### 1 告警码装载实施步骤

1.1 将附件oms-alarm-1045.sql上传到网管主机的omscc账户下。

1.2 执行以下命令加载：

$ dbaccess oms oms-alarm-1045.sql

1.3 加载完成之后，执行以下命令（加粗字体是需要手动操作的）

**telnet 0 8520**

Trying 0.0.0.0...

Connected to 0 (0.0.0.0).

Escape character is '^]'.

HTTP/1.1 200 OK

Please wait...

Welcome to Inaccess Server !

type "logon <name> <password>" first.

none\_0\_0\_0> **l z z**

essage : z logged on

none\_0\_0\_0>**c 2 17 1**

c 2 17 1

message :

connected to alarmprocessor\_2\_17\_1

alarmprocessor\_2\_17\_1>**alarminfo -r**

message :

Refresh alarm base info from db OK!

alarmprocessor\_2\_17\_1>**quit**

message :

disconnected from alarmprocessor\_2\_17\_1

none\_0\_0\_0>**quit**

message : good bye

Connection closed by foreign host.

### 2 gealarm装载实施步骤

1. 进入需要进行日志监控的主机的gealarm账户下，修改gealarm配置文件config.check

2. 1.1 首先将config.check进行备份

$ cd $CINDIR/etc

$ cp config.check config.check.20180417.bak

3. 1.2 进入配置文件

$ vi $CINDIR/etc/config.check

4. 介于BEGIN\_LOGMATCH\_STR和END\_LOGMATCH\_STR之间增加如下配置项

/home/gealarm/genalarm/idsbin/seqscan\.log$:!.\*seq is too large!:1:00003111045:数据库中表顺序扫描次数过多

日志告警监控的配置方法为：

日志绝对路径+日志文件名(正则表达式):关键字:次数门限值:告警码:告警详情

日志绝对路径+日志文件名请按实际情况配置

1. 1.3 修改gealarm配置文件config.check后需要重启使其生效

$ checkdown -y;checkinit