Microsoft

DevCon School

Технологии будущего

Сбор системной телеметрии в реальном времени

Антон Медноногов, Игорь Щегловитов
KasperskyLab

Цели

Поделиться опытом

История развития системы мониторинга и где мы сейчас находимся

Видение мониторинга

Что, как и зачем “мониторить” в облаке

Демонстрация

Разворачивание и настройка системы сбора ,анализа и визуализации системной телеметрии

Инфраструктура Kaspersky Protection Center

#msdevcon

DevCon School
Технологии будущего

Инфраструктура

- Портал my.kaspersky.com
- Продуктовые сервисы:
    - Password Manager
    - SafeKids
    - Secure Connection (VPN)

Стек технологий

- Облачный (Azure и Amazon)
- .NET

Operation модель

- Пишем сервис (код, деплой, тулзы...)
- Готовим документацию (admin guide)
- Передаём сервис на эксплуатацию

Мониторинг

История

#msdevcon

DevCon School
Технологии будущего

SCOM (System Center operation Manager)

SCOM Проверки

- Набор алертов (“лампочек”) в SCOM
- Для алерта определяется “инструкция”:
  - сделать дамп процесса(ов)
  - разбудить “дежурного” разработчика

SCOM Проблемы

- Большая сложность
- Долгий релизный цикл проверок
- Бессистемность проверок

Мониторинг

Развите

#msdevcon

DevCon School
Технологии будущего

Что хотим

- Быстро добавлять/убирать метрики
- Dashboard-ы с ключевыми показателями
- Возможность ретроспективного анализа
- Алерты при серьезных проблемах

Мониторинг

BlackBox - запуск реальных бизнес-процессов, используя публичный API

WhiteBox - получение данных о работе сервиса “изнутри”

BlackBox Мониторинг

То что видит пользователь. Если есть проблема, то она “напрямую” влияет на потребителей

BlackBox Мониторинг

Преимущества

- триггер для немедленного вмешательства
- можно мерить время бизнес-процессов

Недостатки

- сложность реализации
- проблемы с надёжностью

WhiteBox Мониторинг

То как работают “внутренние” компоненты сервиса. Сбои в компонентах не всегда “видны” пользователям

WhiteBox Мониторинг

Преимущества

- максимальная информация о сервисе
- основа для показателей здоровья
- основа для автоматизации

Недостатки

- “бесполезные” метрики
- большой объём/поток данных

WhiteBox 4 Golden Signals*

- Latency (время выполнения запроса)
- Traffic (запрос/сек, кол-во подключений, ...)
- Errors (ошибок/сек, wtf/сек, ...)
- Saturation (ресурсы: cpu, memory, io, ...)

* Site Reliability Engineering (https://landing.google.com/sre/book.html)

Сбор и обработка телеметрии в облаке

#msdevcon

DevCon School
Технологии будущего

Требования

- Быстрое подключение метрик/сервисов
- Низкие затраты на сопровождение
- Масштабирование
- «Реалтайм»

Решение

- Metrics.NET
- Azure Event Hub
- Azure Stream Analytics
- Zabbix

Metrics.NET*

Клиентская библиотека для сбора метрик приложения.

* https://github.com/Recognos/Metrics.NET

Metrics.NET

- Gauges (мгновенное значение)
- Counters (значение которое можно +/-)
- Meters (интенсивность «событий»)
- Histograms (распределение значений)
- Timers (Meters + Histograms)

Metrics.NET

```
Metric.Config.WithReporting(c => c.WithConsoleReport(TimeSpan.FromMinutes(1)));
```

```
private static readonly Timer s_messageProcessingTimer =
    Metric.Timer("queue.received_messages", Unit.Custom("Messages"));
```

```
using (s_messageProcessingTimer.NewContext())
{
    await HandleMessage(message.MessageId, eventType, json.Body);
}
```

Azure Event Hub

«Труба» для потока событий телеметрии. Позволяет «прокачивать» большое количество событий с высокой скоростью и надёжностью.

Azure Event Hub


```
{
  "Name": "partnerapi.requests",
  "MetricType": 5,
  "Histogram": {
    "Last": 185.4409,
    "Mean": 185.61905646621949,
    "Median": 185.4409,
    "StdDev": 2.8788960621162967
  },
  "Rate": {
    "Mean": 0.00083034832381123495,
    "FifteenMinute": 0.0018102658033413838,
    "FiveMinute": 0.0036745717280725521,
    "OneMinute": 0.0075695180938857125
  },
  "Total": {
    "TotalTime": 10909,
    "TotalCount": 65
  }
},
```

Azure Steam Analytics

CEP движок (Complex Event Processing). Позволяет строить SQL запросы к потоку событий.

Azure Steam Analytics

Читает из:

- Event/IOT Hub
- Blob

Пишет в:

- EventHub Service Bus
- Storage Table/Blob/Queue
- Power BI
- Sql Database
- Cosmos DB

Azure Steam Analytics. JSON

```
SELECT
      CASE
          WHEN timerRate.PropertyName = 'Mean' THEN CONCAT(metric.Name, '.rate.mean')
          WHEN timerRate.PropertyName = 'FifteenMinute' THEN CONCAT(metric.Name, '.rate.15min')
          WHEN timerRate.PropertyName = 'FiveMinute' THEN CONCAT(metric.Name, '.rate.5min')
          ELSE CONCAT(metric.Name, '.rate.1min')
      END AS Name,
      timerRate.PropertyValue AS Value,
      1 AS MetricType
  FROM Metrics as metric
  CROSS APPLY GetRecordProperties(metric.Rate) AS timerRate
  WHERE metric.MetricType = 5
```

Azure Steam Analytics. Windows

```
SELECT
    CASE
        WHEN S.AggregatingFunction = 'SUM' THEN CONCAT(M.Name, '.sum')
        WHEN S.AggregatingFunction = 'AVG' THEN CONCAT(M.Name, '.avg')
        ELSE M.Name
    END AS Name,
    CASE
        WHEN S.AggregatingFunction = 'SUM' THEN SUM(M.Value)
        WHEN S.AggregatingFunction = 'AVG' THEN AVG(M.Value)
        ELSE COUNT(*)
    END AS Value,
    1 AS MetricType
FROM Metrics M
JOIN Settings S ON M.Name = S.MetricName
GROUP BY
    M.Name,
    S,
    TumblingWindow(Duration(minute, 1))
```

Azure Steam Analytics. Output

```
WITH
    TimerRates AS ( ... ),
    TimerHistogram AS ( ... ),
    ResultMetrics AS (
        SELECT * FROM TimerRates
        UNION
        SELECT * FROM TimerHistogram
    ),
    AggregatedMetrics AS ( ... )

SELECT *
  INTO PerfCounters
  FROM AggregatedMetrics
```

Демонстрация

Демо

#msdevcon

DevCon School
Технологии будущего

Q&A

Сбор системной телеметрии в реальном времени

Антон Медноногов anton.mednonogov@kaspersky.com
Игорь Щегловитов igor.shcheglovitov@kaspersky.com

#msdevcon

DevCon School
Технологии будущего

Отзывы

Помогите нам стать лучше!

На вашу почту отправлена индивидуальная ссылка на электронную анкету. 3 июня в 23:30 незаполненная анкета превратится в тыкву.

Заполните анкету и подходите к стойке регистрации за приятным сюрпризом!

#msdevcon

Оставляйте отзывы в социальных сетях. Мы все читаем. Спасибо вам! ☺

DevCon School
Технологии будущего