

Tipps & Tricks: Neuerungen im Package DBMS_NETWORK_ACL_ADMIN in Oracle 12c

| | | | |
|---------------|--------|-----------------------|------------|
| Bereich: | PL/SQL | Erstellung: | 07/2013 MP |
| Versionsinfo: | 12.1 | Letzte Überarbeitung: | 07/2013 MP |

Neuerungen im Package DBMS_NETWORK_ACL_ADMIN

Als wir von der Oracle Version 10.2 auf die Version 11.1 migriert haben, waren einige Netzwerkverbindungen/Programme nicht mehr funktionstüchtig.

Erst eine Recherche ergab, dass ein neues Package hier eine "Firewall" um die Datenbank zieht, die zuerst konfiguriert werden muss.

Damit Ihnen das bei der Migration auf Oracle 12c nicht genauso ergeht, hier die wichtigsten Neuerungen/Umstellungen in diesem Bereich:

Bisher wurden ACLs für die Freigabe der Benutzung von fremden Servern/Ports verwendet. Neue Packageaufrufe des Packages DBMS_NETWORK_ACL_ADMIN vereinfachen diese Aufgabe nun.

Wenn Sie eine Applikation besitzen, die auf fremde Webseiten/Webserver zugreift, muss dafür eine ACL gesetzt sein.

Beispiel (als Benutzer SCOTT ausführen):

```
SELECT httpuritype( 'www.munisoft.de' ).getclob()
FROM dual;
```

Übliche Fehlermeldung, wenn ACLs nicht gesetzt sind:

```
ORA-29273: HTTP-Anforderung nicht erfolgreich
ORA-06512: in "SYS.UTL_HTTP", Zeile 1817
ORA-24247: Netzwerkzugriff von Access Control-Liste (ACL) abgelehnt
ORA-06512: in "SYS.HTTPURITYPE", Zeile 41
```

Neue Prozeduren im Package DBMS_NETWORK_ACL_ADMIN

- **APPEND_HOST_ACE**: Neuen Host zur Freigabeliste hinzufügen
- **APPEND_WALLET_ACE**: Walletbenutzung freigeben
- **REMOVE_HOST_ACE**: Host von Freigabeliste entfernen
- **REMOVE_WALLET_ACE**: Freigabe für Walletbenutzung zurücknehmen
- **SET_HOST_ACL**: Neue Portfreigabe für Host und Ports definieren. Sollten vom Benutzer nicht manuell gesetzt werden
- **SET_WALLET_ACL**: Einsetzen der ACL für ein Wallet. Sollten vom Benutzer nicht manuell gesetzt werden

Damit unser SELECT im Beispiel oben funktioniert, definieren wir einen ACE (Access Control Entry):

```
BEGIN
```

```

DBMS_NETWORK_ACL_ADMIN.APPEND_HOST_ACE (
  host      => 'www.muniqsoft.de',
  lower_port => 80, -- Portnummer des Rechners
  ace       => xs$ace_type(
                privilege_list => xs$name_list('http'),
                principal_name => 'SCOTT'
                principal_type => xs_acl.ptype_db) );

END;
/

```

Zur Erklärung:

Privilege List kann sein:

- 'smtp' -- Zugriff nur via UTL_SMTP und UTL_MAIL
- 'http' -- Zugriff via UTL_HTTP Package und HttpUriType
- 'http_proxy' -- Zugriff via UTL_HTTP Package und HttpUriType wenn über einen Proxy kommuniziert wird
- 'connect' -- Zugriff via UTL_TCP, UTL_SMTP, UTL_MAIL, UTL_HTTP, und DBMS_LDAP Packages, der dem Typ HttpUriType

Principal Name kann sein:

- Ein Datenbankbenutzer (z. B. SCOTT)
- Eine Rolle (z. B. MY_APP_ROLE)

Principal Type kann sein:

- XS_ACL.PTYPE_DB für Datenbankbenutzer/Rolle.
- XS_ACL.PTYPE_XS Für Real Application Security Benutzer

Ein weiterer Test als Benutzer SCOTT ergibt:

```

SELECT httpuritype('www.muniqsoft.de').getclob()
FROM dual;

```

```

...<title>Muniqsoft - Home</title>
  <meta name="generator" content="TYPO3 4.2 CMS" />
  <meta name="keywords" content="Oracle Beratung München, Oracle Schulung, Oracle
Schulungen, Oracle Seminare, Training, Consulting, RAC, Real Application Clusters,
Hochverfügbarkeit, Security, Remote Administration, Remote DBA, Support, Inhouse
Kurse, Seminare, Softwareentwicklung, Lizenzen, Workshops, SQL, PLSQL, PL/SQL, Visual
Basic, .NET, Access, APEX, OraDB.SchemaDoc, SchemaDoc, OraDB.Scripts, Script, Skript,
Monitoring, Migration, Security, Schulungsunterlagen, München" />...

```

Wenn Sie dem Benutzer das Recht wieder entziehen möchten, weiterhin auf die Webseite zuzugreifen:

```

BEGIN
  DBMS_NETWORK_ACL_ADMIN.REMOVE_HOST_ACE (
    host      => 'www.muniqsoft.de',
    lower_port => 80,
    upper_port => null,

```

```
ace      => xs$ace_type(  
    privilege_list => xs$name_list('http'),  
    principal_name => 'SCOTT'  
    principal_type => xs_acl.ptype_db));  
remove_empty_acl => TRUE);  
END;  
/
```

Zum Überprüfen gibt es natürlich auch wieder entsprechende Views:

```
SELECT acl_owner, host, lower_port, upper_port  
FROM DBA_HOST_ACLS;
```

oder

```
SELECT * FROM DBA_HOST_ACES;
```

Folgende neue Views stehen zur Verfügung:

- DBA_HOST_ACLS
- USER_HOST_ACES
- DBA_HOST_ACES