GREENPLUM DATABASE

腾讯云大学

六节课

快速上手Greenplum

第二节课

Greenplum备份、安全与高可用

线上直播 | 8月8日 14：00 - 15：00

GREENPLUM DATABASE

腾讯云大学

六节课快速上手Greenplum

第二课

Greenplum 备份、安全与高可用

Greenplum高级解决方案架构师：李兴欣

目录

Greenplum高可用

Greenplum 高可用

Greenplum 数据库软件自身具备多层次容错和冗余功能，同时对于底层硬件设备，Greenplum也提出了很多容 错机制的要求，以保 证系统7x24不间断的运行处理：

- 管理节点

✓部署2台管理节点，为1主1备（Standby）方式

✓主管理节点和 Standby 管理节点自动数据同步

✓主管理节点失败时切换到Standby管理节点

- 数据节点

✓采用镜像技术，将数据节点的primary实例的数据自 动镜像到位于其它数据 节点mirror实例中；

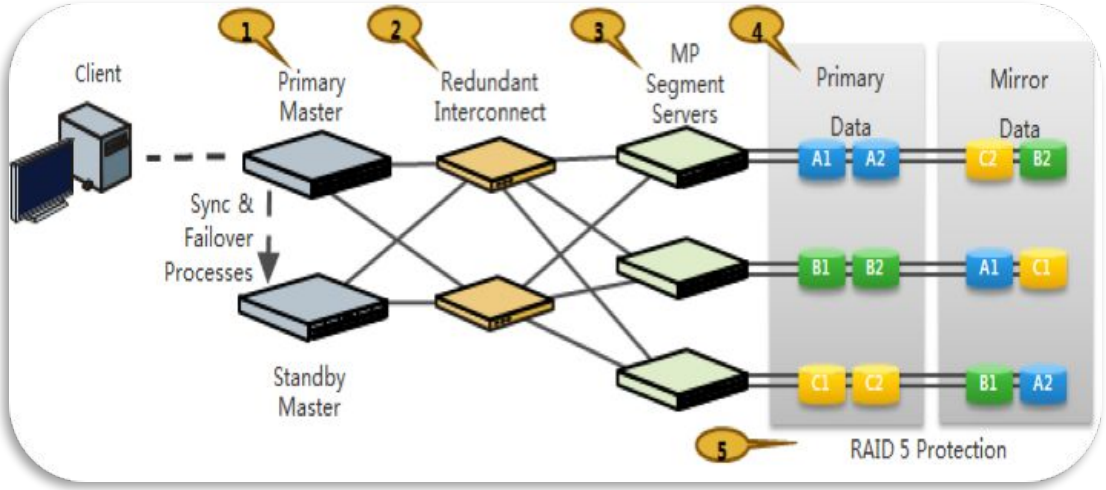
✓Primary实例故障时，自动侦测并启用镜像实例，保证用户数据完整和服 务不中断

- 交换机

✓系统一般部署2台网络交换机

✓正常情况下，2台交换机同时工作，负载均衡

✓异常情况下，如1台交换机故障，另外1台将进行冗余保护



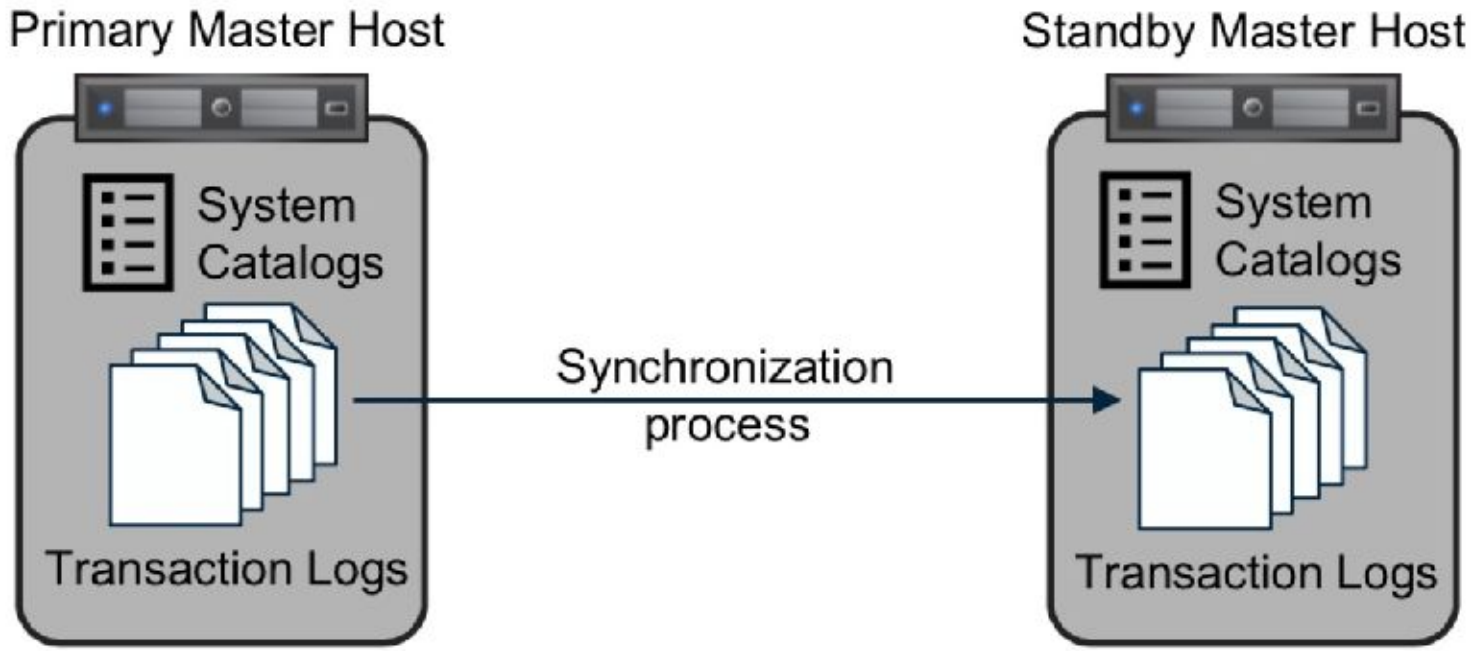
- 服务器

✓ 硬件组件冗余保护(Fan, PSU…)

✓ 服务器硬盘Raid 5保护

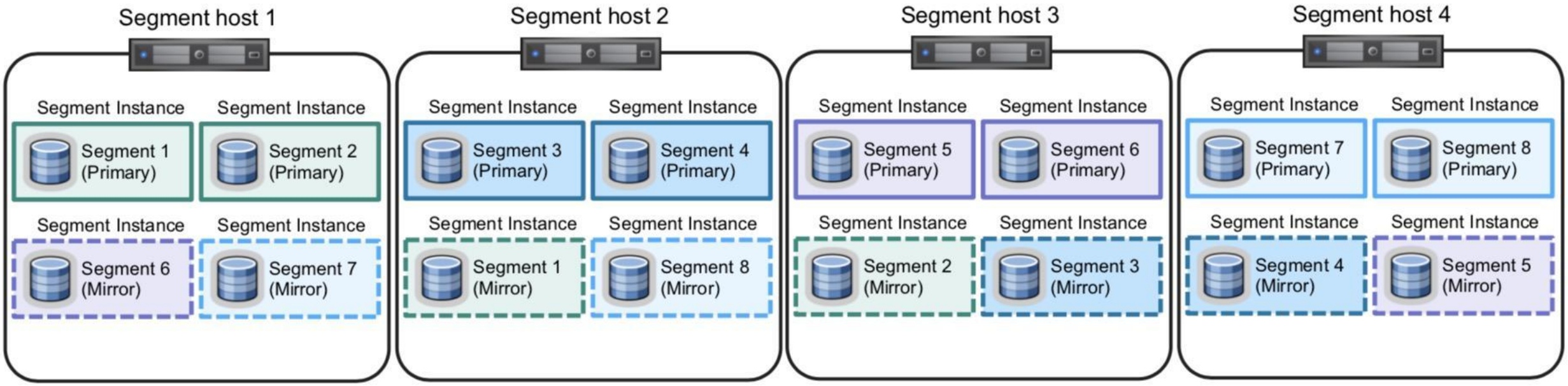
✓ 更换新盘后Raid 5 data 自动重建

Greenplum □ □ □ -master



$ gpstate -f

Greenplum 高可用-segment



$ gpstate -m

$ gprecoverseg

Greenplum高可用-系统表

系统表gp_segment_configuration进行维护所有节点包括master,standby信息

字段名	描述
dbid	每个节点的唯一id
content	每个pair组的id，master-standby为-1，primary-mirror从0开始递增
role	‘p’ primary，‘m’ mirror
preferred_role	初始化时的值，对于一个被promote成primary的mirror节点，role为’p’，preferred_role为’m’
mode	主从同步状态，’s’同步，’n’不同步
status	运行状态，’u’在线，’d’不在线
port	该节点的运行端口
hostname	节点的hostname
address	通常和hostname相同
datadir	该节点的数据目录

Select * from gp_segment_configuration where status = ‘d’;

Greenplum高可用-系统视图

系统视图gp_stat_replication包含walsender进程的复制状态统计信息

column	type	references	description
gp_segment_id	integer		Unique identifier of a segment (or master) instance.
pid	integer		Process ID of the walsender backend process.
usesysid	oid		User system ID that runs the walsender backend process.
usename	name		User name that runs the walsender backend process.
application_name	text		Client application name.
client_addr	inet		Client IP address.
client_hostname	text		Client host name.
client_port	integer		Client port number.
backend_start	timestamp		Operation start timestamp.
state	text		walsender state. The value can be: startup backup catchup streaming
sent_location	text		walsender xlog record sent location.
write_location	text		walreceiver xlog record write location.
flush_location	text		walreceiver xlog record flush location.
replay_location	text		Master standby or segment mirror xlog record replay location.
sync_priority	integer		Priority. The value is 1.
sync_state	text		walsendersynchronization state. The value is sync.
sync_error	text		walsender synchronization error. none if no error.

Greenplum安全

安全

- 身份验证
- 数据库连接和数据加密
- 授权
- 审计

身份验证-pg_hba.conf

GREENPLUM DATABASE 腾讯云大学

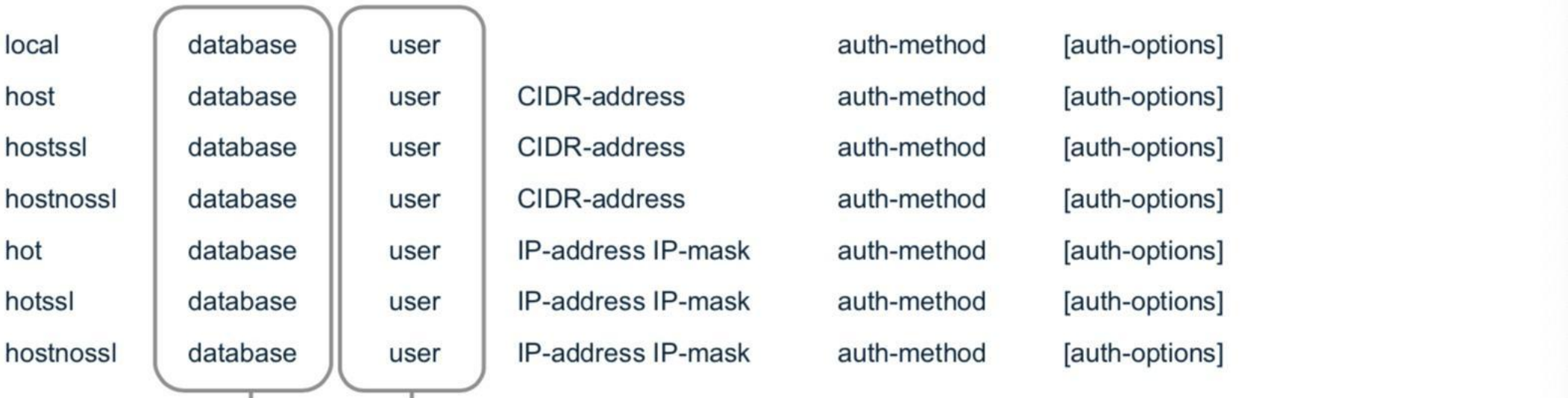
- Handles the user authentication
- The file is located in $MASTER_DATA_DIRECTORY
- Comments are ignored
- File is read line by line
- First matching line is used
- All subsequent lines are ignored
- Pessimistic – if no grants, then deny access
- To be able to access to a Greenplum database from a distant host, the couple role/host has to be set in the configuration file pg_hba.conf

身份验证-pg_hba.conf

local	database	user		auth-method	[auth-options]
host	database	user	CIDR-address	auth-method	[auth-options]
hostssl	database	user	CIDR-address	auth-method	[auth-options]
hostnossl	database	user	CIDR-address	auth-method	[auth-options]
hot	database	user	IP-address IP-mask	auth-method	[auth-options]
hostssl	database	user	IP-address IP-mask	auth-method	[auth-options]
hostnossl	database	user	IP-address IP-mask	auth-method	[auth-options]

- Type of connection
  - local: Connection is coming in over the Unix Domain Socket
  - host: Connection over the network, encryption is optional
  - hostssl: Connection over the network, encryption is enforced
  - hostnossl: Connection over the network, no encryption

身份验证-pg_hba.conf



- Name of the user
  - Role name, or list of role names separated by comma
  - 'all' for all roles
  - @ followed by filename: file containing role names, one per line
  - + role name: a group where access is granted to all members of this group

- Name of database
  - Database name, or list of database names separated by comma
  - 'all' for all databases
  - @ followed by filename: file containing database names, one per line

身份验证-pg_hba.conf

local	database	user		auth-method	[auth-options]
host	database	user	CIDR-address	auth-method	[auth-options]
hostssl	database	user	CIDR-address	auth-method	[auth-options]
hostnossl	database	user	CIDR-address	auth-method	[auth-options]
hot	database	user	IP-address IP-mask	auth-method	[auth-options]
hotssl	database	user	IP-address IP-mask	auth-method	[auth-options]
hostnossl	database	user	IP-address IP-mask	auth-method	[auth-options]

- Network address
  - Only for „host“, „hostssl“ and „hostnossl“ (1st column)
  - Network address might be an IPv4 or IPv6 address

CIDR-Address	IP-Address + IP-Mask		Comment
192.107.2.89/32	192.107.2.89	255.255.255.255	Single network
192.107.2.0/24	192.107.2.0	255.255.255.0	Small network
192.107.0.0/16	192.107.0.0	255.255.0.0	Large nerwork
0.0.0.0/0	0.0.0.0	0.0.0.0	Full network

身份验证-pg_hba.conf

local	database	user		auth-method	[auth-options]
host	database	user	CIDR-address	auth-method	[auth-options]
hostssl	database	user	CIDR-address	auth-method	[auth-options]
hostnossl	database	user	CIDR-address	auth-method	[auth-options]
hot	database	user	IP-address IP-mask	auth-method	[auth-options]
hotssl	database	user	IP-address IP-mask	auth-method	[auth-options]
hostnossl	database	user	IP-address IP-mask	auth-method	[auth-options]

- Authentication method:

•**trust**: 该模式可以不用密码直接连接数据库，不安全，一般用于集群内部或局域网内
•**reject**: 该模式表示拒绝所有请求
•**md5**: 该模式较常用，发送之前使用md5算法加密的密码
•**password**: 该模式是使用明文密码进行身份验证
•**ldap**: 使用LDAP服务器认证
•**gss**: 用GSSAPI和 Kerberos 认证用户，只对TCP/IP 连接可用
•**pam**: 使用操作系统提供的可插入认证模块服务(PAM)认证
•**radius**: 用 RADIUS 服务器认证
•**cert**: 使用SSL客户端证书认证
•**ident:** 通过获取客户端的操作系统用户名，检查是否与被访问的数据库用户名匹配

身份验证-pg_hba.conf

GREENPLUM DATABASE 腾讯云大学

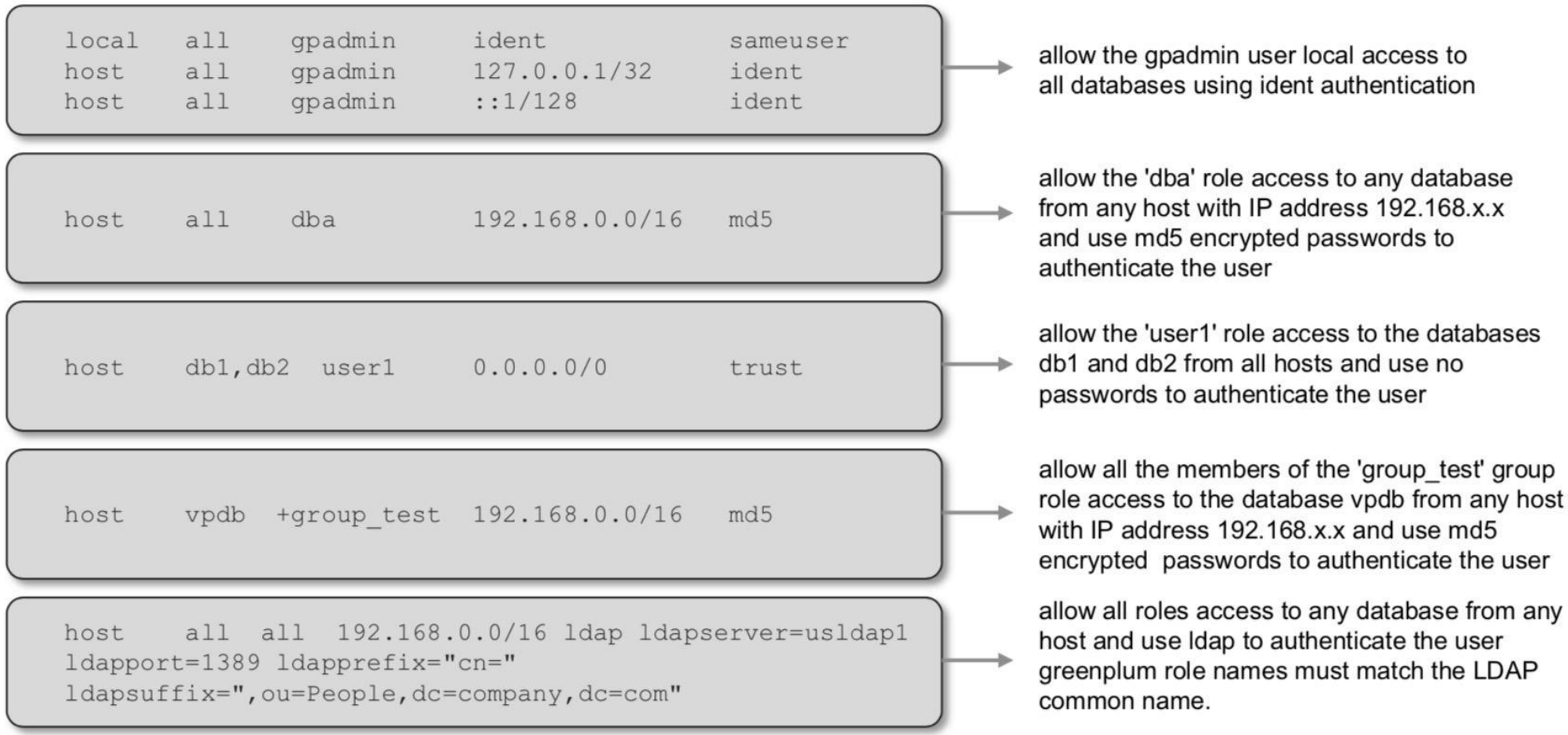
- The command gpstop -u allows to take into account the changes in the file pg_hba.conf
  - Without this command, even if you change the file pg_hba.conf, the new settings won't be took into account.
  - This command doesn't stop the database (only refresh the settings)

- The order of the settings in the file pg_hba.conf is very important.
  - If an access grant is given earlier in the file, this access grant can't change later.

```
host    all     user1   0.0.0.0/0           trust
host    all     user1   192.168.0.0/16      md5
```

This setting won't be applied

身份验证-pg_hba.conf



加密数据和连接-连接

- 客户机和主数据库之间的连接用SSL加密

OpenSSL

$GP_HOME/etc/openssl.cnf

Configuring postgresql.conf

- ssl boolean. Enables SSL connections
- ssl_ciphers string
- ssl_cert_file = 'server.crt'
- ssl_key_file = 'server.key'

SSL server files in the Master and all Segments Data Directory:

- server.crt. Server certificate.
- server.key. Server private key.
- root.crt. Trusted certificate authorities.

```
hostssl  all          gpadmin          192.168.167.130/32 md5
```

```
[gpadmin@gpexp ~]$ psql  -h 192.168.167.129 -d edwdb -p 5432 -U gpadmin
psql (9.4.24)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

edwdb=#
```

加密数据和连接-gpfdist

- Greenplum数据库允许对文件分发服务器、gpfdist和segment主机之间传输的数据进行SSL加密

```
gpfdist   --ssl <certificate_path>
```

```
gpload.yaml SSL -
```

```
CREATE EXTERNAL TABLE ext_expenses ( name text, date date, amount float4, category text,
desc1 text ) LOCATION ('gpfdists://etlhost-1:8081/*.txt', 'gpfdists://etlhost-2:8082/*.txt') FORMAT
'TEXT' ( DELIMITER '|' NULL ' ') ;
```

加密数据和连接-静态数据加密

GREENPLUM DATABASE 腾讯云大学

- 使用pgcrypto模块 加密/解密功能的保护数据库中的静态数据

Table 1. Pgcrypto Supported Encryption Functions

Value Functionality	Built-in	With OpenSSL
MD5	yes	yes
SHA1	yes	yes
SHA224/256/384/512	yes	yes [1]
Other digest algorithms	no	yes [2]
Blowfish	yes	yes
AES	yes	yes [3]
DES/3DES/CAST5	no	yes
Raw Encryption	yes	yes
PGP Symmetric-Key	yes	yes
PGP Public Key	yes	yes

加密数据和连接-静态数据加密

GREENPLUM DATABASE 腾讯云大学

- **General Hashing Functions**
  digest()
  hmac()
- **Password Hashing Functions**
  crypt()
  gen_salt()
- **PGP Encryption Functions**
  pgp_sym_encrypt()
  pgp_sym_decrypt()
  pgp_pub_encrypt()
  pgp_pub_decrypt()
- **Raw Encryption Functions**
  encrypt()
  decrypt()

授权-对象权限

GREENPLUM DATABASE 腾讯云大学

Object Type	Privileges
Tables, Views, Sequences	• SELECT • INSERT • UPDATE • DELETE • RULE • ALL
External Tables	• SELECT • RULE • ALL
Databases	• CONNECT • CREATE • TEMPORARY | TEMP • ALL
Functions	EXECUTE
Procedural Languages	USAGE
Schemas	• CREATE • USAGE • ALL

授权-SHA-256加密用户密码

GREENPLUM DATABASE 腾讯云大学

```
edwdb=# show password_encryption;
 password_encryption
---------------------
 on
edwdb=# set password_hash_algorithm = 'SHA-256‘;
edwdb=# show password_hash_algorithm;
 password_hash_algorithm
-------------------------
 SHA-256

edwdb=# SELECT rolpassword FROM pg_authid WHERE rolname = 'testdb';
             rolpassword
-----------------------------------
 md5cd60468d9c0660a0b414b77befc289a3

edwdb=# drop role testdb ;
DROP ROLE
edwdb=# create role testdb with password '123456' login;
NOTICE:  resource queue required -- using default resource queue "pg_default"
CREATE ROLE
edwdb=# SELECT rolpassword FROM pg_authid WHERE rolname = 'testdb';
                                rolpassword
-----------------------------------------------------------------------
 sha2562f3d7e9c0c03e6dfc8b3caffac9d20508132d11ef1da985dbb5152d04e100f19
```

授权-限制访问时间

GREENPLUM DATABASE 腾讯云大学

```
edwdb=# ALTER ROLE testdb DENY BETWEEN DAY 'Monday' TIME '02:00' AND DAY 'Monday' TIME '04:00'
edwdb-# ;
ALTER ROLE
edwdb=#
edwdb=# ALTER ROLE testdb DROP DENY FOR DAY 'Monday'
```

审计

- pg_log/gpdb-2020-*.csv
  - startup and shutdown of the system
  - segment database failures
  - SQL statements and information
  - SQL statements that result in an error
  - all connection attempts and disconnections

```
gplogfilter –f ‘panic’ 2020-08*.csv >log.panic
```

数据库端口与协议

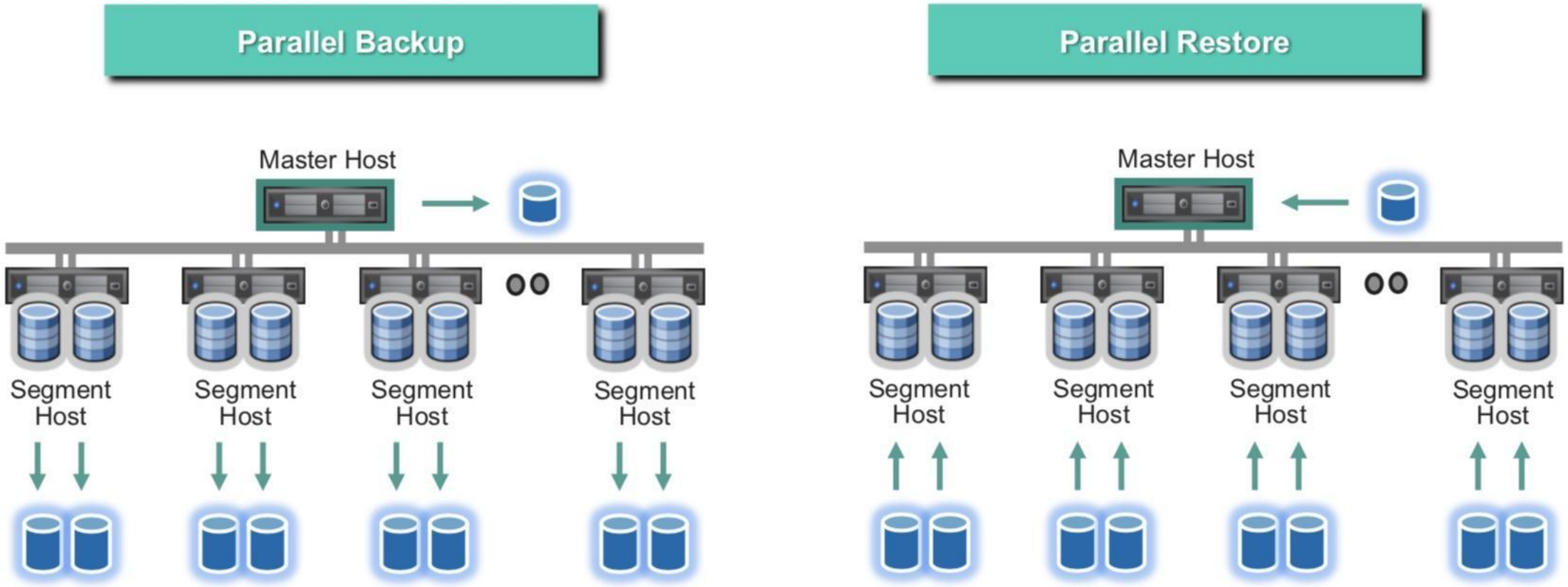
Table 1. Greenplum Database Ports and Protocols

Service	Protocol/Port	Description
Master SQL client connection	TCP 5432, libpq	SQL client connection port on the Greenplum master host. Supports clients using the PostgreSQL libpq API. Configurable.
Segment SQL client connection	varies, libpq	The SQL client connection port for a segment instance. Each primary and mirror segment on a host must have a unique port. Ports are assigned when the Greenplum system is initialized or expanded. The `gp_segment_configuration` system catalog records port numbers for each primary (p) or mirror (m) segment in the `port` column. Run `gpstate -p` to view the ports in use.
Segment mirroring port	varies, libpq	The port where a segment receives mirrored blocks from its primary. The port is assigned when the mirror is set up. The `gp_segment_configuration` system catalog records port numbers for each primary (p) or mirror (m) segment in the `port` column. Run `gpstate -p` to view the ports in use.
Greenplum Database Interconnect	UDP 1025-65535, dynamically allocated	The Interconnect transports database tuples between Greenplum segments during query execution.
Standby master client listener	TCP 5432, libpq	SQL client connection port on the standby master host. Usually the same as the master client connection port. Configure with the `gpinitstandby` utility `-P` option.
Standby master replicator	TCP 1025-65535, gpsyncmaster	The `gpsyncmaster` process on the master host establishes a connection to the secondary master host to replicate the master's log to the standby master.
Greenplum Database file load and transfer utilities: gpfdist, gpload.	TCP 8080, HTTP TCP 9000, HTTPS	The gpfdist file serving utility can run on Greenplum hosts or external hosts. Specify the connection port with the `-p` option when starting the server. The gpload utility runs one or more instances of gpfdist with ports or port ranges specified in a configuration file.
Gpperfmon agents	TCP 8888	Connection port for gpperfmon agents (`gpmmon` and `gpsmon`) executing on Greenplum Database hosts. Configure by setting the `gpperfmon_port` configuration variable in `postgresql.conf` on master and segment hosts.
Backup completion notification	TCP 25, TCP 587, SMTP	The `gpbackup` backup utility can optionally send email to a list of email addresses at completion of a backup. The SMTP service must be enabled on the Greenplum master host.
Greenplum Database secure shell (SSH): gpssh, gpscp, gpssh-exkeys, gppkg	TCP 22, SSH	Many Greenplum utilities use scp and ssh to transfer files between hosts and manage the Greenplum system within the cluster.
Greenplum Platform Extension Framework (PXF)	TCP 5888	The PXF Java service runs on port number 5888 on each Greenplum Database segment host.
Greenplum Command Center (GPCC)	TCP 28080, HTTP/HTTPS, WebSocket (WS), Secure WebSocket (WSS)	The GPCC web server (`gpccws` process) executes on the Greenplum Database master host or standby master host. The port number is configured at installation time.
	TCP 8899, rcp port	A GPCC agent (`ccagent` process) on each Greenplum Database segment host connects to the GPCC rpc backend at port number 8899 on the GPCC web server host.
	UNIX domain socket, agent	Greenplum Database processes transmit datagrams to the GPCC agent (`ccagent` process) on each segment host using a UNIX domain socket.
GPText	TCP 2188 (base port)	ZooKeeper client ports. ZooKeeper uses a range of ports beginning at the base port number. The base port number and maximum port number are set in the GPText installation configuration file at installation time. The default base port number is 2188.
	TCP 18983 (base port)	GPText (Apache Solr) nodes. GPText nodes use a range of ports beginning at the base port number. The base port number and maximum port number are set in the GPText installation configuration file at installation time. The default base port number is 18983.
EMC Data Domain and DD Boost	TCP/UDP 111, NFS portmapper	Used to assign a random port for the mountd service used by NFS and DD Boost. The mountd service port can be statically assigned on the Data Domain server.
	TCP 2052	Main port used by NFS mountd. This port can be set on the Data Domain system using the `nfs set mountd-port` command .
	TCP 2049, NFS	Main port used by NFS. This port can be configured using the `nfs set server-port` command on the Data Domain server.
	TCP 2051, replication	Used when replication is configured on the Data Domain system. This port can be configured using the `replication modify` command on the Data Domain server.
Pgbouncer connection pooler	TCP, libpq	The pgbouncer connection pooler runs between libpq clients and Greenplum (or PostgreSQL) databases. It can be run on the Greenplum master host, but running it on a host outside of the Greenplum cluster is recommended. When it runs on a separate host, pgbouncer can act as a warm standby mechanism for the Greenplum master host, switching to the Greenplum standby host without requiring clients to reconfigure. Set the client connection port and the Greenplum master host address and port in the `pgbouncer.ini` configuration file.

net.ipv4.ip_local_port_range = 10000 65535

Greenplum备份

About Parallel Backups and Restores



New utilities : gpbackup and gprestore

- Designed to improve performance, functionality, and reliability of backups
- gpbackup utilizes ACCESS SHARE LOCK at the individual table level instead of EXCLUSIVE LOCK on pg_class catalog table
- This enables to run DDL statements during the backup like CREATE, ALTER, DROP, and TRUNCATE as long as these aren’t on the table currently being backed up

Full Backups

- 全备

gpbackup --dbname mytest --backup-dir /mybackup

- 支持增量的全备

gpbackup --dbname mytest --backup-dir /mybackup --leaf-partition-data

- DataDomain备份

gpbackup --dbname demo --single-data-file --plugin-config /home/gpadmin/ddboost-test-config.yaml

executablepath: $GPHOME/bin/gpbackup_ddboost_plugin
options:
hostname: "192.0.3.20"
remote_username: "test-dd-remote"
remote_password: "qwer2345erty"
storage_unit: "gpdb-remote"
directory: "test/replication"

Incremental Backups

Incremental backups are efficient when the total amount of data in append-optimized table partitions or column-oriented tables that changed is small compared to the data has not changed.

- supported with
  - Column- and row-oriented append-only tables
  - At the partition level of AO tables
- Back up an AO table if one of the following operations is performed
  - ALTER TABLE
  - DELETE
  - INSERT
  - TRUNCATE
  - UPDATE
  - DROP and then re-create the table

```
gpbackup --dbname mytest --backup-dir /mybackup --leaf-partition-data  --incremental
```

gpbackup_manager

GREENPLUM DATABASE 腾讯云大学

- 显示有关现有备份的信息、删除现有备份或加密安全存储

```
$ gpbackup_manager list-backups

$ gpbackup_manager display-report 20190612154608

$ gpbackup_manager delete-backup 20190620145126

$ gpbackup_manager delete-backup 20190620160656 --plugin-config ~/ddboost_config.yaml
```

Other backup tools

- pg_dump
  can be used to dump only ddl for a schema or database
  pg_dump <db name> -n <schema name> -f DDL_<schema name>.sql –s
  can also be used to create a single backup file of the database/schema on the master
  pg_dump <db name> -n <schema name> -f data_<schema name>.sql -a
- pg_dumpall
  can be used to dump only ddl for global objects (roles and groups)
  pg_dumpall –g > dump_roles.sql
  can also be used to dump only ddl for resource queues
  pg_dumpall –s --resource-queues > dump_resource_queues.sql

Greenplum恢复

gprestore& psql

GREENPLUM DATABASE 腾讯云大学

gprestore --timestamp 20171103152558 --create-db

gprestore --timestamp 20171103152558 --redirect-db demo2

psql –f file

Greenplum使用小技巧

安全-认证

pg_hba.conf格式正确性

$MASTER_DATA_DIRECTORY/pg_log/gpdb_2020*.csv

2020-07-07 17:32:06.763778 CST,"etl","postgres",p56977,th1823688576,"10.2.4.167","50939",2020-07-07 17:32:06 CST,0,con1239887,,seg-1,,,,sx1,"FATAL","28000","no pg_hba.conf entry for host ""10.2.4.167"", user ""etl"", database ""postgres"", SSL off",,,,,,,0,,"auth.c",623,

2020-07-07 15:15:26.768238 CST,,,p351885,th1823688576,,,,0,,,seg-1,,,,,"LOG","00000","received SIGHUP, reloading configuration files",,,,,,,0,,"postmaster.c",4022,
2020-07-07 15:15:26.806472 CST,,,p351885,th1823688576,,,,0,,,seg-1,,,,,"LOG","F0000","end-of-line before authentication method",,,,,"line 93 of configuration file ""/data1/master/gpseg-1/pg_hba.conf""",,0,,"hba.c",1149,
2020-07-07 15:15:26.806496 CST,,,p351885,th1823688576,,,,0,,,seg-1,,,,,"WARNING","01000","pg_hba.conf not reloaded",,,,,,,0,,"postmaster.c",4052,

安全–授权

GREENPLUM DATABASE 腾讯云大学

不要将应用工作任务放在gpadmin下，针对应用不同建立不同角色

gpstart -R

审计

GREENPLUM DATABASE 腾讯云大学

gpconfig -c log_statement -v all

清理空间

rm –rf $DATADIR/pg_log/gpdb-2019-*.csv

不要动: pg_xlog/

备份

RPO 、RTO

- 备份对象
  全库
  重要表
- 备份位置
  本地
  NFS
  本地+scp
  NAS
  Hadoop
- 备份时间
  业务闲时
- 备份频率
  依恢复要求
- 其它
  双集群

感谢观看

Greenplum中文社区公众号

Greenplum微信技术讨论群

GREENPLUM DATABASE®

腾讯云大学

GREENPLUM DATABASE®

腾讯云大学

Q&A