文章
Hao Ma · 一月 15, 2021 阅读大约需 3 分钟

IAM实践指南——OAuth 2.0下的API保卫战（第一部分）

介绍

目前，诸多应用程序通过开放授权框架（OAuth）来安全、可靠、高效地访问各种服务中的资源。InterSystems IRIS目前已兼容OAuth 2.0框架。事实上社区有一篇关于OAuth 2.0和InterSystems IRIS的精彩文章，链接如下。

然而，随着API管理工具的出现，一些组织开始将其用作单点身份验证，从而防止未经授权的请求到达下游服务，并将授权/身份验证复杂性从服务本身分离出来。

您可能知道，InterSystems已经推出了自己的API管理工具，即InterSystems API Management （IAM），以IRIS Enterprise license（IRIS
Community版本不含此功能）的形式提供。这里是社区另一篇介绍InterSystems AIM的精华帖。

这是三篇系列文章中的第一篇，该系列文章将展示如何在OAuth
2.0标准下使用IAM简单地为IRIS中的未经验证的服务添加安全性。

第一部分将介绍OAuth
2.0相关背景，以及IRIS和IAM的初始定义和配置，以帮助读者理解确保服务安全的整个过程。

本系列文章的后续部分还将介绍两种使用IAM保护服务的可能的场景。在第一种场景中，IAM只验证传入请求中的访问令牌，如果验证成功，则将请求转发到后端。在第二种场景中，IAM将生成一个访问令牌（充当授权服务器）并对其进行验证。

因此，第二篇将详细讨论和展示场景1中的配置步骤，第三篇将讨论和演示场景2中的配置以及一些最终要考虑的因素。

如果您想试用IAM，请联系InterSystems销售代表。

OAuth 2.0背景

每个OAuth 2.0授权流程基本上都由4个部分组成：

1. 用户
2. 客户端
3. 授权服务器
4. 资源所有者

简单起见，本文使用“ 资源所有者密码凭证 ” OAuth流（可以在IAM中使用任何OAuth流）。另外，本文将不指定任何使用范围。
注意：因为资源所有者密码凭证流直接处理用户凭证，所以应该只在客户端应用程序高度受信任时使用。在大多数情况下，客户端应为第一方应用程序。

通常，资源所有者密码凭证流遵循以下步骤：

1. 用户在客户端应用程序中输入凭证（如用户名和密码）
2. 客户端应用程序将用户凭证和自身的标识（如客户端ID和客户端密钥）一起发送到授权服务器。授权服务器验证用户凭证和客户端标识，并返回访问令牌

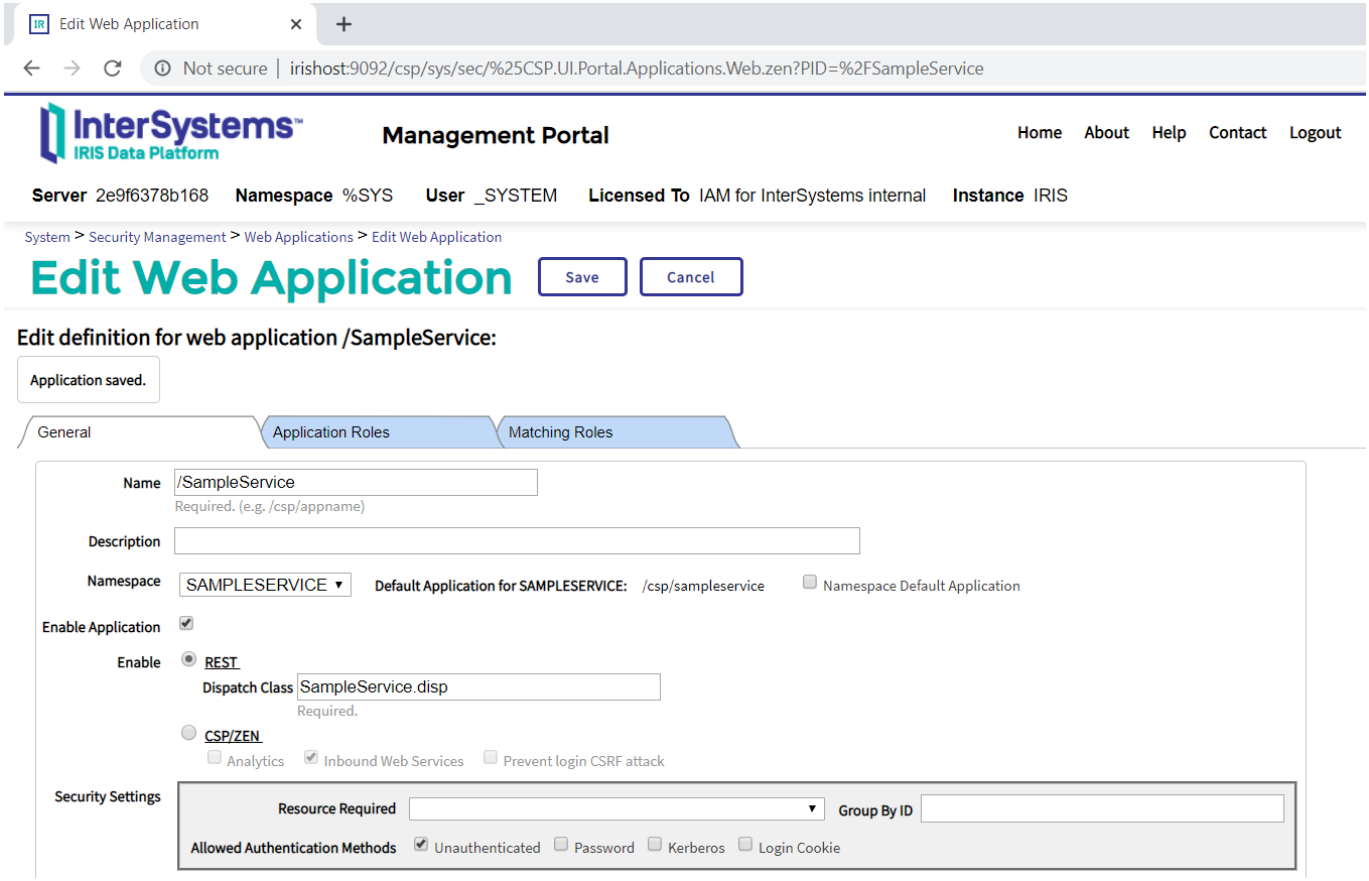
3. 客户端使用令牌访问资源服务器上的资源
4. 资源服务器首先验证收到的访问令牌，然后再将信息返回给客户端

考虑到这种情况，你可以在两种场景下使用IAM应对OAuth 2.0：

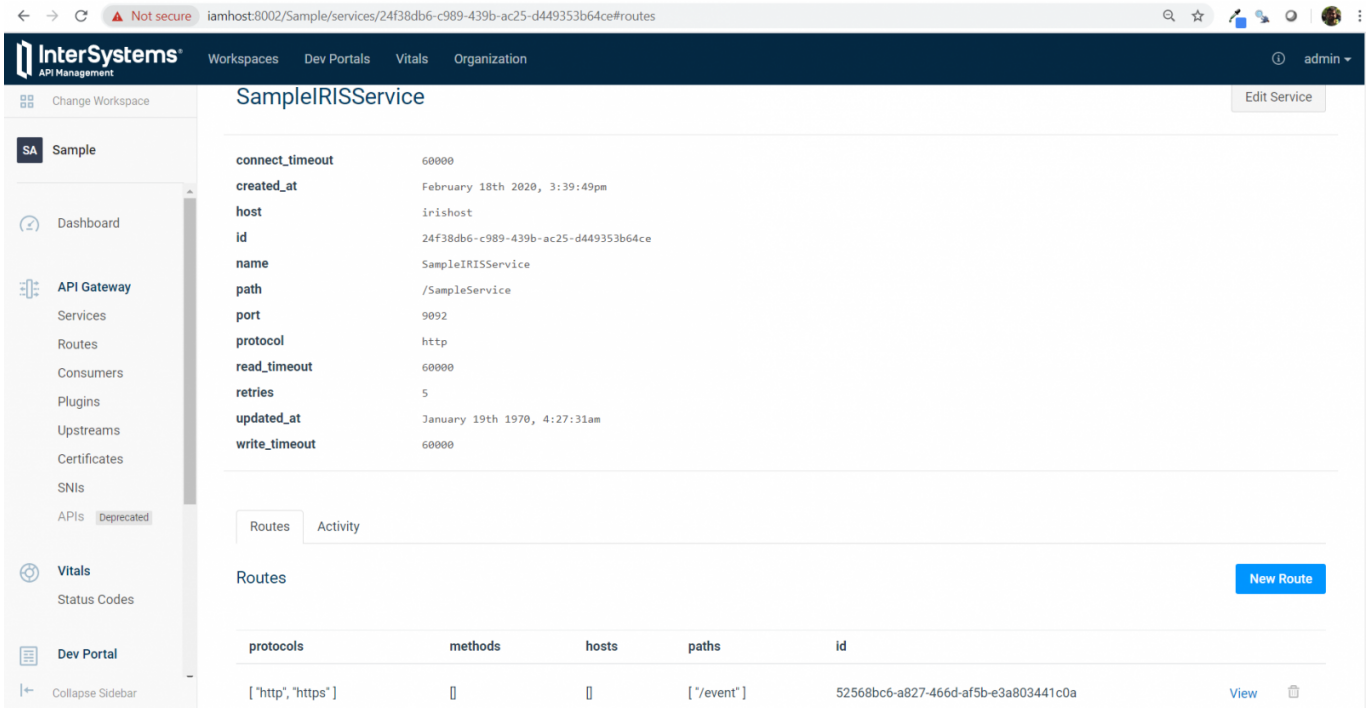
1. IAM充当验证器，验证客户端应用程序提供的访问令牌，仅在访问令牌有效时才将请求转发给资源服务器；在这种情况下，访问令牌将由第三方授权服务器生成
2. IAM既充当授权服务器（向客户端提供访问令牌），又充当访问令牌验证器，在将请求重定向到资源服务器之前验证访问令牌。

IRIS和IAM初始定义和配置

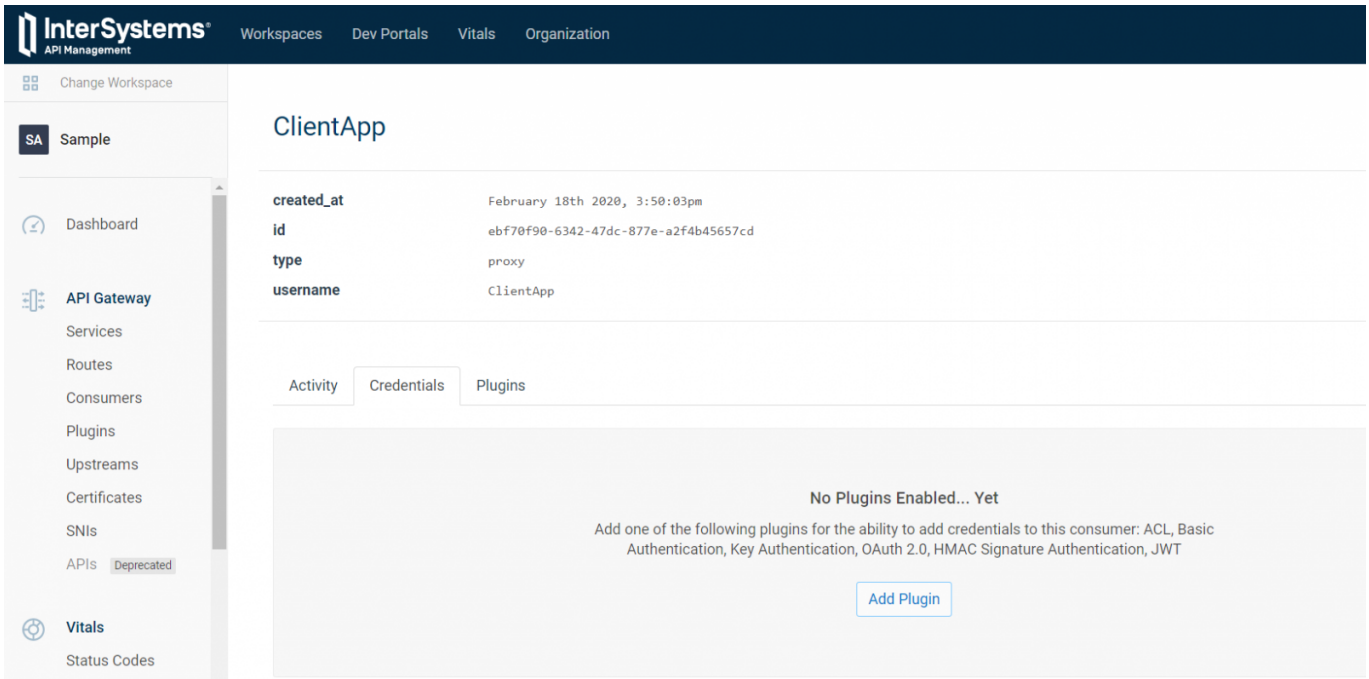
本文中使用名为“ /SampleService ”的IRIS Web应用程序。从下面的截屏中可以看到，这是一个在IRIS中部署的未经身份验证的REST服务：



此外，在IAM端配置了一个名为“ SampleIRISService ”的服务，其包含一个路由，如以下截屏所示：



再者，在IAM中配置了一个名为“ ClientApp ”的客户端（初始没有任何凭据），用来识别谁在调用IAM中的API：



经上述配置，IAM将发送到以下URL的每个GET请求代理到IRIS：

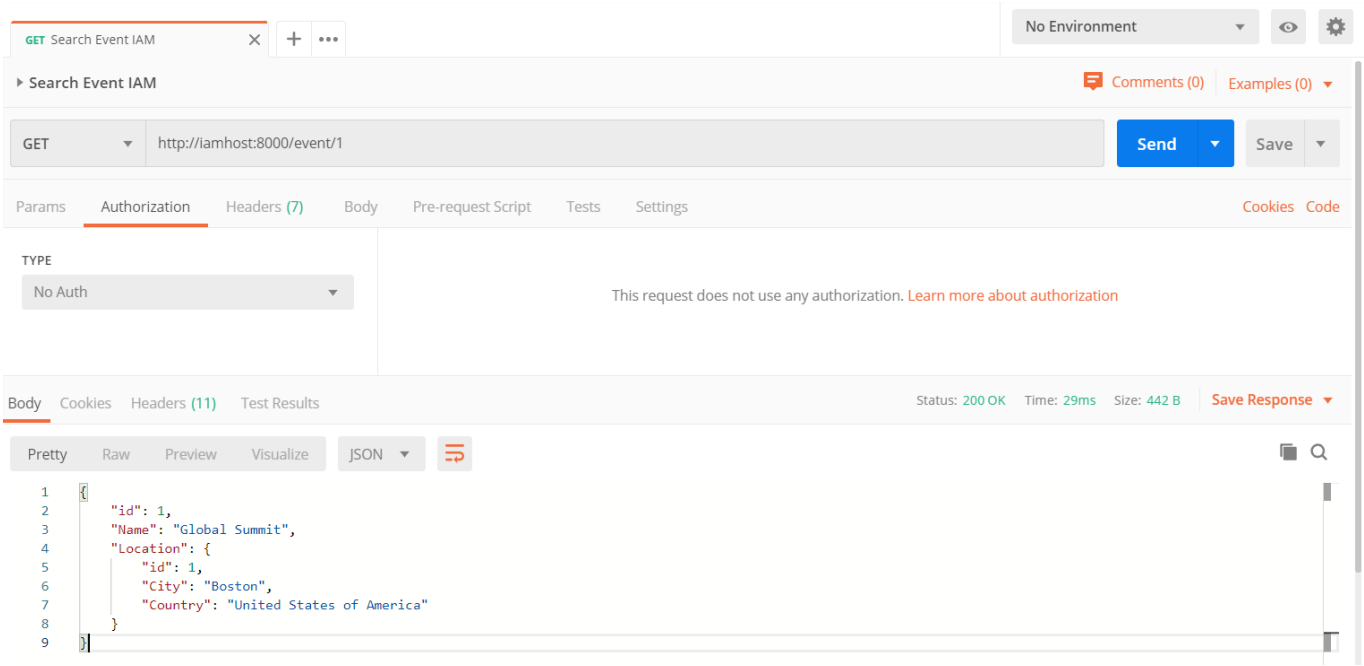
http://iamhost:8000/event

此时还没有使用身份验证。所以，如果将一个简单的GET请求（未进行身份验证）发送到URL：

http://iamhost:8000/event/1

我们将获得期望的响应。

本文中，我们使用名为 “ PostMan ” 的应用程序发送请求并检查响应。在下面的PostMan截屏中，可以看到简单的GET请求及其响应。



请继续阅读本系列的第2篇，了解如何配置IAM来验证传入请求中的访问令牌。

#API #OAuth2 #REST API #安全 #InterSystems IRIS

源URL: https://cn.community.intersystems.com/post/iam%E5%AE%9E%E8%B7%B5%E6%8C%87%E5%8D%97%E2%80%94%E2%80%94oauth-20%E4%B8%8B%E7%9A%84api%E4%BF%9D%E5%8D%AB%E6%88%98%EF%BC%88%E7%AC%AC%E4%B8%80%E9%83%A8%E5%88%86%EF%BC%89