

ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ  
БАЗАМИ ДАННЫХ «ЈАТОВА»

Руководство по настройке. Часть 4.  
Инструкция по безопасной настройке кластера на основе  
компонента «jaDog».

643.72410666.00067-07 98 02-04

Листов 31

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

## АННОТАЦИЯ

Настоящий документ является дополнением к существующему документу «Руководство по безопасности. Часть 27» и описывает рекомендации по безопасной настройке СУБД Jatoba.

Настоящее руководство предназначено для администраторов СУБД, специалистов по информационной безопасности и носит рекомендательный характер.

Степени важности примечаний, применяемые в документе:



**Важная информация** – указания, требующие особого внимания



**Дополнительная информация** – указания, позволяющие упростить работу с изделием



Все примеры в данном документе приведены для СУБД «Jatoba» версии ядра 6.x, для других версий все шаги выполняются аналогично, разница состоит в именах директорий.

Например, СУБД «Jatoba» версии 6.x по умолчанию устанавливается в директорию:

- ОС Windows – «C:\Program Files\GIS\Jatoba\6\bin»;
- ОС Linux – «/usr/jatoba-6/bin».



**Важная информация**

Для сертифицированной версии СУБД «Jatoba» поддерживается работа только на ОС, указанных в формуляре на поставку!

## СОДЕРЖАНИЕ

1. Актуальность версий .....	4
2. Подключение .....	6
2.1. Минимизация количества пользователей/ролей, которым разрешено подключение к БД .....	6
2.2. Минимизация количества узлов/подсетей, с которых разрешено подключение к БД .....	7
2.3. Минимизация количества БД, к которым разрешено подключение .....	7
2.4. Минимизация количества УЗ, которым разрешено подключение к компоненту jaDog .....	8
2.5. Минимизация количества узлов/подсетей, с которых разрешено подключение к компоненту jaDog ..	9
2.6. Измените номер порта, используемый Jatoba на узлах кластера, на нестандартный .....	10
2.7. Измените номера портов, используемые jaDog, на нестандартные .....	11
3. Применение TLS/SSL .....	13
3.1. Настройте проверку SSL-сертификатов при подключении к узлам кластера .....	13
3.2. Настройте проверку SSL-сертификатов при подключении к компоненту jaDog .....	14
3.3. Настройте подключение jaDog к СУБД с помощью SSL-сертификатов .....	15
3.4. Настройте подключение к REST API с помощью SSL-сертификатов .....	16
3.5. Настройте минимальную версию протокола TLS не ниже рекомендованной .....	17
4. Аутентификация .....	19
4.1. Используйте надёжный метод аутентификации при подключении к узлам кластера .....	19
4.2. Используйте надёжный метод аутентификации при подключении к компоненту jaDog .....	19
4.3. Измените пароли всех технических и административных УЗ при переводе системы в эксплуатацию	20
5. Журналирование .....	21
5.1. Настройте параметры журналирования компонента jaDog .....	21
5.2. Настройте журналирование компонентом jaDog событий информационной безопасности .....	22
6. Хеширование и маскирование .....	24
6.1. Настройте стойкий алгоритм хеширования паролей в БД на узлах кластера .....	24
7. Контроль целостности .....	26
7.1. Установите расширение ja_csum и зафиксируйте эталонные контрольные суммы .....	26
8. Резервное копирование .....	27
8.1. Храните резервную копию файла ответов со структурой кластера в удалённом сетевом хранилище	27
Термины и определения .....	28
Перечень сокращений .....	30

## 1. АКТУАЛЬНОСТЬ ВЕРСИЙ

Используйте актуальную версию ПО СУБД «Jatoba» и компонентов, регулярно проверяйте выпуск обновлений.

Чем старше версия используемого программного обеспечения, тем больше времени было у злоумышленников на то, чтобы найти в ней уязвимости и «эксплойты» и, соответственно, тем уязвимее будет информационная система.

Чтобы защитить системы от потенциальных угроз, необходимо своевременно устанавливать обновления безопасности, закрывающие известные уязвимости в программном обеспечении.

Для проверки используемой версии СУБД «Jatoba» можно воспользоваться командой в терминале ОС:

### Пример команды

```
/usr/jatoba-6/bin/postgres --version
```



Мажорные версии PostgreSQL и Jatoba соотносятся следующим образом:

- PostgreSQL 14 - Jatoba 4;
- PostgreSQL 15 - Jatoba 5;
- PostgreSQL 16 - Jatoba 6.

При подключении к СУБД, можно воспользоваться следующей функцией:

### Пример функции

```
SELECT jatoba_version();
```

Для получения версий установленных компонентов необходимо подключиться к БД, в которую они установлены, и выполнить запрос к системному каталогу:

### Пример запроса

```
SELECT extname, extversion FROM pg_catalog.pg_extension;
```

В терминале psql можно воспользоваться метакомандой:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

### Пример метакоманды

\dx

Процедуры обновления СУБД «Jatoba» и компонентов приведены в документе "Руководство по обновлению" или руководствах на компоненты.



Из соображений требований ИБ начиная с мажорной версии 4 компонента jaDog его процессы в ОС выполняются не от имени УЗ root, а от имени технологической УЗ, от которой запущен сервер СУБД «Jatoba».

## 2. ПОДКЛЮЧЕНИЕ

### 2.1. Минимизация количества пользователей/ролей, которым разрешено подключение к БД

Ограничение количества учётных записей, имеющих возможность подключения к СУБД, снижает шансы злоумышленника получить доступ к СУБД.

Возможность подключения к СУБД узла кластера настраивается в конфигурационном файле `pg_hba.conf`.

Наиболее безопасным вариантом будет указание в файле `pg_hba.conf` возможности подключения только технической учётной записи для взаимодействия JaDog с СУБД (`db_connection_settings:user`) и минимально необходимого списка учётных записей администраторов и технических учётных записей приложений.



В процессе развёртывания кластера создаётся (в случае развёртывания с помощью `jadog0` и файла ответов - автоматически, в случае ручного развёртывания - при вызове функции `grant_jadog_role_to_jadog_user('<username>')`) групповая роль `jadog_repl_acc`, являющаяся членом (с параметрами `SET` и `INHERIT`) встроенной роли `pg_read_all_stats` и имеющая атрибуты `INHERIT` и `REPLICATION`. Техническая учётная запись для взаимодействия JaDog с СУБД (примерах ниже - `jadog_user`) включается в роль `jadog_repl_acc`.

В приведённом ниже примере конфигурации настроена возможность подключения только для технической УЗ JaDog (`jadog_user`) и УЗ администратора инстанса СУБД (`db_admin`):

#### Пример конфигурационного файла `pg_hba.conf`

```
# TYPE      DATABASE  USER          ADDRESS          METHOD
# "local" is for Unix domain socket connections only
local      [db_name] db_admin              peer
hostssl    [db_name] jadog_user          127.0.0.1/32     cert
hostssl    [db_name] jadog_user          192.168.239.131/32 cert
hostssl    replication jadog_user          127.0.0.1/32     cert
```

hostssl replication jadowg_user	192.168.239.131/32	cert
---------------------------------	--------------------	------

## 2.2. Минимизация количества узлов/подсетей, с которых разрешено подключение к БД

В дополнение к предыдущему пункту, ограничение в конфигурационном файле `pg_hba.conf` количества адресов/подсетей, с которых возможно подключение к СУБД на каждом узле кластера, позволяет ещё сильнее уменьшить шансы злоумышленника на проникновение в СУБД. Даже в случае получения данных одной из учётных записей злоумышленнику придётся дополнительно получить контроль над хостом в определённой подсети, чтобы подключиться к СУБД.

По возможности не используйте значение 'all' в поле ADDRESS конфигурационного файла `pg_hba.conf`, такая настройка позволит злоумышленнику попытаться подключиться с любого хоста, над которым у него есть контроль. Вместо этого лучше использовать отдельные адреса узлов, с которых необходимо подключение к экземпляру СУБД, либо ограниченные подсети.

В приведённом ниже примере конфигурации настроена возможность подключения технической УЗ JaDog (`jadowg_user`) только с `localhost` и с внешнего адреса самого узла.

### Пример конфигурационного файла `pg_hba.conf`

#	TYPE	DATABASE	USER	ADDRESS	METHOD
	hostssl	[db_name]	jadowg_user	127.0.0.1/32	cert
	hostssl	[db_name]	jadowg_user	192.168.239.131/32	cert
	hostssl replication		jadowg_user	127.0.0.1/32	cert
	hostssl replication		jadowg_user	192.168.239.131/32	cert

## 2.3. Минимизация количества БД, к которым разрешено подключение

В дополнение к предыдущим пунктам, ограничение в конфигурационном файле `pg_hba.conf` количества баз данных, к которым возможно подключение, дополнительно снижает шансы злоумышленника на проникновение в СУБД. Даже в случае получения данных одной из учётных записей и обретения контроля над одним из хостов в определённой подсети злоумышленнику придётся подобрать название базы для подключения.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

По возможности не используйте значение 'all' в поле DATABASE конфигурационного файла pg\_hba.conf, такая настройка позволит злоумышленнику попытаться подключиться данным именем УЗ к любой базе данных.



Данная рекомендация не относится к техническому пользователю для взаимодействия JaDog с СУБД (db\_connection\_settings:user), ему как раз нужна возможность подключения ко всем базам данных.

В приведённом ниже примере конфигурации настроена возможность подключения технической УЗ приложения (appuser) только к БД этого приложения (appdb).

#### Пример конфигурационного файла pg\_hba.conf

#	TYPE	DATABASE	USER	ADDRESS	METHOD
hostssl		appdb	appuser	192.168.239.101/32	cert

#### 2.4. Минимизация количества УЗ, которым разрешено подключение к компоненту jaDog

Ограничение количества учётных записей, имеющих возможность подключения к компоненту JaDog, снижает шансы злоумышленника получить контроль над кластером. Возможность подключения к компоненту JaDog узла кластера настраивается в конфигурационном файле jadog\_hba.cfg (см. документ "Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»" п. 4.2.1.).

В случае использования парольной аутентификации между узлами кластера наиболее безопасным вариантом будет указание в файле конфигурации jadog\_hba.cfg возможности подключения только технической учётной записи для взаимодействия с другими JaDog-сервисами (param\_jadog:interconnect\_user) и минимально необходимого списка учётных записей администраторов.

В приведённом ниже примере конфигурации настроена возможность подключения только УЗ для взаимодействия с другими JaDog-сервисами (admin) и УЗ администратора (administrator).

#### Пример конфигурационного файла jadog\_hba.cfg

#	USER	ADDRESS	METHOD
	admin	127.0.0.1/32	sha-256

№ изменения: \_\_\_\_\_ | Подпись отв. лица: \_\_\_\_\_ | Дата внесения изм: \_\_\_\_\_



admin	192.168.239.0/24	sha-256
administrator	192.168.239.0/24	sha-256

В случае же использования аутентификации между узлами кластера с использованием SSL-сертификатов помимо озвученных выше УЗ в файле конфигурации `jadog_hba.cfg` на каждом узле кластера обязательно должна быть указана возможность подключения для пользователей, имя которых совпадает с полем CN серверных сертификатов остальных узлов кластера (т.к. в таком случае компонент JaDog одного узла кластера при подключении будет представляться другому узлу именем, указанным в поле CN серверного сертификата, и при отсутствии таких записей в `jadog_hba.cfg` межузловое взаимодействие будет невозможно).

В приведённом ниже примере конфигурации настроена возможность подключения только УЗ для взаимодействия с другими JaDog-сервисами (admin) и CN серверных сертификатов других узлов кластера (jadog-node2 и jadog-node3).

#### Пример конфигурационного файла `jadog_hba.cfg`

# USER	ADDRESS	METHOD
admin	127.0.0.1/32	ssl
admin	192.168.239.0/24	ssl
jadog-node2	192.168.239.132/32	ssl
jadog-node3	192.168.239.133/32	ssl

По возможности не используйте значение 'all' в поле USER конфигурационного файла `jadog_hba.cfg` – такая настройка увеличивает для злоумышленника шанс подобрать имя учётной записи методом перебора.

### 2.5. Минимизация количества узлов/подсетей, с которых разрешено подключение к компоненту jaDog

В дополнение к предыдущему пункту, ограничение в конфигурационном файле `jadog_hba.cfg` количества адресов/подсетей, с которых возможно подключение к компоненту jaDog на каждом узле кластера позволяет ещё сильнее уменьшить шансы злоумышленника на получение контроля над кластером. Даже в случае получения данных одной из учётных записей злоумышленнику придётся дополнительно получить контроль над хостом в определённой подсети, чтобы подключиться к кластеру (см. документ "Руководство по

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»" п. 4.2.1.).

По возможности не используйте значение 'all' в поле ADDRESS конфигурационного файла jadog\_hba.cfg, такая настройка позволит злоумышленнику попытаться подключиться с любого хоста, над которым у него есть контроль. Вместо этого лучше использовать отдельные адреса узлов, с которых необходимо подключение к компоненту jaDog, либо ограниченные подсети.

В приведённом ниже примере конфигурации настроена возможность подключения УЗ для взаимодействия с другими jaDog-сервисами (admin) только с localhost и подсети кластера, а CN серверных сертификатов других узлов кластера (jadog-node2 и jadog-node3) - только с адресов соответственных узлов.

#### Пример конфигурационного файла jadog\_hba.cfg

# USER	ADDRESS	METHOD
admin	127.0.0.1/32	ssl
admin	192.168.239.0/24	ssl
jadog-node2	192.168.239.132/32	ssl
jadog-node3	192.168.239.133/32	ssl

#### 2.6. Измените номер порта, используемый Jatoba на узлах кластера, на нестандартный

Изменение стандартного номера порта на случайный усложняет для злоумышленника проведение автоматизированных атак (с помощью ботов или автоматизированных скриптов).

Для изменения номера порта откройте конфигурационный файл postgresql.conf и измените значение параметра port:

#### Пример конфигурации

```
port = 5432
```

Измените стандартное значение 5432 на любой другой номер порта, не задействованный на этом сервере.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

Значение параметра port также можно изменить при помощи команды ALTER SYSTEM:

### Пример запроса

```
ALTER SYSTEM SET port = 5433;
```

После изменения значения параметра port нужно перезагрузить экземпляр СУБД (т.к. параметр имеет контекст postmaster).



Обратите внимание на то, что после изменения номера порта в конфигурации СУБД «Jatoba» нужно указать этот порт в параметрах подключения jaDog к Jatoba

Для того, чтобы указать компоненту jaDog на каком порту работает экземпляр Jatoba, можно воспользоваться командой утилиты jadog\_ctl:

### Пример команды

```
set parameter db_connection_settings:port = '5433'
```

Также можно скорректировать файл конфигурации jadog.yml вручную: изменить номер порта, указанный в строке подключения в секции param\_connection: → port.



Обратите внимание на то, что после ручного изменения конфигурационного файла jadog.yml для вступления новых значений параметров в силу потребуются перезапуск компонента jaDog, что может привести к failover. Таким образом, ручные операции с файлом конфигурации должны выполняться либо до сборки кластера, либо при установленном режиме технического обслуживания (см. документ "Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»" п. 7.16.).

## 2.7. Измените номера портов, используемые jaDog, на нестандартные

Аналогично предыдущему пункту, стандартные порты, используемые компонентом jaDog для своей работы, могут быть использованы злоумышленником в автоматизированной атаке, поэтому их также следует изменить на любые не задействованные на данном сервере.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

Для изменения портов, используемых jaDog, а также адреса, который прослушивает REST API, можно воспользоваться командами утилиты jadog\_ctl:

### Пример команд

```
set parameter param_jadog:port = '12345'  
set parameter param_jadog:user_interface_port = '54321'  
set parameter param_rest_api:rest_api_listen_port = '54443'  
set parameter param_rest_api:rest_api_listen_address =  
'127.0.0.1'
```

Также можно скорректировать файл конфигурации jadog.yml вручную - изменить номера портов и адрес, указанные в секциях param\_jadog и param\_rest\_api:

### Пример конфигурации

```
param_jadog:  
  port: 12345  
  user_interface_port: 54321  
  
param_rest_api:  
  rest_api_listen_port: 54443  
  rest_api_listen_address: 127.0.0.1
```



Обратите внимание на то, что после ручного изменения конфигурационного файла jadog.yml для вступления новых значений параметров в силу потребуется перезапуск компонента jaDog, что может привести к failover. Таким образом, ручные операции с файлом конфигурации должны выполняться либо до сборки кластера, либо при установленном режиме технического обслуживания (см. документ "Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»" п. 7.16.).

### 3. ПРИМЕНЕНИЕ TLS/SSL

#### 3.1. Настройте проверку SSL-сертификатов при подключении к узлам кластера

Наиболее безопасным методом аутентификации при подключении к узлам кластера является метод `cert`, предполагающий проверку подлинности как клиента сервером, так и сервера клиентом, а также задействующий шифрование данных, передаваемых между клиентом и сервером. Применение этого метода аутентификации позволяет защититься от атак типа MITM (Man-in-the-Middle).

Для примера настройки см. документ "Руководство по безопасности. Часть 27." п. 7.1. При добавлении записей в конфигурационный файл `pg_hba.conf` на узлах кластера руководствуйтесь принципами, описанными в п. 4.1. - 4.3. настоящего руководства.

Пример указания сертификатов в конфигурационном файле `postgresql.conf`.

#### Пример конфигурационного файла `pg_hba.conf`

```
ssl = on
ssl_ca_file = '/var/lib/jatoba/certs/root.crt'
ssl_cert_file = '/var/lib/jatoba/certs/server.crt'
ssl_crl_file = '/var/lib/jatoba/certs/root.crl.pem'
ssl_crl_dir = '/var/lib/jatoba/certs/'
ssl_key_file = '/var/lib/jatoba/certs/server.key'
```

Пример настройки проверки сертификатов при подключении технической УЗ (`jadog_user`) в конфигурационном файле `pg_hba.conf` (при указании метода аутентификации `cert` указание параметра `clientcert` не требуется).

#### Пример конфигурации

#	TYPE	DATABASE	USER	ADDRESS	METHOD
hostssl		[db_name]	jadog_user	127.0.0.1/32	cert
hostssl		[db_name]	jadog_user	192.168.239.131/32	cert
hostssl		replication	jadog_user	127.0.0.1/32	cert
hostssl		replication	jadog_user	192.168.239.131/32	cert

### 3.2. Настройте проверку SSL-сертификатов при подключении к компоненту jaDog

Для примера настройки см. документ "Руководство по безопасности. Часть 27." п. 7.1. При добавлении записей в конфигурационный файл `jadog_hba.cfg` на узлах кластера руководствуйтесь принципами, описанными в п. 2.1 - 2.5 данного документа.

Для указания сертификатов, используемых jaDog для соединения между узлами, можно воспользоваться командами утилиты `jadog_ctl`.

#### Пример команд

```
set parameter param_ssl:ssl = 'true'
set parameter param_ssl:ssl_ca_file =
'/var/lib/jatoba/certs/root.crt'
set parameter param_ssl:ssl_cert_file =
'/var/lib/jatoba/certs/server.crt'
set parameter param_ssl:ssl_crl_file =
'/var/lib/jatoba/certs/root.crl.pem'
set parameter param_ssl:ssl_key_file =
'/var/lib/jatoba/certs/server.key'
```

Также можно скорректировать файл конфигурации `jadog.yml` вручную – изменить значения параметров, указанных в секции `param_ssl`.

#### Пример конфигурации

```
param_ssl:
  ssl: true
  ssl_ca_file: /var/lib/jatoba/certs/root.crt
  ssl_cert_file: /var/lib/jatoba/certs/server.crt
  ssl_crl_file: /var/lib/jatoba/certs/root.crl.pem
  ssl_key_file: /var/lib/jatoba/certs/server.key
```



Обратите внимание на то, что после ручного изменения конфигурационного файла `jadog.yml` для вступления новых значений параметров в силу потребуется перезапуск компонента jaDog, что может привести к failover. Таким образом, ручные операции с файлом конфигурации должны выполняться либо до сборки

кластера, либо при установленном режиме технического обслуживания (см. документ "Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»" п. 7.16.).

Пример настройки проверки сертификатов при подключении УЗ для взаимодействия с другими jaDog-сервисами (admin) и CN серверных сертификатов других узлов кластера (jadog-node2 и jadog-node3) в конфигурационном файле jadog\_hba.cfg.

### Пример конфигурации

#	USER	ADDRESS	METHOD
	admin	127.0.0.1/32	ssl
	admin	192.168.239.0/24	ssl
	jadog-node2	192.168.239.132/32	ssl
	jadog-node3	192.168.239.133/32	ssl

### 3.3. Настройте подключение jaDog к СУБД с помощью SSL-сертификатов

Для примера настройки см. документ "Руководство по безопасности. Часть 27." п. 7.2.

Для указания сертификатов, используемых jaDog для подключения к СУБД можно воспользоваться командами утилиты jadog\_ctl.

### Пример команд

```
set parameter db_connection_settings:db_auth_method = 'ssl'
set parameter db_connection_settings:ssl_mode = 'verify-full'
set parameter db_connection_settings:ssl_ca_file =
'/var/lib/jatoba/certs/root.crt'
set parameter db_connection_settings:ssl_crl_file =
'/var/lib/jatoba/certs/root.crl.pem'
set parameter db_connection_settings:ssl_cert_file =
'/var/lib/jatoba/certs/client.jadog_user.crt'
set parameter db_connection_settings:ssl_key_file =
'/var/lib/jatoba/certs/client.jadog_user.key'
```

Также можно скорректировать файл конфигурации jadog.yml вручную: изменить значение параметра db\_auth\_method, указанного в секции db\_connection\_settings.

### Пример конфигурации

```
db_connection_settings:  
db_auth_method: ssl
```

А также изменить пути до сертификатов, указанные в строке подключения в секции

```
param_connection: → sslmode, param_connection: → sslrootcert,  
param_connection: → sslcrl, param_connection: → sslcert и  
param_connection: → sslkey.
```



Обратите внимание на то, что после ручного изменения конфигурационного файла `jadog.yml` для вступления новых значений параметров в силу потребуется перезапуск компонента `jaDog`, что может привести к failover. Таким образом, ручные операции с файлом конфигурации должны выполняться либо до сборки кластера, либо при установленном режиме технического обслуживания (см. документ "Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»" п. 7.16.).

### 3.4. Настройте подключение к REST API с помощью SSL-сертификатов

Для примера настройки см. документ "Руководство по безопасности. Часть 27." п. 7.3.1.

Для указания сертификатов, используемых `jaDog` при подключении к REST API можно воспользоваться командами утилиты `jadog_ctl`.

### Пример команд

```
set parameter param_rest_api:rest_api_ca_file =  
'/var/lib/jatoba/certs/root.crt'  
  
set parameter param_rest_api:rest_api_cert_file =  
'/var/lib/jatoba/certs/server.crt'  
  
set parameter param_rest_api:rest_api_crl_file =  
'/var/lib/jatoba/certs/root.crl.pem'  
  
set parameter param_rest_api:rest_api_key_file =  
'/var/lib/jatoba/certs/server.key'
```



Также можно скорректировать файл конфигурации `jadog.yml` вручную - изменить значения параметров, указанных в секции `param_rest_api`.

### Пример конфигурации

```
param_rest_api:  
  rest_api_ca_file: /var/lib/jatoba/certs/root.crt  
  rest_api_cert_file: /var/lib/jatoba/certs/server.crt  
  rest_api_crl_file: /var/lib/jatoba/certs/root.crl.pem  
  rest_api_key_file: /var/lib/jatoba/certs/server.key
```



Обратите внимание на то, что после ручного изменения конфигурационного файла `jadog.yml` для вступления новых значений параметров в силу потребуются перезапуск компонента `jaDog`, что может привести к failover. Таким образом, ручные операции с файлом конфигурации должны выполняться либо до сборки кластера, либо при установленном режиме технического обслуживания (см. документ "Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»" п. 7.16.).

### 3.5. Настройте минимальную версию протокола TLS не ниже рекомендованной

Версии протокола TLS ниже чем TLSv1.2 имеют известные уязвимости, считаются устаревшими и не рекомендуются к использованию без крайней на то необходимости.

Для ограничения минимальной версии протокола TLS откройте конфигурационный файл `postgresql.conf` и измените значение параметра `ssl_min_protocol_version`.

### Пример конфигурации

```
ssl_min_protocol_version = 'TLSv1.2'
```

Значение параметра `ssl_min_protocol_version` также можно изменить при помощи команды `ALTER SYSTEM`.

### Пример запроса

```
ALTER SYSTEM SET ssl_min_protocol_version = 'TLSv1.2';
```

После изменения значения параметра необходимо перечитать конфигурацию инстанса СУБД.

### Пример функции

```
SELECT pg_reload_conf();
```

Также можно перечитать конфигурацию с использованием команды утилиты `jadog_ctl`.

### Пример команды

```
reload dbs on node 'node_name'
```

Есть возможность перечитать конфигурацию инстанса СУБД сразу на всех узлах кластера с использованием команды утилиты `jadog_ctl`.

### Пример команды

```
reload dbs on cluster
```

## 4. АУТЕНТИФИКАЦИЯ

### 4.1. Используйте надёжный метод аутентификации при подключении к узлам кластера

Рекомендованным методом аутентификации при подключении к СУБД на узлах кластера является аутентификация с проверкой SSL-сертификатов - cert (см. п. 3.1 данного документа). Тем не менее, в случае, если информационная система не поддерживает аутентификацию по сертификату, следует настроить надёжный метод аутентификации в конфигурационном файле `pg_hba.conf` узлов кластера.

Методы аутентификации `trust`, `password`, `ident`, `peer` и `md5` не являются надёжными и не рекомендуются к использованию в промышленной среде. Вместо них рекомендуется использовать один из следующих методов, поддерживаемых JaToba: `scram-sha-256`, `gss`, `sspi`, `ldap`, `radius`, `pam`.

В приведённом ниже примере конфигурации настроена возможность подключения технической УЗ (`jadog_user`) с применением метода аутентификации `scram-sha-256`.

#### Пример конфигурационного файла `pg_hba.conf`

#	TYPE	DATABASE	USER	ADDRESS	METHOD
host		[db_name]	jadog_user	127.0.0.1/32	scram-sha-256
host		[db_name]	jadog_user	192.168.239.131/32	scram-sha-256
host		replication	jadog_user	127.0.0.1/32	scram-sha-256
host		replication	jadog_user	192.168.239.131/32	scram-sha-256

### 4.2. Используйте надёжный метод аутентификации при подключении к компоненту jaDog

Рекомендованным методом аутентификации при подключении к компоненту jaDog является аутентификация с проверкой SSL-сертификатов - `ssl` (см. п. 3.2 данного документа). В случае, если информационная система не поддерживает аутентификацию по сертификату, следует настроить аутентификацию с помощью метода `scram-sha-256`.

В приведённом ниже примере конфигурации настроена аутентификация УЗ для взаимодействия с другими jaDog-сервисами (`admin`) и УЗ администратора (`administrator`) с применением метода `scram-sha-256`.

### Пример конфигурационного файла jadog\_hba.cfg

#	USER	ADDRESS	METHOD
	admin	127.0.0.1/32	sha-256
	admin	192.168.239.0/24	sha-256
	administrator	192.168.239.0/24	sha-256

#### 4.3. Измените пароли всех технических и административных УЗ при переводе системы в эксплуатацию

В случае использования парольной аутентификации вместо SSL в процессе настройки компонента jaDog и развёртывания кластера (вручную или с помощью jadog0) в интерфейсе jaDog и файлах ответов указываются пароли технических и административных учетных записей. Эти пароли могут быть скомпрометированы в процессе настройки, поэтому при переводе системы в промышленную эксплуатацию они должны быть изменены.

## 5. ЖУРНАЛИРОВАНИЕ

### 5.1. Настройте параметры журналирования компонента jaDog

Помимо журналирования событий инстанса СУБД также нужно настроить журналирование событий компонента jaDog.

Для установки параметров журналирования jaDog можно воспользоваться командами утилиты jadog\_ctl.

#### Пример команд

```
set parameter param_path:log_path = '/usr/jatoba-6/var/log/jadog'
set parameter param_log:logs_file = 'true'
set parameter param_log:logs_file_mode = '0600'
set parameter param_log:logs_filename = 'jadog-%a'
set parameter param_log:logs_type = 'csv, security.csv'
set parameter param_log:logs_level = 'info'
```

Также можно скорректировать файл конфигурации jadog.yml вручную - изменить значения параметров, указанных в секциях param\_path и param\_log.

#### Пример конфигурации

```
param_path:
  log_path: /usr/jatoba-6/var/log/jadog

param_log:
  logs_file: true
  logs_file_mode: 0600
  logs_filename: jadog-%a
  logs_level: info
  logs_type: csv, security.csv
```



Обратите внимание на то, что после ручного изменения конфигурационного файла `jadog.yml` для вступления новых значений параметров в силу потребуется перезапуск компонента `jaDog`, что может привести к `failover`. Таким образом, ручные операции с файлом конфигурации должны выполняться либо до сборки кластера, либо при установленном режиме технического обслуживания (см. документ «Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog» п. 7.16.).

## 5.2. Настройте журналирование компонентом jaDog событий информационной безопасности

Не менее важно настроить журналирование событий ИБ компонента `jaDog`.

Для установки параметров журналирования событий ИБ `jaDog` можно воспользоваться командами утилиты `jadog_ctl`:

### Пример команд

```
set parameter param_log:logs_type = 'csv, security.csv'
set parameter param_security_log:security_log_path =
'/usr/jatoba-6/var/log/jadog'
set parameter param_security_log:security_logs_filemode = '0600'
set parameter param_security_log:security_logs_filename =
'security_jadog-%a'
```



Обратите внимание на то, что тип журналирования событий ИБ указывается в значении параметра `logs_type` в секции `param_log` с помощью конструкции типа `'<...>, security.<формат_журналирования>'` (например, `security.csv`). Если его не указать - журнал событий ИБ не будет создан.

Также можно скорректировать файл конфигурации `jadog.yml` вручную - изменить значения параметров, указанных в секциях `param_log` и `param_security_log`:

### Пример конфигурации

```
param_log:
  logs_type: csv, security.csv
```

```
param_security_log:  
  security_log_path: /usr/jatoba-6/var/log/jadog  
  security_logs_filemode: 0600  
  security_logs_filename: security_jadog-%a
```



Обратите внимание на то, что после ручного изменения конфигурационного файла `jadog.yml` для вступления новых значений параметров в силу потребуется перезапуск компонента `jaDog`, что может привести к `failover`. Таким образом, ручные операции с файлом конфигурации должны выполняться либо до сборки кластера, либо при установленном режиме технического обслуживания (см. документ "Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»" п. 7.16.).

## 6. ХЕШИРОВАНИЕ И МАСКИРОВАНИЕ

### 6.1. Настройте стойкий алгоритм хеширования паролей в БД на узлах кластера

В случае использования парольной аутентификации пароль технической УЗ (jadog\_user) должен храниться в СУБД в захешированном стойким алгоритмом (с использованием случайной соли) виде. Тогда даже в случае получения злоумышленником хеша пароля использование им радужных таблиц для определения исходного пароля не принесёт результата.

СУБД «Jatoba» поддерживает два алгоритма хеширования: md5 (менее стойкий) и scram-sha-256 (более стойкий).

Для установки стойкого алгоритма хеширования паролей откройте конфигурационный файл postgresql.conf и измените значение параметра password\_encryption.

#### Пример конфигурации

```
password_encryption = scram-sha-256
```

Значение параметра password\_encryption также можно изменить при помощи команды ALTER SYSTEM.

#### Пример запроса

```
ALTER SYSTEM SET password_encryption = 'scram-sha-256';
```

После изменения значения параметра необходимо перечитать конфигурацию инстанса СУБД.

#### Пример функции

```
SELECT pg_reload_conf();
```

Также можно перечитать конфигурацию с использованием команды утилиты jadog\_ctl.

#### Пример команды

```
reload dbs on node 'node_name'
```

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------



Есть возможность перечитать конфигурацию инстанса СУБД сразу на всех узлах кластера с использованием команды утилиты `jadog_ctl`.

### Пример команды

```
reload dbs on cluster
```



Обратите внимание на то, что после изменения значения параметра и перечитывания конфигурации следует изменить пароль технической УЗ (`jadog_user`) для того, чтобы он перехешировался указанным алгоритмом.

## 7. КОНТРОЛЬ ЦЕЛОСТНОСТИ

### 7.1. Установите расширение `ja_csum` и зафиксируйте эталонные контрольные суммы

Для предотвращения несанкционированного изменения шаблонных баз данных, библиотек, бинарных файлов и файлов конфигурации рекомендуется зафиксировать их контрольные суммы и постоянно наблюдать за фактом их изменения. Для реализации этой функции требуется установить расширение `ja_csum`.

Для примера установки и применения расширения `ja_csum` см. документ «Руководство по настройке. Часть 14. Контроль целостности. Компонент `ja_CSum`».



В случае ручной фиксации эталонных контрольных сумм файлов компонента JaDog неизменными в процессе работы компонента файлами считаются:

- библиотеки;
- бинарные файлы;
- файл конфигурации `jadog.yml`;
- файл конфигурации `jadog_hba.cfg`;
- файл конфигурации `users.yml`.

Фиксация контрольных сумм других файлов расширения может привести к непредвиденным блокировкам УЗ в продуктовой среде!



Обратите внимание на то, что пакет компонента `ja_csum` должен быть установлен на всех хостах до конфигурирования кластера. В случае, если на одном узле кластера расширение будет установлено, а на другом - нет, на узле с отсутствующим пакетом расширения демон Jatoba в определённый момент зафиксирует ошибку и будет остановлен.



Обратите внимание на то, что для функционирования на всех узлах кластера файлы эталонных контрольных сумм должны быть скопированы на все узлы кластера.

## 8. РЕЗЕРВНОЕ КОПИРОВАНИЕ

### 8.1. Храните резервную копию файла ответов со структурой кластера в удалённом сетевом хранилище

Компонент «jaDog» имеет встроенную возможность выгрузки структуры кластера в файл, который впоследствии может быть использован как файл ответа для восстановления состояния кластера в случае вывода злоумышленником из строя одного или нескольких узлов кластера (см. документ "Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog»" п. 3.7.).

При планировании политики создания и хранения резервных копий рекомендуется использовать для сохранения резервных файлов ответов не локальную директорию сервера СУБД, а удалённое сетевое хранилище, физически расположенное в другом ЦОД. Тогда в случае вывода злоумышленником из строя сегмента серверной инфраструктуры файлы ответов останутся доступны для восстановления.



Обратите внимание на то, что для функционирования на всех узлах кластера директория, находящаяся на удалённом файловом сервере, должна быть примонтирована на всех узлах кластера.

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Аутентификационная информация** — информация, используемая при аутентификации субъекта доступа или объекта доступа.

Аутентификация – действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации (ГОСТ Р 58833-2020).

**Администратор СУБД** – субъект доступа, выполняющий административные функции в СУБД и наделенный правами:

- создавать учетные записи пользователей системы управления базами данных;
- модифицировать, блокировать и удалять учетные записи пользователей системы управления базами данных;
- назначать права доступа пользователям системы управления базами данных к объектам доступа системы управления базами данных;
- управлять конфигурацией системы управления базами данных;
- создавать, подключать базы данных.

Администратор СУБД имеет атрибут SUPERUSER и/или обладает системной учетной записью «postgres».

**Администратор БД** – субъект доступа, выполняющий административные функции в БД и наделенный правами:

- создавать учетные записи пользователей базы данных;
- модифицировать, блокировать и удалять учетные записи пользователей базы данных;
- управлять конфигурацией базы данных;
- назначать права доступа пользователям базы данных (пользователей информационной системы) к объектам доступа базы данных;

- создавать резервные копии базы данных и восстанавливать базу данных из резервной копии;
- создавать, модифицировать и удалять процедуры (программный код), хранимые в базе данных.

Администратор БД имеет атрибут CREATEROLE, и возможные атрибуты BYPASSRLS, REPLICATION, а также прочие системные привилегии относительно БД, кроме атрибута CREATEDB.

**Безусловная блокировка пользователя** – это ограничение пользователя в возможности устанавливать новую сессию с СУБД. Безусловная блокировка имеет приоритет над ограничениями, накладываемыми парольными политикам (блокировка вследствие истечения срока действия пароля, временные блокировки при исчерпании попыток ввода пароля и т.п.), применяется независимо от них и не зависит от применяемого метода аутентификации пользователей. Снятие безусловной блокировки не снимает блокировок по парольным политикам и наоборот.

**Завершение сессии пользователя** – принудительное завершение открытой сессии пользователя с БД/СУБД в заданном режиме.

**Пользователь БД** - субъект доступа, имеющий доступ к ограниченному перечню БД и объектов БД. Имеющий следующий набор привилегий:

- создавать и манипулировать объектами доступа БД (таблица, запись или столбец, поле, представление и иные объекты доступа);
- выполнять процедуры (программный код), хранимые в БД.

Пользователь БД имеет обязательный атрибут LOGIN.

**Пользователь СУБД** – см. «Пользователь БД». Для СУБД эти понятия идентичны. СУБД не разграничивает пользователей по отдельным БД. Все пользователи общие, доступ к отдельным БД определяется настройками доступа.

**Роль** – субъект доступа в БД/СУБД, наделенный определенным набором привилегий (чаще всего употребляется как обобщение группы пользователей для выполнения определенного набора действий в БД/СУБД).

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

SQL	–	Structured Query Language
БД	–	База данных
КС	–	Контрольные суммы
КЦ	–	Контроль целостности
ОС	–	Операционная система
СУБД	–	Система управления базами данных
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России

[illegible]

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------