***Oracle研究中心学习笔记：分享一篇关于如何限制IP地址访问Oracle数据库的详细文章，sqlnet.ora文件中TCP.VALIDNODE\_CHECKING参数配置的方法。***

ORACLE的Valid node checking(TCP.VALIDNODE\_CHECKING)是监听的一个功能，可以用于允许或者拒绝指定的IP地址连接数据库，可以把成防火墙在1521端口上面的一个规则。Valid node checking可以定义2个列表，一个是INVITEDNODES列表，指定监听允许连接数据库的IP地址或者是主机名。一个是EXCLUDED\_NODES列表，指定监听不允许连接数据库的IP地址或者是主机名。

RAC环境需要用grid用户修改$ORACLE\_HOME下的sqlnet.ora

[grid@db admin]$ cat sqlnet.ora

# sqlnet.ora Network Configuration File: /u01/app/11.2.0/grid/network/admin/sqlnet.ora

# Generated by Oracle configuration tools.

NAMES.DIRECTORY\_PATH= (TNSNAMES, EZCONNECT)

ADR\_BASE = /u01/app/grid

TCP.VALIDNODE\_CHECKING=yes

TCP.INVITED\_NODES=(192.168.6.24,192.168.6.25)

TCP.EXCLUDED\_NODES=(192.168.6.22,192.168.6.23)

注意：当同时配置2个列表的时候，TCP.INVITED\_NODES比TCP.EXCLUDED\_NODES具有更高的优先性，也就意味着如果IP地址同时在2个列表中时，是允许访问数据库的

根据mos

RAC: TCP.VALIDNODE\_CHECKING Failing after Listener Reload (Doc ID 2109789.1)

n a GRID or RAC environment where TCP.VALIDNODE\_CHECKING is enabled, please be aware that any change to the TCP.INVITED\_NODES or TCP.EXCLUDED\_NODES

parameters would require a complete stop and start of the VIP listeners.

The LSNRCTL reload command after a change to TCP.INVITED\_NODES is breaking the TCP.VALIDNODE feature.  See BUG:22194469 TCP.INVITED\_NODES is Disabled after LSNRCTL Reload

This behavior does not impact the SCAN listeners and does not seem to be present when running a local listener in RDBMS\_HOME.  (Versus GRID)

监听需要stop再start 生效

客户端报错

SQL> conn system/oracle@ttt

ERROR:

ORA-12537: TNS: 连接关闭

监听日志记录

<msg time='2017-12-04T11:12:17.110+08:00' org\_id='oracle' comp\_id='tnslsnr'

type='UNKNOWN' level='16' host\_id='db'

host\_addr='192.168.6.31'>

<txt>TNS-12546: TNS:permission denied

TNS-12560: TNS:protocol adapter error

  TNS-00516: Permission denied