Более 50 проектов по мониторингу

2014	2015	2018	2019	2020
Первый VB-Trend Splunk не SIEM	Старт разработки Smart Monitor	Статус Splunk Elite Partner	Уход Splunk из РФ Smart Monitor ELK	Презентация платформы Smart Monitor OS

VB-Trend 2020

Search anywhere

VB-Trend 2020

VB-Trend 2020: да, удалёнка!

Второй подряд “потрясный” год

splunk> EMBARGO

ЯМы работаем в этом году

2019

2020

VB-Trend 2019 plan>b VolgaBlob

Smart Monitor
Search anywhere

Что поменялось в SM? И зачем?

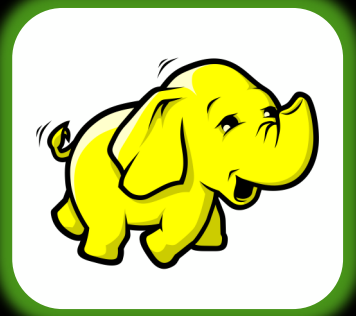
- В 2019 году мы решили сделать Splunk-like Elastic Stack
- В 2020 мы поняли, что этого мало
- Нам надо предложить инструмент для связывания корпоративных хранилищ данных
- Надо помочь увеличить эффективность имеющихся хранилищ
- Надо предоставить платформу для сквозного анализа общего гибридного датасета.

И у нас есть, что вам предложить

Давайте искать везде!

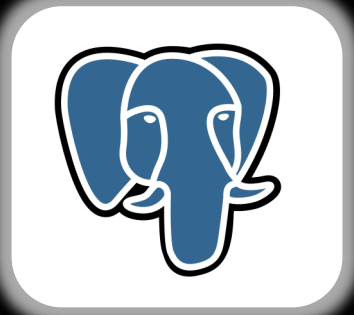
Search

Elastic Search



Hadoop

ClickHouse



PostgreSQL

Splunk

anywhere

Единая платформа для обработки машинных данных во всех корпоративных хранилищах!

Документация

Обязательные

- `name` - имя `lookup`.
- `sourcetype` - тип источника (elastic, clickhouse).
- `idx` - имя индекса или таблицы.

Опциональные

- `condition` - условие выборки (в нотации SML).
- `fields` - список полей для выборки.
- `limit` - максимальное количество данных для выборки.

Примеры запросов

Пример 1:

```
source tables | search database = "hr" | lookup my_click_db name as database OUTPUT engine
```

Пример 2:

Синтаксис: `qsize=<int>`
Описание: Максимальное количество выбираемых данных.
Единицы измерения: единицы. Default: 1000000

Конфигурация источника

Партнерское взаимодействие

VolgaBlob **Partner Program** aims at increasing mutually beneficial cooperation in business intelligence, IT Operations and Cyber Security on Smart Monitor platform.

We know how to turn your data into business value, and are ready to share this in-depth knowledge with our partners!

Our Team is ready to hand over our unique expertise, technical skills and special tools in complex monitoring projects.

Assisting with developing expertise in Data2Value process in BI, IT Ops and Cyber Security

Our technical partners have an all-in-one platform for realizing projects of any complexity. Smart Monitor capabilities are able to solve the issues of different client departments at the same time: IT (infrastructure monitoring, SLA, workload analysis), Security (SOC, SIEM, Antifraud systems, UBA) and Business Intelligence (improving operational efficiency, business process analysis, KPI tracking).

Scaling Machine Data practice and opportunities

Dynamic business scale: from single-instance small projects to margin business unit in different profitable areas. VolgaBlob Company consider as a partner only value-added technical integrators with full cycle project coverage and with the ability to do successful business with us! We don't need "box movers" as partners!

Worldwide Partnership

Multi-language support, the universal search engine, deep dive data analytics and other technical features make Smart Monitor ready for worldwide markets. We look forward to strong Partners in different countries and are ready to support our business together!

BECOME A PARTNER

Безоблачные перспективы

2020

Smart Monitor

Search @nywhere

2021

Community

Smart Monitor Engine

Концепция Search Anywhere

Smart Monitor

- Поиск по данным в любом подключенном хранилище с единым синтаксисом
- Исходные данные остаются нетронутыми, переиндексация не происходит
- Можно положить результаты рядом в любое указанное хранилище

Как использовать?

```
source elk:win_events:1000, clk:events.nix_events qsize=5000
```

Результат запроса:

> 1000 событий из индекса cisco_asa в Elasticsearch

> 5000 событий из таблицы iis_access_log в БД exchange в ClickHouse

Как использовать?

```
source elk:win_events:1000, clk:events.nix_events qsize=5000
```

elk: / clk: / had:

префикс для указания конкретного хранилища

Как использовать?

```
source elk:win_events:1000, clk:events.nix_events qsize=5000
```

win_events / events.nix_events

индекс Elasticsearch / БД и таблица в иных источниках

Как использовать?

```
source elk:win_events:1000, clk:events.nix_events qsize=5000
```

:1000

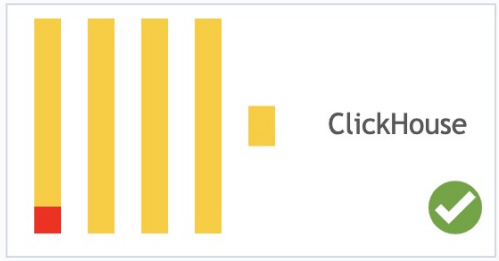
лимит по числу событий от выбранного хранилища

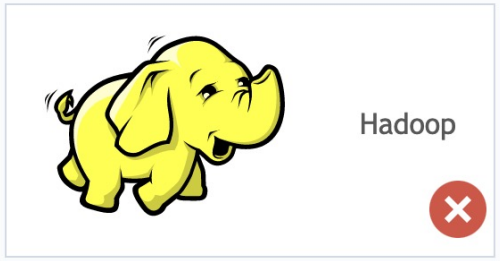
qsize=5000

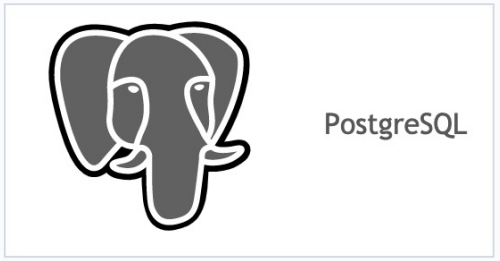
лимит числа событий по умолчанию

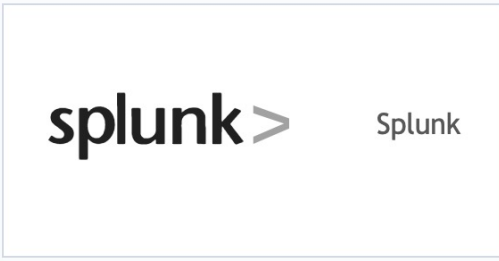
Что подключено?

- ✓ Периодический опрос подключенных хранилищ на предмет обнаружения новых доступных индексов / таблиц
- ✓ Отображение всех подключенных хранилищ и доступных для поиска данных на дашборде для удобства пользователей









Smart Monitor Engine: Что ещё нового?

VB-Trend 2020

Вложенные запросы

```
[ subsearch ]
```

- Поддержка механизмов запуска вложенных запросов (subsearch)
- Фильтрация данных (команда format)
- Добавление данных (команда append)
- Корреляция данных (команда join)
- Нет жёстких ограничений по количеству данных

Справочники

```
| lookup lookup_name lookup_field as data_field output output_field1 ...
```

- Поддержка справочников на основе индексов Elasticsearch
- Поддержка справочников на основе таблиц ClickHouse
- Механизм фильтрации для занесения в справочник только нужных записей
- Возможность указания конкретных полей для занесения в справочник

Поддержка скриптов

```
| script "python3 extract_patterns_for_process.py"
```

- Расширение языка запросов необходимыми пользователю командами
- Запуск скриптов для любых установленных в системе интерпретаторов
- Возможность вынесения выполнения скриптов на отдельный сервер
- Выполнение от имени непривилегированного пользователя

Дополнительные изменения

Ещё больше доступных команд:

- ✓ where
- ✓ timechart
- ✓ dedup
- ✓ sort
- ✓ spath
- ✓ script_mc

Изменения в работе с хранилищами данных:

- ✓ Поддержка scroll-запросов для оптимизации скорости выборки

Дашборды и визуализации

VB-Trend 2020

Проблемы Kibana

- ✖ Невозможно визуализировать произвольный запрос
- ✖ Ограниченные возможности по модификации данных
- ✖ Отсутствие drilldown (только в X-Pack)
- ✖ Проблемы с расположением панелей на дашбордах
- ✖ Проблемы с ресайзингом панелей на дашбордах

Новые визуализации SM

Smart Monitor

- Полный набор базовых визуализация (table, line, area, column, bar, map)
- Возможность запуска произвольного поискового запроса и отображения его результатов
- Drilldown с переходом на поисковую строку, дашборд или произвольную ссылку
- Поддержка различных цветовых тем
- Обратная совместимость с дашбордами Kibana

Пример отображения

```
1 source e:win_events
2 | search agent.hostname
3 | timechart timefield="timestamp" span=15m count(timestamp) by agent.hostname
```

9,587 documents matched in 7,359 ms (11-11-2020 16:57:21 to 12-11-2020 16:57:21)

Last 24 hours | Show dates | Refresh

Documents (9587) | Statistics (97) | Visualization

Select visualization | Add to dashboard | Save as

Apply settings

General | X-Axis | Y-Axis | Legend | Color | Drilldown

Drilldown type

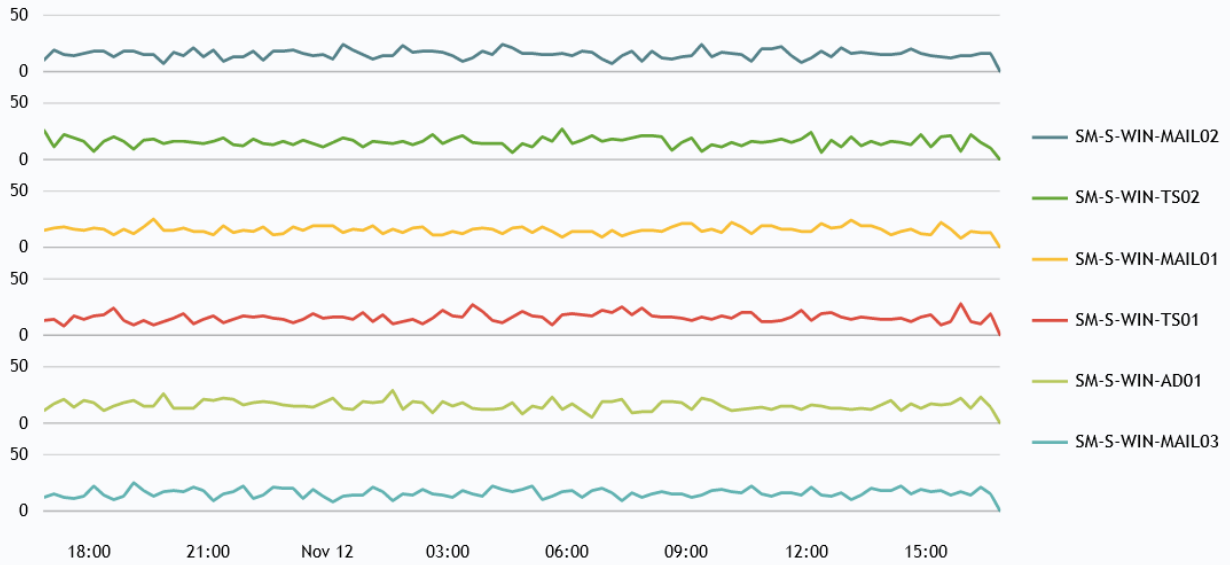
Link to search

Choose drilldown type

SML query

```
1 source e:win_events
2 | search agent.hostname = {{click.value}}
```

Type a SML query to discover



Новый фреймворк для дашбордов

Smart Monitor

- Бесшовная интеграция со страницей создания визуализаций
- Автоматический ресайзинг визуализаций по размеру контента
- Поддержка токенов для фильтров и визуализаций (в разработке)
- Для разработчиков: возможность настраивать дашборды через YAML
- Выравнивание панелей по сетке

Пример отображения

Статистика по инцидентам

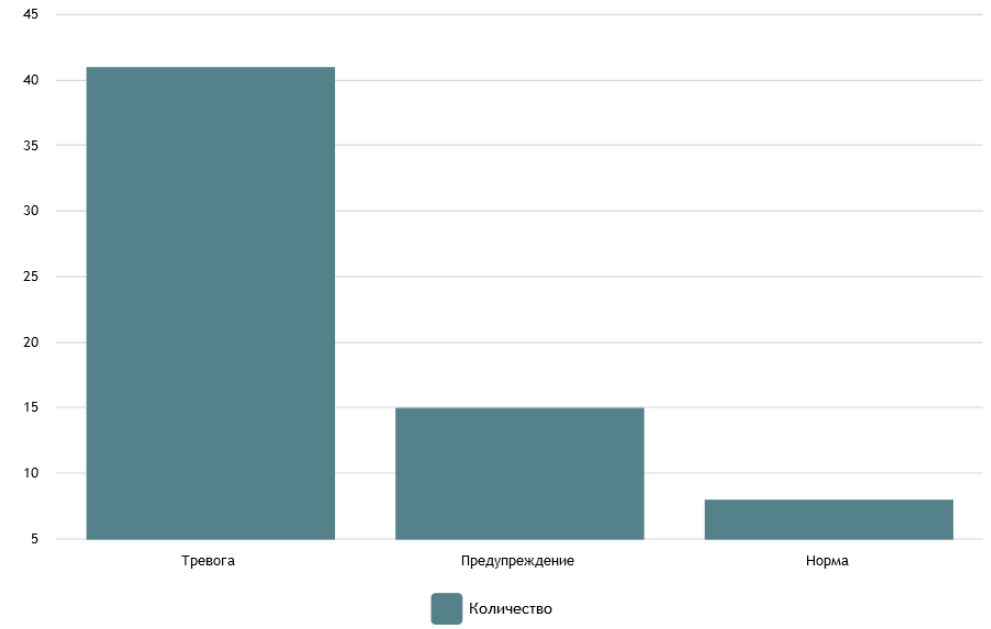
Edit

Time: Last 24 hours — Show dates

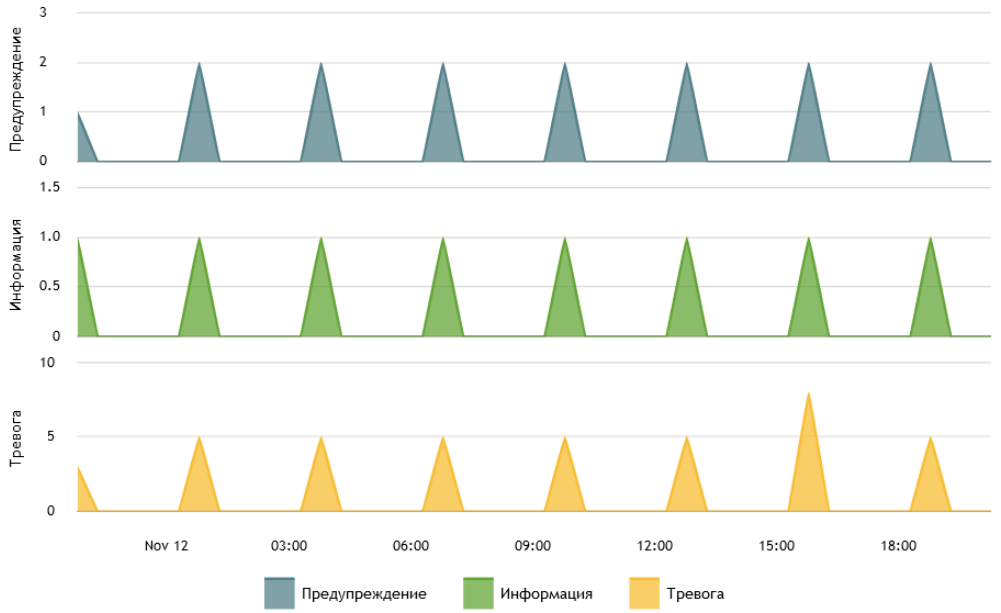
Правило: Все правила

Поиск по инцидентам: *

Распределение инцидентов по уровням критичности



Распределение инцидентов по времени



Перечень инцидентов

incident_title	search_params.start_time	ruseverity
SmartCode: [SNS] Обнаружена сетевая атака на APM (ARM3.vbtrend.local)	2020-11-12T06:02:01.259+0300	Тревога

Smart Beat и Smart Beat Manager

VB-Trend 2020

Проблемы с Elastic Beats

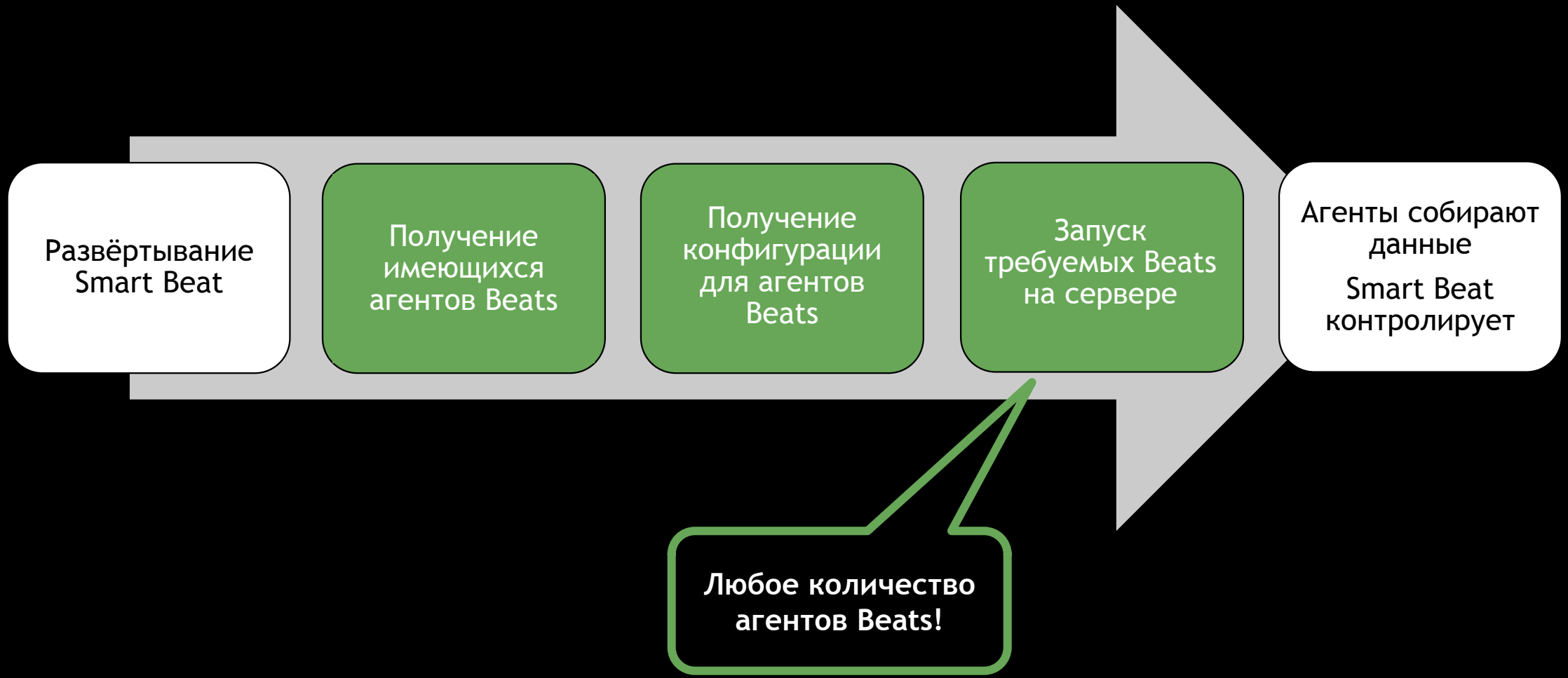
- ✖ Необходимо устанавливать на серверы множество отдельных агентов
- ✖ Процесс обновления агентов потребует переустановки каждого
- ✖ Механизм централизованного управления агентами есть только в X-Pack

Smart Beat

Smart Monitor

- Утилита для управления агентами Beats
- Поддержка централизованного управления конфигурацией агентов
- Запуск нескольких Beats на сервере без необходимости установки множества агентов
- Значительно более простой процесс управления агентами и их обновления

Как это работает



Smart Beats Manager

Smart Monitor

- Управляющий сервер для Smart Beat
- Возможность распространения конфигураций агентов Beats
- Возможность распространения обновленных версий самих Beats
- Веб-интерфейс для просмотра текущей конфигурации и установленных Smart Beat

Развёртывание Smart Monitor

VB-Trend 2020

Процесс развёртывания SMOS

- Установка исходных OSS компонентов Elastic Stack
- Установка плагинов Amazon Open Distro
- Установка плагинов Smart Monitor
- Модификации компонентов Elastic Stack для Smart Monitor
- Внесение базовых настроек для установленных компонентов

Очень долго и требовательно к квалификации исполнителя…

Новые инсталляторы

- Предзаготовленные инсталляционные пакеты для компонентов Elastic Stack с нашими модификациями

- Скрипты автоматической настройки для генерации сертификатов и основных конфигураций

Сокращение времени на развёртывание минимального standalone инстанса с 6 часов до 20 минут!

Демонстрация

VB-Trend 2020

Roadmap 2021

Оставьте голос Zoom чате, пожалуйста: + -

1. Поддержка новых хранилищ данных. **Каких?**
2. Оптимизация производительности и потребления ресурсов
3. Расширение языка запросов (transaction, streamstats, и др.)
4. Поддержка естественного языка в SML, распознавание речи
5. Поддержка нескольких хранилищ одного типа
6. Smart Beat + Smart Beat Manager
7. Smart Monitor Mobile App

Спасибо за внимание!