Продукт Platform V Audit SE (AUD)

Компонент Аудит (AUDT)

Описание функциональных характеристик

Дата	Версия	Описание изменения
30.09.2022	2.3	Версия продукта «Platform V Audit SE» впервые зарегистрирована в Реестре отечественного ПО

Содержание

Описание функциональных характеристик продукта Platform V Audit SE (AUD)

Цель создания

Существует несколько видов аудита, каждый служит своей цели. Самые распространенные — это аудит данных и аудит безопасности.

Platform V Audit SE (AUD) разрабатывался как сервис, позволяющий реализовать аудит событий информационной безопасности (security audit). Его задача — обеспечить поддержку работы сотрудников департамента безопасности (ДБ), выполняющих расследования инцидентов информационной безопасности. Сервис предназначен для регистрации событий, значимых для проведения расследования таких инцидентов.

Platform V Audit SE (AUD) реализует следующие возможности:

- Прием и хранение событий безопасности, возникающих в процессе функционирования компонентов Платформы и прикладных приложений, написанных на ее базе.
- Просмотр агрегированных событий безопасности (в пользовательском интерфейсе) уполномоченными пользователями Платформы.
- Подготовка отчетов и статистики на основании информации обо всех собранных событиях безопасности, возникающих в процессе функционирования Платформы.

Основные функции

Перечень основных функций Platform V Audit SE (AUD)

Основные функции Platform V Audit SE (AUD)

Название функции	Потребитель функции	Аргументы функции	Результат
Сбор событий безопасности из клиентской АС	Прикладные модули (внешние системы)	Набор полей данных о событии, определенный метамоделью	Данные о событиях сохранены и проиндексированы в оперативном хранилище с привязкой ко времени и дате и затем архивированы в архивном хранилище для дат, старше определенного периода
Хранение событий безопасности	Прикладные модули (внешние системы)	Записи о событиях безопасности из прикладного модуля (набор полей)	Данные о событиях хранятся с привязкой ко времени и дате, события из хранилища постоянно доступны для поиска в Platform V Audit SE (AUD)
Просмотр событий безопасности	Департамент безопасности	Записи о событиях безопасности из прикладного	Данные о событиях открываются на просмотр прямо из оперативного хранилища Platform V Audit SE (AUD). Для более старых событий требуется

Название функции	Потребитель функции	Аргументы функции	Результат
		модуля (набор полей)	предварительное извлечение из архивного хранилища в оперативное
Подготовка отчетов по всем событиям	Департамент безопасности	Записи о событиях безопасности и статистика по ним	Отображаемые в интерфейсе графики (экспортируемые в файлы) и таблицы отчетов

Сценарии использования

Пользователи:

- Аудитор* — основной пользователь системы. Это может быть аудитор, не имеющий ограничений на доступ к данным, либо аудитор внешней системы, который имеет доступ только к данным внешней системы, за которую отвечает. Для работы в Platform V Audit SE пользователь должен иметь роли Аудитор АС (ASAuditor) или Аудитор Платформы (PlatformAuditor).
- Администратор* — администрирует Platform V Audit SE (AUD), контролирует работоспособность системы или отвечает за поддержку внешних систем, которые регистрируют сообщения, содержащие бизнес-данные. Для работы в Platform V Audit SE пользователь должен иметь роли ASSupport (Сотрудник сопровождения АС) или PlatformAdmin (Администратор платформы).
- Внешняя система — система, которая регистрирует события над бизнес-сущностями и передает их в Platform V Audit SE (AUD) для хранения.

Символом * обозначены пользователи, входящие в ролевую модель Platform V Audit SE (AUD). Описание ролевой модели приведено Руководстве по эксплуатации.

Сценарий 1. Зарегистрировать метамодель

ОДЛ (основное действующее лицо): Внешняя система.

Цель: Зарегистрировать метамодель, содержащую перечень событий и операций, а также набор из параметров, свойственные для данной системы, чтобы в дальнейшем регистрировать события в соответствии с этой метамоделью.

Основной поток:

Внешняя система регистрирует метамодель. *Система* проверяет ее корректность и наличие идентичной метамодели. Идентичность метамодели проверяется по названию модуля (внешней системы),версии метамодели, а также сверяется контрольная суммы метамодели:

- Если метамодель с таким названием модуля, версией метамодели и контрольной суммой существовала ранее, то в Системе обновляются сведения о метамодели.

- Если метамодель с таким названием модуля, версией метамодели, но с другой контрольной суммой существовала ранее, то ОДЛ получает ошибку регистрации метамодели.
- Если метамодель с таким названием модуля и версией метамодели ранее не существовала, то в Системе регистрируется новая метамодель.

Сценарий 2. Зарегистрировать события

ОДЛ: Внешняя система.

Цель: Сохранить события, связанные с бизнес-сущностями в Platform V Audit SE (AUD).

Предусловие: Соответствующая метамодель событий зарегистрирована.

Основной поток:

Внешняя система передает группу событий и операций в *Систему*. Система валидирует события и операции и сохраняет одновременно в архивное и оперативное хранилище. Технические требования к регистрации сообщений в Platform V Audit SE (AUD) приведены в подразделе *«Нефункциональные требования к продукту» в документе «Детальная архитектура»*.

Сценарий 3. Найти события

ОДЛ: Аудитор — пользователь с ролью Аудитор АС (с ролью ASAuditor) или Аудитор Платформы (с ролью PlatformAuditor).

Цель: Выполнить поиск событий по определенным критериям и найти среди них информацию, необходимую для выполнения конкретной задачи.

Основной поток:

1. ОДЛ указывает период, за который необходимо сделать выборку событий.
2. Система проверяет начало и окончание периода:
    1. Если указанный период не выходит за границы хранения данных в оперативном хранилище, то выполняется переход на шаг 3 основного потока.
    2. Если указанный период выходит за границы хранения данных в архивном хранилище, то Система выдает сообщение, что данные ограничены периодом хранения данных в архиве и возвращает ОДЛ на шаг 2 основного потока.
3. Система предоставляет режимы поиска:
    1. По словам.
    2. По фразе.

3. На языке запросов Lucene.

4. ОДЛ выбирает режим поиска:
    1. «По словам». ОДЛ вводит слова, по которым хочет найти события и операции, содержащие все слова.
    2. «По фразе». ОДЛ вводит фразу, по вхождению которой хочет найти события и операции.
    3. «В формате Lucene». ОДЛ на языке запросов Lucene вводит поисковый запрос.
5. ОДЛ инициирует запрос.
6. Система регистрирует событие аудита о поиске.
7. Система отображает список событий, отсортированный в порядке по времени в порядке от новых к старым.
8. ОДЛ просматривает события.

Сценарий 4. Найти связанные события (через дерево операций)

Дерево операций позволяет просмотреть события, происходившие до и после найденного при помощи поиска.

ОДЛ: Аудитор — пользователь с ролью Аудитор АС (с ролью ASAuditor) или Аудитор Платформы (с ролью PlatformAuditor).

Цель: Определить контекст, в котором произошло событие.

Предусловие: Выбрано интересующее событие.

Основной поток:

1. ОДЛ инициирует построение дерева связанных событий.
2. Система строит дерево связанных событий:
    1. По операциям
3. ОДЛ работает с найденными событиями:
    1. Просматривает на разных уровнях дерева.

Сценарий 5. Импортировать данные из архива

ОДЛ: Администратор — пользователь с ролью ASSupport (Сотрудник сопровождения АС) или PlatformAdmin (Администратор платформы).

Цель: Импортировать данные из архива в оперативное хранилища для выполнения поисковых запросов по ним.

Основной поток

1. ОДЛ указывает параметры поискового запроса к архивному хранилищу. Обязательно указывается период (дата начала и дата окончания). Опционально указываются условия поиска по другим полям (например, user, module и т.д.).

2. Система инициирует задачу импорта данных в отдельную коллекцию.

3. Система уведомляет ОДЛ по окончании импорта данных.

Расширения

P1. Platform V Audit SE (AUD) по параметрам запроса определяет, пересекается ли запрос с ранее выполненными импортами из архива по датам. Если пересекается, то загружает только за те даты, которых еще не хватает.

Альтернативный поток Сценарий 5.1 «Вызов импорта из поиска»

Предусловие: ОДЛ ввел параметры поиска. Система проанализировав их определила, что указан период времени, выходящий за пределы оперативного хранилища, но не выходящий за пределы архивного хранилища (Сценарий 3).

Поток:

Система предлагает выполнить импорт данных из архива за недостающий период дат с дополнительными условиями, которые можно указать для архивного хранилища (user, module и др.). Далее выполняется **Основной поток** с шага 1.

Поток Сценарий 5.2 «Администратор восстанавливает данные в оперативном хранилище»

ОДЛ: Администратор — пользователь с ролью ASSupport (Сотрудник сопровождения АС) и PlatformAdmin (Администратор платформы).

Предусловие: Работа оперативного хранилища восстановлена и регистрация событий в системе возобновлена.

Поток:

1. ОДЛ инициирует восстановление данных из архива за последние несколько дней.

2. Система импортирует данных из архива в оперативное хранилище, устанавливая для каждого события дату истечения на основе даты создания события.

Сценарий 6. Выгрузить события для системы мониторинга

ОДЛ : Система – Platform V Audit SE.

Цель: Передать данные в режиме онлайн в систему мониторинга, в которой настроены оповещения на определенные поступления данных.

Основной поток:

Система в соответствии с указанным фильтром отбирает события и операции и перекладывает их в транспорт, из которого внешняя Kafka производит вычитку данных.

Сценарий 7. Освободить место на дисках

ОДЛ: Администратор — пользователь с ролью ASSupport (Сотрудник сопровождения АС) и PlatformAdmin (Администратор платформы).

Цель: Не допустить переполнения хранилищ.

Сценарий **7.1. Удалить данные из оперативного хранилища**

1. ОДЛ выбирает данные, которые ранее были загружены из архива в оперативное хранилище. ОДЛ делает это либо указывая вручную дату начала и окончания, либо выбирая из списка выполненных импортов, либо выбирая период, покрывающий самые старые даты.
2. ОДЛ инициирует удаление данных.
3. После удаления ОДЛ проверяет процент занятой памяти, отведенной под оперативное хранилище. При необходимости повторяет процедуру удаления данных.

Сценарий **7.2. Инициировать удаление данных из архива**

ОДЛ инициирует процедуру физического удаления данных из архива средствами Hadoop в период наименьшей нагрузки.

Сценарий 8. Получить статистику о количестве событий в оперативном хранилище

ОДЛ: Администратор — пользователь с ролью ASSupport (Сотрудник сопровождения АС) и PlatformAdmin (Администратор платформы).

Цель: Получить информацию о количестве событий в оперативном хранилище в разрезе модулей.

Основной поток:

1. ОДЛ выбирает интересующий его период и инициирует получения статистики.
2. Система выводит количество событий за период по модулям.