Access Control List (ACL)

- In order to access External Network Services such as Mail Servers, SMTP Servers, Web Services, REST APIs, Oracle provides APIs such as **UTL_MAIL**, **UTL_SMTP**, **UTL_HTTP** and APEX provides **APEX_MAIL**, **APEX_WEB_SERVICE** etc. APIs

- Now, to access the aforementioned services, Oracle provides Access Control Layer (ACL) in XML DB to determine which resources can be accessed and who (which user) can access the resources.

- Oracle provides DBMS_NETWORK_ACL_ADMIN and DBMS_NETWORK_ACL_UTILITY for different purposes of ACL.

- In order to provide access to a network resources, following steps are performed:

    1. Create an ACL
    2. Add privilege to the ACL
    3. Assign the ACL to a network
    4. Verify ACL details and privileges
    5. Test the ACL

- In an ACL, a privilege can be deleted and ACL can be dropped too.

- In Order to verify ACL details and privileges, following database views are used:

    - USER_NETWORK_ACLS or DBA_NETWORK_ACLS
    - USER_NETWORK_ACL_PRIVILEGES or DBA_NETWORK_ACL_PRIVILEGES

Access Control List (ACL)

1. Create an ACL

```
BEGIN
  DBMS_NETWORK_ACL_ADMIN.CREATE_ACL (
    acl => 'adbuser.xml',
    description => 'Permissions to access web
service',
    principal => 'ADB_USER',
    is_grant => TRUE,
    privilege => 'connect',
    start_date => SYSTIMESTAMP,
    end_date => NULL
  );
  COMMIT;
END;
/
```

- ***acl*** name of the acl xml file. Generated relative to “/sys/acls” directory in the XML DB.
- ***description*** of the ACL
- ***principal*** the user who wants to access the external network resources. This name is case sensitive.
- ***is_grant*** TRUE to grant privilege and FALSE to deny
- ***privilege*** e.g. ‘connect’ for UTL_HTTP, UTL_MAIL etc. and ‘resolve’ for UTL_INADDR/ IP address resolution. Only the values mentioned above can be used
- ***start_date*** A valid date and since that date the ACL will be active. Default is NULL.
- ***end_date*** A valid date, until that date the ACL will be active and since that date, the ACL will be inactive. Default is NULL.

Access Control List (ACL)

2. Add privilege to the ACL

```
BEGIN
  DBMS_NETWORK_acl_ADMIN.ADD_PRIVILEGE(
    acl => 'adbuser.xml',
    principal => 'ADB_USER',
    is_grant => true,
    privilege => 'resolve',
    start_date => NULL,
    end_date => NULL
  );
 COMMIT;
END;
/
```

- ***acl*** name of the acl xml file. Generated relative to “/sys/acls” directory in the XML DB.
- ***principal*** the user who wants to access the external network resources. This name is case sensitive.
- ***is_grant*** TRUE to grant privilege and FALSE to deny
- ***privilege*** e.g. ‘connect’ for UTL_HTTP, UTL_MAIL etc. and ‘resolve’ for UTL_INADDR/ IP address resolution. Only the values mentioned above can be used
- ***start_date*** A valid date and since that date the ACL will be active. Default is NULL.
- ***end_date*** A valid date, until that date the ACL will be active and since that date, the ACL will be inactive. Default is NULL.

Access Control List (ACL)

3. Assign the ACL to a Network

```
BEGIN
  DBMS_NETWORK_ACL_ADMIN.ASSIGN_ACL (
    acl => 'adbuser.xml',
    host => '*',
    lower_port  => NULL,
    upper_port  => NULL
  );
COMMIT;
END;
/
```

- ***acl*** name of the acl xml file. Generated relative to “/sys/acls” directory in the XML DB.
- ***host*** a valid IP address. * represents all or Open ACL, OPEN ACL is not recommended.
- ***lower_port*** for the concerned IP Host.
- ***upper_port*** for the concerned IP Host.

4. Verify ACL Details and Privileges

```
SELECT acl , host , lower_port , upper_port FROM DBA_NETWORK_ACLS;

SELECT acl , principal , privilege , is_grant FROM DBA_NETWORK_ACL_PRIVILEGES;

SELECT * FROM   TABLE(DBMS_NETWORK_ACL_UTILITY.domains('10.10.9.9'));

SELECT DBMS_NETWORK_ACL_UTILITY.domain_levl('10.10.9.9') FROM dual;
```

Access Control List (ACL)

5. Test the ACL

a) Grant execute privilege on UTL_HTTP to “adb_user”, the principal using sys / admin user which has DBA privilege.

```
GRANT EXECUTE ON UTL_HTTP TO adb_user;
```

b) Execute the anonymous block as shown below.

```
DECLARE
  l_url            VARCHAR2(50) := 'http://10.10.9.9';
  l_http_request   UTL_HTTP.req;
  l_http_response  UTL_HTTP.resp;
BEGIN
  -- Make a HTTP request and get the response.
  l_http_request  := UTL_HTTP.begin_request(l_url);
  l_http_response := UTL_HTTP.get_response(l_http_request);
  UTL_HTTP.end_response(l_http_response);
END;
/
```

c) When the above PLSQL block is executed, it should complete successfully and you **shouldn’t receive the error** mentioned below.

```
ORA-29273: HTTP request failed
ORA-06512: at "SYS.UTL_HTTP", line 1029
ORA-24247: network access denied by access control list (ACL)
ORA-06512: at line 7
```

Access Control List (ACL)

Delete Privilege from an ACL

```
BEGIN
  DBMS_NETWORK_acl_ADMIN.ADD_PRIVILEGE(
    acl => 'adbuser.xml',
    principal => 'ADB_USER',
    is_grant => true,
    privilege => 'resolve'
);
 COMMIT;
END;
/
```

Unassign ACL

```
BEGIN
  DBMS_NETWORK_ACL_ADMIN.unassign_acl (
    acl         => 'adbuser.xml',
    host        => '192.168.2.3',
    lower_port  => 80,
    upper_port  => NULL);

  COMMIT;
END;
/
```

Drop ACL

```
BEGIN

  DBMS_NETWORK_ACL_ADMIN.drop_acl (

    acl => 'adbuser.xml'

  );

  COMMIT;

END;

/
```

SHARPENSKILL.COM