Post-mortem

Концепция

Восстановление работоспособности Linux сервера после инцидента

Дата и время проблемы

2025-04-01 10:50

Дата написания

2025-04-03

Автор

Юлия Ткачук

Проблема

2 апреля, около 10:50 утра, веб-сайт на базе MediaWiki перестал функционировать. На экране отображалась ошибка: “$wgServer must be set in LocalSettings php. See https:/www.mediawiki.org/wiki/Manual:SwgServer.” Это свидетельствовало о проблеме в конфигурационном файле `LocalSettings.php`, связанной с отсутствием или некорректным значением переменной $wgServer. При этом веб-сервер и само веб-приложение физически продолжали работать, а также были настроены резервные копии. Однако, по неизвестной причине сервис перестал отвечать. Требовалось подключиться к серверу и восстановить его работоспособность.

Причина инцидента

- Файл `LocalSettings.php` оказался пустым, из-за чего веб-сайт не мог корректно стартовать;
- На сервере закончилось дисковое пространство в корневом разделе (/), что препятствовало записи и работе с файлами.

Последствия для бизнеса

Веб-сайт был недоступен в течение нескольких часов, что могло вызвать:

- Потерю доверия со стороны пользователей;
- Прерывание внутреннего рабочего процесса, если сайт использовался для корпоративных нужд;

- Потенциальные убытки, если сайт являлся частью коммерческого проекта.

Хронология восстановления сервиса, устранения проблемы

Первым делом, что мы делаем, проверяем или действительно заверенный сайт не работает. На сайте высветило ошибку *“$wgServer must be set in LocalSettings php. See https:/www.mediawiki.org/wiki/Manual:SwgServer.”*, и можем предположить, возможно что-то с хранилищем. Обратим внимание, что также здесь указан файл, а именно `LocalSettings.php`, который подвержен риску пострадать, но это нежелательно, так как это локальные настройки сервера, который содержит основные команды.

Для того, чтобы подключиться к серверу, мы используем Terminal, и подключаемся по IP адресу: *3.122.108.39*. Для этого мы обращаемся к системному администратору, чтобы получить разрешение для подключение к серверу через Terminal и ключ. Вводим ключ через ssh и его полный путь: *ssh -i .ssh/ec2-user@3.122.108.39* и заходим на сервер.

Далее смотрим статус процесса сервера при помощи команды *service httpd status*. Система говорит нам, что он не упал, то есть есть активный (запущен) на The Apache HTTP Server. Теперь пробуем перезапустить сервер, то есть выключаем и включаем одновременно с помощью команды *service httpd start*, но система нам говорит, что невозможно перезапустить сервер, по определенным причинам.. Движемся дальше, и проверим, ведь возможно что ошибка прячется в `LocalSettings.php`, ищем с помощью *find / -type f -name “LocalSettings.php”*, нам выбиваем много ошибок и система говорит, так как мы не находимся не являемся супер пользователем, и мы не имеем права подсмотреть некоторые папки. Но мы пробуем далее, сделать вывод ошибок через команду *2>/dev/null* Делаем это для того, чтобы не видеть кучу ошибок у нас на екранах.

Система нашла один единственный путь, где это файлик у нас находится и мы подсматриваем в него через *cat /var/www/html/mediawiki/LocalSettings.php*, но увы система ничего нам не выдала, тогда мы делаем команду *ls -l /var/www/html/me-bash* и плюс при нажатие кнопки *tab* чтобы посмотреть сколько места занимает этот файл. И нам вышел результат, где показывает что нет в системе места для того чтобы подключить быструю подсказку по *tab*. Это говорит нам о том, что в каких-то системных разделах закончилось место, либо не хватает оперативной памяти. Тогда подсмотрели свободную оперативную память: *free -h* , но проблема лежит не в оперативной памяти, так как места вполне достаточно для работы сервера. Тогда проверили корневой раздел: *df -h* , и он оказался полностью заполненный на 100%, и скорее всего поэтому сервер не отвечает.

Но мы еще раз попытались добраться к нашему файлу `LocalSettings.php` через команду *nano /var/www/html/mediawiki/LocalSettings.php*, чтобы точно убедиться, если какая-то ошибка с этим файлом. И так, первая причина, почему же система ругается, а потому, что файл `LocalSettings.php` является нерабочим, в нем ничего нет, он просто пустой. Вторая причина закончилось место на жестком диске. После этого мы позвонили нашему системному администратору, и предоставили причины проблем, почему возможно возник данный сбой. Далее нам предстояло понять почему пустое место в файле `LocalSettings.php` и как его восстановить, и разобраться с занятым местом в корневом разделе, сделать так, чтобы места стало

больше. В разговоре с системный администратор выяснилось, что на сервере существует копия с содержимым на 100% рабочая версия файла и называется очень схоже как `LocalSettings.php` И просто нужно по этому пути, где есть пустой файл его переписать. То есть сделать его копию.

Так как мы знаем место, где `LocalSettings.php` должен находится, и мы помещаем рабочую версию файла по этому пути: *ls -l /var/www/html/mediawiki/* . И мы нашла очень похожий файл `LoclSettings.php`, и проверили его содержимое: *nano /var/www/html/mediawiki/LoclSettings.php* и содержимое в принципе как и должно быть. С помощью команд *cat* и *cp* мы попытались перезаписать информацию с `LoclSettings.php` в `LocalSettings.php`, но увы нам выдает что не найдено файла или директорию. То есть он его не видет, хотя он существует. И это может также быть связано с нехваткой места. Через команду *ls -l /tmp* смотрим сколько весит, и если возможность ее удалить. Но это нам ничего не дало, поэтому смотрим глубже *du /tmp*, и на этом этапе нам нужно было попросить у системного администратора, разрешение на получение использования команды *sudo*. И тогда с помощью *sudo du /tmp*, подсмотрели, что у нас там есть. Но к огромному сожалению, это нам ничего не дало, так как папка *tmp* весит очень мало, и это нам особо не сможет помочь. Мы продолжили поиск и попробовали с помощью *find / -name "*LocalSettings*" 2>dev/null*, и нашлись два файла, которые нужно было проверить. Первый *cat /home/ec2-user/LocalSettings.php* оказался пустым, а второй *cat /home/ec2-user/LocalSettings (5).php* показал ошибку, и ее нужно было пофиксить. Попробовали сделать путь условным, то есть взять в кавычки и перезаписать его *cat "/home/ec2-user/LocalSettings (5).php" > /var/www/html/mediawiki/LoclSettings.php*, но снова поражение, не достаточно места. То есть, нам нужно было разобраться с недостающим места. Мы указать параметры по месту, чтобы на громоздкие файлы и узнать какой сколько весит: *find / -type f -size +50M 2>/dev/null*, далее пробуем несколько способов: *ls -l /proc/kcore, ls -lh /proc/kcore, ls -l /var/lib/mysql/ib_logfile0, ls -lh /usr/lib/locale/locale-archive.* Но ищем дальше большие файлы, больше 100 мегабайт, чтобы система показала, только самые огромные файлы и указала размеры *find / -type f -size +100M -exec du -h {} + 2>/dev/null* И вуаля мы имеем два размера 299M и 108M. И мы попробовали удалить локальный архив в 108M: *rm /usr/lib/locale/local-archive,* но он выявился защищенным, то есть вероятнее всего, в нем что-то есть важное. Подсмотрели содержимое данного архива с помощью *tar -t, tar -tf* но это не сработало. Продолжили дальше, так как мы сбросили все ошибки с доступа запрещен в черную дыру, и возможно мы не видели огромные файлы в папках, в которые нам запрещено было подсматривать под обычным пользователем. На данном этапе нам снова нужна была помощь системного администратора, а именно в дальнейшем использовать команду *sudo* или *sudo su*. Делаем дальше *sudo find / -type f -size +100M -exec du -h {} + 2>/dev/null,* и ухуу мы нашли файл весом 7.0G, подсмотрели за ним *sudo cat /var/log/httpd/access_log* и понеслась матрица нечитаемых символов. Уничтожили внутренности, но оставили название с помощью *sudo echo " " > /var/log/httpd/access_log,* но снова был крах, даже с помощью *sudo*, он не хочет записываться. Тогда пробуем стать в сессии супер администратора на все команды *sudo su* и вставили наш файл, *find / -type f -size +100M -exec du -h {} + 2>/dev/null* и *echo " " > /var/log/httpd/access_log.* Также мы узнали сколько весит данный файл *du -h /var/log/httpd/access_log*, в результате 4.0K. Далее мы вернулись к обычному пользователю с помощью *exit*. Далее мы выполнили команду *df -h*,

проверить что у нас в результате получилось и он действительно стал легче, так как было 7G, а стало 36% = 6.5G, то есть легче.
Мы попробовали это файл перезаписать снова, *cp "/home/ec2-user/LocalSettings (5).php" /var/www/html/mediawiki/LocalSettings.php*, нас не выкинуло и но мы еще проверили или действительно произошло копирование в этом файле *cat /var/www/html/mediawiki/LocalSettings.php*, и да, файл был не пустым, что может не радовать, и как бы должно заработать, мы обновили для этого сайт, но увы ничего … но через несколько секунд сайт показал ошибку. Продолжили, и следующим посмотрели на статус *sudo service httpd status*, нам показало что *active (running)*, делаем еще раз *sudo service httpd start*, работает дальше. Обновили страницу, но по прежнему ничего. А проблема скрывалась в IP-адресе, при обновлении страницы сервер ломился, совсем не туда куда нужно было. Выходит что, файл был не тот. Тогда мы зашли в файл *nano /var/www/html/mediawiki/LocalSettings.php*, и начали искать неверный IP-адрес который был там прописан, и заменили его на верный, то есть *"https://3.122.108.39",* который мы изначально заходили на наш сервер. Сохранили и вышли с редактора. И перезапустили сайт, и вуаля заработало.

Текущее состояние системы

На текущий момент работоспособность сервера полностью восстановлена. Веб-приложение функционирует стабильно и без сбоев. Все основные сервисы, включая веб-сервер, успешно запущены и находятся в рабочем состоянии. Сайт доступен по корректному IP-адресу, конфигурационные файлы проверены и находятся в актуальном состоянии.

Предложения по недопущению в будущем

Для минимизации риска повторения подобных сбоев были предложены следующие меры:

- Автоматическая проверка доступного пространства на диске с уведомлением в случае превышения при достижении 80% использования;
- Регулярное тестирование резервных копий, чтобы гарантировать их целостность и пригодность для восстановления;
- Мониторинг ключевых конфигурационных файлов, таких как `LocalSettings.php`, с возможностью быстрого отката изменений;
- Создать документирование процессов, регулярно обновлять подробную инструкцию по восстановлению системы в случае сбоя;
- Оптимизация логирования и ротация логов, чтобы избежать чрезмерного накопления данных и переполнения раздела;
- Ограничение доступа к критическим файлам и системным папкам, чтобы избежать случайного удаления или изменения важных данных.

Как можно было избежать проблемы

- При наличии системы мониторинга инцидент был бы замечен и устранен до возникновения сбоя.
- Если бы файл `LocalSettings.php` хранился в *git* или другом системе контроля версий, его восстановление заняло бы несколько минут.