



赋予 Amazon EC2 实例权限

自主进度动手实验室

版本 3.0c

spl01c-creating-ec2-linux

版权归 ©2019 Amazon Web Services, Inc. 及其附属公司所有。保留所有权利。未经 Amazon Web Services, Inc. 事先书面许可，不得复制或转载本文的部分或全部内容。禁止商业性复制、出租或出售。

错误或更正？请发送电子邮件至 aws-course-feedback@amazon.com 联系我们。

其他问题？请通过 <https://aws.amazon.com/contact-us/aws-training/> 联系我们

目录

介绍	3
概述	3
所涵盖之主题	3
登录 AWS 管理控制台	4
创建新的 IAM 角色	4
IAM 角色	4
创建 IAM 角色	5
将既有的 EC2 实例赋予 IAM 角色	6
挑战单元：SSH 进入 EC2 并下 CLI 指令	7
结束您的实验室	8
附录	8
针对 Windows 用户的指示说明：通过 SSH 连接您的 Amazon EC2 实例	8
下载 PuttyGen 将 .Pem 密钥转换为 .PPK 格式	8
下载 PuTTY	9
使用 SSH 和 PuTTY 连接 Amazon EC2 实例。	9
结论	11
其他资源	11

介绍

概述

本实验室课程将带您在 Amazon 云中逐步启动和配置您的第一个 IAM 角色。您将学习如何使用 IAM 策略添加相关的权限，并且通过 IAM 角色将权限赋予给 EC2 实例。您可以使用 IAM 角色委派对 AWS 资源的访问权限，利用 IAM 角色，您可以在您的信任 账户和其他 AWS 可信 账户之间建立信任关系。信任账户拥有要访问的资源，可信账户包含需要资源访问权限的用户。在本次实验室课程结束时，您将会对于 IAM 在安全范畴上能够提供的好处有初步的理解

所涵盖之主题

在此实验室课程结束时，您将能够：

- 创建 IAM 角色。
- 理解如何将 IAM 角色附加至既有的 EC2 实例上。
- 借由 SSH 至 EC2 实例，验证是否有权限存取 S3 服务

登录 AWS 管理控制台

登录 AWS 管理控制台

1. 单击“启动实验”开始实验。
2. 单击“登录网址”，到达 AWS 管理控制台登录界面。
3. 使用这些证书登录控制台：
 - 在登录界面的“用户名”框中，输入“账号”。
 - 在“密码”框中，输入“密码”。
4. 单击“登录”。

创建新的 IAM 角色

在此模块中，您将创建一个新的 IAM 角色，该角色将赋予 EC2 实例可以访问其他 AWS 服务的权限，此实验中会以 S3 为例。

IAM 角色

在 EC2 实例上运行的应用程序必须将 AWS 凭证包含在其 AWS API 请求中。您可以让开发人员将 AWS 凭证直接存储在 EC2 实例中，并允许该实例中的应用程序使用这些凭证。但开发人员随后必须管理凭证，确保他们能安全地将凭证传递给每个实例，并在需要轮换凭证时更新每个 EC2 实例。这需要进行大量的额外工作。

相反，您可以且应使用 IAM 角色管理在 EC2 实例上运行的应用程序的临时凭证。在使用角色时，您不需要将长期凭证 (如用户名和密码或访问密钥) 分配给 EC2 实例。角色可提供临时权限供应用程序在调用其他 AWS 资源时使用。当您启动 EC2 实例时，可指定要与实例关联的 IAM 角色。然后，实例上运行的应用程序可使用角色提供的临时凭证对 API 请求进行签名。

若要使用角色向 EC2 实例上运行的应用程序授予权限，需要进行一点额外配置。EC2 实例上运行的应用程序由虚拟化操作系统从 AWS 中提取。因为存在这一额外分离操作，所以需要执行一个附加步骤将 AWS 角色及其关联权限分配给 EC2 实例，并使这些权限对其应用程序可用。此额外步骤是创建要附加到实例的实例配置文件。实例配置文件包含角色，并且可以为实例上运行的应用程序提供角色的临时凭证。然后，可以在应用程序的 API 调用中使用这些临时凭证访问资源，以及将访问限制为仅角色指定的那些资源。请注意，一次只能将一个角色分配给 EC2 实例，实例上的所有应用程序都共享相同的角色和权限。

以这种方式使用该角色拥有多种优势。因为角色凭证是临时的，并且会自动轮换，所以您不必管理证书，也不必担心长期安全风险。此外，如果您对多个实例使用单个角色，则可以对角色进行更改，而此更改会自动传播到所有实例。


创建 IAM 角色


延续先前实验一的内容，在此实验中您将先创建一个新的 IAM 角色


1. 单击位于上方“服务”菜单，在“安全 & 身份”分类中找到 IAM 并单击或是在空白搜寻栏位上直接输入 IAM。
2. 点击左侧导航栏中的“角色”，然后单击“创建角色”的蓝色按钮。
3. 在 AWS 产品类别中选择 EC2，接着单击“下一步：权限”。


创建角色

选择受信任实体的类型

 **AWS 产品**
EC2、Lambda 和其他

 **其他 AWS 账户**
属于您或第三方

 **Web 身份**
Cognito 或任何 OpenID 提供商

 **SAML 2.0 身份联合**
您的企业目录

允许 AWS 服务代表您执行操作。 [了解更多](#)

选择将使用此角色的服务

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

4. 在“步骤 2: 页面中的筛选策略中输入 S3，并在下方的策略名称中选择 “AmazonS3FullAccess”

创建策略

筛选策略

	策略名称	用作
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	无
<input checked="" type="checkbox"/>	AmazonS3FullAccess	无
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	无
<input type="checkbox"/>	QuickSightAccessForS3StorageManagement...	无

可以尝试点击进入 “AmazonS3FullAccess” 查看该策略的内容。基本上 IAM 策略皆是由 JSON 格式撰写，而该策略简言之是提供 S3 全部的权限

5. 单击“下一步：标签”。

- 单击“下一步：审核”。
- 在步骤 4 页的角色名称中输入“AllowEC2AccessS3”。



角色名称* AllowEC2AccessS3
请使用字母数字和'+=, @_-'字符。最长 64 个字符。

角色描述 Allows EC2 instances to call AWS services on your behalf.
最长 1000 个字符。请使用字母数字和'+=, @_-'字符。

可信任的实体 AWS 服务: ec2.amazonaws.com.cn

策略  AmazonS3FullAccess [策略](#)

- 单击“创建角色”。

将既有的 EC2 实例赋予 IAM 角色

Amazon EC2 控制面板的“Instances”页面上显示了当前所选区域中正在运行的所有 Amazon EC2 实例的列表。您可以在这里看到实例的状态。如果状态不是显示绿色的“Running”，则等待几分钟再刷新列表。

- 单击位于上方“服务”菜单，在“计算”分类中找到 EC2 并单击或是在空白搜寻栏位上直接输入 EC2。
- 选择您的实例。延续前一个实验一的作业，您的实例名称应该是“MyWebServer”。
- 点击上方的“操作”，选择“实例设置”，接着点选“附加/替换 IAM 角色”。



12. 在 IAM 角色的下拉选单中点击稍早创建的 “AllowEC2AccessS3” 。



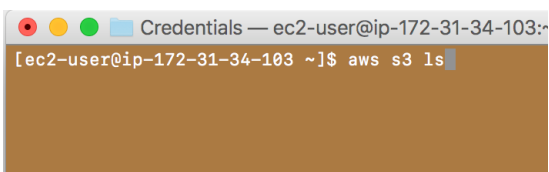
13. 点击 “应用” 。
14. 点击 “关闭” 以回到 EC2 控制页面。

到这边您已经完成 IAM 角色的授与！而且 IAM 角色的权限赋予是会立即生效，这代表此 EC2 实例已经能享用 S3 的服务。

挑战单元：SSH 进入 EC2 并下 CLI 指令

在此挑战中您透过 SSH 登入 EC2 实例。若你先前没有 SSH 到后端主机的经验，可以参考后面附录的介绍

15. SSH 登入之后尝试下以下指令： “aws s3 ls”



16. 预设 EC2 是没有权限存取 S3 服务，但由于在前一个步骤当中我们已经将 IAM 角色附加到该 EC2 实例上，“aws s3 ls” 将可以正常执行。该指令将列出所有 S3 buckets

结束您的实验室

遵循以下步骤关闭控制台、结束您的实验室。

17. 在 AWS 管理控制台的导航栏中，点击“UPT15xxxxxxxxxx@<AccountNumber>”，然后单击“注销”。
18. 在云平台的实验页面上，单击“结束实验”。
19. 在确认消息中，单击“OK”。

附录

针对 Windows 用户的指示说明：通过 SSH 连接您的 Amazon EC2 实例

注意 本部分仅适用于 Windows 用户。如果您运行的是 OSX 或 Linux 系统，则请跳过至下一部分。

在本部分中，您将使用 PuTTY Secure Shell (SSH) 客户端和您服务器的公有 DNS 地址来连接服务器。

所有 Amazon EC2 实例在启动时都分配了两个 IP 地址，即私有 IP 地址 (RFC 1918) 和公有 IP 地址，可通过网络地址转换 (NAT) 直接相互映射。私有 IP 地址只能在 Amazon EC2 网络内使用。公有地址可以在 Internet 网络内使用。

Amazon EC2 也提供内部 DNS 名称和公有 DNS 名称，它们会各自映射到私有和公有 IP 地址。内部 DNS 名称只能在 Amazon EC2 内使用。公有 DNS 名称可解析到 Amazon EC2 网络外的公有 IP 地址和 Amazon EC2 网络内的私有 IP 地址。

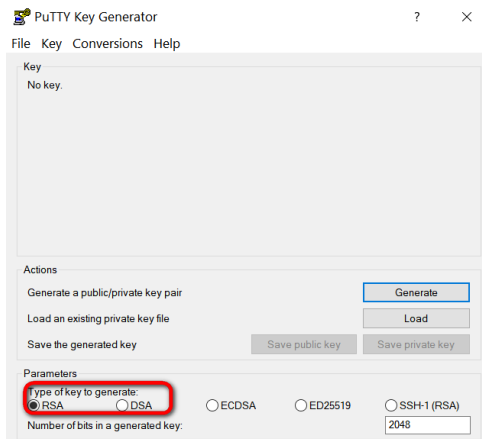
一：下载 PuTTY

注* 使用 PuTTY 您需要下载 PuttyGen 用来将 .pem 密钥 转换为 .ppk 格式

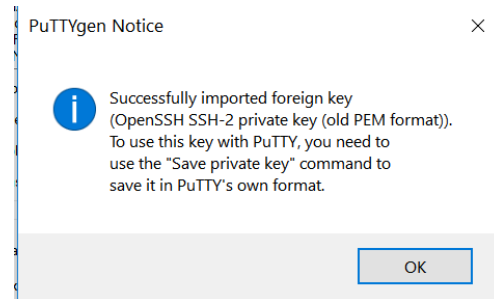
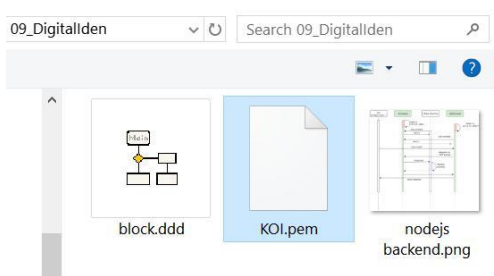
- 17.: 下载 PuttyGen 工具。打开后 点击 Load 加载.pem 证书。点击 Save private key 来保存.ppk 证书。

<https://puttygen.com/download.php?val=4>

18. 下载完毕后 打开 PuttyGen 选择 RSA 加密

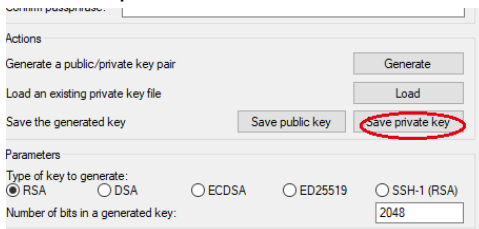


20. 点 load 按钮加载本地的 pem 文件



点击 OK

21. 将转换的 pkk 文件保存到本地 点击 Save private key



使用 SSH 和 PuTTY 连接 Amazon EC2 实例。

22. 如果您的机器上还没有安装 PuTTY 客户端，您可以从这里下载并启动：

<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

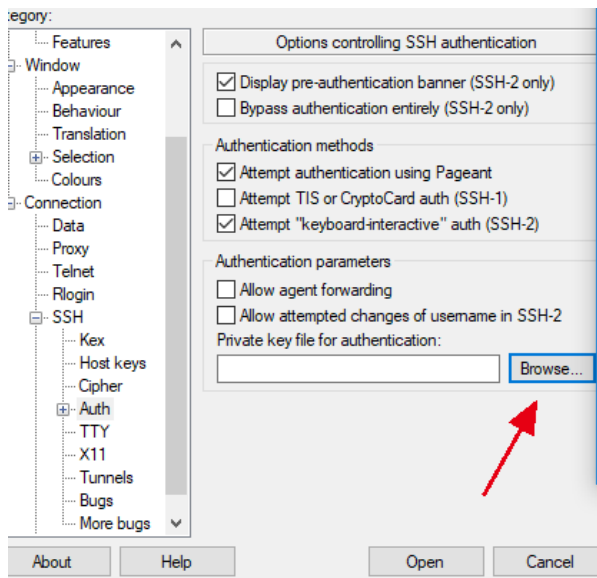
23. 打开 PuTTY.exe（您可能在开始本实验室课程时已经下载）。

24. 在“Host Name”框中，输入 EC2 实例的公有 IP 如图:

“ 公有 IP 52.82.109.131 ”。

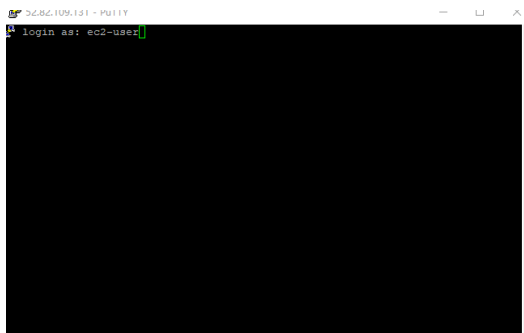
25. 配置:

在 Putty 的设置 Connection->SSH->Auth 里 点击 “ Browse...” 添加.ppk 证书。



26. 单击“Open”。

27. 出现命令行界面 键入: ec2-user 按下 Enter 键



28. 出现以下界面 为 连接成功

