Oracle Database Cloud – Multitenant Service
security lockdown
## Table of Contents

- **Introduction** ............................................................................................................................................................... 3
- **Summary of Security Threats** .................................................................................................................................... 3
- **Specifications** ............................................................................................................................................................. 4  
  - Oracle Database Version and Edition .................................................................................................................... 4  
  - Components not available..................................................................................................................................... 4  
  - Schemas and data.................................................................................................................................................. 4  
- **SQL Syntax** ................................................................................................................................................................. 4  
  - Allowed CREATE statements ................................................................................................................................. 4  
  - Removed SQL statements ..................................................................................................................................... 5  
  - PL/SQL Packages and Types ................................................................................................................................... 5  
  - Included Supplied PL/SQL Packages and Types ..................................................................................................... 5  
- **Database object security** ........................................................................................................................................... 6  
  - Data object limitations .......................................................................................................................................... 7  
  - Query limitations ................................................................................................................................................... 7  
- **Oracle Database Cloud – Multitenant Service specific limitations** ................................................................. 7  
- **Data dictionary access** ........................................................................................................................................... 7  
- **Resource limitations** .................................................................................................................................................. 9
Introduction

The Oracle Database Cloud – Multitenant Service is a multi-tenant environment, based on schema isolation. To ensure the security of each tenant’s data, as well as the overall performance integrity of the entire Oracle Database Cloud – Multitenant Service environment, some aspects of the Oracle Database, Enterprise Edition, have to be curtailed or completely eliminated.

The limitations required to protect security and performance integrity are detailed in this document. None of the limitations listed in this document were put in place as an attempt to limit the functionality of the Multitenant Service. Virtually all standard SQL and PL/SQL syntax and constructs used with the Oracle Database work in the Multitenant Service.

Summary of Security Threats

There are several types of threats which could be used to compromise the Oracle Database Cloud - Multitenant Service and some specifics areas that are potential security weaknesses.

- Any interaction with the operating system or file system including:
  - The use of BFILEs or external LOBs, operating system ACLs, database DIRECTORY capabilities and any option, feature or supplied PL/SQL package that allow file handling (UTIL_FILE, DBFS, XDB, etc.)
- Any native interaction with the network including:
  - Any database capability that provides access to TCP sockets, HTTP or SMTP requests, hostname or IP address lookup, Oracle Streams or Advanced Queues, database links, replication operations, network ACLs or other option, feature or supplied PL/SQL that have network access or permissions. Inbound and outbound Web Service requests are allowed through the use of inbound RESTful Web Services or using the Oracle Application Express Web Services APIs for calling external services. Sending email is also allowed using the Oracle Application Express Mail API, within limits described below.
- Database operations that might allow one tenant user to access another tenant’s data or code including:
  - Any GRANTS on anything to anyone, or any option, feature or supplied PL/SQL that provides granted access to PUBLIC, ANONYMOUS or APEX_PUBLIC_USER.
  - Tenant users with objects with “coded identifiers” that could allow cross-schema access.
  - Any database view that may allow a tenant user to access any information about another tenant. (For example; all DBA_% or V$% data dictionary views and some ALL_% data dictionary views).
- Database operations that might impact the integrity of the service or another user.
  - This is the control of a tenant’s use of any shared system resources, where the tenant could reduce the availability of these resources, either accidentally or maliciously. These shared resources include CPU, I/O, memory or any internal objects or handles that use CPU, I/O and memory. This also includes anything stored in the SYSTEM tablespace, TEMP or UNDO tablespaces.
- Database operations that might be used to launch a denial of service (DoS) attack on the database service itself or on some other system.
  - This consists of many of the threats already mentioned, but specifically includes code that can easily create an attack, like job scheduling.
Specifications

Oracle Database Version and Edition

The current version of the Oracle Database Cloud – Multitenant Service is based on Oracle Database 11g Release 2, Enterprise Edition with each quarterly security patch set applied. The only option included in the service is the Partitioning Option.

Components not available

The following features and components are not part of the current version of the Multitenant Service:

- Oracle Text
- Oracle OLAP
- Oracle Spatial
- Oracle Label Security
- Oracle Warehouse Builder
- Oracle Database Vault
- Oracle Database Extensions for .NET
- Oracle Database Extensions for Java
- Oracle Multimedia

Schemas and data

The following schemas and data are not accessible in the Multitenant Service:

- Sample schemas
- A local Enterprise Manager repository
- Oracle Data Mining RDBMS APIs for file access

SQL Syntax

The following sections describe various SQL syntax in the Oracle Database Cloud - Multitenant Service.

Allowed CREATE statements

CREATE statements have a broad range of syntax and options. The appendices for this paper list all allowed statements, but this list includes the most common allowed CREATE statements in an Oracle Database Cloud – Multitenant Service:

- CREATE TABLE
- CREATE INDEX
- CREATE VIEW
- CREATE PROCEDURE
- CREATE PACKAGE
- CREATE FUNCTION
- CREATE SEQUENCE
- CREATE TRIGGER
- CREATE SESSION
- CREATE DIMENSION
CREATE INDEXTYPE
CREATE OPERATOR
CREATE TYPE

**Removed SQL statements**
The following SQL statements cannot be used in an Oracle Database Cloud - Multitenant Service:

- CREATE CLUSTER
- CREATE JOB (Background jobs can be created through the CLOUD_SCHEDULER package)
- CREATE SYNONYM
- CREATE JAVA
- CREATE ROLE
- CREATE DIRECTORY
- CREATE TABLESPACE
- CREATE DATABASE LINK
- Some ALTER SESSION options, although most session level changes for NLS or character sets are still allowed

Additionally, parallel operations are not supported on the Multitenant Service, so any SQL DDL clauses that allow for parallel operations are not supported.

**PL/SQL Packages and Types**
Oracle Database 11g Release 2 includes many PL/SQL packages to deliver extended functionality. The following sections list the PL/SQL packages that are part of the Oracle Database Cloud - Multitenant Service and some prominent packages which are not included.

**Included Supplied PL/SQL Packages and Types**
The following PL/SQL packages and types are included in the Oracle Database Cloud - Multitenant Service:

- ANYDATA
- ANYDATASET
- ANYTYPE
- AQ$_AGENT
- AQ$_SIG_PROP
- AQ$_SUBSCRIBERS
- DBMS_APPLICATION_INFO
- DBMS_ASSERT
- DBMS_CRYPTO
- DBMS_DB_VERSION
- DBMS_FREQUENT_ITEMSET
- DBMS_LCR
- DBMS_LOB
- DBMS_METADATA
- DBMS_OUTPUT
- DBMS_RANDOM
- DBMS_SQL
- DBMS_STANDARD
- DBMS_STATS
- DBMS_TYPES
All DBMS_XML% packages and types
DBMS_XPLAN
All DBMS_XQUERY% packages and types
DBMSOUTPUT_LINESARRAY
HTF
HTP
All Oracle Application Express API packages except for APEX_PLSQL_JOB and APEX_LDAP
All ODCI% packages and types
All OWA% packages and types
PLTBLM
SCN_TO_TIMESTAMP
STANDARD
STRAGG
SYS_NT_COLLECT
SYS_STUB_FOR_PURITY_ANALYSIS
TIMESTAMP_TO_SCN
UTL_COLL
UTL_COMPRESS
UTL_ENCODE
UTL_GDK
UTL_I18N
UTL_IDENT
UTL_LMS
UTL_MATCH
All UTL_NLA% packages and types
UTL_RAW
UTL_REF
WPG_DOCLOAD
XMLGENFORMATTYPE
XMLSEQUENCE
XMLSEQUENCEFROMREFCURSOR
XMLSEQUENCEFROMREFCURSOR2
XMLSEQUENCEFROMXMLTYPE
XMLSEQUENCETYPE
XMLTYPE
XMLTYPEEXTRA
XMLTYPEI
All XQ% packages and types

All packages not listed here are not available in the Multitenant Service.

**Database object security**

By default, all Oracle Application Express applications and RESTful Web Services execute with the privileges of the schema owner. You can create users within the Oracle Application Express environment and use authentication schemes to limit access to application objects at all levels in your application through Oracle Application Express.

You cannot use a GRANT command to assign access to another user, since other schema owners are not allowed
to access your schema objects in the schema-isolation multi-tenant environment of the Multitenant Service.

You can also assign security across multiple dimensions, including origin, application and users, for any RESTful Web Services.

**Data object limitations**
The following limitations apply to DDL (Data Definition Language) syntax:

- You cannot use any PARALLEL syntax in defining tables
- You cannot use quoted identifiers with special characters
- You cannot define BFILEs or external LOBs
- You cannot use external tables
- You cannot specify any caching for database objects

**Query limitations**
By default, you can use all Oracle SQL syntax for SQL statements used against your Oracle Database Cloud - Multitenant Service. The following limitations apply to SQL queries:

- No PARALLEL hints allowed

**Oracle Database Cloud – Multitenant Service specific limitations**
The core of the Oracle Database Cloud - Multitenant Service development environment is Oracle Application Express, which is also a no-cost option for all versions of the Oracle Database since Oracle Database 10g Release 2. The following areas of functionality are limited when used for applications within the Multitenant Service environment:

- Background Jobs – A Multitenant Service is able to submit jobs, but is limited to a maximum of 10 defined jobs and 5 jobs running or scheduled at any one time. Jobs will be subject to resource limitations imposed by Database Resource Manager, similar to the way overall resources are limited and described below. These limits and conditions will be implemented through a PL/SQL package called CLOUD_SCHEDULER.
- E-mails – A Multitenant Service is limited to 5,000 emails in a 24 hour period.
- Outbound Web Service calls – A Multitenant Service application can make outbound Web Service calls through the APEX_WEB_SERVICE PL/SQL package. These calls can only use HTTPS or SSL and use a proxy server from within the Multitenant Service.
- Oracle Application Express Public API Packages – The APEX_PLSQL_JOB and APEX_LDAP API packages are not available.

**Data dictionary access**
Access to standard data dictionary objects in the Oracle Database is limited, since the security requirements of schema isolation prevent any user from seeing or knowing the existence of other schemas.
The following data dictionary views and synonyms are accessible from an Oracle Database Cloud - Multitenant Service:

- ALL_ALL_TABLES
- ALL_COL_COMMENTS
- ALL_CONS_COLUMNS
- ALL_CONSTRAINTS
- ALL_DEPENDENCIES
- ALL_ERRORS
- ALL_IND_COLUMNS
- ALL_IND_EXPRESSIONS
- ALL_IND_PARTITIONS
- ALL_IND_STATISTICS
- ALL_INDEXES
- ALL_OBJECTS
- ALL_OBJECT_TABLES
- ALL_PLSQL_OBJECT_SETTINGS
- ALL_REFS
- ALL_SEQUENCES
- ALL_SYNONYMS
- ALL_TAB_COLS
- ALL_TAB_COLUMNS
- ALL_TAB_COMMENTS
- ALL_TAB_PARTITIONS
- ALL_TAB_SUBPARTITIONS
- ALL_TABLES
- ALL_TRIGGERS
- ALL_TYPES
- ALL_UPDATABLE_COLUMNS
- ALL_VIEWS
- AUDIT_ACTIONS
- COL
- COLUMN_PRIVILEGES
- DATABASE_COMPATIBLE_LEVEL
- DATABASE_PROPERTIES
- DICTIONARY
- DICT_COLUMNS
- DUAL
- INDEX_HISTOGRAM
- INDEX_STATS
- PRODUCT_COMPONENT_VERSION
- TAB
- NLS_DATABASE_PARAMETERS
- NLS_INSTANCE_PARAMETERS
- NLS_SESSION_PARAMETERS
- ROLE_ROLE_PRIVS
- ROLE_SYS_PRIVS
- ROLE_TAB_PRIVS
- All USER_% views
- V$TIMEZONE_NAMES
You can also view schema objects in both SQL Developer and the SQL section of the Oracle Application Express development environment.

**Resource limitations**

The Oracle Database excels at managing shared resources among thousands of database users. The Oracle Database Cloud – Multitenant Service uses this proven ability to distribute machine resources among tenants.

The Multitenant Service uses Database Resource Manager consumer groups to prevent any tenant from impacting the performance of other tenants. All tenant operations are initially placed in a consumer group with maximum access to resources. If a user exceeds the resource limitations of this initial consumer group, their user process is pushed to a lower priority user group, with a much longer limit on resource consumption, but a lower priority. If a user process exceeds this limit, they are pushed to a lower priority group with a much higher resource limit.

If a user process should exceed this last limit, the process may be terminated. Please be aware that this lowest consumer group allows for the consumption of up to 30 seconds of dedicated CPU time, a threshold which is normally only crossed by runaway processes.