1. **Проанализируйте систему компании и C4-диаграмму в контексте планирования логирования.** Опишите, какие логи нужно собирать и отметьте на схеме, из каких систем требуется сбор логов. Составьте список необходимых логов с уровнем INFO.

Shop:

* Создание заказа (когда, кем, ID созданного заказа)
* Изменения статуса заказа (ID, когда, кем изменено, старое значение, новое значение)

CRM:

* Создание заказа (когда, кем, ID созданного заказа)
* Изменения статуса заказа (ID, когда, кем изменено, старое значение, новое значение)

MES:

* Создание заказа (когда, кем, ID созданного заказа)
* Назначение заказа на исполнителя (кто принял, когда, срок выполнения)
* Изменения статуса заказа (ID, когда, кем изменено, старое значение, новое значение)

Если имеется функционал отправки уведомлений на почту/смс, будет полезно логировать отправку сообщения(когда, кому, связанный элемент), чтобы понимать, действительно ли наблюдается простой на производстве или нарушена система оповещения.

По моему мнению, обязательно необходимо логировать отказы системы, используя уровни Error и Warn, так как жизненный цикл заказа может тормозиться из-за ошибок в API или недоступности какой-то части ресурсов.

1. **Добавьте в файл раздел «Мотивация».** Напишите здесь, почему в систему нужно добавить логирование и что это даст компании. Опишите три-пять технические и бизнес-метрики решения, на которые может повлиять внедрение логирования.

Команда не сможет реализовать единовременно логирование и трейсинг всех выделенных для этого систем. Поэтому опишите, для каких систем нужно настраивать логирование и трейсинг в первую очередь и почему.

Поскольку основные жалобы пользователей и исполнителей связаны с задержкой производства и долгим временем отклика MES, по моему мнению, первоочередно необходимо решать проблемы производительности и качества именно этой системы.

Добавление логирования в систему является важным шагом для повышения эффективности ее работы и обеспечения безопасности. Логирование позволяет отслеживать и документировать действия, события и ошибки, что может дать ощутимые преимущества как в техническом, так и в бизнес-аспектах.

Почему нужно добавить логирование:

* Диагностика и устранение неисправностей: Логи помогают выявить причины сбоев и неполадок в системе, что упрощает процесс устранения ошибок.
* Безопасность и аудит: Логирование позволяет отслеживать подозрительную активность и помогает в расследовании инцидентов безопасности, что критично для защиты данных и соблюдения нормативных требований.
* Производительность: Анализ логов может помочь в выявлении узких мест в системе, что позволяет оптимизировать производительность и уменьшить время отклика.

Метрики, на которые может повлиять внедрение логирования:

* Время реагирования на инциденты:

Техническая метрика: Среднее время реагирования на инциденты может уменьшиться за счет быстрого доступа к логам, что позволяет быстрее идентифицировать источники проблем.

Бизнес-метрика: Уменьшение времени простоя системы ведет к повышению доступности услуг и снижению потерь для компании.

* Частота ошибок и сбоев:

Техническая метрика: Логирование позволяет отслеживать количество и частоту возникающих ошибок, что дает возможность более целенаправленно их устранять.

Бизнес-метрика: Снижение частоты ошибок увеличивает удовлетворенность клиентов и повышает доверие к продукту.

* Производительность системы:

Техническая метрика: Сбор данных о времени выполнения различных операций помогает выявлять узкие места и оптимизировать код и архитектуру.

Бизнес-метрика: Оптимизация производительности приводит к большему количеству успешных транзакций и повышению уровня обслуживания клиентов.

1. **Добавьте раздел «Предлагаемое решение».**

Опишите, как и с помощью каких технологий будет реализовано логирование, какие компоненты нужно внедрить или доработать. Отразите компоненты и новые связи на схеме.

Проработайте политику безопасности в отношении логов — как будет происходить работа с чувствительными данными, кто будет иметь доступ к логам.

Проработайте политику хранения в отношении логов — будет ли это отдельный индекс под систему, сколько они будут храниться и какого размера будут.

Для централизованного сбора, хранения и анализа логов можно использовать ELK Stack (Elasticsearch, Logstash, Kibana), который позволяет собирать, обрабатывать и визуализировать логи. Доступ к логам должны иметь технические специалисты с правами доступа уровня администратора(DevOps, Ведущий разработчик). Описанные в п.2 события логирования не несут в себе личной конфиденциальной информации, поэтому вопрос чувствительности данных в нашем случае не требует никаких специфичных действий.

Я бы разделила логирование по системам и формировала файлы логов с разбиением 1 файл/сутки. Поскольку, исходя из описания задачи, скорость реализации заказа больше 1 месяца уже является проблемой, требующей решения, полагаю разумным настроить автоматическое удаление файлов логирования старше полугода в первое время наладки системы и сократить его до 3 месяцев после наладки производства.

1. **Проработайте необходимые мероприятия для превращения системы сбора логов в систему анализа логов:**

По моему мнению, в данном решении следует применять инструменты для мониторинга и оповещения о критических событиях (Prometeus, Grafana).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

Ссылка на диаграмму

<https://drive.google.com/file/d/1o4mKkTl7OduIVKEhyykFocnC83mrG9iM/view?usp=drive_link>