Mitchell Lewars <mitchelllewars@pingidentity.com>

(no subject)

Mitchell Lewars <mlewars@pingidentity.com> Wed, Jul 27, 2022 at 8:32 AM
Draft

Parts to use PA and PF after they are talking to each other (PF is the OIDC Provider for PA)

1) Add Scope to PF (a keyword or phrase associated with a set of claims ex. email) >> *System>OAuthSettings>ScopeManagement.*

Although there are common OAuth Scopes like profile, email, phone these are arbitrary and really only have meaning to specific clients and their required data/claims.

One is "special" and it's the scope openid, as the specification says that if openid is specified then there should have to be an actual Resource Owner (person) engaged and the openid scope means that an OIDC Policy exists in PF and an ID Token will be returned (ID Token is a JWT with information about the user/resource owner who logged in and is asking the application and client to act on their behalf - for example an Outlook Email client).

2) Create a Signing certificate in PF. >>Securiment>Signing&DecryptionKeys&Certificates
All tokens that PF mints (creates) should be signed to prove that PF actually did the work. This could be a public certificate or a self signed one. Commonly called "jwt-signing"

3) Create the Access Token Instance (ATM - access token manager) >>Applications>OAuth>AccessTokenManagement
The ATM defines the type of token to create, signing certificate, etc. Add claims/attributes to the access token to be mapped by the Access Token Mapping.

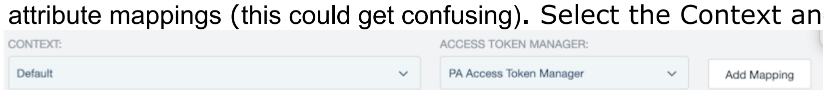
Web Sessions for PingAccess :
OIDC requires resource owner/people to login. You need at least an IdP Adapter, Auth Policy Contract (with a Policy to fulfill it), Relying Party, or some such to provide the claims (at least a sub or subject/username). Whatever initial claims are needed should be added to that source; all other claims could be LDAP, REST or whatever source supplied.

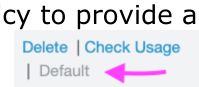
4) Create the IdP adapter Mappings >> Authentication>OAuth>IdPAdapterGrantMapping.
Implicit and AuthCode Grants need a mapping of the Adapter to the Persistent Grant
Often both values are the same :

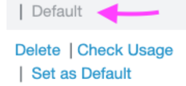
Contract Fulfillment

USER_KEY	username (Adapter)
USER_NAME	username (Adapter)

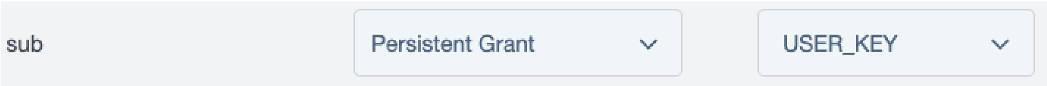
User_Key and User_Name to username

5) Creating access token attribute mappings (this could get confusing). Select the Context and the Access Token Manager to associate. 

There has to be a directory/grant/adapter/policy to provide all the data or claims. Or it could be Default 

(this is specified in the ATM by clicking Default 

Usually the sub is the USER_KEY from the Persistent Grant (the username of the person who logged in)



7) Create the OpenID Connect Claims with a OIDC Policy >> Applications>OAuth>OpenIDConnectPolicyManagement
Add the Policy that will provide the ID Token and claims to PingAccess.
By default it will add a ton of attributes and typically we delete them all and only add what the customer needs for the application. The only required value is **sub**.
sub is usually mapped to the Access Token or Persistent Grant.

6) Create the OAuth Client >> Applications>OAuth>Clients