Gospel Alerts with Prometheus and Grafana alerting engines

Setting up alerting in Prometheus

Docs used

Setting up Prometheus with Slack

https://boxboat.com/2019/08/08/monitoring-kubernetes-with-prometheus/

Prometheus alerts queries

https://awesome-prometheus-alerts.grep.to/rules.html

Sample **values.yaml** file with one alert and Slack integration for a helm upgrade

```
serverFiles:
  alerts:
    groups:
      - name: Instances
        rules:
          - alert: InstanceDown
            expr: up == 0
            for: 1m
            labels:
              severity: page
            annotations:
              description: '{{ $labels.instance }} of job {{ $labels.job
}} has been down for more than 1 minute.'
              summary: 'Instance {{ $labels.instance }} down'
alertmanagerFiles:
  alertmanager.yml:
    route:
      receiver: slack-gospel

    receivers:
      - name: slack-gospel
        slack_configs:
         - channel: '#alerts'
           api_url:
'https://hooks.slack.com/services/T3FRMH99U/BU0NJFQ77/JxCghWgZ7TEhRN1913
mp0hM6'
           send_resolved: true
```

Sample upgrade command in the prometheus namespace

```
helm upgrade -f <location_of_the_file>/values.yaml prometheus
stable/prometheus
```

Recommended alerts for Gospel admins

Node Exporter

- **Out of memory**

```
- alert: OutOfMemory
  expr: node_memory_MemAvailable_bytes / node_memory_MemTotal_bytes *
100 < 10
  for: 5m
  labels:
    severity: page
  annotations:
    summary: "Out of memory (instance {{ $labels.instance }})"
    description: "Node memory is filling up (< 10% left)\n  VALUE = {{
$value }}\n  LABELS: {{ $labels }}"
```

- **Out of disk space**

```
- alert: OutOfDiskSpace
  expr: node_filesystem_avail_bytes* 100/ node_filesystem_size_bytes <
10
  for: 5m
  labels:
    severity: page
  annotations:
    summary: "Out of disk space (instance {{ $labels.instance }})"
    description: "Disk is almost full (< 10% left)\n  VALUE = {{ $value
}}\n  LABELS: {{ $labels }}"
```

- **Disk will fill in 4 hours**

```
- alert: DiskWillFillIn4Hours
  expr: predict_linear(node_filesystem_free_bytes{fstype!~"tmpfs"}[1h],
4 * 3600) < 0
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Disk will fill in 4 hours (instance {{ $labels.instance
}})"
    description: "Disk will fill in 4 hours at current write rate\n
VALUE = {{ $value }}\n  LABELS: {{ $labels }}"
```

- **High CPU load**

```
- alert: HighCpuLoad
  expr: 100 - (avg by(instance)
(irate(node_cpu_seconds_total{mode="idle"}[5m])) * 100) > 80
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "High CPU load (instance {{ $labels.instance }})"
    description: "CPU load is > 80%\n  VALUE = {{ $value }}\n  LABELS:
{{ $labels }}"
```

- **Out of inodes**

```
- alert: OutOfInodes
  expr: node_filesystem_files_free{mountpoint ="/"} /
node_filesystem_files{mountpoint ="/"} * 100 < 10
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Out of inodes (instance {{ $labels.instance }})"
    description: "Disk is almost running out of available inodes (< 10%
left)\n  VALUE = {{ $value }}\n  LABELS: {{ $labels }}"
```

- **Unusual network throughput in**

```
- alert: UnusualNetworkThroughputIn
  expr: sum by (instance) (irate(node_network_receive_bytes_total[2m]))
/ 1024 / 1024 > 100
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Unusual network throughput in (instance {{
$labels.instance }})"
    description: "Host network interfaces are probably receiving too
much data (> 100 MB/s)\n  VALUE = {{ $value }}\n  LABELS: {{ $labels }}"
```

- **Unusual network throughput out**

```
- alert: UnusualNetworkThroughputOut
  expr: sum by (instance) (irate(node_network_transmit_bytes_total[2m]))
/ 1024 / 1024 > 100
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Unusual network throughput out (instance {{
$labels.instance }})"
    description: "Host network interfaces are probably sending too much
data (> 100 MB/s)\n  VALUE = {{ $value }}\n  LABELS: {{ $labels }}"
```

- **Unusual disk read rate**

```
- alert: UnusualDiskReadRate
  expr: sum by (instance) (irate(node_disk_read_bytes_total[2m])) / 1024
/ 1024 > 50
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Unusual disk read rate (instance {{ $labels.instance }})"
    description: "Disk is probably reading too much data (> 50 MB/s)\n
VALUE = {{ $value }}\n  LABELS: {{ $labels }}"
```

- **Unusual disk write rate**

```
- alert: UnusualDiskWriteRate
  expr: sum by (instance) (irate(node_disk_written_bytes_total[2m])) /
1024 / 1024 > 50
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Unusual disk write rate (instance {{ $labels.instance }})"
    description: "Disk is probably writing too much data (> 50 MB/s)\n
VALUE = {{ $value }}\n  LABELS: {{ $labels }}"
```

- **Kubernetes PersistentVolumeClaim pending**

```
- alert: KubernetesPersistentvolumeclaimPending
  expr: kube_persistentvolumeclaim_status_phase{phase="Pending"} == 1
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Kubernetes PersistentVolumeClaim pending (instance {{
$labels.instance }})"
    description: "PersistentVolumeClaim {{ $labels.namespace }}/{{
$labels.persistentvolumeclaim }} is pending\n  VALUE = {{ $value }}\n
LABELS: {{ $labels }}"
```

- **Stateful set has x number of replicas down for more than 5 minutes**

```
- alert: StatefulsetDown
  expr: (kube_deployment_spec_replicas/
kube_deployment_status_replicas_available) != 1
  for: 5m
  labels:
    severity: error
  annotations:
    summary: "StatefulSet down (instance {{ $labels.instance }})"
    description: "A StatefulSet went down\n  VALUE = {{ $value }}\n
LABELS: {{ $labels }}"
```

- **Daemon set has x number of replicas down for more than 5 minutes**

```
- alert: DaemonsetDown
  expr: (kube_daemonset_status_desired_number_scheduled/
kube_daemonset_status_number_available) != 1
  for: 5m
  labels:
    severity: page
  annotations:
    summary: "Daemonset down (instance {{ $labels.instance }})"
    description: "A Daemonset went down\n  VALUE = {{ $value }}\n
LABELS: {{ $labels }}"
```

- **Pod restarts > 1 in the space of 5 minutes - showing all pod restarts**

```
- alert: PodRestart
  expr: kube_pod_container_status_restarts_total == 1
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Pod Restart! (instance {{ $labels.instance }})"
    description: "Pod Restart! \n  VALUE = {{ $value }}\n  LABELS: {{
$labels }}"
```

?????? Are the ones below relevant for Gospel specifically? ??????

- **Prometheus exporter down - applies to all resources monitored**

```
- alert: ExporterDown
  expr: up == 0
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Exporter down (instance {{ $labels.instance }})"
    description: "Prometheus exporter down\n  VALUE = {{ $value }}\n
LABELS: {{ $labels }}"
```

- **Volume out of disk space - appears to only export for Prometheus PVCs**

```
- alert: VolumeOutOfDiskSpace
  expr: kubelet_volume_stats_available_bytes /
kubelet_volume_stats_capacity_bytes * 100 < 10
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Volume out of disk space (instance {{ $labels.instance
}})"
    description: "Volume is almost full (< 10% left)\n  VALUE = {{
$value }}\n  LABELS: {{ $labels }}"
```

- **Kubernetes OutOfDisk**

```
- alert: KubernetesOutofdisk
  expr: kube_node_status_condition{condition="OutOfDisk",status="true"}
== 1
  for: 5m
  labels:
    severity: error
  annotations:
    summary: "Kubernetes OutOfDisk (instance {{ $labels.instance }})"
    description: "{{ $labels.node }} has OutOfDisk condition\n  VALUE =
{{ $value }}\n  LABELS: {{ $labels }}"
```

- **Kubernetes PersistentVolumeClaim pending**

```
- alert: KubernetesPersistentvolumeclaimPending
  expr: kube_persistentvolumeclaim_status_phase{phase="Pending",
persistentvolumeclaim!~"gospel-efs-data"} == 1
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Kubernetes PersistentVolumeClaim pending (instance {{
$labels.instance }})"
    description: "PersistentVolumeClaim {{ $labels.namespace }}/{{
$labels.persistentvolumeclaim }} is pending\n  VALUE = {{ $value }}\n
LABELS: {{ $labels }}"
```

Setting up alerting in Grafana

I recommend this approach if you are to leverage CloudWatch metrics for creating the alerts since Grafana integrates more seamlessly with this data provider.

Docs used

Tutorial for adding Slack integration and Grafana alerts

https://www.devopsage.com/alert-notification-to-slack-from-grafana/

Main doc from Grafana

https://grafana.com/docs/grafana/latest/alerting/notifications/

Adding images with snippets from dashboards

https://grafana.com/docs/grafana/latest/alerting/notifications/#external-image-store