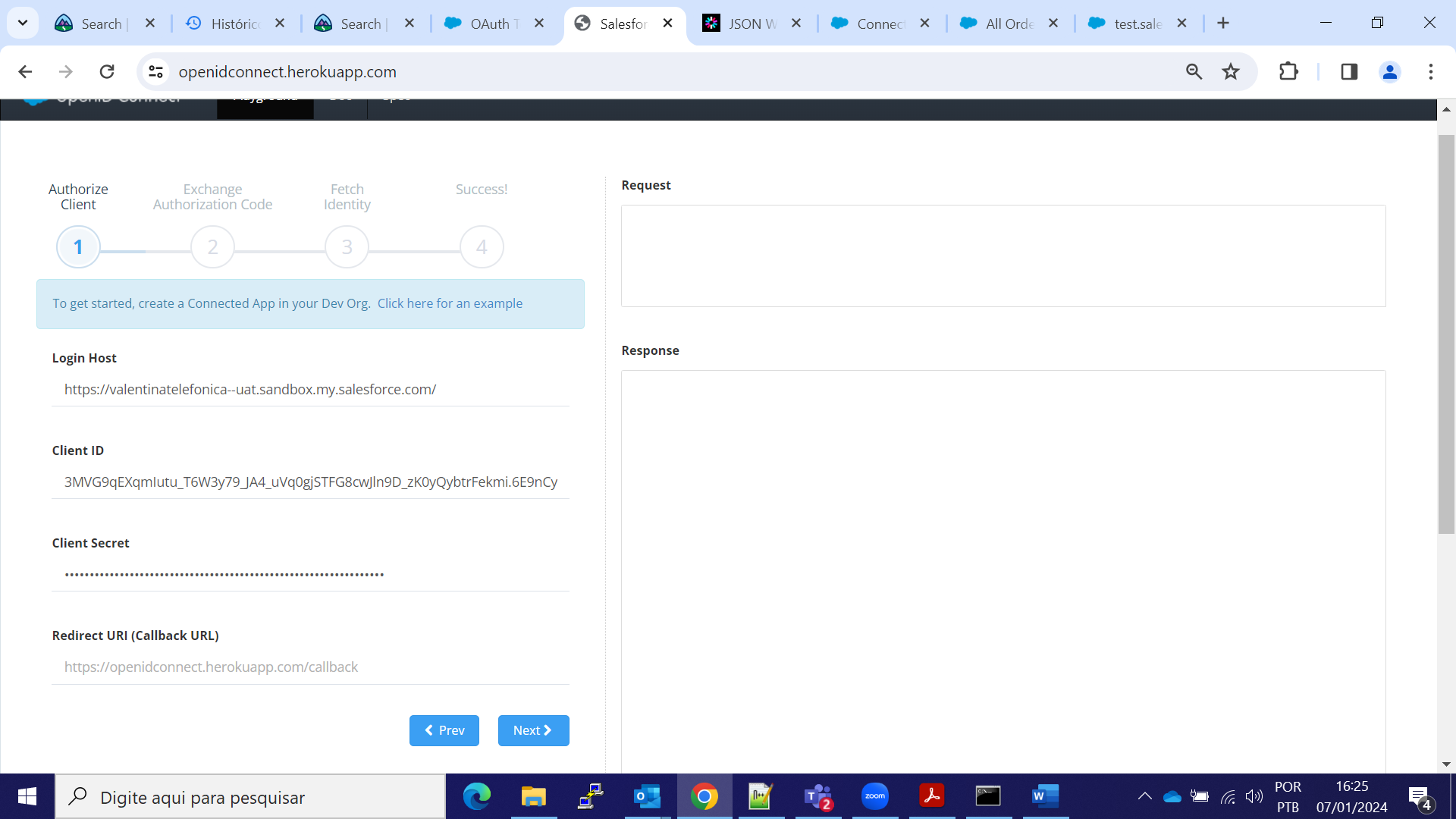
Aplicativo para simular a chamada ao Salesforce: <https://openidconnect.herokuapp.com/>

Trilha Salesforce: <https://trailhead.salesforce.com/content/learn/projects/build-a-connected-app-for-api-integration/implement-the-oauth-20-web-server-authentication-flow>

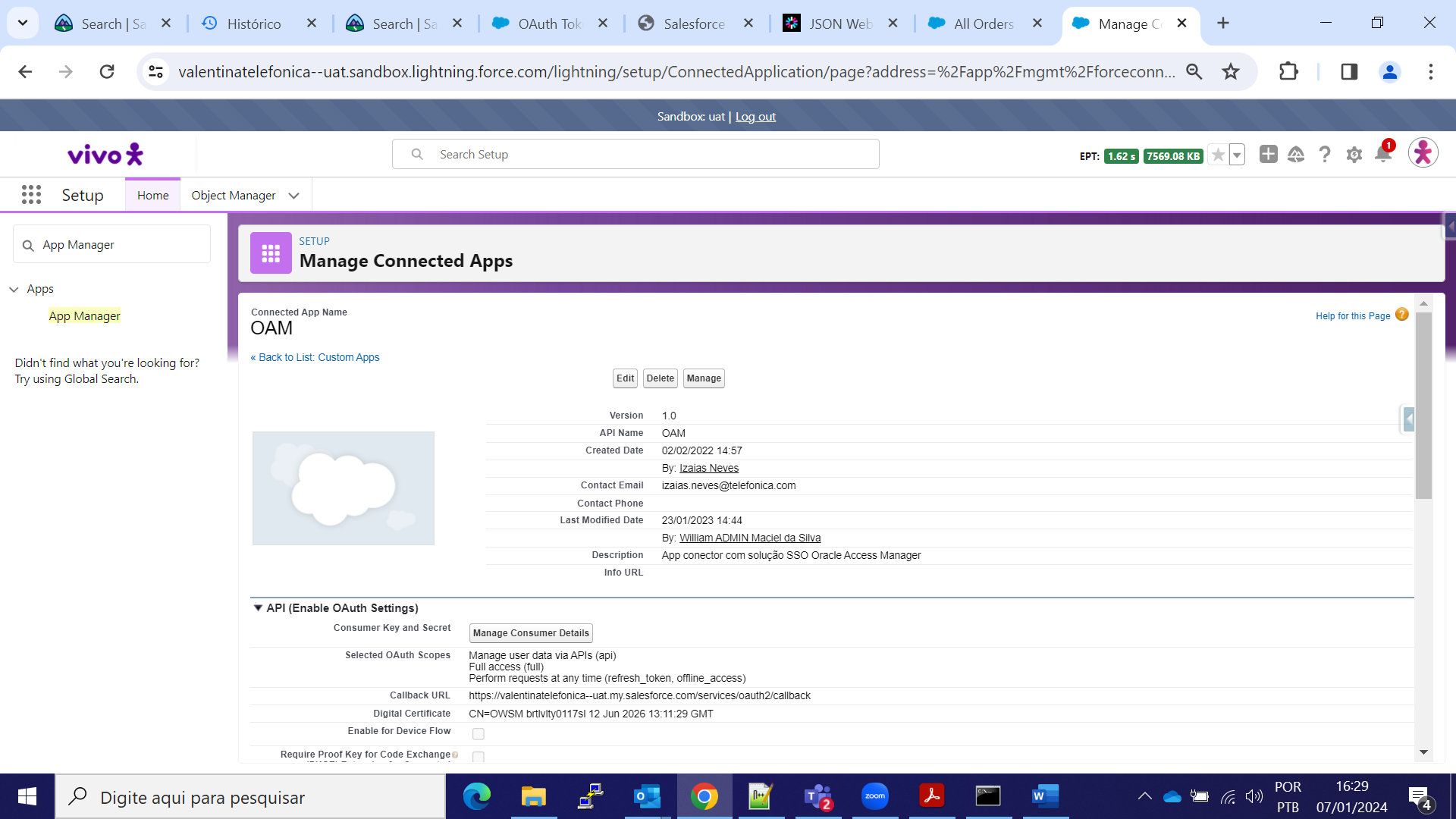
É importante ficar claro que esse fluxo seria algum sistema chamando o Salesforce para obter dados e informações. No P6 e P8 do Valentina é o Salesforce chamando os sistemas externos para obter informação, então a dinâmica muda um pouco, mas o conceito é o mesmo

1)Se autenticando no Salesforce para pedir um authorization code, que é a primeira parte do fluxo.



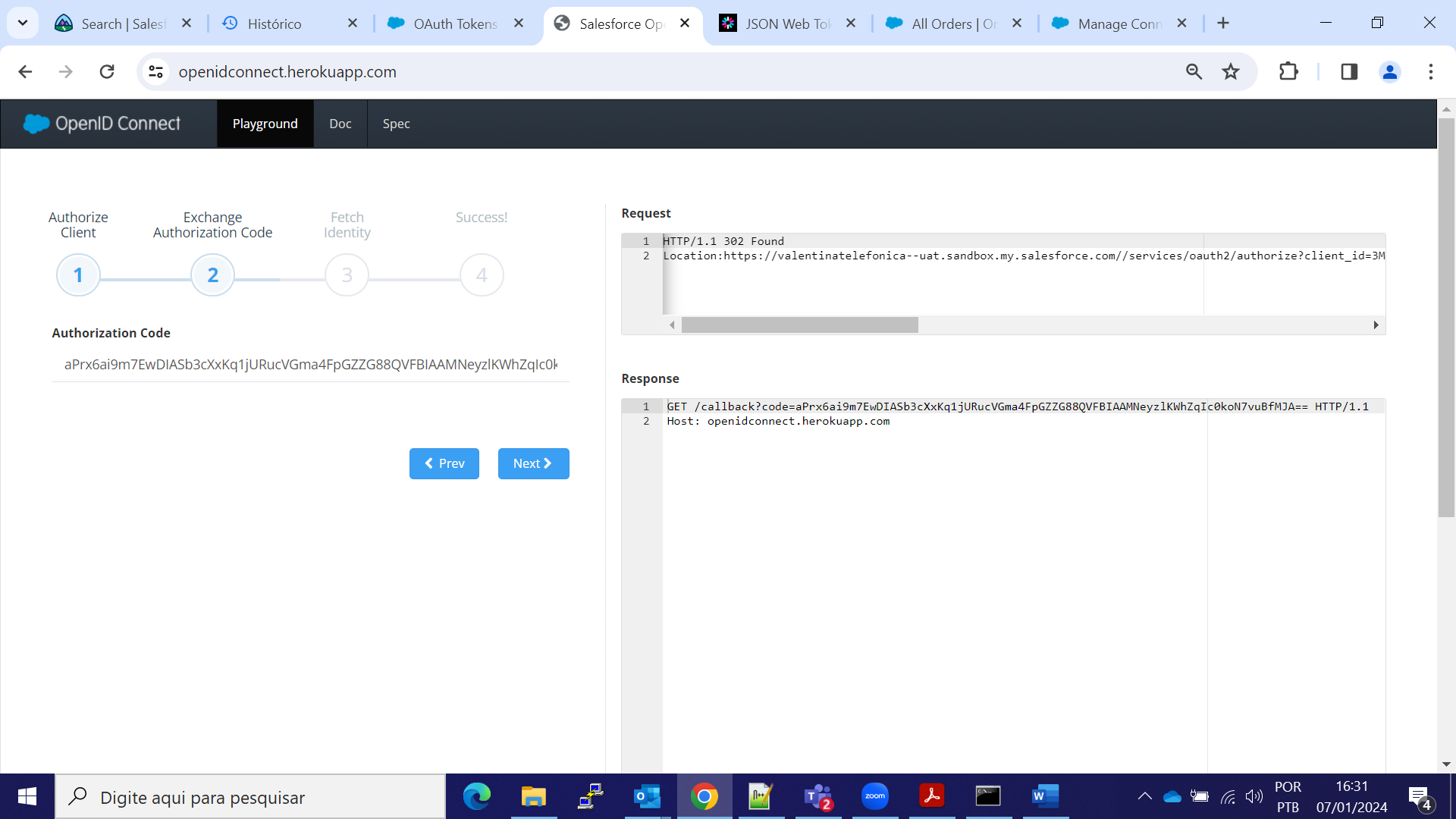
Aqui as configurações do connected app

LEMBRAR QUE PRECISA COLOCAR O APONTAMENTO DO CALLBACK DO HEROKU. AQUI esta ainda o nativo do Valentina



Se eu clicar em Manage Consumer Details encontro o client id e client secret, que devera ser configurado no sistema requisitante.

2)Ao realizar a autenticação é pedido um usuário e senha, e no retorno obtenho o authorization code que é o 1° passo da autenticação no Salesforce.



3) Chamo novamente o Salesforce enviando o authorization code para obter o access token, que é o token utilizado pelas APIs para executar os cenários de negócio

Request

POST /services/oauth2/token HTTP/1.1

Host: valentinatelefonica--uat.sandbox.my.salesforce.com/

Content-length: 307

Content-type: application/x-www-form-urlencoded

grant\_type=authorization\_code&code=aPrx6ai9m7EwDIASb3cXxKq1jURucVGma4FpGZZG88QVFBIAAMNeyzlKWhZqIc0koN7vuBfMJA==&client\_id=3MVG9qEXqmIutu\_T6W3y79\_JA4\_uVq0gjSTFG8cwJln9D\_zK0yQybtrFekmi.6E9nCytlCgPjRH33YjGaOCkr&client\_secret=\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*&redirect\_uri=https%3A%2F%2Fopenidconnect.herokuapp.com%2Fcallback

Response

HTTP/1.1 200 OK

{

"access\_token": "00D780000008iuX!AQYAQFLnilCbpTPs.YxZeJe9O9c\_.7R0ppyyHjHHHTltSeWWBDcIz9dy\_tfZnd7kIqgnzecTa1ZTmnsKY0yGdgvC9PKHQX4I",

"id": "https://test.salesforce.com/id/00D780000008iuXEAQ/00578000000Zl1bAAC",

"id\_token": "eyJraWQiOiIyNDgiLCJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdF9oYXNoIjoiZHlWcU9PYi1JSS1RbGUzVVJWbFNFdyIsInN1YiI6Imh0dHBzOi8vdGVzdC5zYWxlc2ZvcmNlLmNvbS9pZC8wMEQ3ODAwMDAwMDhpdVhFQVEvMDA1NzgwMDAwMDBabDFiQUFDIiwiYXVkIjoiM01WRzlxRVhxbUl1dHVfVDZXM3k3OV9KQTRfdVZxMGdqU1RGRzhjd0psbjlEX3pLMHlReWJ0ckZla21pLjZFOW5DeXRsQ2dQalJIMzNZakdhT0NrciIsImlzcyI6Imh0dHBzOi8vdmFsZW50aW5hdGVsZWZvbmljYS0tdWF0LnNhbmRib3gubXkuc2FsZXNmb3JjZS5jb20iLCJleHAiOjE3MDQ2NTYwODAsImlhdCI6MTcwNDY1NTk2MH0.Nu74BcXAbXN-d8RYYGfJR8kZiwxuC3Ein6UeZ4RX-N55Ge3MY9nxOA7djZ92I35vOjiJ\_Y0rDIftmYmRVsPyY1pM0ZidIqgC4cp3yqhr\_LzwtXy1G5FBfNj4ZKte9\_g6rYXH6VhC2phjCCHfSWxCiq9gocpZ7aFWhowuTEcC3J-gBs3bZrxheukxx6zC9gf7rqUeJp8ljSyr1v6AJm1MBFyQjqMt5wcYgIR9TXE4LCfY3JzmHjlQjdzy1ZKLUlCZLUTDzHwKffkLC9k54MLmKL7XLZblVpm8sKWHS4o9KYQYuPoi2OLNoXupqs-w9E0vdoelYQUTJ7AAOlBoApCk3B0sVAYIxrPLtNiWlFJHjU6Vc\_-f9xbbBRfr7dSJXohLigmgy9ld3kQIspS2kuzweV4UxP3RcSiaibHFR8KqFRT9ZfhZN\_GOU9dsRbAR6dOLB19n9IKQ2I6db4MyHE5I8i4EId-EUow9lUUarqGH9NLdAS3Ri86qXZWoYGPtHOWBUez1bpr1orRETLwmh9KzCzR7rPhEecGA1HRjJ1wcu91EoBm0FtfaVmquOfI5yIFTOlv-BSDFTtgSf3rKC5jbKTtwrpHfdyyh2bRuR-AAt5zwvjKMdwv2C1yLsD8GFglh5NJXR7EdETtimRCoPkrmdiyO4LcOzXvu69DVb9Phtgk",

"instance\_url": "https://valentinatelefonica--uat.sandbox.my.salesforce.com",

"issued\_at": "1704655960444",

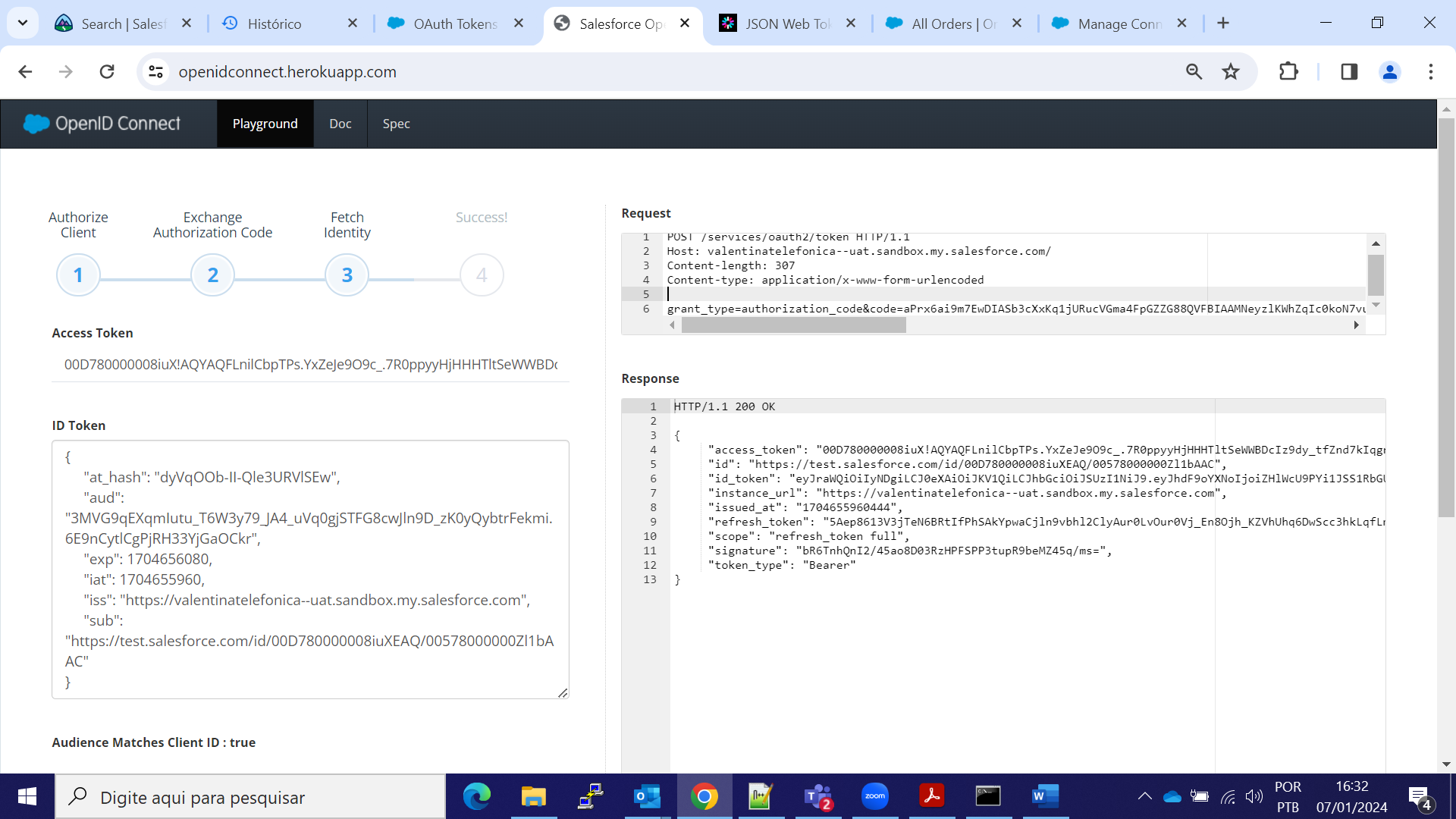
"refresh\_token": "5Aep8613V3jTeN6BRtIfPhSAkYpwaCjln9vbhl2ClyAur0LvOur0Vj\_En8Ojh\_KZVhUhq6DwScc3hkLqfLmuf4s",

"scope": "refresh\_token full",

"signature": "bR6TnhQnI2/45ao8D03RzHPFSPP3tupR9beMZ45q/ms=",

"token\_type": "Bearer"

}



O Access Token retornado é um token opaco, por configuração default do Salesforce. Se eu quiser obter um JWT posso configurar no connected app para retornar o JWT. Com o Token opaco, o sistema requisitante sempre precisar enviar uma chamada ao Salesforce para validar se esse token ainda esta vigente. Por ser opaco o canal não consegue validar as informações de token que estão criptografadas.

Se o Access Token fosse um token JWT, o canal poderia descriptografar e validar o conteúdo dele, que tem uma série de informações inclusive informações de expiração do token, scope e etc. Dessa forma o canal não recisa chamar o Salesforce para validar se o token esta expirado, pode validar internamente descriptografando, e se estiver expirado pode pedir um token novo evitando chamadas desnecessárias. O Scope fica criptografado no Access Token, sendo retornado pelo Salesforce na chamada do canal

Nesse link maiores detalhes sobre as diferenças entre um e outro com pros e contras

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

No output da chamada tbm é retornado o refresh token. O refresh token é um token utilizado para vc pedir um novo access token quando o anterior expirou. O beneficio de se utilizar o refresh token para obter um novo token é que você não precisa realizar todo o processo de autenticação(authorization\_code) novamente, o que levaria mais tempo. Quando você utiliza um refresh token, um novo access e refresh token é concedido. No P6 e P8 é possível ver o exemplo.

O ID Token é uma estrutura de dados assinada que contém atributos de usuário autenticado, incluindo um identificador exclusivo para o usuário e quando o token foi emitido. Ele também identifica o aplicativo cliente solicitante. Por ser um JWT, a conversão dele no site da JWT IO seria:

"id\_token": "eyJraWQiOiIyNDgiLCJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdF9oYXNoIjoiZHlWcU9PYi1JSS1RbGUzVVJWbFNFdyIsInN1YiI6Imh0dHBzOi8vdGVzdC5zYWxlc2ZvcmNlLmNvbS9pZC8wMEQ3ODAwMDAwMDhpdVhFQVEvMDA1NzgwMDAwMDBabDFiQUFDIiwiYXVkIjoiM01WRzlxRVhxbUl1dHVfVDZXM3k3OV9KQTRfdVZxMGdqU1RGRzhjd0psbjlEX3pLMHlReWJ0ckZla21pLjZFOW5DeXRsQ2dQalJIMzNZakdhT0NrciIsImlzcyI6Imh0dHBzOi8vdmFsZW50aW5hdGVsZWZvbmljYS0tdWF0LnNhbmRib3gubXkuc2FsZXNmb3JjZS5jb20iLCJleHAiOjE3MDQ2NTYwODAsImlhdCI6MTcwNDY1NTk2MH0.Nu74BcXAbXN-d8RYYGfJR8kZiwxuC3Ein6UeZ4RX-N55Ge3MY9nxOA7djZ92I35vOjiJ\_Y0rDIftmYmRVsPyY1pM0ZidIqgC4cp3yqhr\_LzwtXy1G5FBfNj4ZKte9\_g6rYXH6VhC2phjCCHfSWxCiq9gocpZ7aFWhowuTEcC3J-gBs3bZrxheukxx6zC9gf7rqUeJp8ljSyr1v6AJm1MBFyQjqMt5wcYgIR9TXE4LCfY3JzmHjlQjdzy1ZKLUlCZLUTDzHwKffkLC9k54MLmKL7XLZblVpm8sKWHS4o9KYQYuPoi2OLNoXupqs-w9E0vdoelYQUTJ7AAOlBoApCk3B0sVAYIxrPLtNiWlFJHjU6Vc\_-f9xbbBRfr7dSJXohLigmgy9ld3kQIspS2kuzweV4UxP3RcSiaibHFR8KqFRT9ZfhZN\_GOU9dsRbAR6dOLB19n9IKQ2I6db4MyHE5I8i4EId-EUow9lUUarqGH9NLdAS3Ri86qXZWoYGPtHOWBUez1bpr1orRETLwmh9KzCzR7rPhEecGA1HRjJ1wcu91EoBm0FtfaVmquOfI5yIFTOlv-BSDFTtgSf3rKC5jbKTtwrpHfdyyh2bRuR-AAt5zwvjKMdwv2C1yLsD8GFglh5NJXR7EdETtimRCoPkrmdiyO4LcOzXvu69DVb9Phtgk",

{

"at\_hash": "dyVqOOb-II-Qle3URVlSEw",

"aud": "3MVG9qEXqmIutu\_T6W3y79\_JA4\_uVq0gjSTFG8cwJln9D\_zK0yQybtrFekmi.6E9nCytlCgPjRH33YjGaOCkr",

"exp": 1704656080,

"iat": 1704655960,

"iss": "https://valentinatelefonica--uat.sandbox.my.salesforce.com",

"sub": "https://test.salesforce.com/id/00D780000008iuXEAQ/00578000000Zl1bAAC"

}

Id da org: 00D780000008iuXEAQ

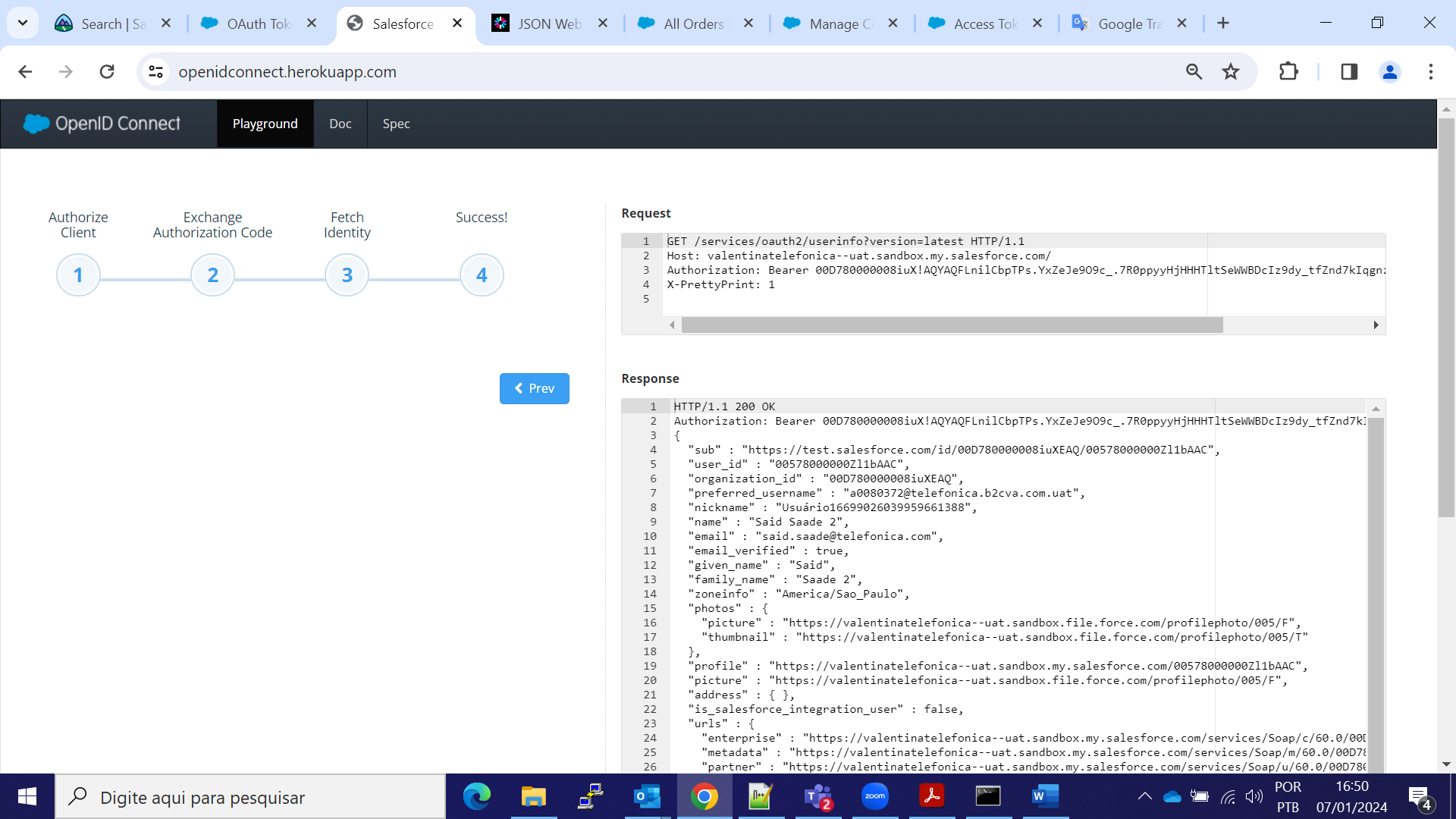
Id fo user que se autenticou: 00578000000Zl1bAAC

Quando realizamos a autenticação no Salesforce utilizando o OAM da Telefonica, o ID token retornado possui muiiiiito mais informação. Por se utilizar o protocolo OPENID, que é customizado, podemos parametrizar algumas informações adicionais a serem retornadas. Veja o P6 e P8 para pegar mais exemplo do que é retornado na org da Vivo.

<https://trailhead.salesforce.com/content/learn/modules/identity_basics/identity_basics_protocols>

No link acima e possível entender mais sobre o OpenId e oq é esse protocolo que trabalha em cima do id token

4) Agora com o access token em mãos executamos uma API para retornar as informações de negócios.



Input

GET /services/oauth2/userinfo?version=latest HTTP/1.1

Host: valentinatelefonica--uat.sandbox.my.salesforce.com/

Authorization: Bearer 00D780000008iuX!AQYAQFLnilCbpTPs.YxZeJe9O9c\_.7R0ppyyHjHHHTltSeWWBDcIz9dy\_tfZnd7kIqgnzecTa1ZTmnsKY0yGdgvC9PKHQX4I

X-PrettyPrint: 1

Output

HTTP/1.1 200 OK

Authorization: Bearer 00D780000008iuX!AQYAQFLnilCbpTPs.YxZeJe9O9c\_.7R0ppyyHjHHHTltSeWWBDcIz9dy\_tfZnd7kIqgnzecTa1ZTmnsKY0yGdgvC9PKHQX4IX-PrettyPrint: 1

{

"sub" : "https://test.salesforce.com/id/00D780000008iuXEAQ/00578000000Zl1bAAC",

"user\_id" : "00578000000Zl1bAAC",

"organization\_id" : "00D780000008iuXEAQ",

"preferred\_username" : "a0080372@telefonica.b2cva.com.uat",

"nickname" : "Usuário16699026039959661388",

"name" : "Said Saade 2",

"email" : "said.saade@telefonica.com",

"email\_verified" : true,

"given\_name" : "Said",

"family\_name" : "Saade 2",

"zoneinfo" : "America/Sao\_Paulo",

"photos" : {

"picture" : "https://valentinatelefonica--uat.sandbox.file.force.com/profilephoto/005/F",

"thumbnail" : "https://valentinatelefonica--uat.sandbox.file.force.com/profilephoto/005/T"

},

"profile" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/00578000000Zl1bAAC",

"picture" : "https://valentinatelefonica--uat.sandbox.file.force.com/profilephoto/005/F",

"address" : { },

"is\_salesforce\_integration\_user" : false,

"urls" : {

"enterprise" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/Soap/c/60.0/00D780000008iuX",

"metadata" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/Soap/m/60.0/00D780000008iuX",

"partner" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/Soap/u/60.0/00D780000008iuX",

"rest" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/",

"sobjects" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/sobjects/",

"search" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/search/",

"query" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/query/",

"recent" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/recent/",

"tooling\_soap" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/Soap/T/60.0/00D780000008iuX",

"tooling\_rest" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/tooling/",

"profile" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/00578000000Zl1bAAC",

"feeds" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/chatter/feeds",

"groups" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/chatter/groups",

"users" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/chatter/users",

"feed\_elements" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com/services/data/v60.0/chatter/feed-elements",

"custom\_domain" : "https://valentinatelefonica--uat.sandbox.my.salesforce.com"

},

"active" : true,

"user\_type" : "STANDARD",

"language" : "en\_US",

"locale" : "pt\_BR",

"utcOffset" : -10800000,

"updated\_at" : "2023-12-14T13:37:51Z",

"is\_app\_installed" : true

}

Podemos criar tbm escopo customizado para uma determinada necessidade. Se eu quero que uma API em especifico so seja executada por um único canal.

Passos:

1. Criar o Scope “Oauth Custom Scope” e atribua ao connected App
2. Envie as credencias(ISS) desse connected APP parao canal
3. ??Necessario confirmar aonde mapeio o que esse custom permission pode visualizar.

https://help.salesforce.com/s/articleView?id=sf.remoteaccess\_oauth\_customscopes.htm&type=5