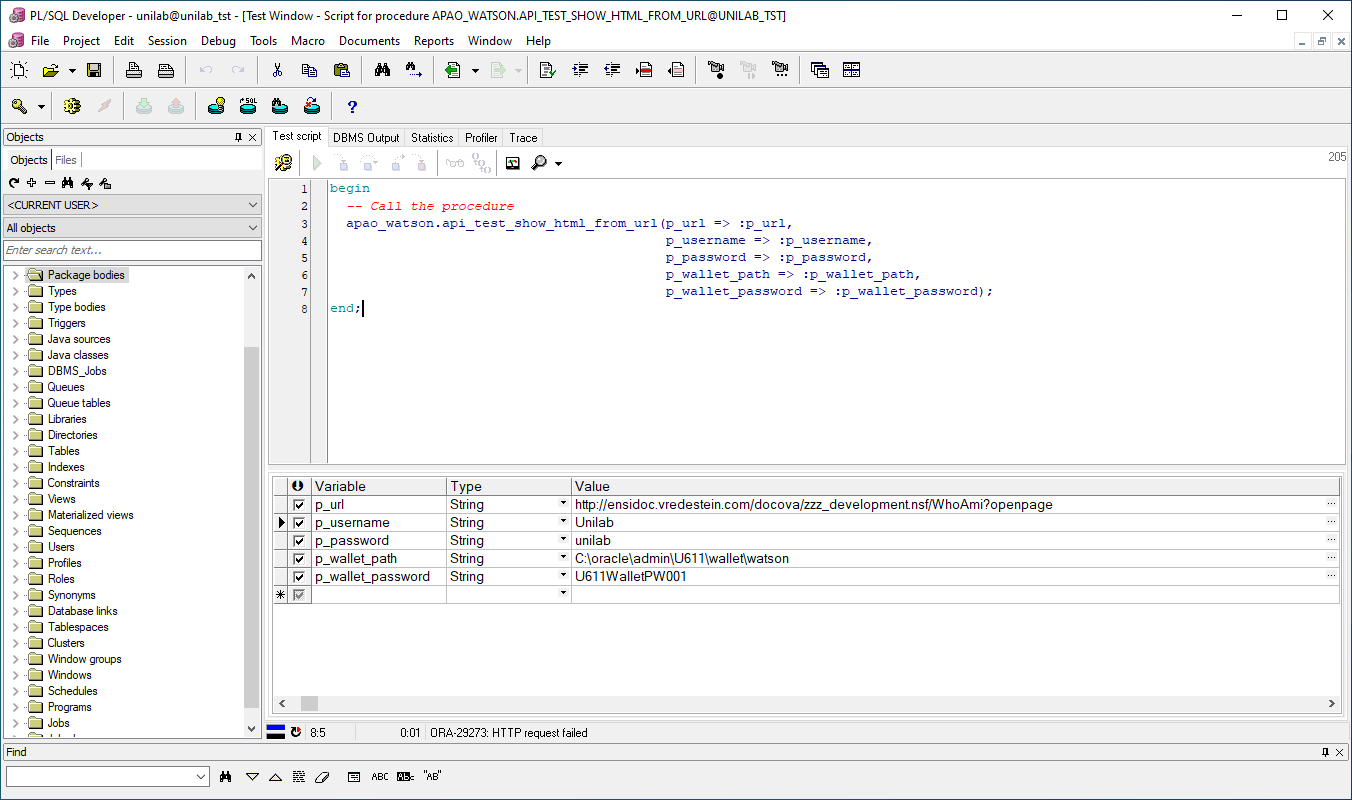
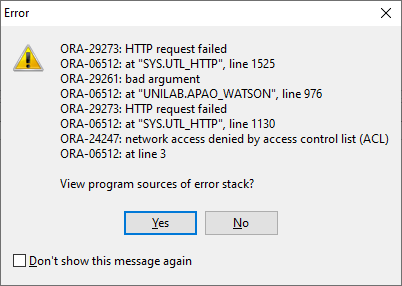
Situatie:

Oracle-wallet aangemaakt, en van apollo-certificaten voorzien.



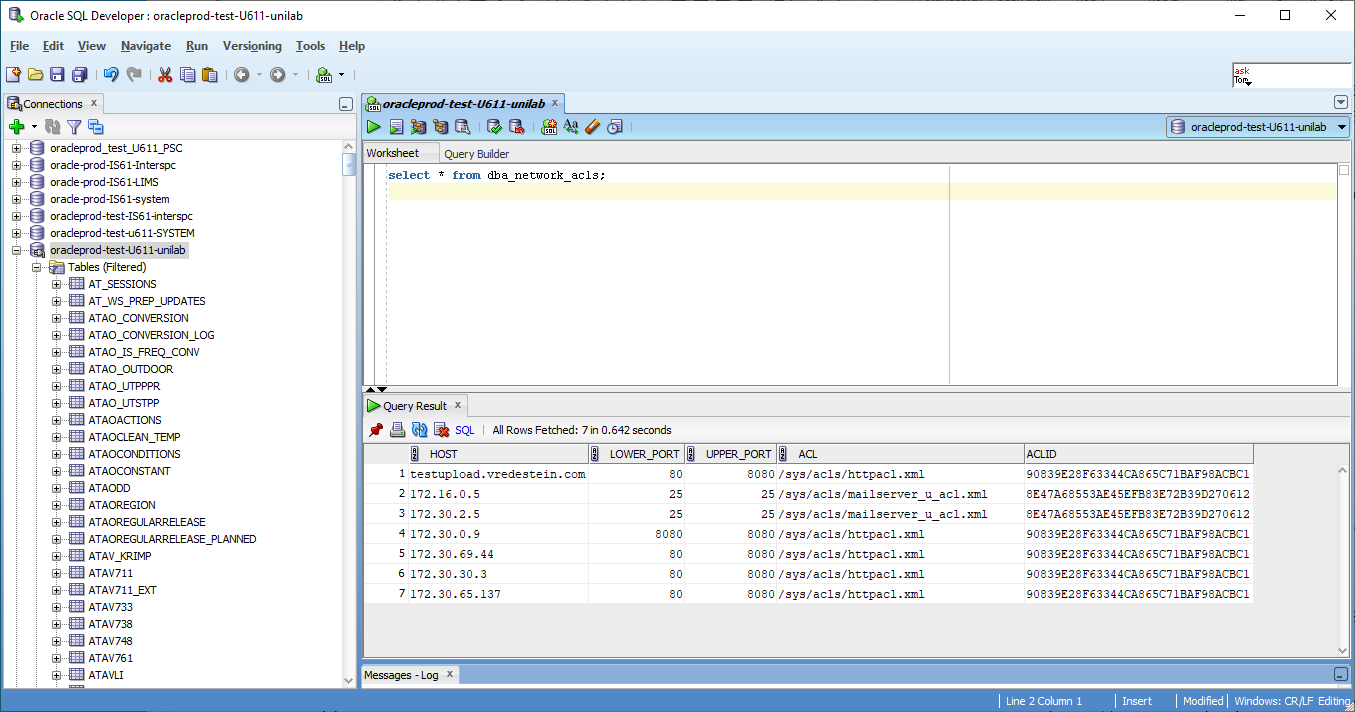
run

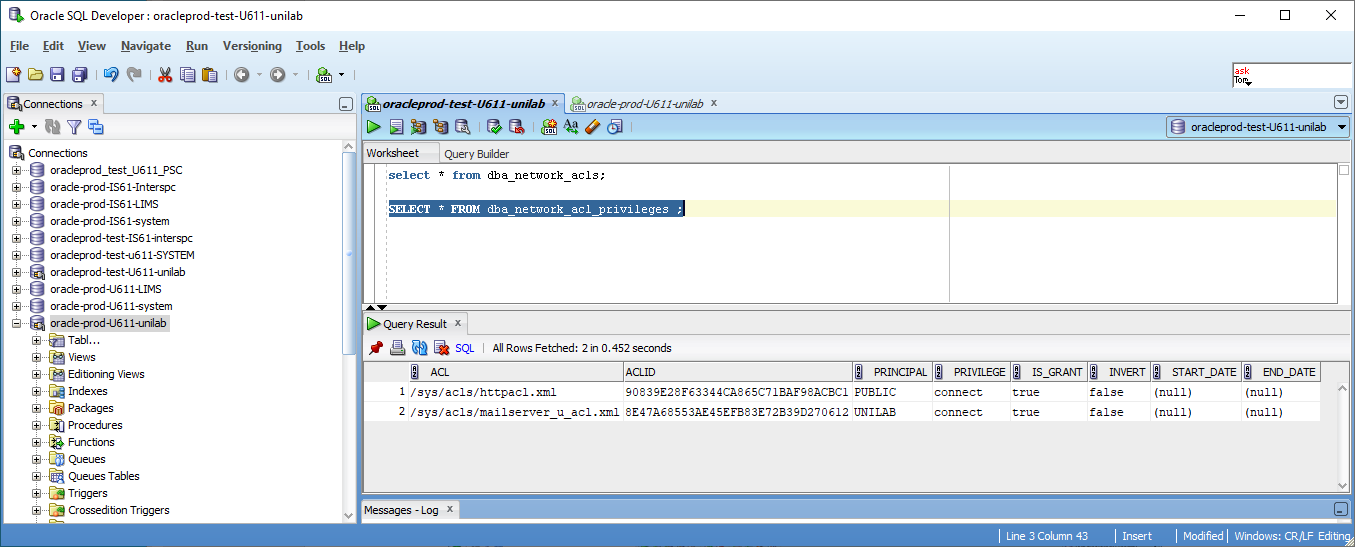


Ora-24247 network access denied by access control list (ACL)

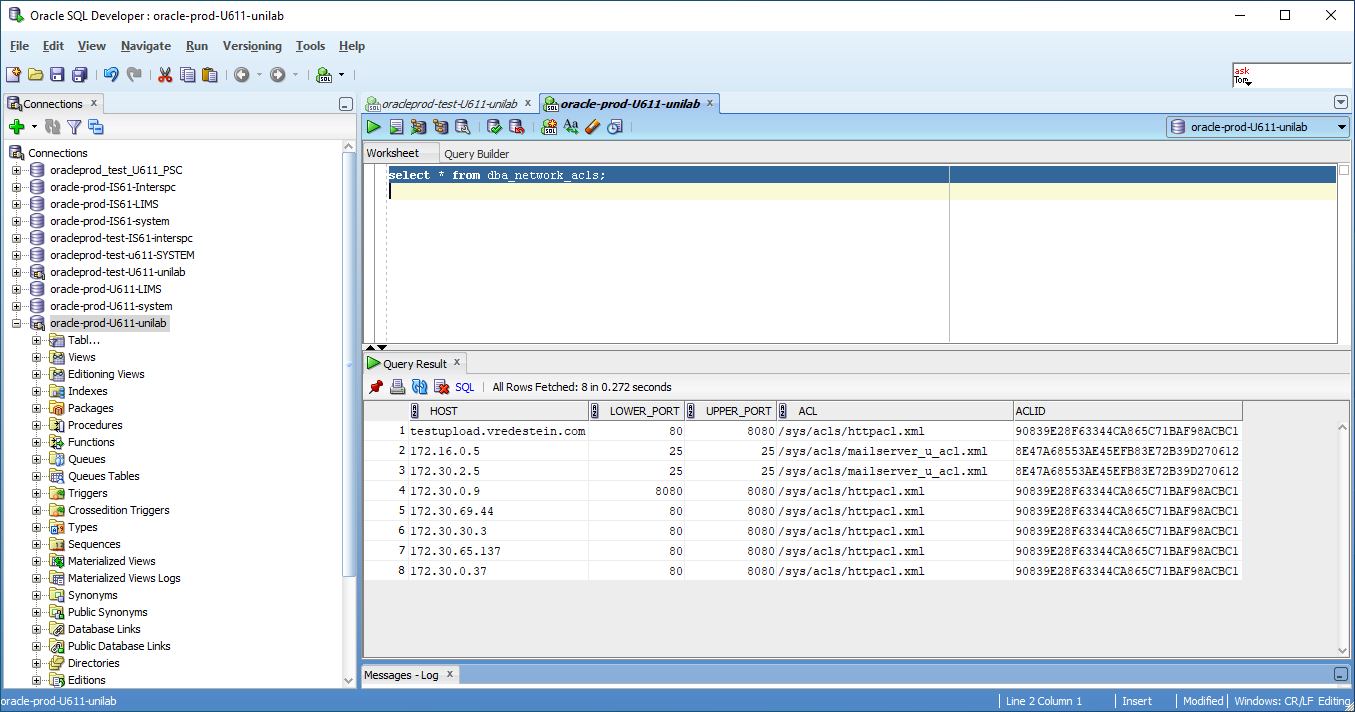
ACL

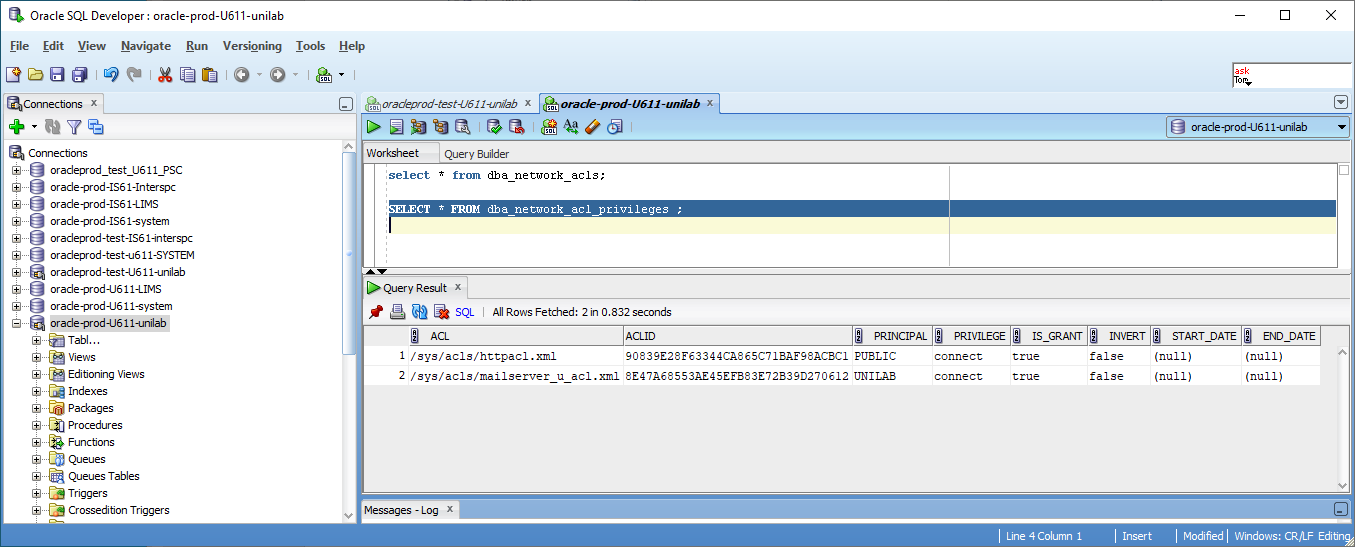
ORACLEPROD\_TEST  
select \* from db\_network\_acls;

 /sys/acls/httpacl.xml  
SELECT \* FROM dba\_network\_acl\_privileges where principal='Unilab';



ORACLEPROD  
select \* from db\_network\_acls;

 Acl = /sys/acls/httpacl.xml  
SELECT \* FROM dba\_network\_acl\_privileges where principal='Unilab';



This new feature gave the DBA a better control on which user can connect to which computer

In order to solve ORA-24247 you will need to:

1) **Create an acl**(if it is not already created)

2) **Add privileges**to the user using the network resources

3) **Assign the acl**to a specific address

**1)** run the following query to check if an ACL exists

SELECT \*

FROM dba\_network\_acls;

If the computer you are trying to connect to is not listed under host, you will need to **create an acl**:

begin

dbms\_network\_acl\_admin.create\_acl (

acl => 'http\_permissions.xml', -- or any other name

description => 'HTTP Access',

principal => 'SCOTT', -- the user name trying to access the network resource

is\_grant => TRUE,

privilege => 'connect',

start\_date => null,

end\_date => null

);

end;

/

commit;

This will create the acl and grant SCOTT the connect privilege.

**2)** IF the acl exists run the following query to verify the user is granted with the appropriate privilege

SELECT \*

FROM dba\_network\_acl\_privileges

where principal='SCOTT';

In order to use UTL\_TCP, UTL\_HTTP, UTL\_SMTP, and UTL\_MAIL the user will need the **connect** privilege

begin

DBMS\_NETWORK\_ACL\_ADMIN.**ADD\_PRIVILEGE**(acl => 'http\_permissions.xml',

principal => 'SCOTT',

is\_grant => true,

privilege => 'connect');

end;

/

commit;

If you need to resolve a host name from a host IP you will need the **resolve** grant as well.

begin

DBMS\_NETWORK\_ACL\_ADMIN.**ADD\_PRIVILEGE**(acl => 'http\_permissions.xml',

principal => 'SCOTT',

is\_grant => true,

privilege => 'resolve');

end;

/

commit;

**3)**The final step is to **assign the acl** to a specific target

BEGIN

dbms\_network\_acl\_admin.**assign\_acl** (

acl => 'http\_permissions.xml',

host => 'NETWORK ADDRESS',

lower\_port => 80,

upper\_port => 80 );

END;

NETWORK-ADDRESS: can be computer name or IP , wildcards are accepted as well for example - '\*.us.oracle.com'\*

**It is important to note that only one ACL can be assigned to any host computer. If you assign a new acl to a target the old acl gets unassigned.**

However, the old acl is not dropped. So, this could cause confusion because even if the acl was already assigned, it is possible that a new assignment overrode it.

This entry was posted in [Uncategorized](https://dbtricks.com/?cat=1) and tagged [ACL](https://dbtricks.com/?tag=acl), [ORA-24247 . Oracle 11](https://dbtricks.com/?tag=ora-24247-oracle-11), [Oracle](https://dbtricks.com/?tag=oracle) on [August 22, 2012](https://dbtricks.com/?p=159).

Test-Run op ZZZ

========== TEST MODE!!! ==========

Library: ZZZ\_Development.nsf

http://Unilab:unilab@ensidoc.vredestein.com/docova/ZZZ\_Development.nsf/UnilabDocumentAgent?OpenAgent&Action=LIST&Link=

Start doc

Methods count 1

End doc

V-DOC-COUNT: 1

==============================================

Unid: 9E356A65B73DD48DC125869200573155

Attachments:

- Method not found

Tweede test, met een methode die wel bestaat op TEST

Library: ZZZ\_Development.nsf

http://Unilab:unilab@ensidoc.vredestein.com/docova/ZZZ\_Development.nsf/UnilabDocumentAgent?OpenAgent&Action=LIST&Link=

Start doc

Methods count 1

One file found

Dit is een test van Patrick\_ENSI-BYWLLC5055.docx

http://Unilab:unilab@ensidoc.vredestein.com/docova/ZZZ\_Development.nsf/0/EF92B1E17B1C2480C125869200583E10/$file/Dit%20is%20een%20test%20van%20Patrick%5fENSI-BYWLLC5055.docx?OpenElement

End doc

==============================================

Unid: EF92B1E17B1C2480C125869200583E10

Attachments: \_+b�秵�-���j��rD5"\_��,.t睡

Save blob: 0

Select method TT205AVX

Copy method: 0

Save method 0 -

http://Unilab:unilab@ensidoc.vredestein.com/docova/ZZZ\_Development.nsf/UnilabDocumentAgent?OpenAgent&Action=UPDATE&Unid=EF92B1E17B1C2480C125869200583E10&Version=TT205AVX+-+2.00&Response=File%20successful%20downloaded&Link=2103081822114336%23BLB

<?xml version="1.0" encoding="UTF-8"?>

<Document>OK</Document>

Result OK

Dit is een test van Patrick\_ENSI-BYWLLC5055.docx - File successful downloaded

|  |
| --- |
| **ORA-24247: network access denied by access control list (ACL) tips**  *Oracle Error Tips by Donald Burleson* |

**Question:**I am having an issue in Apex 3.1;  My application is set up to generate an email whenever the Assigned\_To field is changed.  
  
This is working fine and it is reflected in APEX ADMIN mail queue.   When I press "Send all Mail" in ADMIN I get the message "Mail sent Successfully" at the top of the screen BUT ORA-24247: network access denied by access control list (ACL) appears next to the email and it is never sent.  
  
I have tried to grant network privileges based on the APEX installation manual but the PL/SQL coding generates an error message.

**Answer:**Also note these details on [building an ACL list.](http://www.dba-oracle.com/t_11g_new_acls_plsql.htm)

select \* from dba\_network\_acls;

The Oracle docs note the following about ORA-24247:

**ORA-24247**: network access denied by access control list (ACL).

**Cause:**No access control list (ACL) has been assigned to the target host or the privilege necessary to access the target host has not been granted to the user in the access control list.

**Action:** Ensure that an access control list (ACL) has been assigned to the target host and the privilege necessary to access the target host has been granted to the user.

Your application will encounter an ORA-24247 error if it relies on one of the network packages and no proper ACL has been created. For the use of the following packages it is mandatory to have an ACL for the application user in place in 11g:

UTL\_TCP  
UTL\_SMTP  
UTL\_MAIL  
UTL\_HTTP  
UTL\_INADDR

Oracle Network gives an example of ORA-24247 when using various security measures.

In this example, you are specifying that "the user SCOTT can call only the host www.proligence.com and only for the ports 22 through 55, and not outside it." Now, let's try it:

SQL> grant execute on utl\_http to scott  
  2  /  
Grant succeeded.  
   
SQL> conn scott/tiger  
Connected.  
  
SQL> select utl\_http.request('http://www.pro.com') from dual;  
select utl\_http.request('http://www.pro.com') from dual  
\*  
ERROR at line 1:  
ORA-29273: HTTP request failed  
ORA-06512: at "SYS.UTL\_HTTP", line 1577  
ORA-24247: network access denied by access control list (ACL)  
ORA-06512: at line 1

Note the error "ORA-24247: network access denied by access control list (ACL)." The user called the http server on port 80, which is outside the allowed range 22-55. Therefore the action was prevented.

***Oracle 11g New Features Tips***

ACLs are stored in XML DB.  
XML DB must be installed for the use of ACLs !

The creation of ACLs is a two step procedure.

**The first step** is to create the actual ACL and define the privileges for it:

The general syntax is as follows:

BEGIN  
DBMS\_NETWORK\_ACL\_ADMIN.CREATE\_ACL (  
acl => "file\_name.xml",  
description => "file description",  
principal => "user\_or\_role",  
is\_grant => TRUE|FALSE,  
privilege => "connect|resolve",  
start\_date => null|timestamp\_with\_time\_zone,  
end\_date => null|timestamp\_with\_time\_zone);  
END;

The value ***connect*** for the parameter ***privilege***includes***res*olve!** This is necessary for the package UTL\_INTADDR.  
The parameter ***principal*** specifies the first username granted the ACL and is **case sensitive**!  
If you want to grant multiple users you must use the ***DBMS\_NETWORK\_ACL.ADD\_PRIVILEGE*** procedure to add users.  
Here is an example for an ACL:

BEGIN  
 DBMS\_NETWORK\_ACL\_ADMIN.CREATE\_ACL (  
  acl => 'sysdba-ch-permissions.xml',  
  description => "Permissions for sysdba network',  
  principal => "LUTZ',  
  is\_grant => TRUE,  
  privilege => 'connect');  
END;

This creates an xml file which holds a list of users and privileges. This container is located under /sys/acl/ in the XML DB.

**The second step** is to assign network hosts to the ACL.

After the creation of the ACL you can add hosts to it: Below again you find the general syntax:

BEGIN  
DBMS\_NETWORK\_ACL\_ADMIN.ASSIGN\_ACL (  
acl => "file\_name.xml",  
host => "network\_host",  
lower\_port => null|port\_number,  
upper\_port => null|port\_number);  
END;

And here is an example:

BEGIN  
 DBMS\_NETWORK\_ACL\_ADMIN.ASSIGN\_ACL (  
  acl => 'sysdba-ch-permissions.xml',  
  **host => "\*.sysdba.ch'**,  
  lower\_port => 80,  
  upper\_port => null);  
END;

It is possible to use **wildcards** in the ***hosts parameter***. This allows access to all hosts in the domain.  
**Hostnames are case sensitive**You can use an IP address as well as  a DNS hostname  
Only one ACL can be assigned to a host or domain or IP subnet or port range            (if specified)!  
You can assign multiple hosts to the same ACL by calling *DBMS\_NETWORK\_ACL\_ADMIN.ASSIGN\_ACL* multiple times

Oracle evaluated ACLs in the following sequence:

1. ***fully qualified hostnames*** are evaluated
2. ***hostnames*** with ports
3. ***partial domain names*** and ***sub-domains***

% ***Do not modify the xml files with a text editor!***

The data dictionary views related to ACLs are ***dba\_network\_acls*** and ***dba\_"user\_network\_acl\_privileges***:

LUTZ AS SYSDBA @ orcl SQL> DESC dba\_network\_acls

 Name                         Null"    Type  
 ---------------------------- -------- ------------------------------------  
 HOST                         NOT NULL VARCHAR2(1000)  
 LOWER\_PORT                            NUMBER(5)  
 UPPER\_PORT                            NUMBER(5)  
 ACL                                   VARCHAR2(4000)  
 ACLID                        NOT NULL RAW(16)

LUTZ AS SYSDBA @ orcl SQL> DESC dba\_network\_acl\_privileges

 Name                        Null"    Type  
 ------------------------------------ ----------------------------------------  
 ACL                                   VARCHAR2(4000)  
 ACLID                                 RAW(16)  
 PRINCIPAL                             VARCHAR2(4000)  
 PRIVILEGE                             VARCHAR2(7)  
 IS\_GRANT                              VARCHAR2(5)  
 INVERT                                VARCHAR2(5)  
 START\_DATE                            TIMESTAMP(9) WITH TIME ZONE  
 END\_DATE                              TIMESTAMP(9) WITH TIME ZONE

**How to create and manage ACLs with OEM**

The friends of graphical interfaces can also create and manage ACLs. There is an interface to the XML DB integrated into the Enterprise Manager. Access Control Lists are an XML DB functionality.  
You find the link for the ACLs in the SCHEMA pane in Database Control 11g:

**Other Network Security Features**

The listener is secured by default in 11g.  
It is not possible to manage the listener from remote any more without a password or ***Class of Secure Transports*** (***COST***).  
Only the local user who started the listener can stop it in 11g.  
Still we have a default listener with the name LISTENER and port 1521!     
In  11g and beyond, Oracle has introduced the ability to restrict connections to specific hosts (or IP addresses).   
The access control lists (ACL) are used to restrict the hosts that are allowed to connect to the Oracle database.    
ACL"s are created using the ***dbms\_network\_acl\_admin*** and ***dbms\_network\_acl\_utility*** packages.  Either package can be used to create and manage ACLs.     
Here is an example for an ACL:

 BEGIN  **DBMS\_NETWORK\_ACL\_ADMIN**.CREATE\_ACL (  
acl => 'sysdba-ch-permissions.xml',  
description => "Permissions for sysdba network',    
principal => "LUTZ',    
is\_grant => TRUE,    
privilege => 'connect');  
END;

The ACL is then added to the "http://host:port/sys/acls/" directory.

Please note that you will encounter an [ORA-24247](http://www.dba-oracle.com/t_ora_24247_network_access_denied_by_access_control_list_tips.htm) error if it relies on one of the network packages and no proper ACL has been created.