Google Cloud

Edge Security Bootcamp

LDAP

LDAP policy

- Use the LDAP policy when access to protected resources should be limited to users in your LDAP provider
    - For example your admin users, organization users, and developers
- Use LDAP especially when OAuth token access is either unnecessary or too heavyweight.
- The policy is also designed for retrieving DN metadata for use in API proxy flows.
    - For example you can have an API call execute only when a user is successfully authenticated against LDAP; and then optionally retrieve DN attributes for the user after authentication succeeds.
- This policy is available only in Edge for Private Cloud.

Username / password authentication

- This sample provides authentication against an LDAP provider.

```
<Ldap name="4GLdapPolicy">
   <LdapResource>ldap1</LdapResource>
   <Authentication>
       <UserName ref=”request.header.username”/>
       <Password ref=”request.header.password”/>
       <Scope>subtree</Scope>
       <BaseDN></BaseDN> <!-- default is dc=apigee,dc=com -->
    </Authentication>
 </Ldap>
```

DN attribute authentication

- This policy gets the user’s DN with the email in the request header, then authenticates the user against LDAP with the password provided in the request header

```
<Ldap name="LdapPolicy">
   <LdapResource>ldap1</LdapResource>
   <Authentication>
       <Password ref=”request.header.password”/>
       <SearchQuery>mail={request.header.mail}</SearchQuery>
       <Scope>subtree</Scope>
       <BaseDN></BaseDN> <!-- default is dc=apigee,dc=com -->
    </Authentication>
 </Ldap>
```

Searching LDAP

- This policy references a custom LDAP provider.
- It uses the email address in the request header to identify the user, then retrieves the user’s address, phone, and title from LDAP. The retrieved DN attributes are stored in a variable.
- To search LDAP and retrieve DN attributes, the request must include administrator credentials.

```
<Ldap name="LdapPolicy">
    <!-- using a custom LDAP provider -->
    <LdapConnectorClass>com.custom.ldap.MyProvider</
LdapConnectorClass>
    <LdapResource>MyLdap</LdapResource>
    <Search>
        <BaseDN></BaseDN> <!-- default is dc=apigee,dc=com --
>
        <SearchQuery>mail={request.header.mail}</SearchQuery>
        <Attributes>
            <Attribute>address</Attribute>
            <Attribute>phone</Attribute>
            <Attribute>title</Attribute>
        </Attributes>
        <Scope></Scope> <!-- default is ‘subtree’ -->
    </Search>
</Ldap>
```

THANK YOU