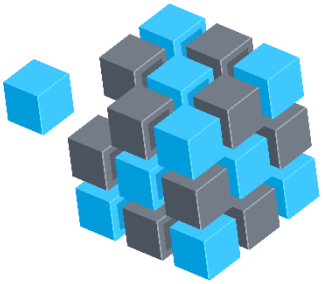

Описание системы ИндексЛог

Оглавление

Краткая информация о системе

ИндексЛог представляет собой многофункциональную платформу для сбора, трансформирования, хранения и поиска по данным различных форматов.

Компоненты платформы ИндексЛог

Платформа разворачивается в виде распределенного кластера на серверах заказчика и имеет в своем составе:

- ИндексЛог_Поиск – распределенный поисково-аналитический движок, в котором хранятся все собираемые данные. Он же производит поиск по этим данным и возвращает искомую выборку JSON-документов. Данные в ИндексЛог_Поиск хранятся в виде JSON-документов, представляющих собой набор полей и значений. Документы логически группируются в индексы, что позволяет распределять их между несколькими серверами ИндексЛог_Поиск и обеспечивают масштабируемость платформы.
- ИндексЛог_Аналитика – сервер, входящий в платформу ИндексЛог, который выступает в роли фронтэнд-решения для работы с движком ИндексЛог_Поиск и управления остальными компонентами стека. ИндексЛог_Аналитика предоставляет интерфейс для отправки поисковых запросов и визуализации результатов, а также содержит готовые дэшборды и вкладки для анализа данных решений, реализованных на платформе ИндексЛог. ИндексЛог_Аналитика имеет встроенную систему кейс-менеджмента для решений по мониторингу и безопасности, позволяющую нескольким пользователям совместно вести расследование одной проблемы.
- Агент ИндексЛог, сервер централизованного управления агентами и регистр пакетов ИндексЛог – унифицированный агент с централизованным управлением и необходимый для централизации этого управления сервер вместе с регистром, содержащим файлы, обеспечивающие интеграции Агента ИндексЛог с источниками данных. Агент ИндексЛог имеет широкую библиотеку готовых интеграций для сбора данных метрик и логов с популярных ИТ продуктов, а также интеграцию ИндексЛог_Защитник для защиты хостов от вредоносного ПО.
- Дополнительно для сбора данных могут использоваться агенты с открытым исходным кодом Beats. Beats представляют собой набор агентов узкого назначения, которые устанавливаются вручную и требуют индивидуальной конфигурации и могут отправлять собранные данные напрямую в ИндексЛог_Поиск или в Logstash для их дополнительной обработки.
- Вместо выделенных серверов ИндексЛог_Поиск для предварительной обработки входящих данных может использоваться решение с открытым исходным кодом Logstash, позволяющее производить манипуляции с полями и значениями в json-документах перед их отправкой в ИндексЛог_Поиск

Решения, реализованные на платформе ИндексЛог

Платформа ИндесЛог предоставляет широкие возможности по работе с данными из разных источников, а также набор инструментов для построения и внедрения в решения заказчика поисковых приложений. На платформе ИндексЛог реализованы следующие решения:

ИндексЛог_Корпоративный поиск

ИндексЛог_Корпоративный поиск позволяет разработчикам строить гибкие поисковые интеграции на базе поисковой платформы ИндексЛог. Поисковые интеграции могут использоваться в электронной торговле, клиентской поддержке, рабочих инструментах, вебсайтах или любом другом приложении с возможностью поиска. ИндексЛог индексирует данные из различных источников (веб-парсер, базы данных, электронные таблицы, документы, архивы электронной почты, базы знаний и др.) и позволяет производить быстрый и точный поиск по ним в режиме реального времени. Для результатов поиска доступны инструменты автозаполнения, фильтрации и классификации, а также инструменты аналитики работы поисковой интеграции. Точность поиска ИндексЛог можно дополнительно повысить с помощью настроек релевантности и учета контекста.

ИндексЛог_Мониторинг

ИндексЛог_Мониторинг нацелен на оптимизацию расходов на эксплуатацию и мониторинг предложений, а также обеспечение высокой доступности ИТ-продукта для конечных пользователей. Решение предоставляет подробную информацию об эксплуатации приложений в продуктивных и тестовых средах. Это набор инструментов, позволяющих в составе единого решения хранить, обрабатывать и анализировать данные логов, метрик инфраструктуры, информацию о доступности приложений, отслеживать их производительность, уровень пользовательского опыта и проводить синтетический мониторинг. Преимущество решения состоит в возможности корреляции данных различных его компонентов, что значительно уменьшает время поиска корневой причины проблем с производительностью или доступностью продукта.

- ИндексЛог_APM

  ИндексЛог_APM – это решение по мониторингу производительности приложений на платформе ИндексЛог. ИндексЛог использует специальные APM-агенты, которые инструментируют выполняемый код приложения и экспортируют в ИндексЛог_Поиск данные о длительности транзакций в этом приложении. Транзакция формируется в результате выполнения приложением входящего запроса и может включать в себя данные о длительности обработки запроса несколькими микросервисами. Также решение отслеживает возникающие в ходе работы приложения ошибки и исключения.

  Интерфейсы ИндексЛог_APM включают в себя:

  - список всех транзакций, обрабатываемых приложением со средней длительностью, частотой обработки и частотой появления ошибок;
  - экран транзакции с информацией о распределении ее длительности, составных частях и их длительности, а также возникающими ошибками;

- ИндексЛог_Инфраструктурный мониторинг

  Инфраструктурный мониторинг собирает данные об эксплуатации серверов, операционных систем, сети, контейнеров Docker, подов Kubernetes и многих других объектов инфраструктуры заказчика. Он позволяет отслеживать нагрузку на элементы инфраструктуры и обладает набором инструментов и визуальных

представлений для удобной группировки и визуализации полученных данных об эксплуатации.

- ИндексЛог_Мониторинг логов

Мониторинг логов собирает в одном интерфейсе содержание логов хостов, сервисов и приложений, запущенных в средах заказчика. Интерфейс мониторинга логов позволяет просматривать поток записей в логе, фильтровать их и искать конкретные записи.

- ИндексЛог_Синтетический мониторинг

Синтетический мониторинг позволяет симулировать запросы к приложению заказчика с удаленного сервера, моделируя активность реальных пользователей. Запросы производятся с заданной частотой, а их содержание полностью настраивается. Это позволяет обеспечить доступность приложения для конечного пользователя и требуемый уровень клиентского опыта.

ИндексЛог_Безопасность

ИндексЛог_Безопасность сочетает в себе инструменты обнаружения угроз SIEM и возможности защиты конечных узлов. Масштабируемость, скорость работы с большими данными и аналитические инструменты решения позволяют увеличить скорость обнаружения угроз и снизить время до восстановления работоспособности систем заказчика. Решение ИндексЛог_Безопасность включает в себя:

- Инструменты сбора и индексации данных.
  - Интеграция ИндексЛог_Защитник унифицированного агента ИндексЛог. Интеграция защищает конечные узлы системы от вредоносного ПО и собирает данные о:
    - Процессах, сетевых событиях, файловой активности, DNS события, события регистра, DLL и драйверов для Windows;
    - Процессах, сетевых событиях и файловой активности для Linux и macOS.
  - Другие интеграции агента ИндексЛог, такие как интеграции с платформами Nginx, MongoDB, Apache HTTP Server и прочие.
  - Агенты с открытым исходным кодом Beats. Ряд открытых агентов с индивидуальной конфигурацией, позволяющих собирать на хостах данные из типовых источников, таких как логи, метрики ОС и сетевой трафик.
- Инструменты обнаружения угроз и аналитики.
  - Движок обнаружения, который автоматически проводит проверки по имеющимся данным на предмет наличия возможных угроз. Для этого он использует правила обнаружения. ИндексЛог_Безопасность имеет встроенный набор правил, который при необходимости можно частично или полностью отключить, а также добавить собственные правила. При срабатывании правила, создается сигнал и появляется возможность начать по нему расследование. Для снижения количества ложных срабатываний правил настраиваться исключения.

- Интерфейс расследования в виде временной шкалы. Запросы и фильтры используются для поиска конкретных событий в потоке данных, затем эти события добавляются на временную шкалу. Эти представления используются для изучения последовательности атаки и обнаружения угроз. Их можно использовать совместно с другими пользователями и прикреплять к кейсам.
- Внутренняя система кейс-менеджмента для совместной работы со случаями нарушения безопасности.

Используемые технологии

- Java
- Библиотека Apache Lucene
- HTML5
- CSS3
- Typescript
- Javascript

Прилагаемые инструменты

ИндексЛог_Поиск

- Хранение и обработка данных в виде json-документов
- Логические группировки документов в виде индекса
- Предварительная планировка индекса с форматами данных для каждого поля
- Обработка документов при индексации
- Операции поиска query и aggregation
- Оценка релевантности документов при выполнении операции поиска
- Работа со статическими и потоковыми данными
- Поддержка цикла хранения данных горячие-теплые-холодные
- Управление потоками данных
- Уменьшение стоимости хранения архивных данных за счет перевода на следующие стадии цикла хранения
- Операции по уменьшению объема данных в индексе при переводе на следующие стадии цикла хранения
- Хранение данных на распределенном кластере
- Настраиваемая репликация данных для обеспечения надежности хранения и скорости поиска
- Распределение ролей между серверами кластера для балансировки нагрузки
- Ролевая модель пользователей
- Аутентификация пользователей с помощью внутренних средств
- Разграничение доступа к возможностям ИндексЛог_Поиск
- Защищенное соединение между серверами ИндексЛог_Поиск
- Защищенное соединение между ИндексЛог_Поиск и Индекс_Лог аналитика
- Защищенное соединение между ИндексЛог_Поиск и агентами ИндексЛог
- Использование внешних сертификатов SSL или сгенерированных встроенными инструментами
- Дополнительные источники данных для ИндексЛог
- Возможность использования обработчика данных с открытым исходным кодом Logstash для предварительной обработки данных перед индексацией
- Возможность использования сборщиков данных с открытым исходным кодом Beats для сбора данных и отправки в ИндексЛог_Поиск напрямую или через Logstash
    - Auditbeat для данных аудита действий пользователей
    - FIlebeat для сбора данных голов и проверки целостности файлов
    - Functionbeat для данных мониторинга облачных сред
    - Heartbeat для синтетического мониторинга удаленных сервисов

- Metricbeat для сбора данных метрик операционной системы и запущенных на хосте приложений
- Packetbeat для сбора данных сетевого трафика

Winlogbeat для сбора данных журнала Windows

ИндексЛог_Аналитика

- Удобный веб-интерфейс для отправки REST API запросов в кластер ИндексЛог_Поиск
- Набор инструментов для создания пользовательских визуализаций
- Визуализация результатов заранее заданного запроса к данным в ИндексЛог_Поиск
- Создание дэшбордов из пользовательских визуализаций
- Просмотр массива документов в выбранном индексе
- Встроенные дэшборды для типовых источников данных
- Возможность создания сигналов (alert) по результатам заранее заданного запроса
- Система управления кейсами
- Управление компонентами стека ИндексЛог через удобный веб-интерфейс
- Настройка ролей и пространств для разграничения доступа к ИндексЛог_Аналитика и функциям ИндексЛог_Поиск
- Консоль разработчика для работы с ИндексЛог_Поиск через самостоятельно написанные API запросы
- Защищенное соединение между браузером конечного пользователя и ИндексЛог_Аналитика

Агент ИндексЛог с централизованным управлением

- Унифицированный способ сбора данных с хостов
- Широкая библиотека готовых интеграций с типовыми источниками данных со встроенными дэшбордами для ИндексЛог_Аналитика и пайплайнами для обработки поступающих данных
- Интеграция ИндексЛог_Защитник для защиты хостов от вредоносного ПО и сбора данных безопасности
- Централизованное управление агентами с помощью политик
- Веб-интерфейс управления политиками и интеграциями
- Выделенный сервер централизованного управления агентами, который проверяет наличие последних версий установленных на каждом агенте интеграций
- Сервер централизованного управления агентами актуализирует конфигурации агентов при изменении их политик
- Регистр пакетов ИндексЛог, из которого ИндексЛог_Аналитика берет список доступных интеграций, и откуда агенты ИндексЛог скачивают их материалы
- Удобный веб-интерфейс для установки новых агентов ИндексЛог
- Отслеживание статуса и установленных интеграций для каждого агента

Требования

- Ubuntu Server Linux 20.04
- Для ИндексЛог_Поиск от 8 GB RAM, от 2 CPU cores, от 16 GB дискового пространства
- Для ИндексЛог_Аналитика 2 GB RAM, 2 CPU cores, от 16 GB дискового пространства