Составьте список данных, которые должны попадать в трейсинг

* ИД пользователя
* ИД заказа
* ссылка на файл с 3D моделью
* Дата создания заказа
* Стоимость заказа
* Статус заказа
* Trace ошибок, возникших в системе

1. **«Мотивация».**

Добавление трейсинга в систему позволит выявить ошибки, возникающие в недрах микросервисной архитектуры приложения. Так как полученные данные позволят снизят затраты разработчиков на поиск и воспроизведение багов в системе. В итоге будем иметь список вызовов , по которым можно понять, где оборвалась цепочка вызовов.

Трейсинг поможет быстро находить причины медленной работы сервиса. Вместо просмотра всей цепочки вызовов, которую нужно к тому же раскрутить, разработчик может посмотреть, сколько, где и с какими параметрами прошёл вызов. У трейсинга как средства устранения неполадок есть дополнительные преимущества, поскольку любое исключение или ошибка обычно фиксируется вместе со всем контекстом запроса.

Трейсинг позволит:

* понять на каком этапе происходит потеря заказа
* выявить причины медленной работы сервиса
* понять полную картину происходящего в системе через средства визуализации

1. **«Предлагаемое решение».**

<https://drive.google.com/file/d/1p1PyaDX_J7O5jVuTcSdmx9OBLyx7EGHK/view?usp=sharing>

1. **«Компромиссы».** Опишите, в каких случаях трейсинг не принесёт пользы или пока невозможен, или его реализация обойдётся слишком дорого.

1) Ограниченные ресурсы

Реализация системы трейсинга может потребовать значительных инвестиций в технологии, программное обеспечение, обучение персонала и техническую поддержку. Если бюджет компании ограничен, а ресурсы дефицитны, инвестиции в трейсинг могут быть нецелесообразны. Особенно это актуально для малых предприятий или стартапов.

2) Сложные технологические ограничения

Существуют случаи, когда системы трейсинга не могут быть внедрены из-за ограничений существующих технологий. Например, если используемое оборудование или программное обеспечение не поддерживает интеграцию с трейсинг-системами, это может сделать его внедрение невозможным или трудоемким.

3) Неподходящая организационная культура

Организации с сильно развитой иерархической структурой или непрерывными изменениями в управлении могут столкнуться с трудностями в внедрении системы трейсинга. Если сотрудники не готовы к изменениям или их работа непрозрачна, может возникнуть сопротивление внедрению новых инструментов, что отразится на общем успехе проекта.

4) Проблемы с конфиденциальностью и безопасностью

В некоторых случаях возможно, что трейсинг будет связан с проблемами конфиденциальности данных и безопасности. Например, если существует строгая регуляция, касающаяся обработки личной информации. Реализация систем трейсинга в таких условиях может быть слишком сложной и затратной, если она не соответствует соответствующим законам и стандартам.

1. **Проработайте аспекты безопасности.** Опишите, какие меры для предотвращения несанкционированного доступа будут предусмотрены для системы трейсинга внутри компании и снаружи если это требуется.

**1. Аутентификация и авторизация**

* **Многофакторная аутентификация (MFA)**: Внедрение многофакторной аутентификации для всех пользователей системы. Это может быть комбинация пароля или одноразового кода.
* **Ролевой доступ**: Определение прав доступа на основе ролей. Каждый пользователь должен иметь доступ только к той информации и функциям, которые необходимы для выполнения их работы.
* **Регулярный аудит прав доступа**: Периодическая проверка и обновление прав доступа для гарантии того, что только актуальные пользователи имеют доступ к системе.

**2. Шифрование**

* **Шифрование данных**: Используйте шифрование при передаче данных (SSL/TLS) и хранении (AES‑256 или другие стандарты) для защиты конфиденциальной информации от несанкционированного доступа.
* **Шифрование логов**: Логи системы трейсинга также должны быть зашифрованы, чтобы предотвратить доступ к информационным потокам.

**3. Защита сети**

* **Файрволы и системы обнаружения вторжений (IDS/IPS)**: Настройка файрволов и систем обнаружения вторжений для мониторинга и защиты сети от несанкционированного доступа.
* **Безопасный доступ**: Использование виртуальных частных сетей (VPN) для удаленного доступа к системе трейсинга. Это гарантирует, что передача данных защищена.

**4. Мониторинг и аудирование**

* **Логирование доступа**: Ведение подробного логирования всех действий пользователей, включая попытки доступа, изменения данных и ошибки входа. Это поможет отслеживать подозрительные действия и обеспечит возможность проведения аудитов.
* **Мониторинг в реальном времени**: Внедрение систем мониторинга, которые будут отслеживать аномалии и выдавать уведомления в случае подозрительных действий.

**5. Обучение и политика безопасности**

* **Обучение сотрудников**: Регулярное обучение персонала по вопросам безопасности, включая предотвращение фишинга и другие методы защиты информации.
* **Разработка и внедрение политики безопасности**: Четкие правила и процедуры доступа к системе трейсинга, а также действия в случае нарушения безопасности.

**6. Обновление и патчи**

* **Регулярные обновления программного обеспечения**: Обновление системы и приложений должно проводиться регулярно для устранения уязвимостей и использования последних исправлений безопасности.
* **Управление уязвимостями**: Проведение регулярных тестов на уязвимости и обеспечение их устранения.

**7. Ограничение доступа к физическим серверам**

* **Физическая безопасность**: Защита физических серверов, на которых размещается система трейсинга. Это включает контроль доступа, видеонаблюдение и ограничение доступа только для авторизованных лиц.

**8. Сегментация сети**

* **Сегментация сети**: Создание отдельных сегментов для разных функций, чтобы ограничить доступ к критическим системам и данным.