

数据库安全

digoal.zhou

自我介绍

•



一枚PGer

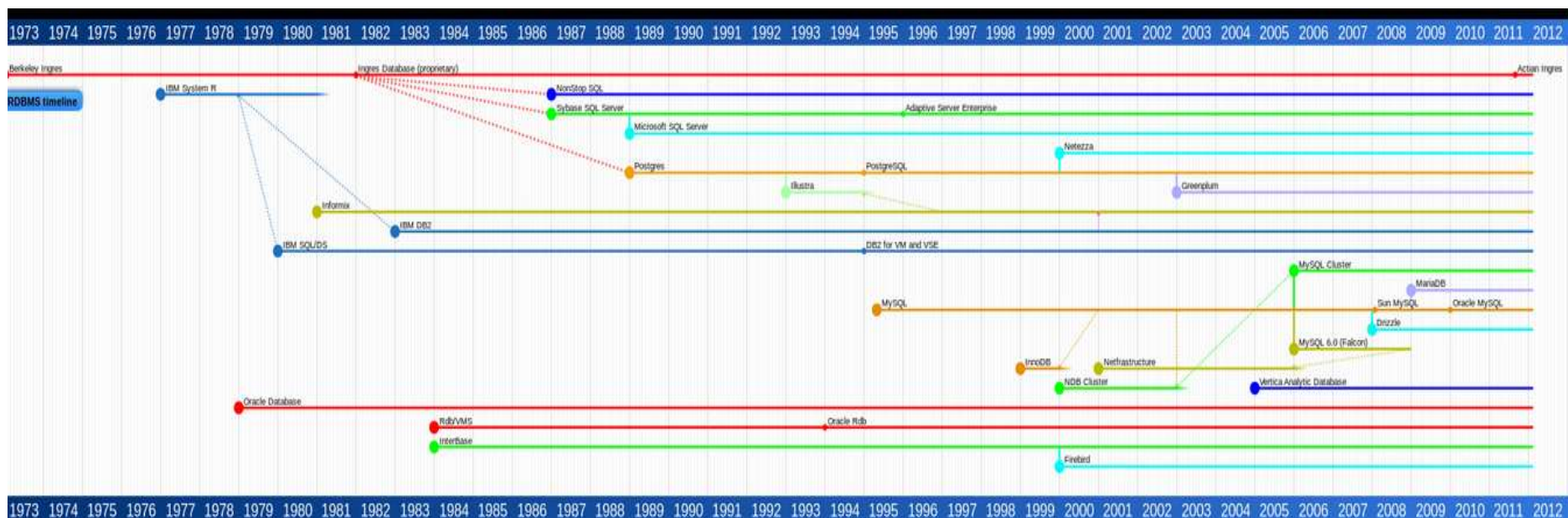
- PostgreSQL 中国社区发起人之一，社区CTO。
- PostgreSQL 中国社区杭州分会会长。
- PostgreSQL 中国社区大学发起人之一。
- DBA+社群联合发起人之一。
- 曾就职于斯凯网络，负责数据库部门，在上市前使用PostgreSQL完成去IOE任务，同时通过SOX审计，成功在纳斯达克上市。
- 现就职于阿里巴巴，负责RDS PG内核组事务。

PostgreSQL发展历程



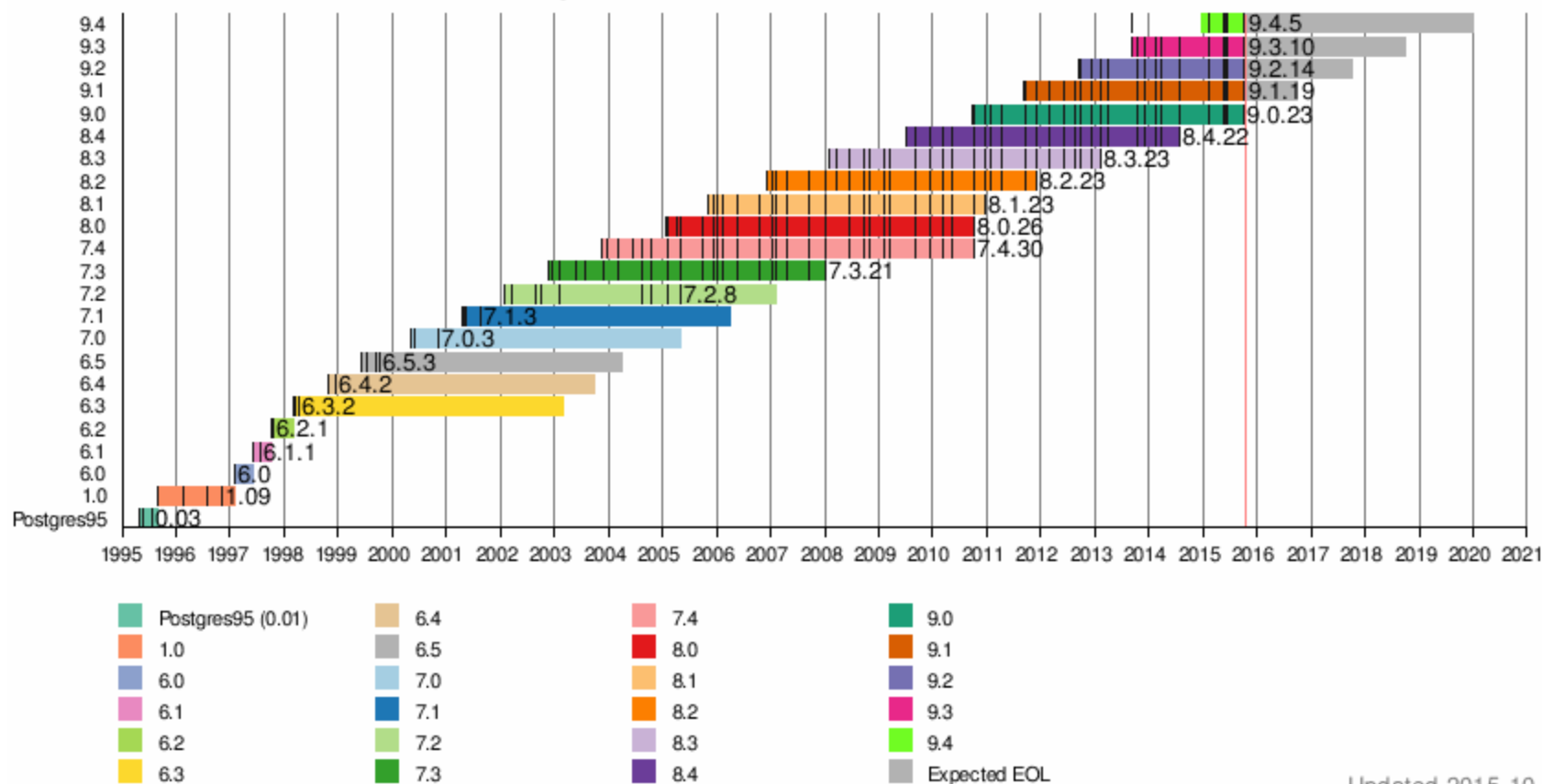
- 1973 *University INGRES* (起源于IBM System R的一系列文档, [Michael Stonebraker](#) and [Eugene Wong](#))
- 1982 INGRES
- 1985 post-Ingres
- 1988 POSTGRES version 1 - 1993 version 4 (END)
- 1995 Postgres95 (伯克利大学学生Andrew Yu, Jolly Chen重写SQL解释器, 替换原项目中的基于Ingres的SQL解释器.为开源奠定了基础)
- 1996 更为PostgreSQL, 发布第一个开源版本, 后交由PostgreSQL社区维护.

主要RDBMS发展历程



PostgreSQL 版本发布历程

PostgreSQL release timeline



Updated 2015-10-22

PostgreSQL 代码活跃度

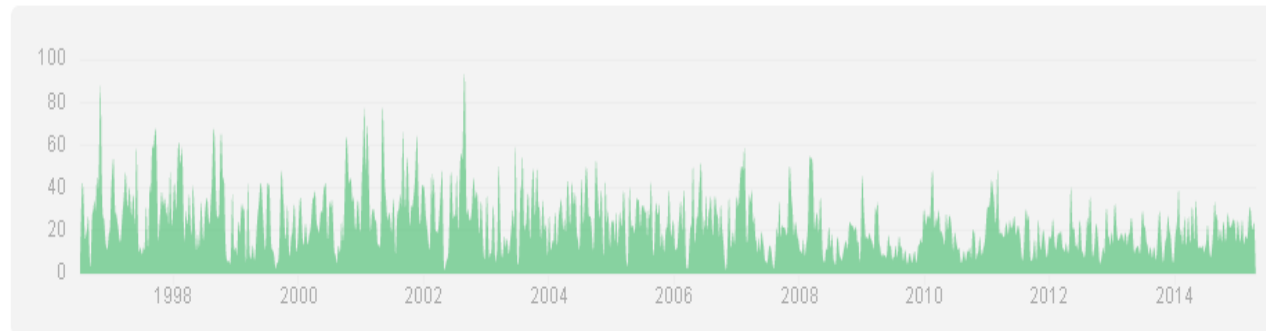
数据取自

<https://github.com/postgres/postgres/graphs>

Jul 7, 1996 – Apr 22, 2015

Contributions to master, excluding merge commits

Contributions: **Commits** ▾



Contributors

Commits

Code frequency

Punch card

Network

Members

Use and to navigate



PostgreSQL 代码托管

数据取自PostgreSQL主代码管理库

<http://git.postgresql.org/gitweb/?p=postgresql.git;a=heads>

[projects](#) / [postgresql.git](#) / [summary](#)

[summary](#) | [shortlog](#) | [log](#) | [commit](#) | [commitdiff](#) | [tree](#)

description This is the main PostgreSQL git repository.

owner Magnus Hagander

last change Tue, 21 Apr 2015 23:03:49 +0000

URL [git://git.postgresql.org/git/postgresql.git](http://git.postgresql.org/git/postgresql.git)

<http://git.postgresql.org/git/postgresql.git>

<ssh://git@git.postgresql.org/postgresql.git>

shortlog

4 hours ago	Peter Eisentraut	Move pg_xlogdump from contrib/ to src/bin/ mas
5 hours ago	Robert Haas	Update FDW docs to reflect existence of CHECK
16 hours ago	Heikki Linnakangas	Add missing installcheck target to pg_rewind's
17 hours ago	Andres Freund	Add 'active_in' column to pg_replication_slots
25 hours ago	Peter Eisentraut	Move pg_test_timing from contrib/ to src/bin/
30 hours ago	Bruce Momjian	Honor OID status of CREATE LIKE'd tables
2 days ago	Peter Eisentraut	Move pg_test_fsync from contrib/ to src/bin/
4 days ago	Bruce Momjian	pg_upgrade: binary_upgrade_create_empty_extens
4 days ago	Stephen Frost	Fix typo in relcache's equalPolicy()

postgresql.git

4 hours ago	master	shortlog	log	tree
5 days ago	REL9_4_STABLE	shortlog	log	tree
7 days ago	REL9_0_STABLE	shortlog	log	tree
7 days ago	REL9_1_STABLE	shortlog	log	tree
7 days ago	REL9_2_STABLE	shortlog	log	tree
7 days ago	REL9_3_STABLE	shortlog	log	tree
3 months ago	REL8_2_STABLE	shortlog	log	tree
3 months ago	REL8_3_STABLE	shortlog	log	tree
9 months ago	REL8_4_STABLE	shortlog	log	tree
4 years ago	REL8_1_STABLE	shortlog	log	tree
4 years ago	REL7_4_STABLE	shortlog	log	tree
4 years ago	REL8_0_STABLE	shortlog	log	tree
5 years ago	REL9_0_ALPHA5_BRANCH	shortlog	log	tree
5 years ago	REL9_0_ALPHA4_BRANCH	shortlog	log	tree
5 years ago	REL7_3_STABLE	shortlog	log	tree
5 years ago	REL8_5_ALPHA3_BRANCH	shortlog	log	tree
5 years ago	REL8_5_ALPHA2_BRANCH	shortlog	log	tree
5 years ago	REL8_5_ALPHA1_BRANCH	shortlog	log	tree
9 years ago	REL7_2_STABLE	shortlog	log	tree
10 years ago	REL7_1_STABLE	shortlog	log	tree
11 years ago	WIN32_DEV	shortlog	log	tree
12 years ago	ecpg_big_bison	shortlog	log	tree
14 years ago	REL7_0_PATCHES	shortlog	log	tree
15 years ago	REL6_5_PATCHES	shortlog	log	tree
16 years ago	REL6_4	shortlog	log	tree
18 years ago	REL2_0B	shortlog	log	tree
18 years ago	Release_1_0_3	shortlog	log	tree

This is the main PostgreSQL git repository.



PostgreSQL 全球贡献者

- Core Team成员
- Josh Berkus (USA, CEO@PostgreSQL Experts Inc.)
 - 主要负责PG推广, 性能测试, 优化, 文档编辑等工作.
- Peter Eisentraut (USA, MeetMe.com)
 - 主要负责了系统建设, 移植, 文档编辑, 国际化, 以及其他增强性的代码工作.
- Magnus Hagander (Sweden, redpill-linpro.se)
 - 帮助维护PostgreSQL WEB主站及基础设施, win32的移植, 以及系统认证等工作.
- Tom Lane (USA, Salesforce)
 - 遍及PostgreSQL代码的各个角落, 包括BUG评估和修复, 性能改进, 优化等.
- Bruce Momjian (USA, EnterpriseDB)
 - 负责维护TODO和FAQ列表, 代码, 发布版本补丁以及培训.
- Dave Page (United Kingdom, EnterpriseDB)
 - 负责pgadmin的开发和维护工作, 同时负责管理postgresql.org主站工程, PostgreSQL的安装程序等.
- 主要贡献者
 - <http://www.postgresql.org/community/contributors/>
- Committers (git@gitmaster.postgresql.org/postgresql.git)
 - 目前有21位committer. (<http://wiki.postgresql.org/wiki/Committers>)



PostgreSQL 全球赞助商

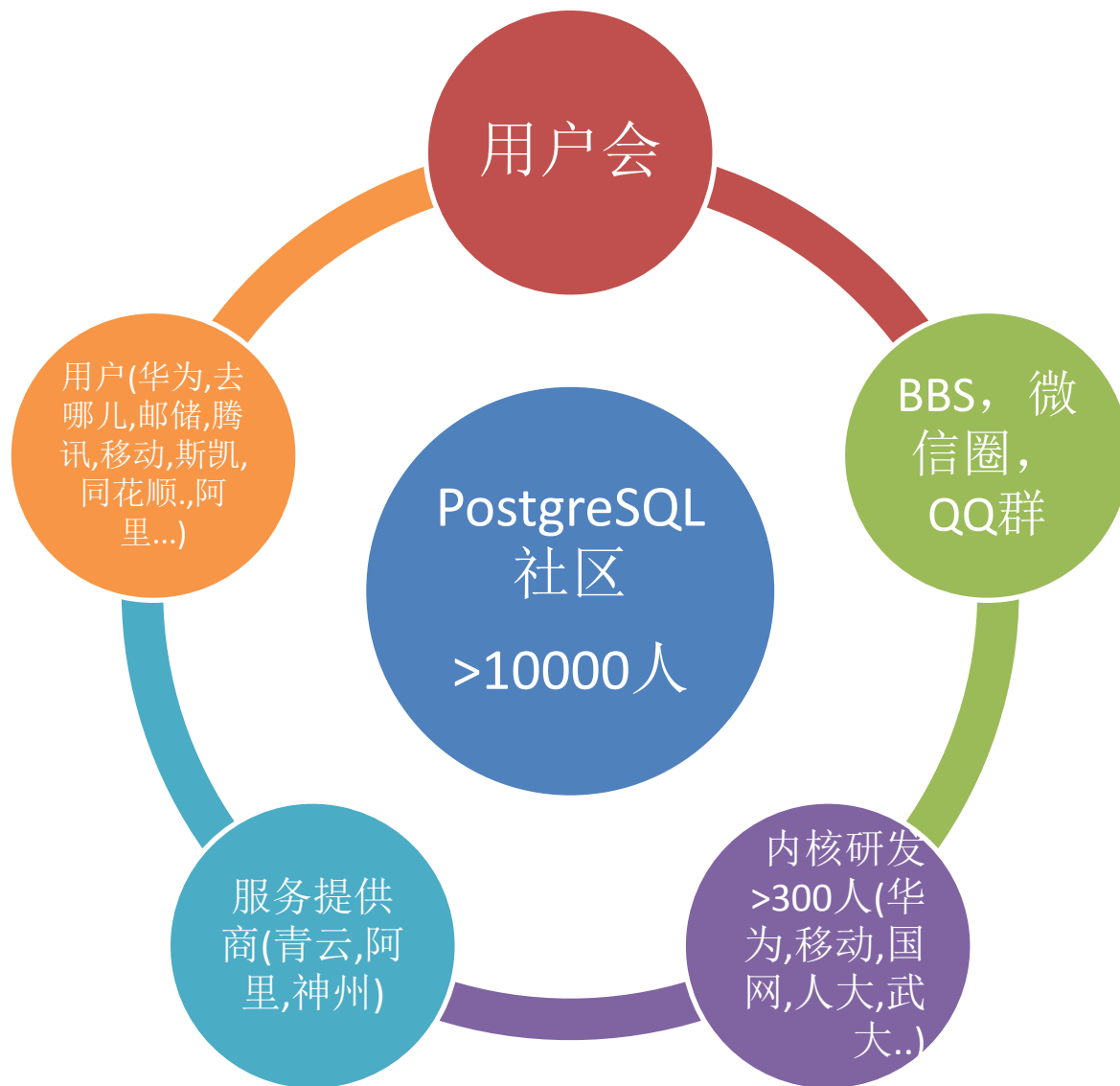
- PostgreSQL全球赞助商 (最新 <http://www.postgresql.org/about/sponsors/>)

Platinum	Entities who have provided at least 3 full years of significant and recurring contribution to PostgreSQL.
Gold	Entities who have provided at least 2 full years of significant and recurring contribution to PostgreSQL.
Silver	Entities who have provided at least 1 full year of significant and recurring contribution to PostgreSQL.
Bronze	Entities who have provided a significant contribution in the last 12 months to PostgreSQL.

- 赞助商列表

Platinum	Gold	Silver	Bronze			
 Dalibo	 creativ GmbH	 Meetme.com	 Google	 Huawei		China
 2ndQuadrant	 PostgreSQL Experts, Inc.	 OmniTI	 hub.org	 Skype		Luxembourg
 Red Hat, Inc.	 conova communications	 CyberTec	 HP	 Rackspace		United States
 EnterpriseDB	 Redpill Linpro	 SRA OSS	 Salesforce	 City of Garden Grove, California		United States
 Command Pro	 NTT Group	 VMware	 Wisconsin Courts	 Aster Data		United States
 aliyun.com		 NEC	 Heroku	 http://networks		France

PostgreSQL中国



PostgreSQL中国

- 关注度趋势



PostgreSQL中国

• 需求分布



PostgreSQL数据库全球使用情况

- 生物制药 {Affymetrix(基因芯片), 美国化学协会, gene(结构生物学应用案例), ...}
- 电子商务 { CD BABY, etsy(与淘宝类似), whitepages, flightstats, Endpoint Corporation ...}
- 学校 {加州大学伯克利分校, 哈佛大学互联网与社会中心, .LRN, 莫斯科国立大学, 悉尼大学, ...}
- 金融 {Journyx, LLC, trusecommerce(类似支付宝), 日本证券交易交所, 邮储银行, 同花顺...}
- 游戏 {MobyGames, ...}
- 政府 {美国国家气象局, 印度国家物理实验室, 联合国儿童基金, 美国疾病控制和预防中心, 美国国务院, 俄罗斯杜马...}
- 医疗 {calorieking, 开源电子病历项目, shannon医学中心, ...}
- 制造业 {Exoteric Networks, 丰田, 捷豹路虎}
- 媒体 {IMDB.com, 美国华盛顿邮报国会投票数据库, MacWorld, 绿色和平组织, ...}
- 开源项目 {Bricolage, Debian, FreshPorts, FLPR, PostGIS, SourceForge, OpenACS, Gforge, ...}
- 零售 {ADP, CTC, Safeway, Tsutaya, Rockport, ...}
- 科技 {Sony, MySpace, Yahoo, Afiliast, APPLE, 富士通, Omnitel, Red Hat, Sirius IT, SUN, 国际空间站, Instagram, Disqus, 去哪儿, 腾讯, 华为, 中兴, 斯凯, 云游, 阿里 ...}
- 通信 {Cisco, Juniper, NTT(日本电信), 德国电信, Optus, Skype, Tlestra(澳洲电讯), 中国移动...}
- 物流 {SF}
- More : <http://www.postgresql.org/about/users/>

许可

- PostgreSQL is released under the PostgreSQL License, a liberal Open Source license, **similar to the BSD or MIT licenses.**
- PostgreSQL Database Management System
- (formerly known as Postgres, then as Postgres95)
- Portions Copyright (c) 1996-2015, The PostgreSQL Global Development Group
- Portions Copyright (c) 1994, The Regents of the University of California
- **Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies.**
- IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

特性

- SQL特性
 - 聚合
 - 窗口
 - 递归
 - 继承
 - 外部表
 - 事件触发器
- 安全特性
 - 存储加密
 - 链路加密
 - 认证方法
 - 行安全策略
- 数据类型特性
 - 几何类型
 - 网络类型
 - 全文检索类型
- JSON, JSONB
- 数组
- 范围
- 复合, 枚举, 域
- PostGIS
- 索引特性
 - btree
 - hash
 - gist
 - spgist
 - gin
 - brin
 - 条件索引/部分索引
 - 函数索引
- 函数特性
 - plpgsql, C, plR, pljava, plpython, plperl, ...
- 扩展特性
 - 流式实时数据处理
 - GPU
 - Aurora
 - UDF
 - UDR,BDR
 - Advisory Lock
 - Madlib, kmean,hll,bloom,
- 功能特性
 - 流复制
 - 模块化
 - 钩子
 - 元表
 - 物化视图, FDW,..



PostgreSQL in China

未来的辉煌我们共同缔造



当年 我们 在一起



PostgreSQL中国用户会 2011 广州



PostgreSQL中国用户会 2012 北京



PostgreSQL中国用户会 2013 杭州

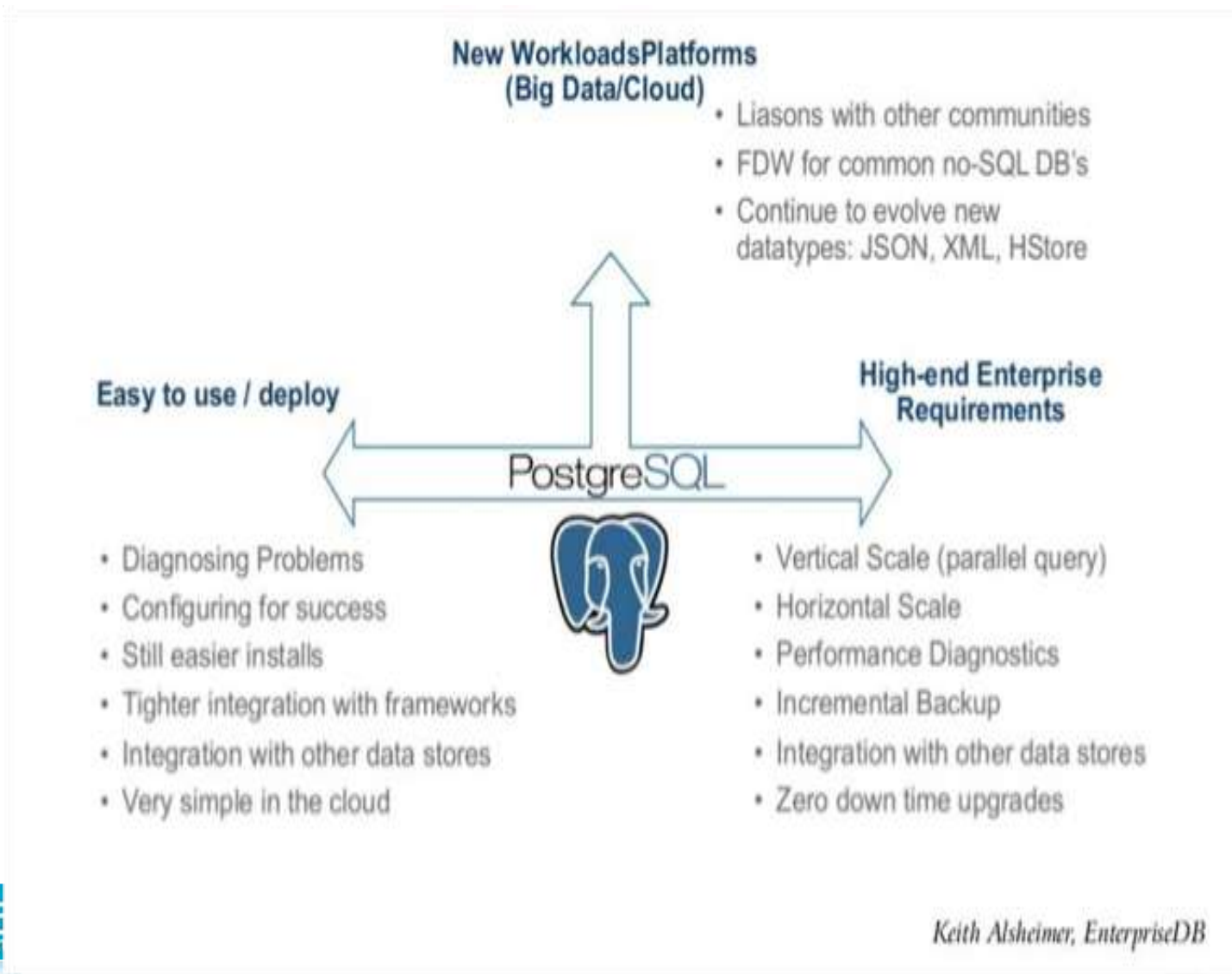


PostgreSQL中国用户会 2014 深圳



明天 PostgreSQL 需要您的参与

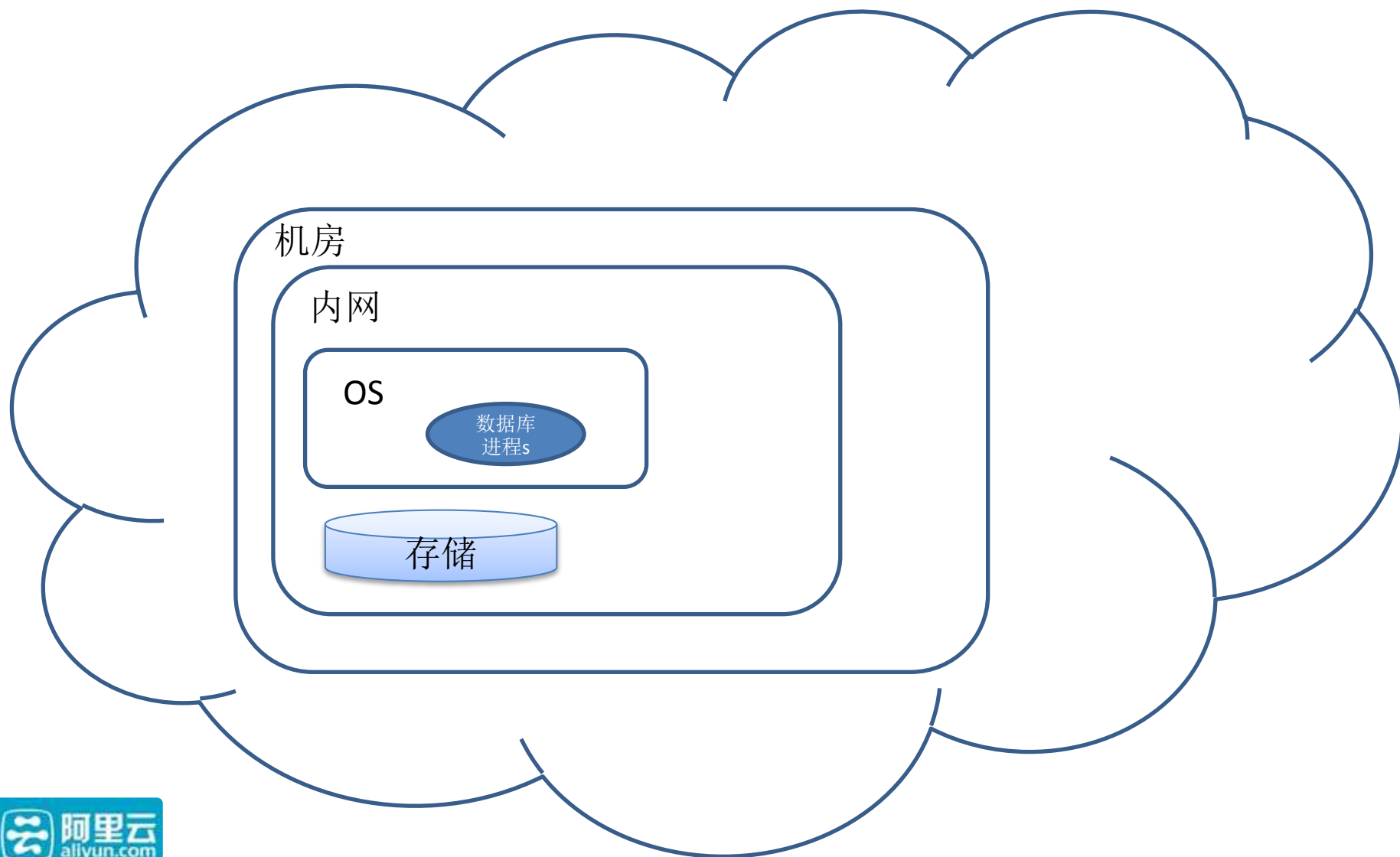
PostgreSQL 未来的发展方向



目录

- 风险在哪里
- 如何防范

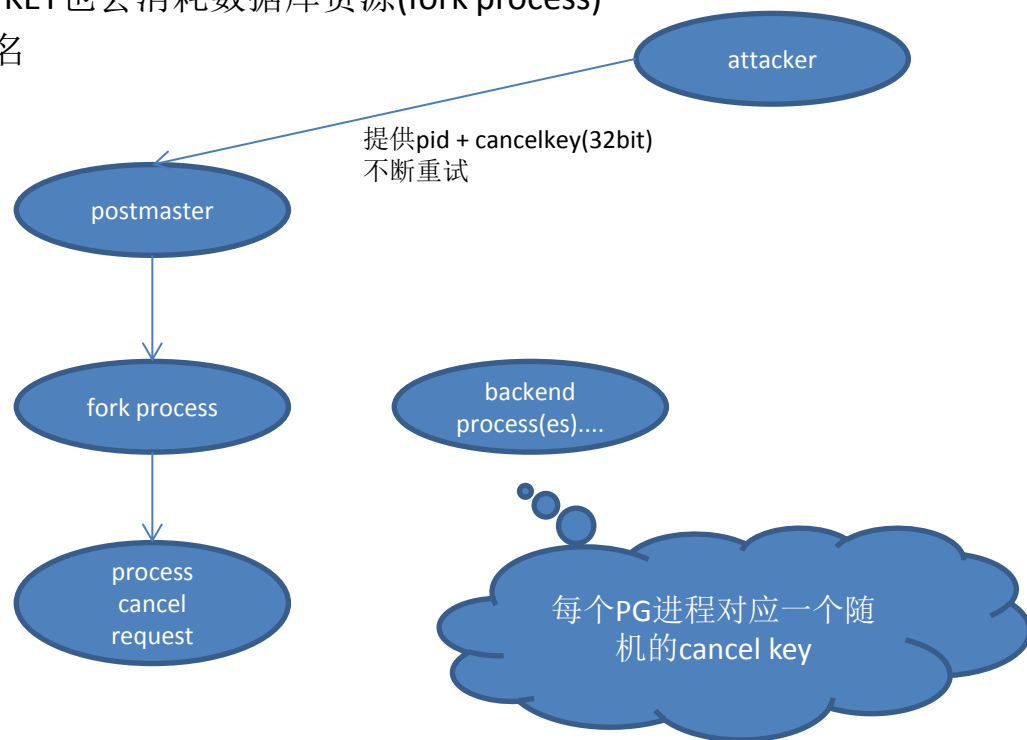
风险在哪里



暴露监听端口

- 风险在哪里
 - 认证攻击
 - 到输入密码阶段, 不输入密码, 占用连接长达1分钟, 多个攻击可以把连接爆满
 - 协议攻击, processCancelRequest
 - 即使没有获取到正确的CANCEL KEY也会消耗数据库资源(fork process)
 - 不需要密码, 用户名, 数据库名

- 如何防范
 - 防火墙(协议层防火墙)
 - 连接池主动断开连接
 - 连接池超时时间小于破解时间
 - 对长连接事务不起作用
 - 黑名单(过滤来源IP)
 - 白名单(过滤来源IP)
 - hack PostgreSQL
 - 类似协议层防火墙, 控制CANCEL阈值
 - 都返回TRUE, 丧失评判标准



暴露监听端口

- 风险在哪里
 - 暴力破解用户密码
- 如何防范
 - pg_hba.conf
 - 密码复杂度
 - 密码更换周期
 - 认证失败延迟响应
 - 不要使用默认用户名或数据库名

密码泄露途径

- 风险在哪里
 - unencrypted password明文存储pg_shadow.passwd
 - ~/.psql_history
 - pg_log/xxx.csv
 - pg_stat_statements
 - 堡垒机日志
 - fdw pg_user_mappings
 - dblink based view
 - 应用程序配置文件
 - 网络层抓包(涉及密码的SQL, 或者pg_hba.conf=password的认证过程)
 - 如何防范
 - 使用加密的密码, create role ... encrypted password '...';
 - 使用psql或其他数据库控制台时, 不记录历史命令。例如psql -n
 - set log_statement='none'; set log_min_duration_statement=-1; set log_duration=off; set pg_stat_statements.track_utility=off; 然后执行敏感SQL, 如创建、修改用户密码。
 - 建议堡垒机过滤敏感信息, 确保堡垒机的日志的私密性
 - 日志披露过滤敏感信息
 - 回收普通用户对pg_user_mappings的查询权限
 - 不在dblink中使用密码
 - 确保应用程序配置文件的私密性
- pg_hba.conf, 使用md5认证方法, 不要使用password认证方法。
- hack PostgreSQL
- 提示输入密码, 隐藏明文; 不写日志; 或日志中转换为MD5;

数据传输

- 风险在哪里
 - 敏感数据可能在传输过程被窃取
- 如何防范
 - 使用SSL连接
 - 敏感数据加密存储和传输

数据窃取

- 风险在哪里
 - 敏感数据可能被非法窃取，如权限分配不当，导致普通用户可以获取敏感数据
 - 数据库被攻击后数据被窃取
- 如何防范
 - 以最小化配置用户权限，如pg_hba.conf, database|schema privilege for public role, object privilege
 - 敏感数据加密存储，需提供解密秘钥才能解密
 - 对敏感数据，审计用户行为，同时记录变更前后的数据 (如通过触发器)
 - hack PostgreSQL(表级，行级审计)

代码窃取

- 风险在哪里
 - 函数内容泄露
- 如何防范
 - 加密函数内容
 - hack PostgreSQL
 - 使用编译函数语言(C)代替解释函数语言(plpgsql, plpython.....)
 - 控制pg_proc.prosrc和pg_get_functiondef()函数的权限

恶意或误操作或SQL注入

- 风险在哪里
 - SQL注入后, 可以drop | truncate table, database, 加用户, 该用户密码, 盗取数据等.....
 - dml 误操作
- 如何防范
 - hack PostgreSQL
 - recyclebin 应对 drop, truncate
 - flashback 应对 DML误操作
 - 建议禁止程序使用非prepared statement
 - 建议程序预防SQL注入, 如添加SQL过滤插件
 - hack PostgreSQL
 - EDB SQL/Protect (配置防SQL注入规则)
 - 数据库快照(文件系统, 虚拟机, ...)
 - 增量备份, 紧急情况下可以使用PITR恢复数据

权限放大

- 风险在哪里
 - 权限被放大
 - 连接配置, 角色权限
 - dlink,fdw (利用 local, localhost trust)
- 如何防范
 - pg_hba.conf收敛
 - 管理账户和应用账户分离
 - 只有管理账户有某些DDL权限(删库, 删schema, 删表, 删表空间, ...)
 - 使用超级用户创建数据库, SCHEMA, 应用所需的对象
 - 创建应用账号角色
 - 回收数据库, schema, language, 应用对象的public权限
 - 将数据库, schema的使用权限赋予给应用账号
 - 将应用需要访问的对象的相关权限赋予给应用账号
 - 通过事件触发器禁止应用账号执行某些DDL
 - 回收函数语言的public权限, 以及普通用户的权限, 用户不能创建函数
 - 控制普通用户使用ONLINE CODE的权限
 - hack PostgreSQL

恶意攻击

- 风险在哪里
 - 利用优化器CBO特性，进行视图攻击，越权访问数据
 - 利用函数安全特性，布下函数, 规则, 触发器陷阱
- 如何防范
 - 强制视图规则优先
 - 使用security_barriers视图
 - 基于安全策略(9.5)来隔离数据
 - hack PostgreSQL
 - 超级用户调用普通用户创建的函数时，自动转换为security definer
 - 创建规则时过滤黑名单函数

潜在风险

- 风险在哪里
 - 已分配事务号的长事务(包括2PC), 导致膨胀, 甚至XID耗尽导致数据库不可用, 必须停库vacuum freeze
- 如何防范
 - 大数据库不使用逻辑备份, 使用物理备份
 - 开启autovacuum
 - 加大maintenance_work_mem, worker processes, 缩小autovacuum scale,factor, 提高IOPS能力
 - 监控数据库年龄, 调度vacuum freeze
 - 监控带事务号的长事务(包括2PC), 设置事务超时
 - hack PostgreSQL
 - 修改可回收deadtuple的评判标准

潜在风险

- 风险在哪里
 - 心跳(堵塞并耗尽连接, 切换时丢事务(只判断time延迟))
- 如何防范
 - 修改心跳机制, 从REDO中获取心跳数据
 - hack PostgreSQL
 - 增加切换延迟评判标准
 - commit_ts, lsn

潜在风险

- 风险在哪里
 - 通过滥用资源(cpu,io,disk,memory,network,errlog)进行攻击
 - dblink, postgres_fdw
 - 即使没有密码，也可以造成频繁fork process，日志爆满，relcache write (global/pg_internal.\$pid)
 - 有密码就更危险，已在数据库服务器所在局域网。
- 如何防范
 - 控制资源使用，如用户级，SQL级
 - hack PostgreSQL
 - cgroup(注意文件系统锁)

外界风险

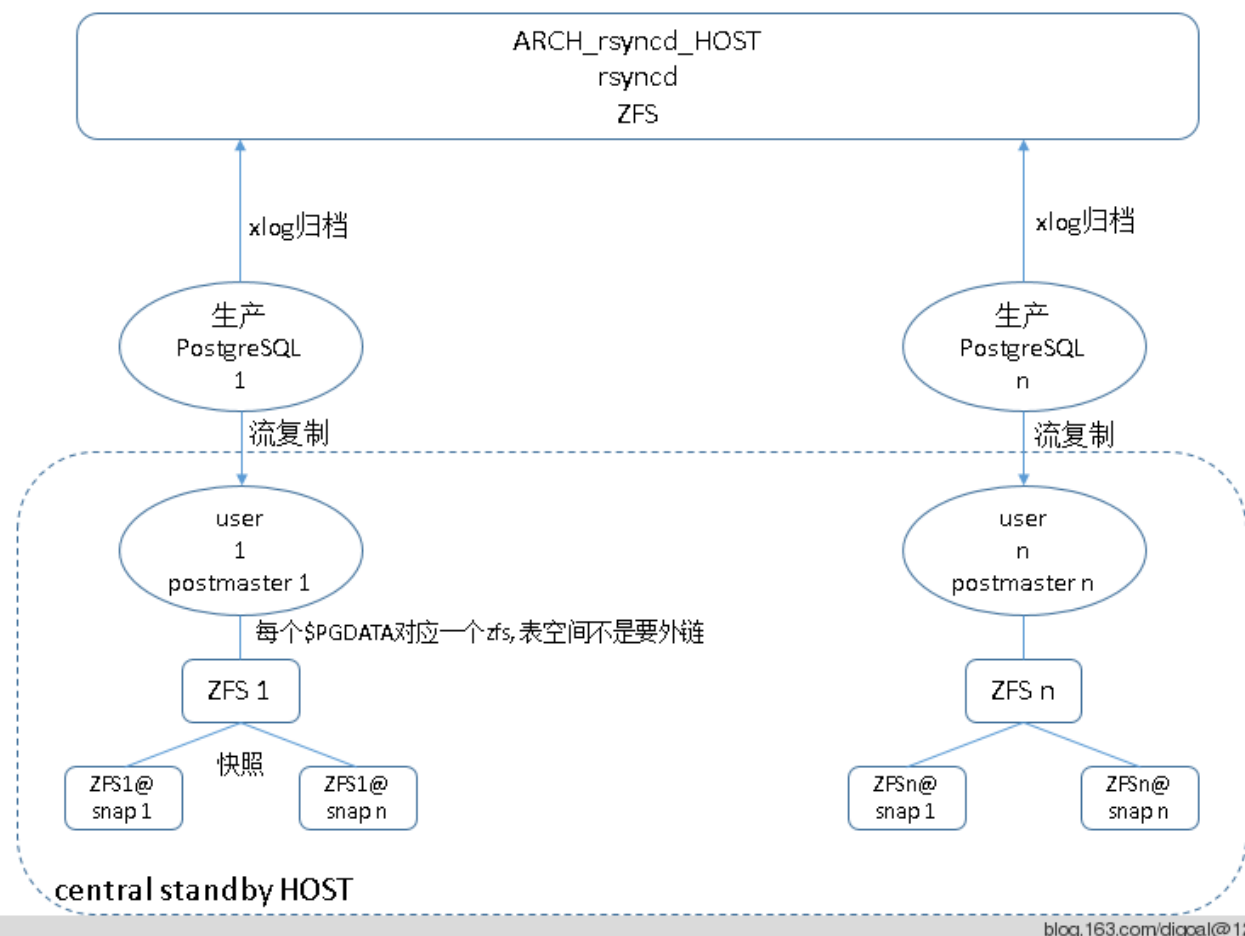
- 风险在哪里
 - 应用程序，（获取密码，SQL注入）
 - 中间件，（获取密码，SQL注入）
 - 操作系统，（破坏，越权，窃取）
 - 服务器、宿主机，（破坏，越权，窃取）
 - 存储，（破坏，窃取）
 - 内网，外网，（窃取）
 - 机房，（破坏，窃取）
- 如何防范
 - 不断完善安全规范

审计

- 审计内容
 - 记录敏感数据表的DQL, DML, DDL操作。
 - DML和TRUNCATE记录变更前后的ROW。
 - DQL和DDL记录完整的SQL。
 - 审计内容还应包含操作用户名，时间，客户端IP，端口，事务号等信息。
 - 连接和断开连接
 - 根据需求配置 `log_statement = '?'` # none, ddl, mod, all
 - 用户级，数据库级，全局配置。
 - hack PostgreSQL(表级，行级)

备份

- 需要考虑的问题
 - SLA
 - 备份耗时
 - 恢复到任意时间点
 - 恢复耗时
 - 空间消耗
 - 网络消耗
 - 性能影响



监控、巡检

- 监控指标

- 对象，数据库，表空间 **size**，表空间 **剩余可用** 空间
- 对象，数据库 **年龄**
- 表，物化视图的 **索引数量**
- 索引 **扫描次数**
- 表，物化视图，索引 **膨胀** 字节数，膨胀比例
- **deadtuple**
- **序列剩余** 次数
- HA，备份，归档，备库延迟状态
- 事件触发器
- 触发器
- 错误日志统计
- 慢SQL及当时的analyze执行计划，
- TOP SQL
- 数据库级别统计信息，回滚数，提交数，命中率，死锁次数，IO TIME，tuple DML次数
- unlogged table, hash index
- 检查点统计信息
- 锁等待
- 活跃度，active, idle, idle in transaction 状态会话数，剩余可用连接数
- 带事务号的长事务，2PC事务
- 网卡利用率，CPU利用率，IO利用率，内存利用率

补丁

- 如何降低对业务的影响
- 小版本升级
- 大版本升级
 - UDR
 - pg_upgrade
 - Londiste3, slony-l, ...

感兴趣PostgreSQL话题点

- 1. PG相比其他数据库的特点，MySQL，Oracle
 - 2. PostgreSQL与MySQL相比，优势何在？
 - 3. 现在网站开发应用PostgreSQL会不会有性能不佳和维护困难的问题？相比较NoSQL呢？
 - 4. PG结合云计算和分布式数据库
 - 5. NOSQL与postgreSQL
 - 6. mysql、Postgresql和MongoDB这三者现在的市场普及度各自在什么水平？
-
- 1. PostgreSQL如何实现异地备份？
 - 2. PostgreSQL中的大数据存储是怎样实现的？
 - 3. PG的数据库安全
 - 4. PostgreSQL的安全性如何？采用什么机制保证数据库的安全？
 - 5. 数据库性能优化
 - 6. PostgreSQL的查询处理和查询优化
 - 7. PostgreSQL是如何实现查询语句的优化的？
 - 8. PostgreSQL中的视图采用规则系统，这样做有什么好处？

感兴趣PostgreSQL话题点

- 1. 想做PG内核开发，应该怎么入手和提高
 - 2. 成为一名合格的DBA需要掌握哪些知识
 - 3. 想要从事数据库开发需要掌握什么？
 - 4. 如何成为一个数据库研发高手
 - 5. 数据库知识的学习路径
 - 6. 不太擅长编程，能做数据库研发么
 - 7. 对象关系数据库怎么理解？相比传统的关系型数据库有什么优势？
-
- 1. 公司需要怎样的数据库人才
 - 2. 从事数据库研发的职业规划和发展
 - 3. PG的最新发展技术，以及如何看待开源
 - 4. 技术是否是青春饭
 - 5. 想求职数据库方面的求职者应该如何做好准备

感兴趣PostgreSQL话题点

- 1. 阿里数据库部门招聘员工,需要他们都具备哪些技能?
 - 2. 阿里数据库部门主要的工作?
 - 3. 阿里数据库部门的加班情况, 日常的工作氛围?
 - 4. 阿里对于postgresql数据库人才的需求是怎么样的?
 - 5. 请介绍下阿里的企业文化?
 - 6. 阿里数据库团队大概有多少, 其中pg团队大概有多少人
 - 7. 阿里在招数据库人才的时候更看中哪些方面的能力
-
- 1. 阿里今年招了多少pg人才
 - 2. pg在阿里的应用情况, pg人才在阿里的的发展情况, pg团队在阿里的主要工作
 - 3. 阿里每年校招和社招的人数和比例 --
 - 4. 阿里的数据库部门的薪水情况? --
 - 5. 如何看待今年阿里的缩招和降薪? --
 - 6. 对于今年阿里缩招, 是今年的特例还是以后阿里的对于人才的需求下降了? --
 - 7. 如何看待今年互联网遭遇的招聘危机?

谢谢！

- QQ/微信：276732431
- BLOG：<http://blog.163.com/digoal@126>
- PostgreSQL 安全指南
 - <http://blog.163.com/digoal@126/blog/static/16387704020155131217736/>
- 2015 PostgreSQL 用户大会
 - 11月20,21日 北京
 - <http://postgres2015.eventdove.com/>

