[**https://github.com/minio/minio/issues/21601**](https://github.com/minio/minio/issues/21601)

**Access Policy with OIDC Groups**

**Question 4**

Why does an access policy with an OIDC Group condition not grant admin:\* permission when the user is a member of another group used in a different access policy?

Background

MinIO Access Policies

Policies define permissions like read, write, or admin:\* on buckets/objects.

Similar to AWS IAM policies.

OIDC Groups

MinIO can integrate with OpenID Connect (OIDC) providers (Keycloak, Auth0, etc.).

Users can belong to multiple OIDC groups.

Policies can be restricted to specific groups using a Condition in the policy.

admin: Permission\*

Full administrative access in MinIO (create buckets, manage users, etc.).

Why Admin Access May Not Be Granted

Policy Evaluation in MinIO

MinIO evaluates each policy independently.

Conditions are applied per policy.

Group-Specific Conditions

If a policy grants admin:\* only for GroupA:

A user in GroupB will not match the condition, even if another policy exists for GroupB.

MinIO does not automatically merge group memberships across policies for condition evaluation.

Effect

User will get permissions only from policies where their group matches the condition.

Being a member of another group in a different policy does not grant admin:\* unless that policy explicitly allows it.

**Example**

Policy Name Groups Allowed Permission

Policy1 GroupA admin:\*

Policy2 GroupB read/write