了解平台服务

Predix平台通过Predix目录提供预构建微服务。微服务在Cloud Foundry市场中提供。您可以根据您应用程序的要求选择要使用的微服务。关于Predix平台上提供的微服务的完整列表，请参见Predix.io上的目录页面。

Predix平台服务使用OAuth2进行认证。服务利用[用户账号和认证（UAA）](https://www.predix.io/docs/?r=207686#SJzDWEsh)web service管理OAuth2客户端。

用户账号和认证（UAA）是Cloud Foundry提供的一个web service，用于管理用户和OAuth2客户端。其主要作用是用作OAuth2提供者，当客户端应用程序代表Cloud Foundry用户使用时为其发布令牌。通过与登录服务器协作，它可以通过用户的Cloud Foundry凭据对其进行认证，也可以使用这些凭据（或其他）用作SSO服务。该服务为管理用户账号和注册OAuth2客户端提供端点。

如果要使用平台服务，您必须首先将UAA服务的一个实例设置为您的可信发布者。然后对服务的所有访问使用指定的可信发布者认证。

下图显示了平台服务如何与用于认证的UAA集成。



平台服务设置

以下任务路线图显示了开始进行Predix平台服务所需的基本步骤。

任务路线图

| **编号** | **任务** | **说明** |
| --- | --- | --- |
| 1 | 设置您的可信发布者。 | 创建用户账号和认证（UAA）服务的一个实例。UAA是每个平台服务用于认证的授权服务器。更多信息，请参见[创建一个UAA服务实例](https://www.predix.io/docs/?r=207685" \l "XpKGAdQ7-ao7RnIco" \t "_self)。***提示：您在您的空间中创建的UAA实例的最大数量为10。作为一项最佳实践，为您的每项服务使用相同的UAA实例。*** |
| 2 | 为您的服务创建一个实例。 | 从Predix.io目录中选择您需要的服务，并为您的服务创建一个实例。更多信息，请参见[创建一个平台服务实例](https://www.predix.io/docs/?r=207684" \l "aQx4m9cA" \t "_self) |
| 3 | 创建OAuth2客户端，设置对您的服务的访问，该服务使用UAA认证。 | 当您创建一个UAA实例时，会自动为您创建一个管理员客户端，用于访问UAA的其他配置。您可以为您的服务实例创建一个具有特定范围的新客户端。如果已经有一个Oauth2客户端，您可以更新该客户端以添加您的服务实例。更多信息，请参见[创建一个OAuth2客户端](https://www.predix.io/docs/?r=207683" \l "uAyBrT9y-ao7RnIco" \t "_self" \o "创建其他OAuth2客户端以访问一个UAA实例的程序。)。 |
| 4 | 更新Oath2客户端以添加服务特定范围或权限。 | 为了使您的应用程序能够访问平台服务，您的JSON网络令牌（JWT）必须包含该平台服务所需的范围。更多信息，请参见[更新OAuth2客户端](https://www.predix.io/docs/?r=207682" \l "cSznH26X-ao7RnIco" \t "_self" \o "更新OAuth2客户端以添加每个平台服务的其他特定权限或范围的程序。)。 |
| 5 | 将您的应用程序与服务实例绑定。 | 如果要在您的应用程序与平台服务之间建立通信，你必须将应用程序与服务绑定。更多信息，请参见[将您的应用程序连接至一个平台服务实例](https://www.predix.io/docs/?r=207681" \l "E1yVyasD" \t "_self" \o "如果要在您创建的服务实例与您的应用程序之间建立通信，您可以将您的应用程序与服务实例绑定。)。 |
| 6 | 开始使用您的服务。 | 当您登录Predix.io时，您的服务实例在控制台页面上列出。关于使用一个特定服务实例的更多信息，请使用Predix.io上每个服务信息页面上的参见文件按钮。 |

使用Cloud Foundry命令设置平台服务

这是使用Cloud Foundry命令行代替Predix.io提供的图形用户界面开始使用平台服务的一个可选步骤。

以下可选步骤显示了使用Cloud Foundry命令行工具开始使用Predix平台服务所需的基本步骤。关于使用图形用户界面的信息，请参见[平台服务设置](https://www.predix.io/docs/?r=207680#QD8MAu9C)。

1. 创建用户账号和认证服务的一个实例，它将作为您的可信发布者。参见[使用命令行创建一个UAA服务实例](https://www.predix.io/docs/?r=207679)。
2. 如果您的应用程序还未部署，请将您的应用程序推送到Cloud Foundry。

参见[创建一个简单的Predix Hello World网页应用程序](https://www.predix.io/docs/?r=207678#IqAL3Fzb)。

1. [将一个应用程序与您的UAA实例绑定](https://www.predix.io/docs/?r=207677#sXp7cw5P)。当您将您的应用程序与您的UAA实例绑定时，您的UAA服务实例的连接详细信息在VCAP\_SERVICES环境变量中填写。
2. 从VCAP\_SERVICES环境变量详细信息中检索UAA实例的issuerID。

当您创建使用您的UAA实例进行认证的其他服务的一个实例时，issuerID是必需的。

1. 选择需要使用的Predix平台服务并创建服务的一个实例。参见[使用Cloud Foundry命令创建一个平台服务实例](https://www.predix.io/docs/?r=207676)。

当您创建平台服务的一个实例时，您必须指定一个可信发布者（您的UAA实例的issuerID）或可信发布者的集合。

1. [将您的应用程序与服务的新实例绑定](https://www.predix.io/docs/?r=207675#E1yVyasD)。

当您将您的服务实例与您的应用程序绑定时，您的服务实例的连接详细信息在VCAP\_SERVICES环境变量中填写。您可以从VCAP\_SERVICES环境变量详细信息中检索以下信息：

* + http-header-name与http-header-value

HTTP标头信息对于服务实例的每次调用来说是必需的。对实例的每次调用必须在其标头中包含http-header-name与http-header-value。

* + oauth-scope

oauth-scope值代表您必须为您的OAuth2客户端添加的权限，以访问一个指定的服务实例。关于OAuth2客户端更新的示例，请参见[使用UAAC更新OAuth2客户端](https://www.predix.io/docs/?r=207674#pOVsUZ0a)。

1. 创建一个Oauth2客户端。参见[使用UAAC创建一个OAuth2客户端](https://www.predix.io/docs/?r=207673)。
2. [更新Oauth2客户端](https://www.predix.io/docs/?r=207672#pOVsUZ0a)以使用一个平台服务。

创建一个UAA服务实例

您可以在您的空间中创建多达10个UAA服务实例。如果您需要其他实例，添加新实例之前首先删除不用的旧实例。

1. 通过https://www.predix.io登录您的Predix账号。
2. 导航至目录 > 服务选项卡，然后点击用户账号和认证标题。
3. 在所需方案上点击订阅。
4. 填写新建服务实例页面上的字段。

| **字段** | **说明** |
| --- | --- |
| 组织 | 选择您的组织。 |
| 空间 | 为您的应用程序选择空间。 |
| 服务实例名称 | 为该UAA服务实例输入一个唯一的名称。 |
| 服务方案 | 选择一个方案。 |
| 管理员客户端密码 | 输入一个客户端密码（这是该UAA实例的管理员密码）。客户端密码可以是任意字母数字字符串。***注：将客户端密码记录在一个安全的位置，以供将来使用。*** |
| 子域 | （可选）除了为UAA创建的域，输入一个您可能需要用到的子域。您不得在子域的名称中添加特殊字符。子域的值不区分大小写。 |

1. 点击创建服务。

您的UAA实例使用以下规范创建：

* 一个客户端标识符（admin）。

***注：一个admin客户端被创建用于启动引导。你可以创建与您的应用程序一起使用的其他客户端。***

* 一个客户端密码（您在创建服务时指定的密码）。

如果要检索您的实例的其他详细信息，您可以将一个应用程序与您的实例绑定。

使用命令行创建一个UAA服务实例

使用命令行代替图形用户界面创建一个UAA服务实例的可选步骤。

您可以在您的空间中创建多达10个UAA服务实例。如果您需要其他实例，您必须删除不用的旧实例并创建一个新实例。

1. 使用Cloud Foundry CLI登录Cloud Foundry。

cf login -a <API\_Endpoint>

根据您注册的Predix.io，<API\_Endpoint>的值为以下其中一个：

* + Predix美国西部

https://api.system.aws-usw02-pr.ice.predix.io

* + Predix美国东部

https://api.system.asv-pr.ice.predix.io

* + Predix日本

https://api.system.aws-jp01-pr.ice.predix.io

* + Predix英国

https://api.system.dc-uk01-pr.ice.predix.io

例如，

cf login -a https://api.system.aws-usw02-pr.ice.predix.io

1. 通过输入以下命令列出在Cloud Foundry市场中的服务。

cf marketplace

UAA服务predix-uaa被列为其中一个可用服务。

1. 通过输入以下命令创建一个UAA实例。

cf create-service predix-uaa <plan> <my\_uaa\_instance> -c '{"adminClientSecret":"<my\_secret>","subdomain":"<my\_subdomain>"}'

其中：

* + <plan>是与服务相关的方案。例如，您可以将 tiered 方案用于predix-uaa服务。
	+ -c选项用于指定以下其他参数。
		- adminClientSecret指定客户端密码。
		- subdomain指定一个除了为UAA创建的域您可能需要用到的子域。这是可选参数。您不得在子域的名称中添加特殊字符。子域的值不区分大小写。

***注： Cloud Foundry CLI句法在Windows与Linux操作系统之间可能会不同。关于您的操作系统的适当句法，请参见Cloud Foundry帮助。例如，如果要查看create service命令的帮助，请运行cf cs。***

您的UAA实例使用以下规范创建：

* 一个客户端标识符（admin）。

***注：一个admi客户端被创建用于启动引导。你可以创建与您的应用程序一起使用的其他客户端。***

* 一个客户端密码（您在创建服务时指定的密码）。

如果要检索您的实例的其他详细信息，您可以将一个应用程序与您的实例绑定。

创建一个predix-uss服务实例，客户端密码为admin，而子域为ge-digital：

cf cs predix-uaa tiered test-1 -c '{"adminClientSecret":"admin","subdomain":"ge-digital"}'

在VCAP SERVICES中的代码为：

"VCAP\_SERVICES": {

"predix-uaa": [

 {

 "credentials": {

 "dashboardUrl": "https://uaa-dashboard.run.asv-pr.ice.predix.io/#/login/04187eb1-e0cf-4874-8218-9fb77a8b4ed9",

 "issuerId": "https://04187eb1-e0cf-4874-8218-9fb77a8b4ed9.predix-uaa.run.asv-pr.ice.predix.io/oauth/token",

 "subdomain": "04187eb1-e0cf-4874-8218-9fb77a8b4ed9",

 "uri": "https://04187eb1-e0cf-4874-8218-9fb77a8b4ed9.predix-uaa.run.asv-pr.ice.predix.io",

 "zone": {

 "http-header-name": "X-Identity-Zone-Id",

 "http-header-value": "04187eb1-e0cf-4874-8218-9fb77a8b4ed9"

 }

 },

 "label": "predix-uaa",

 "name": "testuaa",

 "plan": "Tiered",

 "provider": null,

 "syslog\_drain\_url": null,

 "tags": [],

 "volume\_mounts": []

 }

 ],

创建一个平台服务实例

创建一个服务实例之前平台服务需要您设置一个可信发布者（UAA）。您拥有可信发布者的一个实例之后，您就可以为您的应用程序开发创建平台服务的一个实例。

1. 通过https://www.predix.io登录您的Predix账号。
2. 导航至目录 > 服务选项卡，并点击服务标题。
3. 在所需方案上点击订阅。
4. 填写新建服务实例上的字段。

| **字段** | **说明** |
| --- | --- |
| 组织 | 选择您的组织。 |
| 空间 | 为您的应用程序选择空间。 |
| 用户账号和认证（UAA） | 选择一个现有的UAA实例，或创建一个新的。更多信息，请参见[创建一个UAA服务实例](https://www.predix.io/docs/?r=207671" \l "XpKGAdQ7-ao7RnIco" \t "_self)。 |
| 服务实例名称 | 为该服务实例输入一个唯一的名称。 |
| 服务方案 | 选择一个方案。 |

1. 点击创建服务。

使用Cloud Foundry命令创建一个平台服务实例

您可以使用Cloud Foundry CLI来创建一个平台服务实例：

1. 使用Cloud Foundry CLI登录Cloud Foundry。

cf login -a <API\_Endpoint>

根据您注册的Predix.io，<API\_Endpoint>的值为以下其中一个：

* + Predix美国西部

https://api.system.aws-usw02-pr.ice.predix.io

* + Predix美国东部

https://api.system.asv-pr.ice.predix.io

* + Predix日本

https://api.system.aws-jp01-pr.ice.predix.io

* + Predix英国

https://api.system.dc-uk01-pr.ice.predix.io

例如，

cf login -a https://api.system.aws-usw02-pr.ice.predix.io

1. 通过输入以下命令列出在Cloud Foundry市场中的服务：

cf marketplace

1. 通过输入以下命令创建一个服务实例：

cf create-service <service\_name> <plan> <my\_instance> -c '{"trustedIssuerIds":["<uaa\_instance1\_issuerId>", "<uaa\_instance2\_issuerID>"]}'

其中：

* + <service\_name> 是服务在Cloud Foundry市场中的名称。例如，资产服务为 predix-asset。
	+ <plan> 是与服务相关的方案。例如， predix-acs 服务可以与 basic 方案相关。
	+ <uaa\_instance\_issuerID> 是您的可信发布者（UAA实例）的 issuerID ，例如https://13fa0384-9e2a-48e2-9d06-2c95a1f4f5ea.predix-uaa.grc-apps.svc.ice.ge.com/oauth/token。您可以使用一个逗号分隔列表指定多个可信发布者。您可以在[将您的UAA实例与一个应用程序绑定](https://www.predix.io/docs/t_binding_an_app_to_the_uaa_instance.html)之后从VCAP\_SERVICES环境变量中检索该URL。

***注： Cloud Foundry CLI句法在Windows与Linux操作系统之间可能会不同。关于您的操作系统的适当句法，请参见Cloud Foundry帮助。例如，如果要查看create service命令的帮助，请运行cf cs。***

Cloud Foundry显示一条确认服务实例已创建的消息。将其与一个应用程序绑定之后，您可以从VCAP\_SERVICES环境变量中检索该实例的URI。

创建一个OAuth2客户端

您可以为您的应用程序创建具有指定权限的OAuth2客户端来使用Predix平台服务。通常这是创建完一个服务实例后的第一步工作。

当您创建了一个UAA实例，UAA 仪表板工具就可以用来配置这个UAA实例。您能使用UAA仪表板中的客户端管理选项卡创建OAuth2客户端：

1. 在控制台视图中，选择您的服务所处的空间。
2. 在服务实例页面中，选择您需要配置的UAA实例。
3. 选择配置服务实例选项。
4. 在UAA仪表板登录页面中，指定您的管理员客户端密码并点击登录。
5. 在UAA仪表板中，选择客户端管理选项卡。

客户端管理选项卡包括两部分，客户端和服务实例。服务实例部分显示您已经为您的服务创建的服务实例。

***注：此处显示的服务实例是那些您使用您想要配置的UAA创建的实例。您使用其他UAA实例创建的服务实例不显示在此页面上。***

1. 点击创建客户端按钮打开创建客户端窗体。
2. 在创建客户端窗体中指定以下值：

| **字段** | **说明** |
| --- | --- |
| 客户端ID | 为您正在创建的OAuth2客户端指定一个名称。 |
| 客户端密码 | 指定密码。您要记住该密码，这一点非常重要。如果丢失，该密码无法找回。 |
| 确认客户端密码 | 重新输入客户端密码。 |
| 授权的授权类型 | 从下面选择一个或多个授权类型：* + client\_credentials

当您使用客户端凭据授权类型时，UAA中的OAuth2端点接受客户端ID和客户端密码并提供访问令牌。* + implicit

当您使用隐式授权类型时，UAA直接为客户端发布访问令牌，无需认证该客户端。这减少了获取访问令牌所需往返行程的数量。* + password

当您使用资源所有者密码凭据授权类型时，UAA中的OAuth2端点接受用户名和密码并提供访问令牌。* + authorization\_code

当您使用授权代码授权类型时，客户端将资源所有者定向至UAA，然后UAA反过来通过授权代码将资源所有者定向至客户端。* + refresh\_token

刷新令牌是用于得到访问令牌的凭据。您可以选择这个选项从UAA获得刷新令牌。当目前使用的访问令牌无效或过期时，您可以使用刷新令牌从UAA获得一个新访问令牌，或者获得附加的相同或减少范围的访问令牌关于不同授权类型的更多信息，请参见[RFC 6749](https://tools.ietf.org/html/rfc6749%22%20%5Ct%20%22_blank)。 |
| 范围 | 范围是与一个OAuth客户端相关的许可，用于用户通过应用程序访问资源。用户许可用于授权类型 authorization\_code, password 与 implicit。默认为管理员客户端分配所有需要的范围。对于新的客户端，管理员可以根据客户端要求选择要添加的范围。关于可以分配的范围的完整列表，请参见[UAA授权的范围](https://github.com/GESoftware-CF/uaa/blob/master/docs/UAA-APIs.rst%22%20%5Cl%20%22scopes-authorized-by-the-uaa%22%20%5Ct%20%22_blank)。为了使用OAuth客户端访问Predix平台服务，在UAA服务实例中新增客户端后您必须[更新您的OAuth客户端](https://www.predix.io/docs/?r=133575" \l "by5wfx4s-ao7RnIco)来增加[访问每个服务所需的范围](https://www.predix.io/docs/?r=133574" \l "pDpt7Gv-ao7RnIco)。 |
| 权限 | 权限是指当一个应用程序或API使用其自有凭据访问一个资源时与OAuth客户端相关的许可，不涉及用户。许可用于授权类型 client\_credentials。默认为管理员客户端分配所有需要的权限。对于新的客户端，管理员可以根据客户端要求选择要添加的权限。权限列表与范围列表相同。关于完整的列表，请参见[UAA授权的范围](https://github.com/GESoftware-CF/uaa/blob/master/docs/UAA-APIs.rst%22%20%5Cl%20%22scopes-authorized-by-the-uaa%22%20%5Ct%20%22_blank)。为了使用OAuth客户端访问Predix平台服务，在UAA服务实例中新增客户端后您必须[更新您的OAuth客户端](https://www.predix.io/docs/?r=133575" \l "by5wfx4s-ao7RnIco)来增加[访问每个服务所需的权限](https://www.predix.io/docs/?r=133571" \l "pDpt7Gv-ao7RnIco)。备注：一个admin客户端默认是没有分配修改用户密码的权限。为了修改用户密码，您必须微admin客户端增加uaa.admin权限 |
| 自动批准的范围 | 为客户端指定可以自动批准的范围，无需资源所有者的明确批准。 |
| 重定向URI | 指定一个重定向URI在登录后对客户端进行重定向。例如，http://example-app.com/welcome。当您开始将UAA用作服务提供者时，该URI用于您的外部身份提供者。 |
| 访问令牌有效性 | 指定访问令牌失效时间，单位毫秒。 |
| 刷新令牌有效性 | 指定刷新令牌失效时间，单位毫秒。 |
| 允许的提供者 | 如果有的话，指定外部身份提供者的名称。如果您正在使用外部身份提供者，同时将UAA用作服务提供者，则该字段为必填。 |

下一步：用于您的服务的特点信息[为服务更新您的OAuth2客户端](https://www.predix.io/docs/?r=133570#by5wfx4s-ao7RnIco)。

**使用UAAC创建一个OAuth2客户端**

使用UAA命令行界面（UAAC）代替图形用户界面创建一个OAuth2客户端的可选程序。

您可以使用UAAC管理您的UAA实例。关于安装命令行界面的更多信息，请参见<https://github.com/cloudfoundry/cf-uaac>。

1. 将您的UAA实例指定为预定目标。

uaac target <uaa\_instance\_url>

<uaa\_instance\_url> 是您的可信发布者的URL，例如， https://11fa0273-9e2a-37e2-9d06-2c95a1f4f5ea.predix-uaa.run.aws-usw02-pr.ice.predix.io。您可以在将您的UAA实例与一个应用程序绑定之后从VCAP\_SERVICES环境变量中检索该URL。

1. 使用管理客户端登录。

uaac token client get admin

1. 在提示时指定管理客户端密码。
2. 使用以下命令创建OAuth2客户端：

uaac client add [client\_name]--authorities "uaa.resource"--scope "openid"--autoapprove "openid"--authorized\_grant\_types [authorization\_code|implicit|password|client\_credentials|refresh\_token]--redirect\_uri [redirect\_uri\_1, redirect\_uri\_2, ...]

关于UAA选项的更多信息，例如 scopes 与 authorized\_grant\_types，请参见<https://github.com/GESoftware-CF/uaa/blob/master/docs/UAA-APIs.rst>网页上的UAA文件。

更新OAuth2客户端

为了使用OAuth2客户端从您的应用程序中安全的访问您的Predix平台服务实例，您必须更新您的OAuth2客户端以添加每个平台服务的特定权限或范围。

为了使您的应用程序能够访问平台服务，您的JSON网络令牌（JWT）必须包含该平台服务所需的范围。例如，访问控制服务需要的某些范围为 acs.policies.read acs.policies.write。

OAuth2客户端使用一个授权批准来请求一个访问令牌。根据您使用的授权批准类型，您必须更新您的OAuth2客户端来生成所需的JWT。关于如何创建OAuth2客户端的更多信息，请参见[创建OAuth2客户端](https://www.predix.io/docs/?r=133567#LBV6ivqW-ao7RnIco)

如果您使用UAA仪表板创建其他客户端，客户端被默认创建为用于 client\_credentials 授权类型。另外，会自动为客户端添加某些所需的权限和范围。您必须添加每个服务特定的其他权限或范围。

另外，管理员客户端未分配能够默认更改用户密码的权限。如果您需要更新或更改用户密码，您必须为您的管理员客户端添加 uaa.admin 权限。

以下过程显示了更新使用客户凭据授权的OAuth2客户端所需的步骤。

1. 在控制台视图中，选择您的服务所处的空间。
2. 在服务实例页面中，选择您需要配置的UAA实例。
3. 选择配置服务实例选项。
4. 在UAA仪表板登录页面中，指定您的管理员客户端密码并点击登录。
5. 在UAA仪表板中，选择客户端管理选项卡。

客户端管理选项卡包括两部分，客户端和服务实例。服务实例部分显示您已经为您的服务创建的服务实例。

***注：此处显示的服务实例是那些您使用您想要配置的UAA创建的实例。您使用其他UAA实例创建的服务实例不显示在此页面上。***

1. 在服务实例部分，在您需要更新客户端的服务中点击+ 授权客户端选项。
2. 从列表中选择一个现有客户端或选择添加一个新客户端选项。如果您选择添加一个新客户端，请遵循[创建一个OAuth2客户端](https://www.predix.io/docs/?r=207663#uAyBrT9y-ao7RnIco)中的步骤。
3. 点击提交。
4. 在客户端管理选项卡中，点击与您在上一步中添加的客户端相对应的编辑图标。
5. 在编辑客户端窗体中指定以下值：

| **字段** | **说明** |
| --- | --- |
| 授权的授权类型 | 从下面选择一个或多个授权类型：* + client\_credentials

当您使用客户端凭据授权类型时，UAA中的OAuth2端点接受客户端ID和客户端密码并提供访问令牌。客户端默认通过 client\_credentials授权创建。* + implicit

当您使用隐式授权类型时，UAA直接为客户端发布访问令牌，无需认证该客户端。这减少了获取访问令牌所需往返行程的数量。* + password

当您使用资源所有者密码凭据授权类型时，UAA中的OAuth2端点接受用户名和密码并提供访问令牌。* + authorization\_code

当您使用授权代码授权类型时，客户端将资源所有者定向至UAA，然后UAA反过来通过授权代码将资源所有者定向至客户端。* + refresh\_token

刷新令牌是用于得到访问令牌的凭据。您可以选择这个选项从UAA获得刷新令牌。当目前使用的访问令牌无效或过期时，您可以使用刷新令牌从UAA获得一个新访问令牌，或者获得附加的相同或减少范围的访问令牌关于不同授权类型的更多信息，请参见[RFC 6749](https://tools.ietf.org/html/rfc6749%22%20%5Ct%20%22_blank)。 |
| 范围 | 默认为客户端分配部分需要的范围。对于新的客户端，管理员可以根据所选的授权类型选择要添加的范围。如果您选择authorization\_code,password与implicit授权类型，您必须通过服务特定范围更新范围。关于为每个服务添加的范围的完整列表，请参见[平台服务所需的权限或范围](https://www.predix.io/docs/?r=207661" \l "Mwn2Won" \t "_self)。关于可用的UAA范围的完整列表，请参见[被UAA授权的范围](https://github.com/GESoftware-CF/uaa/blob/master/docs/UAA-APIs.rst%22%20%5Cl%20%22scopes-authorized-by-the-uaa) |
| 权限 | 默认为客户端分配部分需要的权限。对于新的客户端，管理员可以根据所选的授权类型选择要添加的权限。如果您选择 client\_credentials 授权类型，您必须通过服务特定权限更新权限。关于为每个服务添加的范围的完整列表，请参见[平台服务所需的权限或范围](https://www.predix.io/docs/?r=207660" \l "Mwn2Won" \t "_self)。关于可用的UAA权限的完整列表，请参见[被UAA授权的范围](https://github.com/GESoftware-CF/uaa/blob/master/docs/UAA-APIs.rst%22%20%5Cl%20%22scopes-authorized-by-the-uaa) |
| 自动批准的范围 | 为客户端指定可以自动批准的范围，无需资源所有者的明确批准。 |
| 重定向URI | 指定一个重定向URI在登录后对客户端进行重定向。例如，http://example-app.com/welcome。当您开始将UAA用作服务提供者时，该URI用于您的外部身份提供者。 |
| 访问令牌有效性 | 指定访问令牌失效时间，单位毫秒。 |
| 刷新令牌有效性 | 指定刷新令牌失效时间，单位毫秒。 |
| 允许的提供者 | 如果有的话，指定外部身份提供者的名称。如果您正在使用外部身份提供者，同时将UAA用作服务提供者，则该字段为必填。 |

下一步：

在UAA仪表板中您可以完成以下附加的任务：

* 如果您正在使用授权类型如Authorization Code，Implicit或 Resource Owner Password，您可以在UAA中管理用户。
* 您能为用户密码[创建密码策略](https://www.predix.io/docs/?r=133560#SSqTSghl)。
* 您可以使用外部的身份提供者或使用UAA作为一个身份提供者。请参见[管理身份提供者](https://www.predix.io/docs/?r=133559#LigRvar4)。

如果您已经完成了设置OAuth2客户端，您可以[绑定您的应用程序到您的服务实例](https://www.predix.io/docs/?r=133558#E1yVyasD)。

平台服务所需的权限或范围

当您创建一个新的OAuth2客户端时，为客户端分配默认的范围和权限。您必须添加每个服务特定的其他权限或范围。

下表列出了每个平台服务的特定范围和权限，您必须将其添加到您的OAuth2客户端。

| **服务名称** | **权限/范围** |
| --- | --- |
| 访问控制 | * acs.policies.read
* acs.policies.write
* acs.attributes.read
* acs.attributes.write
* predix-acs.zones.<acs\_instance\_guid>.user

如果您使用UAA仪表板，该值会默认添加。当您将您的应用程序与您的ACS服务实例绑定时，它还可以在VCAP\_SERVICES环境变量中生成，用作oauth-scope 。 |
| 租户管理 | * tms.tenant.read
* tms.tenant.write
* predix-tms.zones.<tms\_instance\_guid>.user（默认添加）
 |
| 分析目录 | analytics.zones.<service\_instance\_guid>.user（默认添加） |
| 分析运行时 | analytics.zones.<service\_instance\_guid>.user（默认添加） |
| 资产 | predix-asset.zones.<service\_instance\_guid>.user（默认添加） |
| 事件中心 | * 发布
	+ predix-event-hub.zones.<Predix-Zone-Id>.user
	+ predix-event-hub.zones.<Predix-Zone-Id>.wss.publish
	+ predix-event-hub.zones.<Predix-Zone-Id>.grpc.publish
* 订阅
	+ predix-event-hub.zones.<Predix-Zone-Id>.user
	+ predix-event-hub.zones.<Predix-Zone-Id>.grpc.subscribe
 |
| 时间序列 | * 数据获取
	+ timeseries.zones.<Predix-Zone-Id>.user（默认添加）
	+ timeseries.zones.<Predix-Zone-Id>.ingest
* 数据查询
	+ timeseries.zones.<Predix-Zone-Id>.user（默认添加）
	+ timeseries.zones.<Predix-Zone-Id>.query
 |
| 视图 | * views.zones.<view\_instanceId>.user（默认添加）
* views.admin.user
* views.power.user
 |

使用UAAC更新OAuth2客户端

在Predix.io中使用UAAC代替图形用户界面更新OAuth2客户端的可选步骤。

为了使您的应用程序能够访问平台服务，您的JSON网络令牌（JWT）必须包含该平台服务所需的范围。例如，访问控制服务需要的某些范围为 acs.policies.read acs.policies.write。关于一个服务所需范围的完整列表，请参见每个服务的相关部分。

OAuth2客户端使用一个授权请求一个访问令牌。OAuth2定义了四种授权类型。根据您使用的授权类型，您必须更新您的OAuth2客户端以生成所需的JWT。关于如何创建OAuth2客户端的更多信息，请参见[创建OAuth2客户端](https://www.predix.io/docs/?r=207659#uAyBrT9y-ao7RnIco)。

**更新使用客户端凭据授权的OAuth2客户端**

在您开始前

本步骤使用UAA命令行界面（UAAC）。关于安装UAAC的更多信息，请参见<https://github.com/cloudfoundry/cf-uaac>。

以下步骤显示了更新使用客户凭据授权的OAuth2客户端所需的步骤。

1. 将您的UAA实例指定为预定目标。

uaac target <uaa\_instance\_url>

<uaa\_instance\_url> 是您的可信发布者的URL，例如， https://11fa0273-9e2a-37e2-9d06-2c95a1f4f5ea.predix-uaa.run.aws-usw02-pr.ice.predix.io。您可以在将您的UAA实例与一个应用程序绑定之后从VCAP\_SERVICES环境变量中检索该URL。

1. 使用管理客户端登录UAAC。

uaac token client get admin

提示时指定 <client\_secret> 。

1. 通过所需的权限（范围）更新OAuth2客户端，以访问您的服务实例：

uaac client update admin --authorities <set\_of\_authorities>

其中 <set\_of\_authorities> 是您现有的权限集合加上平台服务所需的权限。您可以使用以下命令检索现有的权限集合：

uaac client get admin

***注：***

***您必须提供一个完整的权限集合，包括现有的权限和您的服务所需的权限。如果您仅指定权限的一个子集，那么现有权限将被覆盖。***

Predix服务所需的权限（范围）如下所述：

|  |  |
| --- | --- |
| **服务名称** | **权限** |
| 访问控制 | * + acs.policies.read
	+ acs.policies.write
	+ acs.attributes.read
	+ acs.attributes.write
	+ predix-acs.zones.<acs\_instance\_guid>.user
 |
| 租户管理 | * + tms.tenant.read
	+ tms.tenant.write
	+ predix-tms.zones.<tms\_instance\_guid>.user
 |
| 分析目录 | analytics.zones.<service\_instance\_guid>.user |
| 分析运行时 | analytics.zones.<service\_instance\_guid>.user |
| 资产 | predix-asset.zones.<service\_instance\_guid>.user |
| 时间序列 | * + 数据获取
		- timeseries.zones.<Predix-Zone-Id>.user
		- timeseries.zones.<Predix-Zone-Id>.ingest
	+ 数据查询
		- timeseries.zones.<Predix-Zone-Id>.user
		- timeseries.zones.<Predix-Zone-Id>.query
 |
| 视图 | * + views.zones.<view\_instanceId>.user
	+ views.admin.user
	+ views.power.user
 |
|  |  |

1. 通过客户端凭据授权再次获取令牌。

uaac token client get admin

1. 如果要验证令牌中的范围已更新，请使用以下命令：

uaac token decode

**更新使用其他授权类型的OAuth2客户端**

在您开始前

本步骤使用UAA命令行界面（UAAC）。关于安装UAAC的更多信息，请参见<https://github.com/cloudfoundry/cf-uaac>。

以下流程显示了更新使用以下任意一种授权的OAuth2客户端所需的步骤。

* 授权代码
* 隐式
* 资源所有者密码
* 刷新令牌

步骤

1. 将您的UAA实例指定为预定目标。

uaac target <uaa\_instance\_url>

<uaa\_instance\_url> 是您的可信发布者的URL，例如， https://11fa0273-9e2a-37e2-9d06-2c95a1f4f5ea.predix-uaa.run.aws-usw02-pr.ice.predix.io。您可以在将您的UAA实例与一个应用程序绑定之后从VCAP\_SERVICES环境变量中检索该URL。

1. 使用管理客户端登录UAAC。

uaac token client get admin

提示时指定 <client\_secret> 。

1. 在UAA中创建一个平台服务所需的用户组。

uaac group add <service\_scope>

其中，<service\_scope>是您需要为您的服务创建的用户组。

Predix平台服务所需的用户组如下所述：

|  |  |
| --- | --- |
| **服务名称** | **范围** |
| 访问控制 | * + acs.policies.read
	+ acs.policies.write
	+ acs.attributes.read
	+ acs.attributes.write
	+ predix-acs.zones.<acs\_instance\_guid>.user
 |
| 租户管理 | * + tms.tenant.read
	+ tms.tenant.write
	+ predix-tms.zones.<tms\_instance\_guid>.user
 |
| 分析目录 | analytics.zones.<service\_instance\_guid>.user |
| 分析运行时 | analytics.zones.<service\_instance\_guid>.user |
| 资产 | predix-asset.zones.<service\_instance\_guid>.user |
| 时间序列 | * + 数据获取
		- timeseries.zones.<Predix-Zone-Id>.user
		- timeseries.zones.<Predix-Zone-Id>.ingest
	+ 数据查询
		- timeseries.zones.<Predix-Zone-Id>.user
		- timeseries.zones.<Predix-Zone-Id>.query
 |
| 视图 | * + view.zones.<view\_instance\_ID>.user
	+ views.admin.user
	+ views/power.user
 |

1. 在UAA中创建一个可以管理平台服务的新用户。

***注：如果用户已经存在了，您可以跳过这一步。***

uaac user add <user\_name> -p [password] --emails <user\_name>@example.com

1. 将成员资格分配给所需的范围。

uaac member add <service\_scope> <user\_name>

您可以使用逗号分隔列表指定多个用户名。

1. 通过一个平台服务所需的范围更新OAuth2客户端。

uaac client update <client\_name> \ --scope <service\_scopes> \ --authorized\_grant\_types <grant\_type> \ --authorities uaa.resource

<grant\_type> 可以是其中一个或 authorization\_code, implicit, password和refresh\_token的组合。您可以使用逗号分隔列表指定多个授权类型。

1. 使用管理用户登录UAAC。

uaac token owner get <service\_client> <service\_user>

提示时指定 <client\_secret> 。

1. 如果要验证令牌中的范围已更新，请使用以下命令：

uaac token decode

将您的应用程序与一个平台服务实例连接

如果要在您创建的服务实例与您的应用程序之间建立通信，您可以将您的应用程序与服务实例绑定。

在您开始前

将您的应用程序推送到Cloud Foundry中。

当您将您的应用程序与您的服务实例绑定时，Cloud Foundry在VCAP\_SERVICES环境变量中提供服务的连接详细信息。Cloud Foundry运行时使用VCAP\_SERVICES环境变量与部署的关于其环境的应用程序进行通信。

您可以从VCAP\_SERVICES环境变量中检索以下实例详细信息：

* 一个用于您的服务实例的 instance\_uri 。
* instance\_GUID 是您的服务实例的 zoneID 。
* 访问您的服务实例的HTTP标头信息。它包括：
	+ http-header-name 用作 Predix-Zone-Id
	+ http-header-value
* 一个用于您的实例的 oauth-scope 。最终用户令牌需要访问特定服务实例的范围。

如果您与一个UAA服务实例绑定，除了 instance\_uri 与 instance\_GUID您将收到以下信息：

* 一个用于您的实例的 uaa\_instance\_issuerId 。当您创建使用您的UAA实例进行认证的其他服务的一个实例时， issuerID 是必需的。

步骤

1. 使用Cloud Foundry CLI登录Cloud Foundry。

cf login -a <API\_Endpoint>

<API\_Endpoint> 的值在您注册Predix.io用户账号时接收的Predix欢迎电子邮件中。根据您注册的Predix.io， <API\_Endpoint> 的值为以下其中一个：

* + Predix美国西部

https://api.system.aws-usw02-pr.ice.predix.io

* + Predix美国东部

https://api.system.asv-pr.ice.predix.io

* + Predix日本

https://api.system.aws-jp01-pr.ice.predix.io

* + Predix英国

https://api.system.dc-uk01-pr.ice.predix.io

例如，

cf login -a https://api.system.aws-usw02-pr.ice.predix.io

该命令产生以下输出：

Email> <your\_predix\_login> Password> <your\_predix\_password> Authenticating...OK Targeted org <your\_predix\_org> Targeted space dev   API endpoint: https://api.system.aws-usw02-pr.ice.predix.io (API version: <version>)   User: <your\_predix\_login> Org:  <your\_predix\_org>  Space: dev

1. 通过输入以下命令将您的应用程序与服务实例绑定：

cf bind-service <your\_app\_name> <service\_instance\_name>

您的应用程序与 <service\_instance\_name> 实例绑定，返回以下消息：

Binding service <service\_instance\_name> to app <your\_app\_name> in org predix-platform / space predix as userx@ge.com...OK TIP: Use 'cf restage' to ensure your env variable changes take effect

1. 通过输入以下命令验证绑定：

cf env <your\_app\_name>

如果您将一个应用程序myApp与一个UAA实例绑定，则返回以下消息：

Getting env variables for app myApp in org predix-platform / space security as userx@ge.com...OK ...],"predix-uaa": [{    "credentials":{     "issuerId":"https://ff27c315-d027-4d1d-a30c-64f49b369ed9.predix-uaa.run.aws-usw02-pr.ice.predix.io/oauth/token",     "uri":"https://ff27c315-d027-4d1d-a30c-64f49b369ed9.predix-uaa.run.aws-usw02-pr.ice.predix.io",      "zone": {"http-header-name": "X-Identity-Zone-Id","http-header-value": "ff27c315-d027-4d1d-a30c-64f49b369ed9"}    },    "label":"predix-uaa",    "name":"my\_uaa\_instance",    "plan":"free",    "tags":[]   }  ],

在本示例中，显示以下值：

* uaa\_instance\_issuerId = https://ff27c315-d027-4d1d-a30c-64f49b369ed9.predix-uaa.run.aws-usw02-pr.ice.predix.io/oauth/token
* uaa\_instance\_uri = https://ff27c315-d027-4d1d-a30c-64f49b369ed9.predix-uaa.run.aws-usw02-pr.ice.predix.io
* uaa\_instance\_GUID = ff27c315-d027-4d1d-a30c-64f49b369ed9

如果您将一个应用程序myApp与ACS服务实例绑定，则返回以下消息：

Getting env variables for app myApp in org predix-platform / space security as userx@ge.com...OK ...],"predix-acs": [{"credentials": {"uri": "https://predix-acs.run.aws-usw02-pr.ice.predix.io","zone": {"http-header-name": "Predix-Zone-Id","http-header-value": "9615a95a-9275-4a82-926d-89f06cbe04e1","oauth-scope": "predix-acs.zones.9615a95a-9275-4a82-926d-89f06cbe04e1.user"}},"label": "predix-acs","name": "acs-sample-instance","plan": "Tiered","provider": null,"syslog\_drain\_url": null,"tags": []}],

在本示例中，显示以下值：

* acs\_instance\_uri = https://predix-acs.run.aws-usw02-pr.ice.predix.io
* acs\_instance\_GUID = 9615a95a-9275-4a82-926d-89f06cbe04e1
* http-header-name = Predix-Zone-Id
* http-header-value = 9615a95a-9275-4a82-926d-89f06cbe04e1
* oauth-scope = predix-acs.zones.9615a95a-9275-4a82-926d-89f06cbe04e1.user