Security and the Oracle Database Cloud Service
Table of Contents

Overview .................................................................................................................. 3
Security architecture ......................................................................................... 4
   User areas ................................................................................................. 4
      Accounts .............................................................................................. 4
      Identity Domains .............................................................................. 4
      Database Cloud Service ................................................................. 5
      Cloud Identity Manager ................................................................. 6
      Signing up for a Database Cloud Service trial ............................... 6
Database Cloud security measures ................................................................. 7
Database Cloud Service security measures ..................................................... 7
Database Cloud application security options ................................................. 7
RESTful Web Service security options ............................................................. 8
   Origin-based security ........................................................................... 9
   OAUTH authentication ........................................................................... 9
   Application-based access ....................................................................... 9
   User-based access ............................................................................... 9
   Logic-based access ............................................................................. 9
Overview

One of the key concerns for organizations as they move to a shared resource model on the Cloud is insuring the security of their data. The Oracle Database Cloud Service, like the Oracle Database that is the foundation of the Database Cloud, has been created from the beginning with the utmost concern for security.

This paper will review several aspects of security and the Oracle Database Cloud –

- The basic architecture of the security domains that are used for the Database Cloud
- Security measures that apply to the overall service
- Security measures that apply to individual Database Cloud Services
- Application security options and
- Security options for RESTful Web Services that access a Database Cloud Service
Security architecture

To understand the security architecture of the Oracle Database Cloud, you need to understand several different types of users and how they interact in the provisioning and management of a Database Cloud Service.

User areas

There are three different areas where user types operate – an account, which represents a business organization, an identity domain, which represents a set of users, and a Database Cloud Service, which users in an identity domain can access.

Accounts

An account is representation of a business organization. An account can contain multiple Identity Domains, and each Identity Domain can contain multiple Database Cloud Services.

An account is created when the first Database Cloud Service is requested for a particular user. The initial requestor for an Account is identified as the Buyer. If the Buyer is requesting a Service through the Oracle Store, the Buyer can specify a different user as the Account Administrator; if the initial request is for a trial, the Buyer and the initial Account Administrator are the same user.

Buyers and Account Administrators are authenticated through their Oracle.com identity. Any Account Administrator can grant or revoke the Account Administrator privilege for any other Oracle.com user.

An Account Administrator has access to the My Account page in the Cloud user interface, which offers a read-only view of all users and Database Cloud Services within an account. This read-only access allows Account Administrators to monitor all users and Services in their Account, but Account Administrators do not have any other management capabilities for those areas.

Account Administrators can create additional Identity Domains or Database Cloud Services for their accounts. An Account Administrator can assign a new Database Cloud Service to an existing Identity Domain within their account.

Identity Domains

An Identity Domain is a pool of users. An account can have one or more Identity Domains, but each Domain is separate and distinct. You must define an Identity Domain when you initially request an account, and the requestor is given a username within the Identity Domain.
Identity Domain membership and privileges are defined with the Cloud Identity Manager, which is described in more detail below.

Members of an Identity Domain can have security roles for one or more of the Cloud Services associated with the Identity Domain. These roles are described in more detail below.

Identity Domain Administrators can see all Database Cloud Services associated with the Identity Domain, and can assign and remove all security roles associated with these Cloud Services, including the Administrator role for any of the Services.

**Database Cloud Service**

A Database Cloud Service is an individual Service within the Oracle Database Cloud. Data within an individual Database Cloud Service is completely separated from data in all other Services in the Oracle Database Cloud, as described in more detail below.

Database Cloud Service administrators can define users for the Services that they administer. Database Cloud Service users can be defined with the Cloud Identity Manager or within the Administration area of the development platform for the Database Cloud Service itself. If a user is defined with the Cloud Identity Manager, they must use the same tool to manage their profile; if a user is defined through the Administration area of the development platform, they must manage their profile through that platform. Administrators and developers for a Database Cloud Service must be defined with the Cloud Identity Manager and given the appropriate security role.

There are three roles for each Database Cloud Service -

- **Service Administrator**, who can create, modify and delete Database Cloud Service users and their privileges, both in the Cloud Identity Manager and the Administration area of the Database Cloud Service development platform

- **Developers**, who can use the development platform within a Database Cloud Service to create applications, but who cannot create, modify or delete users for that Database Cloud Service and

- **End users**, who can run applications within the Database Cloud Service

When a Database Cloud Service is added to an Identity Domain, three individual roles which map to these levels are created within the Identity Domain. The Account Administrator and Identity Domain Administrator are automatically given the Service Administrator role for the initial Database Cloud Service, but all other roles have to be explicitly assigned through the Cloud Identity Manager.
Cloud Identity Manager

This tool is used to administer all users and roles defined as part of the Cloud Identity Domain. A Identity Domain or Service administrator can add, delete and modify users with this tool, or to create, delete, assign or delete roles, as shown here.

Identity Domain Administrators can use the Cloud Identity Manager to access all users defined within their Identity Domain and their roles. Service Administrators only get access to the users defined for their Service, and users of a service can only use the Cloud Identity Manager to modify their own user profile and reset their account password.

For more details on the use of the Cloud Identity Manager, please refer to the documentation for this tool.

Signing up for a Database Cloud Service trial

You can understand the interaction of the different security domains as you go through the process of signing up for a trial of the Database Cloud Service.

When you request a trial, the first step is to log in with your Oracle.com username and password. You are prompted for your mailing information and your credit card is validated, although nothing is charged against your card. The next page is the Service Details page, as shown here. You have two basic choices – to create a trial with a new Identity Domain, or to use an existing Identity Domain.

If you choose to create a new Identity Domain, you are assigned an Identity Domain name, as well as a Service Name. By default, the email address for your Oracle.com account is used for the email address of the Service Administrator and used as the default for the Username, but you can change the Username and the First and Last Name of the Service Administrator. You can also choose to use the same Username for the Identity Domain Administrator, or create a different Username for that role. Once you have completed this page, the users specified are created in your Identity Domain with the appropriate roles.

If you choose to use an existing Identity Domain, you are given the choice of specifying any Identity Domain within the account for which the requestor is an Account Administrator. You can specify a Username for the Service Administrator and this user is created in your Identity Domain. This user does not have any Identity Domain administration privileges.
Database Cloud security measures

All security is based on well-thought out and implemented practices and procedures. The Oracle Database Cloud is implemented with rigorous security practices and procedures based on decades of experience.

The security processes used for the overall Oracle Cloud include secure access to data centers, annual security audits by third parties to insure regulatory security compliance and full auditing of the entire Cloud stack on a quarterly basis.

All data stored in the Oracle Database Cloud benefits from the use of Transparent Data Encryption. Transparent Data Encryption encrypts data stored on disk and in backups, protecting against unauthorized direct file access. The encryption and decryption of your data is handled automatically by the Oracle Database, so you do not have to add programmatic steps to use this powerful security feature.

The Database Cloud has to be protected against the introduction of malicious code which could harm all users. To enforce this level of protection while still allowing users to load data into their Database Cloud Service, data loads are sent to a Secure FTP server, where they are scanned for viruses before the data in the files is loaded into the Database Cloud Service using your database account information. With this approach, malicious data can never be loaded in such a way that it affects other accounts or breaches the security isolation. This two step process also automatically compresses the actual data to be loaded, reducing the time needed to upload data to the Oracle Database Cloud.

Database Cloud Service security measures

The Database Cloud Service is built on a multi-tenant architecture, with database schemas providing the boundaries of tenant isolation. Schemas have been used in the Oracle Database as a method of separating data for decades. To enforce and protect the absolute security of tenants of the Database Cloud Service, some standard Oracle features have been locked down.

For instance, access to any data dictionary view which allows a tenant to see the existence of other schemas has been prohibited. In addition, some SQL syntax is not allowed, such as GRANT or REVOKE, since these options are used to access objects between one schema to another schema owner.

For a detailed list of syntax, objects and operations disallowed in the Database Cloud Service, please see the white paper on the security lockdown of the Database Cloud Service.

Database Cloud application security options

Your Database Cloud Service includes Application Express, which you can use to develop and deploy HTML-based applications through a declarative process. Application Express has been in production since 2004, with
hundreds of thousands of enterprise applications deployed throughout the world. There are a number of features of Application Express that help you to develop secure applications in your Database Cloud Service.

Application Express supports several authentication schemes, which are used to insure that a particular user is properly identified. Application Express gives developers the ability to use authorization schemes, which are ways of allowing access to specific pages, regions within pages or items within regions, based on user identity. As a developer, you have access to the identity of a user at all times, so you can implement procedural limitations based on user identity.

Although Application Express includes robust monitoring tools, you can add in procedural logic to log application and session specific information for further security analysis.

Application Express includes protection against cross-site scripting attacks by providing a way to reference values that automatically escapes special characters, which will not allow any type of script to be included in pages returned to users through the Database Cloud Service applications.

In addition, Application Express gives you the option to automatically protect navigational URLs from being malicious modified. This option, referred to as Session State Protection, generates checksums which are included with any parameters passed as part of a URL to retrieve a page in an application. In addition, you can prevent a page from ever being accessed by a URL, only allowing access as the destination of a navigation link or branch from another page within the application.

Application Express also includes reports which allow you to rapidly see the security options in force for a particular application, as well as to monitor usage of applications and individual pages in applications.

**RESTful Web Service security options**

The Oracle Database Cloud allows access to data within a Database Cloud Service through the use of RESTful Web Services, which can be defined with the RESTful Web Service Wizard. You can specify that access to RESTful calls use HTTPS, which secures communication between the client and the Database Cloud Service.

You can also specify security on a RESTful Web Service in a number of ways. These ways are different from the traditional method of using schema users to implement security. An Oracle Database Cloud Service is based on a single schema, and all RESTful Web Services which access data in this schema are executed by the user who owns the schema. Without any specific security implementations on a RESTful Web Service, the services will return all data that satisfies an SQL statement or is collected by a PL/SQL block.

There are four ways you can add security to your RESTful Web Services –

- Based on the origin of the RESTful Web Service
- Based on the application using the RESTful Web Service
Based on the identity of the user calling the RESTful Web Service or

Based on logic implemented in the RESTful Web Service call itself

Origin-based security

You can specify that a RESTful Web Service module and its templates and handlers can only be accessed for a specified list of origin domains.

OAUTH authentication

RESTful Web Services use the OAUTH2 model of authentication, as shown in this diagram. OAUTH2 authentication is one of the standard authentication flows used on the Internet. To understand how to implement application-based or user-based authentication, you need to understand how the OAUTH authentication process flow works.

OAUTH authentication requires two different tokens – a request token, which allows a client to request authorization, and an access token, which grants access to a specific user.

You can use this process flow to implement access to a specific application or to a specific user, as described below.

Application-based access

To allow a specific application to access RESTful Web Services, you use the OAUTH Request token. To implement this, you would generate a specific token and hard code that token into a specific application client. You would then use OAUTH to check for the request token.

This type of authentication allows you to use a single token to grant access to all of the RESTful Web Services defined in a module to one or more application clients.

User-based access

You can allow access to a RESTful Web Service based on the identity of the authenticated user. If you want access based only on user identity, you would not require an OAUTH Request token and use privileges defined in your Database Cloud Service to limit access to the Web Service. The process of defining and using these privileges is defined in the next section.

Logic-based access

The three methods of implementing security described above grant access to one or more specific RESTful Web Services calls, similar to allowing a connection to a database. In traditional database security, access is granted
based on the identity of the database user making the request. Since all RESTful Web Services in a specific Database Cloud Service are executed by the same database user, this option is not available for these Services. In recognition of this architecture, the SQL command GRANT is not supported in a Database Cloud Service.

However, this does not mean that you cannot limit access to data based on user identity. The identity of a user is established through the Database Cloud Service authentication process, and this identity is available to developers as the OAM_REMOTE_USER parameter, kept securely in the header of all RESTful Web Service requests.

You can use this value as part of a standard WHERE clause, which, for instance, could be used to limit the rows returned from a query to those for the same department as the current user. You could also use this value in more complex logic in either SQL or PL/SQL.