最近数据库勒索病毒又开始出现了

主要是因为客户在连接数据库时使用了盗版版本的 PL/SQL Developer 导致的。在正版的 PL/SQL Developer 软件里面，有一个文件叫做 afterconnect.sql，从名字上来看，该文件将在客户连接数据库之后来执行 SQL 脚本，该文件正常情况下是空的。还有一个文件叫做 login.sql，这个文件当中应该只有一句注释。使用了盗版的，被别有用心的人利用，当病毒触发时，就会将整个数据库加密。

详细信息如下（来自数据与云）：

https://mp.weixin.qq.com/s?__biz=MjM5MDAxOTk2MQ==&mid=2650272273&idx=1&sn=408c33aab5823908c75bf8f995e4fe1e&chksm=be486a07893fe311b4563b32942bfa2ab763b54970c5e9771f9376e8c7c02c6ac4349a6d4346&mpshare=1&scene=1&srcid=1117tgt5ZPnrTTBUGJE63ydv#rd

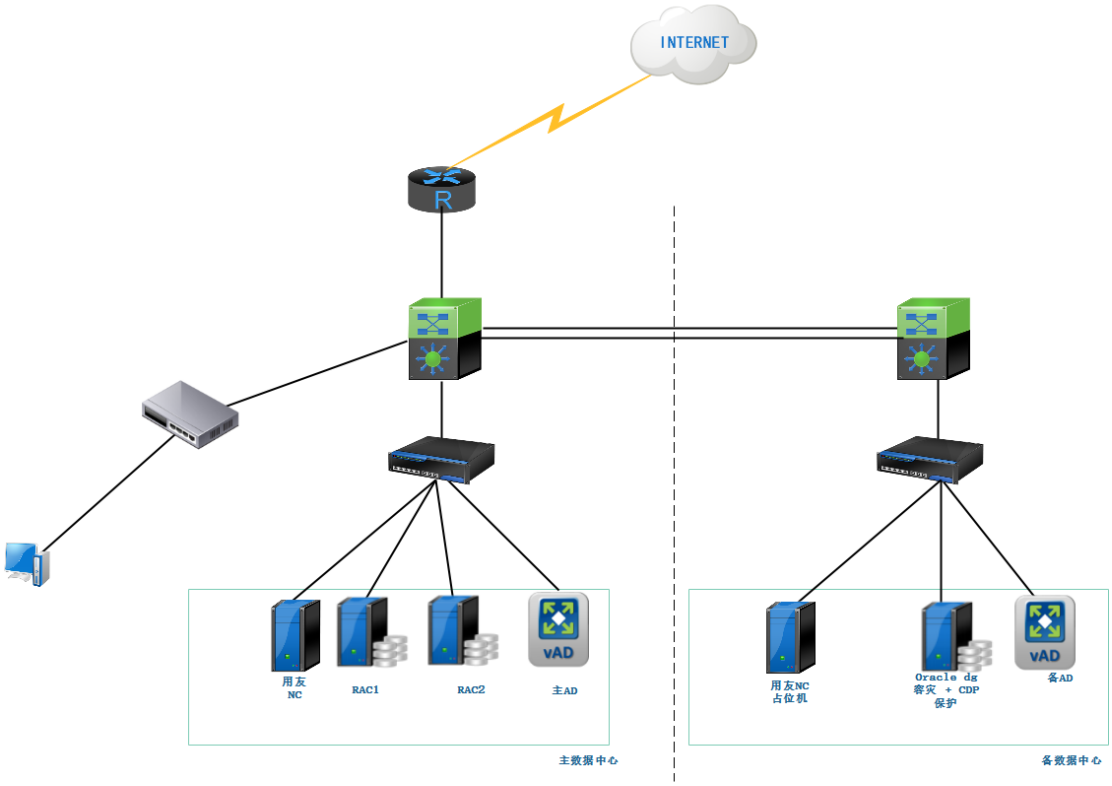
这里以业务层用友 NC，使用自带的中间件，使用 AD 屏蔽底层的 oracle 主备库的差异，底层数据库 oracle rac 为例，来模拟集中情况，其中就有勒索病毒的处理。

数据库层面采用 Oracle rac + dg 单机备机容灾+CDP 备份保护备机

用友 NC 应用层面采用企业级云自带容灾功能，进行容灾、备份保护

用友 NC 应用容灾拓扑：

AD 负载均衡设备可选，负载将数据库请求负载到主库，备库只读可做报表查询



一、正常路径访问

客户端---->用友 NC--->数据库主库

进行正常企业用户模拟办公场景

------ok

正常情况下。用友 NC 访问数据库，从开始启动服务到服务正常工作需要

二、用友 NC 应用故障

用友 NC 应用故障，需要进行恢复

1、发现，本地有备份，直接恢复就行

直接恢复备份，检查业务是否恢复

---ok

2、然后本地若没有相关的备份或者备份数据刚好不能用，需要进行容灾切换

手动页面切换，数据无丢失风险，检查业务是否恢复

---ok

三、数据库 rac 故障（实例故障）：

1、 数据库所在主机 1，故障，导致 RAC1 故障，

RAC2 继续承载工作，自动恢复

2、数据库所在主机 2 也不幸同时出现了故障，本地 rac 集群全部故障

需要异地恢复

进行异地恢复，发现故障前的数据全部都在异地机房，没有数据丢失

恢复后的业务流程，用友 NC--->数据库主库

---ok

四、数据库误删数据（介质故障）

1、人为误删除了一个数据文件，导致数据丢失，开机失败

进行 dg 切换，发现数据都在。然后重新搭建好 rac 环境后重建 DG

----ok

2、在维护数据库过程中，不小心人为 truncate 了一个表

1. create or replace procedure proc1

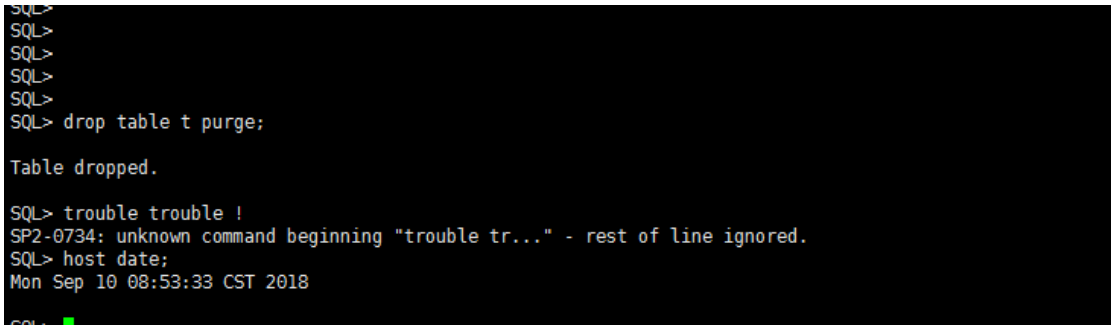
as

```
begin
   for i in 1 .. 100000
   loop
      execute immediate
      'insert into t values ( '||i||')';
      commit;
   end loop;
end;
/
create table t (x int);
exec proc1;
```

查看备库已经有 10 万条记录

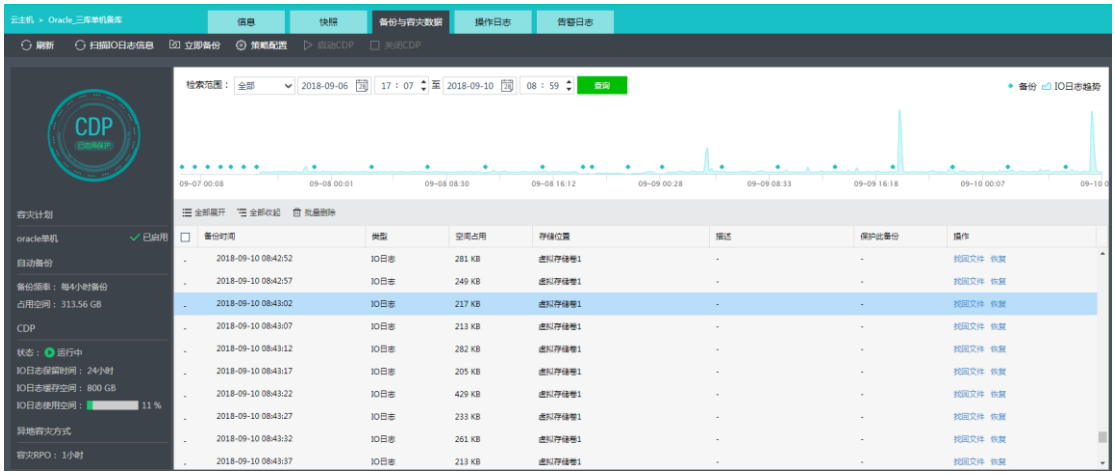
2.误删了数据，

Truncate 误删，或者 drop purge 误删，无法从回收站找回



3.因为是实时应用的，所以备库的数据也是被删除的。

此时恢复 CDP 到 10 分钟前的数据



开机后，把虚拟机网络接到不同的子网，以防 IP 冲突。

```
[oracle@oracle ~]$ dgmgrl sys/oracle@standby
DGMGRL for Linux: Version 11.2.0.4.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle. All rights reserved.

Welcome to DGMGRL, type "help" for information.
Connected.
DGMGRL> show configuration;


Configuration - test

  Protection Mode: MaxPerformance
  Databases:
    racdb     - Primary database
    racdb_std - Physical standby database

Fast-Start Failover: DISABLED

Configuration Status:
ORA-12543: TNS:destination host unreachable
ORA-16625: cannot reach database "racdb"
DGM-17017: unable to determine configuration status
```

然后执行 failover 之后取出被误删的数据。

```
DGMGRL> DGMGRL> failover to racdb_std
Performing failover NOW, please wait...
Failover succeeded, new primary is "racdb_std"
DGMGRL> show configuration;

Configuration - test

  Protection Mode: MaxPerformance
  Databases:
    racdb_std - Primary database
    racdb     - Physical standby database (disabled)
      ORA-16661: the standby database needs to be reinstated

Fast-Start Failover: DISABLED

Configuration Status:
SUCCESS
```

4. 最后取出数据，导入 rac 节点---ok

五、模拟主库中了勒索病毒

主库中了勒索病毒，备库一般也会中招。这个要先看下

需要从 CDP 拉起备库，先正常工作即可，让后重做 DG，切回主站点即可。

重建 DG 这个比较麻烦，但是业务好歹先恢复，不那么着急了。

六、主数据中心正常，灾备演练

在主数据中心正常情况下，进行灾备演练。

预期演练过程中业务中断时间短，数据不丢失

---ok

七、数据中心整体故障，需要进行灾备恢复

演练后业务正常，数据不丢失

---ok

八、业务回迁

主数据中心正常，然后业务回迁。不丢数据，不停业务