BLITZ IDENTITY PROVIDER

Результаты нагрузочного тестирования

Москва, 2024

СОДЕРЖАНИЕ

Введение

Цель тестирования – определение производительности сервера аутентификации Blitz Identity Provider на заданной тестовой конфигурации.

Нагрузочное тестирование позволило оценить производительность системы при росте нагрузки и оценить стабильность и надежность работы сервера аутентификации.

1. Методика тестирования

1.1. Тестовый стенд

Тестовая конфигурация была установлена на виртуальных машинах (ВМ), размещенных на платформе Yandex Cloud. Все ВМ были под управлением Alma Linux 8.8. Перечень виртуальных машин размещен в таблице ниже.

Таблица 1

Конфигурация тестового стенда

Роль	ПО и версия	Кол-во ВМ	CPU, ядра	RAM	Хранилище, объем и тип
Сервер аутентификации	Blitz Identity Provider, 5.18	2	8	8 ГБ	30 ГБ HDD
СУБД	PostgreSQL 10.23	1	6	12 ГБ	572 ГБ SSD
LDAP-каталог	389ds	1	4	4 ГБ	15 ГБ HDD
Балансировщик	Nginx	1	4	4 ГБ	15 ГБ HDD

В качестве генератора запросов на аутентификацию использовалось 3 ВМ с конфигурацией 6 Core и 6GB RAM.

1.2. Процесс аутентификации

В качестве протокола для проведения аутентификации использовался OpenID Connect 1.0 (далее – OIDC).

Тестовый процесс аутентификации состоял из следующих типов запросов:

1. *Инициализация аутентификации* – отправка запроса на аутентификацию в Blitz Identity Provider на URL авторизации (Authorization endpoint).
2. *Проверка логина и пароля* – аутентификация по логину и паролю, результат которой – передача авторизационного кода в систему.
3. *Получение маркера доступа* – операция по обмену авторизационного кода на маркер доступа, которая производится в результате обращения на URL для получения и обновления маркера (Token endpoint).
4. *Получение данных пользователя* – операция по вызову REST-сервиса Blitz Identity Provider, результат которой – получение данных пользователя.

Производился замер времени, который требуется серверу аутентификации на выполнение каждого запроса.

1.3. Сценарий тестирования

В ходе тестирования оценивалась:

- *производительность системы при росте нагрузки*. Замерялась производительность при нагрузках:
  - 600 потоков (далее – низкая нагрузка);
  - 1200 потоков (средняя);
  - 1800 потоков (высокая);

  Все запросы направлялись на кластер Blitz Identity Provider, а балансировщик нагрузки распределял запросы между узлами кластера.

  В качестве показателя производительности рассматривалась время отклика по каждому типу запроса (среднее значение, 95-й и 99-й процентиль).
- *стабильность работы сервера аутентификации*. Для этого было проведено 8-часовое испытания, включавшего следующие фазы:
  - 1800 потоков – 60 минут;
  - 1200 потоков – 30 минут;
  - 600 потоков– 300 минут;
  - 1800 потоков – 60 минут;
  - 1200 потоков – 30 минут.

  Здесь аналогичным образом все запросы направлялись на кластер Blitz Identity Provider, балансировщик нагрузки распределял запросы между узлами кластера.

  На *рис*. 1 отображен реальный график нагрузки, т.е. количество запросов в секунду (визуализация осуществляется по 5-минутным интервалам).

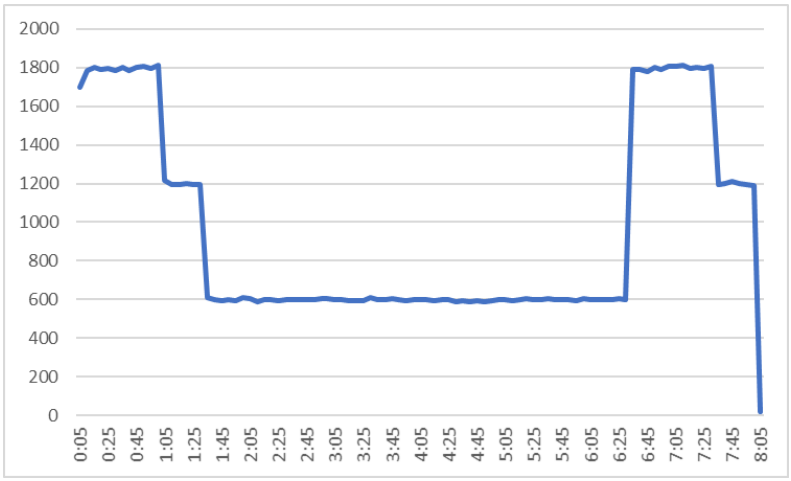


Рисунок 1 – Нагрузка в ходе 8-часового испытания, количество запросов

1.4. Инструменты мониторинга

Показатели работы системы и работы компонентов сервера фиксировались при помощи Apache JMeter v. 5.6.2.

2. Основные результаты тестирования

2.1. Производительность системы при росте нагрузки

Обобщенные результаты тестирования системы приведены в *табл*. 2. Данные результаты отражают поведение кластера Blitz Identity Provider, состоящего из двух ВМ.

Медленнее всего выполняются запросы на проверку логина и пароля, быстрее всего – запросы на получение данных пользователя. Наиболее существенно нагрузка влияет на скорость проверки логина и пароля. Если при увеличении нагрузки в 2 раза время на выполнение данного типа запроса выросло в 1,5 раза (с 15 до 22 мс), то при увеличении нагрузки в 3 раза это время выросло почти в 4,5 раза (с 15 до 65 мс) (*рис*. 2).

В целом, если оценить общую продолжительность аутентификации (сумма 4-х запросов), то окажется, что при низкой нагрузке, соответствующей приблизительно 150 аутентификациям в секунду, в среднем аутентификация занимает 35 mc. При высокой нагрузке в 450 аутентификаций в секунду средняя продолжительной аутентификации составила 116 мс.

Таблица 2

Время отклика системы аутентификации

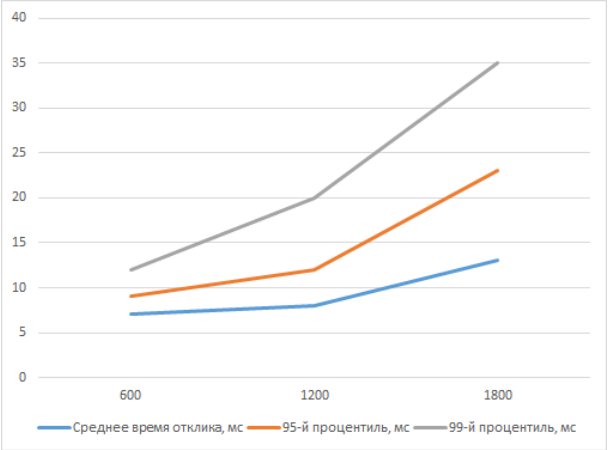
№	Показатель	Нагрузка		
		600	**1200**	**1800**
	Инициализация аутентификации			
1	Среднее время отклика, мс	7	8	13
2	95-й процентиль, мс	9	12	23
3	99-й процентиль, мс	12	20	35
	Проверка логина и пароля			
1	Среднее время отклика, мс	15	22	65
2	95-й процентиль, мс	20	38	116
3	99-й процентиль, мс	28	57	151
	Получение маркера доступа			
1	Среднее время отклика, мс	9	11	22
2	95-й процентиль, мс	12	18	39
3	99-й процентиль, мс	16	27	51
	Получение данных пользователя			
1	Среднее время отклика, мс	4	6	16
2	95-й процентиль, мс	6	11	32
3	99-й процентиль, мс	10	21	46
	Усредненное время выполнения операции*			
1	Среднее время отклика, мс	9	12	29
2	95-й процентиль, мс	16	27	87
3	99-й процентиль, мс	21	41	122
Средняя время аутентификации**, мс		**35**	**47**	**116**

Примечание:

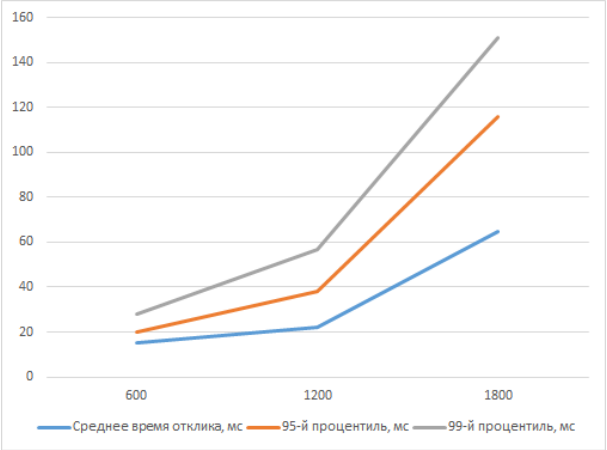
* Усредненное время выполнения каждой из четырех операций – инициализации аутентификации, проверки логина и пароля, получения маркера доступа и получения данных пользователя

** Суммарное время, в среднем необходимое на выполнение указанных четырех операций.

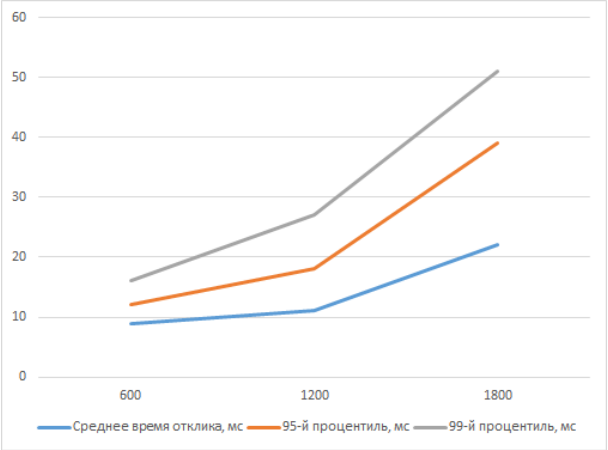
Инициализация аутентификации



Проверка логина и пароля



Получение маркера доступа



Получение данных пользователя

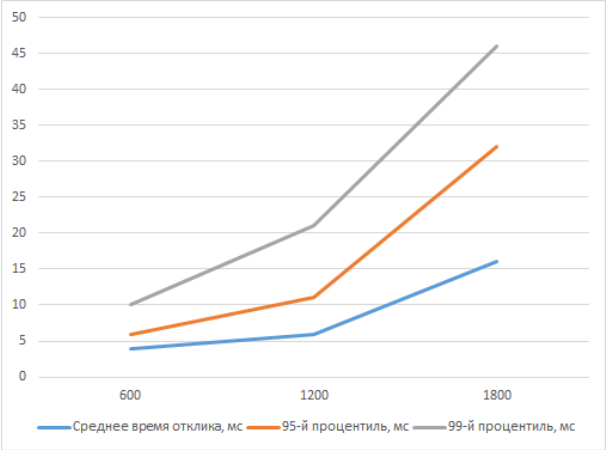


Рисунок 2 – Время выполнения запросов в зависимости от нагрузки, мс

2.2. Стабильность работы сервера аутентификации

Под стабильностью (longevity/endurance) системы понимается отсутствие ошибок и приемлемая производительность при длительной нагрузке. Продолжительность нашего испытания составила 8 часов. Нагрузка принимала наибольшие значения в 1800 запросов в секунду – на начальной и конечной фазе.

В ходе длительной нагрузки ошибок не возникло. Кроме того, при изменении нагрузки система корректно переходила в новый режим работы: при уменьшении нагрузки сокращалось время отклика, при увеличении нагрузки – росло.

На *рис*. 3 и 4 представлены показатели времени отклика на запросы на инициализацию аутентификации и на проверку логина и пароля. Видно, что большинство запросов (99%) на аутентификацию при максимальной нагрузке имеет отклик не выше 42 мс, а запросов на проверку логина и пароля – 190 мс. При низкой нагрузке эти показатели

составили 15 и 35 мс соответственно. Аналогичная картина наблюдалась в запросах на получение маркера доступа и получении данных пользователя.

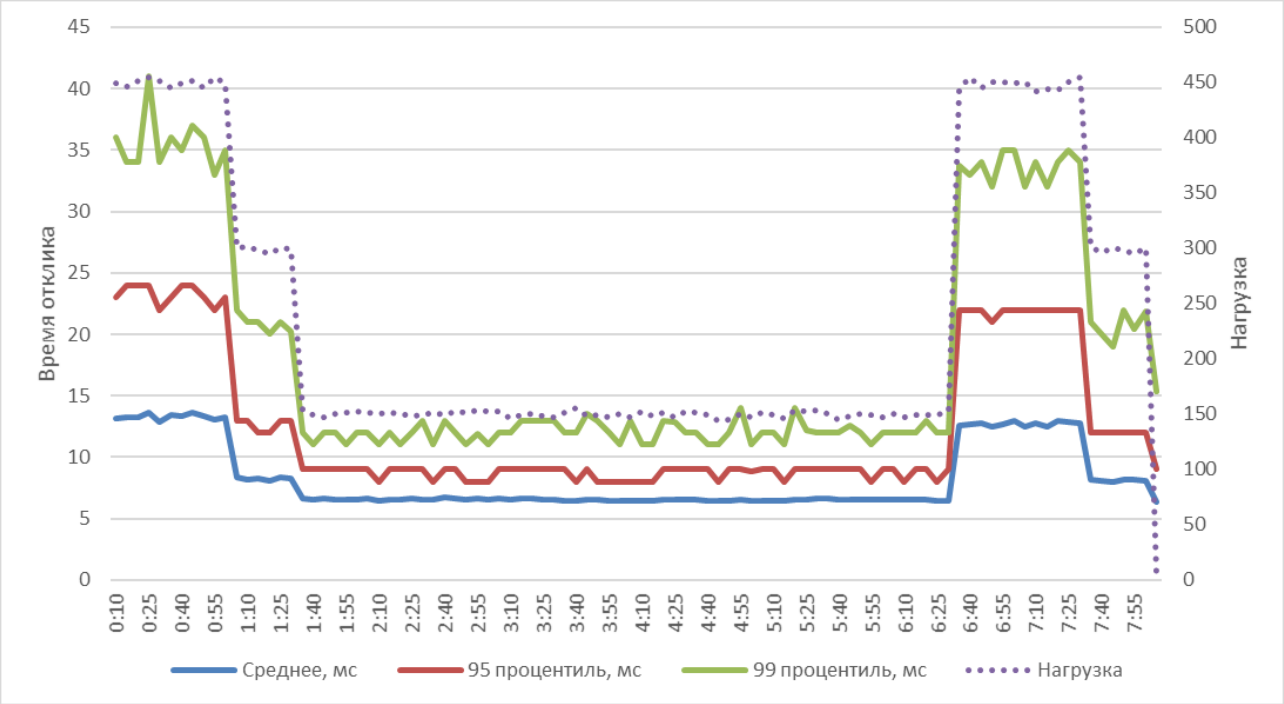


Рисунок 3 – Время выполнения запросов на инициализацию аутентификации в зависимости от времени, мс

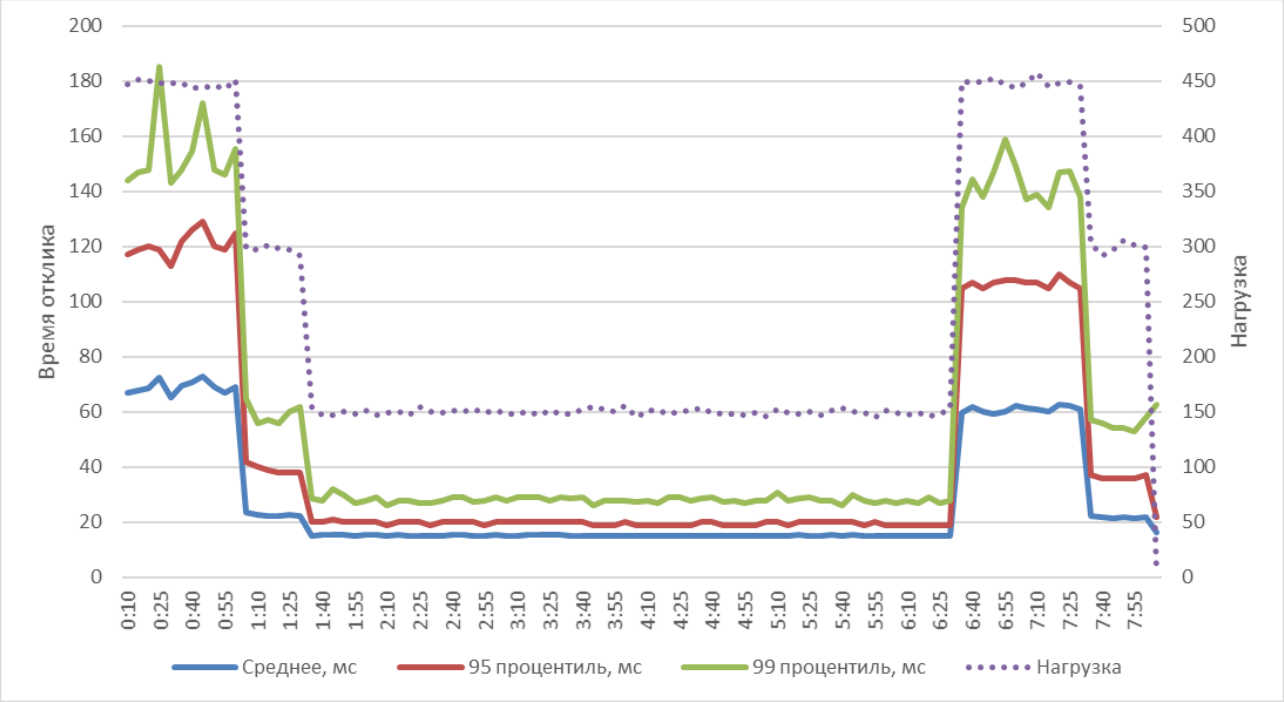


Рисунок 4 – Время выполнения запросов на проверку логина и пароля в зависимости от времени, мс

Заключение

На тестовом стенде начального уровня кластер из 2 виртуальных машин Blitz Identity Provider устойчиво функционирует при нагрузке 1800 запросов в секунду, обеспечивая среднее время отклика одной операции в 29 мс.

На протяжении 8-часового тестового цикла не было зафиксировано ни одного неуспешного запроса.

При использовании промышленных серверов и увеличении их мощности ПО Blitz Identity Provider сможет обеспечить более высокую производительность.