Adminstration Base de Données
TP1

Samet MohamedAmin
SAMET MohamedAmin

2018-03-07

Sommaire

PART 1

Oracle Database creates a set of sample user accounts by default. The sample schema user accounts are all non-administrative accounts, and their tablespace is USERS. To protect these accounts from unauthorized access, the installation process locks and expires these accounts immediately after installation.

In general: - to ensure that a user does not exist: `SELECT username FROM ALL_USERS WHERE username='<username>';` - to remove any the following users: `DROP USER <username> CASCADE;`

The following accounts `BI`, `HR`, `IX`, `OE`, `PM`, `SCOTT` et `SH` have a known account password. And in case the accounts still exist in the data base and have not changed the password, this may represent a security threat and an easy exploit to obtain an unauthorized access to the data.

1.2.1 Remove the sample user 'BI'

The account that owns the `BI` (Business Intelligence) schema included in the Oracle Sample Schemas.

1.2.2 Remove the sample user 'HR'

The account used to manage the `HR` (Human Resources) schema. This schema stores information about the employees and the facilities of the company.

1.2.3 Remove the sample user 'IX'

The account used to manage the `IX` (Information Exchange) schema. This schema manages shipping through business-to-business (`B2B`) applications.

1.2.4 Remove the sample user 'OE'

The account used to manage the `OE` (Order Entry) schema. This schema stores product inventories and sales of the company's products through various channels.

1.2.5 Remove the sample user 'PM'

The account used to manage the `PM` (Product Media) schema. This schema contains descriptions and detailed information about each product sold by the company.

1.2.6 Remove the sample user 'SCOTT'

The SCOTT schema contains the tables `EMP`, `DEPT`, `SALGRADE`, and `BONUS`. The `SCOTT` account is used in examples throughout the Oracle Database documentation set, it is a demonstration account with a simple schema. When you install Oracle Database, the `SCOTT` account is locked and expired.

1.2.7 Remove the sample user 'SH'

The account used to manage the `SH` (Sales) schema. This schema stores business statistics to facilitate business decisions.

PART 2

In general, to get any parameter value:
`SELECT value FROM v$parameter WHERE UPPER(name)='<PARAM-UPPER>';`

2.3 Setting for the 'audit_sys_operations' parameter

`AUDIT_SYS_OPERATIONS` enables or disables the auditing of operations issued by user `SYS`, and users connecting with `SYSDBA` or `SYSOPER` privileges. The audit records are written to the operating system's audit trail. The audit records will be written in XML format if the `AUDIT_TRAIL` initialization parameter is set to XML. We can change its value by: `ALTER SYSTEM SET audit_sys_operations=true SCOPE=spfile;`

2.4 Setting for the 'audit_trail' parameter

`AUDIT_TRAIL` enables or disables database auditing. Values: - `none`: Disables database auditing. - `os`: Enables database auditing and directs all audit records to the operating system's audit trail. - `db`: Enables database auditing and directs all audit records to the database audit trail (the `SYS.AUD$` table). - `db,extended`: Enables database auditing and directs all audit records to the database audit trail (the `SYS.AUD$` table). In addition, populates the `SQLBIND` and `SQLTEXT CLOB` columns of the `SYS.AUD$` table. - `xml`: Enables database auditing and writes all audit records to XML format OS files. - `xml,extended`: Enables database auditing and prints all columns of the audit trail, including SqlText and SqlBind values. We can set the `AUDIT_TRAIL` options by execution this command as an example: `alter system set AUDIT_TRAIL=db scope=spfile;`

2.5 Setting for the 'global_names' parameter

`GLOBAL_NAMES` specifies whether a database link is required to have the same name as the database to which it connects. If the value of `GLOBAL_NAMES` is false, then no check is performed. If you use or plan to use distributed processing, then Oracle recommends that you set this parameter to true to ensure the use of consistent naming conventions for databases and links in a networked environment.

2.6 Setting for the 'local_listener' parameter

Its default value = null Specifies a network name that resolves to an address or address list of Oracle Net local listeners (that is, listeners that are running on

the same machine as this instance). The address or address list is specified in the TNSNAMES.ORA file or other address repository as configured for your system.

2.7 Setting for the 'o7_dictionary_accessibility' parameter

O7_DICTIONARY_ACCESSIBILITY controls restrictions on SYSTEM privileges. If the parameter is set to true, access to objects in the SYS schema is allowed (Oracle7 behavior). The default setting of false ensures that system privileges that allow access to objects in "any schema" do not allow access to objects in the SYS schema. For example, if O7_DICTIONARY_ACCESSIBILITY is set to false, then the SELECT ANY TABLE privilege allows access to views or tables in any schema except the SYS schema (data dictionary tables cannot be accessed). The system privilege EXECUTE ANY PROCEDURE allows access on the procedures in any schema except the SYS schema. If this parameter is set to false and you need to access objects in the SYS schema, then you must be granted explicit object privileges. The following roles, which can be granted to the database administrator, also allow access to dictionary objects: - SELECT_CATALOG_ROLE - EXECUTE_CATALOG_ROLE - DELETE_CATALOG_ROLE

2.8 Setting for the 'os_roles' parameter

OS_ROLES determines whether Oracle or the operating system identifies and manages the roles of each username. Values: - TRUE: The operating system completely manages the role grants for all database usernames. When a user attempts to create a session, the username's security domain is initialized using the roles identified by the operating system. A user can subsequently enable as many roles identified by the operating system as specified by the parameter MAX_ENABLED_ROLES. Revocation by Oracle of roles granted by the operating system is ignored, as are any roles previously granted by Oracle. - FALSE: Oracle identifies and manages the roles.

2.9 Setting for the 'remote_listener' parameter

REMOTE_LISTENER specifies a network name that resolves to an address or address list of Oracle Net remote listeners (that is, listeners that are not running on the same machine as this instance). The address or address list is specified in the TNSNAMES.ORA file or other address repository as configured for your system.

2.10 Setting for the 'remote_login_passwordfile' parameter

Default value is exclusive. `REMOTE_LOGIN_PASSWORDFILE` specifies whether Oracle checks for a password file. Values: - `shared`: One or more databases can use the password file. The password file can contain `SYS` as well as non-SYS users. - `exclusive`: The password file can be used by only one database. The password file can contain `SYS` as well as non-SYS users. - `none` Oracle ignores any password file. Therefore, privileged users must be authenticated by the operating system.

2.11 Setting for the 'remote_os_authent' parameter

`REMOTE_OS_AUTHENT` specifies whether remote clients will be authenticated with the value of the `OS_AUTHENT_PREFIX` parameter.

2.12 Setting for the 'remote_os_roles' parameter

`REMOTE_OS_ROLES` specifies whether operating system roles are allowed for remote clients. The default value, false, causes Oracle to identify and manage roles for remote clients.

2.13 Setting for the 'utl_file_dir' parameter

`UTL_FILE_DIR` lets you specify one or more directories that Oracle should use for PL/SQL file I/O. If you are specifying multiple directories, you must repeat the `UTL_FILE_DIR` parameter for each directory on separate lines of the initialization parameter file. All users can read or write to all files specified by this parameter. Therefore all PL/SQL users must be trusted with the information in the directories specified by this parameter.

2.14 Setting for the 'sec_case_sensitive_logon' parameter

`SEC_CASE_SENSITIVE_LOGON` enables or disables password case sensitivity in the database. Values: - `true`: Database logon passwords are case sensitive. - `false`: Database logon passwords are not case sensitive.

2.15 Setting for the 'sec_max_failed_login_attempts' parameter

`SEC_MAX_FAILED_LOGIN_ATTEMPTS` specifies the number of authentication attempts that can be made by a client on a connection to the server process. After

the specified number of failure attempts, the connection will be automatically dropped by the server process.

2.16 Setting for the 'sec_protocol_error_further_action' parameter

`SEC_PROTOCOL_ERROR_FURTHER_ACTION` specifies the further execution of a server process when receiving bad packets from a possibly malicious client. Values: - `CONTINUE`: The server process continues execution. The database server may be subject to a Denial of Service (DoS) if bad packets continue to be sent by a malicious client. - `(DELAY,integer)`: The client experiences a delay of integer seconds before the server process accepts the next request from the same client connection. Malicious clients are prevented from excessive consumption of server resources while legitimate clients experience a degradation in performance but can continue to function. - `(DROP,integer)`: The server forcefully terminates the client connection after integer cumulative bad packets. The server protects itself at the expense of the client (for example, a client transaction may be lost). The client may reconnect and attempt the same operation.

2.17 Setting for the 'sec_protocol_error_trace_action' parameter

`SEC_PROTOCOL_ERROR_TRACE_ACTION` specifies the action that the database should take when bad packets are received from a possibly malicious client. Values: - `NONE`: The database server ignores the bad packets and does not generate any trace files or log messages. - `TRACE`: A detailed trace file is generated when bad packets are received, which can be used to debug any problems in client/server communication. - `LOG`: A minimal log message is printed in the alert logfile and in the server trace file. A minimal amount of disk space is used. - `ALERT`: An alert message is sent to a DBA or monitoring console.

2.18 Setting for the 'sec_return_server_release_banner' parameter

`SEC_RETURN_SERVER_RELEASE_BANNER` specifies whether or not the server returns complete database software information to clients. Values: - `true`: Returns complete database version information to the client. - `false`: Returns a generic version string to the client.

2.19 Setting for the 'sql92_security' parameter

The SQL92 standards specify that security administrators should be able to require that users have `SELECT` privilege on a table when executing an `UPDATE` or `DELETE` statement that references table column values in a `WHERE` or SET clause. SQL92_SECURITY specifies whether users must have been granted the `SELECT` object privilege in order to execute such `UPDATE` or `DELETE` statements.

2.20 Setting for undocumented '_trace_files_public' parameter

The `_TRACE_FILES_PUBLIC` parameter is used to make trace files used for debugging database applications and events available to all database users. Use of this capability precludes the discrete assignment of privileges based on job function. Additionally, its use may provide access to external files and data to unauthorized users.