**REST API in APEX**

**Architectural constraints/Characteristics**

***Stateless***

Each request from client to server must contain all the information necessary to understand the request, and not use any stored context on the server.

***Caching behavior***

Responses are labeled as cacheable or non-cacheable.

***Uniform interface***

All resources are accessed with a generic interface over HTTP.

***Named resources***

All resources are named using a base URI that follows your Lightning Platform URI.

***Layered components***

 allows for the existence of such intermediaries as proxy servers and gateways to exist between the client and the resources.

***Authentication***

Uses Oath2.0.

**Support for JSON and XML**

JSON is the default. You can use the HTTP ACCEPT header to select either JSON or XML, or append json or xml to the URI

# Compression

The REST API allows the use of compression on the request and the response, using the standards defined by the HTTP 1.1 specification. Compression is automatically supported by some clients, and can be manually added to others. For better performance.

Request compression: Add **Accept-Encoding: gzip** or **Accept-Encoding: deflate** in a request Header.

Response compression : in response header **Content-Encoding: gzip/Content-Encoding: deflate**

# Authorization Through Connected Apps and OAuth 2.0

A connected app requests access to REST API resources on behalf of the client application.

OAuth 2.0 is an open protocol that authorizes secure data sharing between applications through the exchange of tokens.

OAuth authorization flows grant a client app restricted access to REST API resources on a resource server. Each OAuth flow offers a different process for approving access to a client app, but in general the flows consist of three main steps.

1. a connected app, on behalf of a client app, requests access to a REST API resource.
2. In response, an authorizing server grants access tokens to the connected app.
3. A resource server validates these access tokens and approves access to the protected REST API resource.

# Perform Cross-Origin Requests from Web Browsers

Suppose a user visits http://www.example.com and the page attempts a cross-origin request to fetch the user's data from http://service.example.com. A CORS-compatible browser will attempt to make a cross-origin request to service.example.com.

In Salesforce, add the origin serving the code to a CORS allowlist.

1. enter CORS in the Quick Find box, then select **CORS**
2. **New**
3. **Enter a URL Pattern**

You can add (\*) wildcard at 2nd level domain, Example : https://\*.example.com .

If a browser that supports CORS makes a request to an origin in the allowlist, Salesforce returns the origin in the **Access-Control-Allow-Origin** HTTP header along with any additional CORS HTTP headers. If the origin isn’t included in the allowlist, Salesforce returns HTTP status code 403.

# Connected App and OAuth Terminology

<https://help.salesforce.com/articleView?id=sf.remoteaccess_terminology.htm&type=5>

**Access Token:** Instead of using the user’s Salesforce credentials, a consumer (connected app) can use an access token to gain access to protected resources on behalf of the user. For OAuth 2.0, the access token is a session ID and can be used directly.

**Authorization Code**: In Oath 2.0, The authorization code is used to obtain an access token and a refresh token. It expires after 15 minutes.

**Authorization Server:** server that authorizes a resource owner, and upon successful authorization, issues access tokens to the requesting consumer.

**Callback URL:** A callback URL is the URL that is invoked after OAuth authorization for the consume.

**OAuth Endpoint:** OAuth endpoints are the URLs that you use to make OAuth authorization requests to Salesforce.

**Consumer :** A consumer is the website or app that uses OAuth to authorize both the Salesforce user and itself on the user’s behalf. Referred to as client in OAuth 2.0.

**Consumer Key :**A consumer uses a key to identify itself to Salesforce. Referred to as client\_id in OAuth 2.0.

**Consumer Secret :** A consumer uses a secret to establish ownership of the consumer key. Referred to as client\_secret in OAuth 2.0.

**Refresh Token :** Only used in OAuth 2.0, a consumer can use a refresh token to obtain a new access token, without having the end user approve the access again.

**Resource Owner:** The resource owner is the entity (usually the end user) that grants access to a protected resource.

**Resource Server :** The resource server is the server that hosts the protected resource. Your Salesforce org is the resource server that protects your data.

**Token Secret :** A consumer uses this secret to establish ownership of a given token, both for request tokens and access tokens.

# Connected Apps

A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as Security Assertion Markup Language (SAML), OAuth, and OpenID Connect. Connected apps use these protocols to authorize, authenticate, and provide single sign-on (SSO) for external apps.

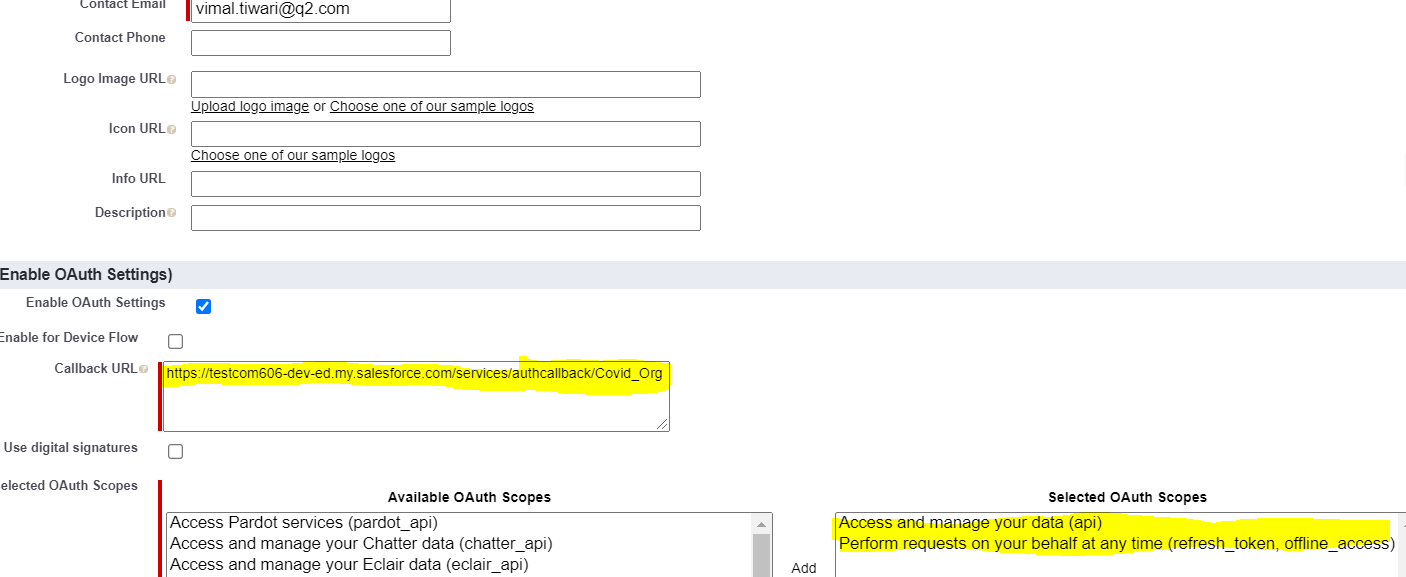
***Developers create and configure authorization flows for connected apps, and admins set policies and permissions to control connected app usage.***

1. **Access Data with API Integration**: web-based or mobile applications that need to pull data from your Salesforce org, you can use connected apps as the clients to request this data. Use OAuth 2.0 **Security**.
   1. Web Server integration – Web -> connected app -> Salesforce
   2. Mobile integration -> mobile to salesforce/ can use mobile SDK instead of connected app.
   3. Server to Server integration -> no need to be real time, can do authorization and authentication in advance by sending JSON WEB TOKEN or JWT
   4. IOT integration -> for devices like TV , having limited input capabilities.
2. **Integrate Service Providers with Salesforce**: SSO
   1. You want your users to be able to log in to their app with their Salesforce credentials. Using SAML 2.0 for user **authentication**.
   2. OpenID Connect is a protocol that enables SSO between two services, like SAML2.0. It adds an authentication layer on top of OAuth 2.0 to enable secure exchange of ID tokens that contain user information alongside OAuth access tokens.
3. **Provide Authorization for External API Gateways:** Using OpenID Connect dynamic client registration, resource servers can dynamically create client apps as connected apps in Salesforce, by sending request to authorization server. The authorization server verifies the resource server’s request and creates the connected app, giving it a unique client ID and client secret.

***Basic Rest Based data movement Demo using Connected App and OAuth2.0***

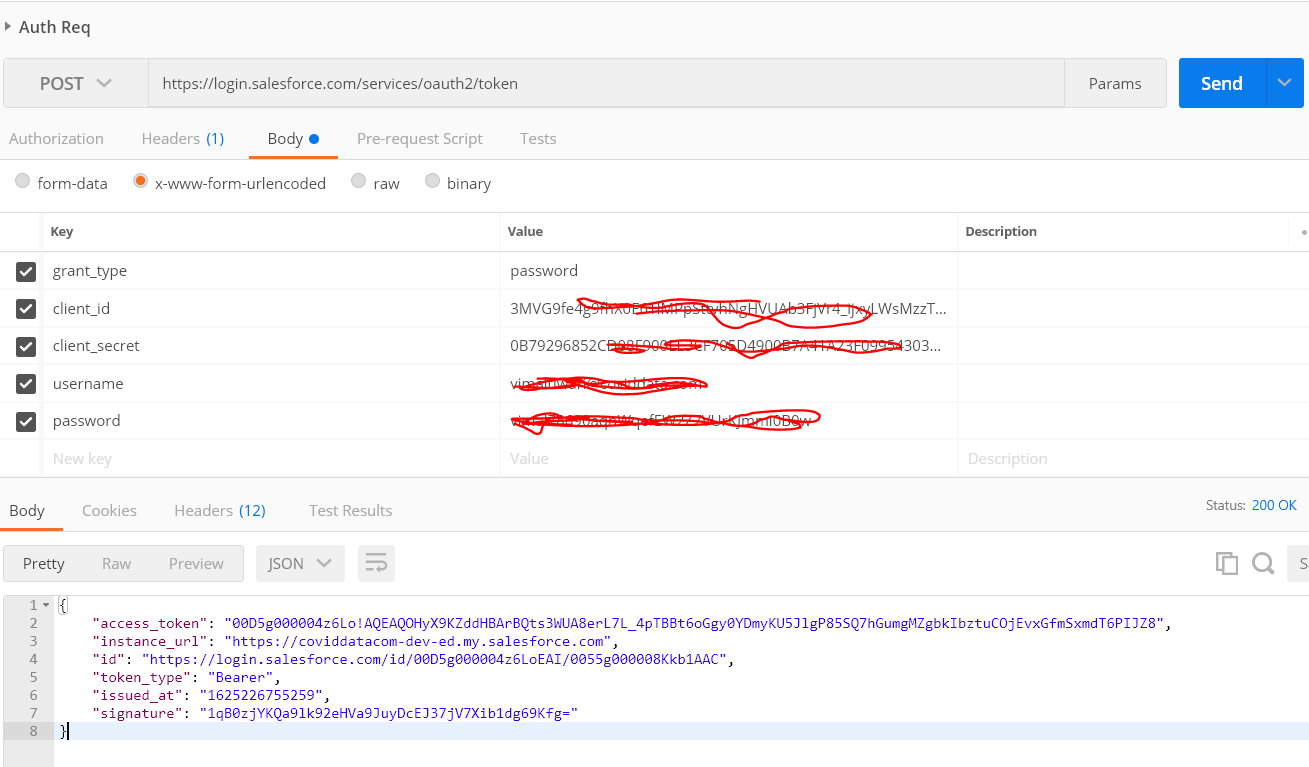
**Steps for Org 1 acting as Server.**

1. In response Server i.e. your org providing service, create Apex class for [Account Rest Services](https://github.com/vimaltiwari2612/Interview-Preparation/blob/master/Salesforce/AccountRestAPI.cls)
2. Create a connected App there.



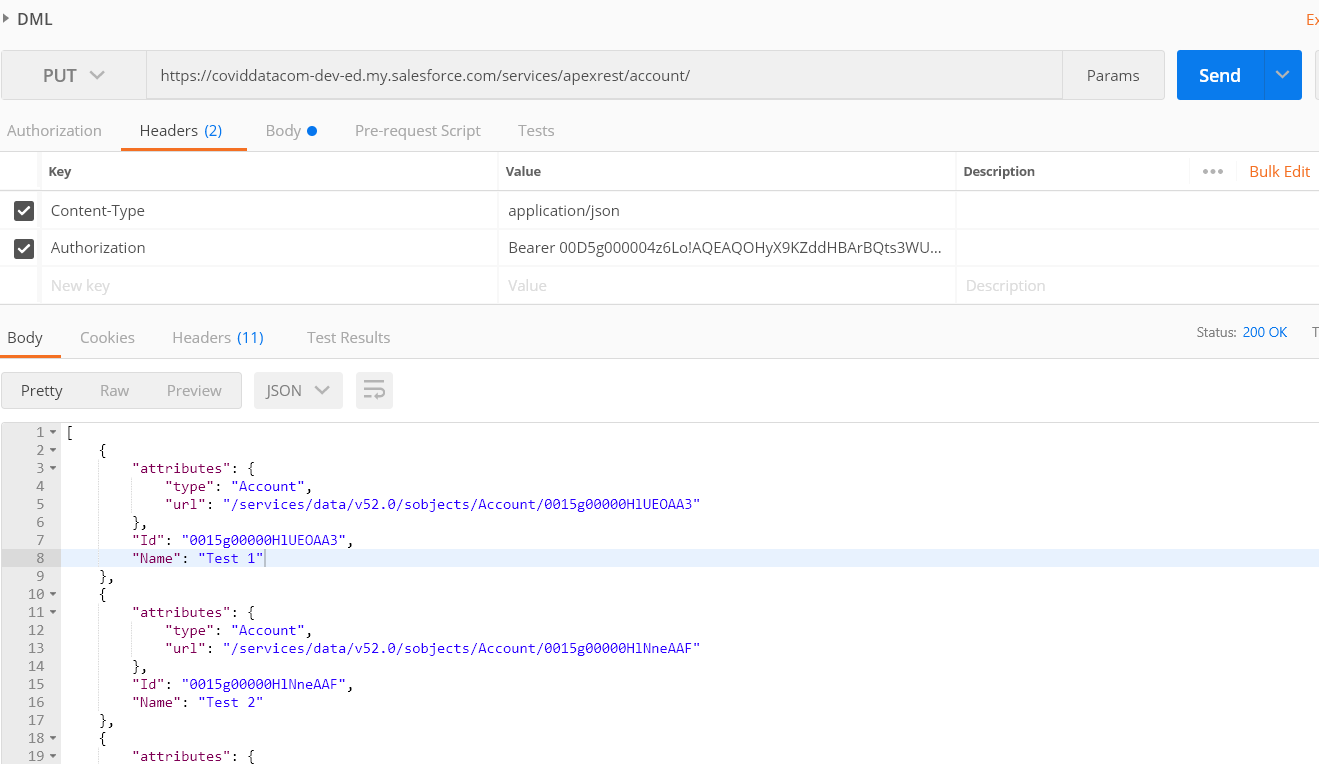
1. Use [Basic Tutorial of Rest API with Oauth2.0](https://medium.com/@salesforce.notes/salesforce-rest-api-tutorial-3bcd39e493f6) for creation and testing Rest Services.

**Auth** :



Rest Testing

**In authorization : Bearer <access-token>// bearer is a prefix**



**Steps for Org 2 acting as Client**

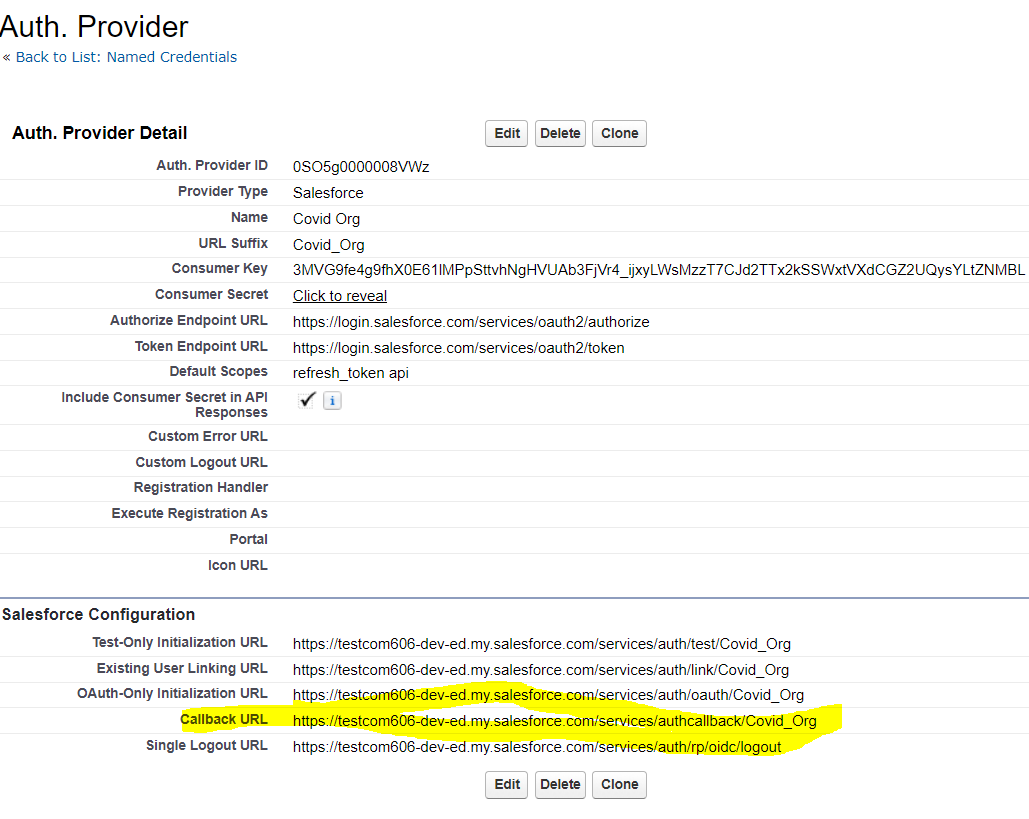
1. Create Authorization Provider – req. in Named Credentials
   1. Setup -> Auth. Provider
   2. Default scope – **refresh\_token full**

**refresh\_token** means – It will get updated token each time the existing token expires for authentication.

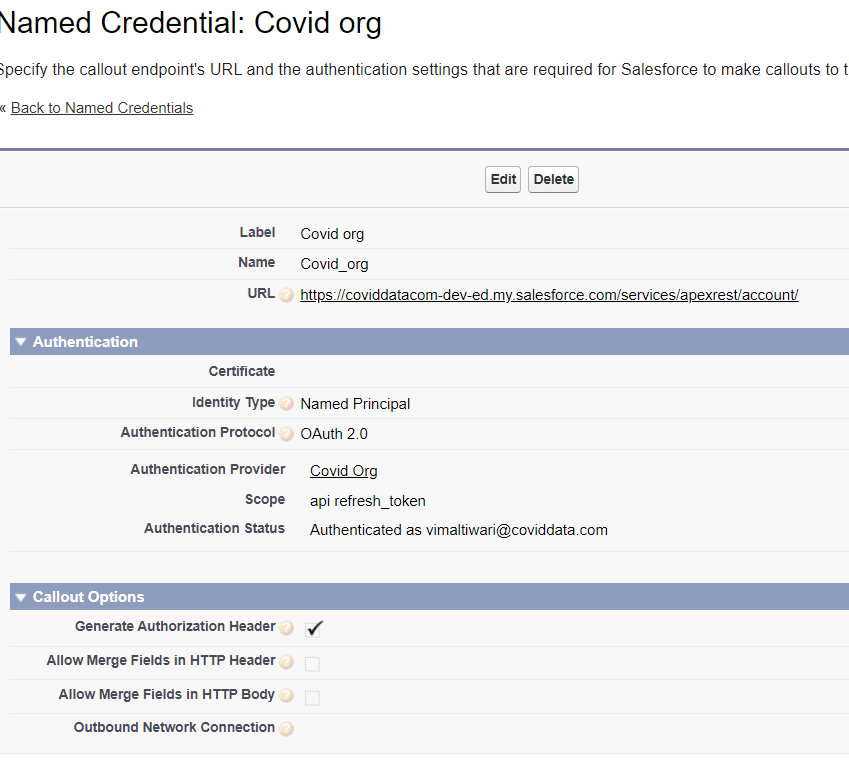
**full** means – full access,

**Api** – Api access.

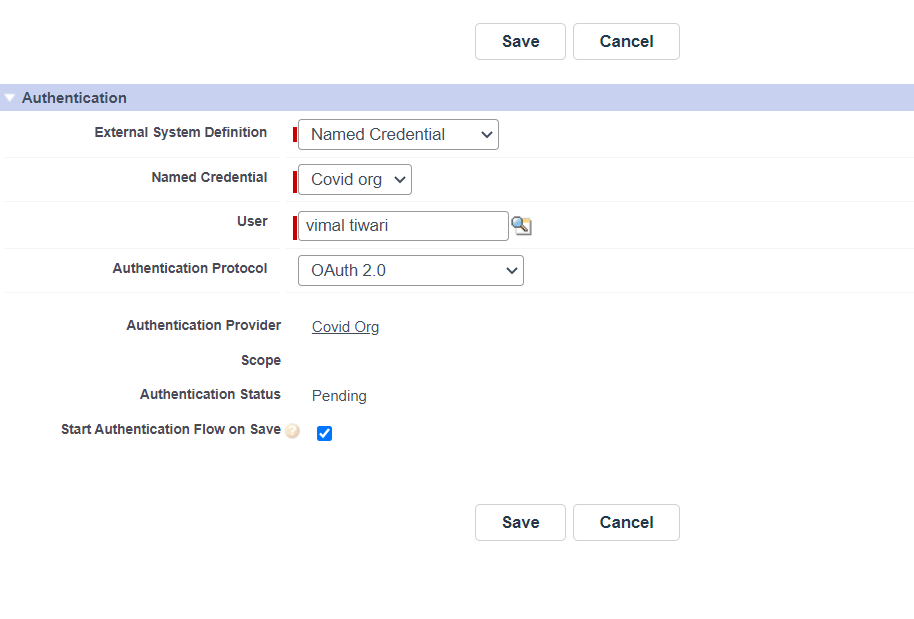
**Call back url – Need to be updated in call back field of connected app in org1.**



1. Create **Named Credentials**
   1. Provide Auth. Provider for Oauth 2.0
   2. Identity type –
      1. Per user – Api callout based on calling user’s context
      2. Named Principal – One user will be used for all callouts, might be the owner.
   3. URL : the base url.
   4. Authentication protocol – **if it is selected, that means system will take care of authentication. No need to do callout for authentication explicitly**.
   5. Authentication status should not be pending. If it is there, setup is not complete.
   6. **Generate authorization header** need to be checked, **if any Authentication protocol is selected.**



1. Give Access of Named Credential to Users – Need in case of **Per user** setting. I have used Permission set.
2. Authentication Settings for External Systems – **Needed in Per user setting**.
   1. Go to my settings -> personal -> Authentication Settings for External Systems
   2. Click new , add NC as external system definition.



1. It’s time to write some apex code and do some fun.

Create new class [**AccountRestClientWithOAuth2**](https://github.com/vimaltiwari2612/Interview-Preparation/blob/master/Salesforce/AccountRestClientWithOAuth2.cls) and use its methods to get and put data.

**For custom Authorization and callouts**:

1. Create remote site setting for base URL.
2. [AccountRestClient](https://github.com/vimaltiwari2612/Interview-Preparation/blob/master/Salesforce/AccountRestClient.cls)
   1. Call setAccessToken to get access token and set it in **platform cache and set time to live**. It is a field in seconds which can save the token expire time, based on server’s details. Ex. 10 min, 5 min etc.
   2. For each callout, check if token is there, then go for other methods
   3. Else refresh -> call the setAccessToken again and get new token, save it again in cache.

Reference :

<https://www.jitendrazaa.com/blog/salesforce/login-to-salesforce-from-salesforce-using-authentication-provider/#more-4516>

<https://developer.salesforce.com/docs/atlas.en-us.apexcode.meta/apexcode/apex_callouts_named_credentials.htm>

<https://salesforce.stackexchange.com/questions/102484/use-of-named-credentials-seem-to-be-tied-to-external-data-source>

**Integration Framework**

**Overview**: Since from UI, we can do real time callouts, because we can prevent user actions, for process based callouts, can’t do it real time. It can be near real time. The framework takes callout request from any context and saves it. Then there will be some process which takes the request Queue and process it.

**Classes Skeleton**

*global class ResponseWrapper{*

*global List<SubResponseWrapper> jsonResponses; // bulk Responses*

*global String returnCode;*

*}*

*global class RequestWrapper{*

*global String endpoint;*

*global List< SubRequestWrapper > bodies;//bulk Request*

*}*

*global abstract class* ***AbstractHTTPServiceClass****{*

*global abstract ResponseWrapper process(String httpType, RequestWrapper rw);*

*}*

*public class SampleHTTPServiceClass extends* ***AbstractHTTPServiceClass*** *{*

*public override ResponseWrapper process (String methodNam, RequestWrapper rw){*

*if(methodName == ‘getRecord’){*

*return getRecord(rw);*

*}else if …..*

*}*

*@httpGet*

*public ResponseWrapper getRecord(RequestWrapper rw){*

*Http h =new Http();*

*HttpRequest req = new HttpRequest();*

*req.setEndpoint(rw.endpoint);*

*HttpResponse res = h.send(req);*

*return new ResponseWrapper(res.getBody());*

*}*

*}*

**Data model**

1. **Integration Log** – to save the details of an integration callout that is to be called.
   1. Service config – Unique name of corresponding service meta data record.
      1. Can create String like “Service.ClassName.Method” etc
   2. Log Status – New, In Progress, Success, Failed.
   3. Retry count.
   4. Status code
   5. Child records - Notes and Attachment
      1. Save Request as file – Request in Json converted in file
      2. Save Response as file - Response in Json converted in file
2. **Service Configuration** – Custom Meta data to save callout information.
   1. Callout Service Class Name
   2. Callout method name – Method name
   3. END-POINT – Named credential name.
   4. Relative URL – service URL that gets added after End point.
   5. Max Retry count
   6. Request Wrapper class
   7. Response Wrapper class
3. **Exception log**– log exception per callout
   1. Error
   2. Error type
   3. Callout Id – Integration log id

**Execution**

1. **Add in Queue - From the Context, where Callout needs to be made**,
   1. Create Integration log by putting required Values.
      1. Provide the meta data records’ unique name to it.
      2. From the meta data,
         1. get the request Wrapper class Name,
         2. create JSON from wrapper.
         3. attach it on integration log as file.
      3. Mark status as In-Progress. As we cannot update it before Callout In same context.
2. **Process Queue** – Some process which takes the set of requests and process them one by one. For example, **Batch**, **Queueable** etc
   1. Get the set of Logs which are not successful yet.
   2. For each Integration log – that is in In-Progress.

Try{

* + 1. Take the meta data record from Pre-queried Meta data list.
    2. If retry count on log < Max retry in Meta data
       1. Get the service class name.
       2. Get the instance of Service class using Reflection. (Type.forName)
       3. Call the Service Class ***process*** method
          1. pass the method type from Meta data record.
          2. get the Request Json from Attachment file, create a RequestWrappper and pass it.
       4. The method will do **Callout**, and returns a response.
       5. If the return code is 200,
          1. update records status to Success.
          2. Get the Response Wrapper as response, Convert into JSON and save it on log’s attachment.
       6. Else
          1. increase the retry count.
          2. Change status of log to FAIL.
       7. Save the return code on Log record.

}catch(Exception e){

Use platform event to Create exception log record. And publish it.

}

* 1. Once the loop gets over. We can again go for retrying the failed logs. For this, don’t do step 6b . Let the log be in IN-Progress, and again trigger the same process.
  2. For some response codes, we don’t want to do anything such as 404, 403. In those cases, remove them from iterating list based on status codes.

**Bulk Request – Sending more than 1 log in single callout.**

**( Request + Response ) size can be 6 MB(sync) and 12MB(Async)**

In case of bulk Requests, the RequestWrapper will contain request for multiple records, and receives responses corresponding to each record in a single ResponseWrapper. Based on the responses, update individual logs.

**If the endpoint takes time to process i.e., possibility of Time out (time more than 120 sec), and response is not gonna be realtime.**

* 1. The Endpoint should some response to notify that, the process will take time.
  2. We will expose an endpoint from our system. That Endpoint will be hit by the other system once it finishes the processing.
  3. We will update the required records.

**Return type constraints for HTTP methods**

public, private, or global class member variables must be types allowed by Apex REST:

* Apex primitives (excluding sObject and Blob). – in wrapper, no Blob or sobjects can be sent.
* sObjects
* Lists or maps of Apex primitives or sObjects (only maps with String keys are supported).

**Request :**

global String string1;

global String string2 { get; set; }

private String privateString;

global transient String transientString; - won’t go in response

global static String staticString; - won’t go in response

**Response :**

{

"string1" : "value for string1",

"string2" : "value for string2",

"privateString" : "value for privateString"

}

**Named Credentials**

It specifies the URL of a callout endpoint and its required authentication parameters in one definition. It handles the authentication by itself, which is not possible in case of Remote site settings.

Fields

1. **URL**: Root/ BASE\_URL of endpoint.
2. **Certificate**: used for digital signature at the time of request.
3. **Identity Type**: Determines whether you're using one set or multiple sets of credentials to access the external system.
   1. **Anonymous**: No identity and therefore no authentication.
   2. **Per User**: Use separate credentials for each user who accesses the external system via callouts. Select this option if the external system restricts access on a per-user basis. After you **grant user access through permission sets or profiles in Salesforce**, users can manage their own authentication settings for external systems in their personal settings. Also set **Authentication Settings for External Systems, in my settings of that user for External Data source/NC.**
   3. **Named Principal**: Use the same set of credentials for all users who access the external system from your org. Select this option if you designate one user account on the external system for all your Salesforce org users.
4. **Authentication protocol**: secure communication between the two systems.
   1. **Password Authentication**: Username and password
   2. **OAuth2**.0
      1. **Authentication Provider**
      2. **Scope : provide the scope for access token. Some common scopes are**
         1. **“api” – allow current current logged in users account using API.**
         2. **“full” –** Allows access to all data accessible by the logged-in user. **full** doesn’t return a refresh token. You must explicitly request the **refresh\_token** scope to get a refresh token.
         3. **“refresh\_token”:** Allows a refresh token to be returned when the requesting client is eligible to receive one.
         4. “**refresh\_token, offline\_access** “: With a refresh token, the app can interact with the user’s data while the user is offline. This token is synonymous with requesting offline\_access
      3. **Start Authentication Flow on Save :** To authenticate to the external system and obtain an OAuth token.
   3. **JWT/ JWT Token Exchange** 
      1. **Issuer:** who issued the JWT
      2. **Scope:** Used in JWT token Exchange
      3. **Token End point:** Used in JWT Token Exchange, JSON Web Token requests are sent to the provider in exchange for access tokens.
      4. **Per User Subject**: In case per user selected, Per user identity like user Id.
      5. **Named Principal Subject**: In case named Principal selected. Provide some string specifies subject.
      6. **Audiences:** External service or other allowed recipients for the JWT.
      7. **Token Valid For:** Time for which token is valid, in Seconds, min, hours, days.
      8. **JWT Signing Certificate:** Certificate verifying the JWT’s authenticity to external system.
   4. **AWS Signature Version 4 -** A protocol to authenticate callouts to resources in Amazon Web Services over HTTP. **The identity type must be named principal.**
      1. **AWS Access Key ID**
      2. **AWS Secret Access Key**
      3. **AWS Region :** AWS region name for NC endpoint.
      4. **AWS service :** AWS utility to access.
5. **Custom Headers and Bodies of Apex Callouts**
   1. **Generate Authorization Header:** By default, Salesforce generates an authorization header and applies it to each callout that references the named credential.
   2. **Allow Merge Fields in HTTP Header** : HTMLENCODE can’t be used on merge fields in HTTP headers.

*// non-standard authentication*

*req.setHeader('X-Username', '{!$Credential.UserName}');*

*req.setHeader('X-Password', '{!$Credential.Password}');*

*// The external system expects “OAuth” as*

*// the prefix for the access token.*

*req.setHeader('Authorization', 'OAuth {!$Credential.OAuthToken}');*

* 1. **Allow Merge Fields in HTTP Body :** HTTP request bodies of callouts, you can apply the HTMLENCODE formula function to escape special characters.

*req.setBody('UserName:{!HTMLENCODE($Credential.Username)}')*

*req.setBody('Password:{!HTMLENCODE($Credential.Password)}')*

**Authentication Providers:** They authenticate users for SSO and authorize Salesforce to access protected third-party data.

**Setup**

Setup | Administer | Security Controls | Auth. Providers | Create New

1. “Consumer Key” and “Consumer Secret”.
2. “Default Scope“, it should have value as “refresh\_token full”. “refresh\_token” and “full” should be separated by space.
3. Authorize Endpoint URL should be something like: <https://AuthenticationProviderinstance/services/oauth2/authorize>
4. Token Endpoint URL: <https://AuthenticationProviderinstance/services/oauth2/token>
5. Once you save “Auth. Provider” in previous step, it will provide you list of URL **Copy Callback URL and edit Connected App we created in service provider Salesforce instance and paste link in callback URL field**.

**Streaming API**

Streaming API lets you push a stream of notifications from Salesforce to client apps based on criteria that you define.

1. Use Change data capture
2. Platform events
3. PushTopics and subscribe using Bayeus client.

A **PushTopic** is an sObject that contains the criteria of events you want to listen. PushTopic queries support all custom objects and some of the popular standard objects, such as Account, Contact, and Opportunity.

*PushTopic pushTopic = new PushTopic();*

*pushTopic.Name = 'AccountUpdates';*

***//The SELECT statement’s field list must include Id.***

***//aggregate queries or semi-joins aren’t supported.***

*pushTopic.Query = 'SELECT Id, Name, Phone FROM Account WHERE BillingCity=\'USA\'';*

*pushTopic.ApiVersion = 37.0;*

***//operation preferences, default all are true***

*pushTopic.NotifyForOperationCreate = true;*

*pushTopic.NotifyForOperationUpdate = true;*

*pushTopic.NotifyForOperationUndelete = true;*

*pushTopic.NotifyForOperationDelete = true;*

***//field preferences***

*pushTopic.NotifyForFields = ‘Referenced’;*

*insert pushTopic;*

| **NotifyForFields** | **Description** |
| --- | --- |
| All | Notifications are generated for all record field changes. |
| Referenced (default) | Changes to fields referenced in the SELECT and WHERE clauses are evaluated. |
| Select | Changes to fields referenced in the SELECT clause are evaluated. |
| Where | Changes to fields referenced in the WHERE clause are evaluated. |

**Soap API**

Web Services Description Language (WSDL) contains the bindings, protocols, and objects to make API calls. Salesforce provides two SOAP API WSDLs for two different use cases.

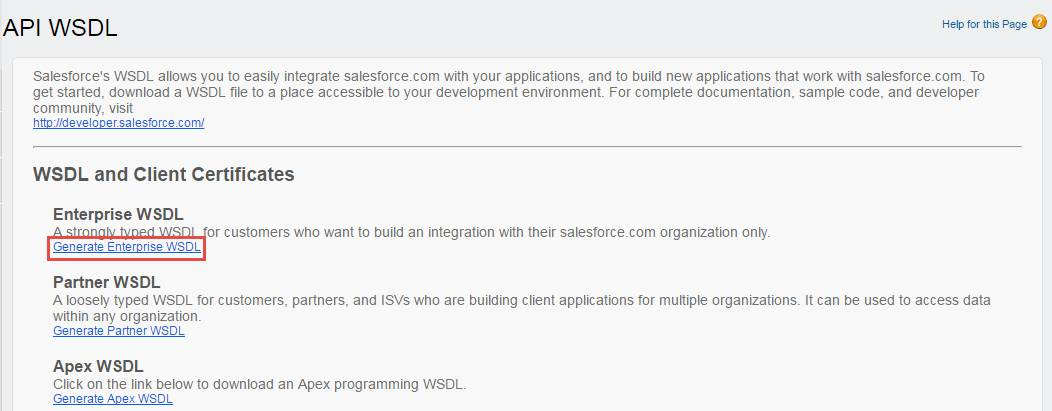
**The enterprise WSDL** - integration for single org

1. It is optimized for a single Salesforce org.
2. It’s strongly typed, and it reflects your org’s specific configuration.

**The partner WSDL -** integration for multiple org

1. is optimized for use with many Salesforce orgs.
2. It’s loosely typed, and it doesn’t change based on an org’s specific configuration.

**Setup-> quick find -> api**



**Demo using Soap Client**: <https://trailhead.salesforce.com/en/content/learn/modules/api_basics/api_basics_soap>

1. Install the soap client.
2. New soap project and upload WSDL. Once it is successful, it shows all the request that can be made to WSDL org.
3. Login-> request 1-> Provide username and password+Security Token
4. Once login is successful, you get Session ID and instance url.
5. For any other request, for example create, Use session Id in SessionHeader.
6. Hit Instance url, with the requests.

**Apex Callout using SOAP web Service**

1. Get the WSDL file, from resource server.
2. Convert wsdl to apex using WSDL2Apex. **The size of any WSDL document can be at most 1MB.**
3. The Apex classes construct the SOAP XML, transmit the data, and parse the response XML into Apex objects. Instead of developing the logic to construct and parse the XML of the web service messages, let the Apex classes generated by WSDL2Apex internally handle all that overhead.

**Expose a Class as a SOAP web Service**

**Source System.**

1. **Define your class as global**.
2. Add the **webservice** keyword and the **static** definition modifier to each method you want to expose.
3. **The webservice keyword provides global access to the method it is added to.**

*global with sharing class MySOAPWebService {*

*webservice static Account getRecord(String id) {*

*// Add your code*

*}*

*}*

1. Generate this WSDL for your class and send it to target developers.
2. For Authentication, external applications must use either the Enterprise WSDL or the Partner WSDL for login functionality.

**Target System:**

1. Go to Apex Classes an Click button "Generate from WSDL" using WSDL .
2. Genersate class from Webservice WSDL. It will generate 2 classes. One for Sync and other for Async calling, i.e. future based.
3. Generate another Class with Enerprise/partner WSDL. It will have all standard meta data methods, like describe() calls, login, logout, create, insert etc
4. Develop a class in Target system where you generated apex class to use **Login** method of Enterprise/ partner WSDL using credentials from Source.
5. Then call the SOAP method developed.

*classGeneratedByWSDL. MySOAPWebService instance = new classGeneratedByWSDL. MySOAPWebService();*

*instance.getRecord(id);*

***when should you use REST vs SOAP?***

1. **If developing public APIs**, in which you don’t have to control over whats going on with he consumer.
2. **APIs that require, a lot of back-and-forth messaging**, with SOAP being stateful the same type of service would require more initialization and state code. Because REST is stateless, the client context is not stored on the server between requests, giving REST services the ability to be retried independently of one another.
3. **Services, that do not need connection all the time** - SOAP services require maintaining an open stateful connection with the client. REST, in contrast, enables requests that are completely independent of each other.
4. **Json response is easy to parse and lightweight. So, response will be quick**.

**Which API Do I Use?**

| **API Name** | **Protocol** | **Data Format** | **Communication** | **When to Use** |
| --- | --- | --- | --- | --- |
| REST API | REST | JSON, XML | Synchronous |  |
| SOAP API | SOAP (WSDL) | XML | Synchronous | SOAP API to create, retrieve, update, or delete records. You can also use SOAP API to perform searches and much more. |
| Chatter REST API | REST | JSON, XML | Synchronous (photos are processed asynchronously) | For chatter based use cases. |
| User Interface API | REST | JSON | Synchronous | Build Salesforce UI for native mobile apps and custom web. |
| Analytics REST API | REST | JSON, XML | Synchronous | For gathering datasets from Analytics Platform |
| Bulk API | REST | CSV, JSON, XML | Asynchronous | Submits a batch for use cases, |
| Metadata API | SOAP (WSDL) | XML | Asynchronous | migrate customization changes |
| Streaming API | Bayeux | JSON | Asynchronous (stream of data) | For near-real-time streams of data that are based on changes in Salesforce records or custom payloads. |
| Apex REST API | REST | JSON, XML, Custom | Synchronous |  |
| Apex SOAP API | SOAP (WSDL) | XML | Synchronous |  |
| Tooling API | REST or SOAP (WSDL) | JSON, XML, Custom | Synchronous | fetch the metadata such as Apex classes, Apex triggers, custom objects, custom fields, etc. If we need to get the list of Custom Objects or Custom fields |

***Platform cache***

1. Using cached data improves the performance of your app and is faster than performing SOQL queries repetitively, making multiple API calls, or computing complex calculations.
2. Use the cache to store static data or data that does not change often.
3. Salesforce evicts cached data based on a least recently used (LRU) algorithm

**Types Of Cache**

1. **Org cache** stores org-wide data that anyone in the org can use.
   1. *time-to-live – Max 48 hours, default is 24 hours*.
2. **Session cache** stores data for an individual user and is tied to that user’s session. The maximum life of a session is 8 hours. Min is 300 sec.

**Partitions:** Caching data to designated partitions ensures that the cache space is not overwritten by other apps or by less critical data.

Cache.Org.put('namespace.partition.key', 0, TTL(optional));

Among all partitions, **there can be only one default partition**. In Default partition, we don’t have to use the fully qualify the key name with the namespace and partition name when adding a key-value pair.

Cache.Org.put('key', 0, TTL(optional));

**Namespace.Partition.Key is the cache key Name format.**

1. Namespace – org namespace. Can use “local” too.
2. Partition – partition name.
3. Key – the key which needs to be put.

**Store and Retrieve Data in Org Cache**

*// Get partition*

***Cache.OrgPartition orgPart = Cache.Org.getPartition('local.CurrencyCache');***

*// Add cache value to the partition. Usually, the value is obtained from a*

*// callout, but hardcoding it in this example for simplicity.*

***orgPart.put('DollarToEuroRate', '0.91');***

*// Retrieve cache value from the partition*

***String cachedRate = (String)orgPart.get('DollarToEuroRate');***

***if (cachedRate != null) {***

*// Display this exchange rate*

***} else {***

*// We have* ***a cache miss****, so fetch the value from the source.*

*// Call an API to get the exchange rate.*

***}***

**Store and Retrieve Data in Session Cache**

*// Get partition*

***Cache.SessionPartition sessionPart = Cache.Session.getPartition('local.CurrencyCache');***

*// Add cache value to the partition*

***sessionPart.put('FavoriteCurrency', 'JPY');***

*// Retrieve cache value from the partition*

***String cachedRate = (String)sessionPart.get('FavoriteCurrency');***

**remove () :- to delete an item from cache**.

**MAX\_TTL\_SECS**: A constant in Org and Session class represents maximum amount of time, in seconds, to keep the cached value in the session cache.

Aggregate functions are available only for the Cache.Org class.

**Don’t add many small items to the Platform Cache within one request. Instead, wrap data in larger items, such as lists, Wrapper Class.**

Access cached values stored in the platform cache from a Visualforce page by using the **$Cache.Session** or **$Cache.Org** global variables.

**$Cache.Session.namespace.partition.key**

**$cache.org. namespace.partition.key**

***Encryption-Decryption - Classic encryption***

1. **EncodingUtil**

* Blob base64Decode(String inputString)
* String base64Encode(Blob inputBlob)
* Blob convertFromHex(String inputString)
* String convertToHex(Blog inputBlob)
* String urlDecode(String inputString, String encodingScheme)
* String urlEncode(String inputString, String encodingScheme)

Note: for URL encode and decode second parameter will be encoding scheme i.e., UTF-8. All methods are static so you can call by class name.

1. **Crypto**

Provides methods for creating digests, message authentication codes, and signatures, as well as encrypting and decrypting information. These functions are using AES algorithm to generate the private key and these functions are using AES128, AES256, AES192 algorithms to encrypt and decrypt information. The AES algorithm requires initialization vector to encrypt and decrypt data. **AES stands for Advanced Encryption Standard algorithm**

*// Security key must be 16 characters string*

***public static key=Crypto.generateAesKey(128);***

*public static String encodeString(String encodingString){*

*Blob blobData =* ***Crypto.encryptWithManagedIV('AES128', key, Blob.valueOf(encodingString));***

*return EncodingUtil.base64Encode(blobData);*

*}*

*public static String decodeString(String str){*

*Blob blobData = EncodingUtil.base64Decode(str);*

*Blob decryptedBlob =* ***Crypto.decryptWithManagedIV('AES128', key, encodedEncryptedBlob);***

*return decryptedBlob.toString();*

*}*

***Platform encryption - Shield Platform Encryption***

Classic encryption uses 128-bit (AES) keys. Shield Encryption uses a stronger 256-bit AES key.

**tenant** secrets are used to derive your encryption keys. They work with the Salesforce-generated master secret, but your tenant secret is specific to your org.

Setup

1. Provide access to **Manage Encryption Keys** (System permission) to user.
2. Go to **Key Management** and **Generate Tenant Secret**. Export it.
3. Go to **Encryption Policy,** choose **Encrypt fields** and select required ones.
4. Destroy the key. Data will be encrypted now.
5. Upload the key to see the data again.

***Outbound messaging In workflows***

Outbound messaging allows you to specify that changes to fields within Salesforce can cause messages with field values to be sent to designated external servers.

It Uses SOAP API.

***Authorization vs Authentication***

*Authorization means, the user is allowed to access the data.*

*Authentication means, who the user is.*

Authentication Techniques

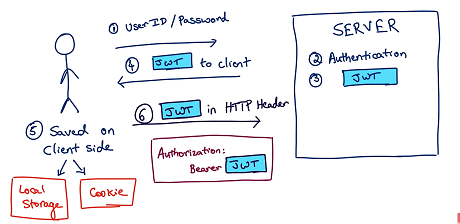
1. **Basic Auth** – Username & Password
2. **Bearer / Token based**
   1. **OAuth 1.0** – get access token by using client key and client secret. Use it for further requests. It is only for web apps.
   2. **OAuth 2.** – same work as OAuth 1.0.
      1. Added delegation of security to Transport layer. So only necessary data is transfers to TL. Also, supports multiple client mode, not only web.
      2. OAuth2 also introduced the use of refresh tokens that allow authentications to expire, unless “refreshed” on a periodic basis.
      3. ***The password grant is one of the simplest OAuth grants and involves only one step.***
3. ***SAML*** *-* Security Assertion Markup Language (**SAML**) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). Generally used for SSO.

**Authorization Techniques**.

1. **API-keys** – using a unique key in header for each service.
2. **Basic Auth** – verify Credentials and decide.
3. **HMAC (Hash-based message authorization code**) – Server and client have a secret key. Sender creates a message , encrypt by key and convert into hash by secure hasing algo. The it is sent to Receiver. Receiver will decodes the value using SHA and secret key, and verify the message.
4. **OAuth 2.0**
5. **JWT**

***JWT - JSON WEB TOKEN – For Authorization NOT Authentication***

**The JWT Bearer Flow** is an OAuth flow in which an external app (also called client or consumer app) sends a signed JSON string to Salesforce called JWT to obtain an access token. The access token can then be used by the external app to read & write data in Salesforce.



**Why JWT?**

*For authorization, we can use Session Ids. By the problem with the session ids are*

1. *The server needs to cache the session Ids to identify the user.*
2. *If there are multiple servers, we need a shared cache which saves session Ids.*
3. *If cache failed, user needs to authenticate again.*

*With JWT, Server doesn’t need to save any kind of data, for any user. At the time of authentication. Servers gives User a signed JWT with a private key and creates a signature., which the users need to use every time while requesting. In each request, the JWT comes, and server verifies the signature and authorizes the user.*

Unlike some other OAuth Flows, the JWT flow does not require end-user interaction to operate. The external app sends the JWT and authenticates itself without manual intervention.

Steps

1. Generate a private Key and a digital Certificate.
2. Create connected app and upload digital certificate. **We need to pre-authenticate it once**, because JWT is for authorization not for authentication .
   1. Hit below URL.

**https://<yourinstance>.salesforce.com/services/oauth2/authorize?response\_type=token&client\_id=<consumer key>&redirect\_uri=sfdc://oauth/jwt/success**

* + 1. Either by Web server
    2. User-Agent OAuth Flow

1. Create JWT.
   1. Header – Algo and type

{  
"alg": "RS256",  
"typ": "JWT"  
}

* 1. JWT Claim –
     1. Issuer – consumer key
     2. Subject – username
     3. Audience – login.salesforce.com
     4. Expiration – now + time

{  
"iss": "Consumer key",  
"sub": "[U](mailto:toufik.atba@gmail.com)sername",  
"aud": "[https://<login or test>.salesforce.com](https://login.salesforce.com/)",  
"exp": "now + 2 minutes in Unix timestamp"  
}

* 1. Base64 URL encode the Header and the Claims.

jwt\_part1 = Base64URLencode(JWT Header);  
jwt\_part2 = Base64URLencode(JWT Claims);

* 1. Using the private key sign the encoded header and claims separated by a dot using SHA256 with RSA

jwt\_signature = sign\_sha256\_RSA( jwt\_part1+"."+jwt\_part2, "private key")

1. Build the final JWT assertion – header + claim + signature.

jwt\_assertion = jwt\_part1+"."+jwt\_part2+"."+jwt\_signature

1. Create a post request.

*POST* ***https://login.salesforce.com/services/oauth2/token***

***Header****:*

***Content-Type****: application/x-www-form-urlencoded*

***Body***

***grant\_type****=urn:ietf:params:oauth:grant-type:jwt-bearer*

***assertion****=<put the jwt assertion here>*

***OR***

***Authorization= Bearer <JWT*** *assertion* ***>***

1. Response will be having **access\_token,** which can be used in subsequent requests to perform allowed operations in Salesforce.

Reference : <https://medium.com/@salesforce.notes/salesforce-oauth-jwt-bearer-flow-cc70bfc626c2>

[***https://medium.com/swlh/how-json-web-tokens-work-211ce7b705f7***](https://medium.com/swlh/how-json-web-tokens-work-211ce7b705f7)

# OAuth 2.0 Authorization Errors

|  |  |
| --- | --- |
| access\_denied | User denied access to the client app. |
| authorization\_pending | For the device flow, the user hasn’t approved the device for access. |
| immediate\_unsuccessful | The immediate parameter is set to true, and the user isn’t logged in or hasn’t previously approved the client’s access. |
| inactive\_org | Org is locked, closed, or suspended. |
| inactive\_user | User is set to inactive by the org’s admin. |
| invalid\_app\_acess | User isn’t approved by an admin to access this app. |
| invalid\_assertion\_type | Specified assertion type isn’t supported. |
| invalid\_client\_credentials | Client secret is invalid. |
| invalid\_client\_id | Client identifier is invalid. |
| invalid\_grant | One of the following:   * Invalid authorization code. For the SAML assertion flow, make sure that the client sends a URL-encoded assertion and assertion\_type. * Invalid user credentials. * Invalid user. * Invalid assertion. * Invalid audience. * IP restricted or invalid login hours. * Indicates that the code\_verifier value was invalid (not base64 encoded, for example) or wasn’t the valid verifier for the given code\_challenge. * Indicates that a code\_challenge wasn’t specified, so the code\_verifier wasn’t expected but was specified. * User hasn’t approved the connected app. * Authentication failure. * For the device flow, the device flow isn’t enabled for the connected app or the Salesforce server isn’t able to grant an access token. * For the refresh token flow, the refresh or access token is expired. |
| invalid\_request | One of the following errors.   * HTTPS is required. * HTTP GET is required. * HTTP POST is required. * The code\_challenge value was invalid, such as not being base64 encoded. * Flow doesn’t support and didn’t expect a code\_challenge parameter. * Out-of-band isn’t supported. * The JWT bearer and SAML assertion bearer flows require a refresh\_token scope. Install and preauthorize the app. * For the device flow, the device code specified in the polling request is invalid. * For the username-password flow, the scope parameter isn’t supported. * For the refresh token flow, the secret type isn’t supported. |
| invalid\_scope | The requested scope is invalid, unknown, or malformed. |
| rate\_limit\_exceeded | Number of login attempts has been exceeded. |
| redirect\_uri\_mismatch | Redirect URI mismatch with connected app definition. |
| redirect\_uri\_missing | Redirect URI not provided. |
| server\_error | The number of authorization requests from the client app exceeds the hourly limit. |
| slow\_down | For the device flow, the client app is polling the authorization server more frequently than the recommended minimum interval. |

***CrypotGraphy***

**Symmetric algorithms** - A single key is used to encrypt data.

**Asymmetric algorithms** -Two keys are used to encrypt and decrypt messages. While one key(public) is used to encrypt the message, the other key(private) can only be used to decrypt it.

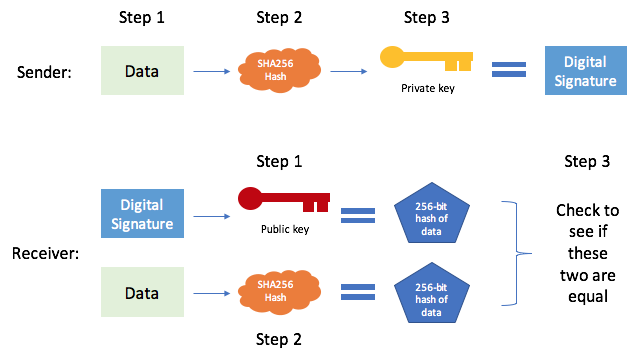
**HS256 and RS256 Scenario**

**HS256 can create a signature for a given sample of data using a single key**.

**RS256 uses pair of keys to do the same. A signature can only be generated using the private key. And the public key has to be used to verify the signature**.

Digital Signature

SHA256 – Secure hashing algo generated 256 bit hashed bits.



***OAuth 2.0***

***Grant Types* - 5 grant\_type for acquiring an access token:**

* **Authorization code grant –** signed into an application using your Facebook or Google account.
  1. Get authorization code from authorization Server.

Request - *GET (Authorization Endpoint)*

*?response\_type=code*

*&client\_id={CLIENT ID}*

*&redirect\_uri={REDIRECT URI}*

*&scope={SCOPES}*

*&state={STATE}*

Response - *LOCATION : {REDIRECT URI}*

*?code={AUTHORIZATION CODE}*

*&state={STATE}*

* 1. Send Post request Token Endpoint with AUTHORIZATION CODE

Request - POST (Token Endpoint)

Authorization : Basic <BASE64({CLIENT ID}:{CLIENT SECRET})>

**grant\_type=authorization\_code**

&code={AUTHORIZATION CODE}

&redirect\_uri={REDIRECT URI}

Response –

{

*"access\_token" : {ACCESS TOKEN},*

*"token\_type" : {TOKEN TYPE >> Bearer},*

*"refresh\_token" : {REFRESH TOKEN},*

*"expires\_in" : {Lifetime in seconds}*

*}*

* **Implicit grant -** It is intended to be used for user-agent-based clients (e.g. single page web apps) ***that can’t keep a client secret because all of the application code and storage is easily accessible.*** Secondly instead of the authorization server returning an authorization code which is exchanged for an access token, **the authorization server returns an access token directly.**

**Request -**

GET (Authorization Endpoint)  
?response\_type=token  
&redirect\_uri={REDIRECT URI}  
&scope={SCOPES}  
&state={STATE}

**Response –**

LOCATION : {REDIRECT URI}  
#access\_token={ACCESS TOKEN}  
&token\_type={TOKEN TYPE >> Bearer}  
&expires\_in={EXPIRES IN}  
&state={STATE}

* **Resource owner credentials grant – Grant type is password**

POST (Token Endpoint)  
Authorization: Basic <BASE64({CLIENT ID}:{CLIENT SECRET})> **grant\_type=password** &username={USERNAME}  
 &password={PASSWORD}  
 &scope={SCOPES}

* **Client credentials grant -** this grant is suitable for machine-to-machine authentication where a specific user’s permission to access data is not required. uses the client\_id and the client\_secret credentials of a Client to authorize and access protected data from a Resource Server.

POST (Token Endpoint)  
Authorization : Basic <BASE64({CLIENT ID}:{CLIENT\_SECRET})> grant\_type=client\_credentials  
 &scope={SCOPES}

* **Refresh token grant -** The Refresh Token Grant Flow is specially used to gain new access\_token from the Authorization Server by providing the refresh\_token to the Token Endpoint.

POST (Token Endpoint)  
Authorization : Basic <BASE64({CLIENT ID}:{CLIENT SECRET})> **grant\_type=refresh\_token**  
 refresh\_token={REFRESH TOKEN}  
 scope={SCOPES}

<https://athiththan11.medium.com/oauth-2-grant-types-a-story-guide-582580a3c4c2>

***Caching in Rest -***

When a consumer requests a resource representation, the request goes through a cache or a series of caches (local cache, proxy cache, or reverse proxy) toward the service hosting the resource. If any of the caches along the request path has a fresh copy of the requested representation, it uses that copy to satisfy the request. If none of the caches can satisfy the request, the request travels to the service (or origin server as it is formally known).

* Usually, browsers treat all GET requests cacheable.
* POST requests are not cacheable by default but can be made cacheable
  1. if either an **Expires** header or
     1. The Expires HTTP header specifies an absolute expiry time for a cached representation

**Expires: Fri, 20 May 2016 19:20:49 IST**

* 1. a **Cache-Control** header with a directive, to explicitly allows caching, is added to the response. These directives determine whether a response is cacheable, and if so, by whom, and for how long e.g. max-age or s-maxage directives.

**Cache-Control: max-age=3600**

* Responses to PUT and DELETE requests are not cacheable at all.

**Application layer Protocols**

**HTTP –**

Codes

* **1xx: Informational** – Communicates transfer protocol-level information.
* **2xx: Success** – Indicates that the client’s request was accepted successfully.
* **3xx: Redirection** – Indicates that the client must take some additional action in order to complete their request.
* **4xx: Client Error** – This category of error status codes points the finger at clients.
* **5xx: Server Error** – The server takes responsibility for these error status codes.

Examples

* **200** – OK - request has been successful. Generally GET/POST
* **201** – Created – new resource has been created. POST/PUT
* **202** – long running process
* **204** – Request Successful but doesn’t need to return anything – Delete/Patch
* **304** – for caching – if response has not been modified, can use same cached response, if it gets modified, 200 will come.
* **400** - can’t understand the request & process a request due to a client error. Missing data, domain validation, and invalid formatting
* **401** – Authentication failed
* **403** – Request is valid, but not authorized to access some resources, permission needed.
* **404** – Resource not found
* **409** – When the resource is already being used by some other process.
* **410** - Resource requested is no longer available and will not be available again.
* **500** – Request can’t be completed due to unexpected issue. Need to log issue and debug.

**Transport layer protocols**

| ***Transmission control protocol (TCP)*** | ***User datagram protocol (UDP)*** |
| --- | --- |
| TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data. | UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission. |
| TCP is reliable as it guarantees the delivery of data to the destination router. | The delivery of data to the destination cannot be guaranteed in UDP. |
| TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgement of data. | UDP has only the basic error checking mechanism using checksums. |
| Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver. | There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer. |
| TCP is comparatively slower than UDP. | UDP is faster, simpler, and more efficient than TCP. |
| Retransmission of lost packets is possible in TCP, but not in UDP. | There is no retransmission of lost packets in the User Datagram Protocol (UDP). |
| TCP has a (20-60) bytes variable length header. | UDP has an 8 bytes fixed-length header. |
| TCP is heavy weight. | UDP is lightweight. |
| TCP does not support Broadcasting. | UDP supports Broadcasting. |
| TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet. | UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP. |

# Integration Patterns and Practices

## **List of Patterns**

| **Pattern** | **Scenario** |
| --- | --- |
| [Remote Process Invocation—Request and Reply](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_remote_process_invocation_state.htm) | Salesforce invokes a process on a remote system, waits for completion of that process, and then tracks state based on the response from the remote system.  Example : Calling Rest/Soap callout in Sync  Remote Process Invocation - State Tracking Using Lightning |
| [Remote Process Invocation—Fire and Forget](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_remote_process_invocation_fire_forget.htm) | Salesforce invokes a process in a remote system but doesn’t wait for completion of the process. Instead, the remote process receives and acknowledges the request and then hands off control back to Salesforce.  Example :   1. Platform events, 2. Outbound msgs, 3. future methods and do callouts.   Remote Process Invocation - Fire and Forget Pattern |
| [Batch Data Synchronization](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_batch_data_sync.htm) | Data stored in Salesforce is created or refreshed to reflect updates from an external system, and when changes from Salesforce Platform are sent to an external system. Updates in either direction are done in a batch manner.   1. Salesforce Change Data Capture – near real time – to insert into other system.   Batch Data Syncrhonization Pattern - Salesforce Master   1. Salesforce Bulk API to insert in salesforce |
| [Remote Call-In](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_remote_call_in.htm) | Data stored in salesforce Platform is created, retrieved, updated, or deleted by a remote system.  Remote Call In - Remote System Calling In Using REST APIRemote Call In - Remote System Calling In Using SOAP API |
| [UI Update Based on Data Changes](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_ui_updates_from_data_changes.htm) | The Salesforce user interface must be automatically updated as a result of changes to Salesforce data.  The recommended solution to this integration problem is to use the Salesforce Streaming API   * A PushTopic with a query definition that allows you to: * Specify what events trigger an update * Select what data to include in the notification * A JavaScript-based implementation of the Bayeux protocol (currently CometD) that can be used by the user interface * A Visualforce page or Lightning component * A JavaScript library included as a static resource   UI Update Based on Data Changes Pattern |
| [Data Virtualization](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_data_virtualization.htm) | Salesforce accesses external data in real time. This removes the need to persist data in Salesforce and then reconcile the data between Salesforce and the external system. It consists of view, search, and modify data that is stored outside of Salesforce, without moving the data from the external system into Salesforce.   1. Salesforce Connect - Salesforce Connect maps data tables in external systems to external objects in your org. External objects are similar to custom objects, except that they map to data located outside your Salesforce org. 2. Request-Reply pattern   Data virtualization using Salesforce Connect |

## **Pattern Selection Matrix**

| **Source/Target** | **Type** | | | **Timing** | | **Key Patterns to Consider** |
| --- | --- | --- | --- | --- | --- | --- |
| **Process Integration** | **Data Integration** | **Virtual Integration** | **Synchronous** | **Asynchronous** |
| Salesforce –> System | X |  |  | X |  | [Remote Process Invocation—Request and Reply](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_remote_process_invocation_state.htm) |
|  | X | [Remote Process Invocation—Fire and Forget](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_remote_process_invocation_fire_forget.htm) |
|  | X |  | X |  | [Remote Process Invocation—Request and Reply](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_remote_process_invocation_state.htm) |
|  | X | [UI Update Based on Data Changes](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_ui_updates_from_data_changes.htm) |
|  |  | X | X |  | [Data Virtualization](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_data_virtualization.htm) |
| System –> Salesforce | X |  |  | X |  | [Remote Call-In](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_remote_call_in.htm) |
|  | X | [Remote Call-In](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_remote_call_in.htm) |
|  | X |  | X |  | [Remote Call-In](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_remote_call_in.htm) |
|  | X | [Batch Data Synchronization](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_batch_data_sync.htm) |

[*https://developer.salesforce.com/docs/atlas.en-us.224.0.integration\_patterns\_and\_practices.meta/integration\_patterns\_and\_practices/integ\_pat\_intro\_overview.htm*](https://developer.salesforce.com/docs/atlas.en-us.224.0.integration_patterns_and_practices.meta/integration_patterns_and_practices/integ_pat_intro_overview.htm)