

Как заставить предупреждения боцмана замолчать от сигнальной метки на кластере аналитики Tetration

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Настройка](#)

[Доступ к сигнальной метке](#)

[Тишина через Редактора Правила](#)

[Раздел тишины](#)

Введение

Эта статья описывает шаги в то, как заставить предупреждения Боцмана замолчать от Сигнальной метки на Кластере Аналитики Tetration.

Предварительные условия

Требования

Cisco рекомендует иметь знание этих тем:

- Боцман

Используемые компоненты

- Боцман

Общие сведения

Боцман является открытым исходным кодом, лицензируемый MIT, контролируя и система предупреждения, разработанная Exchange стека. Это имеет выразительный предметно-ориентированный язык для оценки предупреждений и создания подробных уведомлений. Это также позволяет вам протестировать свои предупреждения против истории для более быстрого опыта разработки.

Боцман интегрирован в Аналитике Tetration для передачи предупреждений к группе по поддержке - Центр технической поддержки Cisco (TAC) и команда реагирования. Предупреждения располагаются между этими категориями:

- ADM
- Пакетный двигатель
- Боцман
- Кластер
- Коллектор
- Компактор
- Двигатель данных
- Друид
- Hadoop
- Волшебный поток
- Индексатор монго
- Сеть
- Конвейер
- Сервер политик
- Датчик
- система
- Tsd
- UI
- Служитель зоопарка

Эти компоненты имеют свои собственные отдельные специализированные предупреждения, основанные прочь известных неполадок, которые происходят для компонентов индивидуально.

Настройка

Доступ к сигнальной метке

Выберите в Мониторе опцию Сигнальной метки [Предупреждения]

Default



Monitoring



 Agents 

 Hawkeye [Charts] 

 Abyss [Pipeline] 

 Sentinel [Alerts] 

 Falcon [Jobs] 

 Digger [TSD] 

 Consul [Cluster] 

% **Warning:** Это только доступно через роль Службы поддержки пользователей.

Тишина через Редактора Правил

У ботмана есть способность модифицировать правила или алгоритм, который она использует для генерации предупреждений в самой системе.

Jump to:

alert

lookup

macro

notification

template

Toggle Syntax Highlighting

Validate

```
411 # $qgraph = q("")
412 # $checkMetric = avg($q)
413 # $critThreshold = <fail if metric is greater than this threshold>
414 # $qgraph = $q
415 # macro = checkMetricWithFallingThresholdForCritAlert
416 # }
417 macro checkMetricWithFallingThresholdForCritAlert {
418   template = metricWithThreshold
419   autoClose = true
420   ignoreUnknown = true
421   crit = $checkMetric <= $critThreshold
422   macro = typeCritical
423 }
424 # This alert is the master alert of all checkMissing alerts.
425 alert pipeline.heartbeatMissingAlert {
426   $status = active
427   # All pipeline checkMissing alerts
428   $alert = pipeline.checkMissing*|collector.checkMissing*|batchmover.checkMissing*|druid.checkMissing*|datamover.checkMissing*
429   $description = The following heartbeat alerts ($alert) are in critical state.
430   macro = checkAlertStatus
431   macro = typeInfo
432 }
433
434 $tags_all_pipelines = component_name=*,instance=prod
435 $tags_main_pipeline = component_name=main_pipeline,instance=prod
436 $tags_af_pipeline = component_name=active_flow,instance=prod
437 $tags_batch_movers = component_name=batchmover_bidir|batchmover_machineinfo,instance=prod
438 $tags_data_movers = component_name=datamover_flowinfo|datamover_machineinfo,instance=prod
439 # 15 minutes
```

% Warning: Любые постоянные изменения на этих правилах требуют письменного согласия , потому что они также используются для аналитических данных.

Раздел тишины

С функцией Тишины в Боцмане можно избежать предупреждений, которые получены во время выбранного периода времени от Аналитики Tetratop без потребности отредактировать предоставленные стандартные правила.

start date

Format: yyyy-mm-dd HH:MM[:SS] [MST/-0700]. UTC if no timezone. Uses now if blank.

end date

duration

Specify either end date or duration.

alert

Optional.

hosts

Optional. Globs, separated by commas (,), pipes (|), or spaces. Example: `ny-web01, ny-redis*`.

other tags

Optional. Ex: `port=637?,cluster=1,iface=lo*|if*`. tags are globs, separated by pipes (|). Example: `port=637?`. Auto forget

If the alert becomes unknown during the silence period, automatically forget it.

start

▲ end

alert

tags

edit

Совет: Это - очень важная функция, поскольку она позволяет сторонние

предупреждения, которые забивают систему и были уже определены, чтобы быть отключенными. Когда ключевой компонент выключается в системе, которая используется большим количеством других компонентов, как правило, предупреждения передаются из всех компонентов. Одно из преимуществ функции Тишины должно быть в состоянии проникнуть в это заранее.