179 DBMS_SFW_ACL_ADMIN

The DBMS_SFW_ACL_ADMIN package provides interfaces for administering and managing access control policies for the "database service firewall" feature. Each policy is represented by an access control list (ACL) containing hosts that are allowed access to a specific database service. Local listeners and server processes validate all inbound client connections against the ACL.

This chapter contains the following topics:

DBMS_SFW_ACL_ADMIN Security Model

This package is owned by the DBSFWUSER schema. The procedures in this package can be run only by the DBSFWUSER user.

DBMS_SFW_ACL_ADMIN Operational Notes

These operation notes apply to `DBMS_SFW_ACL_ADMIN`.

- An ACL contains entries, which are called "ace", for "access control entries".
- You add entries to an ACL using the IP_ADD_ACE Procedure and IP_ADD_PDB_ACE Procedure. After calling these procedures, you call the COMMIT_ACL Procedure to send the updated ACL to the listeners. Similarly, if you remove entries from an ACL using the IP_REMOVE_ACE Procedure, IP_REMOVE_ACL Procedure, IP_REMOVE_PDB_ACE Procedure, or IP_REMOVE_PDB_ACL Procedure, you need to call theCOMMIT_ACL Procedure to update the ACL on the listeners.
- Access control must be enabled using the new `FIREWALL` endpoint attribute and the new `LOCAL_REGISTRATION_ADDRESS_`*listenerName* parameter. The configuration can be done manually in `listener.ora` or through the Server Control Utility (SRVCTL). Refer to the *Oracle Database Net Services Reference* and the *Oracle Real Application Clusters Administration and Deployment Guide* for configuration instructions.
- You can query the `IP_ACL` table to show the committed ACLs. But to see the ACLs that have been sent to the local listeners, you have to query the `V$IP_ACL` or `GV$IP_ACL` view. The `IP_ACL` table can contain ACLs that are not in `[G]V$IP_ACL` because the database services for those ACLs were not running at the time of the commit. When the services are running, you can call the COMMIT_ACL procedure again to send the committed ACLs in the IP_ACL table to the local listeners.

  In an Oracle RAC environment, `GV$IP_ACL` can be used to query ACLs across the database cluster, and `V$IP_ACL` to query ACLs in the connected instance.

DBMS_SFW_ACL_ADMIN Examples

These three examples show how `DBMS_SFW_ACL_ADMIN` can be used to administer and manage access control policies.

The following example adds three access control entries to the ACL and commits them.

```
## Connect to DBSFWUSER
SQL> connect dbsfwuser/<password>
Connected.

## Create an ACL for database service SVC1
SQL> exec dbms_sfw_acl_admin.ip_add_ace('svc1','192.168.12.1');
PL/SQL procedure successfully completed.

SQL> exec dbms_sfw_acl_admin.ip_add_ace('svc1','192.168.12.2');
PL/SQL procedure successfully completed.

SQL> exec dbms_sfw_acl_admin.ip_add_ace('svc1','test02.example.com');
PL/SQL procedure successfully completed.

## Commit the ACLs to the DB ACL table.
## This sends the ACLs for running services to ALL local Listeners
SQL> exec dbms_sfw_acl_admin.commit_acl;
PL/SQL procedure successfully completed.
```

The following example retrieves the ACLs committed from the previous example.

```
SQL> select * from ip_acl;
SERVICE_NAME               HOST
-----------------------    -------------------
"SVC1.EXAMPLE.COM"         192.168.12.1
"SVC1.EXAMPLE.COM"         192.168.12.2
"SVC1.EXAMPLE.COM"         TEST02.EXAMPLE.COM

## View ACLs sent to the local Listeners
## NOTE: ACLs are sent ONLY to running services
SQL> select * from v$ip_acl;
SERVICE_NAME               HOST                   CON_ID
----------------------     -----------------      --------
SVC1.EXAMPLE.COM           192.168.12.1           1
SVC1.EXAMPLE.COM           192.168.12.2           1
SVC1.EXAMPLE.COM           TEST02.EXAMPLE.COM     1
```

The following example adds access control entries for pluggable database "PDB1" using various host formats.

```
SQL> exec dbms_sfw_acl_admin.ip_add_pdb_ace('pdb1','192.168.12.3');
PL/SQL procedure successfully completed.

SQL> exec dbms_sfw_acl_admin.ip_add_pdb_ace('pdb1','192.168.12.0/23');
PL/SQL procedure successfully completed.

SQL> exec dbms_sfw_acl_admin.ip_add_pdb_ace('pdb1','192.168.12.*');
PL/SQL procedure successfully completed.

SQL> exec dbms_sfw_acl_admin.commit_acl;
PL/SQL procedure successfully completed.
```

Summary of DBMS_SFW_ACL_ADMIN Subprograms

This table lists the `DBMS_SFW_ACL_ADMIN` subprograms and briefly describes them.

Table 179-1 DBMS_SFW_ACL_ADMIN Package Subprograms

Subprogram	Description
COMMIT_ACL Procedure	Commits changes to the ACL tables, and propagates the changes to the local listeners for database instances.
IP_ADD_ACE Procedure	Adds an access control entry to the ACL for a database service.
IP_ADD_PDB_ACE Procedure	Adds an access control entry to the ACL for all the database services in a pluggable database (PDB).
IP_REMOVE_ACE Procedure	Removes an entry from the ACL for a database service.
IP_REMOVE_ACL Procedure	Removes all entries from the ACL for a database service.
IP_REMOVE_PDB_ACE Procedure	Removes an access control entry from the ACL for all the database services in a pluggable database (PDB).
IP_REMOVE_PDB_ACL Procedure	Removes all entries from the ACL for all the database services in a pluggable database (PDB).

COMMIT_ACL Procedure

This procedure commits changes to the ACL tables. It also propagates the changes to the local listeners for database instances.

If you have changed access entries for database services, but the database services were not running at the time when you called the COMMIT_ACL procedure, then those changes will be committed to the ACL tables, but they will not be sent to the local listener. To send the entries to the listener, start up the database services, and call the COMMIT_ACL procedure again.

This procedure returns when the operation has completed successfully.

Syntax

```
DBMS_SFW_ACL_ADMIN.COMMIT_ACL;
```

Parameters

None

IP_ADD_ACE Procedure

This procedure adds an access control entry to the ACL for a database service.

Syntax

```
DBMS_SFW_ACL_ADMIN.IP_ADD_ACE (
  p_service_name   IN   VARCHAR2,
  p_host           IN   VARCHAR2);
```

Parameters

Table 179-2 IP_ADD_ACE Procedure Parameters

Parameter	Description
p_service_name	The name of the database service for which you want to add an access control entry.
p_host	The host of the client that is allowed access to the service. This value can be a host name, an IPv4 address, or an IPv6 address. Wildcard "*" for IPv4 and CIDR format are also allowed.

IP_ADD_PDB_ACE Procedure

This procedure adds an access control entry to the ACL for all the database services in a pluggable database (PDB).

Syntax

```
DBMS_SFW_ACL_ADMIN.IP_ADD_PDB_ACE (
  p_pdb_name   IN  VARCHAR2,
  p_host       IN  VARCHAR2);
```

Parameters

Table 179-3 IP_ADD_PDB_ACE Procedure Parameters

Parameter	Description
p_pdb_name	The name of the PDB.
p_host	The host of the client that is allowed access to the database services in the PDB. This value can be a host name, an IPv4 address, or an IPv6 address. Wildcard "*" for IPv4 and CIDR format are also allowed.

IP_REMOVE_ACE Procedure

This procedure removes an entry from the ACL for a database service.

Syntax

```
DBMS_SFW_ACL_ADMIN.IP_REMOVE_ACE (
  p_service_name   IN  VARCHAR2,
  p_host           IN  VARCHAR2);
```

Parameters

Table 179-4 IP_REMOVE_ACE Procedure Parameters

Parameter	Description
p_service_name	The name of the database service from which you want to remove an access control entry.

Table 179-4 (Cont.) IP_REMOVE_ACE Procedure Parameters

Parameter	Description
p_host	The host that you want to remove from the ACL. This value can be a host name, an IPv4 address, or an IPv6 address. Wildcard "*" for IPv4 and CIDR format are also allowed. This has to match the existing value exactly. You can query the `IP_ACL` table to get the list of entries for a database service.

IP_REMOVE_ACL Procedure

This procedure removes all entries from the ACL for a database service.

Syntax

```
DBMS_SFW_ACL_ADMIN.IP_REMOVE_ACL (
  p_service_name   IN   VARCHAR2);
```

Parameters

Table 179-5 IP_REMOVE_ACL Procedure Parameters

Parameter	Description
p_service_name	The name of the database service whose ACL you want to clear.

IP_REMOVE_PDB_ACE Procedure

This procedure removes an access control entry from the ACL for all the database services in the specified pluggable database (PDB).

Syntax

```
DBMS_SFW_ACL_ADMIN.IP_REMOVE_PDB_ACE (
  p_pdb_name   IN   VARCHAR2,
  p_host       IN   VARCHAR2);
```

Parameters

Table 179-6 IP_REMOVE_PDB_ACE Procedure Parameters

Parameter	Description
p_pdb_name	The name of the PDB.
p_host	The host that you want to remove from the ACL. This value can be a host name, an IPv4 address, or an IPv6 address. Wildcard "*" for IPv4 and CIDR format are also allowed. This has to match the existing value exactly. You can query the `IP_ACL` table to get the list of entries for a database service.

IP_REMOVE_PDB_ACL Procedure

This procedure removes all entries from the ACL for all the database services in the specified pluggable database (PDB).

Syntax

```
DBMS_SFW_ACL_ADMIN.IP_REMOVE_PDB_ACL (
  p_pdb_name   IN   VARCHAR2);
```

Parameters

Table 179-7   IP_REMOVE_PDB_ACL Procedure Parameters

Parameter	Description
p_pdb_name	The name of the PDB.