Using Password File Authentication

This section describes how to authenticate an administrative user using password file authentication.

See Also: *SQL*Plus User's Guide and Reference* for syntax of the `CONNECT` command

Operating System Group	UNIX	Windows
OSDBA	`dba`	`ORA_DBA`
OSOPER	`oper`	`ORA_OPER`

See Also: Your operating system specific Oracle documentation for information about creating the OSDBA and OSOPER groups

Preparing to Use Password File Authentication

To enable authentication of an administrative user using password file authentication you must do the following:

1. Create an operating system account for the user.

2. If not already created, Create the password file using the `ORAPWD` utility:

```
ORAPWD FILE=filename PASSWORD=password ENTRIES=max_users
```

3. Set the `REMOTE_LOGIN_PASSWORDFILE` initialization parameter to `EXCLUSIVE`.

4. Connect to the database as user `SYS` (or as another user with the administrative privilege).

5. If the user does not already exist in the database, create the user. Grant the `SYSDBA` or `SYSOPER` system privilege to the user:

```
GRANT SYSDBA to scott;
```

This statement adds the user to the password file, thereby enabling connection `AS SYSDBA`.

Connecting Using Password File Authentication

Administrative users can be connected and authenticated to a local or remote database by using the SQL*Plus `CONNECT` command. They must connect using their username and password and with the `AS SYSDBA` or `AS SYSOPER` clause. For example, user `scott` has been granted the `SYSDBA` privilege, so he can connect as follows:

```
CONNECT scott/tiger AS SYSDBA
```

However, since `scott` has not been granted the `SYSOPER` privilege, the following command will fail:

```
CONNECT scott/tiger AS SYSOPER
```

See Also: "Creating and Maintaining a Password File" on page 1-20 for instructions for creating and maintaining a password file

Creating and Maintaining a Password File

You can create a password file using the password file creation utility, `ORAPWD`. For some operating systems, you can create this file as part of your standard installation.

This section contains the following topics:

Using ORAPWD

When you invoke the password file creation utility without supplying any parameters, you receive a message indicating the proper use of the command as shown in the following sample output:

```
orapwd
```

```
Usage: orapwd file=<fname> password=<password> entries=<users>
where
file - name of password file (mand),
password - password for SYS (mand),
```

Note: Operating system authentication takes precedence over password file authentication. Specifically, if you are a member of the OSDBA or OSOPER group for the operating system, and you connect as SYSDBA or SYSOPER, you will be connected with associated administrative privileges regardless of the *username/password* that you specify.

If you are not in the OSDBA or OSOPER groups, and you are not in the password file, then the connection will fail.

See Also: *SQL*Plus User's Guide and Reference* for syntax of the `CONNECT` command

See Also: Your operating system specific Oracle documentation for information on using the installer utility to install the password file


```
entries - maximum number of distinct DBAs and OPERs (opt),
There are no spaces around the equal-to (=) character.
```

The following command creates a password file named `acct.pwd` that allows up to 30 privileged users with different passwords. In this example, the file is initially created with the password `secret` for users connecting as `SYS`.

```
ORAPWD FILE=acct.pwd PASSWORD=secret ENTRIES=30
```

Following are descriptions of the parameters in the `ORAPWD` utility.

FILE

This parameter sets the name of the password file being created. You must specify the full path name for the file. The contents of this file are encrypted, and the file cannot be read directly. This parameter is mandatory.

The types of filenames allowed for the password file are operating system specific. Some operating systems require the password file to be a specific format and located in a specific directory. Other operating systems allow the use of environment variables to specify the name and location of the password file. See your operating system specific Oracle documentation for the names and locations allowed on your platform.

If you are running multiple instances of Oracle using Oracle9*i* Real Application Clusters, the environment variable for each instance should point to the same password file.

PASSWORD

This parameter sets the password for user `SYS`. If you issue the `ALTER USER` statement to change the password for `SYS` after connecting to the database, both the password stored in the data dictionary and the password stored in the password file are updated. This parameter is mandatory.

ENTRIES

This parameter specifies the number of entries that you require the password file to accept. This number corresponds to the number of distinct users allowed to connect

Caution: It is critically important to the security of your system that you protect your password file and the environment variables that identify the location of the password file. Any user with access to these could potentially compromise the security of the connection.

to the database as `SYSDBA` or `SYSOPER`. The actual number of allowable entries can be higher than the number of users because the `ORAPWD` utility continues to assign password entries until an operating system block is filled. For example, if your operating system block size is 512 bytes, it holds four password entries. The number

of password entries allocated is always multiple of four.
Entries can be reused as users are added to and removed from the password file. If you intend to specify REMOTE_LOGON_PASSWORDFILE=EXCLUSIVE, and to allow the granting of SYSDBA and SYSOPER privileges to users, this parameter is required.

Setting REMOTE_LOGIN_ PASSWORDFILE

In addition to creating the password file, you must also set the initialization parameter REMOTE_LOGIN_PASSWORDFILE to the appropriate value. The values recognized are described as follows:

Caution: When you exceed the allocated number of password entries, you must create a new password file. To avoid this necessity, allocate a number of entries that is larger than you think you will ever need.

Value Description

NONE Setting this parameter to NONE causes Oracle to behave as if the password file does not exist. That is, no privileged connections are allowed over non-secure connections. NONE is the default value for this parameter.

EXCLUSIVE An EXCLUSIVE password file can be used with only one database. Only an EXCLUSIVE file can contain the names of users other than SYS. Using an EXCLUSIVE password file allows you to grant SYSDBA and SYSOPER system privileges to individual users and have them connect as themselves.

SHARED A SHARED password file can be used by multiple databases. However, the only user recognized by a SHARED password file is SYS. You cannot add users to a SHARED password file. All users needing SYSDBA or SYSOPER system privileges must connect using the same name, SYS, and password. This option is useful if you have a single DBA administering multiple databases.

Adding Users to a Password File

When you grant SYSDBA or SYSOPER privileges to a user, that user's name and privilege information are added to the password file. If the server does not have an EXCLUSIVE password file (that is, if the initialization parameter REMOTE_LOGIN_PASSWORDFILE is NONE or SHARED) you receive an error message if you attempt to grant these privileges.

A user's name remains in the password file only as long as that user has at least one of these two privileges. If you revoke both of these privileges, the user is removed from the password file.

To Create a Password File and Add New Users to It

1. Follow the instructions for creating a password file as explained in "Using ORAPWD" on page 1-20.

2. Set the REMOTE_LOGIN_PASSWORDFILE initialization parameter to EXCLUSIVE.

3. Connect with SYSDBA privileges as shown in the following example:

```
CONNECT SYS/password AS SYSDBA
```

4. Start up the instance and create the database if necessary, or mount and open an existing database.

5. Create users as necessary. Grant SYSDBA or SYSOPER privileges to yourself and other users as appropriate. See "Granting and Revoking SYSDBA and SYSOPER Privileges".

Granting the SYSDBA or SYSOPER privilege to a user causes their username to be added to the password file. This enables the user to connect to the database as SYSDBA or SYSOPER by specifying username and password (instead of using SYS). The use of a password file does not prevent OS authenticated users from connecting if they meet the criteria for OS authentication.

Suggestion: To achieve the greatest level of security, you should set the REMOTE_LOGIN_PASSWORDFILE initialization parameter to EXCLUSIVE immediately after creating the password file.

Granting and Revoking SYSDBA and SYSOPER Privileges

If your server is using an EXCLUSIVE password file, use the GRANT statement to grant the SYSDBA or SYSOPER system privilege to a user, as shown in the following example:

```
GRANT SYSDBA TO scott;
```

Use the REVOKE statement to revoke the SYSDBA or SYSOPER system privilege from a user, as shown in the following example:

```
REVOKE SYSDBA FROM scott;
```

Because SYSDBA and SYSOPER are the most powerful database privileges, the ADMIN OPTION is not used. Only a user currently connected as SYSDBA (or INTERNAL) can grant or revoke another user's SYSDBA or SYSOPER system privileges. These privileges cannot be granted to roles, because roles are only available after database startup. Do not confuse the SYSDBA and SYSOPER database privileges with operating system roles, which are a completely independent feature.

Viewing Password File Members

Use the V$PWFILE_USERS view to see the users who have been granted SYSDBA or SYSOPER system privileges for a database. The columns displayed by this view are as follows:

Maintaining a Password File

This section describes how to:

- Expand the number of password file users if the password file becomes full
- Remove the password file

See Also: Chapter 25, "Managing User Privileges and Roles" for more information on system privileges

Column	Description
USERNAME	This column contains the name of the user that is recognized by the password file.
SYSDBA	If the value of this column is TRUE, then the user can log on with SYSDBA system privileges.
SYSOPER	If the value of this column is TRUE, then the user can log on with SYSOPER system privileges.

- Avoid changing the state of the password file

Expanding the Number of Password File Users

If you receive the file full error (ORA-1996) when you try to grant SYSDBA or SYSOPER system privileges to a user, you must create a larger password file and re-grant the privileges to the users.

To Replace a Password File

1. Note the users who have SYSDBA or SYSOPER privileges by querying the V$PWFILE_USERS view.
2. Shut down the database.
3. Delete the existing password file.
4. Follow the instructions for creating a new password file using the ORAPWD utility in "Using ORAPWD" on page 1-20. Ensure that the ENTRIES parameter is set to a number larger than you think you will ever need.
5. Follow the instructions in "Adding Users to a Password File" on page 1-23.

Removing a Password File

If you determine that you no longer require a password file to authenticate users, you can delete the password file and reset the REMOTE_LOGIN_PASSWORDFILE initialization parameter to NONE. After you remove this file, only those users who

can be authenticated by the operating system can perform database administration operations.

Changing the Password File State

The password file state is stored in the password file. When you first create a password file, its default state is `SHARED`. You can change the state of the password file by setting the initialization parameter `REMOTE_LOGIN_PASSWORDFILE`. When you start up an instance, Oracle retrieves the value of this parameter from the

Caution: Do not remove or modify the password file if you have a database or instance mounted using `REMOTE_LOGIN_PASSWORDFILE=EXCLUSIVE` (or `SHARED`). If you do, you will be unable to reconnect remotely using the password file. Even if you replace it, you cannot use the new password file, because the timestamps and checksums will be wrong.

parameter file stored on your client machine. When you mount the database, Oracle compares the value of this parameter to the value stored in the password file. If the values do not match, Oracle overwrites the value stored in the file.