific rule set
- Custom log shipping component to create service oriented dashboards



Home > Citizens and day-to-day life > **Digital documents gov.gr**

Citizens and day-to-day life

Certificates and copies

Citizen’s identity information and identification documents
Find your AMKA, register online at Taxisnet etc.

Citizens of other States
Issue of residence permit, grant of asylum, insurance for foreigners, certification of permanent residence of a citizen of an EU Member State, etc.

Civil society organisations
Civil society organisations, Public benefit organisations

Digital documents gov.gr

Below you may find a list of available services related to the selected life event.

Authorise another person to act on your behalf

Check the validity of a document issued via gov.gr

Digitally certify a document

Digitally certify a private agreement

Issue a formal declaration

Issue an e-Apostille

Verify an e-Apostille

~300M transactions

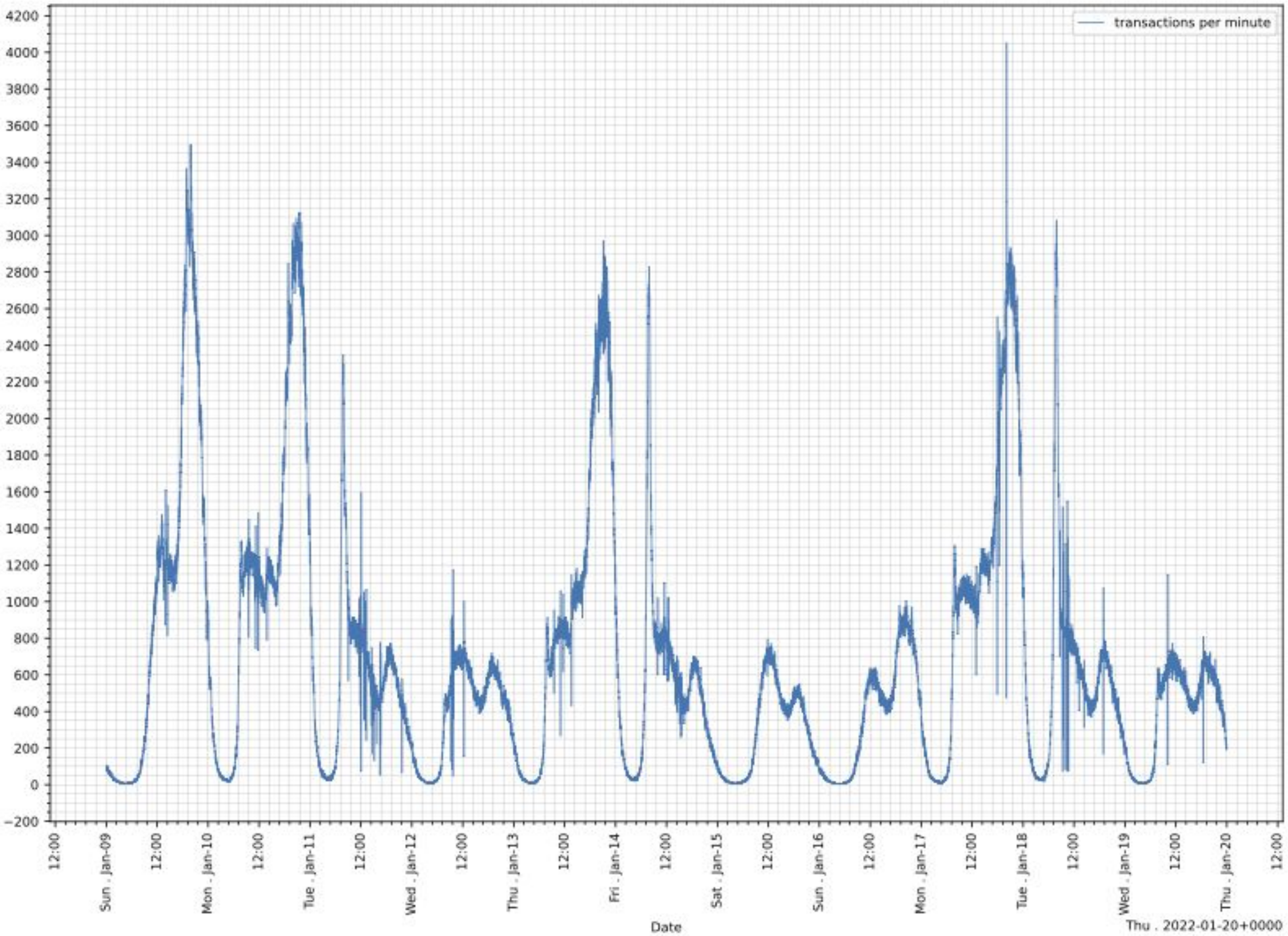
~8,5M citizens

20K r/s

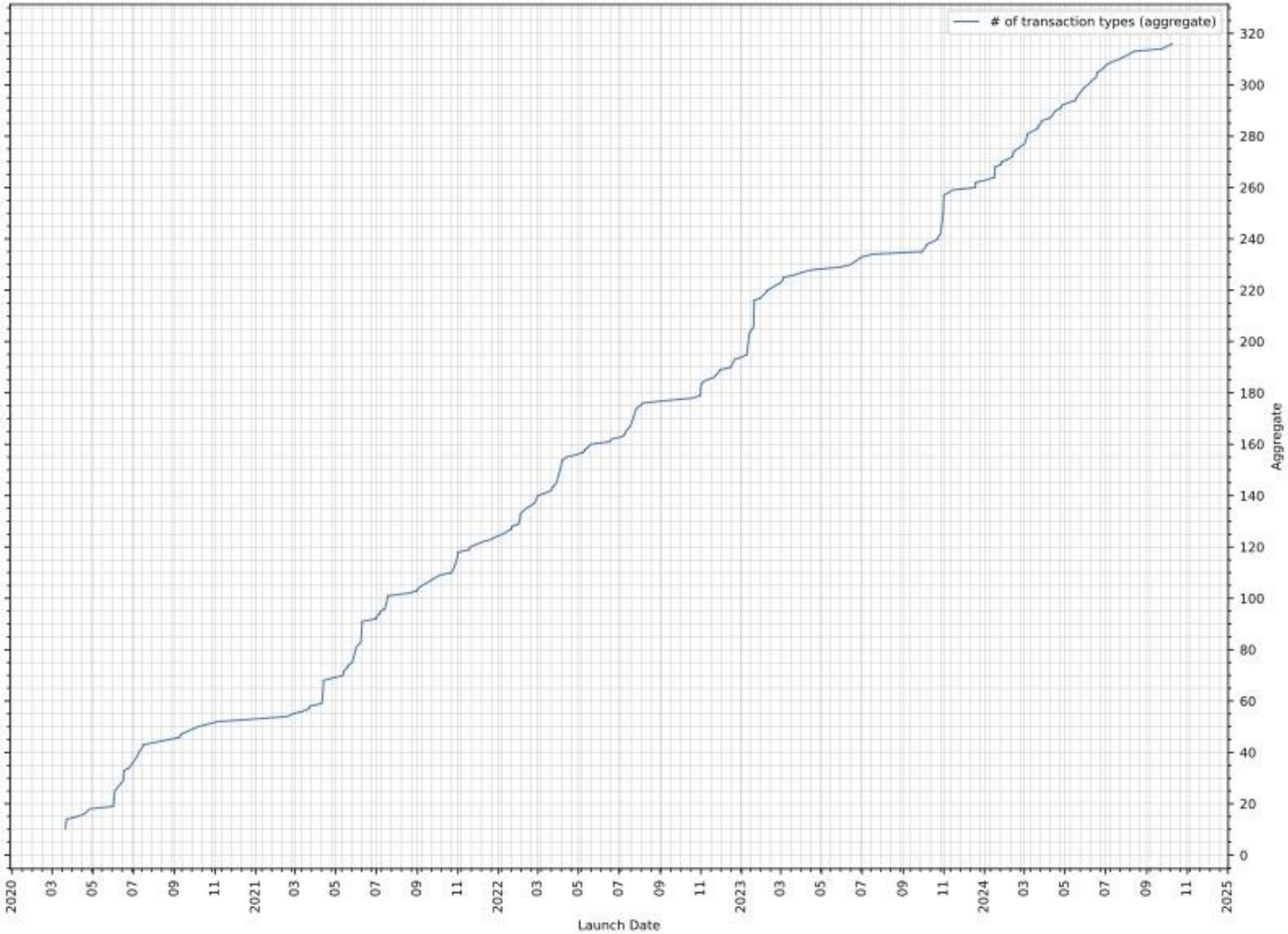
~6500 doc/min

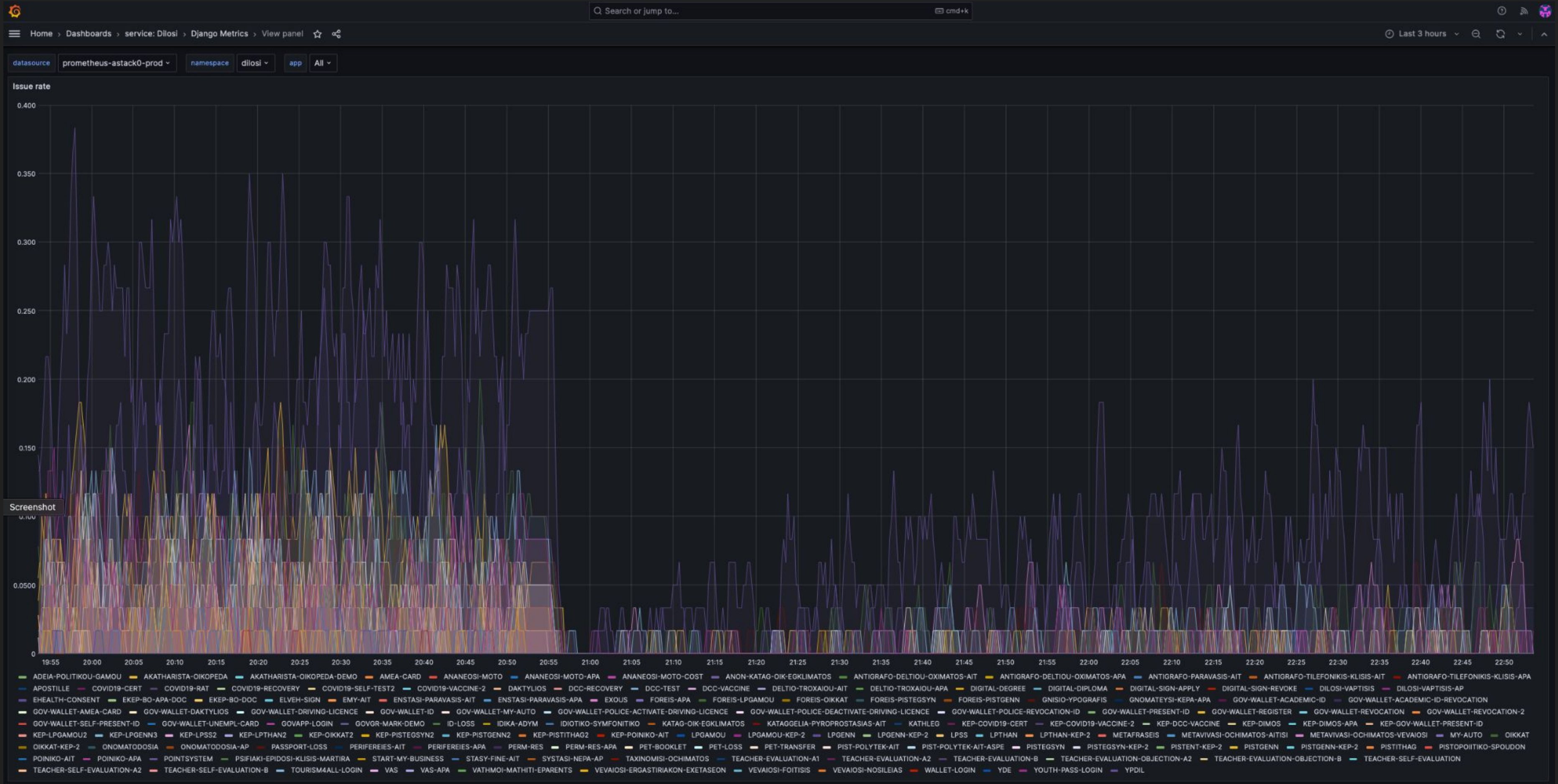
~100 docs/sec

10 days with the highest traffic during COVID-19



Aggregate number of the different transaction types launched throughout the years using AppStack





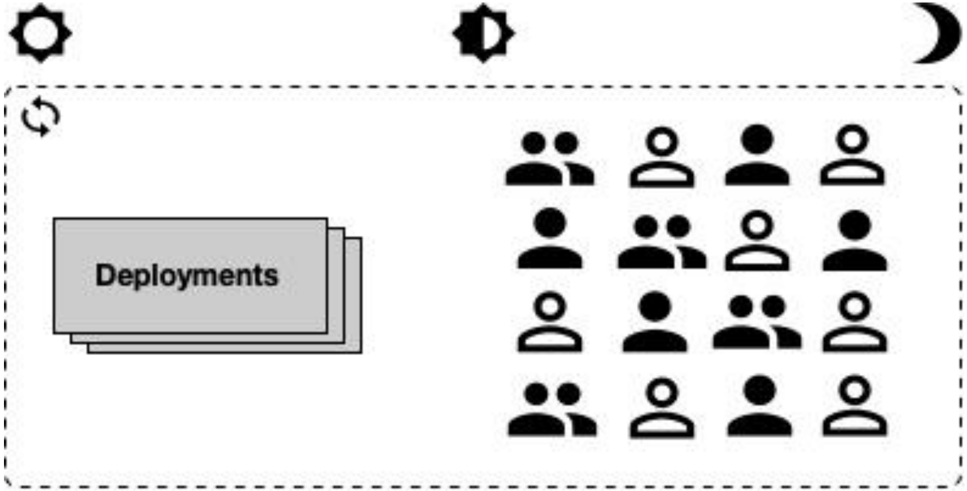
Home › Dashboards › service: Dilosi › Django Metrics › View panel

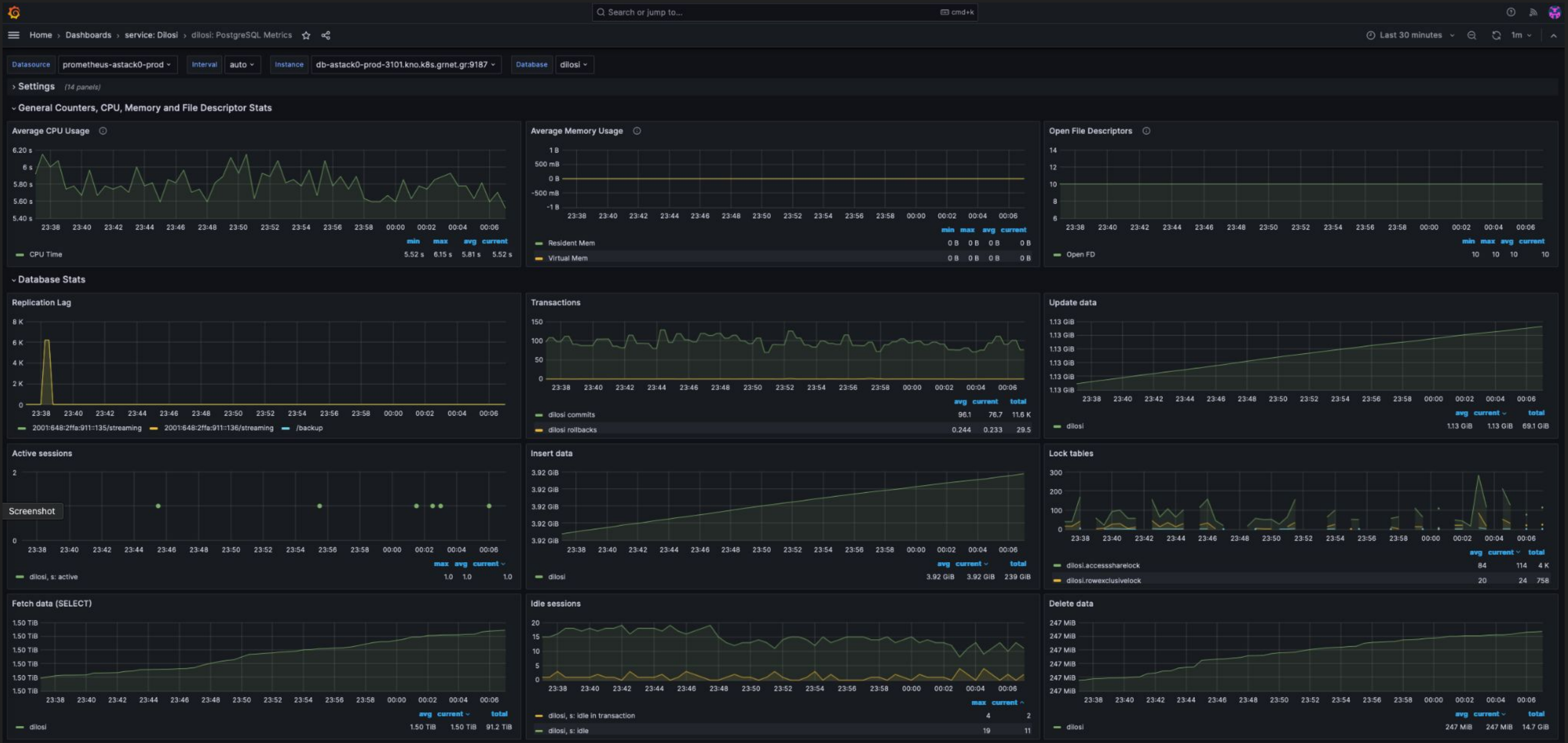
datasource: prometheus-astack0-prod
namespace: dilosi
app: All

Issue rate

Search or jump to...
cmd+k
Last 3 hours
Screenshot
0.400
0.350
0.300
0.250
0.200
0.150
0.100
0.0500
0
19:55
20:00
20:05
20:10
20:15
20:20
20:25
20:30
20:35
20:40
20:45
20:50
20:55
21:00
21:05
21:10
21:15
21:20
21:25
21:30
21:35
21:40
21:45
21:50
21:55
22:00
22:05
22:10
22:15
22:20
22:25
22:30
22:35
22:40
22:45
22:50
ADEIA-POLITIKOU-GAMOU AKATHARISTA-OIKOPEDA AKATHARISTA-OIKOPEDA-DEMO AMEA-CARD ANANEOSI-MOTO ANANEOSI-MOTO-APA ANANEOSI-MOTO-COST ANON-KATAG-OIK-EGKLIMATOS ANTIGRAFO-DELTIOU-OXIMATOS-AIT ANTIGRAFO-DELTIOU-OXIMATOS-APA ANTIGRAFO-PARAVASIS-AIT ANTIGRAFO-TILEFONIKIS-KLISIS-AIT ANTIGRAFO-TILEFONIKIS-KLISIS-APA
APOSTILLE COVID19-CERT COVID19-RAT COVID19-RECOVERY COVID19-SELF-TEST2 COVID19-VACCINE-2 DAKTYLIOS DCC-RECOVERY DCC-TEST DCC-VACCINE DELTIO-TROXAIOU-AIT DELTIO-TROXAIOU-APA DIGITAL-DEGREE DIGITAL-DIPLOMA DIGITAL-SIGN-APPLY DIGITAL-SIGN-REVOKE DILOSI-VAPTISIS DILOSI-VAPTISIS-AP
EHEALTH-CONSENT EKEP-BO-APA-DOC EKEP-BO-DOC ELVEH-SIGN EMY-AIT ENSTASI-PARAVASIS-AIT ENSTASI-PARAVASIS-APA EXOUS FOREIS-APA FOREIS-LPGAMOU FOREIS-OIKKAT FOREIS-PISTEGSYN FOREIS-PISTGENN GNISIO-YPOGRAFIS GNOMATEYSI-KEPA-APA GOV-WALLET-ACADEMIC-ID GOV-WALLET-ACADEMIC-ID-REVOCATION
GOV-WALLET-AMEA-CARD GOV-WALLET-DAKTYLIOS GOV-WALLET-DRIVING-LICENCE GOV-WALLET-ID GOV-WALLET-MY-AUTO GOV-WALLET-POLICE-ACTIVATE-DRIVING-LICENCE GOV-WALLET-POLICE-DEACTIVATE-DRIVING-LICENCE GOV-WALLET-POLICE-REVOCATION-ID GOV-WALLET-PRESENT-ID GOV-WALLET-REGISTER GOV-WALLET-REVOCATION GOV-WALLET-REVOCATION-2
GOV-WALLET-SELF-PRESENT-ID GOV-WALLET-UNEMPL-CARD GOVAPP-LOGIN GOVGR-MARK-DEMO ID-LOSS IDIKA-ADYM IDIOTIKO-SYMFONITIKO KATAG-OIK-EGKLIMATOS KATAGGELIA-PYROPROSTASIAS-AIT KATHLEG KEP-COVID19-CERT KEP-COVID19-VACCINE-2 KEP-DCC-VACCINE KEP-DIMOS KEP-DIMOS-APA KEP-GOV-WALLET-PRESENT-ID
KEP-LPGAMOU2 KEP-LPGENN3 KEP-LPSS2 KEP-LPTHAN2 KEP-OIKKAT2 KEP-PISTEGSYN2 KEP-PISTGENN2 KEP-PISTITHAG2 KEP-POINIKO-AIT LPGAMOU LPGAMOU-KEP-2 LPGENN LPGENN-KEP-2 LPSS LPTHAN LPTHAN-KEP-2 METAFRASEIS METAVIVASI-OCHIMATOS-AITISI METAVIVASI-OCHIMATOS-VEVAIOSI MY-AUTO OIKKAT
OIKKAT-KEP-2 ONOMATODOSIA ONOMATODOSIA-AP PASSPORT-LOSS PERIFEREIES-AIT PERIFEREIES-APA PERM-RES PERM-RES-APA PET-BOOKLET PET-LOSS PET-TRANSFER PIST-POLYTEK-AIT PIST-POLYTEK-AIT-ASPE PISTEGSYN PISTEGSYN-KEP-2 PISTENT-KEP-2 PISTGENN PISTGENN-KEP-2 PISTITHAG PISTOPOIITIKO-SPOUDON
POINIKO-AIT POINIKO-APA POINTSYSTEM PSIFIAKI-EPIDOSI-KLISIS-MARTIRA START-MY-BUSINESS STASY-FINE-AIT SYSTASI-NEPA-AP TAXINOMISI-OCHIMATOS TEACHER-EVALUATION-A1 TEACHER-EVALUATION-A2 TEACHER-EVALUATION-B TEACHER-EVALUATION-OBJECTION-A2 TEACHER-EVALUATION-OBJECTION-B TEACHER-SELF-EVALUATION
TEACHER-SELF-EVALUATION-A2 TEACHER-SELF-EVALUATION-B TOURISM4ALL-LOGIN VAS VAS-APA VATHMOI-MATHITI-EPARENTS VEVAIOSI-ERGASTIRIAKON-EXETASEON VEVAIOSI-FOITISIS VEVAIOSI-NOSILEIAS WALLET-LOGIN YDE YOUTH-PASS-LOGIN YPDIL

our architecture allows for multiple deployments per day, even with thousands of users connected





Home › Dashboards › service: Dilosi › dilosi: PostgreSQL Metrics

Last 30 minutes · 1m

Datasource: prometheus-astack0-prod · Interval: auto · Instance: db-astack0-prod-3101.kno.k8s.grnet.gr:9187 · Database: dilosi

› Settings *(14 panels)*

⌄ General Counters, CPU, Memory and File Descriptor Stats

Average CPU Usage

	min	max	avg	current
CPU Time	5.52 s	6.15 s	5.81 s	5.52 s

Average Memory Usage

	min	max	avg	current
Resident Mem	0 B	0 B	0 B	0 B
Virtual Mem	0 B	0 B	0 B	0 B

Open File Descriptors

	min	max	avg	current
Open FD	10	10	10	10

⌄ Database Stats

Replication Lag

2001:648:2ffa:911::135/streaming · 2001:648:2ffa:911::136/streaming · /backup

Transactions

	avg	current	total
dilosi commits	96.1	76.7	11.6 K
dilosi rollbacks	0.244	0.233	29.5

Update data

	avg	current	total
dilosi	1.13 GiB	1.13 GiB	69.1 GiB

Active sessions

	max	avg	current
dilosi, s: active	1.0	1.0	1.0

Insert data

	avg	current	total
dilosi	3.92 GiB	3.92 GiB	239 GiB

Lock tables

	avg	current	total
dilosi.accesssharelock	84	114	4 K
dilosi.rowexclusivelock	20	24	758

Fetch data (SELECT)

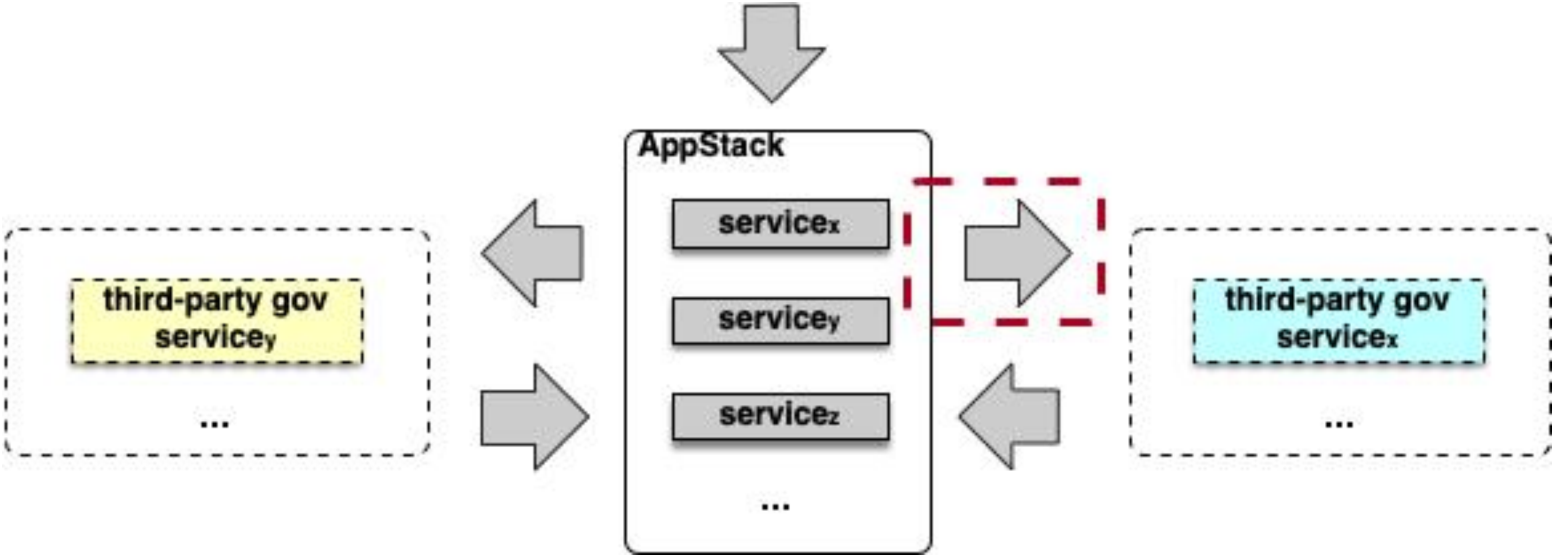
	avg	current	total
dilosi	1.50 TiB	1.50 TiB	91.2 TiB

Idle sessions

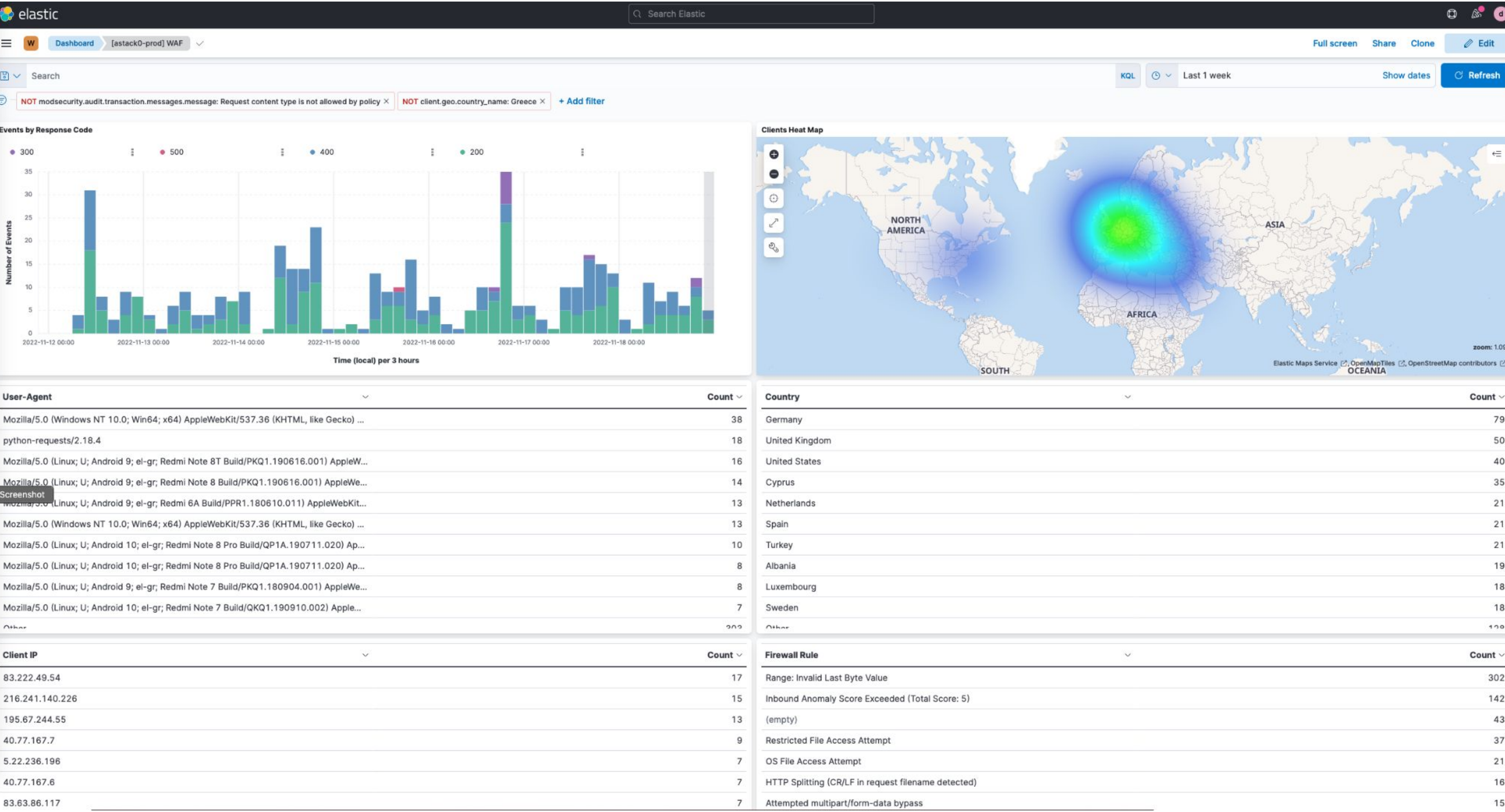
	max	current
dilosi, s: idle in transaction	4	2
dilosi, s: idle	19	11

Delete data

	avg	current	total
dilosi	247 MiB	247 MiB	14.7 GiB


AppStack
service$_x$
service$_y$
service$_z$
...
third-party gov service$_y$
...
third-party gov service$_x$
...

48hr



NOT modsecurity.audit.transaction.messages.message: Request content type is not allowed by policy ×

NOT client.geo.country_name: Greece ×

Events by Response Code

Clients Heat Map

NORTH AMERICA
ASIA
AFRICA
SOUTH
OCEANIA
zoom: 1.0
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

User-Agent	Count
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) ...	38
python-requests/2.18.4	18
Mozilla/5.0 (Linux; U; Android 9; el-gr; Redmi Note 8T Build/PKQ1.190616.001) AppleW...	16
Mozilla/5.0 (Linux; U; Android 9; el-gr; Redmi Note 8 Build/PKQ1.190616.001) AppleWe...	14
Mozilla/5.0 (Linux; U; Android 9; el-gr; Redmi 6A Build/PPR1.180610.011) AppleWebKit...	13
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) ...	13
Mozilla/5.0 (Linux; U; Android 10; el-gr; Redmi Note 8 Pro Build/QP1A.190711.020) Ap...	10
Mozilla/5.0 (Linux; U; Android 10; el-gr; Redmi Note 8 Pro Build/QP1A.190711.020) Ap...	8
Mozilla/5.0 (Linux; U; Android 9; el-gr; Redmi Note 7 Build/PKQ1.180904.001) AppleWe...	8
Mozilla/5.0 (Linux; U; Android 10; el-gr; Redmi Note 7 Build/QKQ1.190910.002) Apple...	7
Other	303

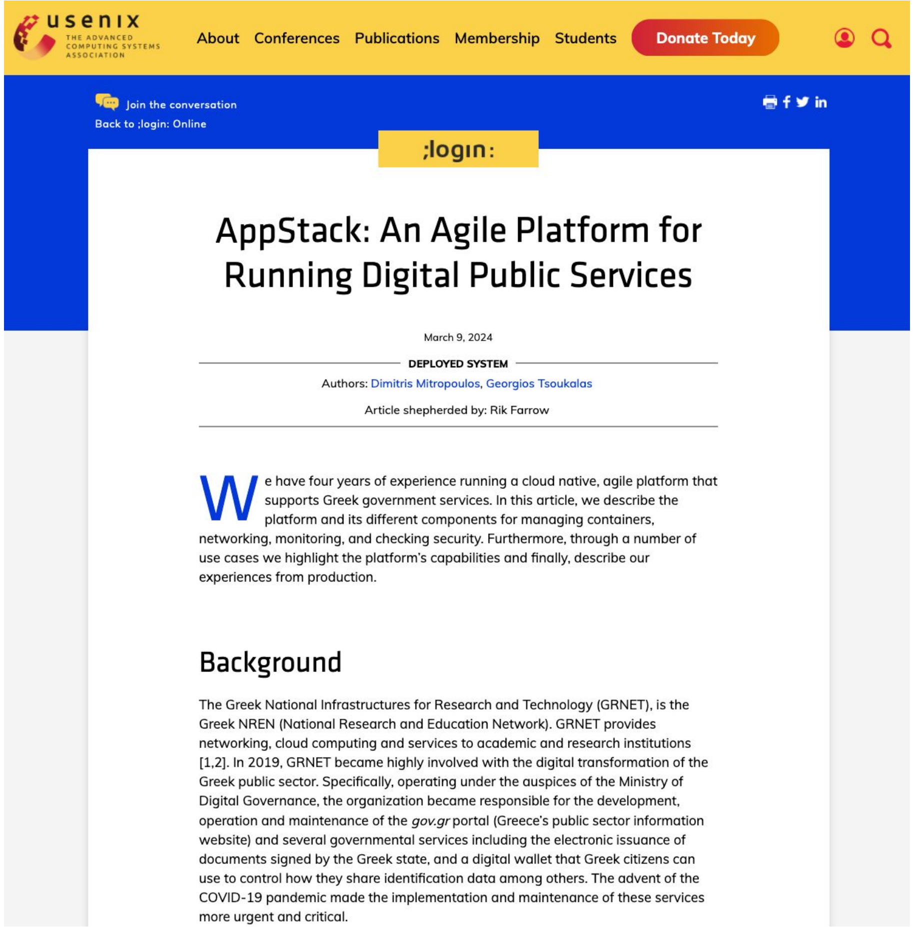
Country	Count
Germany	79
United Kingdom	50
United States	40
Cyprus	35
Netherlands	21
Spain	21
Turkey	21
Albania	19
Luxembourg	18
Sweden	18
Other	128

Client IP	Count
83.222.49.54	17
216.241.140.226	15
195.67.244.55	13
40.77.167.7	9
5.22.236.196	7
40.77.167.6	7
83.63.86.117	7

Firewall Rule	Count
Range: Invalid Last Byte Value	302
Inbound Anomaly Score Exceeded (Total Score: 5)	142
(empty)	43
Restricted File Access Attempt	37
OS File Access Attempt	21
HTTP Splitting (CR/LF in request filename detected)	16
Attempted multipart/form-data bypass	15

Moving forward

- Work on disaster recovery solutions
  - Replicate data and applications across multiple cloud offerings and on-premises environments
- Managing container image vulnerabilities
  - The platform already enables the periodic scanning of container images via open-source scanners (e.g. Trivy) to identify and address vulnerabilities in images early in the development lifecycle
- Dive deeper into monitoring
  - SLOs, Observability, etc



AppStack: An Agile Platform for Running Digital Public Services

March 9, 2024

DEPLOYED SYSTEM

Authors: Dimitris Mitropoulos, Georgios Tsoukalas

Article shepherded by: Rik Farrow

We have four years of experience running a cloud native, agile platform that supports Greek government services. In this article, we describe the platform and its different components for managing containers, networking, monitoring, and checking security. Furthermore, through a number of use cases we highlight the platform's capabilities and finally, describe our experiences from production.

Background

The Greek National Infrastructures for Research and Technology (GRNET), is the Greek NREN (National Research and Education Network). GRNET provides networking, cloud computing and services to academic and research institutions [1,2]. In 2019, GRNET became highly involved with the digital transformation of the Greek public sector. Specifically, operating under the auspices of the Ministry of Digital Governance, the organization became responsible for the development, operation and maintenance of the *gov.gr* portal (Greece's public sector information website) and several governmental services including the electronic issuance of documents signed by the Greek state, and a digital wallet that Greek citizens can use to control how they share identification data among others. The advent of the COVID-19 pandemic made the implementation and maintenance of these services more urgent and critical.

thank you!