UAA服务设置

开始使用某些Predix平台服务之前，您必须将一个UAA服务实例设置为可信发布者。

**任务路线图**

| **编号** | **任务** | **说明** |
| --- | --- | --- |
| 1 | （可选）如有必要，配置您的代理设置。 | 根据您的位置和网络配置，您可能需要配置您的代理设置，以便访问远程资源。参见[定义与远程资源的代理连接](https://www.predix.io/docs/?r=52230#NAaO6p6A)。 |
| 2 | （可选）部署一个Predix Hello World网页应用程序。 | [创建一个简单的Predix Hello World网页应用程序](https://www.predix.io/docs/?r=52229#IqAL3Fzb)。 |
| 3 | 创建UAA服务实例。 | 参见[创建一个UAA服务实例](https://www.predix.io/docs/?r=52228#XpKGAdQ7-Q0CoIStl)。 |
| 4 | 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。参见[创建一个OAuth2客户端](https://www.predix.io/docs/?r=52227#uAyBrT9y-ao7RnIco)。 |
| 5 | 创建用户组以设置用户需要的许可。 | 一个用户组代表一个用户的权限。参见[在一个UAA实例中创建用户组](https://www.predix.io/docs/?r=52226#ZHglCMC7)。 |
| 6 | 在UAA实例中创建用户。 | 如果UAA要认证用户，用户必须首先在UAA中创建。您既可以在UAA本地创建用户也可以与外部身份提供者联合。关于在本地创建用户的信息，请参见[在一个UAA实例中创建用户](https://www.predix.io/docs/?r=52225#RulzoBew)。如果要通过UAA设置联合身份，请参见[使用UAA进行SAML联合](https://www.predix.io/docs/?r=52224#LigRvar4)。 |
| 7 | 将您的应用程序与服务实例绑定。 | 参见[将一个应用程序与UAA实例绑定](https://www.predix.io/docs/?r=52223#sXp7cw5P)。 |

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. 用您的Predix账号登录https://www.predix.io。
2. 导航至目录 > 服务选项卡，然后点击“用户账号和认证”选项。
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服务实例的可选过程。

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。

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": {"issuerId": "https://ge-digital.sb-uaa.grc-apps.svc.ice.ge.com/oauth/token","subdomain": "ge-digital","uri": "https://ge-digital.sb-uaa.grc-apps.svc.ice.ge.com","zone": {"http-header-name": "X-Identity-Zone-Id","http-header-value": "011d56b9-831e-407d-98d0-da4c1c946862"}},"label": "predix-uaa","name": "test-1","plan": "tiered","provider": null,"syslog\_drain\_url": null,"tags": []}],

将一个应用程序与UAA实例绑定

您必须将您的应用程序与您的UAA实例绑定，以便在VCAP\_SERVICES环境变量中提供其连接的详细信息。Cloud Foundry运行时使用VCAP\_SERVICES环境变量在部署的应用程序与其环境之间进行通信。

您可以从VCAP\_SERVICES环境变量中检索以下UAA实例详细信息：

* 一个用于您的实例的dashboard\_url。您可以使用这个URL来访问UAA Dashboard工具管理UAA实例。
* 一个除了为UAA创建的域您可能需要用到的子域subdomain。
* 一个用于您的实例的 uaa\_instance\_uri 。
* 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。
* 一个 uaa\_instance\_GUID 是您的实例的 zoneID 。
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. 通过输入以下命令将应用程序与服务实例绑定：

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

<uaa\_instance\_name> 实例与您的应用程序绑定，将返回以下消息：

Binding service <uaa\_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>

返回与以下消息类似的消息：:

1. Getting env variables for app myApp in org predix-platform / space security as userx@ge.com...
2. OK
3. ...
4. ],
5. "predix-uaa": [
6. {
7. "credentials":
8. {
9. "dashboardUrl": "https://uaa-dashboard.run.asv-pr.ice.predix.io/#/login/ff27c315-d027-4d1d-a30c-64f49b369ed9",
10. "issuerId":
11. "https://ff27c315-d027-4d1d-a30c-64f49b369ed9.predix-uaa.run.aws-usw02-pr.ice.predix.io/oauth/token",
12. "subdomain": "ff27c315-d027-4d1d-a30c-64f49b369ed9",
13. "uri":
14. "https://ff27c315-d027-4d1d-a30c-64f49b369ed9.predix-uaa.run.aws-usw02-pr.ice.predix.io",
15. "zone": {
16. "http-header-name": "X-Identity-Zone-Id",
17. "http-header-value": "ff27c315-d027-4d1d-a30c-64f49b369ed9"
18. }
19. },
20. "label":
21. "predix-uaa",
22. "name":
23. "my\_uaa\_instance",
24. "plan":
25. "free",
26. "tags":
27. []
28. }

   ],

在本样例中，显示以下值：

* + dashboard\_url = https://uaa-dashboard.run.asv-pr.ice.predix.io/#/login/ff27c315-d027-4d1d-a30c-64f49b369ed9
	+ uaa\_instance\_issuerId = https://ff27c315-d027-4d1d-a30c-64f49b369ed9.predix-uaa.run.aws-usw02-pr.ice.predix.io/oauth/token
	+ subdomain = 04187eb1-e0cf-4874-8218-9fb77a8b4ed9
	+ 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

解除UAA实例与您的应用程序的绑定

解除一个服务实例的绑定：

cf unbind-service <your\_app\_name> <uaa\_instance\_name>

服务实例与应用程序解除绑定，返回以下消息：

Unbinding app predix-service from service userX in org predix-platform / space predix as userx@ge.com...OK

删除一个UAA实例

删除一个服务实例：

cf delete-service predix-uaa <uaa\_instance\_name>