138
DBMS_NETWORK_ACL_UTILITY

The DBMS_NETWORK_ACL_UTILITY package provides the utility functions to facilitate the evaluation of access control list (ACL) assignments governing TCP connections to network hosts.

> **See Also:**
>
> For more information, see ""Managing Fine-grained Access to External Network Services"" in *Oracle Database Security Guide*

The chapter contains the following topics:

- Security Model
- Examples
- Summary of DBMS_NETWORK_ACL_UTILITY Subprograms

DBMS_NETWORK_ACL_UTILITY Security Model

EXECUTE on the DBMS_NETWORK_ACL_UTILITY package is granted to PUBLIC.

DBMS_NETWORK_ACL_UTILITY Examples

The CONTAINS_HOST Function in this package indicates if a domain or subnet contains a given host or IP address.

It can be used in conjunction with the CHECK_PRIVILEGE_ACLID Function in the DBMS_NETWORK_ACL_ADMIN package to determine the privilege assignments affecting a user's permission to access a network host. The return value of the CONTAINS_HOST Function in can also be used to order the ACL assignments by their precedence.

Example 1

For example, for SCOTT's permission to connect to www.hr.example.com:

```
 SELECT host, lower_port, upper_port, acl,
    DECODE(
        DBMS_NETWORK_ACL_ADMIN.CHECK_PRIVILEGE_ACLID(aclid, 'SCOTT', 'connect'),
           1, 'GRANTED', 0, 'DENIED', NULL) privilege
    FROM (SELECT host, acl, aclid, lower_port, upper_port,
              DBMS_NETWORK_ACL_UTILITY.CONTAINS_HOST('www.hr.example.com', host)
                precedence
         FROM dba_network_acls)
WHERE precedence > 0
ORDER BY precedence DESC, lower_port nulls LAST;
```

```
  HOST                   LOWER_PORT UPPER_PORT  ACL                  PRIVILEGE
```

```
   -------------------- ---------- ---------- -------------------- ---------
   www.hr.example.com           80         80 /sys/acls/www.xml    GRANTED
   www.hr.example.com         3000       3999 /sys/acls/www.xml    GRANTED
   www.hr.example.com                         /sys/acls/www.xml    GRANTED
   *.hr.example.com                           /sys/acls/all.xml
   *.example.com                              /sys/acls/all.xml
```

Example 2

For example, for `SCOTT`'s permission to do domain name resolution for www.hr.example.com:

```
SELECT host, acl,
  DECODE(
    DBMS_NETWORK_ACL_ADMIN.CHECK_PRIVILEGE_ACLID(aclid, 'SCOTT', 'resolve'),
      1, 'GRANTED', 0, 'DENIED', null) privilege
  FROM (SELECT host, acl, aclid,
               DBMS_NETWORK_ACL_UTILITY.CONTAINS_HOST('www.hr.example.com', host)
                 precedence
          FROM dba_network_acls
         WHERE lower_port IS NULL AND upper_port IS NULL)
 WHERE precedence > 0
 ORDER BY precedence DESC;

HOST                   ACL                          PRIVILEGE
---------------------- ---------------------------- ---------
www.hr.example.com     /sys/acls/hr-www.xml         GRANTED
*.hr.example.com       /sys/acls/hr-domain.xml
*.example.com          /sys/acls/corp-domain.xml
```

Note that the "resolve" privilege takes effect only in ACLs assigned without any port range (when `lower_port` and `upper_port` are `NULL`). For this reason, the example does not include `lower_port` and `upper_port` columns in the query.

Related Topics

- CONTAINS_HOST Function
  This function determines if the given host is equal to or contained in the given host, domain, or subnet. It handles different representation of the same IP address or subnet. For example, an IPv4-mapped IPv6 address is considered equal to the IPv4-native address it represents. It does not perform domain name resolution when evaluating the host or domain.

Summary of DBMS_NETWORK_ACL_UTILITY Subprograms

This table lists and briefly describes the `DBMS_NETWORK_ACL_UTILITY` package subprograms.

Table 138-1   DBMS_NETWORK_ACL_UTILITY Package Subprograms

Subprogram	Description
CONTAINS_HOST Function	Determines if the given host is equal to or contained in the given host, domain, or subnet
DOMAIN_LEVEL Function	Returns the domain level of the given host name, domain, or subnet
DOMAINS Function	For a given host, this function returns the domains whose ACL assigned is used to determine if a user has the privilege to access the given host or not.

Table 138-1 (Cont.) DBMS_NETWORK_ACL_UTILITY Package Subprograms

Subprogram	Description
EQUALS_HOST Function	Determines if the two given hosts, domains, or subnets are equal

CONTAINS_HOST Function

This function determines if the given host is equal to or contained in the given host, domain, or subnet. It handles different representation of the same IP address or subnet. For example, an IPv4-mapped IPv6 address is considered equal to the IPv4-native address it represents. It does not perform domain name resolution when evaluating the host or domain.

Syntax

```
DBMS_NETWORK_ACL_UTILITY.CONTAINS_HOST (
   host       IN    VARCHAR2,
   domain     IN    VARCHAR2)
 RETURN NUMBER;
```

Parameters

Table 138-2 CONTAINS_HOST Function Parameters

Parameter	Description
`host`	Network host
`domain`	Network host, domain, or subnet

Return Values

Returns a non-`NULL` value if the given host is equal to or contained in the related host, domain, or subnet:

- If `domain` is a hostname, returns the level of its domain + 1
- If `domain` is a domain name, returns the domain level
- If `domain` is an IP address or subnet, return the number of significant address bits of the IP address or subnet
- If domain is the wildcard "*", returns 0

The non-`NULL` value returned indicates the precedence of the domain or subnet for ACL assignment. The higher the value, the higher is the precedence. `NULL` will be returned if the host is not equal to or contained in the given host, domain or subnet.

Examples

```
SELECT host, acl, precedence
  FROM (select host, acl,
               DBMS_NETWORK_ACL_UTILITY.CONTAINS_HOST('192.0.2.3', host)
                 precedence
          FROM dba_network_acls)
 WHERE precedence > 0
 ORDER BY precedence DESC;
```

```
HOST                   ACL                        PRECEDENCE
---------------------- -------------------------- ----------
192.0.2.3              /sys/acls/hr-www.xml               32
::ffff:192.0.2.0/120   /sys/acls/hr-domain.xml            24
::ffff:192.0.0.0/104   /sys/acls/corp-domain.xml           8
```

DOMAIN_LEVEL Function

This function returns the domain level of the given host name, domain, or subnet.

Syntax

```
DBMS_NETWORK_ACL_UTILITY.DOMAIN_LEVEL (
    host   IN VARCHAR2)
  RETURN NUMBER;
```

Parameters

Table 138-3   DOMAIN_LEVEL Function Parameters

Parameter	Description
host	Network host, domain, or subnet

Return Values

The domain level of the given host, domain, or subnet.

Usage Notes

Note that this function cannot handle IPv6 addresses and subnets, and subnets in CIDR notation.

Examples

```
SELECT host, acl, domain_level
  FROM (select host, acl,
               DBMS_NETWORK_ACL_UTILITY.DOMAIN_LEVEL(host) domain_level
          FROM dba_network_acls)
 order by domain_level desc;

HOST                   ACL                          DOMAIN_LEVEL
---------------------- ---------------------------- ------------
www.hr.example.com     /sys/acls/hr-www.xml                    4
*.hr.example.com       /sys/acls/hr-domain.xml                 3
*.example.com          /sys/acls/corp-domain.xml               2
```

DOMAINS Function

For a given host, this function returns the domains whose ACL assigned determines if a user has the privilege to access the given host or not. When the IP address of the host is given, return the subnets instead.

Syntax

```
DBMS_NETWORK_ACL_UTILITY.DOMAINS (
    host   IN VARCHAR2)
  RETURN DOMAIN_TABLE PIPELINED;
```

Parameters

Table 138-4 DOMAINS Function Parameters

Parameter	Description
`host`	Network host

Return Values

The domains or subnets for the given host.

Usage Notes

Note that this function cannot handle IPv6 addresses. Nor can it generate subnets of arbitrary number of prefix bits for an IPv4 address.

Examples

```
select * from table(dbms_network_acl_utility.domains('www.hr.example.com'));

DOMAINS
--------------------------
www.hr.example.com
*.hr.example.com
*.example.com
*.com
*
```

EQUALS_HOST Function

This function determines if the two given hosts, domains, or subnets are equal. It handles different representation of the same IP address or subnet. For example, an IPv4-mapped IPv6 address is considered equal to the IPv4- native address it represents. It does not perform domain name resolution when comparing the two hosts or domains.

Syntax

```
DBMS_NETWORK_ACL_UTILITY.EQUALS_HOST (
   host1    IN    VARCHAR2,
   host2    IN    VARCHAR2)
 RETURN NUMBER;
```

Parameters

Table 138-5 EQUALS_HOST Function Parameters

Parameter	Description
`host1`	Network host, domain, or subnet to compare
`host2`	Network host, domain, or subnet to compare

Return Values

1 if the two hosts, domains, or subnets are equal. 0 otherwise.

Examples

```
SELECT host, acl
  FROM dba_network_acls
 WHERE DBMS_NETWORK_ACL_UTILITY.EQUALS_HOST('192.0.2.*', host) = 1;

HOST                   ACL
---------------------- ----------------------------
::ffff:192.0.2.0/120   /sys/acls/hr-domain.xml
```