04-800K: AIOps: Continuous and Automated IT and AI Monitoring

Assynath Thompson Mlay, amlaytho

MSIT 2025

Lab 7: From anomaly detection to incidents

Lab Preparations:

Creating Clusters

Figure 1: Creating a cluster.

```
istio-gateway-istio     LoadBalancer   34.118.239.246   <pending>     15021:31877/TCP,80:30610/TCP   8s
kubernetes              ClusterIP      34.118.224.1     <none>        443/TCP                        31m
paymentservice          ClusterIP      34.118.226.219   <none>        50051/TCP                      18s
productcatalogservice   ClusterIP      34.118.232.88    <none>        3550/TCP                       18s
recommendationservice   ClusterIP      34.118.237.132   <none>        8080/TCP                       17s
redis-cart              ClusterIP      34.118.229.247   <none>        6379/TCP                       17s
shippingservice         ClusterIP      34.118.233.49    <none>        50051/TCP                      16s
serviceaccount/grafana created
configmap/grafana created
service/grafana created
deployment.apps/grafana created
configmap/istio-grafana-dashboards created
configmap/istio-services-grafana-dashboards created
deployment.apps/jaeger created
service/tracing created
service/zipkin created
service/jaeger-collector created
serviceaccount/kiali created
configmap/kiali created
clusterrole.rbac.authorization.k8s.io/kiali created
clusterrolebinding.rbac.authorization.k8s.io/kiali created
role.rbac.authorization.k8s.io/kiali-controlplane created
rolebinding.rbac.authorization.k8s.io/kiali-controlplane created
service/kiali created
deployment.apps/kiali created
serviceaccount/loki created
configmap/loki created
configmap/loki-runtime created
service/loki-memberlist created
service/loki-headless created
service/loki created
statefulset.apps/loki created
serviceaccount/prometheus created
configmap/prometheus created
clusterrole.rbac.authorization.k8s.io/prometheus created
clusterrolebinding.rbac.authorization.k8s.io/prometheus created
service/prometheus created
deployment.apps/prometheus created
NAME                    TYPE           CLUSTER-IP       EXTERNAL-IP     PORT(S)                                                                    AGE
grafana                 ClusterIP      34.118.236.236   <none>          3000/TCP                                                                   26s
istio-egressgateway     ClusterIP      34.118.239.226   <none>          80/TCP,443/TCP                                                             2m39s
istio-ingressgateway    LoadBalancer   34.118.234.218   34.134.184.94   15021:31203/TCP,80:30392/TCP,443:30376/TCP,31400:32669/TCP,15443:31123/TCP   5m56s
istiod                  ClusterIP      34.118.228.39    <none>          15010/TCP,15012/TCP,443/TCP,15014/TCP                                      6m7s
jaeger-collector        ClusterIP      34.118.226.13    <none>          14268/TCP,14250/TCP,9411/TCP,4317/TCP,4318/TCP                             19s
kiali                   ClusterIP      34.118.230.5     <none>          20001/TCP,9090/TCP                                                         14s
loki                    ClusterIP      34.118.228.196   <none>          3100/TCP,9095/TCP                                                          8s
loki-headless           ClusterIP      None             <none>          3100/TCP                                                                   9s
loki-memberlist         ClusterIP      None             <none>          7946/TCP                                                                   9s
prometheus              LoadBalancer   34.118.225.173   <pending>       9090:30475/TCP                                                             3s
tracing                 ClusterIP      34.118.231.222   <none>          80/TCP,16685/TCP                                                           20s
zipkin                  ClusterIP      34.118.226.218   <none>          9411/TCP                                                                   20s
```

Figure 2: Cluster being deployed with services.

```
NAME                TYPE           CLUSTER-IP      EXTERNAL-IP    PORT(S)                                                                      AGE
grafana             ClusterIP      34.118.236.236  <none>         3000/TCP                                                                     26s
istio-egressgateway ClusterIP      34.118.239.226  <none>         80/TCP,443/TCP                                                               2m39s
istio-ingressgateway LoadBalancer  34.118.234.218  34.134.184.94  15021:31203/TCP,80:30392/TCP,443:30376/TCP,31400:32669/TCP,15443:31123/TCP   5m56s
istiod              ClusterIP      34.118.228.39   <none>         15010/TCP,15012/TCP,443/TCP,15014/TCP                                        6m7s
jaeger-collector    ClusterIP      34.118.226.13   <none>         14268/TCP,14250/TCP,9411/TCP,4317/TCP,4318/TCP                               19s
kiali               ClusterIP      34.118.230.5    <none>         20001/TCP,9090/TCP                                                           14s
loki                ClusterIP      34.118.228.196  <none>         3100/TCP,9095/TCP                                                            8s
loki-headless       ClusterIP      None            <none>         3100/TCP                                                                     9s
loki-memberlist     ClusterIP      None            <none>         7946/TCP                                                                     9s
prometheus          LoadBalancer   34.118.225.173  <pending>      9090:30475/TCP                                                               3s
tracing             ClusterIP      34.118.231.222  <none>         80/TCP,16685/TCP                                                             20s
zipkin              ClusterIP      34.118.226.218  <none>         9411/TCP                                                                     20s
```

Figure 3: Cluster created successfully.

Lab Task1: Train a Prophet model with seasonality for normal operation.

```
current users = 150
last_target_users = 150
run time = 3272.716132015
current users = 150
last_target_users = 150
run time = 3273.716502432
current users = 150
last_target_users = 150
run time = 3274.717503553
current users = 150
last_target_users = 150
run time = 3275.7177619740005
current users = 150
last_target_users = 150
run time = 3276.718627739
current users = 150
last_target_users = 150
run time = 3277.7191158699998
current users = 150
last_target_users = 150
run time = 3278.7195555510007
current users = 150
last_target_users = 150
```

Figure 4: Running Locust

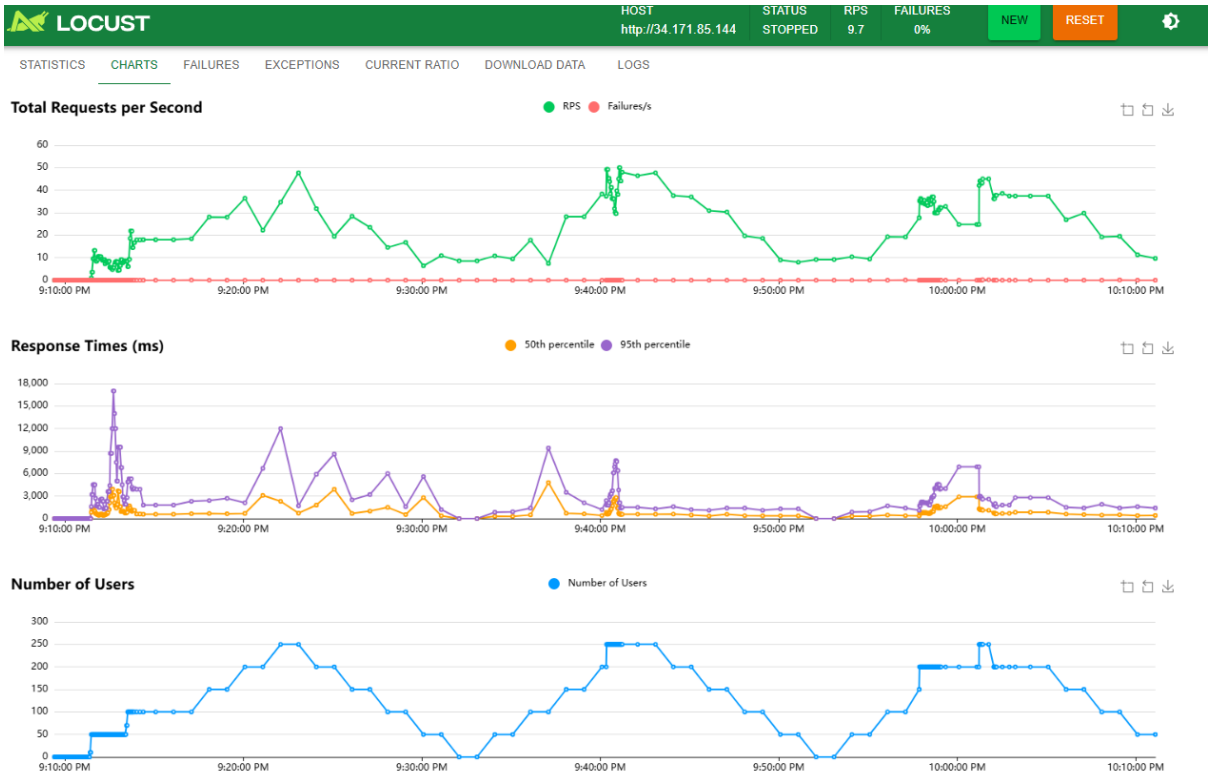


Figure 5: Charts viewed on Locust.

```
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ docker push assynath/newmonitorapp:latest
The push refers to repository [docker.io/assynath/newmonitorapp]
7f64aad4d977: Pushed
54e2c53dc51a: Pushed
bb3546cd9163: Pushed
d64122b2e44b: Pushed
ad05cdcb59cd: Mounted from library/python
3a9ca0e18fd5: Mounted from library/python
42ca3c4e0243: Mounted from library/python
c0f1022b22a9: Mounted from library/python
latest: digest: sha256:ada56ee33e4bf99563b0a0dd34144dccc3a6a8d2bc493401bd3d46ae3da0085d size: 1998
```

Figure 6: After modifying the monitor app Pushing on docker hub.

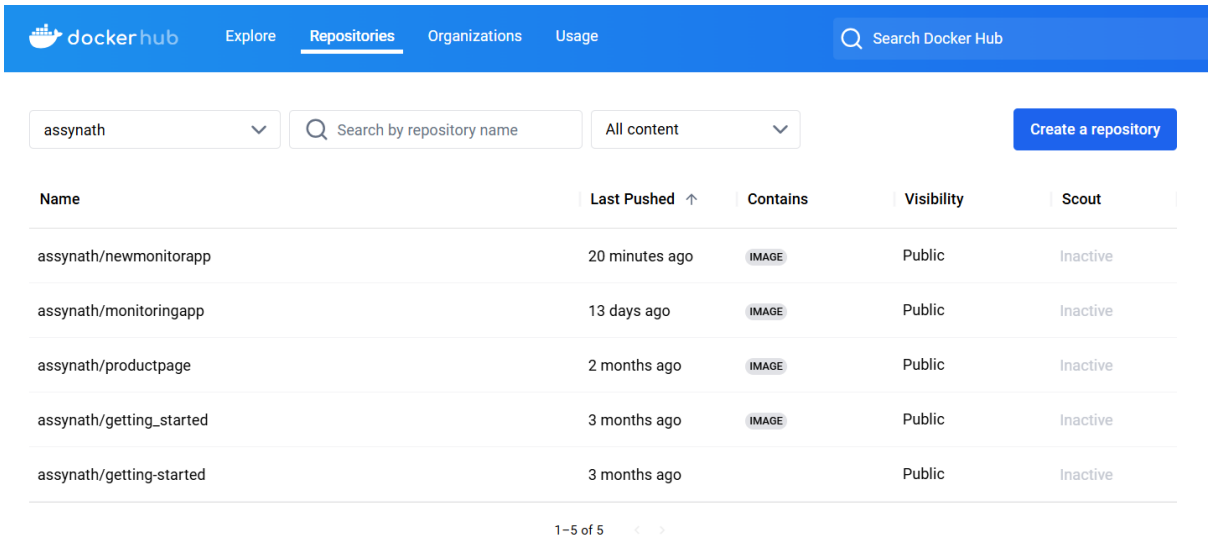


Figure 7: Pushed on dockerhub.

```
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ docker build -t assynath/newmonitorapp:latest .
[+] Building 490.7s (11/14)
 => [internal] load build definition from Dockerfile
 => => transferring dockerfile: 619B
 => [internal] load metadata for docker.io/library/python:3.11-slim
 => [auth] library/python:pull token for registry-1.docker.io
 => [internal] load .dockerignore
 => => transferring context: 2B
 => [1/5] FROM docker.io/library/python:3.11-slim@sha256:370c586a6ffc8c619e6d652f81c094b34b14b8f2fb9251f092de23f16e299b78
 => CACHED [2/5] WORKDIR /app
 => [internal] load build context
 => => transferring context: 2.57MB
 => [3/5] COPY . /app
 => [4/5] RUN pip install --no-cache-dir -r requirements.txt
 => [5/5] RUN sed -i 's/np.float_/np.float64/g' $(pip show prophet | grep Location | cut -d' ' -f2)/prophet/forecaster.py
 => exporting to image
 => => exporting layers
 => => writing image sha256:398fcf524d084d589b6e7063ffe7082410bc25371608b79c917afaa38690db87
 => => naming to docker.io/assynath/newmonitorapp:latest
```

Figure 8: Dockerizing the image.

```
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ kubectl apply -f monskeleton_deploy_template.yaml
deployment.apps/monskeletondeploy created
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ kubectl get deployments
NAME                    READY   UP-TO-DATE   AVAILABLE   AGE
adservice               1/1     1            1           4h16m
cartservice             1/1     1            1           4h16m
checkoutservice         1/1     1            1           4h16m
currencyservice         1/1     1            1           4h16m
emailservice            1/1     1            1           4h16m
frontend                1/1     1            1           4h16m
istio-gateway-istio     1/1     1            1           4h16m
loadgenerator           0/0     0            0           4h16m
monskeletondeploy       0/0     0            0           3m2s
paymentservice          1/1     1            1           4h16m
productcatalogservice   1/1     1            1           4h16m
recommendationservice   1/1     1            1           4h16m
redis-cart              1/1     1            1           4h16m
shippingservice         1/1     1            1           4h16m
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ kubectl scale deployment monskeletondeploy --replicas=1
deployment.apps/monskeletondeploy scaled
```

Figure 9: Scaling the monskeleton.

```
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ kubectl get deployments
NAME                    READY   UP-TO-DATE   AVAILABLE   AGE
adservice               1/1     1            1           4h56m
cartservice             1/1     1            1           4h56m
checkoutservice         1/1     1            1           4h56m
currencyservice         1/1     1            1           4h56m
emailservice            1/1     1            1           4h56m
frontend                1/1     1            1           4h56m
istio-gateway-istio     1/1     1            1           4h56m
loadgenerator           0/0     0            0           4h56m
monskeletondeploy       1/1     1            1           42m
paymentservice          1/1     1            1           4h56m
productcatalogservice   1/1     1            1           4h56m
recommendationservice   1/1     1            1           4h56m
redis-cart              1/1     1            1           4h56m
shippingservice         1/1     1            1           4h56m
```

Figure 10: Monskeleton has been scaled.

```
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ kubectl get pods
NAME                                    READY   STATUS    RESTARTS   AGE
adservice-64586ccfb9-9tlbz              2/2     Running   0          4h23m
cartservice-6bd5c944b4-6bbs4            2/2     Running   0          4h23m
checkoutservice-6d4bcd6f95-6nwcn        2/2     Running   0          4h23m
currencyservice-f987888c-bvt8w          2/2     Running   0          4h23m
emailservice-56fbcfbbf7-f9vjr           2/2     Running   0          4h23m
frontend-cb9967686-sdbxs                2/2     Running   0          4h23m
istio-gateway-istio-657cb6db8f-62f8w    1/1     Running   0          4h23m
monskeletondeploy-5c786ddcc4-htmk7      2/2     Running   0          5m11s
paymentservice-794b5dfdf7-9lcqz         2/2     Running   0          4h23m
productcatalogservice-74b4c878d5-gnx5r  2/2     Running   0          4h23m
recommendationservice-65dd5bd87c-qp4zg  2/2     Running   0          4h23m
redis-cart-7ff8f4d6ff-ztd92             2/2     Running   0          4h23m
shippingservice-699bcb7fd5-8pkqm        2/2     Running   0          4h23m
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ kubectl logs monskeletondeploy-5c786ddcc4-htmk7
21:59:13 - cmdstanpy - INFO - Chain [1] start processing
21:59:13 - cmdstanpy - INFO - Chain [1] done processing
Actual value: nan
Predicted value: 3.0811769499520683
```

Figure 11: Getting the logs for the monskeleton.

```
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ kubectl logs monskeletondeploy-5c786ddcc4-44q6h
22:37:04 - cmdstanpy - INFO - Chain [1] start processing
22:37:04 - cmdstanpy - INFO - Chain [1] done processing
Actual value: 3.0330578512396693
Predicted value: 3.081176968743822
+-----------------------------+-------------+-----------+-----------+
| Timestamp                   |   Anomalies |       MAE |      MAPE |
+=============================+=============+===========+===========+
| 2024-12-09 22:37:04.839168 |           0 | 0.0481191 | 0.0158649 |
+-----------------------------+-------------+-----------+-----------+
Actual value: 3.0517241379310343
Predicted value: 3.0853101633426574
+-----------------------------+-------------+-----------+-----------+
| Timestamp                   |   Anomalies |       MAE |      MAPE |
+=============================+=============+===========+===========+
| 2024-12-09 22:37:04.839168 |           0 | 0.0481191 | 0.0158649 |
+-----------------------------+-------------+-----------+-----------+
| 2024-12-09 22:38:04.890523 |           0 | 0.033586  | 0.0110056 |
+-----------------------------+-------------+-----------+-----------+
```

Figure 12: Logs from the Monskeleton

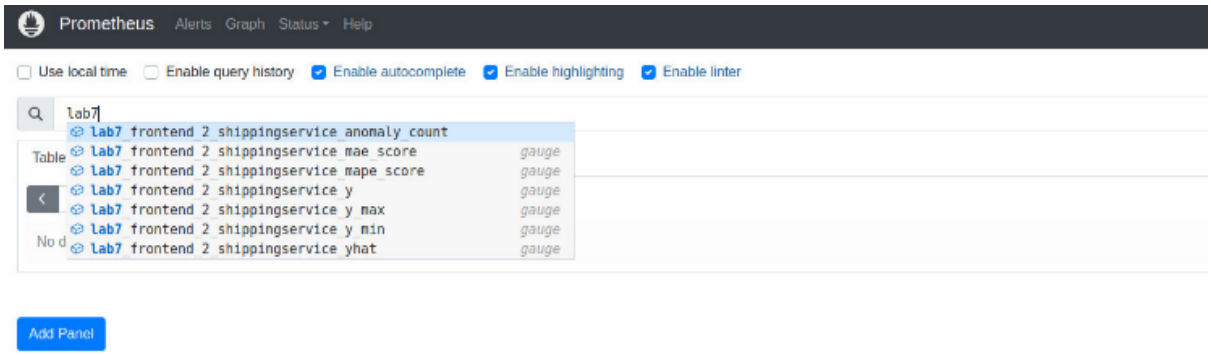
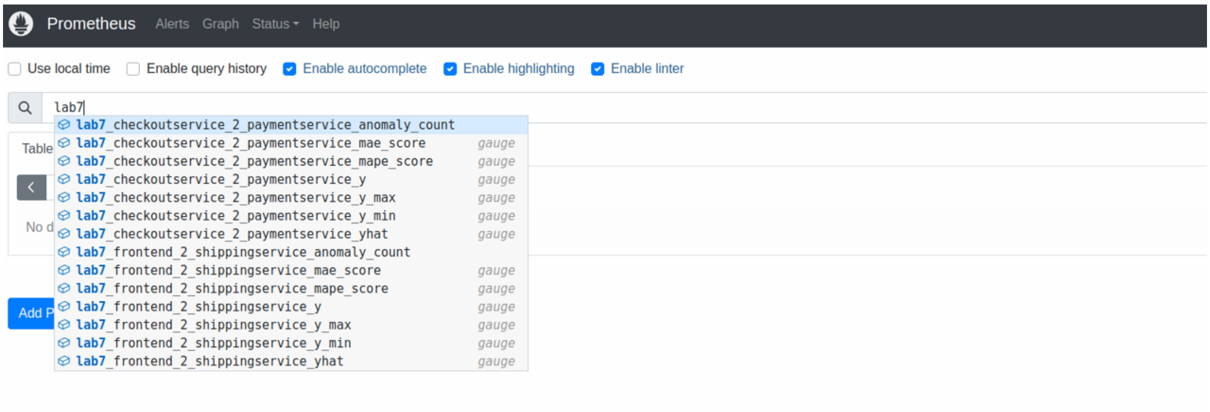


Figure 13: New metrics on Prometheus.

Lab Task2: Train and deploy anomaly monitors for 2 selected services.



Lab Task3: Implement an Incident detection monitor consuming 2 anomaly metrics.

```
Error fetching data from Prometheus: list index out of range
Frontend --> ProductCatalogService Anomaly Count: 0.0
Frontend --> Shipping Anomaly Count: 0
No Incident detected. Total temperature: 0
Service frontend to productcatalogservice: 0,  Service frontend to shipping: 0, Total Temperature: 0
Error fetching data from Prometheus: list index out of range
Frontend --> ProductCatalogService Anomaly Count: 0.0
Frontend --> Shipping Anomaly Count: 0
No Incident detected. Total temperature: 0
Service frontend to productcatalogservice: 0,  Service frontend to shipping: 0, Total Temperature: 0
Error fetching data from Prometheus: list index out of range
Frontend --> ProductCatalogService Anomaly Count: 0.0
Frontend --> Shipping Anomaly Count: 0
No Incident detected. Total temperature: 0
Service frontend to productcatalogservice: 0,  Service frontend to shipping: 0, Total Temperature: 0
Error fetching data from Prometheus: list index out of range
Frontend --> ProductCatalogService Anomaly Count: 0.0
Frontend --> Shipping Anomaly Count: 0
No Incident detected. Total temperature: 0
Service frontend to productcatalogservice: 0,  Service frontend to shipping: 0, Total Temperature: 0
```

```
2024-12-09 12:00:05 - INFO - Starting Prometheus metrics server on port 8098
2024-12-09 12:00:05 - ERROR - Error fetching data from Prometheus: list index out of range
2024-12-09 12:00:05 - INFO - Frontend --> ProductCatalogService Anomaly Count: 0.0
2024-12-09 12:00:05 - INFO - Frontend --> Shipping Anomaly Count: 0
2024-12-09 12:00:05 - INFO - No Incident detected. Total temperature: 0
2024-12-09 12:00:05 - INFO - Service frontend to productcatalogservice: 0, Service frontend to shipping: 0, Total
 Temperature: 0
```

Figure 14: After pushing the docker image.

Lab Task4: Detect Istio-generated raw anomalies and triggered incidents

```
INFO:__main__:Started incident detector on port 8002
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 1, Active Services: 1, Status: NORMAL, Accumulators: {'frontend_shipping': 1, 'checkout_payment': 0}
INFO:__main__:Temperature: 2, Active Services: 1, Status: NORMAL, Accumulators: {'frontend_shipping': 2, 'checkout_payment': 0}
INFO:__main__:Temperature: 4, Active Services: 2, Status: NORMAL, Accumulators: {'frontend_shipping': 2, 'checkout_payment': 2}
INFO:__main__:Temperature: 6, Active Services: 2, Status: SEV1, Accumulators: {'frontend_shipping': 3, 'checkout_payment': 3}
INFO:__main__:Temperature: 8, Active Services: 2, Status: SEV1, Accumulators: {'frontend_shipping': 4, 'checkout_payment': 4}
INFO:__main__:Temperature: 8, Active Services: 2, Status: SEV1, Accumulators: {'frontend_shipping': 4, 'checkout_payment': 4}
INFO:__main__:Temperature: 8, Active Services: 2, Status: SEV1, Accumulators: {'frontend_shipping': 4, 'checkout_payment': 4}
```

Figure 15: Sev1

```
INFO:__main__:Started incident detector on port 8002
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 0, Active Services: 0, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 0}
INFO:__main__:Temperature: 1, Active Services: 1, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 1}
INFO:__main__:Temperature: 2, Active Services: 1, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 2}
INFO:__main__:Temperature: 3, Active Services: 1, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 3}
INFO:__main__:Temperature: 4, Active Services: 1, Status: NORMAL, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 4}
INFO:__main__:Temperature: 5, Active Services: 1, Status: SEV2, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 5}
INFO:__main__:Temperature: 5, Active Services: 1, Status: SEV2, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 5}
INFO:__main__:Temperature: 5, Active Services: 1, Status: SEV2, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 5}
INFO:__main__:Temperature: 5, Active Services: 1, Status: SEV2, Accumulators: {'frontend_shipping': 0, 'checkout_payment': 5}
```

Figure 16: Sev2

Lab Task5: Train and deploy anomaly monitors for 2 selected services.

Sudden increases in user activity can lead to anomalies and potential incidents. Transient load testing helps manage these situations. Reducing response time can resolve issues faster.

The test simulated temporary spikes in user activity:

Two spikes occurred within 20 minutes

First spike: 500 users for 1-2 minutes, starting at 5 minutes

Second spike: 2000 users for 5-6 minutes, starting at 15 minutes

The system handled short spikes well:

Anomaly detectors responded to increased load

Accumulators rose during spikes but didn't trigger false alarms

After spikes, accumulators gradually returned to normal

No Sev 1 (both services affected) or Sev 2 (one service affected) incidents occurred during brief spikes

This shows the system can distinguish between short-term issues and real problems, avoiding unnecessary alerts.

```
asnath@AssynathJr:~/AIOps_Labs/Lab7/Lab7$ locust --host="http://34.116.186.33" -f locustfile_step_transient_new.py --web-port 8090 --headless -u 250 -r 100 --run-time 20m
```

```
2024-12-10 06:42:49 - INFO - Shipping Anomalies: 98,
productcatalog Anomalies: 4
2024-12-10 06:42:49 - INFO - Total Temperature: 102,
Severity: Severity 1 Incident
+--------------------+----------------------+
| Metric             | Value                |
+====================+======================+
| Shipping           | 98                   |
+--------------------+----------------------+
| productcatalog     | 4                    |
+--------------------+----------------------+
| Total Temperature | 102                   |
+--------------------+----------------------+
| Severity           | Severity 1 Incident |
+--------------------+----------------------+
2024-12-10 06:43:49 - INFO - Shipping Anomalies: 99,
productcatalog Anomalies: 2
2024-12-10 06:43:49 - INFO - Total Temperature: 101,
Severity: Severity 1 Incident
+--------------------+----------------------+
| Metric             | Value                |
+====================+======================+
| Shipping           | 99                   |
+--------------------+----------------------+
| productcatalog     | 2                    |
+--------------------+----------------------+
| Total Temperature | 101                   |
+--------------------+----------------------+
| Severity           | Severity 1 Incident |
+--------------------+----------------------+
```

Figure 17: Transient changes

```
+---------------------------------+-------------+
| Metric                          | Value       |
+=================================+=============+
| lab7_frontend_2_productcatalog  | 0           |
+---------------------------------+-------------+
| lab7_frontend_2_shippingservice | 2           |
+---------------------------------+-------------+
| Total Temperature               | 2           |
+---------------------------------+-------------+
| Severity                        | No Incident |
+---------------------------------+-------------+
+---------------------------------+-------------+
| Metric                          | Value       |
+=================================+=============+
| lab7_frontend_2_productcatalog  | 0           |
+---------------------------------+-------------+
| lab7_frontend_2_shippingservice | 2           |
+---------------------------------+-------------+
| Total Temperature               | 2           |
+---------------------------------+-------------+
| Severity                        | No Incident |
+---------------------------------+-------------+
2024-12-10 08:00:07 - INFO - Querying Prometheus for lab7_frontend_2_productcatalog: sum(lab7_frontend_2_
```

Figure 18: Transient Applied

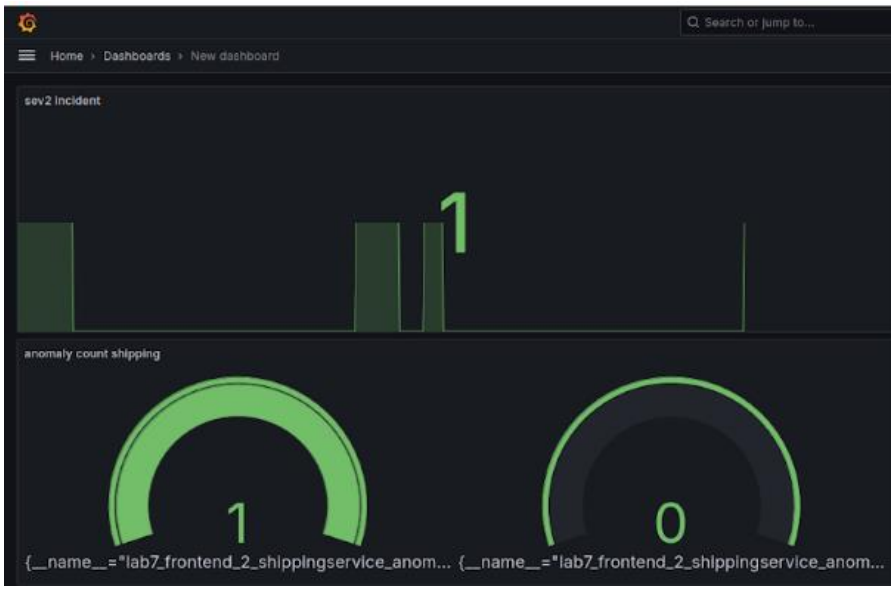
Timestamp	Anomalies	MAE	MAPE
2024-12-10 07:56:48.305273	0	0.0560018	0.0169703
2024-12-10 07:57:48.454026	1	13.4583	0.800223
2024-12-10 07:58:48.589895	1	9.50858	0.738683
2024-12-10 07:59:48.714058	0	0.330603	0.108857
2024-12-10 08:00:48.851003	0	0.0878307	0.0267476
2024-12-10 08:01:48.984744	0	0.214204	0.0677604
2024-12-10 08:02:49.141073	0	0.419466	0.110422
2024-12-10 08:03:49.267913	0	0.702936	0.172031
2024-12-10 08:04:49.409718	1	1.36845	0.287763
2024-12-10 08:05:49.563195	1	1.58847	0.319009
2024-12-10 08:06:49.738663	1	8.92663	0.72448

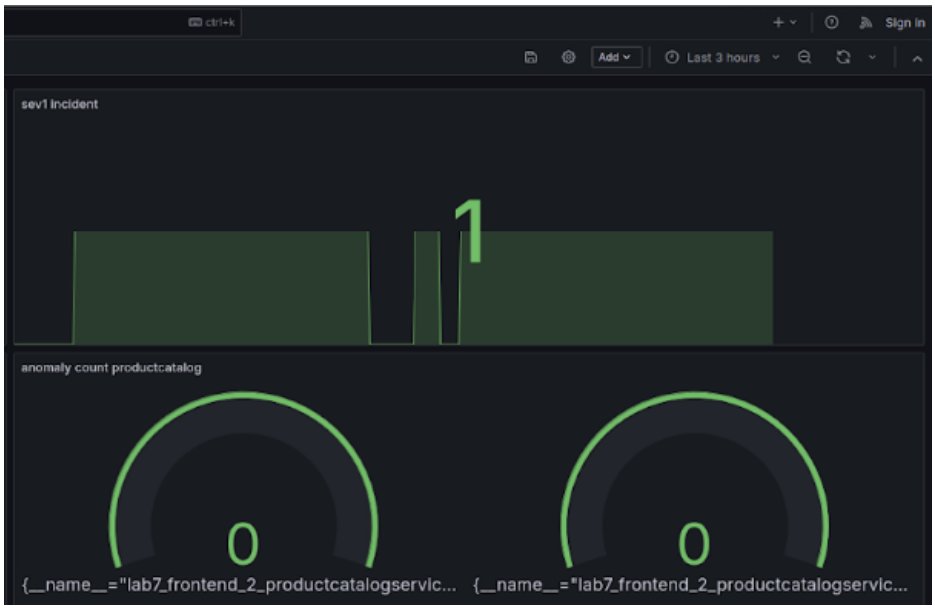
2024-12-10 08:29:11,942 - INFO - Actual value: 8.752244165170557, Predicted value: 3.4801290620292218

Timestamp	Anomalies	MAE	MAPE
2024-12-10 07:56:07.507875	1	1.37734	0.291225
2024-12-10 07:57:07.642889	1	14.7978	0.815135
2024-12-10 07:58:07.765937	1	36.5387	0.915789
2024-12-10 07:59:07.890923	1	1.60225	0.322643
2024-12-10 08:00:08.028545	0	0.0396201	0.011905
2024-12-10 08:01:08.158877	0	0.0278542	0.00819392
2024-12-10 08:02:08.292720	0	0.323105	0.087361
2024-12-10 08:03:08.440746	1	1.39299	0.291893
2024-12-10 08:04:08.567073	1	3.52072	0.509963
2024-12-10 08:05:08.702048	1	6.19746	0.646613

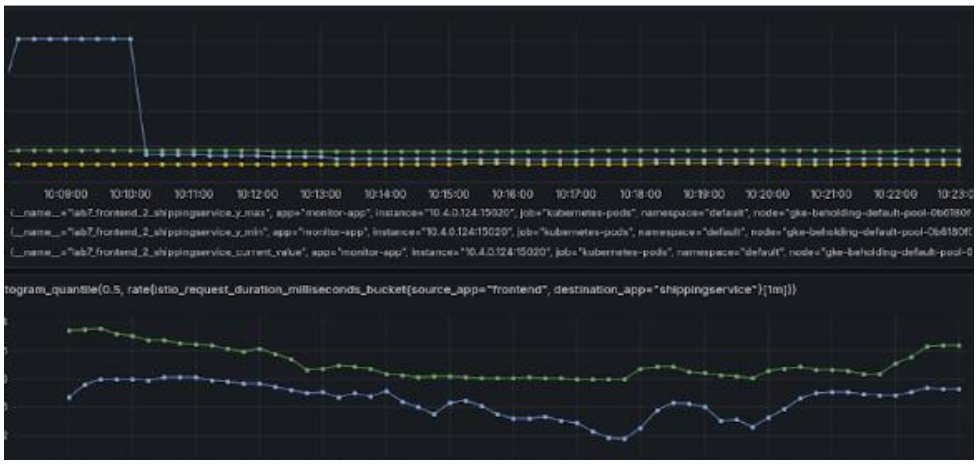
Figure 19: Transient changes anomalies in two services

Lab Task6


Search or jump to...
Home › Dashboards › New dashboard
sev2 incident
1
anomaly count shipping
1
0
{__name__="lab7_frontend_2_shippingservice_anom...
{__name__="lab7_frontend_2_shippingservice_anom...


ctrl+k
Sign in
Add
Last 3 hours
sev1 incident
1
anomaly count productcatalog
0
0
{__name__="lab7_frontend_2_productcatalogservic...
{__name__="lab7_frontend_2_productcatalogservic...


y, ymin, ymax productcatalog
20000
15000
10000
5000
0
histogram_quantile(0.5, rate(istio_request_duration_milliseconds_bucket{source_app="frontend", destination_app="productcatalogservice"}[1m]))
20000
15000
10000
5000
0



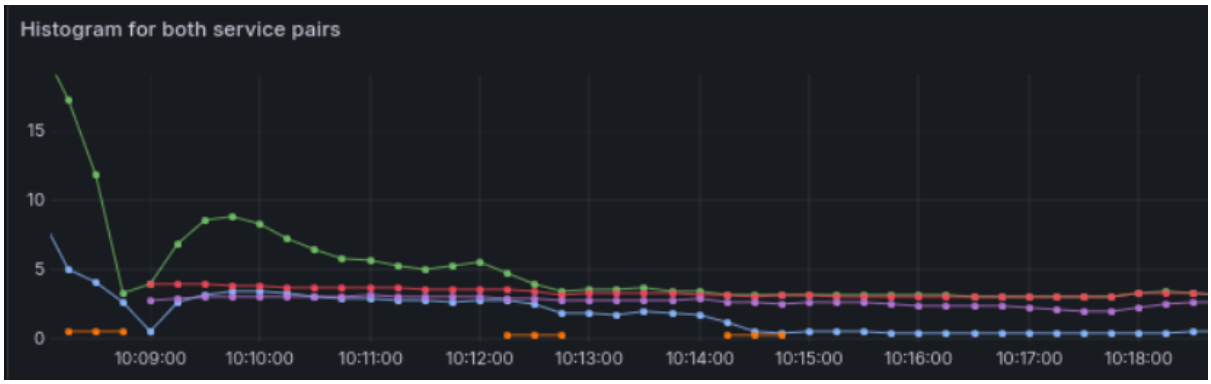


Figure 20: MAPE gauge