Oracle NoSQL Database cloud service – Authentication and Authorization FAQ

Oracle NoSQL Database cloud service is a fully managed NoSQL database cloud service for today's most demanding applications that require low latency responses, flexible data models, and elastic scaling for dynamic workloads.

What is Oracle NoSQL Database cloud service Fine-Grained Access Control (FGAC)?

It is an entitlement role or table level role that can be granted to a developer and/or user of an application.

When should one use Oracle NoSQL Database cloud service FGAC?

FGAC can benefit any application that tracks information in an Oracle NoSQL Database cloud table. Through an application client, the user can read or write records to the table.

For example, let us consider two users (user1 and user 2) accessing the same table. We want to allow user1 to write and read data, while we want to restrict user 2 (who is part of a reporting application) to only read data from the table. In this case, the user with ANDC_FullAccessRole along with Identity Domain Administrator or Application Administrator creates the table, the Application Administrator or Identity Domain Administrator can create the users (user1 and user2) and can assign the table level role READ_WRITE to user 1 and READ_TABLE access to user 2.

Is it possible to build applications with Oracle NoSQL Database cloud service FGAC?

Yes. As mentioned previously, different roles can be associated with an application. This will allow only authorized usage of an Oracle NoSQL Database cloud table in the service entitlement. Let us try and understand some of the concepts and terms used:

🧍	Oracle Cloud Account Administrator	Is the administrator of the Oracle Cloud service and has access to Oracle Cloud’s User Interface. The Account Admin can upgrades from trail account to paid services, can update existing services and can terminate a paid subscription to an Oracle Cloud service. There could be a single Account Administrator for a given company/entity that manages all the services that company has subscribed to.
🧍	Identity Domain Administrator	Is the administrator who can create users and grant entitlement roles or table level roles to users NOTE: If this user also has ANDC_FullAccessRole then the administrator can create tables
🧍	Application Administrator	Is the administrator who has the service level roles such as ANDC_FullAccessRole which is an administrator role and ANDC_ReadOnlyRole and/or ANDC_ReadWriteRole which are data operation roles. He can further grant FGAC Table Level roles to other application users.
🧍	Application user/developer/user	A person that is assigned table level roles to perform operations on tables. This person could be someone that is initially developing the applications and doing testing/debugging. This person could be referred to as simply a user of the service or an application user.

	Application	A user with Identity Domain Administrator (can create users) or Application Administrator (DDL operations) along with ANDC_ FullAccessRole creates a table which is represented as an IDCS resource(called an Application) and can be viewed on the IDCS administration console by users having Identity Domain Administrator. On the IDCS administration console, application developers and users can be granted table (IDCS resource) level roles to perform various operations on the table.

How does Authentication and FGAC work?

The flow chart as part of **"How should I provide roles to application users for specific tables? Below** gives a quick overview of the steps required to setup Authentication and FGAC for your entitlement. For detailed steps with screen shots, refer to Getting Started with Oracle NoSQL Database cloud.

How do I get started with Oracle NoSQL Database cloud service FGAC?

Refer to Getting started with Oracle NoSQL Database cloud to learn how to create an entitlement. Refer to the following document to create users and assign roles.

What are the roles that can be assigned to users?

FGAC is categorized into entitlement roles and table level roles.

ENTITLEMENT ROLE

When a cloud account gets created the first user gets Cloud Account Administrator, Identity Domain Administrator and ANDC_ FullAccessRole roles. For subsequent users, if there is a need for a particular user to be able to create tables, then he/she should be provided with Identity Domain Administrator (can create users) or Application Administrator(DDL operations) along with ANDC_ FullAccessRole.
The rest of the service level roles will allow users to work with any tables that are created under that subscription (service entitlement).

Role	Description	Admin
ANDC_FullAccessRole	Role having full access to Oracle NoSQL Database cloud tables under your service entitlement • Create or drop tables, create or drop indexes, alter table limits (in addition should have Identity Domain Administrator or Application Administrator) • Alter table schema • read, write table rows	Yes

ANDC_ReadOnlyRole	Read rows from any Oracle NoSQL Database cloud table assigned to the service entitlement	No
ANDC_ReadWriteRole	Read and write rows from/to any Oracle NoSQL Database cloud table assigned to the service entitlement	No

TABLE LEVEL ROLES

The Application Administrator or Identity Domain Administrator can grant application/table level roles to other users for specific tables. The Table Level roles are:

Role	Description
READ_TABLE	Read records from a given table
INSERT_TABLE	Insert or update records in the table
DELETE_TABLE	Delete records from the table
INDEX_CREATE	Create an index on the table
INDEX_DROP	Drop an index created on the table
ALTER_TABLE	Alter the definition of a table. NOTE: User with this role cannot alter the table limits. Table Limits can be changed only by the user with ANDC_FullAccessRole
READ_WRITE	Super set of READ_TABLE, INSERT_TABLE and DELETE_TABLE
TABLE_ADMIN	Super set of INDEX_CREATE, INDEX_DROP and ALTER_TABLE

NOTE: Role changes to a user will take some time to reflect on the cloud. So if you have made changes to a user by adding or removing roles then please wait for some time before you can try a NoSQL operation.

What privilege are needed to create a table?

To create a table in Oracle NoSQL Database cloud service a user would need the following roles

1. Either Identity Domain Administrator or Application Administrator
2. ANDC_FullAccessRole.

What privilege are assigned to the user who sign’s up for the Cloud Account?

By default Identity Domain Administrator, Application Administrator and ANDC_FullAccessRole are assigned to the user who sign's up for the Cloud Account.

Are there any specific FGAC attributes for Indexes that I create?

Creation and maintenance of indexes is an expensive operation and it is important to have these operations assigned to specific users of the application. An Identity Domain Administrator can grant index specific table roles such as - INDEX_CREATE and INDEX_DROP to allow users to create and drop indexes.

How should I provide roles to application users for specific tables?

There are 2 types of users – Application Administrator user and application user/developer. The Application Administrator has the ANDC_FullAccesRole and can create tables and the Identity Domain Administrator can create users and grant roles. To create new users, follow the steps:

1. Login to your cloud account.
2. Get into the User Management Dashboard from My Service Console or the IDCS Admin Console.
3. In the Identity Domain Console, under Users widget click on Add a new user and provide a valid email address
4. An email will be sent to the user and he/she can login to activate the account and reset the password.
5. The Application Administrator user would then go to the Applications Dashboard from the Admin Console
6. The Application Administrator user/ANDC_FullAccessRole creates a table instance.
7. He/She should select the Oracle NoSQL Database Cloud Service table instance (It will begin with ANDC_*).
8. Go to the application roles tab.
9. This will list all the application roles specific to Oracle NoSQL Database cloud service.
10. Click on the menu to the right of any of the application role and click on Assign users.
11. Select the user to assign the specific application role.
12. In the pop-up window click Assign.

Note: Once the user is created and appropriate roles are granted, the Application Administrator user should provide the client id, client secret and entitlement id to the user/developer to add to the user's credentials file along with his cloud username and password.

Can FGAC be applied on specific columns of a table?

No – column level access roles are not supported in Oracle NoSQL Database cloud service.

Can FGAC be applied on specific data cells of a table?

No – cell level access roles are not supported in Oracle NoSQL Database cloud service.

Can I migrate application code written with Oracle NoSQL Cloud Simulator to work with the actual Oracle NoSQL Database cloud service?

Yes - you can migrate the application written with Oracle NoSQL Cloud Simulator to Oracle NoSQL Database cloud service by including the authentication/security and pointing to the actual Oracle NoSQL Database cloud service. See next question to see an example of the minimal code changes.

What are the Authentication/Security information related changes required in the application code built against Oracle NoSQL Database Cloud Simulator before running against the actual Oracle

NoSQL Database Cloud Service?

Before including the authentication/security related code changes, it is required to create users and assign roles. Refer to Getting started with Oracle NoSQL Database cloud for more details.

Developers can use the Oracle NoSQL Database Cloud Simulator that can be downloaded from the Oracle NoSQL Cloud SDK and Oracle NoSQL Cloud Java Driver to test applications for prior to running in Oracle NoSQL Database cloud service. This is a locally running light weight database instance. Once the application is built, debugged and tested locally the developer needs to do very minimal changes to the application code to run against Oracle NoSQL Database cloud service. Before making the changes the application developer should have the following in his/her environment:

1. Entitlement Id (should be provided by the Application Administrator)
2. Client id (should be provided by the Application Administrator)
3. Client secret (should be provided by the Application Administrator)
4. Cloud account – username and password.
5. IDCS url (should be provided by the Application Administrator)

Once the above information is obtained, the developer should create a folder *.andc* in his/her home ($HOME or '~' in unix like systems OR 'C:\Users\<user/owner>\' in windows) directory and create a *credentials* file

~/.andc/credentials OR C:\Users\<user/owner>\.andc/credentials

The contents of the *credentials* file are:

andc_username=<cloud user name> (step 4)
andc_user_pwd=<cloud account password> (step 4)
andc_client_id=<client id> (step 2)
andc_client_secret=<client_secret> (step 3)

The following are the code changes that must be made to change the connection from the local system to Oracle NoSQL Database cloud service:

Oracle NoSQL Database Cloud Simulator	Oracle NoSQL Database cloud service
URL serviceURL = new URL("http", hostname, port, "/"); NoSQLHandleConfig config = new NoSQLHandleConfig(serviceURL); **config.setAuthorizationProvider(new ExampleAccessTokenProvider(tenantId));** /* * Open the handle */ NoSQLHandle handle = NoSQLHandleFactory.createNoSQLHandle(config)	URL serviceURL = new URL("https", "ans.uscom-east-1.oraclecloud.com", 443, "/"); NoSQLHandleConfig config = new NoSQLHandleConfig(serviceURL); **config.setAuthorizationProvider(new DefaultAccessTokenProvider(entitlementId, idcsurl));** /* * Open the handle */ NoSQLHandle handle = NoSQLHandleFactory.createNoSQLHandle(config)

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oraclenosql   facebook.com/oracle   twitter.com/oraclenosql

Integrated Cloud Applications & Platform Services

ORACLE®