**AWS动手实验IAM**

**实验目的**

创建一个能够拥有EC2所有权限的IAM用户  
找到URL并使用新建IAM用户登陆  
了解策略对服务访问的影响

**实验要求**

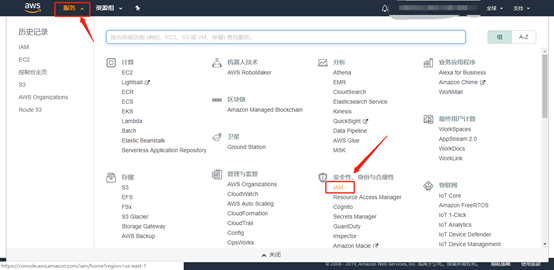
了解AWS Identity and Access Management（IAM）的基本概念

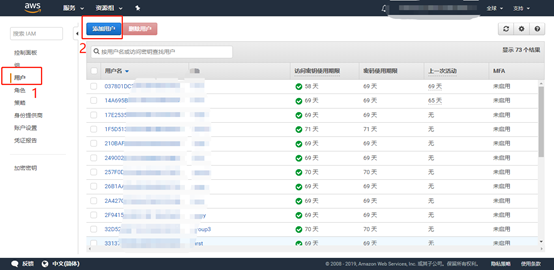
**实验原理**

AWS身份和访问管理（IAM），能够帮您在AWS中管理用户和用户权限。借助IAM，您可以集中管理用户，安全证书，如访问键，和权限控制哪些AWS资源，用户可以访问。

概念：  
**User**  
User(用户)，操作AWS资源的最直观，也是最终的载体。  
我们注册AWS用的账户也叫根账户，具有AWS所有的访问权限，AWS建议日常使用不要使用根账户来操作。而是单独在IAM控制台终创建User。  
**Group**  
Group（组），可以将用户分组，也可以定义组策略。  
**Role**  
Role（角色），可以绑定一系列的策略（Policies），常用来定义第三方登陆账户的AWS操作权限，或者接入应用对AWS的操作权限。和组不同，Role并不能添加已有的用户。  
**Policies**  
Policies（策略），定义对AWS操作权限的描述，AWS其实已经有了很多内建策略，如果我们并不需要那么细粒度的权限把控，其实并不需要我们来自己定义。  
**Identity Provider**  
Identity Provider（身份提供商），如果需要外部提供商登陆，比如常见Google，FaceBook这类的，就需要添加Identity provider并配置相关选项，在两者建立互信机制。

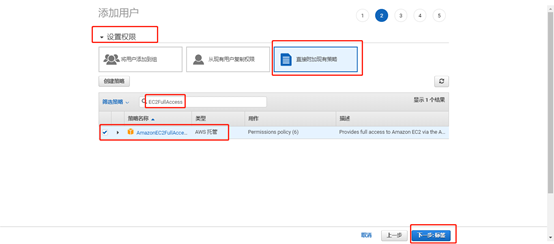
**实验步骤**

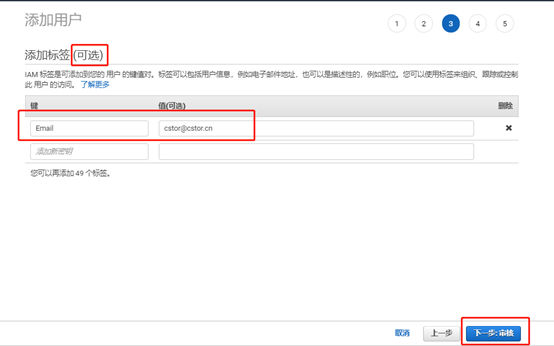
1.在AWS控制台的“服务”菜单上，单击IAM。  


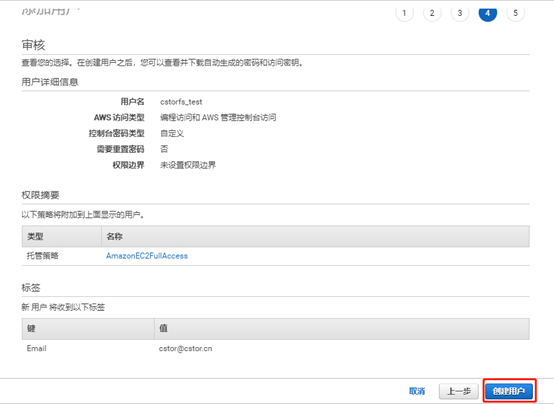
2.单击“用户”，单击添加用户，如下：  


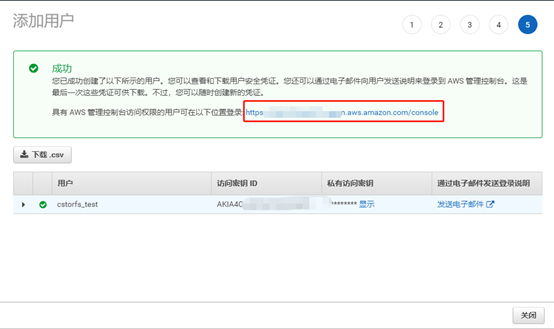
3.在“设置用户详细信息”选项卡中配置下列信息：

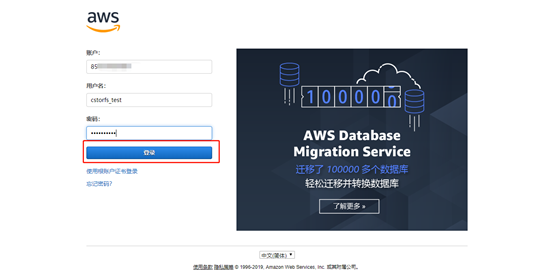
**用户名**：自定义  
**编程访问**：为 AWS API、AWS CLI、SDK和其它开放工具启用access Key和secret access Key。  
**AWS管理控制台访问**：Amazon Wen Services访问  
**控制台密码**：我们自定义一个密码。  
如下：  

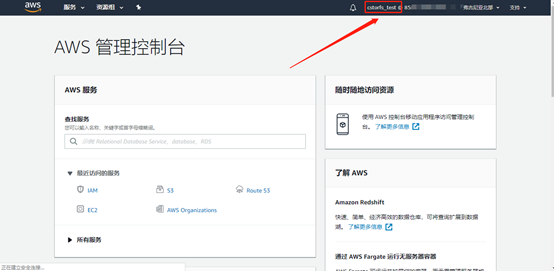

4.在“设置权限”选择卡中，选择“直接附加现有策略”，在搜索框中搜索“EC2FullAccess”，然后勾选它。单击“下一步：标签”，如下：  


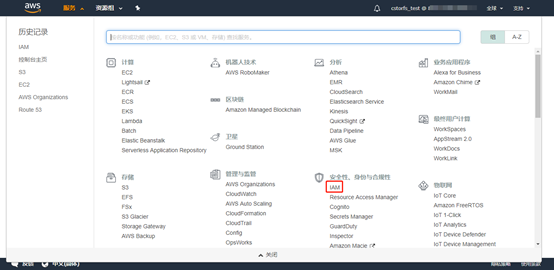
5.在“添加标签（可选）”选项卡中，为这个用户添加一个标签。如下：  


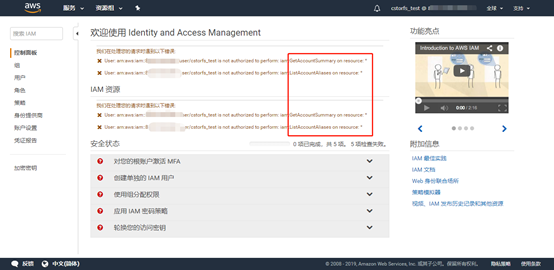
6.审核刚刚设置，点击“创建用户”，如下：  


7.页面显示成功，把登陆URL复制下来。  


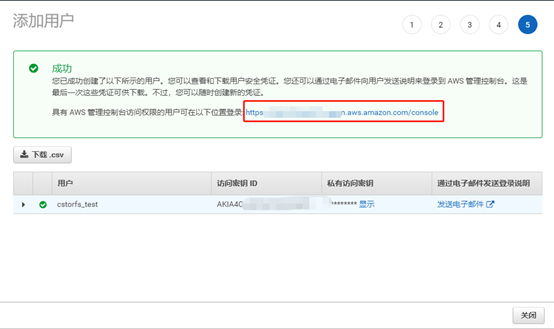
8.使用复制的URL打开新页面，并输入我们新建的用户名及密码，单击“登陆”，如下：  


9.然后我们就登陆到AWS Console了。在右上角可以看到我们的用户名  


10.在AWS控制台的左上角，单击“服务”菜单，然后点击“IAM”，如下：  


11.显示错误，因为此用户，没有访问IAM的权限，它仅拥有EC2的权限。  


**实验结果**

1.创建出一个IAM用户。  


2.使其能登陆AWS管理控制台  
