**«Post-Mortem» отчет по восстановлению**

**работы Linux-сервера**

Дата и время инцидента: **04.03.2025, 09.00**

Дата и время устранения инцидента: **04.03.2025, 09.00 - 12.15**

Группа: **111124-ptm**

Отчёт составил: **Алекс Сидоренко**

**1. Описание инцидента**

На сервере с веб-приложением (**MediaWiki**), обслуживаемое **Apache** (**httpd**) произошел сбой, из-за которого сайт перестал работать. Сбой был обнаружен группой (**111124-ptm**) при запуске веб-приложения. Причины сбоя были неизвестны, требовалось провести диагностику и восстановить работоспособность сервера.

**2. Причины инцидента**

В процессе диагностики были выявлены следующие проблемы:

**Технические**:

* Заполнен диск из-за неконтролируемого роста лог-файла **/var/log/httpd/access\_log**.
* Файл конфигурации приложения **LocalSettings.php** находился в неверной директории.
* В файле конфигурации (**MediaWiki**) был указан неправильный **$wgServer**.

**Организационные**:

* Отсутствие механизма автоматической очистки старых логов
* Отсутствие мониторинга дискового пространства.

**3. Предпринятые шаги по восстановлению**

**Этап 1: Проверка состояния сервера и сервисов**

* Проверено, что сайт не открывается (ссылка в виде IP-адреса **http://3.69.175.208** предоставлена администратором).
* Подключение к серверу по SSH.
* Проверка состояния **httpd** (service httpd status)– **сервис работает** (Active: active (running)).
* Попытка запуска **httpd** (service httpd restart) - **привела к ошибке** (причина - недостаточно прав на systemctl).
* Перезапуск **httpd** “с правами” (sudo systemctl restart httpd.service) - **работает**.
* Проверка состояния **httpd** (sudo systemctl status httpd.service) - **сервис работает**.
* Проверка доступности сайта - **сайт не работает**.

**Этап 2: Анализ ошибок и проблемы с настройками**

* Анализ логов **Apache** выявил **ошибку конфигурации**.
* Веб-приложение не может найти файл конфигурации **LocalSettings.php** (на главной странице есть упоминание об его отсутствии).
* Файл конфигурации **LocalSettings (5).php** находится в неправильной директории: **/home/ec2-user/** вместо **/var/www/html/mediawiki/**.
* При попытке открыть **LocalSettings (5).php** командой cat появилось сообщение об отсутствии места на диске (**No space left on device**).

**Этап 3: Освобождение дискового пространства**

* Проверка дискового пространства (df -h) показала, что нет места на диске.
* Проверка оперативной памяти (free -h) показала, что её достаточно для работы сервера (mem-2,9Гб , total-3,8Гб, swap =0).
* Анализ файлов, которые занимают много места (sudo find / -type f -size +100M | xargs sudo du -h) выявил, что большую часть (**7.0Гб**) занимает лог веб-сервера (/**var/log/httpd/access\_log**). **Аccess log** - это журнал работы web-сервера, в который он записывает все запросы, которые он обрабатывает. **Использовано все доступное дисковое пространство**.
* Удаление файл лога (sudo rm -rf /var/log/httpd/access\_log), предварительно необходимо делать архивную копию, т.к. в нем может быть полезная информация (например, для анализа «секьюрити»).
* Проверка дискового пространства (df -h) – показала, что **проблема не устранена**.
* Для ее устранения были выполнены следующие действия:
* Проверка удаления файла в /var/log/httpd/**access\_log** (sudo cd /var/log/httpd, ls -a, sudo find / -type f -size +100M | xargs sudo du -h) - показала, что **файл удален**.
* Перезапуск Bash (source ~/.bashrc) и сервиса Apache (sudo systemctl restart httpd.service).
* Проверка (df -h) подтвердила освобождение места.

**Этап 4: Восстановление файла конфигурации**

* Проверка, что находится в **/var/www/html/mediawiki/** (ls -la).
* Обнаружен старый файл настроек: **LocalSettings.php**.
* Копирование файла настроек в нужное место (cp ~/"**LocalSettings (5).php**" /var/www/html/mediawiki/**NewLocalSettings.php**)
* Проверка наличия файла (ls -la /var/www/html/mediawiki/) - **файл появился**.
* Создание копии старого файла настроек (mv LocalSettings.php LocalSettings.php.bkp)
* Замена старого файла конфигурации(mv NewLocalSettings.php LocalSettings.php).
* Удаление пустого и некорректно завершенного файла(rm .LocalSettings.php.swp).
* Проверка доступности сайта (по ссылке http) - **сайт недоступен**.
* Перезапуск **Apache** (sudo systemctl restart httpd.service) - **сайт недоступен**.
* Проверка файла настроек (vim /var/www/html/mediawiki/**LocalSettings.php**) выявила неверный IP-адрес в конфигурации MediaWiki – сайт перенаправлял запросы на некорректный сервер (**$wgServer** = "**https://18.153.51.162**" вместо **"**[**https://3.69.175.208**](https://3.69.175.208)**"**).
* Коррекция IP-адреса: **$wgServer = "**[**https://3.69.175.208**](https://3.69.175.208)**"**.

**Этап 5: Тестирование и перезапуск**

* Перезапуск сервера – веб-приложение (**MediaWiki) снова доступно.**

**4. Итог и рекомендации**

**Итог:**

* Файл конфигурации восстановлен и находится в нужной директории.
* Освобождено место на диске.
* Восстановлена работа веб-приложения.

**Рекомендации:**

* **Автоматизация очистки логов** (предотвратит подобные сбои):
* Внедрение скрипта (**/home/ec2-user/backup\_logs.sh**), который будет автоматически архивировать и удалять старые логи (**7 дней**).
* Скрипт протестирован. Мониторинг работы показал его эффективность:

———————————————————————————————————

#!/bin/bash

DATE=$(date «+%Y%m%d-%M»)

# Архивируем логи

tar -czvf /home/ec2-user/"$DATE"\_access\_log.tar.gz /var/log/httpd/access\_log

# Очищаем текущий лог-файл access\_log

echo "" > /var/log/httpd/access\_log

# Удаляем архивы старше 7 дней

find /home/ec2-user/ -name «\*.tar.gz» -mtime +7 | xargs rm

———————————————————————————————————

* **Создание cron-задачи** (crontab -e) - выполняет очистку раз в день.
* 0 0 \* \* \* /home/ec2-user/backup\_logs.sh - запуск каждую ночь в 00:00
* **Мониторинг дискового пространства:**
* Настроить **автоматические оповещения**, если диск заполнен более чем на 80%.
* Настроить cron-задачу для проверки дискового пространства раз в день (например, df -h через cron).
* **Автоперезапуск Apache при сбоях** (sudo systemctl restart httpd.service)

**Вывод**:

Веб-приложение (**MediaWiki)** успешно восстановлено, причины сбоя выявлены и устранены. Введены меры по предотвращению аналогичных сбоев, включая автоматическую очистку логов. Проблему можно предотвратить заранее, если настроить систему уведомлений и мониторинга.