睿创神脑
RUICHUANGSHENNAO

PolarDB
PostgreSQL

PostgreSQL
实例连接访问控制

睿创神脑
RUICHUANGSHENNAO

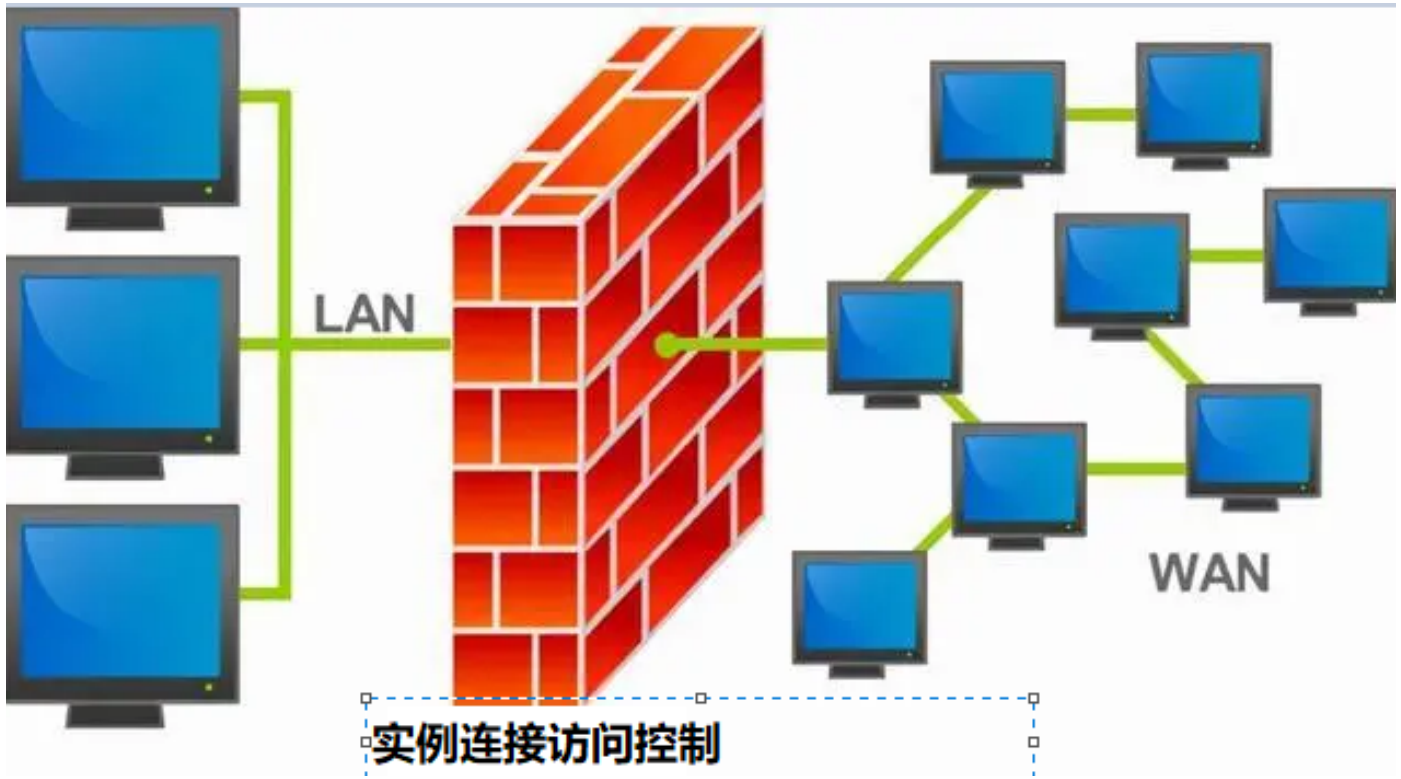
PolarDB PostgreSQL

Objectives

- PostgreSQL实例访问控制概述
- pg_hba.conf文件配置

实例连接访问控制概述

- 实例访问控制就像是一道防火墙，用它来控制来自于不同主机、不同用户是否允许访问指定的数据库、以及验证方式。



睿创神脑
RUICHUANGSHENNAO

pg_hba.conf文件

PolarDB PostgreSQL

- 客户端认证是由一个配置文件（通常名为pg_hba.conf并被存放在数据目录中）控制（HBA表示基于主机的认证）。
- 在initdb初始化数据目录时，它会安装一个默认的pg_hba.conf文件。不过我们也可以把认证配置文件放在其它地方。
- pg_hba.conf文件的常用格式是一组记录，每行一条。空白行将被忽略， #注释字符后面的任何文本也被忽略。记录不能跨行。
- 一条记录由若干用空格/或制表符分隔的域组成。如果域值用双引号包围，那么它可以包含空格。在数据库、用户或地址域中 引用一个关键字（例如，all或replication）将使该词失去其特殊 含义，并且只是匹配一个有该名字的数据库、用户或主机。

pg_hba.conf文件

名单格式

- TYPE：指定连接类型
- DATABASE：指定连接的数据库名
- USER：指定连接的用户名
- ADDRESS：指定访问的客户端主机
- METHOD：指定验证方式

pg_hba.conf文件

名单格式

- TYPE：指定连接类型
  - local：表示本地连接，只对Unix/Linux系统有效，使用socket方式登录
  - host：表示主机通过TCP/IP连接
  - hostssl：表示主机连接需要SSL加密方式连接

睿创神脑
RUICHUANGSHENNAO

pg_hba.conf文件

PolarDB PostgreSQL

名单格式

- DATABASE：指定连接的数据库
  - all：表示所有的数据库
  - db_name：表示指定的数据库
  - replication：表示主备复制时的连接

pg_hba.conf文件

名单格式

- USER：指定连接的用户
  - all：表有所有用户
  - user_name：表示指定的用户
  - +group_name：表示一组用户
  - @file_name：表示文件中包含的用户列表

睿创神脑
RUICHUANGSHENNAO

pg_hba.conf文件

PolarDB PostgreSQL

名单格式

- ADDRESS：指定连接的客户端
  - 127.0.0.1/32：表示本地客户端主机
  - 0.0.0.0/0：表示所有客户端主机
  - host_name：表示指定的主机名（hosts文件中包含）
  - ip_addr/net_mask：表示指定的ip地址或者网段

pg_hba.conf 示例：

```
host    all         +g1          0.0.0.0/0              md5      #g1组

host    all         u1           192.168.18.0/24        md5     #某个网段
```

睿创神脑
RUICHUANGSHENNAO

pg_hba.conf文件

PolarDB PostgreSQL

名单格式

- METHOD：指定验证方式
  - trust：信任客户端连接，无需提供密码
  - scram-sha-256：这是当前提供的方法中最安全的一种，但是旧的客户端库不支持这种方法。
  - md5：它能防止口令嗅探并且防止口令在服务器上以明文存储，但是无法保护攻击者想办法从服务器上窃取了口令哈希的情况。
  - password：方法password以明文形式发送口令，因此它对于口令“嗅探”攻击很脆弱。
  - ident：该模式下系统会将请求发起者的操作系统用户映射为PostgesSQL数据库内部用户，并以该内部用户的权限登录，且此时无需提供登录密码。操作系统用户与数据库内部用户之间的映射关系会记录在pg_ident.conf文件中。
  - peer：该模式使用连接发起端的操作系统名进行身份验证。仅限于Linux、BSD、Mac OS X和Solaris，并且仅可用于本地服务器发起的连接。
  - reject：该模式表示拒绝所有请求。

睿创神脑
RUICHUANGSHENNAO

pg_hba.conf文件

PolarDB PostgreSQL

常见配置实例

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     trust
# IPv4 local connections:
host    all             all             127.0.0.1/32            trust
# IPv6 local connections:
host    all             all             ::1/128                 trust
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     trust
host    replication     all             127.0.0.1/32            trust
host    replication     all             ::1/128                 trust
host    all              +g1            192.168.18.0/24         md5
host    all             cuug            0.0.0.0/0               ident   map=cuug
```

睿创神脑
RUICHUANGSHENNAO

pg_hba.conf文件

PolarDB PostgreSQL

冲突处理规则：

```
host    testdb  u1      pg-xc2              trust
host    all     all     192.168.18.0/24     md5
host    all     all     0.0.0.0/0           reject
```

处理的优先级是根据先后顺序(规则被匹配后，下面的规则就跳过了)：

1、信任来自pg-xc2主机的u1用户访问testdb数据库
2、来自于192.168.18.0网段的所有用户访问所有数据库需要密码验证
3、初了上面的连接允许外，其它的连接请求全部拒绝
4、如果把第三行放在最前面，则拒绝所有主机的连接请求（包括另外两个连接设置）

睿创神脑
RUICHUANGSHENNAO

PolarDB
PostgreSQL

总结

- PostgreSQL实例访问控制概述
- pg_hba.conf文件配置

睿创神脑
RUICHUANGSHENNAO

PolarDB PostgreSQL

练习

- 1、配置postgresql.conf, 开启csvlog, 同时开启连接日志记录.
- 2、配置pg_hba.conf, 允许所有来源IP使用md5认证方式访问数据库实例.
- 3、连接数据库, 并观察日志, 是否记录了来源信息.

睿创神脑
RUICHUANGSHENNAO

PolarDB PostgreSQL