

# Интеграция серверов PostgreSQL в корпоративную сеть

ООО «ИТСК»

Технологический центр 1С

Пучков В.В.

26,01,2018



# ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР 1С В ИТСК



# Требования к технологическим решениям

---

- **Безопасность**
- **Соответствие корпоративным стандартам**
- **Надёжность**

## Корпоративные системы, которые мы используем с PostgreSQL

---



# Почему Kerberos

---

- Единая точка входа (single sign in)
- Пароль не передаётся по сети
- Аутентифицируются и клиент и сервер
- Просто красивое инженерное решение



# Процесс аутентификации Kerberos

---



Клиент

KDC



TGS 

KDC – Key Distribution Center  
TGS – Ticket Granting Service  
TGT – Ticket Granting Ticket



Сервер СУБД 

# Процесс аутентификации Kerberos

---



Клиент 

KDC



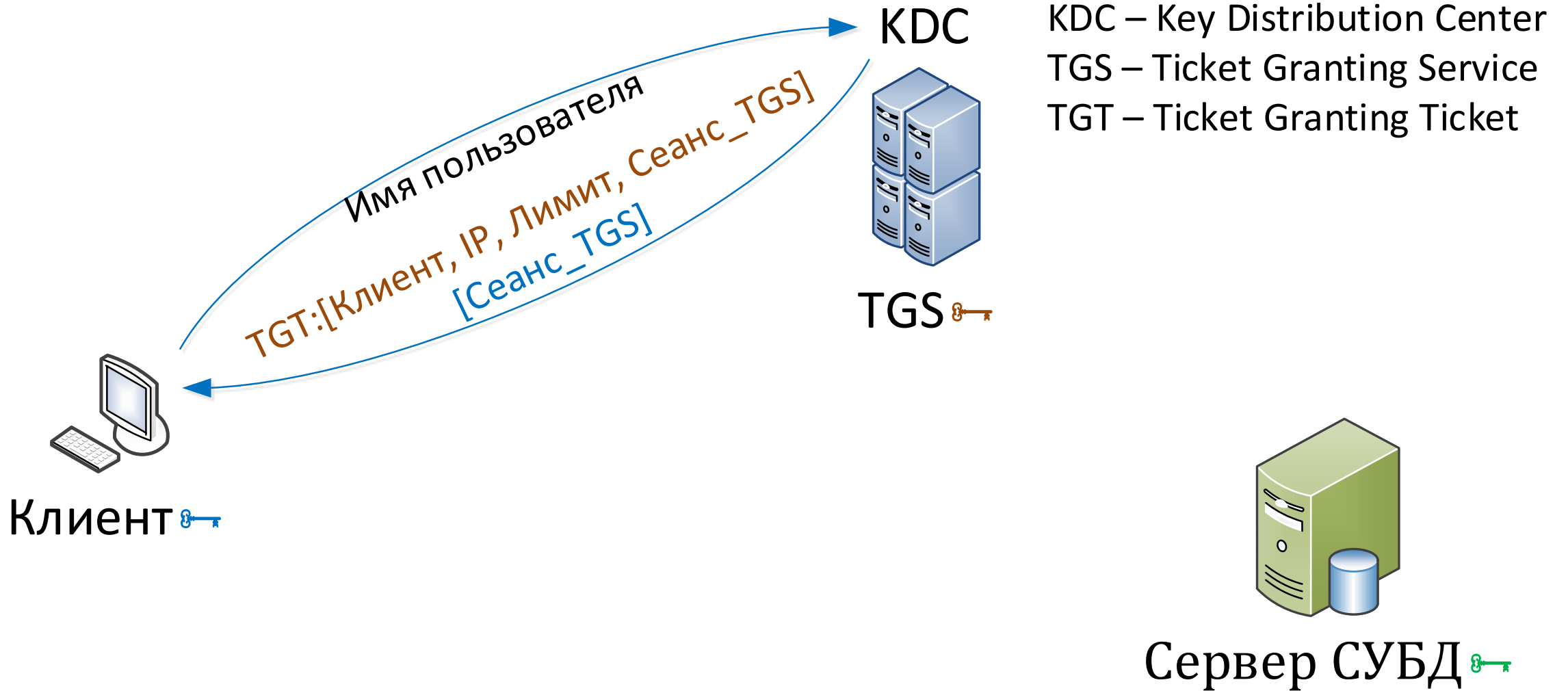
TGS 

KDC – Key Distribution Center  
TGS – Ticket Granting Service  
TGT – Ticket Granting Ticket



Сервер СУБД 

# Процесс аутентификации Kerberos





# Процесс аутентификации Kerberos

KDC



TGS 

KDC – Key Distribution Center  
TGS – Ticket Granting Service  
TGT – Ticket Granting Ticket  
SPN – Service Principal Name



Клиент 

TGT:[Клиент, IP, Лимит, Сеанс\_TGS]

Сеанс\_TGS 

Запрос подключения

KDC, SPN



Сервер СУБД 

# Процесс аутентификации Kerberos

KDC



KDC – Key Distribution Center  
TGS – Ticket Granting Service  
TGT – Ticket Granting Ticket  
SPN – Service Principal Name

TGS



Сервер СУБД



Клиент

TGT:[Клиент, IP, Лимит, Сеанс\_TGS]

Сеанс\_TGS

SPN

SPN, TGT  
Auth: [Клиент, Время]

Ticket:SPN,[Клиент, IP, Лимит,  
Сеанс\_Сервиса]  
[Сеанс\_Сервиса]

# Процесс аутентификации Kerberos



Клиент 

TGT:[Клиент, IP, Лимит, Сеанс\_TGS]

Ticket:SPN,[Клиент, IP, Лимит, Сеанс\_Сервиса]

Сеанс\_TGS , Сеанс\_Сервиса 

KDC



TGS 

KDC – Key Distribution Center

TGS – Ticket Granting Service

TGT – Ticket Granting Ticket

SPN – Service Principal Name



Сервер СУБД 

# Процесс аутентификации Kerberos

KDC





TGS 

KDC – Key Distribution Center  
TGS – Ticket Granting Service  
TGT – Ticket Granting Ticket  
SPN – Service Principal Name



Клиент 

TGT:[Клиент, IP, Лимит, Сеанс\_TGS]  
Ticket:SPN,[Клиент, IP, Лимит, Сеанс\_Сервиса]  
Сеанс\_TGS , Сеанс\_Сервиса 

Ticket  
Auth: [Клиент, Время]



Сервер СУБД 

# Процесс аутентификации Kerberos

KDC



TGS 

KDC – Key Distribution Center  
TGS – Ticket Granting Service  
TGT – Ticket Granting Ticket  
SPN – Service Principal Name



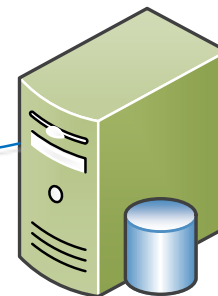
Клиент 

TGT:[Клиент, IP, Лимит, Сеанс\_TGS]

Ticket:SPN,[Клиент, IP, Лимит, Сеанс\_Сервиса]

Сеанс\_TGS , Сеанс\_Сервиса 

[Время]



Сервер СУБД 

Сеанс\_Сервиса 

# Настройка Kerberos для сервера PostgreSQL под Windows

---

1. **Установить PostgreSQL, посмотреть имя сервиса (зависит от инсталлятора)**
2. **Настроить запуск PostgreSQL под доменной УЗ (не забыть про права на каталоги, включая stats\_temp\_directory)**

## 3. Зарегистрировать SPN:

```
Setspn -A pgsql-9.6.7-1.1C-x64/<имя компьютера с доменом> <УЗ без домена>
```

## 4. pg\_hba.conf:

```
host      all      all      <подсеть>      sspi      include_realm=1 map=m1
```

## 5. pg\_ident.conf:

```
m1          /^ (.* ) @GAZPROM-NEFT\ .LOCAL$      \1
```

```
m1          /^ (.* ) @GAZPROM-NEFT$      \1
```

## 6. psql:

```
Create role "<UserName>" with login;
```

# Настройка Kerberos для сервера PostgreSQL под Linux

---

## Настройка Kerberos для сервера PostgreSQL под Linux

---





# Настройка Kerberos для сервера PostgreSQL под Linux

---

1. Собрать PostgreSQL из исходников, выполнив **`./configure --with-krb-srvnam=POSTGRES`**

2. Создать keytab:

```
ktpass -princ POSTGRES/<сервер>.gazprom-neft.local@GAZPROM-NEFT.LOCAL -  
mapuser <УЗ> -pass "<пароль>" -crypto All -ptype KRB5_NT_PRINCIPAL -out  
<файл.keytab>
```

Скопировать keytab на сервер PostgreSQL, установить права:

```
chmod 0400 <файл>.keytab
```

```
chown postgres:postgres <файл>.keytab
```

# Настройка Kerberos для сервера PostgreSQL под Linux

---

## 3. `/etc/krb5.conf`

```
...  
[libdefaults]  
dns_lookup_realm = false  
dns_lookup_kdc = true  
default_realm = GAZPROM-NEFT.LOCAL  
[realms]  
GAZPROM-NEFT.LOCAL = {  
    kdc = <контроллер домена>  
    admin_server = <контроллер домена>  
}  
[domain_realm]  
.gazprom-neft.local = GAZPROM-NEFT.LOCAL  
gazprom-neft.local = GAZPROM-NEFT.LOCAL
```

# Настройка Kerberos для сервера PostgreSQL под Linux

---

## 4. postgresql.conf:

```
krb_server_keyfile = '/etc/sysconfig/postgresql/<файл>.keytab'
```

## 5. pg\_hba.conf:

```
host      all      all <подсеть>          gss          include_realm=1  krb_realm=GAZPROM-  
NEFT.LOCAL      map=m1
```

## 6. pg\_ident.conf:

```
m1          /^ (.* ) @GAZPROM-NEFT\ .LOCAL$      \1  
m1          /^ (.* ) @GAZPROM-NEFT$              \1
```

## 7. psql:

```
Create role "<UserName>" with login;
```

## PostgreSQL + Kerberos

---



# PostgreSQL + Kerberos

---



# PostgreSQL + Kerberos + 1C?

---





## PostgreSQL + Kerberos + 1C?

---



## PostgreSQL + Kerberos + 1C?

---

**1С в данный момент не поддерживает доменную аутентификацию с PostgreSQL, даже в среде Windows.**



# Безопасность 1С + PostgreSQL

---

1. Разделение тестовых и продуктивных серверов
2. Ограничивать разрешённые хосты в `pg_hba.conf`
3. Разные владельцы для разных баз
4. Отбирать `superuser` после создания баз, владельца БД и всех объектов в ней(!) достаточно, но...

```
2019-01-27 19:20:17.007 MSK; ERROR:  permission denied to set parameter "lc_messages"
```

```
2019-01-27 19:20:17.007 MSK; STATEMENT:  SET lc_messages to 'en_US.UTF-8';
```

Проблема донесена до 1С, надеемся, что будет решена в ближайшее время

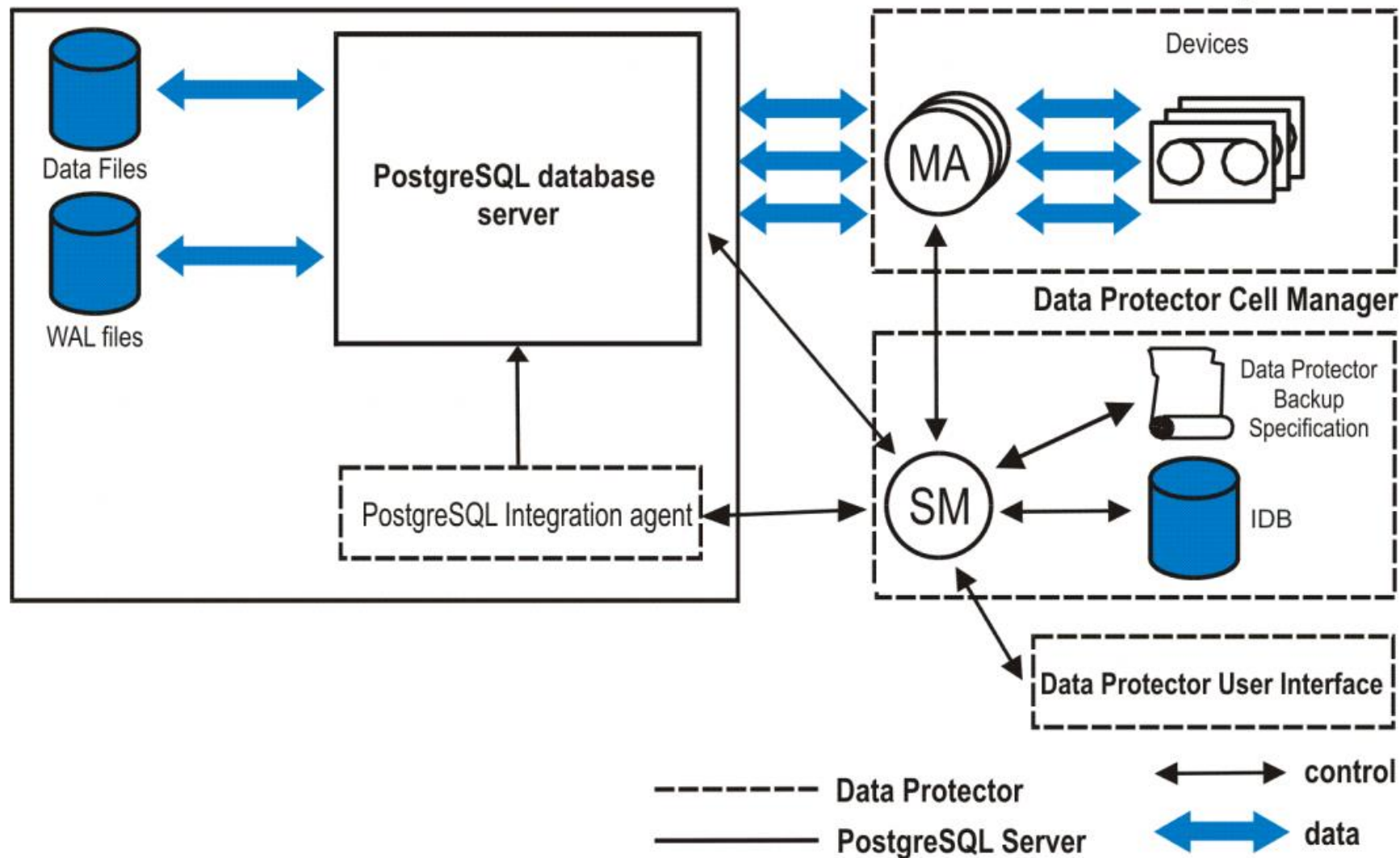
## Резервное копирование

---

- Бывший HP DataProtector, бывший OmniBackup
- Поддержка дисковых и ленточных архивов
- Единый центр управления и мониторинга
- Интегрируется с PostgreSQL :
- Начиная с версии 2018.11 (10.20) поддерживает PostgreSQL 10 и новее
- Умеет делать полные РК и РК WAL-файлов
- Позволяет выполнять Point-in-Time Recovery
- Позволяет выполнять миграцию кластера в другой каталог и/или на другой сервер

# Схема работы DataProtector + PostgreSQL

## PostgreSQL host



1. На стороне Cell Manager для каждого сервера заполняется файл экземпляров `<имя_сервера>%INSTANCE_LIST:`

```
INSTANCE_LIST=('postgresql-x64-10');
```

2. Для каждого экземпляра надо создать файл вида `<имя_сервера>%<имя_экземпляра>:`

## Windows

```
username='postgres';
password='';
port=5432;
archive_dir='E:\pgbackup\archive\';
binary_dir='C:\Program
Files\PostgreSQL\10\bin';
slave_host='';
slave_archive_dir='';
slave_data_dir='';
OSUSER='MSK01-DPSVC';
OSGROUP='GAZPROM-NEFT';
```

## Linux

```
username='postgres';
password='';
port=5432;
archive_dir='/pgbackup/9.6/archive/';
binary_dir='/usr/pgsql-9.6/bin/';
slave_host='';
slave_archive_dir='';
slave_data_dir='';
OSUSER='root';
OSGROUP='wheel';
```

## Последовательность действий при копировании

---

1. Выполняет `pg_start_backup()`
2. Копирует файлы кластера
3. Выполняет `pg_stop_backup()`
4. Перенаправляет архивацию WAL:

```
parameter "archive_command" changed to '"C:/Program Files/OmniBack/bin/pgsqlbar.exe" -stage %p -backup'
```

4. Копирует файлы из текущего архивного каталога
5. Возвращает архивацию WAL:

```
parameter "archive_command" changed to "archlog.bat %p %f"
```

## Последовательность действий при восстановлении

---

1. Копирует файлы кластера
2. Настраивает `recovery.conf`:

```
restore_command='"C:/Program Files/OmniBack/bin/pgsqlbar.exe" -stage %p -restore  
pg_xlog/%f'recovery_target_time='2018-08-22 09:58:49'recovery_target_action='promote'
```

4. Запускает кластер

## Что делать, если система РК не интегрируется с PostgreSQL?

---

1. **Настраиваем резервное копирование через pg\_basebackup**
2. **Настраиваем archive\_command**
3. **Настраиваем СРК на копирование каталога, в который осуществляется резервное копирование средствами PostgreSQL**

## Единая система мониторинга серверного ландшафта ГПН

### Плюсы

- Круглосуточная служба поддержки
- Отработанная система эскалации
- Настраиваемые уровни предупреждений
- Хорошо подходит для предотвращения критических проблем
- Хранит архивы метрик, позволяет производить анализ постфактум

### Минусы

- Тяжеловесная
- Ограничения в настройке визуализации
- Database Performance Analyzer до сих пор не поддерживает PostgreSQL



## Примеры запросов для мониторинга

- **Зависшие сессии**

```
select
    count(datname),
    datname
from
    pg_stat_activity
where
    state like 'idle in%' and
    ( current_timestamp - state_change ) > interval '1 minute' and
    datid not in ( select oid from pg_database where datistemplate )
group by datname
```

- **Архивирование WAL**

```
select
    case when ( last_failed_time > last_archived_time ) then failed_count else 0 end as failed_count,
    cast( last_archived_time as varchar ) ||
        case
            when ( last_failed_time > last_archived_time ) then
                '<br>' || cast( last_failed_time as varchar )
            else '' end
from
    pg_stat_archiver
```

Application Details

Application Name: pg\_stat\_activity on [redacted]

Application Status: Application status is Up

Server Status: Server status is Up

| Component Name      | Component Type               | Component Status |
|---------------------|------------------------------|------------------|
| Зависшие транзакции | ODBC User Experience Monitor | Up               |
| Архивация WAL       | ODBC User Experience Monitor | Up               |
| Ожидания            | ODBC User Experience Monitor | Up               |

Summary

Node Status: Node is Up. Application 'PostgreSQL (lgs\_msk\_eson\_rw)' has state: Warning.

Polling IP Address: [redacted]

Dynamic IP: No

Machine Type: Windows 2012 R2 Server

Node Category: Server

DNS: [redacted]

System Name: [redacted]

Description: Hardware: Intel® Family 6 Model 37 Stepping 1 AT&T COMPATIBLE • Software: Windows Version 6.3 (Build 9600 Multiprocessor Free)

Location:

Contact:

SysObjectID: [redacted]

Last Boot: Friday, January 18, 2019 6:18 AM

Software Version: 6.3 (Build 9600 Multiprocessor Free)

Software Image: Unknown

Hardware: Virtual, host unknown

No of CPUs: 16

Telnet: [redacted]

Web Browse: [redacted]

Application Custom Properties

|                                       |  |
|---------------------------------------|--|
| Alert                                 | False  |
| MailTo1                               | mon-infrastructure@gazprom-neft.ru; rsd-1-o-bas-is-alerts@gazprom-neft.ru; |
| Контактное лицо_РГ                    | 1С-ИТОК-Базис  |
| Эскалация_доступность                 | Оповестить по телефону   |
| Эскалация_опрос                       | Наряд  |
| Эскалация_приложение_к_ритичности     | Оповестить по телефону   |
| Эскалация_приложение_п_предупреждение | Для информации   |

Components

| Component Name      | Statistic | Message   | Response Time | Port |
|---------------------|-----------|-----------|---------------|------|
| Архивация WAL       | 0         | 45,790994 | 189 ms        | N/A  |
| Зависшие транзакции | 0         |           | 175 ms        | N/A  |
| Ожидания            | 0         |           | 304 ms        | N/A  |

CPU Load & Memory Statistics

|                          |                |
|--------------------------|----------------|
| Current Average CPU Load | 8 %            |
| Memory Used              | 15.413 GB 22 % |
| Memory Available         | 53.306 GB 78 % |
| Total Memory             | 68.719 GB      |

AppStack Environment for pg\_stat\_activity

Applications (1)

Servers (1)

Virtual Clusters (1)

Virtual Datacenters (1)

Virtual Centers (1)

Data Stores (1)

Volumes (3)

LUNS (1)

Pools (1)

Storage Arrays (1)

Last 5 Notes (0)

Application Availability

pg\_stat\_activity

Jan 21 2019, 12:00 am - Jan 28 2019, 6:00 am

Last 25 Application Events

|                    |  |
|--------------------|--|
| 1/27/2019 3:06 AM  | Application "pg_stat_activity" on node [redacted] is up  |
| 1/27/2019 3:01 AM  | Application "pg_stat_activity" on node [redacted] is down  |
| 1/24/2019 1:12 PM  | Application "pg_stat_activity" on node [redacted] is up  |
| 1/24/2019 1:11 PM  | Application "pg_stat_activity" on node [redacted] is managed again. Polling and statistics collection have been resumed. |
| 1/24/2019 11:40 AM | Application "pg_stat_activity" on node [redacted] has been unmanaged. Polling and statistics collection are suspended.   |
| 1/24/2019 1:12 AM  | Application "pg_stat_activity" on node [redacted] is down  |
| 1/24/2019 1:08 AM  | Application "pg_stat_activity" created on node [redacted]  |

Availability Statistics

| Period       | Availability |
|--------------|--------------|
| Today        | 100.000 %    |
| Yesterday    | 99.653 %     |
| Last 7 Days  | 89.271 %     |
| Last 30 Days | 89.271 %     |
| This Month   | 89.271 %     |
| This Year    | 89.271 %     |

Active Application Alerts (0)

| Alert Name | Message | Triggering Object | Active Time | Related Node |
|------------|---------|-------------------|-------------|--------------|
|------------|---------|-------------------|-------------|--------------|

Газпром нефть | 34

## Components

[HELP](#)

| COMPONENT NAME  | STATISTIC | MESSAGE                 | RESPONSE TIME  | PORT |
|---|-----------|-------------------------|--|------|
|   Current Number of Locks on Server                     | 36        |                         | 68 ms     | N/A  |
|   Database Cache Hit Ratio (%)                          | 95.18     |                         | 63 ms     | N/A  |
|   Database Size (MB)                                    | 19.882 K  |                         | 742 ms    | N/A  |
|   Database Success Rate (%)                             | 100       |                         | 53 ms     | N/A  |
|   Size of the Largest Table (MB)                        | 7023      | pg_toast_1954679        | 33 ms     | N/A  |
|   Table with the biggest number of Index Scans          | 17.786 K  | _reference6938 / public | 52 ms     | N/A  |
|   Table with the biggest number of Row Reads            | 71.546 G  | _inforg7952             | 54 ms     | N/A  |
|   Table with the biggest number of Sequential Scans | 139.089 M | _reference6938 / public | 105 ms  | N/A  |
|   Total Active Server Connections                   | 17        |                         | 24 ms   | N/A  |
|   Total Indexes in Current Database                 | 4428      |                         | 40 ms   | N/A  |
|   Total Number of Tables in Current Database        | 5759      |                         | 40 ms   | N/A  |

## И ЧТО В РЕЗУЛЬТАТЕ?

- Системы корпоративного уровня зачастую относятся к PostgreSQL несколько свысока
- Это отношение достаточно быстро меняется в лучшую сторону
- Мы все можем этому поспособствовать