

01-企业的多账户策略 (Multi-Account Strategy for Enterprises)

【Domain 1的组织复杂性设计 (Design for Organizational Complexity)】——企业的多账户策略

Hello大家好欢迎回来，我们今天将讨论企业的多账户策略内容，是SAP-C01 2019新版考试蓝图中【Domain 1的组织复杂性设计 (Design for Organizational Complexity)】的第一篇内容。

如需查看【SAP-C01 2019 新版考试蓝图】的内容[请点击这里](#)。

AWS解决方案架构师认证 Professional / AWS Certified Solutions Architect—Professional —2019系列的课程的最终目的是帮助大家顺利通过新版考试。随着后续系列课程的持续深入，我们的目标是将所有SAP-C01新版考试涉及到的内容、考点逐步推出系列课程，帮助大家备考。此系列课程也同样适用于想了解和学习AWS的同学，请大家多多支持。

企业的多账户策略

我之前就职的企业，有十几个AWS账户，为了管好这么多的账户，需要提前做好账户的规划和管理策略。作为一个解决方案架构师来说，了解多AWS账户所带来的管理挑战，以及掌握一些多账户管理的方法和策略是非常重要的。让我们进一步了解这部分内容：

企业采用多AWS账户策略通常都会是一个非常棒的选择，因为它提供了最大数量的资源和足够程度的安全隔离。当前很多企业实际只是使用一个区域层面隔离的解决方案，仅用一个AWS账户，如他们可能会在东京区域部署开发环境，然后在首尔区域部署生产环境，通过将企业不同的环境部署在不同的AWS区域中实现资源隔离，很多情况下这种隔离的程度是不够的，也不是我们推荐的最佳实践，因为如果创建了IAM用户及相应策略分配给了开发人员，而这个策略又没有进行合理安全配置，开发人员是可以访问首尔区域生产环境的，如发生误操作等情况有可能会影响生成环境的业务稳定性。

所以，在类似这种场景下，企业配置并拥有多个AWS账户是最佳实践，为开发人员单独创建一个AWS账户，并为生产环境也单独创建一个AWS账户部署资源，这样可以避免开发账户意

外访问生产环境资源从而导致影响业务的稳定性，除非我们给其开对应的权限策略。

企业使用多AWS账户时，常见的账户体系结构：

- 1、身份账户体系结构 (Identity Account Architecture)
- 2、日志账户体系结构 (Logging Account Architecture)
- 3、发布账户体系结构 (Publishing Account Structure)
- 4、账单结构 (Billing Structure)

微信公众号：AWS爱好者 // www.iloveaws.cn

AWS爱好者

企业采用多AWS账户策略通常都会是一个非常棒的选择，因为它提供了最大数量的资源和足够程度的安全隔离。

常见的多账户体系结构

- 身份账户体系结构 (Identity Account Architecture)
- 日志账户体系结构 (Logging Account Architecture)
- 发布账户体系结构 (Publishing Account Structure)
- 账单结构 (Billing Structure)



下面的内容我们将对这4种常见的账户体系结构进行讨论：

1、身份账户体系结构 (Identity Account Architecture)

假设您的企业是多AWS账户环境，当用户有变动时您肯定不希望在每个AWS账户下都要管理用户变动。比如您企业有5个AWS账户，分别部署了不同的业务环境，来了一个新员工，他在这些不同业务环境中有不同的工作职责，这样需要在这5个AWS账户分别给新员工建立用户，分配权限，这样的分散管理的方式过不了多久管理任务就会变的越来越糟糕。

推荐的作法是，在单一的中心区域对所有用户进行集中管理，以取代在每个AWS账户单独管理用户的方式，并允许他们访问多个AWS账户下的不同的AWS资源。这种在单一的中心区域对所有用户进行管理可以通过跨账户IAM角色和身份联合 (Federation) 来达成。关于这些具体的内容我们会在后面接下来的系列课程中讨论，现在我们只要了解概念即可。

身份账户体系结构 (Identity Account Architecture)

推荐的作法是，在单一的中心区域对所有用户进行集中管理，并允许他们访问多个AWS账户下的不同的AWS资源。

可以通过跨账户IAM角色和身份联合 (Federation) 来达成。



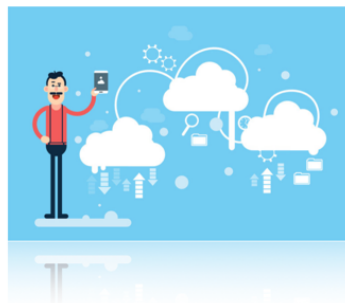
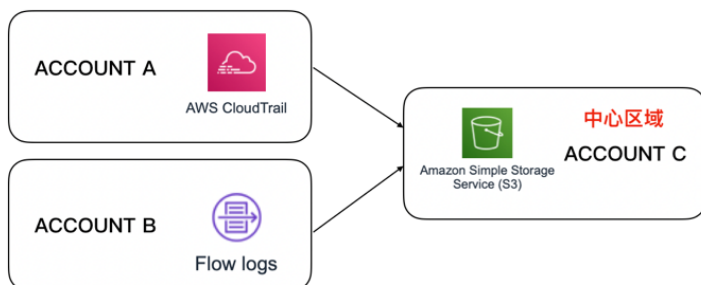
2、日志账户体系结构 (Logging Account Architecture)

多账户环境通常将所有账户的所需日志都存储在一个中心区域，在这个中心区域集中对日志进行定期监控和分析，如有三个AWS账户，ACCOUNT A 和 ACCOUNT B，以及 ACCOUNT C。我们在ACCOUNT C中配置一个S3存储桶负责集中存储ACCOUNT A和B的相关日志，将A和B账户的CloudTrail、vpc flow日志、config log日志等配置成发送到ACCOUNT C中心账户的S3存储桶中集中存储，这个架构就是日志集中存储账户体系结构。

您可以定期集中分析ACCOUNT C的S3存储桶日志，也可以使用splunk等工具从S3存储桶中获取日志，进行安全、审计、监控、排错等其他的需求分析，通过单一的节点实现所有管理的AWS账户的日志存储、分析、监控需求。

日志账户体系结构 (Logging Account Architecture)

将所有账户的所需日志都集中存储在一个中心区域, 在这个中心区域集中对日志进行定期监控和分析



3、发布账户体系结构 (Publishing Account Structure)

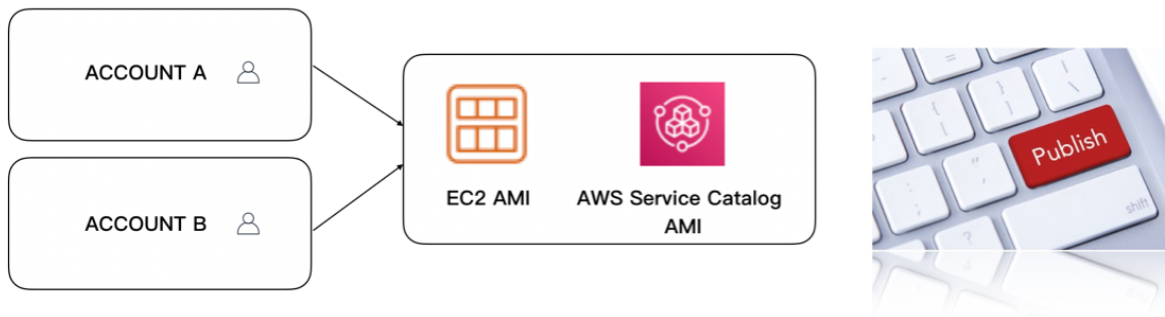
我们可能会遇到这种场景, 企业使用多个AWS账户, 且有多多个开发团队使用这些账户进行开发工作, 他们需要启动EC2实例, 有的开发团队启动的是Centos AMI, 有的开发团队启动了Amazon linux AMI, 还有开发团队启动了Ubuntu AMI, 这样会导致开发环境不统一, 也谈不上标准化, 且在后续开发的过程中, 因为环境的复杂性可能会造成环境调试或者安全相关问题。

那么要如何解决这个问题呢? 通常情况下的作法是企业的安全团队负责提供golden image(黄金镜像), 如果有多个AWS账户, 需要确保开发人员只能启动安全团队批准的, 提供的经过安全加固的镜像启动实例, 这样, 在启动实例时就实现了AMI标准化管理。

这也就是发布账户体系结构, 这种架构对于希望集中管理整个企业预先批准的AMI及AWS Cloudformation模板的客户而言可能是非常有帮助的。我们看下这个图, 图中的EC2 AMI, 我们假设这个AMI是由企业安全团队创建。这个AMI可以分享给所有其他AWS账户, 并且您可以创建IAM策略, 使得开发人员在启动EC2实例时只能使用此AMI。您可以使用AWS的Service Catalog服务来实现, 这是发布账户体系结构。

发布账户体系结构 (Publishing Account Structure)

发布账户体系结构, 这种架构对于希望集中管理整个企业预先批准的AMI及AWS Cloudformation模板的客户而言可能是非常有帮助的。



4、账单结构(Billing Structure)

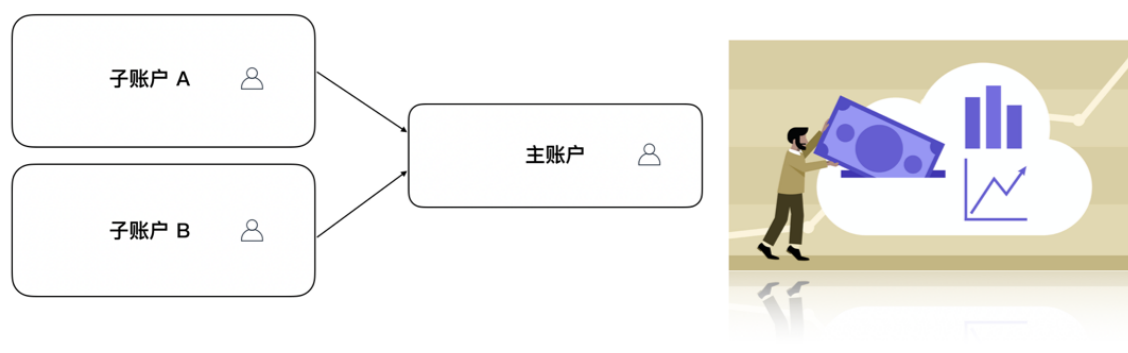
当企业是多AWS账户环境时, 您可以使用AWS Organizations的整合账户功能, 建立组织的主账户并整合和支付所有成员AWS子账户, 使得您可以在一个主账户上追踪整个企业的AWS子账户的账单, 并可为多个AWS子账户在主账户上进行统一支付。

在整合账户后最大的好处就是使得企业的AWS账单易于追踪, 在主账户上可以非常清晰的查看所有子账户的AWS账单, 当然也享有合并所有账户使用量优惠等等, 在这里就不在过多扩展了, 我们将在后续系列的教程中深入讨论。

账单结构(Billing Structure)

您可以使用AWS Organizations的整合账户功能, 建立组织的主账户并整合和支付所有成员AWS子账户, 使得您可以在一个主账户上追踪整个企业的AWS子账户的账单, 并可以为多个AWS子账户在主账户上进行统一支付。

统一账户支付+易于账单追踪+合并使用量+0功能使用费用



我们今天的课程介绍了当企业中设置多个AWS账户后，可能需要面对的一些挑战，以及一些常见的多账户体系结构。在本篇教程中我们在一个较高的层面概述了这些挑战以及我们如何设计多AWS账户的架构，我们会在后续的教程中深入详细讨论这部门内容。

我们今天将讨论企业的多账户策略内容，是SAP-C01 2019新版考试蓝图中【Domain 1的组织复杂性设计（Design for Organizational Complexity）】的第一篇内容，01-企业的多账户策略（Multi-Account Strategy for Enterprises）。

希望此系列教程能为您通过 AWS解决方案架构师认证 Professional 认证考试带来帮助，如您有任何疑问，请联系我们：

微信公众号：AWS爱好者 // www.iloveaws.cn

AWS爱好者

如您有帮助，可支付宝请作者喝冰可乐🥤



请帮忙推荐给更多的人

【AWS爱好者】微信公众号



扫码加作者微信号，拉入【AWS爱好者】微信群



扫码加入知识星球

