受监管着 AWS 陆区的 OU 结构：以制药行业为例

AWS 规范性指导

AWS 规范性指导: 受监管着 AWS 陆区的 OU 结构：以制药行业为例

Table of Contents

受监管着 AWS 陆区的 OU 结构：以制药行业为例

Katja Mueller、Petar Forai 和 Keval Sheth，Amazon Web Services（AWS）

2023 年 3 月（文档历史记录）

AWS 提供了多种支持特定行业（包括医疗保健）的 Landing Zone 加速器配置。Landing Zone Accelerator for Healthcare 与 AWS Control Tower 之配合使用，可简化多账户环境的管理和治理，该环境符合 AWS 最佳实践和多个全球合规框架。协调治理的一个重要方面是使用组织单位 (OUs) 进行分组 AWS 账户 ，这样您就可以将其作为一个单元进行管理。

本指南探讨了随着公司云成熟度的提升，重新设计现有 OU 结构的最佳实践和注意事项。它根据一家大型制药公司的 AWS Control Tower 实施情况介绍了一个实际示例，并讨论了从实施中吸取的经验教训。 AWS landing zone 的设计不是一次性的。它能够而且应当得到发展。通过应用本指南中重点介绍 AWS 的最佳实践和技巧，可以成功而高效地实现这种演变。

概述

我们与一家跨国制药公司合作，在 AWS 上开展了概念验证（PoC）活动，以探索他们如何将现有应用程序从本地迁移到 AWS Cloud。当他们开始扩展和加快迁移工作流以包括生产工作负载时，他们显然需要一个受到监管且合规的 AWS 登录区，以助力其实现目标。我们使用 AWS Control Tower 设计和实施新的 AWS 登录区。

新 AWS 登录区及其组织的一个重要方面是其组织单位（OU）的结构。OU 是使用 AWS Organizations 创建的 AWS 账户的逻辑分组。您可以使用 OU 将 AWS 账户组织成层次结构，并且更轻松一致地应用管理和治理控制。

您可以将基于策略的控件附加到某个 OU 和 AWS 账户。OU 内的子 OU 会自动继承这些控件。因此，OU 在管理 AWS Organizations 中的安全性和治理方面起着至关重要的作用。

策略是包含一个或多个语句的 JSON 文档，这些语句用于定义要应用到一组 AWS 账户的控件。AWS Organizations 目前支持四种类型的策略，也称为服务控制策略（SCP）。SCP 定义了可在不同 AWS 账户中使用的 AWS 服务和操作。例如，您可以使用 SCP 要求 Amazon Elastic Compute Cloud（Amazon EC2）实例的启动使用特定的实例类型。

策略类型

SCP 策略类型包括以下几种：

- 允许列表和拒绝列表是您应用 SCP 以筛选可供账户使用的权限时的补充策略。
- 标签策略帮助您维护一致的标签，包括各账户中的标签键和标签值的首选大小写处理。
- 备份策略为支持的资源类型配置备份，例如备份的时间窗口和跨 AWS 区域备份的目标保管库。
- 人工智能服务退出政策支持或禁用全球 AWS 人工智能（AI）服务的持续改进。

策略继承行为：当您将某个策略附加到特定 OU 时，直接位于该 OU 下的账户或任何子 OU 将继承此策略。当您将策略附加到特定账户时，该策略仅影响该账户。您可以通过引入异常策略来覆盖继承的策略。继承明确允许所有权限从根（OU）传递到该 OU 和子 OU 中的每个 AWS 账户，除非您明确拒绝权限。要拒绝某项权限，您可以创建其他策略并将其附加到相应的 OU 或 AWS 账户。有关策略继承和异常的更多信息，请参阅 AWS Organizations 文档。

AWS Control Tower 还使用 OU 结构提供自己的一套侦测和预防性控制（也称为护栏）。AWS Control Tower 预防性控制通过使用 AWS Organizations 中的 SCP 来防止采取措施。侦测控制使用 AWS Config 来报告与控件的配置偏差。有关这些控制的更多信息，请参阅 AWS Control Tower 文档。

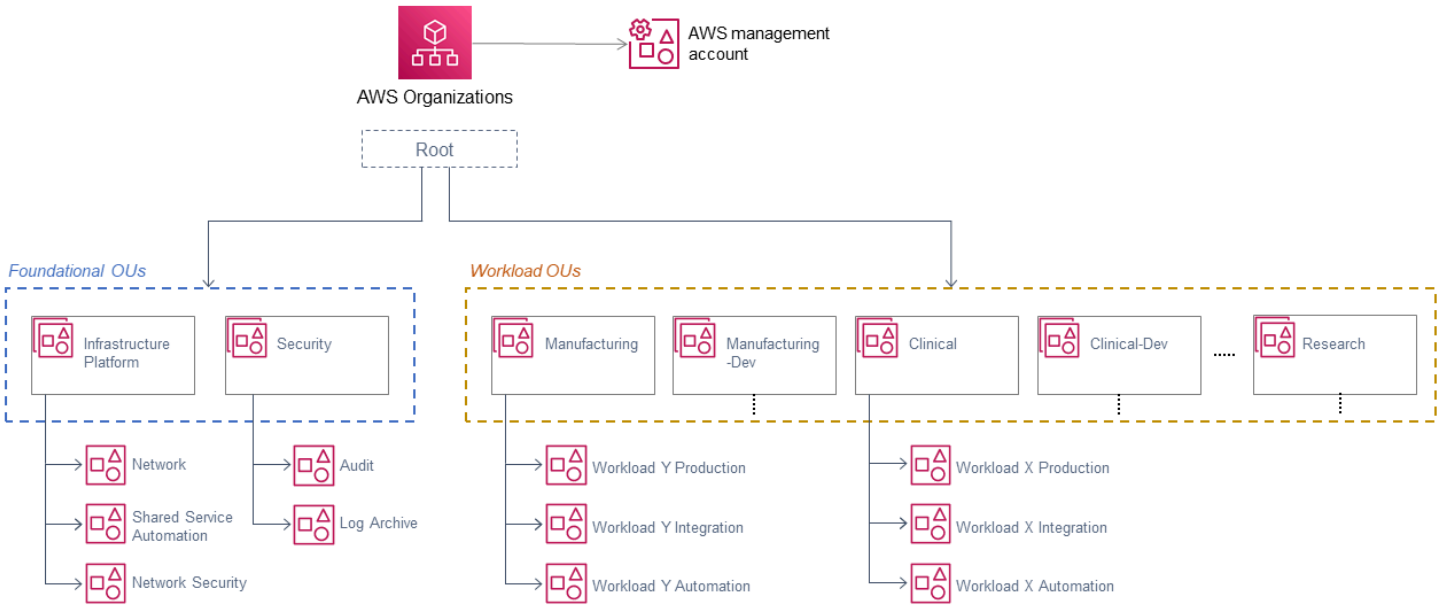
您还可以启用 AWS Security Hub CSPM 来自动执行安全最佳实践检查，将安全提醒聚合到一个位置和格式中，并了解所有 AWS 账户的整体安全状况。

OU 设计：第 1 阶段

在我们的例子中，对于这家跨国制药公司来说，组织和OU的初始设计 AWS Organizations 严格遵循了设立 AWS 建议 AWS Control Tower。有关示例，请参阅医疗保健领域的着陆区加速器。 AWS AWS Control Tower 最初配置了一个带有通用基础 OU 的简单 OU 结构，如博客文章《组织单位最佳实践》中所述 AWS Organizations，包括安全 OU、平台基础架构 OU 和公司特定的 OU。

架构设计

以下图表展示了最初的 OU 架构。



安全 OU

安全 OU 将与安全功能 AWS 账户 相关的广泛分组在一起，并使用两个帐户（审计和日志存档）来存储安全操作数据，以便集中记录和审核对环境的访问。 AWS 诸如 Amazon 之类 GuardDuty 的核心安全服务 AWS Security Hub CSPM 位于审计账户中。

基础设施平台 OU

基础架构平台 OU 组合在一起 AWS 账户 ，提供基础架构基础。最初部署在此 OU 中的 AWS 账户 是中央网络组件（网关、防火墙、中央网络集线器和类似服务）。

其他 OU

其他针对公司的特定 OU（例如临床 OU）会在较低层级的组织架构中增强原有的基础 OU。工作负载是通过多账户结构和这些 OU 内的独立环境来实施的。

有几个考虑因素促成了这一最初的设计：

- 嵌套的 OU 当时不可用，需要 AWS Control Tower 进行大量自定义。
- 最初指定给云的初始工作负载侧重于公司的特定方面，例如临床试验或生产设备分析（功能视角）。
- 该公司将工作环境分为五种类型（开发、验证、集成、训练和生产）。该公司需要一个在没有生产工作负载所需严格 AWS 控制的情况下开发应用程序的游乐场。诸如 OU 之类的开发 Manufacturing-Dev OU 就是为此目的分配的。
- 工作负载自动化是每个应用程序生态系统的一部分，无需进行分离。
- 基础设施认证 (IQ) 和 GxP 合规流程不需要区分 OU 级别的 AWS 控制措施。

OU 设计：第 2 阶段

在我们的示例中，这家制药公司通过将合格的生产工作负载部署到现有的 OU 中，加快进入了云技术发展的新阶段。这启动了对初始设计的审查，随着越来越多的工作量迁移到受监管的 AWS 着陆区，第一阶段的结构受到了挑战。

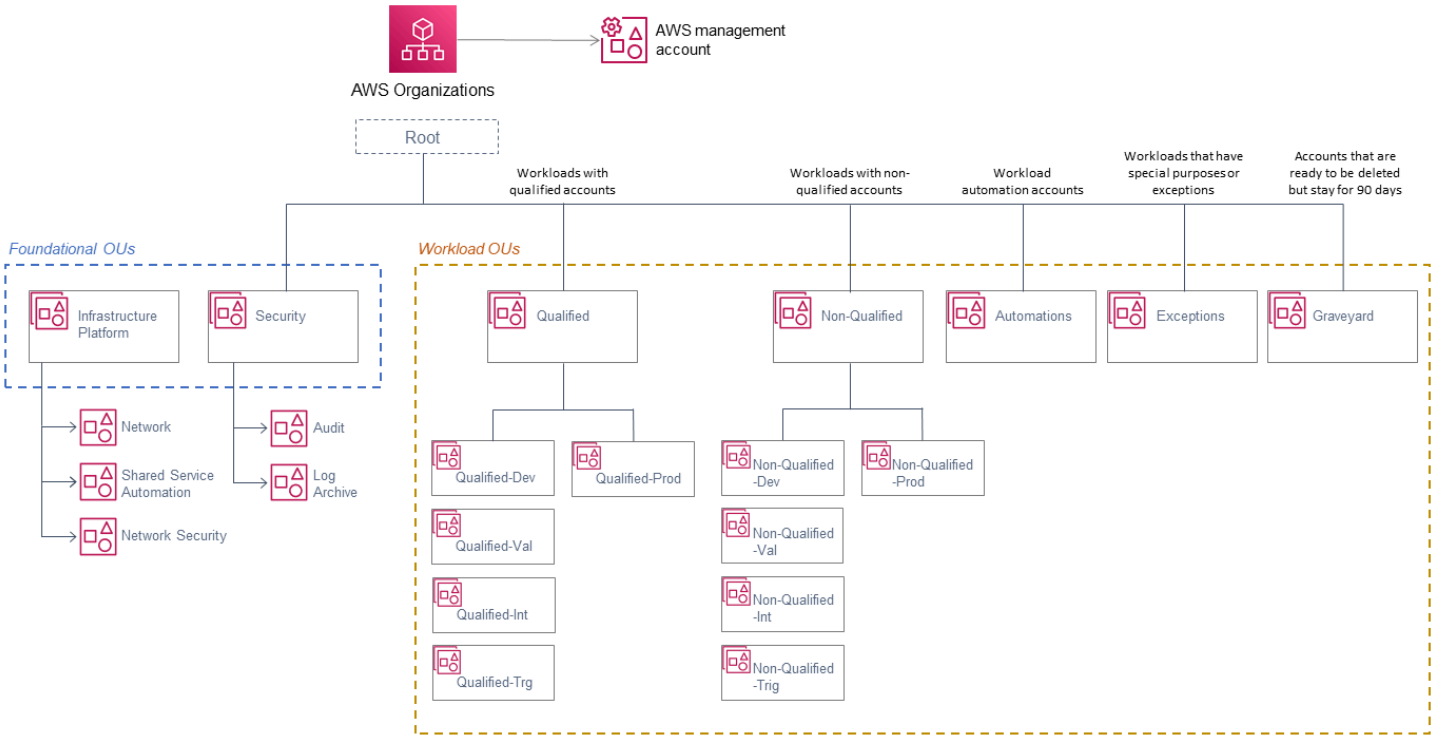
以下新的要求和见解变得至关重要：

- 该公司实施了数据共享工作负载模式，这样一来，应用程序便具备了多用途特性，不再能够被分配到诸如“临床”或“制造”这样的独立 OU 中了。
- 资格认证（尤其是持续性的资格认证）成为了许多工作负载至关重要的环节。这些工作负载必须被纳整合到运营流程中，以便它们能够更轻松地遵循安全最佳实践。合格的工作负载需要更严格的 AWS 控制，这些控制措施是在第 1 阶段在 OU 级别设置的。
- 嵌套的 OU 功能已在中可用 AWS Control Tower。
- 通过提升技能和积累经验，我们对哪些特定策略适用于工作负载有了更深入的理解。
- 该公司明确并达成了一个基于责任协调的运营模式。
- 工作负载分段和结构蓝图已经成熟，并被用于工作负载迁移。

由于这些原因，在第二阶段实施了新的设计并 AWS 账户 迁移到了该新结构。这个新结构包含了以下部分中描述的 OU。

架构设计

以下图表展示了第 2 阶段的 OU 架构。



安全 OU

安全 OU 包含 AWS 账户 与安全功能广泛相关的内容，并使用两个帐户（审计和日志存档）来存储安全操作数据，以便对环境进行集中记录和审核访问。 AWS 诸如 Amazon 之类 GuardDuty 的核心安全服务 AWS Security Hub CSPM 位于审计账户中。此 OU 与最初的设计保持不变。

基础设施平台 OU

基础设施平台 OU 包含基础基础设施账户，例如跨 AWS 着陆区域的联网和共享自动化。此 OU 与最初的设计保持不变。

合格的 OU

合格的 OU 包含需要合格基础设施（例如严格的变更管理、资格认证和验证）的工作负载。

Non-qualified OU

Non-Qualified OU 包含没有 GxP 要求或对业务不至关重要的工作负载。

自动化 OU

Automations OU 包含用于工作负载自动化的共享资源，例如用于基础架构管理的持续集成和持续交付 (CI/CD) 管道。根据需求的不同，自动化操作可以分散到不同的环境中，也可以托管在单个 AWS 账户中。

异常 OU

异常 OU 包含需要特殊处理的工作负载，若不特殊处理，这些工作负载会被策略阻止。例如，可广泛访问和可读的 Amazon Simple Storage Service（Amazon S3）存储桶将属于异常 OU。

Graveyard OU

Graveyard OU 包含 AWS 账户 将要删除的工作负载。在账户到期或被删除之前，应删除这些账户中的策略，以便实现高效且简便的管理访问权限。

OU 迁移和验证

在我们所举的跨国制药公司的示例中，云平台工程团队和变更管理团队共同制定了迁移计划和时间表。在计划过程中，对 AWS 账户进行了审查，并根据业务影响和重要性进行了排序。

新的 OU 结构与现有的 OU 结构并行部署，以便分阶段实施新策略和逐步迁移。我们创建了带有子 OU 的新的空 OU，并且为这些子 OU 分配了 AWS Organizations 策略和 AWS Control Tower 控件。

这些 AWS Organizations 策略是通过在新结构上应用所需的策略来手动迁移的。我们使用手动抽查来验证 AWS Organizations 策略，并使用自动化机制来验证 AWS Control Tower 控件。只有在这些检查成功之后，AWS 账户才被移动到新的 OU 中。

账户迁移是半自动的，并采用了阶段性或批量处理的方式。最初的迁移以那些被认为不太重要的 AWS 账户为目标，每次迁移使用五个 AWS 账户作为一个批次。迁移批次不超过 10 个账户。在进行账户迁移时，审核人员和测试人员使用 AWS Control Tower 控制台来确认这些账户已成功移动到正确的 OU，并且还对 AWS CloudTrail 日志进行监控以查找错误。审核人员还对 AWS Service Catalog 和 AWS Control Tower 控制台进行了检查，以查看是否存在任何偏差或处于受污染或未知状态的账户。

对 OU 内账户布局的更改并未影响资源的连接性或可访问性。没有报告发生生产应用程序中断情况。

吸取的经验教训和最佳实践

- OU 结构设计不是一次性的。随着一家公司加大云采用力度，并将更多的工作负载迁移到 AWS 登录区，其 OU 设计（以及隐含的策略理念）也会自然而然地发生变化。
- 不要将 OU 误认为是文件夹；请将它们视为策略的目标。OU 及其层次结构为 AWS 账户提供结构元素，应始终将其视为策略的容器。我们建议您将需要相同策略集的所有 AWS 账户放在同一 OU 中。本指南还扩展到嵌套的 OU（OU 内的 OU）。

  那些需要集中共享功能以及实现跨工作负载数据共享能力的 AWS 环境（这种需求在企业数据平台中较为常见），在不基于业务线（LOB）功能分类的 OU 结构中更容易得到妥善处理。例如，就 AWS Organizations 中的策略而言，用于制造应用的生产环境与用于临床试验分析应用的生产环境并无不同。
- 尊重并使用继承。当您将某个策略附加到特定 OU 时，直接位于该 OU 下或任何子 OU 下的 AWS 账户将继承此策略。当您将策略附加到特定 AWS 账户时，该策略仅影响该 AWS 账户。

  从一个 OU 结构迁移到另一个 OU 结构的工作，取决于现有策略在该 OU 或 AWS 账户级别上的配置程度。另一个重要的因素在于，在现有的 OU 层级结构中，策略继承的使用程度如何，或者这种继承是否被中断了。随着不规则或偏离常规的继承路径的实施，迁移的复杂性也随之增加。例如，如果在单个 AWS 账户级别实施策略，或者频繁做出策略异常处理（这会中断继承），那么将这些策略迁移到新的结构中将会付出大量额外工作量。在这类复杂度极高的情况下，我们建议您在迁移规划过程中投入时间来审查并重新设计策略继承机制。
- 同时注意 AWS Organizations 策略和 AWS Control Tower 控件。OU 结构由 AWS Control Tower 和 AWS Organizations 共享。AWS Control Tower 提供自己的一套侦测和预防性控件。这些控件适用于 AWS 账户或 OU 级别。AWS Organizations 在 OU 级别编排策略。在 OU 迁移中，我们建议您先迁移 AWS Organizations 策略，因为这些策略对合规性的影响更大。我们建议您在第二个迁移步骤中对新的 OU 结构应用 AWS Control Tower 控件。
- 更新 AWS 账户需要时间。您必须使用 AWS Control Tower 将现有 AWS 账户单独重新注册到新的 OU 结构中。此操作较费时。如果您拥有大量的账户，我们建议您通过自动化手段来简化这项工作，从而实现对 AWS 账户 OU 放置的控制和自动化处理。以下是两个示例场景：
  - 手动更改小规模迁移：迁移主管在 AWS 管理控制台 中将每个 AWS 账户从其旧 OU 重新分配到其新 OU 中。当所有 AWS 账户的重新分配完成后，迁移主管单独为每个 AWS 账户或为所有 OU 打开 AWS Control Tower。在 AWS Control Tower中重新注册 AWS 账户对于每个 AWS 账户都需要 10-15 分钟，具体取决于账户内使用的 AWS 区域数量。AWS Control Tower 允许最多五次此类操作同时并行运行。

- 自定义更改自动化：自动化可以简化并节省工作量。例如，您可以自动管理 AWS 账户从创建到迁移和终止的整个生命周期。您可以使用 AWS Control Tower 账户工厂更改 AWS 账户的 OU 分配并运行重新注册流程。这种自动化支持大规模迁移数百个 AWS 账户。

资源

- AWS Organizations 用户指南（AWS 文档）
- AWS Organizations 术语和概念（AWS 文档）
- 服务控制策略（SCP）（AWS 文档）
- AWS Organizations API 参考（AWS 文档）
- AWS Control Tower 用户指南（AWS 文档）
- 介绍医疗保健登录区加速器（AWS 博客文章）
- 使用 AWS Organizations 和 AWS Control Tower 管理多账户环境（AWS 博客文章）
- Best Practices for Organizational Units with AWS Organizations（AWS 博客文章）
- AWS Security Reference Architecture（AWS SRA）（AWS 规范性指导）
- 在 AWS 上建立您的云基础（AWS 白皮书）
- 使用多个账户组织您的 AWS 环境（AWS 白皮书）

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
初次发布	—	2023 年 3 月 28 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。