Blitz Identity Provider

Версия 5.34

Инструкции по обновлению

04 августа 2026

Оглавление

Важно

Если обновление ставится с пропуском промежуточных версий, то устанавливать `blitz.bin` нужно только от последней версии, а остальные настройки выполнить по всем пропускаемым при обновлении релизам.

Внимание

При обновлении достаточно скопировать файл дистрибутива на сервер и в каталоге с ним выполнить команду `./blitz-XX.bin`, где `XX` - номер версии.

```
./blitz-5.33.9.bin
```

Ключи в команду, как это делается при установке, добавлять не нужно.

Внимание

В случае СУБД PostgreSQL нужно проверить по актуальному файлу `resources.zip`, какие в нем появились новые DDL-скрипты, и выполнить их, если такие изменения отсутствуют в текущей схеме БД.

Глава 1

5.33 -> 5.34

> **Внимание**
>
> Перед выполнением данного обновления в обязательном порядке должно быть проведено резервное копирование директории `/usr/share/identityblitz/blitz-config`.

1. В случае использования СУБД PostgreSQL применить скрипт `031-5.34.0.sql`.
2. Остановить приложения `blitz-*`.
3. В случае выполнения дополнительных HTTP-вызовов в Java-процедурах необходимо заменить устаревшие вызовы, выполнив скрипт:

```
find /usr/share/identityblitz/blitz-config -name '*.java' -exec sed -i 's/
↪HttpCall\.CallResponse/CallResponse/g' {} +
```

```
find /usr/share/identityblitz/blitz-config -name '*.java' -exec sed -i 's/
↪body()/body().asMap()/g' {} +
```

4. В случае использования внешнего поставщика идентификации VK ID необходимо скорректировать настройки. В файле `/usr/share/identityblitz/blitz-config/blitz.conf` в разделе `blitz.prod.local.idp.federation.points.vkid` найти блок конфигурации VK ID, например, `vkid_1`. Изменить следующие параметры, подставив новые значения:
   - `authUri`:

     ```
     "authUri" : "https://id.vk.ru/authorize"
     ```

   - `dataUri`:

     ```
     "dataUri" : "https://id.vk.ru/oauth2/user_info"
     ```

   - `tokenUri`:

     ```
     "tokenUri" : "https://id.vk.ru/oauth2/auth"
     ```

Листинг 1: Пример блока

```
"authUri" : "https://id.vk.ru/authorize",
"dataUri" : "https://id.vk.ru/oauth2/user_info",
"tokenUri" : "https://id.vk.ru/oauth2/auth"
```

5. Установить `blitz-5.34.bin`.

6. Запустить приложения `blitz-*`.

Глава 2

5.28 -> 5.31

> **Внимание**
>
> Перед выполнением данного обновления в обязательном порядке должно быть проведено резервное копирование директории `/usr/share/identityblitz/blitz-config`.

1. В случае использования СУБД PostgreSQL применить скрипты:
   - `026-5.29.0.sql`,
   - `027-5.30.0.sql`,
   - `028-5.31.0.sql`.

   > **Примечание**
   >
   > При применении возможны сообщения вида `ЗАМЕЧАНИЕ` / `WARNING`. Это ожидаемое поведение.

2. Установить `blitz-5.31.bin`.
3. В версии `5.31` переработан механизм настройки CAPTCHA. В связи с этим необходимо выполнить следующие действия:
   1. В файле `/usr/share/identityblitz/blitz-config/blitz.conf`:
      - В разделе `blitz.prod.local.idp` целиком удалить блок с CAPTCHA, при этом необходимо в отдельном файле сохранить значения параметров `plainParams.sitekey` / `secureParams.secret` для каждого типа CAPTCHA (будут использоваться далее при настройке).
      - В описанных ниже разделах (если такие существуют) удалить строки с полем `initJs` и изменить название поле `name` на `sysname`:
        - `blitz.prod.local.idp.login.methods.password.captcha`,
        - `blitz.prod.local.idp.provisioning.recovery.captcha`,
        - `blitz.prod.local.idp.provisioning.registration.captcha`,
        - `blitz.prod.local.idp.externalIdps.captcha`.
   2. В директории `/etc/blitz-config/captchas/` доступны два типа CAPTCHA:
      - `reCaptchaV3`, конфигурационный файл: `/etc/blitz-config/captchas/reCaptchaV3/reCaptchaV3.json`.

- `yandexSmartCaptcha`, конфигурационный файл: `/etc/blitz-config/captchas/yandexSmartCaptcha/yandexSmartCaptcha.json`.

В соответствии с тем, какая CAPTCHA была настроена ранее, необходимо выполнить настройки в соответствующем конфигурационном файле, при этом:

- значение `plainParams.sitekey` задать в параметре `jsConf.sitekey`.
- значение `secureParams.secret` задать в параметре `secretKey.value`.

4. В версии `5.31` для корректной работы сервиса `blitz-keeper` в режиме Token Exchange необходимо внести изменения в правила доступа по Token Exchange к защищаемым сервисам, которые создаются в директории `/usr/share/identityblitz/blitz-config/token_exchange/rules/`. В `subjectTokenCond` нужно добавить блок `"userAttrs": {}`:

```
"subjectTokenCond": {
"clientRights": [],
"userRights": [],
"userAttrs": {},
"scopes": ["openid"],
"userClaims": {},
"userGroups": []
}
```

5. Удалить устаревший импорт в Java-процедурах, выполнив скрипт:

```
for f in $(find /usr/share/identityblitz/blitz-config -name '*.java'); do
    sed -i 's/JsObj/JsObject/' $f;
done

for f in $(find /usr/share/identityblitz/blitz-config -name '*.java'); do
    sed -i 's/com.identityblitz.core.loop.JsObject/com.identityblitz.idp.
↪extensions.types.JsObject/' $f;
done

for f in $(find /usr/share/identityblitz/blitz-config -name '*.java'); do
    sed -i 's/com.identityblitz.idp.federation.matching.JsObject/com.
↪identityblitz.idp.extensions.types.JsObject/' $f;
done
```

6. Настроить задачи завершения сессий.

    1. В файле `/usr/share/identityblitz/blitz-config/blitz.conf`:

        - В раздел `tasks.executionRules` добавить:

```
{
     "maxAttempts" : 2,
     "name" : "postpone",
     "queue" : "postpone",
     "redeliveryDelayInSec" : 60
}
```

        - В раздел `tasks.queues` добавить:

```
{
     "dequeueBatchSize" : 10,
     "dequeuePeriodInSec" : 30,
     "executorPoolSize" : 5,
     "name" : "postpone"
 }
```

2. В файле `/etc/default/blitz-idp` в JAVA_OPTS добавить опцию:

```
-DblitzDispatchedQueues=postpone
```

7. Поскольку теперь, в версии `5.31`, утверждения (claims), разрешенные в `scope`, автоматически не добавляются в `access_token`, их нужно добавить вручную для каждого приложения. Это предотвратит увеличение `access_token` из-за ненужных атрибутов.

> **Совет**
>
> Помимо анализа `access_token`, приложение можно настроить так, чтобы оно получало данные пользователя через сервис `/blitz/oauth/me`.

> **Внимание**
>
> При использовании кастомной темы вместо переменных `regUrl` и `recUrl` теперь нужно писать `reg.url` и `rec.url` соответственно.

8. Необходимо добавить переменную, определяющую путь к `boot.conf`, в `/etc/default/blitz-idp`, `/etc/default/blitz-console`, `/etc/default/blitz-recovery`, `/etc/default/blitz-registration`:

```
export BOOT_FILE=/usr/share/identityblitz/blitz-config/boot.conf
```

Глава 3

5.26 -> 5.28

1. В случае использования СУБД PostgreSQL применить скрипты:
   - `024-5.27.0.sql`,
   - `025-5.28.0.sql`.
2. Установить `blitz-5.28.bin`.
3. Появилась возможность на втором факторе подтверждать вход вводом пароля. В связи с этим необходимо внести следующие изменения в файл конфигурации `/usr/share/identityblitz/blitz-config/blitz.conf`:
   - в разделе `blitz.prod.local.idp.login.methods.password` изменить конфигурацию на профилированную:

```
"password":{
 "profiles" : {
  "1": {
    Прежнее содержимое раздела password
  }
 }
}
```

   - при необходимости добавить метод входа по паролю в раздел `blitz.prod.local.idp.login.factors` во второй список:

```
"login" : {
     "factors" : [
         [
             …
         ],
         [
             {
                 "enabled" : false,
                 "method" : "password"
             },
             …
         ]
     ],
     …
 }
```

   - далее в консоли управления настроить и активировать метод подтверждения входа по паролю.

4. Добавлена возможность использовать для входа на первом факторе разовый код на основе времени (TOTP). В связи с этим необходимо внести следующие изменения в файл конфигурации `/usr/share/identityblitz/blitz-config/blitz.conf` даже при неиспользовании данного метода:

   - в разделе `blitz.prod.local.idp.login.factors` в первый фактор необходимо добавить:

   ```
   {
   "enabled" : false,
   "method" : "totp"
   }
   ```

   - в разделе `blitz.prod.local.idp.login.methods.totp` необходимо сменить конфигурацию на профилированную, а также убрать поля `android-download-url`, `ios-download-url`, `windows-download-url`, `issuer-label`, `user-label-attr` (эти поля перемещаются в другой раздел файла конфигурации):

   ```
   "totp": {
       "profiles": {
           "1": {
               "look-ahead-depth": 10,
               "look-backward-depth": 10,
               "tempLockAfter": 10,
               "tempLockForMin": 15
           },
           "2": {
               "look-ahead-depth": 10,
               "look-backward-depth": 10,
               "tempLockAfter": 10,
               "tempLockForMin": 15
           }
       }
   }
   ```

   - поля `android-download-url`, `ios-download-url`, `issuer-label`, `user-label-attr` теперь доступны в отдельном разделе `blitz.prod.local.idp.totp`. Поле `windows-download-url` больше не поддерживается. Пример конфигурационного файла:

   ```
   "totp": {
       "android-download-url": "https://play.google.com/store/apps/details?
   ↪id=com.google.android.apps.authenticator2",
       "ios-download-url": "https://itunes.apple.com/us/app/google-
   ↪authenticator/id388497605?mt=8",
       "issuer-label": "Blitz IDP",
       "look-ahead-depth": 15,
       "look-backward-depth": 15,
       "user-label-attr": "email"
   }
   ```

5. При использовании RabbitMQ необходимо внести изменения изменения в файл конфигурации `/usr/share/identityblitz/blitz-config/blitz.conf`. Переименованы следующие параметры подключения к RabbitMQ в блоке `blitz.prod.local.idp.events` в разделах `drivers.${driver_id}`:

   - Параметр `recovery_interval` переименован в `recoveryInterval`;
   - Параметр `properties.connections` переименован в `properties`;
   - Параметр `properties.publish` переименован в `deliveryProps`. Данный параметр предназначен для хранения свойств сообщения и регулирует отправку (`AMQP.BasicProperties`). В данном параметре можно конфигурировать только `deliveryMode` (значение по умолчанию 2 - Persistent).

Пример файла конфигурации:

```
"events": {
    "drivers": {
        "rabbit_driver": {
            "properties": { // optional
                "virtual": {
                    "host": "testVhost"
                }
            },
            "server": {
                "host": "localhost",
                "port": 5672
            },
            "type": "RMQ",
            "recoveryInterval": 60, // default 60
            "user": {
                "password": "quest",
                "username": "guest"
            },
            "ssl": { // optional
                "protocol": "TLSv1.2" // optional
            },
            "deliveryProps": { //optional
                "deliveryMode": 2 // default = 2
           },
            "channelsSize": 8, // default = 8
            "poolSize": 8 // default = 8
        }
    }
}
```

6. Добавлена возможность входа методом входящего звонка (flashCall) на первом факторе. В связи с этим необходимо внести следующие изменения в файл конфигурации `/usr/share/identityblitz/blitz-config/blitz.conf`.

   - При использовании метода:

     1. В разделе `blitz.prod.local.idp.login.factors` в первый фактор необходимо добавить:

        ```
        {
          "enabled" : false,
          "method" : "flashCall"
        }
        ```

     2. Необходимо удалить из конфигурационного файла из раздела `blitz.prod.local.idp.login.methods` старую конфигурацию для flashCall метода, поскольку больше нет обратной поддержки старого формата опций:

        ```
        "flashCall" : {
           "callTempLockAfter" : 10,
           "callTempLockForMin" : 15,
           "flow" : "flashcall.FlashCallFlow",
           "mobileAttrName" : "mobile",
           "psw-expire-time-sec" : 300,
           "psw-length" : 4,
           "psw-max-attempts" : 10,
           "tempLockAfter" : 10,
        ```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
    "tempLockForMin" : 15
}
```

3. Далее необходимо настроить метод в консоли. Для этого перейдите в раздел `Источники данных` и убедитесь, что мобильный атрибут может быть использован для операций поиска. Затем перейдите в раздел `Аутентификация` на вкладку `Первый фактор`. В разделе `Вход по входящему звонку` задайте соответствующие настройки.

- При неиспользовании метода:

  В разделе конфигурационного файла `blitz.prod.local.idp.login.methods` поместить старую конфигурацию в блок:

```
“flashCall” : {
  “profiles” : {
    “2” : {
      //Старые ключи
    }
  }
}
```

Глава 4

5.23 -> 5.26

1. В случае использования СУБД PostgreSQL применить скрипт: `023-5.26.0.sql`.
2. Установить `blitz-5.26.bin`.
3. В конфигурационном файле в параметр `attrs` прописать атрибуты для разрешений `blitz_api_sys_users`, `blitz_api_sys_users_chg`, `blitz_api_user`, `blitz_api_user_chg`. Ниже показан пример добавления атрибутов для разрешения `blitz_api_user`.

```
"attrs" : [
    "sub",
    "family_name",
    "company",
    "given_name"],
"client-level" : false,
"deprecated" : false,
"descriptions" : {
    "default" : "Получение атрибутов"
},
"enabled" : true,
"names" : {
    "default" : "blitz_api_user"
},
"sysname" : "blitz_api_user"
},
```

Глава 5

5.22.5 -> 5.23

1. В случае использования СУБД PostgreSQL применить скрипт: `022-5.23.0.sql`.
2. На серверах с Blitz Identity Provider установить JDK 11. Определить актуальное значение `JAVA_HOME`.
3. В файлах конфигурации `/etc/default/blitz-*` указать новое значение параметра `JAVA_HOME`.
4. Установить `blitz-5.23.bin`.
5. Теперь Blitz Identity Provider позволяет сохранять группы пользователя в организации, полученные от внешнего поставщика ЕСИА, и передавать их по запросу в утверждениях токена идентификации. Для того чтобы задействовать данную возможность, необходимо выполнить следующие действия:
   1. Открыть файл конфигурации `/usr/share/identityblitz/blitz-config/blitz.conf`.
   2. В секции `blitz.prod.local.idp.federation.points.esia.org.scopes` добавить разрешение на получение данных о группах пользователя `http://esia.gosuslugi.ru/org_grps`.

      ```
      "org" : {
         ...,
         "scopes" : [
              ...,
              "http://esia.gosuslugi.ru/org_grps"
         ]
      },
      ...
      ```

      В результате группы пользователя будут сохраняться в базе данных в атрибуте `org.groupNames`.
   3. Для передачи групп пользователя из атрибута `org.groupNames` в утверждение (`claim`) токена идентификации, внести изменения в секцию `blitz.prod.local.idp.federation.points.esia.claims`. Ниже показан пример передачи параметра в утверждение с именем `org_groups`.

      ```
      "claims" : [
         {
          "name" : "org_groups",
          "value" : "org.groupNames"
         }
      ]
      ```
6. При наличии настроек провести миграцию имен в новый формат в блоке `blitz.prod.local.idp.internal-store-jdbc.pool`:
   - `max_total_conn` -> `maxTotalConn`,
   - `max_idle_conn` -> `maxIdleConn`,

- `min_idle_conn` -> `minIdleConn`,
- `max_wait_conn_ms` -> `maxWaitConnMs`.

В тот же блок добавить параметры расширенной настройки пула соединений.

Пример настроек после редактирования:

```
"internal-store-jdbc" : {
     "pool" : {
         "maxIdleConn" : 10,
         "maxTotalConn" : 20,
         "maxWaitConnMs" : 30000,
         "minIdleConn" : 7,
         "testOnBorrow" : false,
         "testOnCreate" : false,
         "testOnReturn" : false,
         "testWhileIdle" : true,
         "timeBetweenEvictionRunsMillis" : 30000,
         "validationQuery" : ""
     }
}
```

7. При необходимости задействовать следующие новые возможности:
   - Потребовать при восстановлении доступа подтверждение по второму фактору только в случае, если для пользователя включен хотя бы один метод из списка методов дополнительной проверки (`Необходимость дополнительной проверки` -> `Требовать, если доступна`).
   - Добавить параметры `obj_type` (тип пользователя) и `roles` (типы ролей пользователя) в вызов сервиса аутентификации ЕСИА.
   - Добавить возможность регистрации пользователя во внешнем поставщике при входе через него.
   - Настроить отображение в консоли и Личном кабинете информации о привязанных внешних аккаунтах пользователя. Настройку можно сделать в консоли, посредством процедуры на Java и через API.
   - В процедуру обработки запросов RADIUS добавить функции, позволяющие выбирать способ подтверждения входа и отображать краткую инструкцию по способам подтверждения.
   - Настроить интервал считывания глобальной конфигурации кластера Couchbase Server.

Глава 6

5.21.1 -> 5.22.5

1. Установить `blitz-5.22.5.bin`.
2. При необходимости задействовать новые возможности:
   - Настроить первичный вход по электронной почте.
   - Выбрать хранилище учетных записей для первичного входа по SMS.
   - Настроить аутентификацию с ЕСИА с использованием КриптоПро JCP.
   - Отключить запоминание логина пользователя для будущих входов.
   - Добавить в процедуру входа вызов сброса сессии.
   - Добавить в процедуру входа кастомные ошибки.
   - Настроить метки приложений и задействовать их в процедуре входа.
   - Кастомизировать логотип и CSS-оформление Личного кабинета.
   - Настроить получение признака `isIdentified` из Tinkoff ID.
3. Если профили первого и второго фактора для методов входа по коду из SMS/push, с помощью электронной почты или ключа безопасности ранее были объединены, необходимо открыть файл конфигурации `/usr/share/identityblitz/blitz-config/blitz.conf` и разделить профили вручную в секциях `email`, `sms`, `webAuthn` раздела `idp.login.methods`. В настройки второго фактора не нужно переносить параметры `bind`, `storeRouter`, `factorCoverage` (только для `webAuthn`).

Листинг 1: Пример разделения профилей для входа с помощью электронной почты

```
"email": {
    "profiles": {
        "1": {
            "attr": "${email-}",
            "bind": [
                [
                    {
                        "attr": "email",
                        "value": "${login}"
                    }
                ]
            ],
            "psw-expire-time-sec": 300,
            "psw-length": 6,
            "psw-max-attempts": 3,
            "tempLockAfter": 100,
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
            "tempLockForMin": 1,
            "storeRouter": {}
        },
        "2": {
            "attr": "${email-}",
            "psw-expire-time-sec": 300,
            "psw-length": 6,
            "psw-max-attempts": 3,
            "tempLockAfter": 100,
            "tempLockForMin": 1
        }
    }
}
```

Листинг 2: Пример разделения профилей для входа по коду из SMS/push

```
"sms": {
    "profiles": {
        "1": {
            "bind": [
                [
                    {
                        "attr": "personal_mobile",
                        "value": "${login}"
                    }
                ],
                [
                    {
                        "attr": "uid",
                        "value": "${login}"
                    }
                ]
            ],
            "channels": [
                {
                    "attr": "${personal_mobile-}${uid-}",
                    "type": "push"
                },
                {
                    "attr": "${personal_mobile-}",
                    "type": "sms"
                }
            ],
            "psw-expire-time-sec": 30,
            "psw-length": 2,
            "psw-max-attempts": 3,
            "tempLockAfter": 10,
            "tempLockForMin": 15,
            "storeRouter": {}
        },
        "2": {
            "channels": [
                {
                    "attr": "${personal_mobile-}${uid-}",
                    "type": "push"
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
                },
                {
                    "attr": "${personal_mobile-}",
                    "type": "sms"
                }
            ],
            "psw-expire-time-sec": 30,
            "psw-length": 2,
            "psw-max-attempts": 3,
            "tempLockAfter": 10,
            "tempLockForMin": 15
        }
    }
}
```

Листинг 3: Пример разделения профилей для входа с помощью ключа безопасности

```
"webAuthn" : {
    "profiles" : {
        "1" : {
            "alwaysApplicable" : true,
            "bind" : [
                [
                    {
                        "attr" : "surname",
                        "value" : "mysurname"
                    }
                ]
            ],
            "factorCoverage" : 2,
            "storeRouter" : {
                "cases" : [
                    {
                        "matchers" : [
                            {
                                "not" : false,
                                "pattern" : "myemail@m.ru",
                                "source" : "${login}"
                            }
                        ],
                        "result" : "dldap01"
                    }
                ]
            },
            "trustedAttestationModes" : [
                "FULL",
                "FULL_NO_ROOT",
                "SELF"
            ]
        },
        "2" : {
            "alwaysApplicable" : false,
            "trustedAttestationModes" : [
                "FULL",
                "FULL_NO_ROOT",
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
                    "SELF"
                ]
            }
        }
}
```

Глава 7

5.20.0 -> 5.21.0 (5.21.1)

1. В случае использования СУБД PostgreSQL применить скрипт: `021-5.21.0.sql`.
2. Установить `blitz-5.21.0`.bin.
3. При необходимости задействовать новую возможность: настроить доступ к сетевым службам по протоколу RADIUS.
4. В новой версии изменился установленный по умолчанию идентификатор поставщика идентификации `issuer`, а также URL сервиса OpenID Connect Discovery:

   - В предыдущих версиях `issuer` соответствовал значению `domain`, где `domain` – внешнее имя домена системы. Теперь `issuer` формируется как `domain/context`, где `context` – URL-путь, на котором функционирует Blitz Identity Provider.
   - В предыдущих версиях сервис OIDC Discovery располагался по адресу `https://<issuer>/<context>/oauth/.well-known/openid-configuration`. Теперь адрес формируется как `https://<issuer>/.well-known/openid-configuration`.

   С учетом вышесказанного после установки обновления сервис OIDC Discovery автоматически переместится на адрес `https://<domain>/<context>/.well-known/openid-configuration`.

   Система продолжит работу, поскольку для обратной совместимости со старого адреса настроен редирект на новый адрес. В данной ситуации вы можете пойти по одному из следующих путей:

   1. Не менять настройки приложений, но явно указать значение `issuer` в секции `blitz.prod.local.idp.net` файла конфигурации `/usr/share/identityblitz/blitz-config/blitz.conf` как всё, что стоит перед `/.well-known/openid-configuration`. Это позволит избежать лишних редиректов при функционировании системы.

      > **Внимание**
      >
      > Решение не рекомендуется в долгосрочной перспективе.

      ```
      "net" : {
         "domain" : "demo.idblitz.ru",
         "issuer" : "demo.idblitz.ru/blitz/oauth",
         ...
      },
      ...
      ```

   2. Рекомендуется Привести настройки своей системы и подключенных приложений в соответствие с новыми правилами, указав в них значение адреса OIDC Discovery как `https://<domain>/<context>/.well-known/openid-configuration`.

Глава 8

5.18.0 -> 5.20.0

1. В случае использования СУБД PostgreSQL применить скрипт: `020-5.20.0.sql`.
2. Установить `blitz-5.20.0`.bin.
3. При необходимости настроить новые способы аутентификации:
    - подтверждение входа по входящему звонку (Flash Call);
    - автоматическая идентификация пользователя по свойствам сессии;
    - вход через внешний поставщик VK ID.
4. При необходимости задействовать новые возможности кастомизации работы с помощью программирования на Java:
    - запрос ввода пользователем контрольного вопроса (готовая процедура);
    - получение геоданных пользователя;
    - кастомизация логики операций с хранилищами данных.

Глава 9

5.16.2 -> 5.18.0

1. В случае использования СУБД PostgreSQL применить скрипты:
    1. `018-5.17.0.sql`
    2. `019-5.18.0.sql`
2. Найти в конфигурационном файле `blitz.conf` блок настроек `blitz.prod.local.idp.provisioning.recovery`. Внести в блок следующие изменения:
    1. Переименовать настройку `security-question` в `system-security-questions`.
    2. Создать блок `factor2` и перенести в него целиком секцию `methods` с содержимым. Удалить исходную секцию `methods`.
    3. В блоке `factor2` установить `"mode" : "by_user_required_factor"`.

Листинг 1: Пример блока после редактирования

```
"recovery" : {
    "dropInactivityLock" : true,
    "factor2" : {
        "methods" : [
            "email",
            "sms",
            "totp"
        ],
        "mode" : "by_user_required_factor"
    },
    "recovery-contacts" : [
        "phone_number",
        "email"
    ],
    "search-attrs" : [
        "email",
        "phone_number"
    ],
    "system-security-questions" : {
        "attrs" : [
            "family_name"
        ]
    }
}
```

3. Установить `blitz-5.18.0.bin`.

Глава 10

5.15.x -> 5.16.x

1. В настройках `nginx` закрыть доступ на адреса `/blitz/metrics` из внешних сетей:

```
location /blitz/metrics {
    return 404;
}
```

2. При использовании для приложений особых `bundle` с помощью `lang-variant` (опциональное поле `lang-variant` в настройках приложения) нужно все варианты языка прописать в настройку `lang` в `blitz.conf` в настройку `lang-variant`.

   Пример:

```
"lang": {
    "ignore-browser": false,
    "lang-variants": ["12345", "12346"], // this field
    "languages": ["ru","en"],
    "portal-lang-cookie": {
        "domain": ".identityblitz.ru",
        "name": "portal_lang"
    }
}
```

3. Установить новый `blitz.bin`.
4. При необходимости настроить сбор метрик функционирования в **`Prometheus`** через непосредственное обращение к `/blitz/metrics` по внутренним адресам серверов приложений.
5. При необходимости настроить хранение настроек приложений в отдельных файлах.

Глава 11

5.14.0 -> 5.15.x

1. В случае использования СУБД PostgreSQL применить скрипты:
    a. `017-5.15.0.sql`
2. Установить новый `blitz.bin`.

Глава 12

5.11.x -> 5.14.0

1. В случае использования СУБД PostgreSQL применить скрипты:
   a. `015-5.12.0.sql`,
   b. `016-5.13.0.sql`
2. Установить новый `blitz.bin`.
3. В разделе *«Внешний вид»* проверить, что для всех шаблонов в поле *«Название шаблона»* задано уникальное имя. Если есть несколько шаблонов с одинаковым названием, то переименовать их.
4. Для каждого настроенного внешнего поставщика идентификации в новом блоке *«Выбор пользователя»* заполнить значения настроек *«Имя пользователя»* и *«Идентификатор пользователя»*. Пример заполнения:
   - Имя пользователя – `${given_name-} ${family_name-}`
   - Идентификатор пользователя – `${email&maskInMiddle(4,8)}`

   Настройка используется в процессе привязки пользователя при первом входе через внешний поставщик идентификации. На основе настройки пользователю показывается карточка найденной для привязки учетной записи в Blitz Identity Provider, соответствующей учетной записи внешнего поставщика идентификации.
5. Проверить функции входа через внешние поставщики идентификации, если внешний вид экранов привязки при входе будет нарушен, то скорректировать используемые темы внешнего вида.
6. Корректировка настроек в конфигурационном файле `console.conf`:
   a. Если используется вход в консоль управления по логину/паролю, то в `console.conf` добавить настройку `roleClaim` с пустым значением:

   Пример:

```
{
"login" : {
    "fp" : {

    ...
    "subjectClaim" : "sub",
    "roleClaim" : "",
    ...
    },
    "mode" : "credentials"
}
}
```

b. Если используется функция входа в консоль управления через SSO, то в `console.conf` в блок `login.fp` добавить настройку `roleClaim`. В качестве значения указать имя атрибута из `id_token`, в котором передается роль администратора (обычные названия ролей: `root`, `security`, `sysadmin`, `app_admin`, `ui_admin`, `support`, берутся из файла настроек `credentials` из `roles.name`). Настроить, чтобы внешняя IDP передавала атрибут с ролью. Атрибут может быть текстовым (`String`) – тогда передается одна роль, или массивом строк (`ArrayOfString`), тогда можно передавать множество ролей.

Пример:

```
{
"login" : {
    "fp" : {

    ...
    "subjectClaim" : "sub",
    "roleClaim" : "SOME_CLAIM_NAME",
    ...
    },
    "mode" : "sso"
}
}
```

Из меню *“Администраторы”* консоли можно удалить тех пользователей-админов, которые входят только через внешний SSO-вход.

Глава 13

5.10.0 -> 5.11.x

1. В случае использования СУБД PostgreSQL применить скрипты `000-service-tasks.sql`, `013-tasks.sql`, `014-sec_ch_ua.sql`.
2. Проверить нестандартные строчки в `custom_messages`. Если в строчках с текстами писем используется функция `$[device.mkey&dic(dics.devices)]`, то заменить ее на `$[device.mkey&dic(dics.devices,os.ver)]`.
3. Установить новый `blitz.bin`.
4. В файле `play.conf` скорректировать настройки подключения к memcached – добавить `operationTimeout`, `timeoutExceptionthreshold`, `maxReconnectDelay`:
   - `operationTimeout` – время ожидания выполнения запроса к memcached в мс;
   - `timeoutExceptionThreshold` – количество попыток выполнения запроса, после которых узел считается не доступным;
   - `maxReconectDelay` – интервал между попытками установить соединение с узлом в секундах.

   Пример конфига с добавленными настройками с рекомендуемыми значениями:

   ```
   "memcached" : {
   "operationTimeout" : 1000,
   "timeoutExceptionThreshold" : 1,
   "maxReconnectDelay" : 10,
   "servers" : [
       …
   ]
   }
   ```

5. В случае использования СУБД PostgreSQL при необходимости переключить обработку задач с брокера RabbitMQ на брокер jdbc (это можно сделать если RabbitMQ больше ни для чего не используется и есть желание отказаться от его дальнейшего использования). Брокер jdbc рекомендуется использовать только в средах с небольшой нагрузкой.

   Для настройки использования брокера jdbc необходимо:

   - Проверить, что в блоке настроек `stores` в файле `blitz.conf` задана настройка `default-type` в значении jdbc:

     ```
     "stores" : {
     "default-type" : "jdbc"
     },
     ```

   - В файл `blitz.conf` в блоке `tasks` скорректировать настройки брокера следующим образом:

```
"tasks" : {
"broker-type" : "task-store",
"executionRules" : [
   {
   "maxAttempts" : 2,
   "queue" : "blitz-tasks",
   "redeliveryDelayInSec" : 60
   }
],
"queues" : [
   {
   "dequeueBatchSize" : 10,
   "dequeuePeriodInSec" : 30,
   "executorPoolSize" : 5,
   "name" : "blitz-tasks"
   }
]
}
```

- Серверу, выполняющему обработку задач, добавить параметр запуска `akka.coordinated-shutdown.phases.service-stop.timeout` в значении `30s`:

```
Dakka.coordinated-shutdown.phases.service-stop.timeout=30s
```