

**BLITZ IDENTITY PROVIDER**

**Результаты нагрузочного тестирования**

## **СОДЕРЖАНИЕ**

<b>ВВЕДЕНИЕ.....</b>	<b>3</b>
<b>1. МЕТОДИКА ТЕСТИРОВАНИЯ .....</b>	<b>3</b>
1.1. ТЕСТОВЫЙ СТЕНД .....	3
1.2. ПРОЦЕСС АУТЕНТИФИКАЦИИ.....	4
1.3. СЦЕНАРИЙ ТЕСТИРОВАНИЯ.....	4
1.4. ИНСТРУМЕНТЫ МОНИТОРИНГА.....	5
<b>2. ОСНОВНЫЕ РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ.....</b>	<b>5</b>
2.1. ПРОИЗВОДИТЕЛЬНОСТЬ СИСТЕМЫ ПРИ РОСТЕ НАГРУЗКИ.....	5
2.2. СТАБИЛЬНОСТЬ РАБОТЫ СЕРВЕРА АУТЕНТИФИКАЦИИ .....	8
<b>ЗАКЛЮЧЕНИЕ .....</b>	<b>9</b>

## 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 следующих виртуальных машинах:

- сервер аутентификации Blitz Identity Provider – на 2-х серверах 2 Core CPU, 2GB RAM, 30GB HDD;
- база данных Blitz Identity Provider – на 3-х серверах 2 Core CPU, 14GB RAM, 150GB HDD + 110SSD. Оба накопителя подключались по интерфейсу SATA, на магнитных дисках размещались данные, а на твердотельных – индексы;
- балансировщик – на сервере 2 Core CPU, 4GB RAM, 30GB HDD;
- LDAP-каталог с учетными данными пользователей – на сервере 2 Core CPU, 4GB RAM, 30GB HDD.

Схема тестового стенда представлена на *рис. 1*.

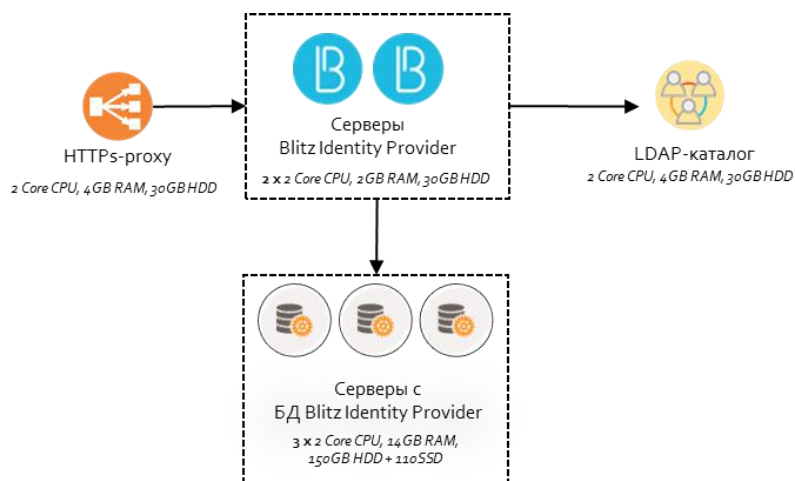


Рисунок 1 – Схема тестового стенда Blitz Identity Provider

В качестве генератора запросов на аутентификацию использовалась машина с конфигурацией 2 Core и 4GB RAM.

При оценке производительности использовался Blitz Identity Provider Enterprise Edition версии 2.9.

## 1.2. Процесс аутентификации

В качестве протокола для проведения аутентификации использовался OpenID Connect 1.0 (далее – OIDC), взаимодействие в рамках которого соответствует Authorization Code Flow спецификации OAuth 2.0.

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 запросов в секунду (далее – низкая нагрузка);
  - 1200 запросов в секунду (средняя);
  - 1700 запросов в секунду (высокая);
  - 2500 запросов в секунду (пиковая).

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 испытание, включавшего следующие фазы (на *рис. 2* отображен график нагрузки):
  - 1700 запросов в секунду – 60 минут;
  - 1200 запросов в секунду – 30 минут;
  - 600 запросов в секунду – 300 минут;
  - 1700 запросов в секунду – 60 минут;

- 1200 запросов в секунду – 30 минут.

Отслеживалось возникновение ошибок, а также производился мониторинг производительности системы. Для этого все время теста было разбито на 5-минутные интервалы, по каждому из которых рассчитывалось время отклика на каждый тип запроса (среднее значение, медиана, 95-й и 99-й процентиль).

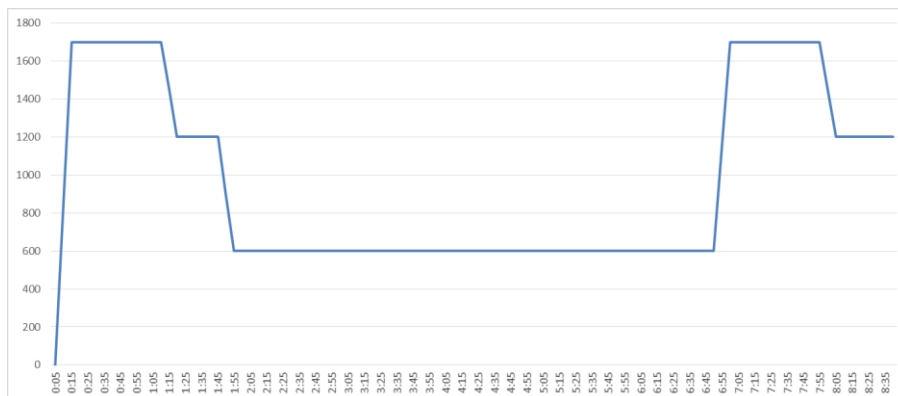


Рисунок 2 – Нагрузка на систему в ходе 8-часового испытания

## 1.4. Инструменты мониторинга

Показатели работы системы и работы компонентов сервера фиксировались при помощи Apache JMeter v. 2.13.

## 2. Основные результаты тестирования

### 2.1. Производительность системы при росте нагрузки

Обобщенные результаты тестирования системы приведены в *табл. 1*. Медленнее всего выполняются запросы на проверку логина и пароля, быстрее всего – запросы на получение авторизационного кода.

Время отклика растет линейно в зависимости от нагрузки. На примере самого медленного запроса по проверке логина и пароля видно, что при увеличении нагрузки с 600 до 1700 запросов в секунду среднее время отклика растет с 31 до 84 мс. В то же время при пиковой нагрузке в 2500 запросов среднее время отклика достигает уже 220 мс (*рис. 3*).

В целом, если оценить общую продолжительность аутентификации (сумма 4-х запросов), то окажется, что при низкой нагрузке, соответствующей приблизительно 150 аутентификациям в секунду, большинство (99%) аутентификаций длятся менее 0,5 с., при высокой (425 аутентификаций) – 1,1 с. При пиковой нагрузке в 625 аутентификаций в секунду большинство процессов аутентификации укладывалось в 2,7 с., что также можно считать приемлемым результатом.

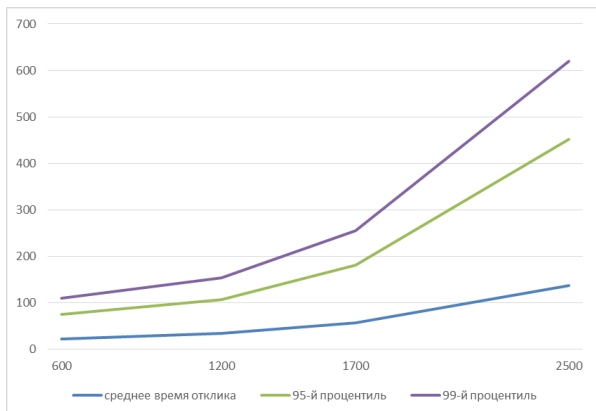
**Время отклика системы аутентификации**

Этап / показатель		Нагрузка			
		600	1200	1700	2500
<b>Инициализация аутентификации</b>					
1	Среднее время отклика, мс	21	34	56	136
2	95-й перцентиль, мс	74	106	180	451
3	99-й перцентиль, мс	110	153	255	619
<b>Проверка логина и пароля</b>					
1	Среднее время отклика, мс	31	53	84	220
2	95-й перцентиль, мс	92	135	218	437
3	99-й перцентиль, мс	125	188	299	705
<b>Получение маркера доступа</b>					
1	Среднее время отклика, мс	29	48	73	186
2	95-й перцентиль, мс	89	125	201	544
3	99-й перцентиль, мс	119	172	279	679
<b>Получение данных пользователя</b>					
1	Среднее время отклика, мс	27	44	70	165
2	95-й перцентиль, мс	87	122	201	508
3	99-й перцентиль, мс	118	167	273	650
<b>Усредненное время выполнения операции<sup>1</sup></b>					
1	Среднее время отклика, мс	27	45	71	177
2	95-й перцентиль, мс	86	122	200	485
3	99-й перцентиль, мс	118	170	277	663
<b>Средняя продолжительность аутентификации<sup>2</sup>, мс</b>		<b>108</b>	<b>179</b>	<b>283</b>	<b>707</b>
<b>99-й перцентиль продолжительности аутентификации, мс</b>		<b>472</b>	<b>680</b>	<b>1106</b>	<b>2653</b>

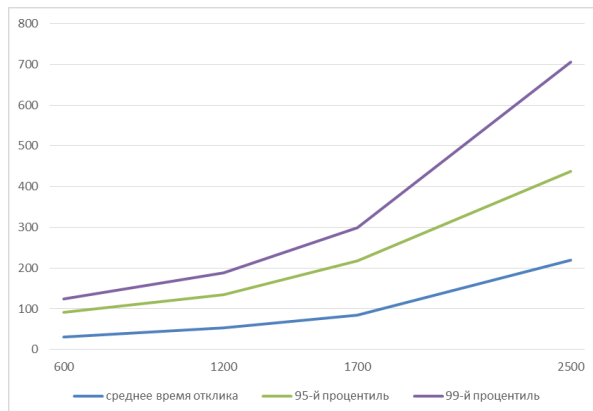
<sup>1</sup> Усредненное время выполнения каждой из четырех операций – инициализации аутентификации, проверки логина и пароля, получения маркера доступа и получения данных пользователя.

<sup>2</sup> Суммарное время, необходимое на выполнение указанных четырех операций.

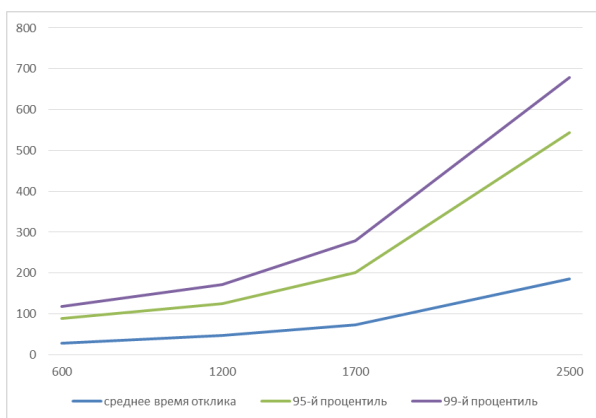
### Инициализация аутентификации



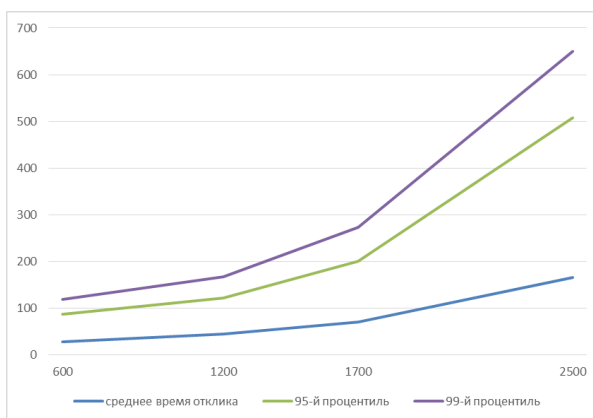
### Проверка логина и пароля



### Получение маркера доступа



### Получение данных пользователя



### Проведение аутентификации в целом

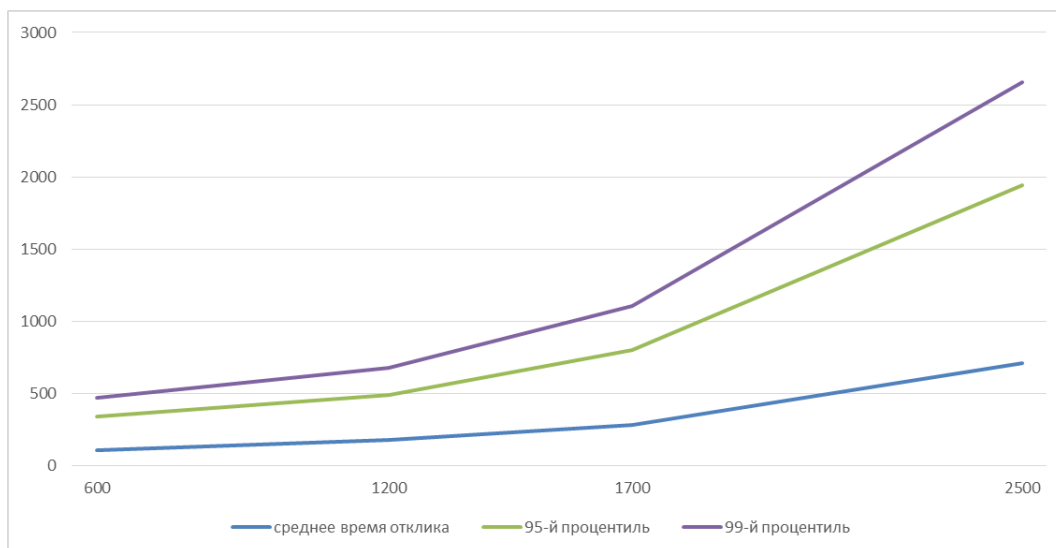


Рисунок 3 – Время выполнения запросов в зависимости от нагрузки, мс

## 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 имела 2 пика (в 1700 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. 4* и *5* представлены показатели времени отклика запросов на инициализацию аутентификации и на проверку логина и пароля. Видно, что большинство запросов (99%) на аутентификацию при максимальной нагрузке имеет отклик не выше 270 мс, а запросов на проверку логина и пароля – 320 мс. При низкой нагрузке эти показатели составили 110 и 120 мс соответственно. Аналогичная картина наблюдалась в запросах на получение маркера доступа и получении данных пользователя.

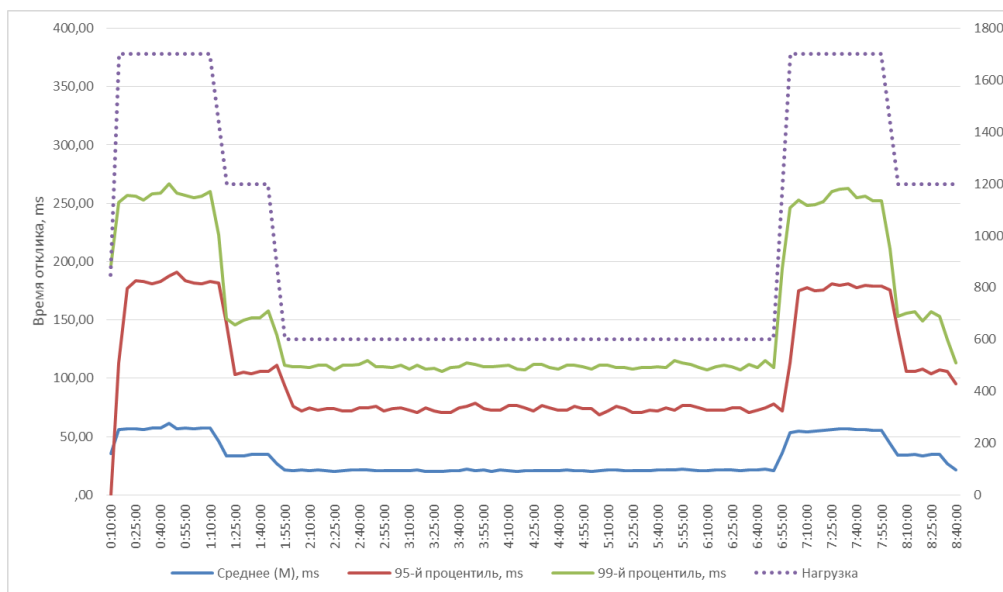


Рисунок 4 – Время выполнения запросов на инициализацию аутентификации в зависимости от времени, мс



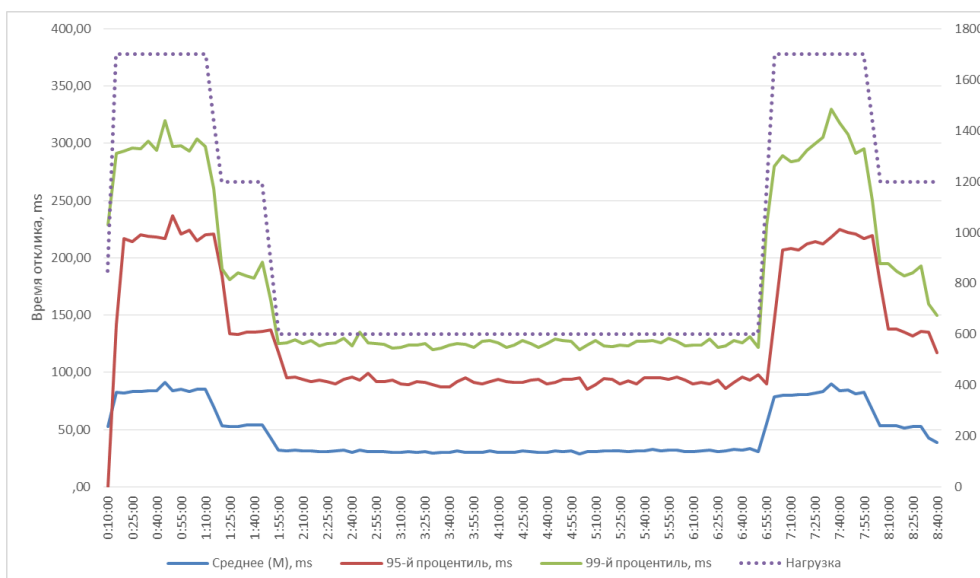


Рисунок 5 – Время выполнения запросов на проверку логина и пароля в зависимости от времени, мс

## Заключение

На тестовом стенде начального уровня ПО Blitz Identity Provider устойчиво функционирует при нагрузке 1700 запросов в секунду, обеспечивая среднее время отклика одной операции в 70 мс (95% запросов имели отклик менее 200 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.