

Содержание

Система алармов	3
<i>Категории алармов</i>	3
<i>Полный перечень алармов (20+ правил)</i>	3
<i>Процесс обработки алармов</i>	4
<i>Особенности</i>	4

Система алармов

Категории алармов

Критичность	Алармы	Описание	Реакция
Critical	ePDG_Service_Down, ePDG_High_Attach_Failure_Rate, ePDG_PGW_Unreachable, ePDG_AAA_Unreachable, ePDG_Diameter_Watchdog_Timeout	Компонент недоступен, массовый отказ соединений, узлы недоступны	Немедленная эскалация: Email + SNMP Trap + Webhook. Повтор раз в 1 час
Warning	ePDG_High_IKEv2_Latency, ePDG_High_GTP_Latency, ePDG_High_IKEv2_Error_Rate, ePDG_High_GTP_Error_Rate, ePDG_High_Memory_Usage, ePDG_High_CPU_Usage, ePDG_Low_Disk_Space, ePDG_High_Error_Log_Rate	Деградация производительности, аномалии ресурсов	Email. Повтор раз в 4 часа. Подавляется при наличии Critical на том же компоненте

Полный перечень алармов (20+ правил)

```
flowchart LR
  AL["ePDG Alert Rules  
20+"] --> CR["Critical  
5 rules"]
  AL --> WR["Warning  
8 rules"]
  AL --> INFO["Recording  
34 rules"]
  CR --> C1["Service_Down  
availability == 0"]
  CR --> C2["Attach_Failure_Rate  
> 10%"]
  CR --> C3["PGW_Unreachable  
connection_status{s2b} == 0"]
  CR --> C4["AAA_Unreachable  
connection_status{swm} == 0"]
  CR --> C5["Diameter_Watchdog_Timeout  
watchdog_status == 0"]
  WR --> W1["High_IKEv2_Latency  
p95 > 1.0 s"]
  WR --> W2["High_GTP_Latency  
p95 > 0.5 s"]
  WR --> W3["High_IKEv2_Error_Rate  
> 5%"]
  WR --> W4["High_GTP_Error_Rate  
> 5%"]
  WR --> W5["High_Memory_Usage  
> 80%"]
  WR --> W6["High_CPU_Usage  
> 80%"]
  WR --> W7["Low_Disk_Space  
< 10%"]
  WR --> W8["High_Error_Log_Rate  
> 10/s"]
  INFO --> I1["attach_success_rate  
preaggregated"]
  INFO --> I2["p95_p99_latency  
preaggregated"]
  INFO --> I3["throughput  
preaggregated"]
```

Процесс обработки алармов

sequenceDiagram participant M as Метрика (Prometheus) participant R as Alert Rule (PromQL) participant AM as Alertmanager participant E as Email (SMTP) participant SG as SNMP Trap Gateway participant NMS as Внешняя NMS participant W as Webhook (ChatOps) M->>R: Значение превышает порог R->>R: Ожидание (for: 1-10 мин) R->>AM: Alert FIRING AM->>AM: Group by [alertname, component] AM->>AM: Inhibition check (critical подавляет warning) alt severity = critical AM->>E: Email [CRITICAL] AM->>SG: Webhook → SNMP Trap SG->>NMS: SNMP v2c Trap (OID .1.3.6.1.4.1.43823.1.2.X) AM->>W: Webhook (Telegram / PagerDuty) else severity = warning AM->>E: Email [WARNING] end Note over M,R: Метрика возвращается в норму R->>AM: Alert RESOLVED R->>SG: clear-trap (paired notification) AM->>E: Email [RESOLVED]

Особенности

- **Inhibition:** Critical-алармы автоматически подавляют Warning для того же компонента
- **Grouping:** Алармы группируются по alertname + component с 30-секундным окном
- **Dead time / Hysteresis:** параметр for от 1 до 10 минут предотвращает ложные срабатывания
- **Trap pairing:** raise/clear одновременных событий для соответствия RFC 3877 ALARM-MIB