Migration of users/roles, permissions and ownership

The Single to Flex migration tool will copy all users/roles existing in single server to flexible server. Database objects ownership and permissions will be the same in flexible server as in your single server post a successful migration.

How to enable this feature?

This capability is currently in private preview and is enabled on flexible server on a need basis. Once enabled, migration will automatically include users/roles migration along with data migration. Please share the following details to get this feature enabled on your flexible server.

Name of the flexible server –

Azure Region -

Limitations

1. AAD users will not be migrated as a part of this solution. To mitigate this limitation, you should manually create all AAD users present in your single server on your target server before running the migration. If AAD users are not created on target server, migration will fail with appropriate error messages.
2. If the target server has **only** SCRAM-SHA-256 authenticated enabled, connection to flexible server using the users/roles on single server will fail since the passwords are restored using md5 encryption. To mitigate this limitation, please include MD5 option to the **azure.accepted_password_auth_method** server parameter.

How do I verify if roles and permissions were migrated?

Users/roles verification

- Compare the roles and their memberships by running **\du+** on source and target.
  Note: **azure_superuser** (superuser of sspg) will not be present in flexible server.
  Replication users will also not be present on flexible server if the single server has a read replica.
  All other users/roles should be present in the target server post a successful migration.
- Check if you are able to login using the same passwords for the users/roles on target server.

Ownership verification

Compare the output of the following commands on source and target server.

- \dt for tables
- \dn for schemas
- \ds for sequences
- \dx for extensions
- \df+ for functions and procedures
- \dv for views

Permissions (Grants/revokes) verification

There is no single query or command that can be run to verify the permissions of the database objects. Brute force method would be to take a schema dump on source and target and see if grants and revoke statements matches.