AppStack

An Agile Platform for Running Digital Public Services

Dimitris Mitropoulos
dimitro@grnet.gr

National Infrastructures for Research and Technology

Roadmap

1. GRNET Scope
2. Operating digital public services: challenges
3. A unified computing environment for gov.gr horizontal services
4. Tackling problems with different OSS components
5. Experiences from production
6. Future directions (via internships)

GRNET S.A. – 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

From **2019**, GRNET operates under the **Ministry of Digital Governance**. GRNET provides:

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

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

Users

- Members of the academic and research community
- Network Operation Centers
- Students
- Public hospital personnel
- Public administration personnel
- Citizens

(up until 2019)

Copernicus BDR HARMONI Eudoxus Apella ~okeanos ~okeanos-global ~okeanos-knossos Diavlos Zeus Delos365 AcademicID HIDM ViMa Argo DNS NTP Mail AaaS parltv FOD Eduroam Redmine Phabricator Phabricator JIRA Piwik Wordpress Limesurvey Sympa Confluence Massmail TravelExpenses SecureNotes XMPP Chat Webdns4 Nextcloud OpenVPN LDAP FTP SnipeIT Netbox Syslog RADIUS Observium Mon LG IDP AbuseIO Jenkins Puppet FAI Icinga Prometheus Elasticsearch Graphite Grafana Bacula PostgreSQL MariaDB

gov.gr: portal and services

(summer ‘19)

challenges?

self-hosted

multiple services

resiliency

security

constant changes

scalability

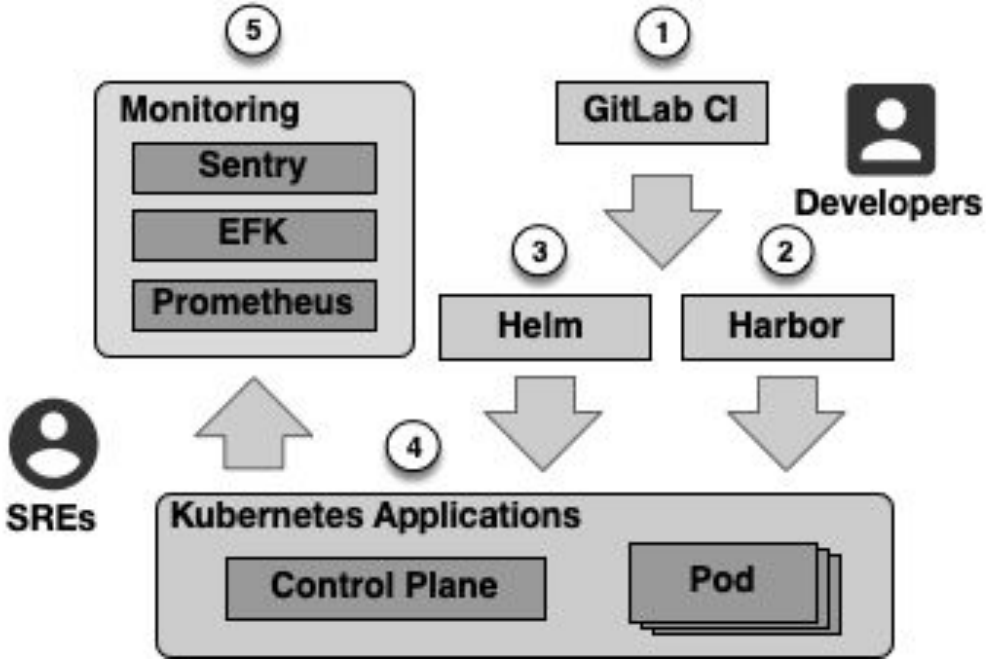
team collaboration

AppStack

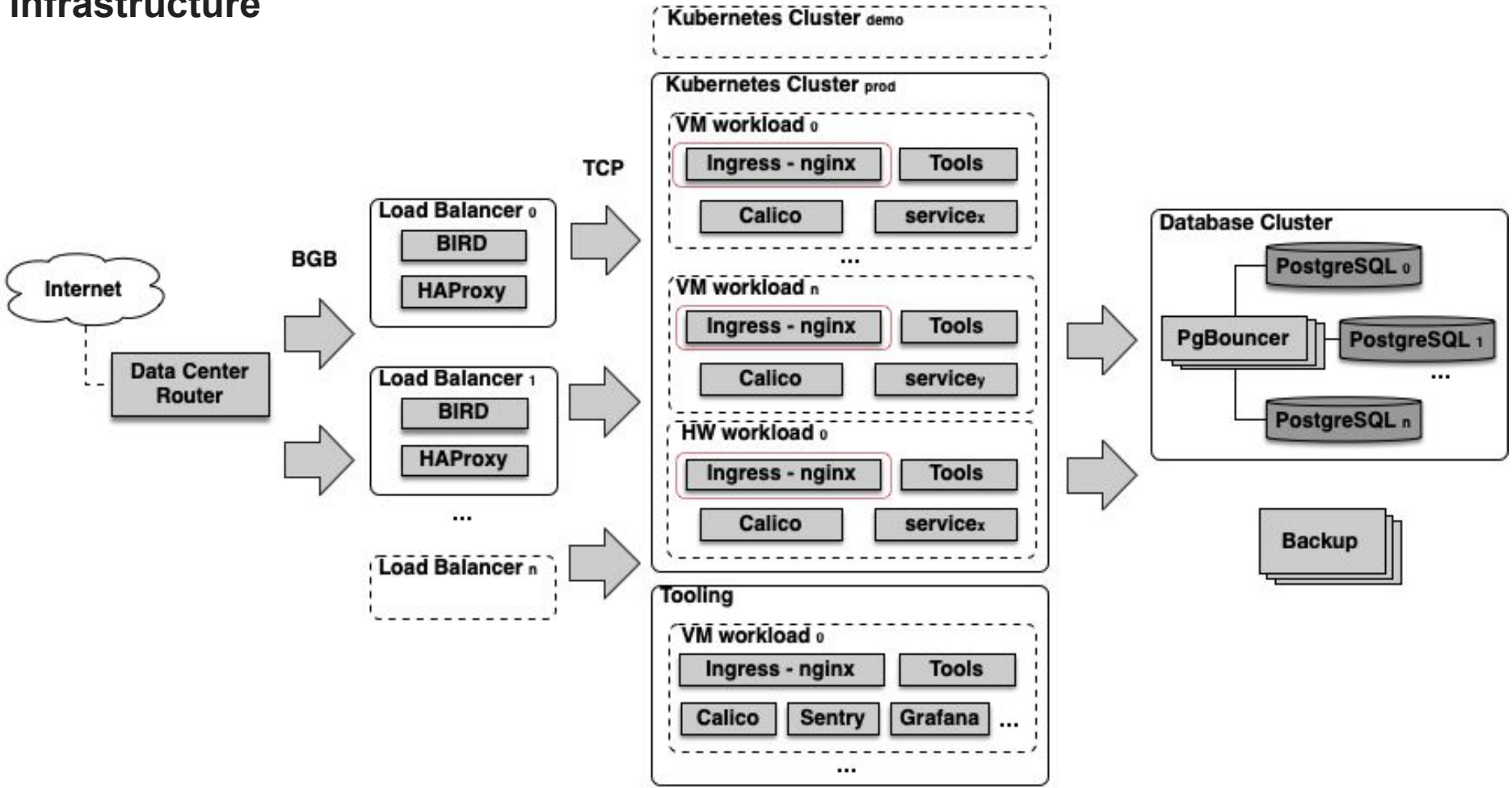
a unified computing environment for gov.gr services

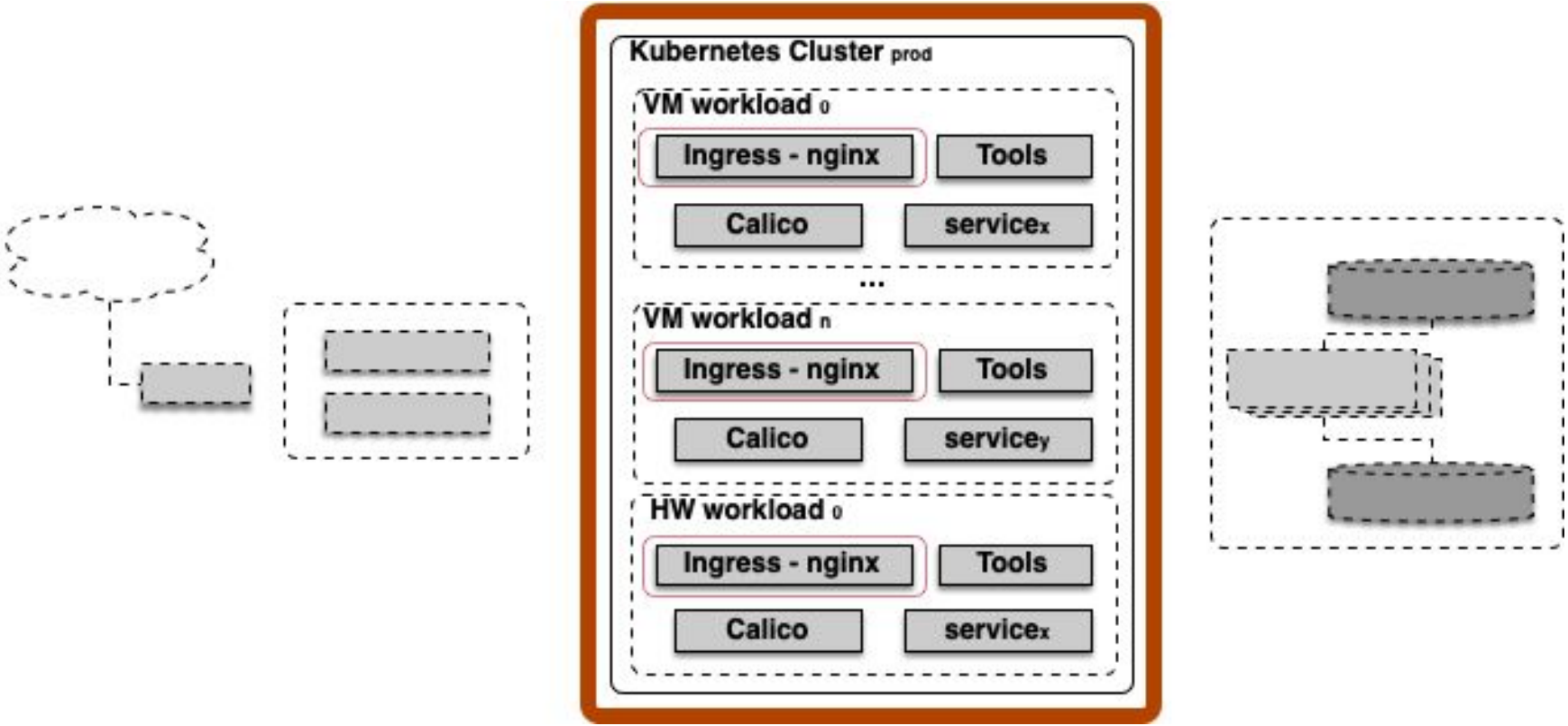
currently hosting:
dilosi, gov.gr, edupass, DGC, EIDAS, firstreg, gov wallet, auth, vouchers and more

pipeline


5
1
Monitoring
Sentry
EFK
Prometheus
GitLab CI
Developers
3
2
Helm
Harbor
SREs
4
Kubernetes Applications
Control Plane
Pod

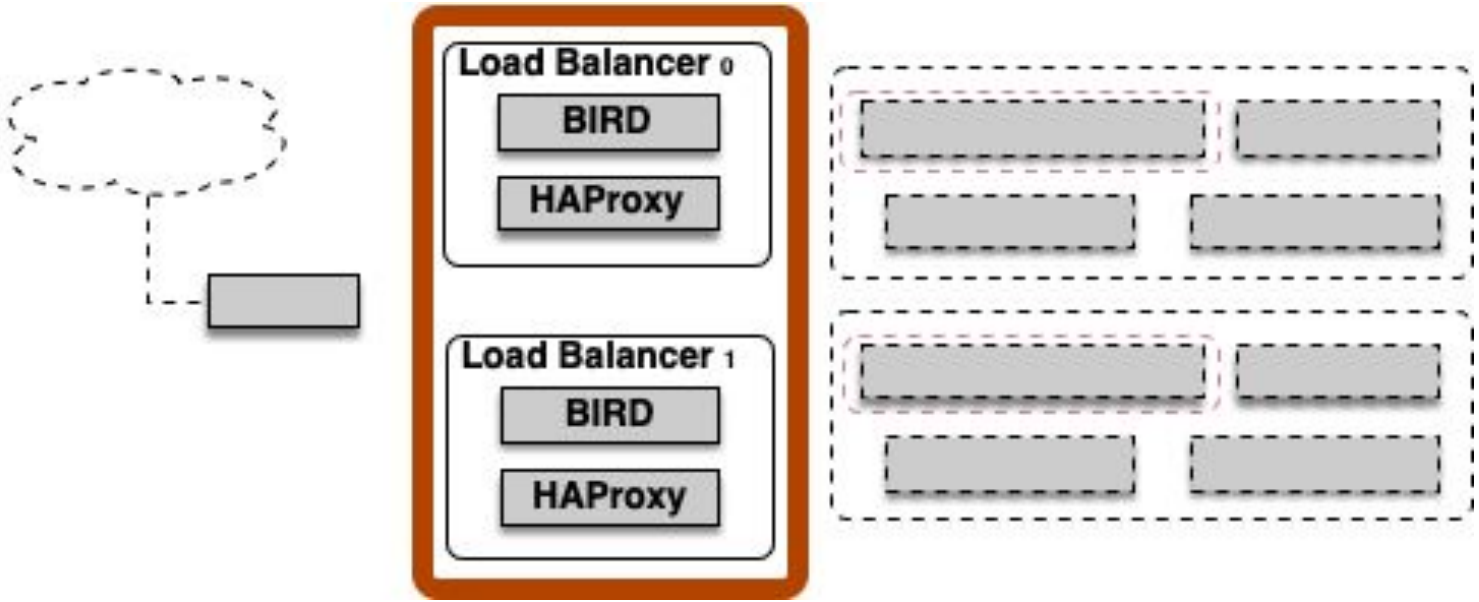
infrastructure




Kubernetes Cluster prod
VM workload 0
Ingress - nginx
Tools
Calico
servicex
...
VM workload n
Ingress - nginx
Tools
Calico
servicey
HW workload 0
Ingress - nginx
Tools
Calico
servicex

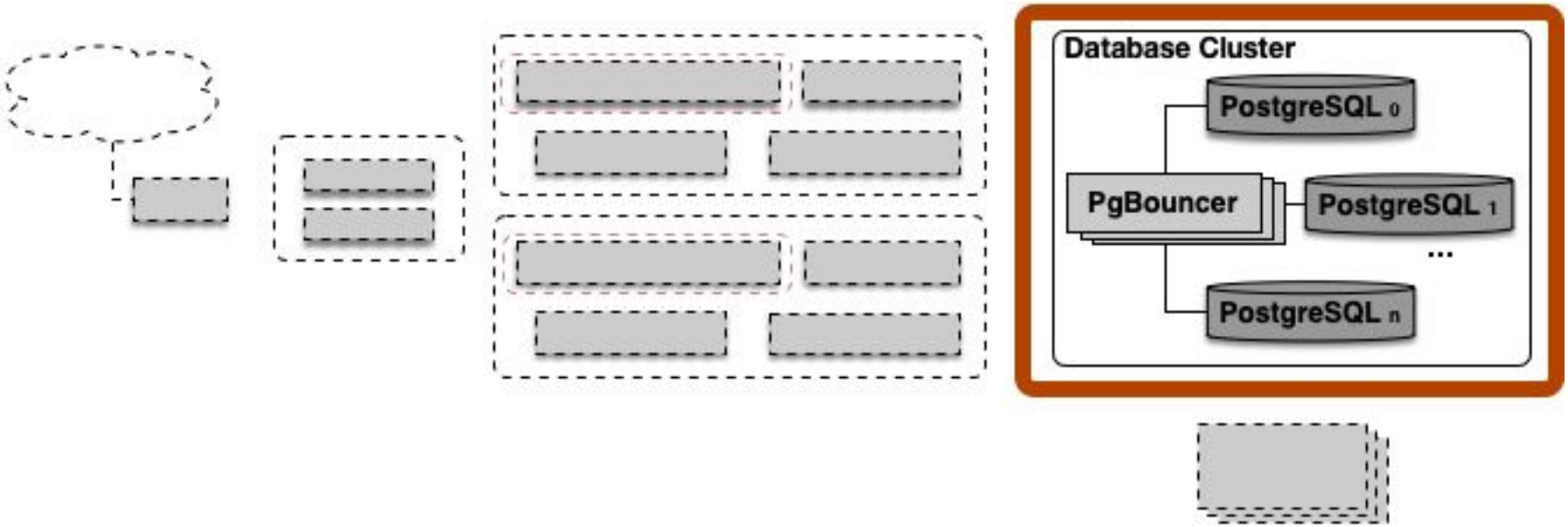
Kubernetes benefits

- dynamic environment support
- in-cluster load balancing
- automated rollouts and rollbacks
- self-healing


Load Balancer 0
BIRD
HAProxy
Load Balancer 1
BIRD
HAProxy

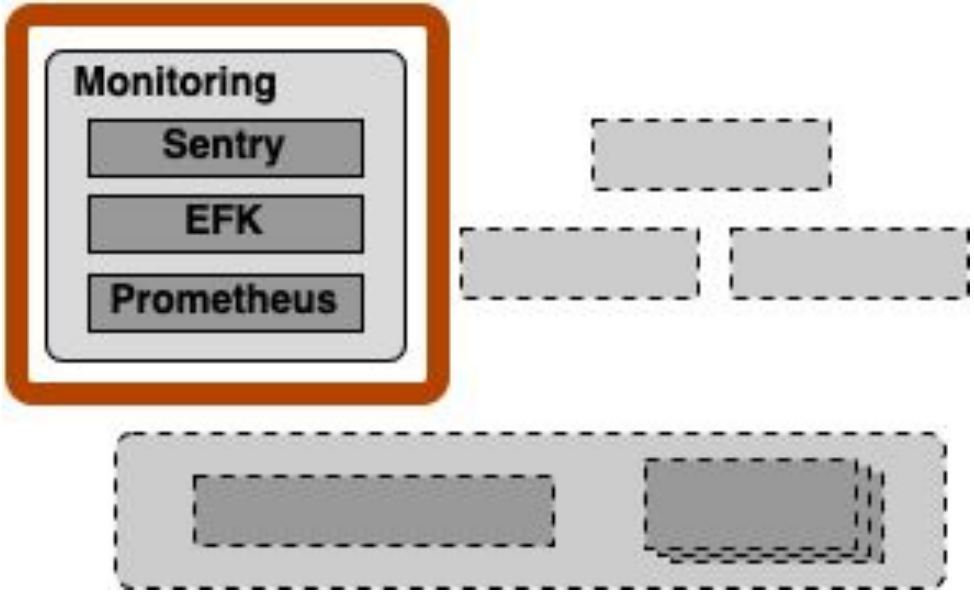
Load balancer setup benefits

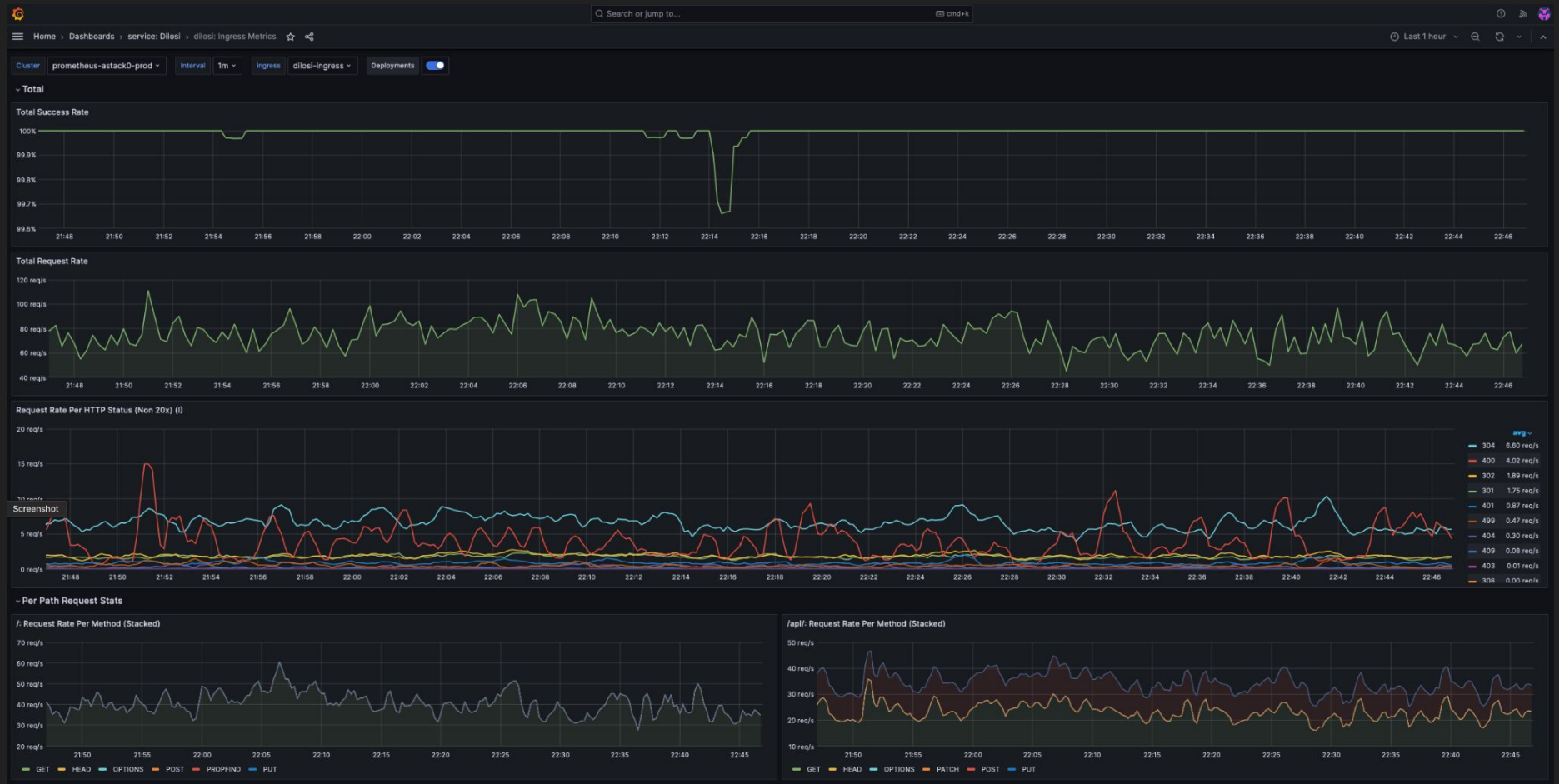
- BGP support (BIRD)
- dynamic IP routing (BIRD)
- TCP/HTTP load balancing (HAProxy)
- high traffic website support (HAProxy)
- high availability (both)

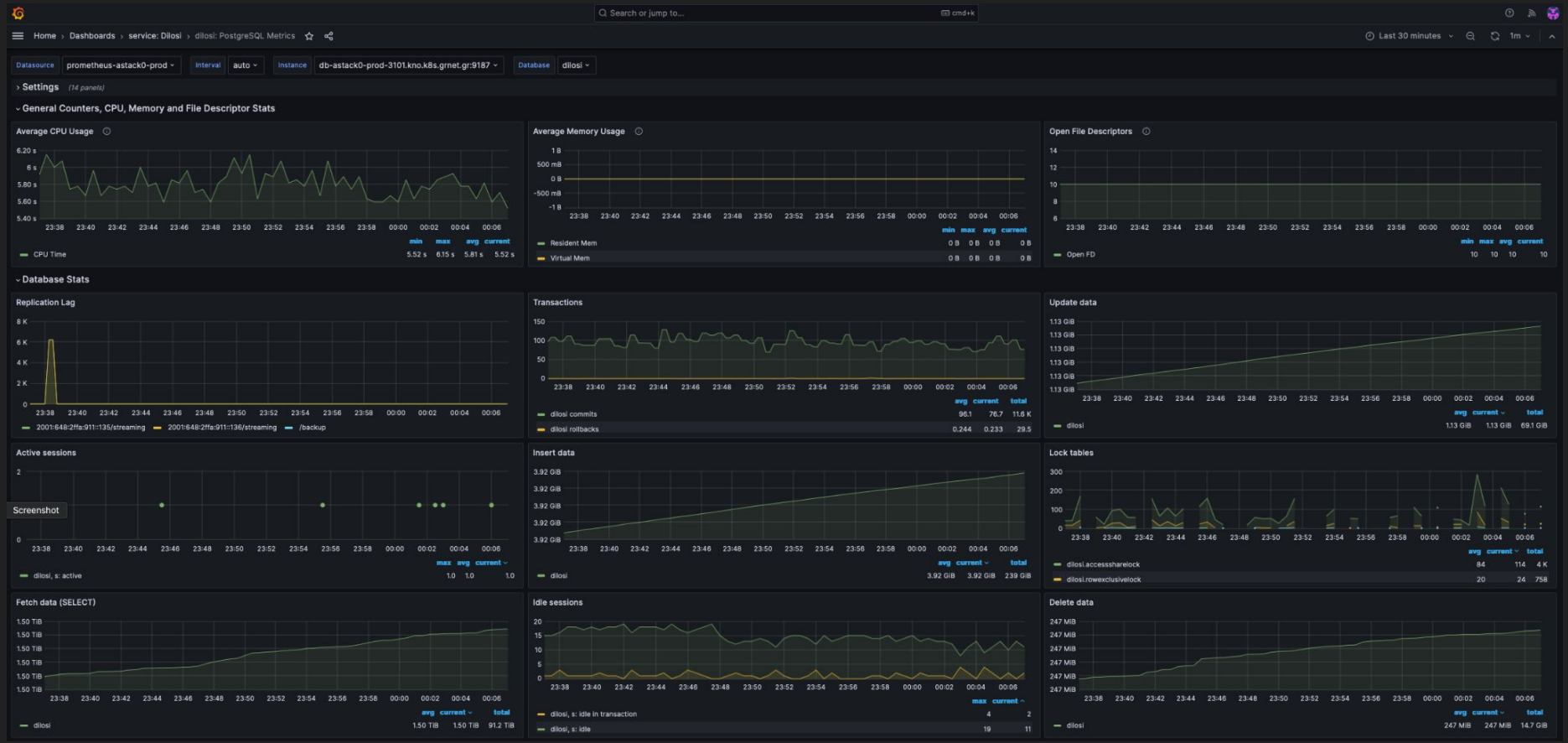

Database Cluster
PostgreSQL 0
PgBouncer
PostgreSQL 1
...
PostgreSQL n

PgBouncer benefits

- lightweight connection pool
- improve idle and short-lived connections at the database server
- uses actual Postgres connections when needed


Monitoring
Sentry
EFK
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
Total Success Rate
100%
99.9%
99.8%
99.7%
99.6%
Total Request Rate
120 req/s
100 req/s
80 req/s
60 req/s
40 req/s
Request Rate Per HTTP Status (Non 20x) (i)
20 req/s
15 req/s
5 req/s
0 req/s
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
Screenshot
Per Path Request Stats
/: Request Rate Per Method (Stacked)
70 req/s
60 req/s
50 req/s
40 req/s
30 req/s
20 req/s
GET HEAD OPTIONS POST PROPFIND PUT
/api/: Request Rate Per Method (Stacked)
50 req/s
40 req/s
30 req/s
20 req/s
10 req/s
GET HEAD OPTIONS PATCH POST PUT


Search or jump to... cmd+k
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
CPU Time 5.52 s 6.15 s 5.81 s 5.52 s
Average Memory Usage
Resident Mem 0 B 0 B 0 B 0 B
Virtual Mem 0 B 0 B 0 B 0 B
Open File Descriptors
Open FD 10 10 10 10
Database Stats
Replication Lag
2001:648:2ffa:911::135/streaming
2001:648:2ffa:911::136/streaming
/backup
Transactions
dilosi commits 96.1 76.7 11.6 K
dilosi rollbacks 0.244 0.233 29.5
Update data
dilosi 1.13 GiB 1.13 GiB 69.1 GiB
Active sessions
dilosi, s: active 1.0 1.0 1.0
Insert data
dilosi 3.92 GiB 3.92 GiB 239 GiB
Lock tables
dilosi.accesssharelock 84 114 4 K
dilosi.rowexclusivelock 20 24 758
Fetch data (SELECT)
dilosi 1.50 TiB 1.50 TiB 91.2 TiB
Idle sessions
dilosi, s: idle in transaction 4 2
dilosi, s: idle 19 11
Delete data
dilosi 247 MiB 247 MiB 14.7 GiB
Screenshot

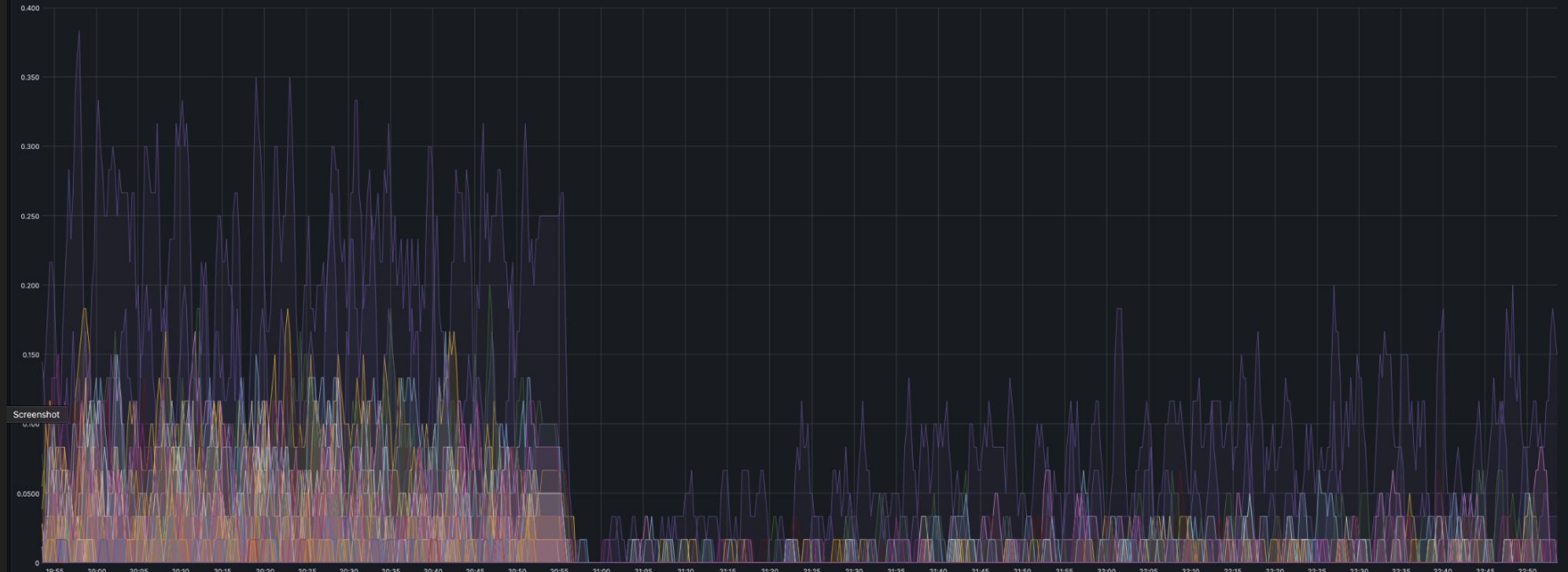
Search or jump to... cmd+k

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

Last 3 hours

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

Issue rate

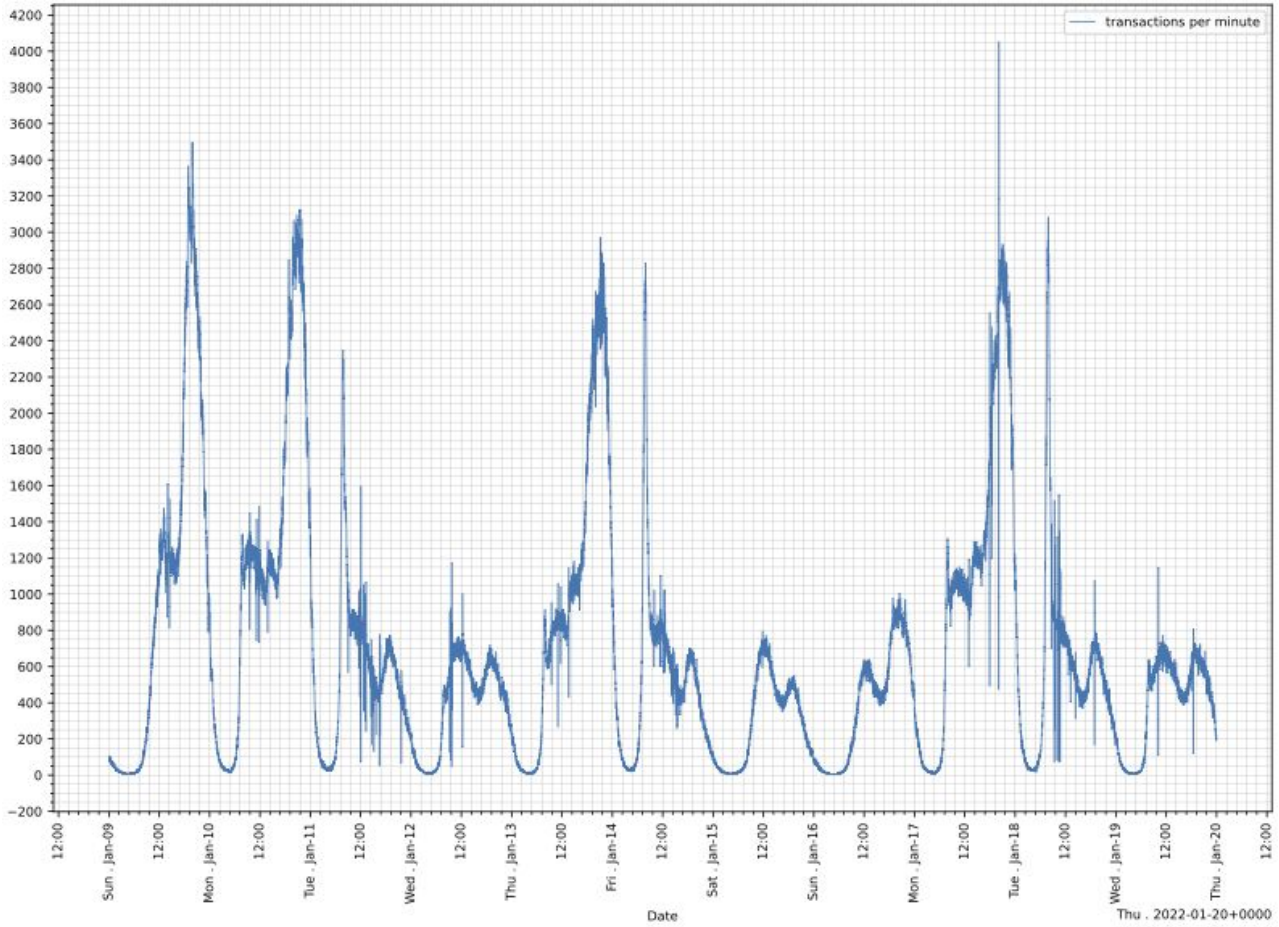


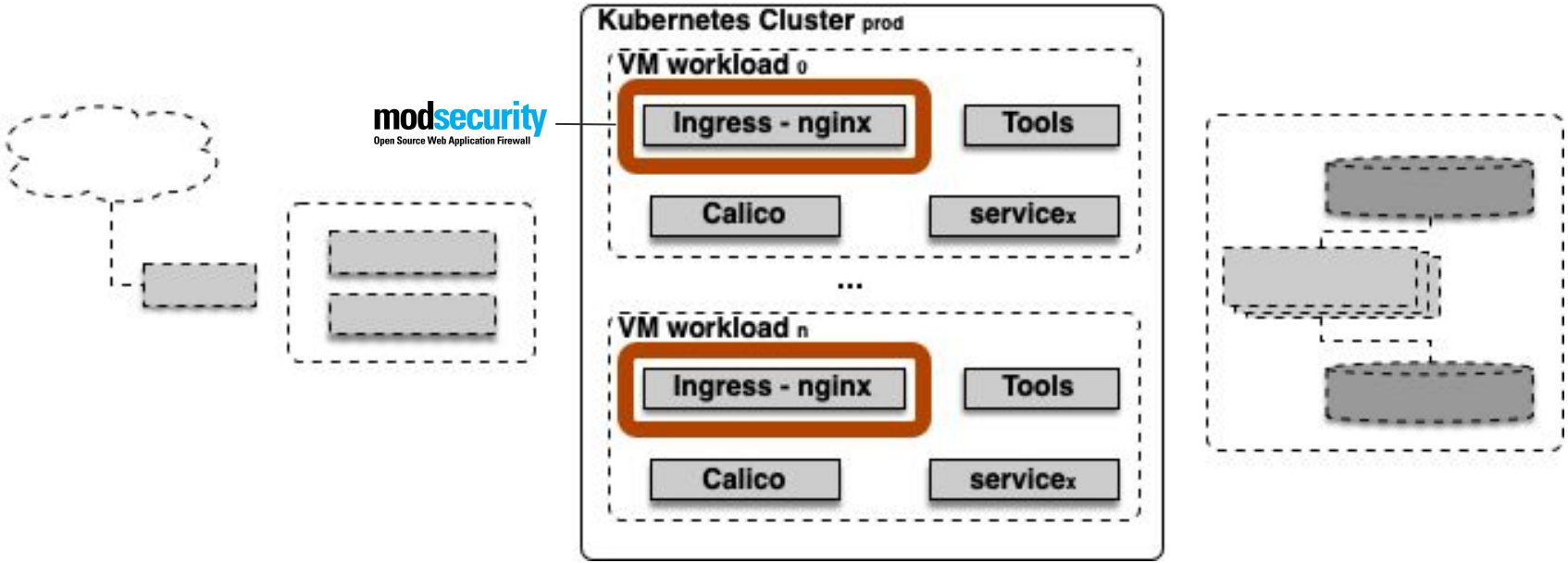
Screenshot

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

~275M transactions
~8,3M citizens
20K r/s
~6500 doc/min
~100 docs/sec

10 days with the highest traffic during COVID-19




modsecurity
Open Source Web Application Firewall
Kubernetes Cluster prod
VM workload 0
Ingress - nginx
Tools
Calico
servicex
...
VM workload n
Ingress - nginx
Tools
Calico
servicex

ModSecurity benefits

- well-established Web Application Firewall (WAF)
- OWASP (Open Web Application Security Project) Core Rule Set
- allows for a service-specific rule set
- effective

elastic

Search Elastic

Dashboard / [astack0-prod] WAF

Full screen | Share | Clone | Edit

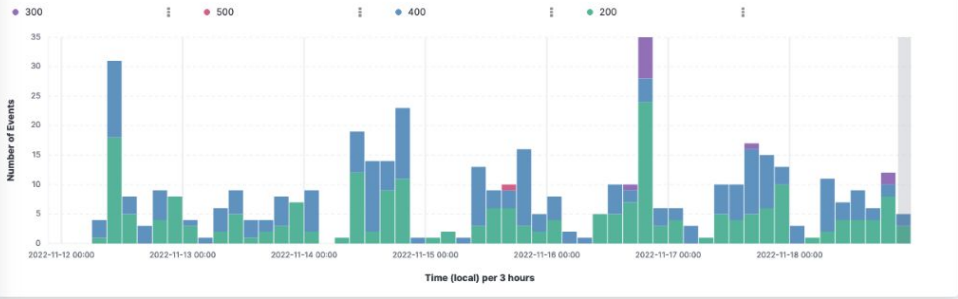
Search | KQL | Last 1 week | Show dates | Refresh

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

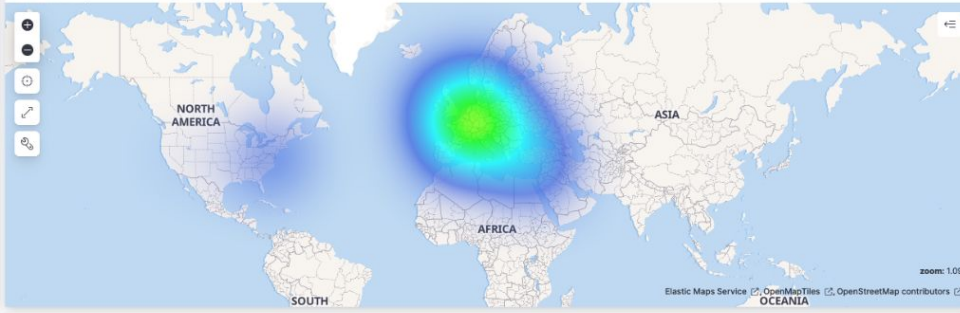
NOT client.geo.country_name: Greece ×

+ Add filter

Events by Response Code



Clients Heat Map



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	202

Screenshot

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

Infrastructure evolution

1.5TB Storage

100 Pods

25 Services

30 VMs

10 BMSs

50TB Storage

900 Pods

200 Services

150 VMs

50 BMSs

Experiences from production

- our architecture allows for multiple deployments per day, even with thousands of users connected
- we can respond to changing conditions quickly and minimize the impact of an issue by swiftly implementing and deploying a solution
- by carefully monitoring different metrics such as request / response times, success rates and more, we are able to tune parameters including the number of container pods and database connection timeouts, to keep the system from reaching several bottlenecks
- our infrastructure setup enabled us to keep all services up and running during a 48-hour data center shutdown that occurred due to extensive electrical work

work in progress

(more OSS)

Image scanning for vulnerabilities

aqua

trivy

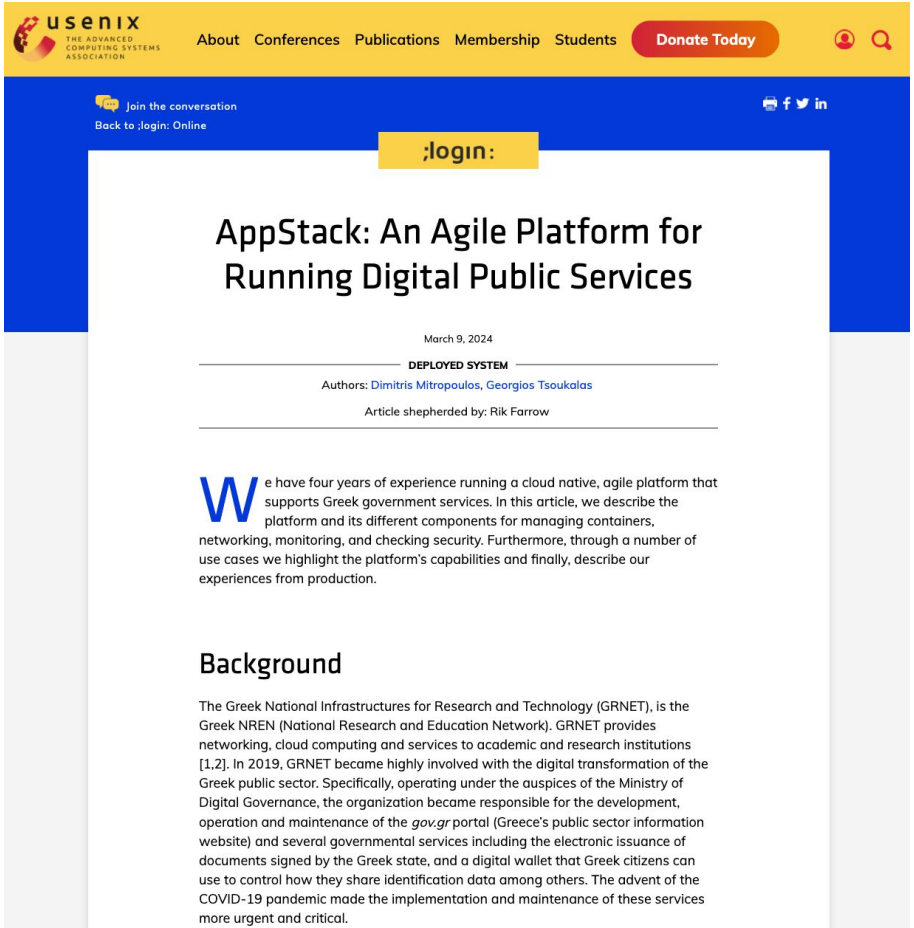
Static Application Security Testing (SAST)

Evaluating linters for K8 resources

KubeLinter

Recap

- *AppStack*: a CI/CD, cloud-native approach for the development and operation of *gov.gr* services
- an enabling environment for integrating *open-source software* components
- in this context, DevOps can address *reliability* and *security* challenges by incorporating suitable OSS tools such as scalability mechanisms and firewalls
- OSS-based internship potential



https://www.usenix.org/publications/loginonline/appstack-agile-platform-running-digital-public-services

thank you!

(questions?)