aws

用户指南

AWS Control Tower

AWS Control Tower: 用户指南

Table of Contents

什么是 AWS Control Tower？

AWS Control Tower 提供了一种按照规范性最佳实践设置和管理 AWS 多账户环境的简单方法。AWS Control Tower 协调了其他几项AWS 服务的能力 AWS Organizations，包括 AWS Service Catalog AWS IAM Identity Center、和，在不到一小时的时间内建立着陆区。资源是代表您设置和管理的。

AWS Control Tower 编排扩展了的功能。 AWS Organizations为了帮助防止您的组织和账户脱离最佳实践，AWS Control Tower 采用了控制措施（有时也称为护栏）。例如，您可以使用控件来帮助确保创建安全日志和必要的跨账户访问权限，且不会对其进行更改。

如果您要托管多个账户，那么拥有一个便于账户部署和账户管理的编排层是有益的。您可以采用 AWS Control Tower 作为配置账户和基础设施的主要方式。借助 AWS Control Tower，您可以更轻松地遵守公司标准、满足监管要求和遵循最佳实践。

AWS Control Tower 使分布式团队中的最终用户能够通过 Account Factory 中的可配置账户模板快速配置新 AWS 账户。同时，您的中央云管理员可以监控所有账户是否符合已建立的全公司合规政策。

简而言之，AWS Control Tower 根据与数千家企业合作建立的最佳实践，提供了设置和管理安全、合规的多账户 AWS 环境的最简单方法。有关使用 AWS Control Tower 以及 AWS 多账户策略中概述的最佳实践的更多信息，请参阅AWS 多账户策略：最佳实践指南。

功能

AWS Control Tower 具有以下功能：

- 着陆区 — Landing zone 是一个基于安全和合规最佳实践的架构良好的多账户环境。它是企业范围的容器，用于存放您希望遵守合规性监管的所有组织单位 (OU)、账户、用户和其他资源。登录区可以扩展以满足任何规模的企业的需求。
- 控制 — 控件（有时称为护栏）是一条高级规则，可为您的整体 AWS 环境提供持续的治理。它以简明的语言表达。存在三种控制措施：预防性、侦查性和主动性。三类指导适用于控制措施：强制性、强烈建议或选修性。有关控件的详细信息，请参阅 控件的工作原理。
- A@@ ccount Fac tory — Account Factory 是一个可配置的账户模板，可帮助使用预先批准的账户配置标准化新账户的配置。AWS Control Tower 提供了一个内置的账户工厂，可帮助您自动执行组织中的账户配置工作流程。有关更多信息，请参阅使用 Account Factory 配置和管理账户。
- 控制面板 — 控制面板可让您的中央云管理员团队持续监督您的着陆区。使用控制面板查看企业中已配置的账户、为策略实施启用的控件、为持续检测策略不合规性而启用的控件，以及按账户和 OU 组织的不合规资源。

AWS Control Tower 如何与其他 AWS 服务交互

AWS Control Tower 建立在值得信赖和可靠的 AWS 服务之上 AWS Service Catalog，包括 AWS IAM Identity Center、和 AWS Organizations。有关更多信息，请参阅集成服务。

您可以将 AWS Control Tower 与其他 AWS 服务整合到一个解决方案中，以帮助您将现有工作负载迁移到 AWS。有关更多信息，请参阅如何利用 AWS Control Tower 以及 CloudEndure 如何将工作负载迁移到 AWS。

配置、治理和可扩展性

- 自动账户配置：AWS Control Tower 通过Account Factory（或“自动售货机”）自动部署和注册账户，该工厂是在中预配置产品之上作为抽象构建的。 AWS Service CatalogAccount Factory 可以创建和注册 AWS 账户，并自动执行对这些账户应用控制和策略的过程。
- 集中式治理：通过利用的功能 AWS Organizations，AWS Control Tower 建立了一个框架，确保您的多账户环境中一致的合规和治理。该 AWS Organizations 服务为管理多账户环境提供了基本功能，包括账户的中央治理和管理、 AWS Organizations 通过 API 创建账户以及服务控制策略 (SCP)。

- 可扩展性：您可以直接在 AWS Control Tower 控制台中工作或在 AWS Control Tower 控制台中 AWS Organizations工作来构建或扩展自己的 AWS Control Tower 环境。注册现有组织并将现有账户注册到 AWS Control Tower 后，您可以在 AWS Control Tower 中看到您的更改反映在 AWS Control Tower 中。您可以更新您的 AWS Control Tower 着陆区以反映您的更改。如果您的工作负载需要更多高级功能，则可以利用其他 AWS 合作伙伴解决方案以及 AWS Control Tower。

您是 AWS Control Tower 的首次用户吗？

如果您是此服务的新用户，建议您阅读以下内容：

1. 如果您需要有关如何规划和组织着陆区的更多信息，请参阅规划你的 AWS Control Tower 着陆区和AWS AWS Control Tower 着陆区的多账户策略。
2. 如果您已准备好创建您的第一个登录区，请参阅 AWS Control Tower 入门。
3. 有关偏差检测和预防的信息，请参阅 在 AWS Control Tower 中检测并解决偏差。
4. 有关安全性详细信息，请参阅 AWS Control Tower 中的安全。
5. 有关更新 landing zone 和成员账户的信息，请参阅AWS Control Tower 中的配置更新管理。

AWS Control Tower 的工作原理

本节简要介绍了 AWS Control Tower 的工作原理。您的 landing zone 是一个架构精良的多账户环境，可以存放您的所有资源。 AWS 您可以使用此环境对所有 AWS 账户强制执行合规性法规。

AWS Control Tower 着陆区的结构

AWS Control Tower 中着陆区的结构如下：

- Root — 包含着陆区域中所有其他 OU 的父级。
- 安全 OU — 此 OU 包含日志存档和审核帐户。这些账户通常被称为共享账户。启动着陆区时，您可以为这些共享账户选择自定义名称，并且可以选择将现有 AWS 账户引入 AWS Control Tower，以确保安全和记录。但是，以后不能重命名这些帐户，也不能在初始启动后添加现有帐户，以保证安全性和日志记录。
- Sandbox OU — Sandbox OU 是在你启动着陆区时创建的（如果你启用了它）。此注册的 OU 和其他注册的 OU 包含您的用户用来执行 AWS 工作负载的注册账户。
- IAM 身份中心目录 — 此目录存放您的 IAM 身份中心用户。它定义了每个 IAM 身份中心用户的权限范围。
- IAM Identity Center 用户 — 这些是您的用户在您的着陆区域中执行 AWS 工作时可以假设的身份。

设置着陆区后会发生什么

在您设置着陆区时，AWS Control Tower 会代表您在您的管理账户中执行以下操作：

- 创建包含在 AWS Organizations 组织根结构中的两个组织单位 (OU)：安全和沙盒（可选）。
- 在安全 OU 中创建或添加两个共享帐户：日志存档帐户和审核帐户。
- 如果您选择默认的 AWS Control Tower 配置，或者它允许您自行管理身份提供商，则在 IAM Identity Center 中创建一个包含预配置群组和单点登录访问权限的云原生目录。
- 应用所有强制性的预防性控制措施来执行策略。
- 应用所有必需的检测控件来检测配置违规。
- 预防性控制不适用于管理账户。
- 除管理账户外，控制措施适用于整个组织。

安全地管理您的 AWS Control Tower 着陆区和账户内的资源

- 创建着陆区时，会创建许多 AWS 资源。要使用 AWS Control Tower，您不得在本指南所述的支持方法之外修改或删除这些 AWS Control Tower 托管资源。删除或修改这些资源将导致您的 landing zone 进入未知状态。有关详细信息，请参阅 创建和修改 AWS Control Tower 资源的指南
- 当您启用可选控件（带有强烈推荐或选择性指导的控件）时，AWS Control Tower 会创建在您的账户中管理的 AWS 资源。请勿修改或删除 AWS Control Tower 创建的资源。这样做可能会导致控件进入未知状态。

共享账户有哪些？

在 AWS Control Tower 中，着陆区中的共享账户是在设置过程中配置的：管理账户、日志存档账户和审计账户。

什么是管理账户？

这是您专门为着陆区（landing zone）创建的账户。此账户用于为您的 landing zone 中的所有内容计费。它还用于 Account Factory 配置帐户，以及管理 OU 和控件。

> **Note**
>
> 不建议从 AWS Control Tower 管理账户运行任何类型的生产工作负载。创建一个单独的 AWS Control Tower 账户来运行您的工作负载。

有关更多信息，请参阅 管理账户。

什么是日志存档账户？

此账户可用作 landing zone 中所有账户的 API 活动和资源配置日志的存储库。

有关更多信息，请参阅 日志存档账户。

什么是审计账户？

审计账户是一个受限账户，旨在让您的安全和合规团队能够读写您的 landing zone 中所有账户。从审计账户，您可以通过仅授予 Lambda 函数的角色对审核账户进行编程访问。审计账户不支持手动登录到其他账户。有关 Lambda 函数和角色的更多信息，请参阅配置 Lambda 函数以代入另一个函数。
AWS 账户

有关更多信息，请参阅 审计账户。

控件的工作原理

控制是一条高级规则，可为您的整体 AWS 环境提供持续的治理。每个控件都强制执行一条规则，并用通俗易懂的语言表达。您可以随时从 AWS Control Tower 控制台或 AWS Control Tower API 中更改有效的选修或强烈推荐的控制措施。强制性控制始终适用，并且无法更改。

预防性控制措施可防止采取行动。例如，名为 “不允许更改 Amazon S3 存储桶的存储桶策略” (以前称为 “禁止更改日志存档策略”) 的选择性控件可防止日志档案共享账户中的任何 IAM 策略更改。任何试图执行被阻止的操作的尝试都将被拒绝并登录 CloudTrail。资源也已登录 AWS Config。

Detective 控件会在特定事件发生时对其进行检测并将操作记录在内CloudTrail。例如，强烈推荐使用名为 “检测是否为附加到 Amazon EC2 实例的 Amazon EBS 卷启用了加密” 的控件可以检测未加密的 Amazon EBS 卷是否已连接到您的着陆区中的 EC2 实例。

在您的账户中配置资源之前，主动控制会检查资源是否符合贵公司的政策和目标。如果资源不合规，则不会对其进行配置。主动控制通过 AWS CloudFormation 模板监控将在您的账户中部署的资源。

对于那些熟悉的人 AWS：在 AWS Control Tower 中，预防性控制是通过服务控制策略 (SCP) 实施的。Detective 控件是通过 AWS Config 规则实现的。主动控制是通过 AWS CloudFormation 挂钩实现的。

相关主题

- 在 AWS Control Tower 中检测并解决偏差

AWS Control Tower 是如何使用的 StackSets

AWS Control Tower 用于 AWS CloudFormation StackSets 在您的账户中设置资源。每个堆栈集都有 StackInstances 对应于账户和 AWS 区域 每个账户的堆栈集。AWS Control Tower 为每个账户和每个地区部署一个堆栈集实例。

AWS Control Tower 会根据 AWS CloudFormation 参数 AWS 区域 有选择地将更新应用于某些账户。将更新应用于某些堆栈实例时，其他堆栈实例可能会处于 Outdated (过时) 状态。这是正常的，也是预期行为。

当堆栈实例处于 Outdated (过时) 状态时，通常意味着对应于该堆栈实例的堆栈未采用堆栈集中的最新模板。堆栈仍采用旧模板，因此它可能未包含最新的资源或参数。堆栈仍然完全可用。

以下是根据更新期间指定的 AWS CloudFormation 参数简要概述预期的行为：

如果堆栈集更新包括对模板的更改（也就是说，如果指定了`TemplateBody`或`TemplateURL`属性），或者指定了`Parameters`属性，则在更新指定账户中的堆栈实例之前，将所有堆栈实例的状态 AWS CloudFormation 标记为 “已过期” 和 AWS 区域。如果堆栈集更新不包括对模板或参数的更改，则 AWS CloudFormation 更新指定账户和区域中的堆栈实例，同时保留所有其他堆栈实例的现有堆栈实例状态。要更新与堆栈集关联的所有堆栈实例，请勿指定 `Accounts` 或 `Regions` 属性。

有关更多信息，请参阅《 AWS CloudFormation 用户指南》中的 “更新堆栈集”。

术语

以下是你将在 AWS Control Tower 文档中看到的一些术语的简要回顾。

首先，很高兴知道 AWS Control Tower 与该 AWS Organizations 服务共享许多术语，包括本文档中出现的组织和组织单位 (OU) 这两个术语。

- 有关组织和组织单位的更多信息，请参阅AWS Organizations 术语和概念。如果您不熟悉 AWS Control Tower，那么该术语是一个不错的起点。
- AWS Organizations是一项 AWS 服务，可帮助您在扩展和扩展工作负载时集中管理您的环境 AWS。AWS Control Tower 依 AWS Organizations 靠创建账户、在 OU 级别实施预防性控制以及提供集中账单。
- Ac AWS count Factory AWS 账户是使用 AWS Control Tower 中的账户工厂配置的账户。有时，Account Factory被非正式地称为账户的 “自动售货机”。
- 您的 AWS Control Tower 主 AWS 区域是部署您的 AWS Control Tower 着陆区的区域。你可以在 landing zone 设置中查看你的家乡区域。
- AWS Service Catalog允许您集中管理常用部署的 IT 服务。在本文档中，Account Factor AWS Service Catalog y 用于配置新 AWS 账户，包括来自自定义蓝图的账户。
- AWS CloudFormation StackSets是一种扩展堆栈功能的资源，因此您可以通过单个操作和单个模板跨多个账户和地区创建、更新或删除堆栈。 CloudFormation
- 堆栈实例是对区域内目标账户中的堆栈的引用。
- 堆栈是您可以作为一个单元管理的 AWS 资源集合。
- 聚合器是一种 AWS Config 资源类型，它从组织内的多个账户和区域收集 AWS Config 配置和合规性数据，允许您在单个账户中查看和查询这些合规性数据。
- 一致性包是 AWS Config 规则和补救措施的集合，可以作为单个实体部署到一个账户和一个区域，也可以部署在整个组织中 AWS Organizations。您可以使用一致性包来帮助自定义 AWS Control Tower 环境。有关提供更多详细信息的技术博客，请参阅相关信息。
- AWS Control Tower 中的基准是您可以应用于目标的一组资源和特定配置。最常见的基准目标可能是组织单位 (OU)。例如，名为的基准可用于帮助您`AWSControlTowerBaseline`在 AWS Control Tower 中注册组织单元。在着陆区设置和更新期间，基准目标可能是共享账户，也可以是整个着陆区的特定设置。
- 蓝图：蓝图是一种封装了一些元数据的构件，这些元数据描述了在账户中部署的基础架构组件。例如， AWS CloudFormation 模板可以用作 AWS Control Tower 账户的蓝图。

- 偏移：由 AWS Control Tower 安装和配置的资源发生变化。没有漂移的资源使 AWS Control Tower 能够正常运行。
- 不合规资源：违反定义特定侦探控制的 AWS Config 规则的资源。
- 共享账户：AWS Control Tower 在您设置着陆区时自动创建的三个账户之一：管理账户、日志存档账户和审计账户。在设置过程中，您可以为日志存档帐户和审核帐户选择自定义名称。
- 成员账户：成员账户属于 AWS Control Tower 组织。可以在 AWS Control Tower 中注册或取消注册该成员账户。当注册的 OU 包含已注册账户和未注册账户混合时：
  - 在 OU 上启用的预防控制适用于其中的所有账户，包括未注册的账户。之所以如此，是因为预防性控制是在组织单位级别而不是账户级别对SCP实施的。有关更多信息，请参阅 AWS Organizations 文档中的服务控制策略继承。
  - OU 上启用的 Detective 控制不适用于已取消注册的帐户。

  一个账户一次只能是一个组织的成员，其费用将记入该组织的管理账户。可以将成员账户移至组织的根容器。
- AWS 账户： AWS 账户充当资源容器和资源隔离边界。 AWS 账号可以关联账单和付款。 AWS 账户与 AWS Control Tower 中的用户账户（有时称为 IAM 用户账户）不同。通过 Account Factory 配置过程创建的 AWS 账户就是账户。 AWS 也可以通过账户注册或 OU 注册流程将账户添加到 AWS Control Tower。
- 控制：控制（也称为护栏）是一项高级规则，可为您的整个 AWS Control Tower 环境提供持续的管理。每个控件都会强制执行一条规则。使用 SCP 实施预防性控制。Detective 控件是通过 AWS Config 规则实现的。主动控制是通过 AWS CloudFormation 挂钩实现的。有关更多信息，请参阅 控件的工作原理。
- 着陆区：着陆区是一种提供推荐起点的云环境，包括默认账户、账户结构、网络和安全布局等。在 landing zone 中，您可以部署利用您的解决方案和应用程序的工作负载。
- 嵌套组织单元：AWS Control Tower 中的嵌套组织单元是包含在另一个组织单元中的组织单元。一个嵌套 OU 只能有一个父 OU，每个账户只能是一个组织单位的成员。嵌套的 OU 会创建层次结构。当您将策略附加到层次结构中的一个 OU 时，它会向下流动并影响其下所有 OU 和帐户。AWS Control Tower 中嵌套的 OU 层次结构最多可以有五个级别。
- 父 OU：层次结构中位于当前 OU 正上方的 OU。每个 OU 只能有一个父 OU。
- 子组织单位：层次结构中位于当前 OU 之下的任何 OU。一个 OU 可以有多个子 OU。
- OU 层次结构：在 AWS Control Tower 中，嵌套 OU 的层次结构最多可以有五个级别。嵌套顺序被称为等级。层次结构的顶部被指定为级别 1。
- 顶级 OU：顶级 OU 是指直接位于根目录下的任何 OU，而不是根本身。根不被视为 OU。

定价

使用 AWS Control Tower 不收取任何额外费用。您只需为 AWS Control Tower 支持的 AWS 服务以及您在着陆区使用的服务付费。例如，您需要为使用 Account Factory 配置账户的 Service Catalog 付费，以及 AWS CloudTrail 为在着陆区域中跟踪的事件付费。有关与 AWS Control Tower 相关的定价和费用的信息，请参阅 A WS Control Tower 定价。

如果您在 AWS Control Tower 中使用账户运行临时工作负载，则与之相关的成本可能会增加。 AWS Config有关详细信息，请参阅 AWS Config 定价。有关管理这些费用的更多具体信息，请联系您的 AWS 客户代表。要详细了解如何 AWS Config 使用 AWS Control Tower，请参阅使用监控资源变化 AWS Config。

如果您在 AWS Control Tower 之外实施 AWS CloudTrail 跟踪，则可以将其与 AWS Control Tower 一起使用。但是，如果您还选择加入由 AWS Control Tower 管理的跟踪，则可能会产生重复的费用。除非您有特殊要求，否则我们不建议您设置外部路线。如果您在着陆区设置或更新期间选择加入，AWS Control Tower 会在管理账户中为您设置并激活组织级别的 CloudTrail 跟踪。有关管理 CloudTrail 成本的信息，请参阅管理 CloudTrail 成本。

设置

在 AWS Control Tower 首次使用之前，请按照本节中的步骤创建 AWS 账户并保护您的 AWS Control Tower 管理账户。有关专门针对的其他设置任务的信息 AWS Control Tower，请参阅AWS Control Tower 入门。

报名参加 AWS

当您注册 Amazon Web Services (AWS) 时，您的 AWS 账户会自动注册使用中的所有服务 AWS，包括 AWS Control Tower。如果您已经有一个 AWS 帐户，请跳到下一个任务。如果您没有 AWS 帐户，请按照以下步骤创建一个。

请记下您的 AWS 账号，因为其他任务需要使用该账号。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。
2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。
2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

为您的账户提供安全保障

您可以在 AWS Organizations 文档中找到有关如何设置保护 AWS Control Tower 账户安全的最佳实践的更多指南。

- 管理账户的最佳实践
- 成员账户的最佳实践

后续步骤

AWS Control Tower 入门

AWS Control Tower 入门

本入门程序适用于 AWS Control Tower 管理员。当您准备好使用 AWS Control Tower 控制台或 API 设置着陆区时，请按照以下步骤操作。

如果您目前是 AWS Control Tower 的 AWS 客户，但不妨先阅读名为 “” 的部分规划你的 AWS Control Tower 着陆区，然后再继续操作。

主题

AWS Control Tower 快速入门指南

如果您不熟悉 AWS，可以按照本节中的步骤快速开始使用 AWS Control Tower。如果您想立即自定义 AWS Control Tower 环境，请参阅 第 2 步。配置并启动您的着陆区 。

> **Note**
>
> AWS Control Tower 设置付费服务 AWS CloudTrail，例如、 AWS Config、亚马逊 CloudWatch、亚马逊 S3 和亚马逊 VPC。使用这些服务时，可能会产生费用，如定价页面所示。 AWS 管理控制台显示任何付费服务的使用情况和产生的费用。AWS Control Tower 本身不会产生任何额外费用。

开始之前

在开始设置过程之前，最重要的决定是选择您的居住区域。您的主 AWS 区域是您运行大部分工作负载或存储大部分数据的区域。设置好您的 AWS Control Tower 着陆区后，便无法对其进行更改。有关如何选择主区域的更多信息，请参阅 设置着陆区的管理提示 。

> **Note**
>
> 默认情况下，AWS Control Tower 会选择您的账户当前运营所在的区域作为您的主区域。您可以在 AWS 管理控制台屏幕的右上角看到您当前的区域。

快速入门过程假设您将接受 AWS Control Tower 环境中资源的默认值。这些选择中有许多可以在以后更改。名为 “” 的部分中列出了一些一次性选择 对 landing zone 配置的期望 。

如果您创建了一个新 AWS 账户，它会自动满足设置 AWS Control Tower 所需的先决条件。您可以继续执行随后的步骤。

快速入门步骤

1. 使用您的管理员用户凭据登录 AWS 管理控制台。
2. 导航到 AWS Control Tower 控制台，网址为 https://console.aws.amazon.com/controltower。
3. 确认你在你想要的家乡地区工作。
4. 选择 “设置着陆区”。
5. 按照控制台中的说明进行操作，接受所有默认值。您需要输入账户的电子邮件地址、日志存档账户和审核账户。
6. 确认您的选择，然后选择设置着陆区。
7. AWS Control Tower 需要大约 30 分钟才能在您的着陆区设置所有资源。

有关如何设置 AWS Control Tower（包括自定义环境的方法）的更详细版本，请阅读并遵循接下来的几个主题中的步骤。

> **Note**
>
> 如果您是首次使用该产品的客户，但遇到设置问题，请联系 Su AWS pport 寻求诊断帮助。

先决条件：自动对您的管理账户进行启动前检查

在 AWS Control Tower 设置着陆区之前，它会自动对您的账户进行一系列启动前检查。您无需对这些检查采取任何行动，这些检查可确保您的管理账户已准备就绪，可以进行建立 landing zone 的更改。以下是 AWS Control Tower 在设置着陆区之前运行的检查：

- 的现有服务限制 AWS 账户 必须足以让 AWS Control Tower 启动。有关更多信息，请参阅AWS Control Tower 中的限制和配额。
- AWS 账户 必须订阅以下 AWS 服务：
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon SNS
  - Amazon Virtual Private Cloud (Amazon VPC)
  - AWS CloudFormation
  - AWS CloudTrail
  - Amazon CloudWatch
  - AWS Config
  - AWS Identity and Access Management (IAM)
  - AWS Lambda

> **Note**
>
> 默认情况下，所有账户都订阅这些服务。

AWS IAM Identity Center （IAM 身份中心）客户的注意事项

- 如果已经设置 AWS IAM Identity Center （IAM 身份中心），则 AWS Control Tower 主区域必须与 IAM 身份中心区域相同。
- IAM 身份中心只能安装在组织的管理账户中。
- 根据您选择的身份源，三个选项适用于您的 IAM Identity Center 目录：
  - IAM 身份中心用户存储：如果 AWS Control Tower 设置了 IAM 身份中心，则 AWS Control Tower 会在 IAM 身份中心目录中创建群组，并为您选择的用户配置成员账户对这些群组的访问权限。
  - 活动目录：如果为 AWS Control Tower 的 IAM 身份中心设置了活动目录，则 AWS Control Tower 不会管理 IAM 身份中心目录。它不会将用户或组分配给新 AWS 帐户。
  - 外部身份提供商：如果为 AWS Control Tower 的 IAM 身份中心设置了外部身份提供商 (IdP)，则 AWS Control Tower 会在 IAM 身份中心目录中创建群组，并为您为成员账户选择的用户配置对这些群组的访问权限。在创建账户期间，您可以在 Account Factory 中指定来自外部 IdP 的现有用户，当 AWS Control Tower 在 IAM Identity Center 和外部 IdP 之间同步同名用户时，AWS Control Tower 会允许该用户访问新出售的账户。您还可以在外部 IdP 中创建群组，使其与 AWS

Control Tower 中默认群组的名称相匹配。当您将用户分配到这些群组时，这些用户将有权访问您注册的帐户。

有关使用 IAM 身份中心和 AWS Control Tower 的更多信息，请参阅 关于 IAM 身份中心账户和 AWS Control Tower 的注意事项

AWS Config 和 AWS CloudTrail 客户的注意事项

- AWS 账户 无法在组织管理账户中为 AWS Config 或启用可信访问权限 CloudTrail。有关如何禁用可信访问的信息，请参阅有关如何启用或禁用可信访问的 AWS Organizations 文档。
- 如果您计划在 AWS Control Tower 中注册的任何现有账户中已有 AWS Config 记录器、交付渠道或聚合设置，则在设置了着陆区之后，您必须在开始注册账户之前修改或删除这些配置。此预检查不适用于着陆区启动期间的 AWS Control Tower 管理账户。有关更多信息，请参阅注册拥有现有 AWS Config 资源的账户。
- 如果您在 AWS Control Tower 中使用账户运行临时工作负载，则可能会看到与 Config 相关的成本增加。 AWS 有关管理这些费用的更多具体信息，请联系您的 AWS 客户代表。
- 当您向 AWS Control Tower 注册账户时，您的账户将受 AWS Control Tower 组织的 AWS CloudTrail 跟踪管理。如果您已在账户中部署了 CloudTrail 跟踪，则可能会看到重复的费用，除非您在将该账户注册到 AWS Control Tower 之前删除该账户的现有跟踪。有关组织级跟踪和 AWS Control Tower 的信息，请参阅。定价

> **Note**
>
> 启动时，必须在管理账户中为受 AWS Control Tower 管理的所有区域激活 AWS 安全令牌服务 (STS) 终端节点。否则，启动可能会在配置过程中半途而废。

从控制台开始使用 AWS Control Tower

本入门程序适用于 AWS Control Tower 管理员。当您准备好使用 AWS Control Tower 控制台设置着陆区时，请按照以下步骤操作。从头到尾，大约需要半个小时。此过程需要一些先决条件和三个主要步骤。

如果您目前是 AWS Control Tower 的 AWS 客户，但不妨先阅读名为 “” 的部分规划你的 AWS Control Tower 着陆区，然后再继续操作。

主题

第 1 步：创建您的共享账户电子邮件地址

如果你要用新的方式设置着陆区 AWS 账户，请参阅设置。

- 要使用新的共享账户设置您的着陆区，AWS Control Tower 需要两个尚未与之关联的唯一电子邮件地址 AWS 账户。这些电子邮件地址中的每一个都将用作协作收件箱（共享电子邮件账户），供企业中从事与 AWS Control Tower 相关的特定工作的不同用户使用。
- 如果您是首次设置 AWS Control Tower，并且要将现有安全账户和日志存档账户引入 AWS Control Tower，则可以输入现有 AWS 账户的当前电子邮件地址。

电子邮件地址是必填的：

- 审计账户 — 此账户适用于需要访问 AWS Control Tower 提供的审计信息的用户团队。您还可以将此账户用作第三方工具的访问点，这些工具将对您的环境执行程序化审计，以帮助您进行合规性审计。
- 日志存档账户 — 此账户适用于需要访问您的 landing zone 中已注册 OU 中所有已注册账户的所有日志信息的用户团队。

这些账户是在您创建 landing zone 时在安全 OU 中设置的。作为最佳实践，我们建议您在这些账户中执行操作时，应使用具有适当范围权限的 IAM Identity Center 用户。

> **Note**
>
> 如果您指定现有 AWS 账户作为您的审计和日志存档账户，则现有账户必须通过一些启动前检查，以确保没有资源与 AWS Control Tower 的要求发生冲突。如果这些检查不成功，则可能无法成功设置 landing zone。特别是，账户不得有现有 AWS Config 资源。有关更多信息，请参阅 引入现有安全账户或日志账户的注意事项。

为清楚起见，本用户指南始终使用默认名称来指代共享帐户：日志存档和审计。阅读本文档时，如果您选择对其进行自定义，请记住替换您最初为这些账户提供的自定义名称。您可以在账户详情页面上查看带有自定义名称的账户。

> **Note**
>
> 为了与 AWS 多账户策略保持一致，我们正在更改有关某些 AWS Control Tower 组织单位 (OU) 默认名称的术语。在我们进行过渡以提高这些名称的清晰度时，您可能会注意到一些不一致之处。安全 OU 以前被称为核心 OU。沙盒 OU 以前被称为自定义 OU。

对 landing zone 配置的期望

设置 AWS Control Tower 着陆区的过程分为多个步骤。您的 AWS Control Tower 着陆区的某些方面是可以配置的。其他选项在设置后无法更改。

安装过程中要配置的关键项目

- 你可以在设置过程中选择你的顶级 OU 名称，也可以在设置 landing zone 之后更改 OU 名称。默认情况下，顶级 OU 命名为 “安全” 和 “沙盒”。有关更多信息，请参阅 建立架构良好的环境的指导方针。
- 在设置过程中，您可以为 AWS Control Tower 创建的共享账户选择自定义名称，默认情况下称为日志存档和审计，但在设置后无法更改这些名称。（这是一次性选择。）
- 在设置过程中，您可以选择为 AWS Control Tower 指定现有 AWS 账户以用作审计和日志存档账户。如果您计划指定现有 AWS 账户，并且这些账户有现有资源，则必须先删除现有 AWS Config 资源，然后才能将这些账户注册到 AWS Control Tower。 AWS Config（这是一次性选择。）
- 如果您是首次设置，或者要升级到着陆区版本 3.0，则可以选择是否允许 AWS Control Tower 为您的组织设置组织级别的 AWS CloudTrail 跟踪，也可以选择退出由 AWS Control Tower 管理的跟踪并管理自己的 CloudTrail 跟踪。在更新着陆区时，您可以随时选择加入或选择退出由 AWS Control Tower 管理的组织级跟踪。
- 在设置或更新着陆区时，您可以选择为 Amazon S3 日志存储桶和日志访问存储桶设置自定义的保留政策。
- 您可以选择指定先前定义的蓝图，用于从 AWS Control Tower 控制台配置自定义的成员账户。如果您没有可用的蓝图，则可以稍后自定义帐户。请参阅 使用 Account Factory 自定义 (AFC) 自定义账户。

无法撤消的配置选项

- 设置了着陆区后，您就无法更改自己的主区域。
- 如果您使用 VPC 配置 Account Factory 账户，则在创建 VPC CIDR 后无法对其进行更改。

第 2 步。配置并启动您的着陆区

在启动 AWS Control Tower 着陆区之前，请确定最合适的主区域。有关更多信息，请参阅 设置着陆区的管理提示 。

> **Important**
>
> 在部署 AWS Control Tower 着陆区后更改您的主区域需要退役以及 AWS 支持部门的协助。此做法不是推荐做法。

了解如何使用 AWS CLI 中的配置和启动您的着陆区使用 API 开始使用 AWS Control Tower。

要在控制台中配置和启动 landing zone，请执行以下一系列步骤。

准备：导航到 AWS Control Tower 控制台

1. 打开网络浏览器，然后导航到 AWS Control Tower 控制台，网址为 https://console.aws.amazon.com/controltower。
2. 在控制台中，确认您正在所需的 AWS Control Tower 主区域工作。然后选择 “设置您的着陆区”。

步骤 2a. 查看并选择您所在 AWS 的地区

请确保您已正确指定您为家乡地区选择的区域。 AWS 在您部署 AWS Control Tower 之后，您无法更改主区域。

在设置过程的这一部分中，您可以添加所需的任何其他 AWS 区域。如果需要，您可以稍后添加更多区域，也可以将区域从监管中移除。

选择其他 AWS 地区进行治理

1. 该面板显示当前的区域选择。打开下拉菜单，查看可供监管的其他区域的列表。
2. 选中每个区域旁边的复选框，将其纳入 AWS Control Tower 的管理。您的主区域选择不可编辑。

拒绝访问某些区域

要拒绝访问某些 AWS 区域中的 AWS 资源和工作负载，请在区域拒绝控制部分中选择启用。默认情况下，此控件的设置为 “未启用”。

步骤 2b. 配置您的组织单位 (OU)

如果您接受这些 OU 的默认名称，则无需执行任何操作即可继续安装。要更改 OU 的名称，请直接在表单字段中输入新名称。

- 基础 OU — AWS Control Tower 依赖于最初命名为安全 OU 的基础组织单元。您可以在初始设置期间和之后从 OU 详细信息页面更改此 OU 的名称。此安全 OU 包含您的两个共享帐户，默认情况下，这两个帐户分别称为日志存档帐户和审核帐户。
- 其@@ 他 OU — AWS Control Tower 可以为您设置一个或多个其他 OU。除了安全 OU 之外，我们建议您在 landing zone 中配置至少一个额外的 OU。如果此附加 OU 用于开发项目，我们建议您将其命名为 Sandbox OU，如中所建立架构良好的环境的指导方针述。如果您在 AWS Organizations 中已有组织单元，则可能会看到跳过在 AWS Control Tower 中设置其他 OU 的选项。

步骤 2c. 配置您的共享账户、日志记录和加密

在设置过程的这一部分中，面板显示了您共享的 AWS Control Tower 账户名称的默认选择。这些账户是你的 landing zone 的重要组成部分。请勿移动或删除这些共享帐户。在设置过程中，您可以为审核和日志存档帐户选择自定义名称。或者，您可以一次性选择将现有 AWS 账户指定为共享账户。

您必须为日志存档和审计账户提供唯一的电子邮件地址，并且可以验证之前为管理账户提供的电子邮件地址。选择 “编辑” 按钮以更改可编辑的默认值。

关于共享账户

- 管理账户 — AWS Control Tower 管理账户属于根级别。管理账户允许 AWS Control Tower 账单。该账户还拥有您的 landing zone 的管理员权限。您不能在 AWS Control Tower 中创建单独的账单账户和管理员权限账户。

  在此设置阶段，为管理账户显示的电子邮件地址不可编辑。它显示为确认信息，因此，如果您有多个账户，则可以检查自己编辑的管理账户是否正确。
- 两个共享帐户 — 您可以为这两个帐户选择自定义名称，也可以自带帐户，并且必须为每个新帐户或现有帐户提供唯一的电子邮件地址。如果您选择让 AWS Control Tower 为您创建新的共享账户，则这些电子邮件地址必须还没有关联 AWS 账户。

要配置共享帐户，请填写所需的信息。

1. 在控制台上，输入最初名为日志存档帐户的帐户的名称。许多客户决定保留该账户的默认名称。
2. 为此账户提供一个唯一的电子邮件地址。

3. 输入最初名为审计账户的账户的名称。许多客户选择将其命名为安全账户。
4. 为此账户提供一个唯一的电子邮件地址。

（可选）配置日志保留

在此设置阶段，您可以为在 AWS Control Tower 中存储日志的 Amazon S3 存储桶自定义 AWS CloudTrail 日志保留策略，以天或年为增量，最长不超过 15 年。如果您选择不自定义日志保留期，则标准账户日志记录的默认设置为 1 年，访问日志记录的默认设置为 10 年。更新或重置 landing zone 时，此功能也可用。

（可选）自行管理访问权限 AWS 账户

您可以选择 AWS Control Tower 是通过 AWS Identity and Access Management (IAM) 设置 AWS 账户 访问权限，还是自行管理 AWS 账户 访问权限，可以选择使用您可以自己设置和自定义的 AWS IAM Identity Center 用户、角色和权限，或者使用其他方法（例如外部 IdP），用于直接联合账户或通过 IAM Identity Center 对多个账户进行联合。您可以稍后更改此选择。

默认情况下，AWS Control Tower 会根据使用多个账户组织 AWS 环境中定义的最佳实践指南，为您的着陆区设置 AWS IAM 身份中心。大多数客户选择默认值。有时需要其他访问方法，以满足特定行业或国家/地区的监管要求，或者在无法使用 AWS IAM Identity Center AWS 区域 的地方。

不支持在账户级别选择身份提供商。此选项仅适用于整个着陆区。

有关更多信息，请参阅 IAM 身份中心指南。

（可选）配置 AWS CloudTrail 跟踪

作为最佳实践，我们建议您设置日志记录。如果您希望允许 AWS Control Tower 设置组织级别的 CloudTrail 跟踪并为您进行管理，请选择加入。如果您想使用自己的 CloudTrail 跟踪或第三方日志工具管理日志记录，请选择退出。根据要求在控制台中确认您的选择。在更新 landing zone 时，您可以更改您的选择，也可以选择加入或选择退出组织级别的路线。

您可以随时设置和管理自己的 CloudTrail 跟踪，包括组织级别和账户级别的跟踪。如果您设置了重复的 CloudTrail跟踪，则在记录 CloudTrail 事件时可能会产生重复的费用。

（可选）配置 AWS KMS keys

如果您想使用加密密钥对资源进行加密和解 AWS KMS 密，请选中该复选框。如果您已有密钥，则可以从下拉菜单中显示的标识符中选择它们。您可以通过选择 “创建密钥” 来生成新密钥。您可以在任何时候更新着陆区时添加或更改 KMS 密钥。

当您选择 “设置着陆区” 时，AWS Control Tower 会执行预检查以验证您的 KMS 密钥。密钥必须满足以下要求：

- 已启用
- 对称
- 不是多区域密钥
- 已向策略添加了正确的权限
- 密钥在管理账户中

如果密钥不符合这些要求，您可能会看到错误标语。在这种情况下，请选择另一个密钥或生成一个密钥。请务必编辑密钥的权限策略，如下一节所述。

更新 KMS 密钥策略

在更新 KMS 密钥策略之前，必须先创建 KMS 密钥。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的创建密钥策略。

要在 AWS Control Tower 中使用 KMS 密钥，您必须通过添加 AWS Config 和所需的最低权限来更新默认 KMS 密钥策略 AWS CloudTrail。作为最佳实践，我们建议您在任何策略中包含所需的最低权限。更新 KMS 密钥策略时，您可以在单个 JSON 语句中或逐行添加权限。

该过程介绍如何通过添加允许 AWS Config 和 CloudTrail AWS KMS 用于加密的策略声明，在 AWS KMS 控制台中更新默认 KMS 密钥策略。政策声明要求您包括以下信息：

- **`YOUR-MANAGEMENT-ACCOUNT-ID`**— 将在其中设置 AWS Control Tower 的管理账户的 ID。
- **`YOUR-HOME-REGION`**— 您在设置 AWS Control Tower 时将选择的主区域。
- **`YOUR-KMS-KEY-ID`**— 将与策略一起使用的 KMS 密钥 ID。

更新 KMS 密钥策略

1. 在以下位置打开 AWS KMS 控制台 https://console.aws.amazon.com/kms
2. 在导航窗格中，选择客户管理的密钥。
3. 在表中，选择要编辑的密钥。
4. 在密钥策略选项卡中，确保您可以查看密钥策略。如果您无法查看密钥策略，请选择切换到策略视图。
5. 选择编辑，然后通过为和添加以下策略声明来更新默认 KMS 密钥策略 CloudTrail。 AWS Config

AWS Config 政策声明

```
{
    "Sid": "Allow Config to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "config.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID"
}
```

CloudTrail 政策声明

```
{
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
        }
    }
}
```

6. 选择保存更改。

KMS 密钥策略示例

以下示例策略显示了在添加授予权限 AWS Config 和 CloudTrail 最低所需权限的策略声明后，您的 KMS 密钥策略可能是什么样子。示例策略不包括您的默认 KMS 密钥策略。

```
{
    "Version": "2012-10-17",
    "Id": "CustomKMSPolicy",
    "Statement": [
        {
        ... YOUR-EXISTING-POLICIES ...
        },
        {
            "Sid": "Allow Config to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
        },
        {
            "Sid": "Allow CloudTrail to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
              ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
```

```
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

要查看其他示例策略，请参阅以下页面：

- 在《AWS CloudTrail 用户指南》中@@ 授予加密权限。
- 开发人员指南@@ 中使用服务相关角色时 KMS 密钥所需的权限（Less3 存储桶交付）。AWS Config

> **防范攻击者**
>
> 通过在策略中添加某些条件，您可以帮助防止一种特定类型的攻击，即混淆副手攻击，这种攻击发生在实体强迫权限更高的实体执行操作（例如跨服务模仿）时发生。有关政策条件的一般信息，另请参阅在策略中指定条件。

AWS Key Management Service (AWS KMS) 允许您创建多区域 KMS 密钥和非对称密钥；但是，AWS Control Tower 不支持多区域密钥或非对称密钥。AWS Control Tower 会对您的现有密钥进行预检查。如果您选择多区域密钥或非对称密钥，则可能会看到一条错误消息。在这种情况下，请生成另一个密钥以用于 AWS Control Tower 资源。

有关的更多信息 AWS KMS，请参阅《AWS KMS 开发人员指南》。

请注意，默认情况下，AWS Control Tower 中的客户数据是使用 SSE-S3 进行静态加密的。

（可选）配置和创建自定义成员账户

当您按照创建账户工作流程添加成员账户时，您可以选择指定先前定义的蓝图，用于从 AWS Control Tower 控制台配置自定义成员账户。如果您没有可用的蓝图，则可以稍后自定义帐户。请参阅 使用 Account Factory 自定义 (AFC) 自定义账户。

第 3 步。查看并设置着陆区

设置的下一部分将向您展示 AWS Control Tower 对您的着陆区所需的权限。选中一个复选框可展开每个主题。您将被要求同意这些权限（这可能会影响多个账户），并同意总体服务条款。

待敲定

1. 在控制台上查看服务权限，准备就绪后，选择我了解 AWS Control Tower 代表我管理 AWS 资源和执行规则时将使用的权限。
2. 要完成选择并初始化启动，请选择设置 landing zon e。

这一系列步骤将开始设置着陆区（Landing zone）的过程，这可能需要大约三十分钟才能完成。在设置过程中，AWS Control Tower 会创建您的根级别、安全 OU 和共享账户。其他 AWS 资源被创建、修改或删除。

> **⚠ 确认 SNS 订阅**
>
> 您为审计账户提供的电子邮件地址将收到来自 AWS Control Tower 支持的每个 AWS 地区的AWS 通知 — 订阅确认电子邮件。要在您的审计账户中接收合规电子邮件，您必须在来自 AWS Control Tower 支持的每个 AWS 区域的每封电子邮件中选择确认订阅链接。

使用 API 开始使用 AWS Control Tower

本入门程序适用于 AWS Control Tower 管理员。此过程需要一些先决条件，包括两个主要步骤。

在此过程中，您将使用来自 AWS Control Tower 的 API 和其他 AWS 服务来配置和启动着陆区。这些 API 允许您通过控制台或通过 AWS CloudFormation 以编程方式创建 AWS Control Tower 环境。 AWS CLI

在启动 AWS Control Tower 着陆区之前，请执行以下先决任务：

- 确定最合适的家乡区域。有关更多信息，请参阅 设置着陆区的管理提示 。
- 查看 先决条件：自动对您的管理账户进行启动前检查 以了解自动启动前检查的信息，这些检查可确保您的管理账户已准备就绪，可以进行建立 landing zone 的更改。

主题

- 对使用 API 进行着陆区配置的期望

- 第 1 步：配置您的着陆区
- 第 2 步：启动您的着陆区
- 确定你的着陆区
- 更新你的着陆区
- 重置 landing zone 以解决漂移问题
- 停用你的着陆区
- 示例：仅使用 API 设置 AWS Control Tower 着陆区
- 使用启动着陆区 AWS CloudFormation

对使用 API 进行着陆区配置的期望

设置 AWS Control Tower 着陆区的过程分为多个步骤。您的 AWS Control Tower 着陆区的某些方面是可以配置的。其他选项在设置后无法更改。

安装过程中要配置的关键项目

- 你可以在设置过程中选择你的基础 OU 名称，也可以在设置好着陆区后更改 OU 名称。默认情况下，基础 OU 命名为 “安全” 和 “沙盒”。有关更多信息，请参阅 建立架构良好的环境的指导方针。
- 在设置过程中，您可以为 AWS Control Tower 创建的共享账户选择自定义名称，默认情况下称为日志存档和审计，但在设置后无法更改这些名称。（这是一次性选择。）
- 在使用 API 进行设置期间，您必须为 AWS Control Tower 指定现有 AWS 账户以用作审计和日志存档账户。要指定现有 AWS 账户，如果这些账户有现有 AWS Config 资源，则必须先删除或修改现有 AWS Config 资源，然后才能将这些账户注册到 AWS Control Tower。（这是一次性选择。）
- 如果您是首次设置，或者要升级到着陆区版本 3.0，则可以选择是否允许 AWS Control Tower 为您的组织设置组织级别的 AWS CloudTrail 跟踪，也可以选择退出由 AWS Control Tower 管理的跟踪并管理自己的 CloudTrail 跟踪。在更新着陆区时，您可以随时选择加入或选择退出由 AWS Control Tower 管理的组织级跟踪。
- 在设置或更新着陆区时，您可以选择为 Amazon S3 日志存储桶和日志访问存储桶设置自定义的保留政策。

无法撤消的配置选项

- 设置了着陆区后，您就无法更改自己的主区域。
- 如果您要为账户配置 VPC，则在创建 VPC CIDR 后无法对其进行更改。

接下来的章节详细介绍了安装前提条件和步骤，并附有说明和注意事项。有关其他代码示例，请参阅示例：仅使用 API 设置 AWS Control Tower 着陆区。

第 1 步：配置您的着陆区

设置 AWS Control Tower 着陆区的过程分为多个步骤。AWS Control Tower 着陆区的某些方面是可配置的，但其他选项在设置后无法更改。要在启动 landing zone 之前详细了解这些重要注意事项，请查看 对 landing zone 配置的期望 。

在使用 AWS Control Tower 着陆区 API 之前，您必须先从其他 AWS 服务调用 API 来配置您的着陆区，然后才能启动。该过程包括三个主要步骤：

- 创建一个新 AWS Organizations 组织，
- 设置您的共享账户电子邮件地址，
- 并创建具有调用 landing zone API 所需权限的 IAM 角色或 IAM 身份中心用户。

第 1 步。创建包含你的 landing zone 的组织：

1. 调用 AWS Organizations `CreateOrganization` API 并启用所有功能以创建基础 OU。AWS Control Tower 最初将其命名为安全 OU。此安全 OU 包含您的两个共享帐户，默认情况下，这两个帐户分别称为日志存档帐户和审核帐户。

   ```
   aws organizations create-organization --feature-set ALL
   ```

   AWS Control Tower 可以设置一个或多个其他 OU。除了安全 OU 之外，我们建议您在 landing zone 中配置至少一个额外的 OU。如果此附加 OU 用于开发项目，我们建议您将其命名为 Sandbox OU，如中所AWS AWS Control Tower 着陆区的多账户策略述。

第 2 步。如有@@ 必要，可配置共享账户：

要设置您的着陆区，AWS Control Tower 需要两个电子邮件地址。如果您是首次使用着陆区 API 设置 AWS Control Tower，则必须使用现有的安全账户和日志存档 AWS 账户。您可以使用现有电子邮件地址的当前电子邮件地址 AWS 账户。这些电子邮件地址中的每一个都将用作协作收件箱（共享电子邮件账户），供企业中从事与 AWS Control Tower 相关的特定工作的不同用户使用。

要开始设置新的着陆区，如果您没有现有 AWS 帐户，则可以使用 AWS Organizations API 配置安全和日志存档 AWS 帐户。

1. 调用 AWS Organizations `CreateAccount` API 在安全 OU 中创建日志存档账户和审核账户。

```
aws organizations create-account --email mylog@example.com --account-name "Logging
 Account"
```

```
aws organizations create-account --email mysecurity@example.com --account-name
 "Security Account"
```

2. （可选）使用 AWS Organizations `DescribeAccount` API 检查`CreateAccount`操作的状态。

第 3 步。创建所需的服务角色

创建以下 IAM 服务角色，让 AWS Control Tower 能够执行设置您的着陆区所需的 API 调用：

- AWSControlTowerAdmin
- AWSControlTowerCloudTrailRole
- AWSControlTowerStackSetRole
- AWSControlTowerConfigAggregatorRoleForOrganizations

有关这些角色及其策略的更多信息，请参阅在 AWS Control Tower 中使用基于身份的策略（IAM 策略）。

要创建 IAM 角色，请执行以下操作：

1. 创建具有调用所有 landing zone API 所需权限的 IAM 角色。或者，您可以创建 IAM Identity Center 用户并分配必要的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
```

```
                "controltower:ListLandingZones",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "sso:*",
                "sso-directory:*",
                "logs:*",
                "cloudformation:*",
                "kms:*",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:GetSAMLProvider",
                "iam:CreateSAMLProvider",
                "iam:CreateServiceLinkedRole",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

第 2 步：启动您的着陆区

AWS Control Tower `CreateLandingZone` API 需要一个着陆区版本和一个清单文件作为输入参数。您可以使用清单文件来配置以下功能：

- （可选）配置日志保留
- （可选）自行管理访问权限 AWS 账户
- （可选）配置 AWS CloudTrail 跟踪
- （可选）配置 AWS KMS keys

编译清单文件后，您就可以创建新的着陆区了。

> **Note**
>
> 使用 API 配置和启动着陆区时，AWS Control Tower 不支持区域拒绝控制。使用 API 成功启动您的着陆区后，您可以使用 AWS Control Tower 控制台配置区域拒绝控制。

1. 调用 AWS Control Tower `CreateLandingZone` API。此 API 需要一个 landing zone 版本和清单文件作为输入。

```
aws controltower create-landing-zone --landing-zone-version 3.3 --manifest "file://
LandingZoneManifest.json"
```

LandingZoneManifest.json 清单示例：

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
```

```
   "accessManagement": {
        "enabled": true
   }
}
```

> **Note**
>
> 如示例所示， CentralizedLogging 和 SecurityRoles 账户AccountId的必须不同。

输出：

```
{
   "arn": "arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

2. 调用 GetLandingZoneOperation API 来检查CreateLandingZone操作的状态。GetLandingZoneOperationAPI 返回的状态为SUCCEEDEDFAILED、或IN_PROGRESS。

```
aws controltower get-landing-zone-operation --operation-identifier "55XXXXXX-
eXXX-4XXX-aXXX-44XXXXXXXXXX"
```

输出：

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "Thu Nov 09 20:39:19 UTC 2023",
        "endTime": "Thu Nov 09 21:02:01 UTC 2023",
        "status": "SUCCEEDED"
    }
}
```

3. 当状态返回为时SUCCEEDED，您可以调用 GetLandingZone API 来查看 landing zone 配置。

```
aws controltower get-landing-zone --landing-zone-identifier "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

输出：

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "333333333333"
            },
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "CORE"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
```

```
        "status": "PROCESSING",
        "version": "3.3"
    }
}
```

确定你的着陆区

致电ListLandingZones可以帮助您确定您的账户是否已经设置了 AWS Control Tower。此 API 会在任何商业区域返回一个着陆区标识符 (ARN)，无论该着陆区的主区域如何。着陆区 ARN 在区域上是独一无二的。

```
aws controltower list-landing-zones --region us-east-1
```

对于选择加入的区域，只有当您在与 *ListLandingZones* API 的主区域相同的区域调用 API 时，API 才会返回着陆区域标识符。例如，如果您的着陆区设置在 af-south-1 中，而您调用 af-south -1，则 AP *ListLandingZones* I 会返回着陆区标识符。如果你的着陆区是在 af-south-1 中设置的，而你调用 **ListLandingZones** ap-east-1，那么 API 不会返回着陆区标识符。

输出：

```
{
   "landingZones" [
        "arn": "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
   ]
}
```

更新你的着陆区

当有新的着陆区版本可用时，或者要对着陆区配置进行其他更新，您可以调用 UpdateLandingZone API 并引用更新的清单文件。此 API 会返回一个OperationIdentifier，然后您可以在调用 GetLandingZoneOperation API 时使用它来检查更新操作的状态。

更新着陆区

1. 调用 AWS Control Tower UpdateLandingZone API 并参考更新的着陆区版本或更新后的清单。

```
aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-
identifier "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
 --manifest file://LandingZoneManifest.json
```

LandingZoneManifest.json：

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays":2555
            },
            "accessLoggingBucket": {
                "retentionDays": 2555
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

输出：

```
{
```

```
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

（可选）重新注册 OU 以更新账户

对于账户少于 300 的已注册 AWS Control Tower OU，您可以使用 AWS Control Tower 控制台访问控制面板中的 O U 页面，然后选择重新注册 OU 以更新该 OU 中的账户。

重置 landing zone 以解决漂移问题

创建着陆区时，着陆区以及所有组织单位 (OU)、账户和资源都符合您选择的控件强制执行的管理规则。当您和您的组织成员使用 landing zone 时，这种合规状态可能会发生变化。这些变化被称为漂移。

要确定您的着陆区是否处于漂移状态，您可以调用 GetLandingZone API。此 API 返回着陆区的漂移状态为DRIFTED或IN_SYNC。

要解决着陆区内的漂移问题，您可以使用 ResetLandingZone API 将着陆区重置回其原始配置。例如，AWS Control Tower 默认启用 IAM Identity Center 来帮助您 AWS 账户管理自己的，但是如果您在禁用 IAM 身份中心的情况下配置原始着陆区参数，则调用会ResetLandingZone保持禁用的 IAM 身份中心配置。

只有在使用最新可用的 landing zone 版本时，才能使用ResetLandingZone该 API。您可以调用 GetLandingZone API 并将您的 landing zone 版本与最新可用版本进行比较。如有必要，你可以 更新你的着陆区 让你的着陆区使用最新的可用版本。在这些示例中，我们使用版本 3.3 作为最新版本。

1. 调用 GetLandingZone API。如果 API 返回的漂移状态为DRIFTED，则您的着陆区处于漂移状态。
2. 调用 ResetLandingZone API 将您的着陆区重置为其原始配置。

```
aws controltower reset-landing-zone --landing-zone-identifier
 "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

输出：

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
```

```
}
```

> **Note**
>
> 重置着陆区不会更新着陆区版本。查看 更新你的着陆区 有关更新 landing zone 版本的详细信息。

停用你的着陆区

清理所有着陆区资源的过程称为停用着陆区。

> **Important**
>
> 我们强烈建议您仅在打算停止使用登录区时才执行此停用过程。在您停用现有的登录区后，无法重新创建此登录区。

有关停用着陆区的更多详细信息，包括有关 AWS Control Tower 如何处理您的数据和现有数据的重要信息 AWS Organizations，请查看演练：停用 AWS Control Tower 着陆区。

要停用着陆区，请调用 `DeleteLandingZone` API。此 API 会返回一个`OperationIdentifier`，然后您可以在调用 `GetLandingZoneOperation` API 时使用它来检查删除操作的状态。

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

输出：

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

示例：仅使用 API 设置 AWS Control Tower 着陆区

本示例演练是一份配套文档。有关解释、注意事项和更多信息，请参阅使用 API 开始使用 AWS Control Tower。

先决条件

在创建 AWS Control Tower 着陆区之前，您必须创建一个组织、两个共享账户和一些 IAM 角色。本演练教程包括这些步骤，以及示例 CLI 命令和输出。

第 1 步。创建组织和两个必需的帐户。

```
aws organizations create-organization --feature-set ALL
aws organizations create-account --email example+log@example.com --account-name "Log
 archive account"
aws organizations create-account --email example+aud@example.com --account-name "Audit
 account"
```

第 2 步。创建所需的 IAM 角色。

AWSControlTowerAdmin

```
cat <<EOF >controltower_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://controltower_trust.json
cat <<EOF >ct_admin_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
```

```
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
 AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy
```

AWSControlTowerCloudTrailRole

```
cat <<EOF >controltower_trust.json
        {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerCloudTrailRole --path /service-role/ --
assume-role-policy-document file://cloudtrail_trust.json
cat <<EOF >cloudtrail_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
```

```
EOF
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://
cloudtrail_role_policy.json
```

AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerStackSetRole --path /service-role/ --
assume-role-policy-document file://cloudformation_trust.json
cat <<EOF >stackset_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerStackSetRole --policy-name
 AWSControlTowerStackSetRolePolicy --policy-document file://stackset_role_policy.json
```

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

第 3 步。获取账户 ID 并生成 landing zone 清单文件。

以下示例中的前两个命令将您在步骤 1 中创建的账户的账户 ID 存储到变量中。然后，这些变量有助于生成 landing zone 清单文件。

```
sec_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Audit account") | .Id')
log_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Log archive account") | .Id')

cat <<EOF >landing_zone_manifest.json
{
   "governedRegions": ["us-west-1", "us-west-2"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "$log_account_id",
```

```
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            }
        },
        "enabled": true
    },
    "securityRoles": {
        "accountId": "$sec_account_id"
    },
    "accessManagement": {
        "enabled": true
    }
}
EOF
```

第 4 步。使用最新版本创建着陆区。

您必须使用清单文件和最新版本来设置 landing zone。此示例显示版本 3.3。

```
aws --region us-west-1 controltower create-landing-zone --manifest file://
landing_zone_manifest.json --landing-zone-version 3.3
```

输出将包含一个 arn 和一个操作标识符，如以下示例所示。

```
{
    "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNUOL2AXXX",
    "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
}
```

第 5 步。（可选）跟踪您的着陆区创建操作的状态。

要跟踪状态，请使用上一个`create-landing-zone`命令输出中的操作标识符。

```
aws --region us-west-1 controltower get-landing-zone-operation --operation-identifier
 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx
```

状态输出示例：

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "2024-02-28T21:49:31Z",
        "status": "IN_PROGRESS"
    }
}
```

您可以使用以下示例脚本来帮助您设置循环，该循环会像日志文件一样一遍又一遍地报告操作的状态。这样你就不必继续输入命令了。

```
while true; do echo "$(date) $(aws --region us-west-1 controltower get-landing-
zone-operation --operation-identifier 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx | jq -
r .operationDetails.status)"; sleep 15; done
```

显示有关您的着陆区的详细信息

第 1 步。找到着陆区的 ARN

```
aws --region us-west-1 controltower list-landing-zones
```

输出将包括着陆区的标识符，如以下输出示例所示。

```
{
    "landingZones": [
        {
            "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX"
        }
    ]
}
```

第 2 步。获取信息

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
 arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX
```

以下是您可能看到的输出类型的示例：

```
{
    "landingZone": {
```

```
        "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "9750XXXX4444"
            },
            "governedRegions": [
                "us-west-1",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "012345678901",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "ACTIVE",
        "version": "3.3"
    }
}
```

使用启动着陆区 AWS CloudFormation

您可以通过 AWS CloudFormation 控制台 AWS CloudFormation 或通过配置和启动 landing zone AWS CLI。本节提供使用 API 启动着陆区的说明和示例 AWS CloudFormation。

主题

使用启动着陆区的先决条件 AWS CloudFormation

1. 从中 AWS CLI，使用 AWS Organizations `CreateOrganization` API 创建组织并启用所有功能。

   有关更详细的说明，请查看 第 1 步：配置您的着陆区 。

2. 从 AWS CloudFormation 控制台或使用部署一个在管理账户中创建以下资源的 AWS CloudFormation 模板： AWS CLI
   - 日志存档账户（有时称为 “记录” 账户）
   - 审计账户（有时称为 “安全” 账户）
   - AWSControlTowerAdmin、AWSControlTowerCloudTrailRoleAWSControlTowerConfigAggregatorRoleF和AWSControlTowerStackSetRole服务角色。

     有关 AWS Control Tower 如何使用这些角色执行着陆区 API 调用的信息，请参阅步骤 1：配置您的着陆区。

```
Parameters:
  LoggingAccountEmail:
    Type: String
    Description: The email Id for centralized logging account
  LoggingAccountName:
    Type: String
    Description: Name for centralized logging account
  SecurityAccountEmail:
    Type: String
    Description: The email Id for security roles account
  SecurityAccountName:
    Type: String
    Description: Name for security roles account
```

```
Resources:
  MyOrganization:
    Type: 'AWS::Organizations::Organization'
    Properties:
      FeatureSet: ALL
  LoggingAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref LoggingAccountName
      Email: !Ref LoggingAccountEmail
  SecurityAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref SecurityAccountName
      Email: !Ref SecurityAccountEmail
  AWSControlTowerAdmin:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerAdmin
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: controltower.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub >-
          arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
  AWSControlTowerAdminPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerAdminPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action: 'ec2:DescribeAvailabilityZones'
            Resource: '*'
      Roles:
        - !Ref AWSControlTowerAdmin
  AWSControlTowerCloudTrailRole:
```

```
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerCloudTrailRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudtrail.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerCloudTrailRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerCloudTrailRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action:
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
            Resource: !Sub >-
              arn:${AWS::Partition}:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerCloudTrailRole
  AWSControlTowerConfigAggregatorRoleForOrganizations:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerConfigAggregatorRoleForOrganizations
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: config.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSConfigRoleForOrganizations
  AWSControlTowerStackSetRole:
    Type: 'AWS::IAM::Role'
```

```
    Properties:
      RoleName: AWSControlTowerStackSetRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerStackSetRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerStackSetRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action: 'sts:AssumeRole'
            Resource: !Sub 'arn:${AWS::Partition}:iam::*:role/
AWSControlTowerExecution'
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerStackSetRole

Outputs:
  LogAccountId:
    Value:
      Fn::GetAtt: LoggingAccount.AccountId
    Export:
      Name: LogAccountId
  SecurityAccountId:
    Value:
      Fn::GetAtt: SecurityAccount.AccountId
    Export:
      Name: SecurityAccountId
```

使用创建新的着陆区 AWS CloudFormation

从 AWS CloudFormation 控制台或使用 AWS CLI，部署以下 AWS CloudFormation 模板来创建 landing zone。

```
Parameters:
```

```
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: List
    Description: List of governed regions
  SecurityOuName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOuName:
    Type: String
    Description: The sandbox Organizational Unit name
  CentralizedLoggingAccountId:
    Type: String
    Description: The AWS account ID for centralized logging
  SecurityAccountId:
    Type: String
    Description: The AWS account ID for security roles
  LoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for centralized logging bucket
  AccessLoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for access logging bucket
  KMSKey:
    Type: String
    Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
 logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
        - Key: "keyname2"
          Value: "value2"
      Manifest:
        governedRegions:
          Ref: GovernedRegions
        organizationStructure:
          security:
```

```
        name:
          Ref: SecurityOuName
      sandbox:
        name:
          Ref: SandboxOuName
    centralizedLogging:
      accountId:
        Ref: CentralizedLoggingAccountId
      configurations:
        loggingBucket:
          retentionDays:
            Ref: LoggingBucketRetentionPeriod
        accessLoggingBucket:
          retentionDays:
            Ref: AccessLoggingBucketRetentionPeriod
        kmsKeyArn:
          Ref: KMSKey
      enabled: true
    securityRoles:
      accountId:
        Ref: SecurityAccountId
    accessManagement:
      enabled: true
```

使用管理现有着陆区 AWS CloudFormation

通过将着陆区导入 AWS CloudFormation 到新的或现有 AWS CloudFormation 堆栈中，您可以使用来管理已经启动的着陆区。有关详细信息和说明，请查看 “将现有资源纳入 CloudFormation 管理”。

要检测和解决着陆区内的漂移问题，您可以使用 AWS Control Tower 控制台 AWS CLI、或 ResetLandingZoneAPI。

后续步骤

现在，您的着陆区设置好了，就可以开始使用了。

要详细了解如何使用 AWS Control Tower，请参阅以下主题：

- 有关建议的管理做法，请参阅最佳实践。
- 您可以设置具有特定角色和权限的 IAM Identity Center 用户和群组。有关建议，请参阅 设置群组、角色和策略的建议 。

- 要开始通过您的 AWS Organizations 部署注册组织和帐户，请参阅管理现有组织和账户。
- 您的最终用户可以使用 Account Factory 在您的着陆区中配置自己的 AWS 账户。有关更多信息，请参阅配置和配置账户的权限。
- 为确保AWS Control Tower 的合规性验证这一点，您的中央云管理员可以查看日志存档帐户中的日志档案，指定的第三方审计员可以查看审计（共享）帐户中的审计信息，该帐户是安全组织的成员。
- 要了解有关 AWS Control Tower 功能的更多信息，请参阅相关信息。
- 请尝试访问精选的 YouTube 视频列表，这些视频详细介绍了如何使用 AWS Control Tower 功能。
- 您可能需要不时更新着陆区，以获取最新的后端更新、最新的控件并保留您的着陆区 up-to-date。有关更多信息，请参阅AWS Control Tower 中的配置更新管理。
- 如果您在使用 AWS Control Tower 时遇到问题，请参阅故障排除。

> **Important**
>
> 如果您尚未为账户的根用户启用 MFA，请立即启用。有关根用户最佳做法的更多信息，请参阅保护账户根用户的最佳实践。

AWS Control Tower 中的限制和配额

本章介绍在使用 AWS Control Tower 时应记住的 AWS 服务限制和配额。如果您由于服务配额问题而无法设置着陆区，请联系AWS Support。

有关特定于控件的限制的更多信息，请参阅控制限制。

> 新的《控件参考指南》
>
> 有关 AWS Control Tower 控件的信息已移至 AWS 控制塔控件参考指南。

AWS Control Tower 的局限性

本节介绍了 AWS Control Tower 中的已知限制和不支持的用例。

- AWS Control Tower 存在总体并发限制。通常，一次只能进行一次操作。此限制允许有两个例外情况：
  - 可选控件可以通过异步过程同时激活和停用。一次最多可以进行一百 (100) 个与控制相关的操作，无论这些操作是从控制台调用还是从 API 调用。在这100个操作中，一次最多有20个可以是主动控制操作。
  - 可以通过异步流程在 Account Factory 中同时配置、更新和注册账户，最多可以同时进行五 (5) 次与账户相关的操作。一次只能对一个账户执行取消管理操作。
- 可以更改安全 OU 中共享账户的电子邮件地址，但您必须更新着陆区才能在 AWS Control Tower 控制台中看到这些更改。
- 在 AWS Control Tower 着陆区内，每个 OU 有五 (5) 个 SCP 的上限。
- AWS Control Tower 支持您的着陆区组织中的多达 10,000 个账户，这些账户分配给您的所有 OU。
- 拥有超过 300 个直接嵌套账户的现有 OU 无法在 AWS Control Tower 中注册或重新注册。有关注册 OU 的限制的更多信息，请参阅区域和堆栈集限制。
- 由于某些依赖项不可用，因此无法在 AWS Control Tower (cfcT) 中进行 AWS 区域自定义：
  - 亚太地区（雅加达和大阪）
  - 以色列（特拉维夫）
  - 中东（阿联酋）
  - 欧洲（西班牙）

  - 亚太地区（海得拉巴）
  - 欧洲（苏黎世）
  - 加拿大西部（卡尔加里）

  如果您将 cfcT 部署到您的 AWS Control Tower 主区域，则可以使用 cfCT 在这些区域部署和管理资源，但无法在这些区域构建 cfcT。

- AWS Control Tower Account Factory for Terraform (AFT) 在以下 AWS 区域版本中不可用，因为某些依赖项不可用：
  - 以色列（特拉维夫）
  - 中东（阿联酋）
  - 欧洲（西班牙）
  - 亚太地区（海得拉巴）
  - 欧洲（苏黎世）
  - 加拿大西部（卡尔加里）
- 以下区域不支持 IAM 身份中心。
  - 中东（阿联酋）区域，me-central-1
  - 亚太地区（海得拉巴）区域，ap-south-2
  - 加拿大西部（卡尔加里），ca-west-1

  有关 IAM Identity Center 的更多 AWS 区域 信息和支持，请参阅 Identity and A ccess Managem AWS ent 用户指南中的区域和终端节点。
- 以下区域不支持 AWS Service Catalog。
  - 加拿大西部（卡尔加里），ca-west-1

  有关不支持的区域中的 AWS Control Tower 功能的更多信息 AWS Service Catalog，请参阅AWS Control Tower 已在 AWS 加拿大西部（卡尔加里）上市。
- 调用控制 API 来激活或停用控件时，AWS Control Tower 中的限制`EnableControl`和`DisableControl`更新限制为一百 (100) 个并发操作。十个操作 (10) 可以同时进行，其余操作则排队。您可能需要调整代码以等待完成。
- 在 100 个控制操作的总体限制范围内，一次最多可以有 20 个操作是主动控制操作。
- 当您使用基于 Terraform 的蓝图通过 Account Factory 自定义 (AFC) 配置账户时，您只能将这些蓝图部署到一个蓝图。 AWS 区域默认情况下，AWS Control Tower 会部署到主区域。

请求提高限额

服务配额控制台提供有关 AWS Control Tower 配额的信息。您可以使用“服务限额”控制台查看默认的服务限额或可调整限额请求增加限额。

可以通过 Service Quotas 控制台查看以下配额

- 并发账户操作配额：可以同时执行的最大并发账户操作数。默认值：5，最大值：10，可调
- 单个 OU 中的账户数量：一个 OU 中可以存在的 AWS Control Tower 托管账户的最大数量。如果您添加的账户超过此限制，则无法在 AWS Control Tower 中执行 OU 注册流程。要详细了解每个 OU 的账户数量，请查看 AWS C 区域和堆栈集限制 ontrol Tower 文档。默认值：300，不可调节。
- 组织单位 (OU) 的并发操作：可以同时执行的最大并发操作数。默认：1，不可调。

例如，您可以请求将配额从最多十个并发账户相关操作中的五个增加到十个。配额增加后，AWS Control Tower 的某些性能特征可能会发生变化。例如，当组织单位中有更多账户时，更新组织单位可能需要更长时间。或者，在具有五个 SCP 的 OU 上完成操作可能需要比使用三个 SCP 更长的时间。

> **Note**
>
> 增加服务配额的请求可能需要最多两天才能生效。请务必从您的 AWS Control Tower 主区域申请增加配额。

或者，您可以联系AWS 支持部门，请求增加 AWS Control Tower 中某些资源的配额。或者，您可以观看下面的视频，并学习如何自动增加某些服务配额。

视频：自动请求增加与 AWS Control Tower 相关的服务配额

本视频 (7:24) 介绍如何根据 AWS Control Tower 中的部署自动增加相关集成 AWS 服务的服务配额。它还展示了如何为您的组织自动注册新帐户到 AWS 企业支持中。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

AWS Control Tower 中配额增加的视频演练。

在此环境中配置新账户时，您可以使用生命周期事件触发自动请求增加指定服务配额 AWS 区域。

有关 AWS 配额的更多信息，请参阅《AWS 一般参考》。

控制限制

> **新的《控件参考指南》**
>
> 有关 AWS Control Tower 控件的信息已移至 AWS 控制塔控件参考指南。

如果您修改 AWS Control Tower 资源（例如 SCP），或者删除任何 AWS Config 资源（例如配置记录器或聚合器），AWS Control Tower 将无法再保证控件按设计运行。因此，您的多账户环境的安全性可能会受到损害。安全分 AWS 担责任模式适用于您可能做出的任何此类更改。

> **Note**
>
> AWS Control Tower 在更新着陆区时将控件的 SCP 重置为标准配置，从而帮助维护环境的完整性。从设计上讲，您可能对 SCP 所做的更改会被控件的标准版本所取代。

AWS Control Tower 中的某些控件无法在 AWS Control Tower 可用 AWS 区域 的地方运行，因为这些区域不支持所需的底层功能。此限制会影响 Sec urity Hub 服务托管标准：AWS Control Tower 中的某些侦探控制措施、某些主动控制措施和某些控制措施。有关区域可用性的更多信息，请参阅区域服务列表文档和 Sec urity Hub 控件参考文档。

在混合治理的情况下，控制行为也受到限制。有关更多信息，请参阅 配置区域时避免混合治理。

有关 AWS Control Tower 如何管理区域和控制的限制的更多信息，请参阅激活 AWS 选择加入区域的注意事项。

您可以在 AWS Control Tower 控制台中查看每个控件的区域。

以下 AWS 区域不支持 Security Hub 服务托管标准中的控件：AWS Control Tower。

- 亚太地区（香港）区域，ap-east-1
- 亚太地区（雅加达）区域，ap-southeast-3
- 亚太地区（大阪）区域，ap-northeast-3
- 欧洲（米兰）区域，eu-south-1
- 非洲（开普敦）区域，af-south-1
- 中东（巴林）区域，me-south-1
- 以色列（特拉维夫），il-central-1

- 中东（阿联酋）区域，me-central-1
- 欧洲（西班牙）区域，eu-south-2
- 亚太地区（海得拉巴）区域，ap-south-2
- 欧洲（苏黎世）区域，eu-central-2
- 亚太地区（墨尔本）区域，ap-southeast-4
- 加拿大西部（卡尔加里），ca-west-1

以下内容 AWS 区域 不支持主动控制。

- 加拿大西部（卡尔加里）

下表显示了某些情况下不支持的主动控制 AWS 区域。

控制标识符	不支持的区域
CT.REDSHIFT.PR.5	ap-southeast-4、ap-southeast-2、ap-southeast-3、eu-central-2、eu-southeast-2、il-central-1、me-central-1、me-central-1
CT.DAX.PR.2	us-west-1
CT.GLUE.PR.2	不支持

下表显示了某些情况下不支持的 AWS Control Tower 侦探控件 AWS 区域。

控制标识符	不支持的区域
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-northeast-3、ap-southeast-3、il-central-1、ap-southeast-4、ca-west-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_EMR_MASTER_NO_PUBLIC_IP	ap-northeast-3、ap-southeast-3、af-southeast-1、eu-southeast 1、il-central-1、me-central-1、eu-southeast-2、ap-southeas

控制标识符	不支持的区域
	t-2、ap-southeast-2、eu-central-2、ap-southeast-2 southeast-4，ca-west-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK	eu-south-2
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	ap-northeast-3、ap-southeast-3、ap-southeast-3、ap-southeast-2、ca-west-1
AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS	ap-northeast-3、ap-southeast-3、af-southeast-1、eu-southeast 1、il-central-1、me-central-1、eu-southeast-2、ap-southeast-2、ap-southeast-2、eu-central-2、ap-southeast-2 southeast-4，ca-west-1
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	ap-northeast-3、ap-southeast-3、af-southeast-1、eu-southeas-1、us-west-1、il-central-1、me-central-1、eu-southeast-1、eu-southeast-2、eu-southeal-2、eu-central-2 central-southeast-4、ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-southeast-3、il-central-1、eu-southeast 2、ap-southeast-2、eu-central-2、ap-southeast-4、ca-west-1
AWS-GR_RESTRICTED_SSH	af-southeast-1、ap-northeast-3、ap-southeast-2、ap-southeast-3、ap-southeast -4、eu-central-2、eu-southeast-1、eu-southeast-1、eu-southeast-1、eu-southeast me-central-1
AWS-GR_DMS_REPLICATION_NOT_PUBLIC	af-south-1、ap-southeast-2、ap-southeast-3、ap-southeast-4、eu-central-2、eu-southeast-1、eu-southeast-2、il-central-1、il-central-1、cawest-1 ca-west-1

控制标识符	不支持的区域
AWS-GR_RDS_SNAPSHOTS_PUBLIC_PROHIBITED	af-southeast-1、ap-southeast-4、eu-central-2、eu-south-1、eu-south-2、il-central-1
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	ap-northeast-3
AWS-GR_ENCRYPTED_VOLUMES	af-south-1、ap-northeast-3、eu-south-1、il-central-1
AWS-GR_RESTRICTED_COMMON_PORTS	af-south-1、ap-northeast-3、eu-central-2、eu-south-1、eu-south-2、il-central-1、me-central-1、me-central-1
AWS-GR_IAM_USER_MFA_ENABLED	il-central-1、me-central-1、eu-south-2、ap-southeast 2、eu-central-2、ap-southeast-4、ca-west-1
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	il-central-1、me-central-1、eu-south-2、ap-southeast 2、eu-central-2、ap-southeast-4、ca-west-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	il-central-1，ca-west-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	il-central-1、me-central-1、ca-west-1
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	il-central-1、eu-south-2、eu-central-2
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2、eu-south-2
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	ap-south-2、eu-south-2
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-southeast-2、ap-southeast-3、eu-southeast-2、ca-west-1
AWS-GR_EC2_VOLUME_INUSE_CHECK	ca-west-1

控制标识符	不支持的区域
AWS-GR_EBS_OPTIMIZED_INSTANCE	ca-west-1

区域和堆栈集限制

如果您计划将监管范围扩展到拥有大量账户的组织实体 AWS 区域，则可能会遇到 AWS CloudFormation 堆栈集对组织整体规模的限制。您可以使用以下公式估算限制：

组织中的托管账户数量 x 受管区域数量 <= 150,000

一般而言，我们预计，将治理范围扩展到 OU 时支持的账户数量会随着受管区域数量的增加而减少。

如果您在将监管范围扩展到 OU 时激活 AWS Control Tower 可用的区域超过 15 个，则此限制就会变得显而易见。降低了每个组织单位 (OU) 的账户数量上限。

例如，如果激活 22 个区域，则限制为每个 OU 220 个账户，而不是 300 个。如果您需要将监管范围扩展到拥有超过 220 个账户的 OU，则必须减少激活区域的数量。这种减少是由于堆栈集限制造成的。

指导方针：

- 已激活 15 个区域后，最多支持 300 个账户的 OU
- 在 22 个激活区域中，最多支持 220 个账户的 OU
- 在 16 到 21 个已激活区域的情况下，支持的最大 OU 规模在 220-300 个账户之间
- 在 23 个以上的激活区域中，支持的最大组织单位规模小于 220 个账户

AWS Control Tower 功能的地区差异

AWS Control Tower 的行为存在某些差异 AWS 区域，因为 AWS Control Tower 会协调其他 AWS 服务的行为。例如：

- AWS Service Catalog 并非在所有可用 AWS Control Tower AWS 区域 的地方都可用，这会改变这些地区的 Account Factory 行为。
- 在某些区域，Account Factory 定制 (AFC) 不可用，因为服务目录无法支持蓝图的底层功能。
- AWS 区域 由于缺少底层功能，某些控件并非全部可用。
- AWS 区域 由于缺乏底层功能，AFT 和 cfCT 并非全部可用。

要最好地确定您的 AWS Control Tower 环境的行为，请确定您的所在区域。然后，评估以下项目。有关更多详细信息，请参阅 AWS Control Tower 中的限制和配额。

- 在你想要的家乡地区 AWS Service Catalog 有吗？
- 你需要的控件是否可用？ 请参阅控制限制。
- IAM 身份中心是否在您想要的家乡区域可用？

新增：AWS Control Tower 控件参考指南

有关 AWS Control Tower 中控件的信息已移至新的指南，即《AWS 控制塔控件参考指南》。

AWS Control Tower 管理员的最佳实践

本主题主要面向管理账户管理员。

管理账户管理员负责解释 AWS Control Tower 控制阻止其成员账户管理员执行的一些任务。本主题介绍了传授这些知识的一些最佳实践和程序，并提供了有关高效设置和维护 AWS Control Tower 环境的其他技巧。

向用户解释访问权限

AWS Control Tower 控制台仅适用于拥有管理账户管理员权限的用户。只有这些用户才能在您的 landing zone 内执行管理工作。根据最佳实践，这意味着您的大多数用户和成员账户管理员将永远看不到 AWS Control Tower 控制台。作为管理账户管理员组的成员，您有责任酌情向成员账户的用户和管理员解释以下信息。

- 解释用户和管理员可以访问 landing zone 内的哪些 AWS 资源。
- 列出适用于每个组织单位 (OU) 的预防性控制措施，以便其他管理员可以相应地计划和执行其 AWS 工作负载。

解释资源访问权限

某些管理员和其他用户可能需要解释他们在您的 landing zone 内可以访问的 AWS 资源。此类访问可以包括编程访问和基于控制台的访问。一般而言，允许对 AWS 资源进行读取和写入权限。要在内部执行工作 AWS，您的用户需要在一定程度上访问他们完成工作所需的特定服务。

有些用户（例如您的 AWS 开发人员）可能需要了解他们可以访问的资源，这样他们才能创建工程解决方案。其他用户（例如在 AWS 服务上运行的应用程序的最终用户）不需要知道您的 landing zone 内的 AWS 资源。

AWS 提供了用于识别用户 AWS 资源访问范围的工具。确定用户访问的范围后，您可以根据组织的信息管理策略与用户共享该信息。有关这些工具的更多信息，请参阅下面的链接。

- AWS 访问顾问 — AWS Identity and Access Management (IAM) 访问顾问工具允许您通过分析 IAM 实体（例如用户、角色或群组）调用 AWS 服务的上次时间戳来确定开发人员拥有的权限。您可以审核服务访问权限并删除不必要的权限，还可以根据需要自动执行该过程。有关更多信息，请参阅我们的 AWS 安全博客文章。

- IAM 策略模拟器 — 使用 IAM 策略模拟器，您可以测试基于 IAM 和基于资源的策略并对其进行故障排除。有关更多信息，请参阅使用 IAM 策略模拟器测试 IAM 策略。
- AWS CloudTrail 日志 — 您可以查看 AWS CloudTrail 日志，以查看用户、角色或所采取的操作 AWS 服务。有关的更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

  AWS Control Tower 着陆区管理员采取的操作可在着陆区管理账户中查看。成员账户管理员和用户采取的操作可在共享日志存档账户中查看。

  您可以在活动页面中查看 AWS Control Tower 事件的摘要表。

解释预防性控制

预防性控制可确保贵组织的帐户符合您的公司政策。预防性控制的状态要么是强制执行，要么是未启用。预防性控制通过使用服务控制策略 (SCP) 来防止策略违规。相比之下，侦探控制通过定义的 AWS Config 规则将存在的各种事件或状态通知您。

您的某些用户（例如 AWS 开发人员）可能需要了解适用于他们使用的任何账户和 OU 的预防性控制措施，这样他们才能创建工程解决方案。以下过程提供有关如何根据组织的信息管理策略为正确的用户提供此信息的一些指导。

> **Note**
>
> 此过程假设您已经在 landing zone 中创建了至少一个子 OU 以及至少一个 AWS IAM Identity Center 用户。

向需要了解的用户展示预防性控制措施

1. 登录 AWS Control Tower 控制台，网址为 https://console.aws.amazon.com/controltower/。
2. 从左侧导航栏中选择 “组织”。
3. 从表中，选择您的用户需要有关适用控件信息的 OU 的名称。
4. 记下 OU 的名称和适用于此 OU 的控件。
5. 对用户需要相关信息的每个 OU 重复上述两个步骤。

有关控件及其功能的详细信息，请参阅关于 AWS Control Tower 中的控件。

规划你的 AWS Control Tower 着陆区

当您完成设置过程时，AWS Control Tower 会启动一个与您的账户关联的密钥资源，称为着陆区，它可以作为您的组织及其账户的主场。

> **Note**
>
> 每个组织可以有一个登录区。

有关在规划和设置着陆区时应遵循的一些最佳做法的信息，请参阅AWS AWS Control Tower 着陆区的多账户策略。

设置 AWS Control Tower 的方法

您可以在现有组织中设置 AWS Control Tower 着陆区，也可以先创建一个包含您的 AWS Control Tower 着陆区的新组织。

- 在现有组织中启动 AWS Control Tower：本部分适用于已 AWS Organizations 准备好接受 AWS Control Tower 管理的客户。
- 在新组织中启动 AWS Control Tower：本部分适用于没有现 AWS Organizations有 OU 和账户的客户。

> **Note**
>
> 如果您已经有 AWS Organizations 着陆区，则可以将 AWS Control Tower 管理范围从现有着陆区扩展到组织中的部分或全部现有 OU 和账户。请参阅管理现有组织和账户。

比较功能

以下是将 AWS Control Tower 添加到现有组织或将 AWS Control Tower 管理扩展到 OU 和账户之间的区别的简要比较。此外，如果您要从 AWS 着陆区解决方案迁移到 AWS Control Tower，则需要考虑一些特殊注意事项。

关于添加到现有组织：您可以在控制 AWS 台中完成将 AWS Control Tower 添加到现有组织中的操作。在本例中，您已经在 AWS Organizations 服务中创建了一个组织，该组织目前尚未在 AWS Control Tower 上注册，您想在之后添加一个着陆区。

当您向现有组织添加着陆区时，AWS Control Tower 会在该 AWS Organizations 级别上设置一个并行结构。它不会更改您现有组织内的 OU 和帐户。

关于扩展治理：扩展治理适用于已在 AWS Control Tower 注册的单个组织中的特定 OU 和账户，这意味着该组织已经存在着陆区。扩展监管意味着扩展 AWS Control Tower 的控制范围，使其限制适用于该注册组织内的特定 OU 和账户。在这种情况下，你不是在启动新的着陆区，而只是在为你的组织扩展当前的着陆区。

> **Important**
>
> 特别注意事项：如果您目前正在使用AWS 着陆区解决方案 (ALZ) AWS Organizations，请在尝试在组织中启用 AWS Control Tower 之前，请咨询您的 AWS 解决方案架构师。AWS Control Tower 无法进行预检查来确定 AWS Control Tower 是否会干扰您当前的着陆区部署。有关更多信息，请参阅演练：从 ALZ 移动到 AWS Control Tower。另外，有关将账户从一个着陆区转移到另一个着陆区的信息，请参阅 如果账户不符合先决条件怎么办？

在现有组织中启动 AWS Control Tower

通过在现有组织中设置 AWS Control Tower 着陆区，您可以立即开始与现有 AWS Organizations 环境并行工作。您在其中创建的其他 OU 保持不变，因为它们未在 AWS Organizations AWS Control Tower 中注册。您可以继续完全按原样使用这些 OU 和账户。

AWS Control Tower 使用您现有组织的管理账户作为其管理账户进行整合。无需新的管理账户。您可以从现有管理账户启动您的 AWS Control Tower 着陆区。

> **Note**
>
> 要在现有组织上设置 AWS Control Tower，您的服务限制必须允许创建至少两个额外账户。

将 AWS Control Tower 添加到现有组织中的影响

AWS Control Tower 在您的组织中创建了两个账户：一个审计账户和一个日志账户。这些账户将你的团队采取的行动记录在他们的个人终端用户账户中。审计和日志存档账户显示在您的 AWS Control Tower 着陆区域内的安全 OU 中。

当您设置着陆区时，AWS Control Tower 添加的账户将成为您现有账户的一部分 AWS Organizations，因此它们将成为您现有组织账单的一部分。

能力摘要

在现有 AWS Organizations 组织中启用 AWS Control Tower 可以为该组织提供多项重大增强。

- 它允许您组织的各个组统一计费，因为 AWS Control Tower 添加的账户将成为您现有组织的一部分。
- 它使您能够通过组织单位中的一个管理账户管理所有账户。
- 它简化了您应用和实施控制措施的方式，这些控制措施涵盖现有账户和新账户的安全性和合规性。

> **Important**
>
> 在现有 AWS Organizations 组织中启动 AWS Control Tower 着陆区并不能将该组织的 AWS Control Tower 管理扩展到其他未在 AWS Control Tower 注册的 OU 或账户。

要在您的现有组织中启动 AWS Control Tower，请按照中概述的流程进行操作AWS Control Tower 入门。

有关 AWS Control Tower 如何与现有 AWS Organizations 组织交互的更多信息，请参阅使用 AWS Control Tower 管理组织和账户。

在新组织中启动 AWS Control Tower

如果您是 AWS Control Tower 的新手并且还没有使用过 AWS Organizations，那么最好从我们的设置文档开始。

当你没有设置组织时，AWS Control Tower 会自动为你设置一个组织。

AWS AWS Control Tower 着陆区的多账户策略

AWS Control Tower 客户经常寻求有关如何设置 AWS 环境和账户以获得最佳效果的指导。AWS 创建了一组统一的建议，称为多账户策略，以帮助您充分利用自己的 AWS 资源，包括 AWS Control Tower 着陆区。

从本质上讲，AWS Control Tower 充当与其他 AWS 服务配合使用的编排层，这些服务可帮助您实施针对 AWS 账户和的多 AWS 账户建议。 AWS Organizations在您的着陆区设置完毕后，AWS Control Tower 将继续协助您在多个账户和工作负载中维护您的公司策略和安全实践。

大多数着陆区会随着时间的推移而发展。随着 AWS Control Tower 着陆区中组织单位 (OU) 和账户数量的增加，您可以通过有助于有效组织工作负载的方式扩展 AWS Control Tower 的部署。本章提供规范性指导，说明如何根据 AWS 多账户策略规划和设置您的 AWS Control Tower 着陆区，并随着时间的推移对其进行扩展。

有关组织单位最佳做法的一般性讨论，请参阅组织单位的最佳实践 AWS Organizations。

AWS 多账户策略：最佳实践指南

AWS 架构良好的环境的最佳实践建议您将资源和工作负载分成多个 AWS 账户。您可以将 AWS 账户视为独立的资源容器：它们提供工作负载分类，并在出现问题时缩小爆炸半径。

AWS 账户的定义

AWS 账户充当资源容器和资源隔离边界。

> **Note**
>
> AWS 账户与通过联邦或 AWS Identity and Access Management (IAM) 设置的用户账户不同。

关于 AWS 账户的更多信息

AWS 账户可以隔离资源并遏制 AWS 工作负载面临的安全威胁。账户还提供了一种计费和工作负载环境管理机制。

该 AWS 账户是为您的工作负载提供资源容器的主要实现机制。如果您的环境架构良好，则可以有效地管理多个 AWS 帐户，从而管理多个工作负载和环境。

AWS Control Tower 设置了一个架构良好的环境。它依赖于 AWS 账户以及账户 AWS Organizations，这些账户可以帮助管理可能跨多个账户的环境更改。

架构良好的环境的定义

AWS 将架构良好的环境定义为以 landing zone 开头的环境。

AWS Control Tower 提供了一个自动设置的着陆区。它会对环境中的多个账户实施控制措施，以确保遵守您的公司指导方针。

着陆区的定义

landing zone 是一个云环境，它提供了一个推荐的起点，包括默认账户、账户结构、网络和安全布局等。在 landing zone 中，您可以部署利用您的解决方案和应用程序的工作负载。

建立架构良好的环境的指导方针

以下各节将介绍架构良好的环境的三个关键组成部分是：

- 多个 AWS 账户
- 多个组织单位 (OU)
- 精心策划的结构

使用多个 AWS 账户

一个账户不足以搭建一个架构良好的环境。通过使用多个帐户，您可以最好地支持您的安全目标和业务流程。以下是使用多账户方法的一些好处：

- 安全控制-应用程序具有不同的安全配置文件，因此它们需要不同的控制策略和机制。例如，与审计师交谈并指向托管支付卡行业 (PCI) 工作负载的单一账户要容易得多。
- 隔离：账户是安全保护的单位。可以在不影响其他人的情况下将潜在的风险和安全威胁控制在一个账户中。因此，出于安全考虑，您可能需要将账户彼此隔离开来。例如，您的团队可能具有不同的安全配置文件。
- 许多团队 — 团队有不同的职责和资源需求。通过设置多个帐户，团队不会像使用同一个帐户时那样互相干扰。
- 数据隔离-将数据存储隔离到一个帐户有助于限制有权访问数据并可以管理数据存储的人数。这种隔离有助于防止未经授权泄露高度私密的数据。例如，数据隔离有助于支持对《通用数据保护条例》(GDPR) 的遵守。
- 业务流程 — 业务部门或产品通常具有完全不同的目的和流程。可以建立个人账户来满足企业的特定需求。
- 账单 — 账户是在账单级别分开项目的唯一途径，包括转账费用等。多账户策略有助于跨业务部门、职能团队或个人用户创建单独的可计费项目。
- 配额分配 — AWS 配额是按账户设置的。将工作负载分成不同的账户可以为每个账户（例如项目）提供明确的个人配额。

使用多个组织单位

AWS Control Tower 和其他账户编排框架可以进行跨账户界限的更改。因此， AWS 最佳实践涉及跨账户变更，这可能会破坏环境或破坏其安全性。在某些情况下，变更可能影响整体环境，而不仅仅是政策。因此，我们建议您至少设置两个必备账户，即制作和暂存账户。

此外，出于管理和控制的目的， AWS 账户通常被分组为组织单位 (OU)。OU 旨在跨多个账户执行策略。

我们的建议是，您至少要创建一个不同于生产环境的预生产（或暂存）环境，并具有不同的控制和策略。生产和暂存环境可以作为单独的 OU 创建和管理，并按单独的账户计费。此外，您可能还需要设置沙盒 OU 来进行代码测试。

在 landing zone 中为 OU 使用精心策划的结构

AWS Control Tower 会自动为您设置一些 OU。随着您的工作负载和需求随着时间的推移而扩大，您可以扩展原始的 landing zone 配置以满足您的需求。

> **Note**
>
> 示例中给出的名称遵循设置多账户 AWS 环境的建议 AWS 命名约定。在设置了着陆区后，您可以通过在 OU 详情页面上选择 “编辑” 来重命名 OU。

建议

在 AWS Control Tower 为您设置了第一个必需的 OU（安全 OU）之后，我们建议在您的着陆区再创建一些组织单元。

我们建议您允许 AWS Control Tower 再创建至少一个名为沙盒组织单元。此 OU 适用于您的软件开发环境。如果您选择沙盒组织单元，AWS Control Tower 可以在创建着陆区期间为您设置沙盒 OU。

您可以自己设置另外两个推荐的 OU：基础架构 OU，用于包含您的共享服务和网络帐户，以及一个用于包含生产工作负载的 OU，称为工作负载 OU。您可以通过组织单位页面上的 AWS Control Tower 控制台在着陆区域中添加其他 OU。

除了自动设置的 OU 之外，推荐的 OU

- 基础架构 OU — 包含您的共享服务和网络帐户。

  > **Note**
  >
  > AWS Control Tower 不会为您设置基础设施 OU。

- Sandbox OU — 软件开发 OU。例如，它可能有固定的支出限额，或者可能未连接到生产网络。

> **Note**
>
> AWS Control Tower 建议您设置沙盒 OU，但它是可选的。它可以在配置 landing zone 时自动设置。

- 工作负载 OU-包含运行您的工作负载的帐户。

> **Note**
>
> AWS Control Tower 不会为您设置工作负载组织单位。

有关更多信息，请参阅 AWS Control Tower 的生产入门组织。

具有完整多账户 OU 结构的 AWS Control Tower 示例

AWS Control Tower 支持嵌套的 OU 层次结构，这意味着您可以创建满足组织要求的分层 OU 结构。您可以根据 AWS 多账户策略指南构建一个 AWS Control Tower 环境。

您还可以构建一个更简单、更扁平的 OU 结构，该结构性能良好，并且符合 AWS 多账户指南。仅仅因为您可以构建分层 OU 结构，并不意味着必须这样做。

- 要查看带有 AWS 多账户指导的扩展扁平化 AWS Control Tower 环境中显示一组 OU 示例的示意图，请参阅示例：扁平 OU 结构中的工作负载。
- 有关 AWS Control Tower 如何使用嵌套 OU 结构的更多信息，请参阅AWS Control Tower 中嵌套的 OU。
- 有关 AWS Control Tower 如何与 AWS 指南保持一致的更多信息，请参阅 AWS 白皮书《使用多个账户组织您的 AWS 环境》。

链接页面上的图表显示已创建了更多基础 OU 和更多 OU。这些 OU 可以满足更大规模部署的额外需求。

在 “基础 OU” 列中，在基本结构中添加了两个 OU：

- Security_Prod OU — 为安全策略提供只读区域以及漏洞安全审计区域。
- 基础设施 OU — 您可能希望将之前建议的基础架构 OU 分成两个 OU，即 Infrastructure_Test（用于预生产基础架构）和 Infrastructure_Prod（用于生产基础架构）。

在 “其他 OU” 区域中，基本结构中又添加了几个 OU。以下是随着环境的发展，建议创建的下一个 OU：

- 工作负载 OU — 以前推荐但可选的工作负载 OU 已分为两个 OU，即 Workloads_Test（用于预生产工作负载）和 Workloads_Prod（用于生产工作负载）。
- PolicyStaging OU — 允许系统管理员在完全应用控制和策略之前对其进行测试。
- 已暂停的 OU — 为可能已被暂时禁用的帐户提供位置。

关于 Root

根不是 OU。它是管理账户以及组织中所有 OU 和账户的容器。从概念上讲，根包含所有 OU。它无法删除。在 AWS Control Tower 中，您无法在根级别管理已注册的账户。取而代之的是管理 OU 中的已注册账户。有关有用的图表，请参阅 AWS Organizations 文档。

设置着陆区的管理提示

- 你工作最多的 AWS 地区应该是你的家乡地区。
- 设置你的着陆区，然后从你的家乡区域部署你的 Account Factory 账户。
- 如果您在多个 AWS 区域进行投资，请确保您的云资源位于您要完成大部分云管理工作和运行工作负载的区域。
- 通过将工作负载和日志保存在同一个 AWS 区域，可以降低与跨区域移动和检索日志信息相关的成本。
- 审计和其他 Amazon S3 存储桶是在您启动 AWS Control Tower 的同一 AWS 区域创建的。我们建议您不要移动这些存储桶。
- 您可以在日志存档账户中创建自己的日志存储桶，但不建议这样做。请务必保留 AWS Control Tower 创建的存储桶。
- 您的 Amazon S3 访问日志必须与源存储桶位于同一 AWS 区域。
- 启动时，必须在 AWS Control Tower 支持的所有区域的管理账户中激活 AWS 安全令牌服务 (STS) 终端节点。否则，启动可能会在配置过程中半途而废。
- AWS Control Tower 仅支持为已启用的控件添加标签。有关更多信息，请参阅 AWS Control Tower 支持为已启用的控件添加标签。
- 我们建议为 AWS Control Tower 管理的每个账户启用多重身份验证 (MFA)。

关于 VPC 的注意事项

- AWS Control Tower 创建的 VPC 仅限于可用 AWS 控制塔的范围。 AWS 区域 一些在不支持的区域运行工作负载的客户可能希望禁用使用您的 Account Factory 账户创建的 VPC。他们可能更喜欢使用 Service Catalog 产品组合创建新 VPC，或者创建仅在所需区域运行的自定义 VPC。
- AWS Control Tower 创建的 VPC 与为所有人创建的默认 VPC 不同 AWS 账户。在支持 AWS Control Tower 的区域，AWS Control Tower 在创建 AWS Control Tower VPC 时会删除默认 VPC。
- 如果您删除自己所在 AWS 区域的默认 VPC，则最好在所有其他 AWS 区域将其删除。

设置群组、角色和策略的建议

在设置登录区时，最好提前确定哪些用户需要访问特定账户，以及其中的原因。例如，安全帐户应仅供安全团队访问，管理帐户应仅可供云管理员团队访问，依此类推。

有关此主题的更多信息，请参阅AWS Control Tower 中的身份和访问管理。

建议的限制

您可以通过设置仅允许管理员管理 AWS Control Tower 操作的 IAM 角色或策略来限制对组织的管理访问范围。推荐的方法是使用 IAM 策略`arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`。启用该`AWSControlTowerServiceRolePolicy`角色后，管理员只能管理 AWS Control Tower。请务必在每个账户中包含适当的访问权限， AWS Organizations 用于管理您的预防控制和 SCP AWS Config，以及用于管理侦探控制的访问权限。

当您在登录区中设置共享审计账户时，我们建议您将 `AWSSecurityAuditors` 组分配给您账户中的所有第三方审计人员。此组授予其成员只读权限。账户不得对其审计的环境具有写入权限，因为这可能不符合针对审计人员提出的责任分离要求。

您可以在角色信任策略中施加条件，以限制与 AWS Control Tower 中某些角色交互的账户和资源。我们强烈建议您限制对该`AWSControlTowerAdmin`角色的访问权限，因为它允许广泛的访问权限。有关更多信息，请参阅角色信任关系的可选条件。

创建和修改 AWS Control Tower 资源的指南

我们建议您在在 AWS Control Tower 中创建和修改资源时采用以下最佳实践。在更新服务时，本指南可能会发生变化。请记住，责任共担模式适用于您的 AWS Control Tower 环境。

一般指南

- 请勿修改或删除 AWS Control Tower 创建的任何资源，包括管理账户、共享账户和成员账户中的资源。如果您修改这些资源，则可能需要更新 landing zone 或重新注册 OU，而修改可能会导致合规报告不准确。

  特别是：

  - 保持活跃的 AWS Config 录音机。如果您删除 Config 记录器，则侦探控件将无法检测和报告偏差。由于信息不足，不合规的资源可能会被报告为 “合规”。
  - 请勿修改或删除在安全组织单位 AWS Identity and Access Management (OU) 的共享账户中创建的 (IAM) 角色。修改这些角色可能会要求您更新登录区。
  - 请勿从您的成员账户中删除该`AWSControlTowerExecution`角色，即使在已取消注册的账户中也是如此。如果这样做，您将无法在 AWS Control Tower 中注册这些账户，也无法注册其直系父级 OU。
- 不要禁止 AWS 区域 通过 SCP 或 AWS Security Token Service ()AWS STS使用任何东西。这样做会导致 AWS Control Tower 进入未定义状态。如果您不允许使用区域 AWS STS，则您在这些区域中的功能将失败，因为在这些区域中将无法进行身份验证。取而代之的是，依靠 AWS Control Tower 区域拒绝功能（如控件所示）AWS 区域、“ AWS 根据请求拒绝访问”（适用于着陆区域级别）或应用于 OU 的控制区域拒绝控制（在 OU 级别起作用以限制对区域的访问）。
- 必须应用 AWS Organizations `FullAWSAccess` SCP，不应与其他 SCP 合并。对此 SCP 的更改不会被报告为偏差；但是，如果拒绝访问某些资源，某些更改可能会以不可预测的方式影响 AWS Control Tower 的功能。例如，如果 SCP 被分离或修改，则帐户可能会失去对 AWS Config 录制器的访问权限或在 CloudTrail 日志中造成空白。
- 请勿使用 AWS Organizations `DisableAWSServiceAccess` API 关闭您设置着陆区的组织的 AWS Control Tower 服务访问权限。如果您这样做，如果没有消息支持，某些 AWS Control Tower 漂移检测功能可能无法正常运行 AWS Organizations。这些偏差检测功能有助于确保 AWS Control Tower 能够准确报告贵组织中组织单位、账户和控制的合规状态。有关更多信息，请参阅 AWS Organizations API 参考API_DisableAWSServiceAccess中的。
- 通常，AWS Control Tower 一次只能执行一个操作，必须先完成该操作，然后才能开始另一个操作。例如，如果您在启用控件的过程已在运行时尝试配置帐户，则账户配置将失败。

  例外：

  - AWS Control Tower 允许并行操作部署可选控件。有关更多信息，请参阅并发部署以了解可选控件。
  - AWS Control Tower 允许使用 Account Factory 对账户执行多达十个并发创建、更新或注册操作。

> **Note**
>
> 有关 AWS Control Tower 创建的资源的更多信息，请参阅共享账户有哪些？。

关于账户和 OU 的提示

- 我们建议您将每个注册的 OU 最多保留 300 个账户，这样您就可以在需要更新账户时使用 “重新注册 OU” 功能更新这些账户，例如在配置新的监管区域时。
- 为了缩短注册 OU 所需的时间，我们建议您将每个 OU 的账户数保持在 150 左右，尽管限制为每个 OU 300 个账户。一般而言，注册 OU 所需的时间会根据您的 OU 运营所在区域的数量乘以 OU 中的账户数量而增加。
- 据估计，拥有 150 个账户的 OU 大约需要 2 小时来注册和启用控制，大约需要 1 小时才能重新注册。此外，具有许多控件的 OU 的注册时间比控件较少的 OU 需要更长的时间。
- 允许更长时间注册 OU 的一个问题是，此过程会阻止其他操作。有些客户愿意允许更长的时间注册或重新注册 OU，因为他们更愿意在每个 OU 中允许更多帐户。

何时以 root 用户身份登录

某些管理任务要求您必须以根用户身份登录。您可以以 root 用户身份登录账户工厂在 AWS Control Tower 中创建的。 AWS 账户

您必须以根用户身份登录才能执行以下操作：

- 更改某些账户设置，包括账户名称、根用户密码或电子邮件地址。有关更多信息，请参阅 使用 AWS Control Tower 或使用 AWS Control Tower 更新和移动账户工厂账户 AWS Service Catalog。
- 要关闭 AWS 账户.
- 有关需要根用户登录凭证的操作的更多信息，请参阅《AWS Account Management 参考指南》中需要根用户凭证的任务。

> **Note**
>
> 要更改或启用您的 S AWS upport 计划，您必须以根用户身份登录，或者是具有相应 IAM 权限的用户。 。

以根用户身份登录

1. 打开AWS 登录页面。

   如果您没有需要访问的电子邮件地址，则可以从 AWS Control Tower 获取该地址。 AWS 账户 打开管理账户的控制台，选择账户，然后查找电子邮件地址。

2. 输入您需要访问的电子邮件地址 AWS 账户 ，然后选择 “下一步”。
3. 选择 Forgot password? (忘记密码？)，以将密码重置说明发送到根用户电子邮件地址。
4. 从根用户邮箱中打开密码重置电子邮件，然后按照说明重置密码。
5. 打开AWS 登录页面，然后使用您的重置密码登录。

AWS Organizations 指导

- 您可以在 AWS Organizations 文档中找到有关保护您的 AWS Control Tower 管理账户和成员账户安全的最佳实践指南。
  - 管理账户的最佳实践
  - 成员账户的最佳实践
- 请勿使用 AWS Organizations 更新已在 AWS Control Tower 注册的 OU 所附的服务控制策略 (SCP)。这样做可能会导致控件进入未知状态，这将要求您重置着陆区或在 AWS Control Tower 中重新注册您的 OU。相反，您可以创建新的 SCP 并将其附加到 OU，而不必编辑 AWS Control Tower 创建的 SCP。
- 将已注册的个人账户从注册的 OU 之外移入 AWS Control Tower 会导致必须解决的偏差。请参阅 监管偏差类型。
- 如果您使用 AWS Organizations 在向 AWS Control Tower 注册的组织内创建、邀请或转移账户，则这些账户不会由 AWS Control Tower 注册，也不会记录这些更改。如果您需要通过 SSO 访问这些账户，请参阅成员账户访问权限。
- 如果您使用将组织单位移 AWS Organizations 至由 AWS Control Tower 创建的组织，则外部 OU 不会由 AWS Control Tower 注册。
- AWS Control Tower 处理权限筛选的方式与 AWS Organizations 以前不同。如果您的账户配置了 AWS Control Tower 账户工厂，则最终用户可以在 AWS Control Tower 控制台中看到所有 OU 的名称和父级，即使他们无权直接从 AWS Organizations 中检索这些姓名和父项。
- AWS Control Tower 不支持对组织使用混合权限，例如查看组织单位的父级但不支持查看组织单位名称的权限。因此，AWS Control Tower 管理员需要拥有完全权限。

- 必须应用 AWS Organizations `FullAWSAccess` SCP，不应与其他 SCP 合并。对此 SCP 的更改不会被报告为偏差；但是，如果拒绝访问某些资源，某些更改可能会以不可预测的方式影响 AWS Control Tower 的功能。例如，如果 SCP 被分离或修改，则帐户可能会失去对 AWS Config 录制器的访问权限或在 CloudTrail 日志中造成空白。
- 请勿使用 AWS Organizations `DisableAWSServiceAccess` API 关闭您设置着陆区的组织的 AWS Control Tower 服务访问权限。如果您这样做，如果没有消息支持，某些 AWS Control Tower 漂移检测功能可能无法正常运行 AWS Organizations。这些偏差检测功能有助于确保 AWS Control Tower 能够准确报告贵组织中组织单位、账户和控制的合规状态。有关更多信息，请参阅 AWS Organizations API 参考API_DisableAWSServiceAccess中的。

IAM 身份中心指南

> **Note**
>
> SSO 是技术行业中用来表示单点登录的缩写。一般而言，SSO 是一种会话和用户身份验证服务。它允许某人使用一组登录凭据访问多个应用程序。在提及中的单点登录功能时 AWS，我们指的是名为、缩写为 AWS Identity and Access ManagementIAM 或 IAM 身份中心的 AWS 服务。

AWS Control Tower 建议您使用 AWS Identity and Access Management (IAM) 来监管对您的访问权限 AWS 账户。但是，您可以选择 AWS Control Tower 是否为您设置 IAM 身份中心，是否以最有效地满足您的业务需求的方式为自己设置 IAM 身份中心，或者是否选择其他账户访问方法。

默认情况下，AWS Control Tower 会根据使用多个账户组织 AWS 环境中定义的最佳实践指南，为您的着陆区设置 AWS IAM 身份中心。大多数客户选择默认值。有时需要其他访问方法，以满足特定行业或国家/地区的监管要求，或者在无法使用 AWS IAM Identity Center AWS 区域 的地方。

选择一个选项

在控制台中，您可以选择在着陆区设置过程中自行管理 IAM 身份中心，而不必允许 AWS Control Tower 为您设置。以后，您可以随时选择更改此选择，方法是修改着陆区设置并在 “着陆区设置” 页面上更新您的着陆区。

停用 AWS Control Tower 中的 IA AWS M 身份中心，或者开始使用 AWS IAM 身份中心

1. 导航至 landing zone 设置页面
2. 选择 “配置” 选项卡

3. 然后选择相应的单选按钮，更改您 AWS 对 IAM 身份中心的选择。

在您选择以身份提供商的身份自行管理 AWS IAM 身份中心后，AWS Control Tower 将仅创建管理 AWS Control Tower 所需的角色和策略，例如`AWSControlTowerAdmin`和。`AWSControlTowerAdminPolicy`对于自行管理的着陆区，AWS Control Tower 不再为客户特定用途创建 IAM 角色和分组，不在着陆区设置过程中，也不会在使用 Account Factory 配置账户期间。

> **Note**
>
> 如果您从 AWS Control Tower 着陆区移除 AWS IAM 身份中心，则不会删除 AWS Control Tower 创建的用户、群组和权限集。我们建议您移除这些资源。

拥有替代身份提供商 (IdPs)（例如 Azure AD、Ping 或 Okta）的 Account Factory 客户可以按照 AWS IAM 身份中心流程连接到外部身份提供商并加入他们的 IdP。通过修改着陆区设置，您可以随时恢复让 AWS Control Tower 生成您的分组和角色。

- 有关 AWS Control Tower 如何根据您的身份来源与 IAM Identity Center 配合使用的具体信息，请参阅本用户指南入门页面的启动前检查部分中的 AWS IAM Identity Center 客户注意事项。
- 有关 AWS Control Tower 行为如何与 IAM 身份中心和不同身份源交互的更多信息，请参阅 IAM 身份中心用户指南中的更改身份源的注意事项。
- 与 AWS IAM 身份中心和 AWS Control Tower 合作有关使用 AWS Control Tower 和 IAM 身份中心的更多信息，请参阅。

Account Factory 指南

使用 Account Factory 在 AWS Control Tower 中配置新账户时，您可能会遇到问题。有关如何解决这些问题的信息，请参阅 AWS Control Tower 用户指南疑难解答新账户预置失败中的部分。

我们建议您创建联合用户或 IAM 角色而不是 IAM 用户。联合用户和 IAM 角色为您提供临时证书。IAM 用户拥有长期证书，可能难以管理。有关更多信息，请参阅 IAM 用户指南中的 IAM 身份（用户、用户组和角色）。

如果您在 Account Factory 中配置新账户或使用 AWS Control Tower 注册账户功能时以 IAM 用户或 IAM 身份中心用户身份进行了身份验证，请验证您的用户是否有权访问您的 AWS Service Catalog 投

资组合。否则，您可能会收到来自 Service Catalog 的错误消息。有关更多信息，请参阅 AWS C 未找到启动路径错误 ontrol Tower 用户指南的 “疑难解答” 部分。

> **Note**
>
> 一次最多可以配置五个账户。

关于订阅 SNS 主题的指南

- `aws-controltower-AllConfigNotifications`SNS 主题接收发布的所有事件 AWS Config，包括合规性通知和 Amazon CloudWatch 事件通知。例如，如果发生了控制违规，本主题会通知您。它还提供有关其他类型事件的信息。（从AWS Config配置此主题时他们发布的内容中了解更多信息。）
- 来自`aws-controltower-BaselineCloudTrail`跟踪@@ 的数据事件也设置为发布到 `aws-controltower-AllConfigNotifications` SNS 主题。
- 要接收详细的合规通知，我们建议您订阅 `aws-controltower-AllConfigNotifications` SNS 主题。本主题汇总了来自所有子女账户的合规性通知。
- 要接收漂移通知和其他通知以及合规性通知，但总体上减少通知，我们建议您订阅 `aws-controltower-AggregateSecurityNotifications` SNS 主题。
- 要接收有关 AWS Control Tower Account Factory for Terraform (AFT) 错误的通知，您可以订阅 AFT 存储库中显示的名aft_failure_notifications为的 SNS 主题。例如：

```
resource "aws_sns_topic" "aft_failure_notifications" {
    name = "aft-failure-notifications"
    kms_master_key_id = "alias/aws/sns"
}
```

- 所有 SNS 主题均使用磁盘加密进行静态加密。有关更多信息，请参阅数据加密。

有关 SNS 主题和合规性的更多信息，请参阅预防和通知。

KMS 密钥指南

AWS Control Tower 可与 AWS Key Management Service (AWS KMS) 配合使用。或者，如果您希望使用自己管理的加密密钥来加密和解密您的 AWS Control Tower 资源，则可以生成和配置。 AWS

KMS keys您可以在任何时候更新着陆区时添加或更改 KMS 密钥。作为最佳实践，我们建议您使用自己的 KMS 密钥并不时对其进行更改。

AWS KMS 允许您创建多区域 KMS 密钥和非对称密钥。但是，AWS Control Tower 不支持多区域密钥或非对称密钥。AWS Control Tower 会对您的现有密钥进行预检查。如果您选择多区域密钥或非对称密钥，则可能会看到一条错误消息。在这种情况下，请生成另一个密钥以用于 AWS Control Tower 资源。

对于运营 AWS CloudHSM 集群的客户：创建与您的 CloudHSM 集群关联的自定义密钥存储库。然后，您可以创建 KMS 密钥，该密钥位于您创建的 CloudHSM 自定义密钥存储中。您可以将此 KMS 密钥添加到 AWS Control Tower。

您必须对 KMS 密钥的权限策略进行具体更新才能使其与 AWS Control Tower 配合使用。有关详细信息，请参阅名为的部分更新 KMS 密钥策略。

基于人工智能的服务和 AWS Control Tower

您可以创建服务控制策略 (SCP)，允许您选择不让基于 AI 的服务存储您的数据。 AWS这些SCP政策规定，基于人工智能的服务，例如Amazon Rekognition或Amazon，不能存储和使用您的CodeWhisperer数据来改进其他基于人工智能的服务。 AWS

这些 AI 选择退出 SCP 政策可以适用于您的整个组织、组织单位或特定账户。这些政策是全球性的。您可以在文档中的 AI 服务选择退出政策中找到有关这些政策的 AWS Organizations 更多信息。

有关使用 AI 的 AWS 服务列表以及策略示例，请参阅《AWS Organizations 用户指南》中的 AI 服务选择退出策略语法和示例。

AWS Control Tower 中的配置更新管理

您的中央云管理员团队的成员有责任随时更新您的 landing zone。更新您的着陆区可确保 AWS Control Tower 得到修补和更新。此外，为了保护您的 landing zone 免受潜在的合规性问题的影响，中央云管理员团队的成员应在发现并报告漂移问题后立即解决这些问题。

> **Note**
>
> AWS Control Tower 控制台会显示何时需要更新您的着陆区。如果您看不到更新选项，则说明您的着陆区已经是最新的。

下表包含 AWS Control Tower 着陆区更新版本列表，以及每个版本说明的链接。

版本	发行日期	描述
3.3	12-12-2023	着陆区版本 3.3
3.2	6-09-2023	着陆区版本 3.2
3.1	2-09-2023	着陆区版本 3.1
3.0	7-26-2022	着陆区版本 3.0
2.9	4-22-2022	着陆区版本 2.9
2.8	2-10-2022	着陆区版本 2.8
2.7	4-8-2021	着陆区版本 2.7
2.6	12-29-2020	着陆区版本 2.6
2.5	11-18-2020	着陆区版本 2.5
2.4	无	无
2.3	3-5-2020	着陆区版本 2.3
2.2	11-13-19	着陆区版本 2.2

版本	发行日期	描述
2.1	6-24-19	着陆区版本 2.1

每次更新着陆区时，您都有机会修改着陆区设置。

更新的好处

- 您可以更改您的管辖区域
- 您可以更改日志保留政策
- 您可以添加或移除 “区域拒绝” 控件
- 您可以应用 AWS KMS 加密密钥
- 您可以激活或停用组织级别 CloudTrail 的跟踪。
- 你可以解决着陆区漂移问题

当你更新着陆区时，你会自动收到 AWS Control Tower 的最新功能。在着陆区设置页面上查看您当前的着陆区域版本。

如果更新失败，AWS Control Tower 不会回滚到之前的着陆区版本。你可能会发现你的着陆区处于不确定状态。如果是，请联系 AWS 支持人员。有关解决更新失败的更多信息，请参阅无法更新着陆区。

更新着陆区时，您有机会清除未使用的 AWS 身份中心（以前称为 AWS SSO）映射。有关更多信息，请参阅现场说明：在 AWS Control Tower 升级期间自动清除未使用的 IAM 身份中心映射。

> 更新和重置的先决条件-关闭申请人付款
>
> 在更新或重置着陆区之前，请确保日志存档账户的 Amazon S3 日志存储桶未启用 “申请者付款” 功能。在开始更新或重置过程之前，必须关闭该功能。当 AWS Control Tower 设置您的日志存储桶时，此功能不会启用。因此，只有随后激活 “申请者付款” 功能的客户才必须将其关闭。有关更多信息，请参阅适用于 CloudTrail和使用申请方付款存储桶的 Amazon S3 存储桶政策。

关于更新

需要更新才能纠正治理偏差，或者迁移到新版本的 AWS Control Tower。要全面更新 AWS Control Tower，您必须先更新您的着陆区，然后单独更新已注册的账户。您可能需要在不同的时间执行三种类型的更新。

- 着陆区更新：大多数情况下，此类更新是通过在着陆区设置页面上选择更新来执行的。您可能需要执行 landing zone 更新来解决某些类型的漂移，并且可以在必要时选择 “重置”。
- 一个或多个单独账户的更新：如果关联的信息发生了变化，或者发生了某些类型的偏差，则必须更新账户。如果账户需要更新，则该账户的状态将在账户页面上显示更新可用。

  要更新单个账户，请导航至账户详情页面，然后选择更新账户。也可以通过手动流程、选择 “重新注册 OU” 或使用自动脚本方法更新账户，如本页后面部分所述。
- 完全更新：完全更新包括您的登录区更新，后跟对已注册 OU 中所有已注册账户的更新。新版本的 AWS Control Tower（例如 2.9、3.0 等）需要进行全面更新。

> **Note**
>
> 完成 landing zone 更新后，您将无法撤消更新或降级到先前版本。

更新您的登录区

更新 AWS Control Tower 着陆区的最简单方法是通过着陆区设置页面，您可以通过在 AWS Control Tower 控制面板的左侧导航栏中选择着陆区设置来访问该页面。

着陆区设置页面显示着陆区的当前版本，并列出了所有可能可用的更新版本。如果您需要更新您的版本，可以选择 Update (更新) 按钮。

> **Note**
>
> 或者，您也可以手动更新您的登录区。无论您使用 Update (更新) 按钮还是手动过程，更新大致需要相同的时间。要仅手动更新登录区，请参阅后面的步骤 1 和 2。

手动更新

以下过程将引导您手动完成 AWS Control Tower 全面更新的步骤。要更新个人账户，请参阅在控制台中更新账户。

手动更新您的 landing zone，每个 OU 拥有任意数量的账户

1. 打开网络浏览器，然后导航到 AWS Control Tower 控制台，网址为 https://console.aws.amazon.com/controltower/home/update。
2. 检查向导中的信息，并选择 Update (更新)。这将更新 landing zone 的后端以及您的共享帐户。此过程可能需要半个多小时的时间。
3. 更新您的成员账户（对于包含超过 300 个账户的 OU，必须遵循此程序）。
4. 从左侧导航窗格中选择 “组织”。
5. 要更新每个账户，请按照中给出的步骤操作在控制台中更新账户。

> （可选）重新注册 OU 以更新账户
>
> 对于账户少于 300 的已注册 AWS Control Tower OU，您可以前往控制面板中的 OU 页面，然后选择重新注册 OU 以更新该 OU 中的账户。

使用 “重置和重新注册” 解决漂移问题

当你和你的组织成员使用着陆区时，经常会发生漂移。

在 AWS Control Tower 中，漂移检测是自动进行的。自动扫描 SCP 可帮助您识别需要更改或配置更新的资源，这些资源必须进行更改或配置更新才能解决偏差。

要修复大多数类型的漂移，请在着陆区域设置页面上选择重置。此外，您可以通过选择重新注册 OU 来解决某些类型的偏差。有关漂移类型及其解决方法的更多信息，请参阅监管偏差类型和在 AWS Control Tower 中检测并解决偏差。

漂移分辨率的一种特殊情况发生在角色漂移上。如果所需角色不可用，控制台会显示警告页面和一些有关如何恢复该角色的说明。在解决角色偏差问题之前，您的着陆区域不可用。此漂移重置与完全着陆区重置不同。有关更多信息，请参阅名为 “不要删除必需的角色” 一节中的需要立即解决的漂移类型。

⚠ 当你采取措施解决 landing zone 版本上的漂移问题时，可能有两种行为。

- 如果您使用的是最新的着陆区版本，则当您选择 “重置” 然后选择 “确认” 时，您的漂移着陆区资源将重置为保存的 AWS Control Tower 配置。landing zone 版本保持不变。
- 如果您使用的不是最新版本，则必须选择 “更新”。着陆区已升级到最新的着陆区版本。漂移问题已作为此过程的一部分得到解决。

使用自动化配置和更新账户

您可以通过多种方法在 AWS Control Tower 中配置或更新个人账户：

- 您可以使用 AWS Control Tower Account Factory for Terraform (AFT) 配置和自定义账户。有关更多信息，请参阅 适用于 Terraform 的 AWS Control Tower Account Factory (AFT) 概述。
- 您可以使用 AWS Control Tower (cfcT) 的自定义项来更新账户。有关更多信息，请参阅 AWS Control Tower (cfcT) 的自定义项概述 。
- 脚本自动化：如果您更喜欢使用 API 方法，则可以使用 Service Catalog 的 API 框架更新账户，并在批处理过程中更新账户。 AWS CLI 你可以为每个账户调用 Service Catalog 的 `UpdateProvisionedProduct`API。您可以使用此 API 编写脚本以逐个更新账户。在添加区域进行治理时，有关此方法的更多信息，请参阅博客文章《在新 AWS 区域中启用护栏》。

  您一次最多可以更新五 (5) 个帐户。您必须等待至少一个账户更新成功后才能开始下一次账户更新。因此，如果您有很多账户，这个过程可能需要很长时间，但并不复杂。有关此方法的更多信息，请参阅演练：通过 Service Catalog API 在 AWS Control Tower 中自动配置账户。

ⓘ 视频演练

专视频演练为使用脚本自动配置账户而设计，但这些步骤也适用于账户更新。使用 `UpdateProvisionedProduct` API 代替 `ProvisionProduct` API。

通过脚本实现自动化的另一个步骤是检查 AWS Control Tower `UpdateLandingZone` 生命周期事件的成功状态。将其用作触发器，开始更新个人账户，如视频中所述。生命周期事件标志着一系列活动的完成，因此该事件的发生意味着着陆区域更新已完成。登录区更新必须在账户更新开始之前完成。有关处理生命周期事件的更多信息，请参阅生命周期事件。

另请参阅：

- 使用 AWS CloudShell 来使用 AWS Control Tower.
- 在 AWS Control Tower 中自动执行任务 .

在 AWS Control Tower 中自动执行任务

许多客户更喜欢在 AWS Control Tower 中自动执行任务，例如账户配置、控制分配和审计。您可以通过调用以下电话来设置这些自动操作：

- AWS Service Catalog API
- AWS Organizations API
- AWS Control Tower API
- C AWS LI

该相关信息页面包含许多优秀的技术博客文章的链接，这些文章可以帮助您在 AWS Control Tower 中自动执行任务。以下各节提供了指向本 AWS Control Tower 用户指南中可帮助您自动执行任务的区域的链接。

自动执行控制任务

您可以通过 AWS Control Tower API 自动执行与应用和移除控件（也称为护栏）相关的任务。有关详细信息，请参阅 AWS Control Tower API 参考。

有关如何使用 AWS Control Tower API 执行控制操作的更多信息，请参阅博客文章 AWS Control Tower 发布 API，这是针对您的组织单位的预定义控件。

自动执行着陆区任务

AWS Control Tower 着陆区 API 可帮助您自动执行与着陆区相关的某些任务。有关详细信息，请参阅 AWS Control Tower API 参考。

自动化 OU 注册

AWS Control Tower 基准 API 可帮助您自动执行某些任务，例如注册 OU。有关详细信息，请参阅 AWS Control Tower API 参考。

自动关闭账户

您可以使用 AWS Organizations API 自动关闭 AWS Control Tower 成员账户。有关更多信息，请参阅通过关闭 AWS Control Tower 成员账户 AWS Organizations。

自动配置和更新账户

AWS Control Tower 账户工厂定制 (AFC) 可帮助您通过 AWS Control Tower 控制台创建账户，并使用我们称之为蓝图的自定义 AWS CloudFormation 模板。从某种意义上说，此过程是自动化的，因为您可以在设置单个蓝图后重复创建新帐户和更新帐户，而无需维护管道。

适用于 Terraform 的 AWS Control Tower Account Factor y (AFT) 遵循一种 GitOps 模型，在 AWS Control Tower 中自动执行账户配置和账户更新流程。有关更多信息，请参阅 使用适用于 Terraform 的 AWS Control Tower Account Factory（AFT）配置账户 。

AWS Control Tower (cfcT) 的自定义可帮助您自定义 AWS Control Tower 着陆区，并与 AWS 最佳实践保持一致。使用 AWS CloudFormation 模板和服务控制策略 (SCP) 实现自定义。有关更多信息，请参阅 AWS Control Tower (cfcT) 的自定义项概述 。

有关自动账户配置的更多信息和视频，请参阅演练：AWS Control Tower 中的自动账户配置和使用 IAM 角色自动配置账户。

另请参阅通过脚本更新账户。

账户的程序化审计

有关以编程方式审计账户的更多信息，请参阅 AWS Control Tower 审计账户的编程角色和信任关系。

自动执行其他任务

有关如何使用自动请求方法增加某些 AWS Control Tower 服务配额的信息，请观看此视频：自动提高服务限制。

有关涵盖自动化和集成用例的技术博客，请参阅自动化和集成。

有两个开源示例 GitHub 可帮助您完成某些与安全相关的自动化任务。

- 名为 aws-control-tower-org-setup-sample 的示例显示了如何自动将审核帐户设置为安全相关服务的委托管理员。
- 名为 aws-control-tower-account- 的示例setup-using-step-functions显示了在配置和配置新账户时如何使用 Step Functions 自动执行安全最佳实践。此示例包括将委托人添加到组织共享的 AWS Service Catalog 投资组合中，以及将组织范围内的 AWS IAM Identity Center 群组自动关联到新账户。它还说明了如何删除每个区域的默认 VPC。

AWS 安全参考架构包括用于自动执行与 AWS Control Tower 相关的任务的代码示例。有关更多信息，请参阅 “AWS 规范性指南” 页面和相关的 GitHub 存储库。

有关将 AWS Control Tower 与 AWS CloudShell一项便于在 AWS CLI 中工作的 AWS 服务结合使用的信息，请参阅AWS CloudShell 和 AWS CLI。

由于 AWS AWS Control Tower 是的编排层 AWS Organizations，因此通过 API 和 CLI 可以获得许多其他 AWS 服务。有关更多信息，请参阅相关 AWS 服务。

使用 AWS CloudShell 来使用 AWS Control Tower

AWS CloudShell 是一项便于在 AWS CLI 中工作的 AWS 服务 — 它是一个基于浏览器、经过预先验证的 shell，您可以直接从启动。 AWS Management Console无需下载或安装命令行工具。您可以通过首选外壳（Bash PowerShell 或 Z shell）为和其他 AWS 服务运行 AWS CLI 命令。 AWS Control Tower

当您AWS CloudShell 从启动时 AWS Management Console，用于登录控制台的 AWS 凭据将在新的 shell 会话中可用。当你与其他 AWS 服务交互时，你可以跳过输入配置凭证，而你将使用预先安装在外壳程序计算环境中的 AWS CLI 版本 2。你已通过预先身份验证。 AWS Control Tower AWS CloudShell

获取 IAM 权限 AWS CloudShell

AWS Identity and Access Management 提供访问管理资源，允许管理员向 IAM 用户和 IAM Identity Center 用户授予访问权限 AWS CloudShell。

管理员向用户授予访问权限的最快方法是通过 AWS 托管策略。AWS 托管式策略 是由 AWS创建和管理的独立策略。以下的 AWS 托管策略 CloudShell 可以附加到 IAM 身份：

- `AWSCloudShellFullAccess`：授予使用权限，并 AWS CloudShell 具有对所有功能的完全访问权限。

如果您想限制 IAM 用户或 IAM Identity Center 用户可以执行的操作范围 AWS CloudShell，则可以创建使用`AWSCloudShellFullAccess`托管策略作为模板的自定义策略。有关限制中可供用户执行的操作的更多信息 CloudShell，请参阅AWS CloudShell 用户指南中的使用 IAM 策略管理 AWS CloudShell 访问和使用情况。

> **Note**
>
> 您的 IAM 身份还需要一个授予调用权限的策略 AWS Control Tower。有关更多信息，请参阅使用 AWS Control Tower 控制台所需的权限。

与 AWS Control Tower 使用进行交互 AWS CloudShell

AWS CloudShell 从启动后 AWS Management Console，您可以立即开始 AWS Control Tower 从命令行界面与之交互。 AWS CLI 命令在中以标准方式工作 CloudShell。

> **Note**
>
> AWS CLI 在中使用时 AWS CloudShell，您无需下载或安装任何其他资源。您已经在 shell 中进行了身份验证，因此无需在拨打电话之前配置凭据。

启动 AWS CloudShell

- 从中 AWS Management Console，您可以 CloudShell 通过选择导航栏上的以下可用选项来启动：
  - 选择图 CloudShell 标。
  - 开始在搜索框中输入 “cloudshell”，然后选择相应 CloudShell选项。

  现在你已经开始了 CloudShell，你可以输入任何你需要使用的 AWS CLI 命令 AWS Control Tower。例如，您可以检查自己的 AWS Config 状态。

AWS CloudShell 用于帮助设置 AWS Control Tower

在执行这些程序之前，除非另有说明，否则您必须登录到着陆区域的主区域，并且必须以 IAM Identity Center 用户或对包含您的着陆区的管理账户具有管理权限的 IAM 用户身份登录。 AWS Management Console

1. 在开始配置 landing zone 之前，您可以通过以下方式在中 AWS CloudShell 使用 AWS Config CLI 命令来确定配置记录器和传送渠道 AWS Control Tower 的状态。

   查看您的 AWS Config 状态

   查看命令：

   - `aws configservice describe-delivery-channels`
   - `aws configservice describe-delivery-channel-status`
   - `aws configservice describe-configuration-recorders`
   - `The normal response is something like "name": "default"`

2. 如果您有现有的 AWS Config 录音机或传送渠道，需要在设置 landing z AWS Control Tower one 之前将其删除，则可以输入以下命令：

   管理您先前存在 AWS Config 的资源

   删除命令：

   - `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

   > **Important**
   >
   > 请勿删除 AWS Config 的 AWS Control Tower 资源。这些资源的丢失可能导致 AWS Control Tower 进入不一致的状态。

   有关更多信息，请参阅 AWS Config 文档

   - 管理配置记录器 (AWS CLI)
   - 管理传递通道

3. 此示例显示了为启用或禁用可信 AWS CloudShell 访问而输入的 AWS CLI 命令 AWS Organizations。因为 AWS Control Tower 您不需要为启用或禁用可信访问权限 AWS Organizations，这只是一个示例。但是，如果您要在中自动执行或自定义操作，则可能需要启用或禁用其他 AWS 服务的可信访问权限。 AWS Control Tower

   启用或禁用可信服务访问权限

   - `aws organizations enable-aws-service-access`
   - `aws organizations disable-aws-service-access`

使用创建 Amazon S3 存储桶 AWS CloudShell

在以下示例中，您可以使用 AWS CloudShell 创建 Amazon S3 存储桶，然后使用PutObject方法将代码文件作为对象添加到该存储桶中。

1. 要在指定 AWS 区域创建存储桶，请在命令行中输入以下 CloudShell 命令：

```
aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
```

如果调用成功，命令行将显示来自服务的响应，输出与以下类似：

```
{
    "Location": "/insert-unique-bucket-name-here"
}
```

> **Note**
>
> 如果您不遵守命名存储桶的规则（例如，仅使用小写字母），则会显示以下错误：调用 CreateBucket 操作时出现错误 (InvalidBucketName)：指定的存储桶无效。

2. 要上传文件并将其作为对象添加到刚刚创建的存储桶中，请调用以下PutObject方法：

```
aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body
 add_prog.py
```

如果对象成功上传到 Amazon S3 存储桶，则命令行会显示来自该服务的响应，类似于以下输出：

```
{
           "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebeea56\""}
```

ETag是已存储对象的哈希值。它可用于检查上传到 Amazon S3 的数据元的完整性。

使用创建 AWS Control Tower 资源 AWS CloudFormation

AWS Control Tower 与一项服务集成 AWS CloudFormation，该服务可帮助您对 AWS 资源进行建模和设置，从而减少创建和管理资源和基础架构所花费的时间。您可以创建一个描述所需的所有 AWS 资源（例如控件资源）AWS::ControlTower::EnabledControl的模板。 AWS CloudFormation 为您配置和配置这些资源。

使用时 AWS CloudFormation，您可以重复使用模板来一致且重复地设置 AWS Control Tower 资源。只需描述一次您的资源，然后在多个 AWS 账户 区域中一遍又一遍地配置相同的资源。

AWS Control Tower 和 AWS CloudFormation 模板

要为和相关服务配置 AWS Control Tower 和配置资源，必须了解AWS CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述了您要在 AWS CloudFormation 堆栈中配置的资源。如果你不熟悉 JSON 或 YAML，可以使用 D AWS CloudFormation esigner 来帮助你开始使用 AWS CloudFormation 模板。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的什么是 AWS CloudFormation Designer？。

AWS Control Tower 支持在中创建`AWS::ControlTower::EnabledControl`（控制资源）、`AWS::ControlTower::LandingZone`（着陆区）和`AWS::ControlTower::EnabledBaseline`（基线）。 AWS CloudFormation有关更多信息，包括这些资源类型的 JSON 和 YAML 模板示例，请参阅AWS CloudFormation 用户指南AWS Control Tower中的。

> **Note**
>
> 并发操作的限制`EnableControl`和`DisableControl`更新 AWS Control Tower 为 100 个，其中最多 20 个操作与主动控制有关。

要查看 CLI 和控制台的一些 AWS Control Tower 示例，请参阅使用启用控件 AWS CloudFormation。

了解更多关于 AWS CloudFormation

要了解更多信息 AWS CloudFormation，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation API Reference
- AWS CloudFormation 命令行界面用户指南

自定义您的 AWS Control Tower 着陆区

您的 AWS Control Tower 着陆区的某些方面可以在控制台中进行配置，例如区域选择和可选控件。其他更改可以在控制台之外进行自动化。

例如，您可以使用 AWS Control Tower 的自定义功能（一种适用于 AWS CloudFormation 模板和 AWS Control Tower 生命周期事件的 GitOps风格自定义框架）为着陆区创建更广泛的自定义设置。

从 AWS Control Tower 控制台进行自定义

要对您的着陆区进行这些自定义，请按照 AWS Control Tower 控制台提供的步骤进行操作。

在安装过程中选择自定义名称

- 您可以在设置过程中选择您的顶级 OU 名称。您可以随时使用 AWS Organizations 控制台重命名 OU，但是在中更改 OU AWS Organizations 可能会导致可修复的偏差。
- 您可以选择共享的审核和日志存档帐户的名称，但在设置后无法更改名称。（这是一次性选择。）

> **提示**
>
> 请记住，在中重命名 OU AWS Organizations 并不能更新 Account Factory 中相应的预配置产品。要自动更新预配置的产品（并避免偏移），您必须通过 AWS Control Tower 执行 OU 操作，包括创建、删除或重新注册 OU。

选择 AWS 区域

- 您可以通过选择特定 AWS 区域进行治理来自定义您的着陆区。按照 AWS Control Tower 控制台中的步骤进行操作。
- 在更新 landing zone 时，你可以选择和取消选择 AWS 区域进行治理。
- 您可以将 “区域拒绝” 控件设置为 “已启用” 或 “未启用”，并控制用户对非治理 AWS 区域中大多数 AWS 服务的访问权限。

有关 cfCT AWS 区域 在哪些地方有部署限制的信息，请参阅控制限制。

通过添加可选控件进行自定义

- 强烈推荐和选择性控制是可选的，这意味着您可以通过选择要启用的控制来自定义着陆区的执法级别。默认情况下，可选控件未启用。
- 可选的数据驻留控制允许您自定义存储区域并允许访问您的数据。
- 集成 Security Hub 标准中的可选控件允许您扫描 AWS Control Tower 环境以检查是否存在安全风险。
- 可选的主动控制允许您在 AWS CloudFormation 资源配置之前对其进行检查，以确保新资源符合您环境的控制目标。

自定义您的 AWS CloudTrail 路线

- 当您将着陆区更新到 3.0 或更高版本时，您可以选择加入或选择退出由 AWS Control Tower 管理的组织级 CloudTrail 路径。您可以随时更新着陆区（Landing zone）时更改此选择。AWS Control Tower 会在您的管理账户中创建组织级别的跟踪，并根据您的选择，该跟踪进入活动或非活动状态。着陆区 3.0 不支持账号级别的 CloudTrail 路径；但是，如果您需要这些路径，则可以配置和管理自己的路线。重复跟踪可能会产生额外费用。

在控制台中创建自定义成员账户

- 您可以从 AWS Control Tower 控制台创建自定义的 AWS Control Tower 成员账户，也可以更新现有成员账户以添加自定义设置。有关更多信息，请参阅 使用 Account Factory 自定义 (AFC) 自定义账户。

在 AWS Control Tower 控制台之外自动进行自定义

有些自定义无法通过 AWS Control Tower 控制台获得，但可以通过其他方式实现。例如：

- 在配置过程中，你可以使用 Account F actory for Terraform (AFT) 以 GitOps风格的工作流程自定义帐户。

  AFT 与 Terraform 模块一起部署，该模块可在 A FT 存储库中找到。
- 您可以使用 AWS 控制塔 (cfcT) 的自定义功能来自定义 AWS Control Tower 着陆区，这是一套基于 AWS CloudFormation 模板和服务控制策略 (SCP) 构建的功能。您可以将自定义模板和策略部署到组织内的个人账户和组织单位 (OU)。

  cfCT 的源代码可在GitHub 存储库中找到。

AWS Control Tower (cfcT) 定制的好处

我们称之为 AWS Control Tower 定制 (cfcT) 的功能包可帮助您为着陆区创建比在 AWS Control Tower 控制台中创建更广泛的自定义项。它提供了一种 GitOps风格的自动化流程。您可以重塑您的 landing zone 以满足您的业务需求。

此infrastructure-as-code自定义过程将 AWS CloudFormation 模板与 AWS 服务控制策略 (SCP) 和 AWS Control Tower 生命周期事件集成，因此您的资源部署与着陆区保持同步。例如，当您使用 Account Factory 创建新账户时，可以自动部署附加到该账户和 OU 的资源。

> **Note**
>
> 与 Account Factory 和 AFT 不同，cfcT 不是专门用于创建新账户，而是通过部署你指定的资源来自定义着陆区域中的账户和 OU。

优势

- 扩展自定义的安全 AWS 环境 — 您可以更快地扩展您的多账户 AWS Control Tower 环境，并将 AWS 最佳实践整合到可重复的自定义工作流程中。
- 实例化您的需求 — 您可以使用表达您的政策意图的 AWS CloudFormation 模板和服务控制策略根据您的业务需求自定义 AWS Control Tower 着陆区。
- 利@@ 用 AWS Control Tower 生命周期事件进一步实现自动化 — 生命周期事件允许您根据之前一系列事件的完成情况部署资源。您可以依靠生命周期事件来帮助您将资源自动部署到账户和 OU。
- 扩展您的网络架构-您可以部署自定义的网络架构，以改善和保护您的连接，例如传输网关。

其他氟氯化碳示例

- AWS 架构博客文章《使用服务目录和 AWS Control Tower 自定义项部署一致的 DNS》中给出了使用 AWS Control Tower 定制 (cfcT) 的网络用例示例。
- aws-samples存储库中提供了与 cfcT 和 GuardDuty Amazon 相关的具体示例。 GitHub
- 有关 cfCT 的其他代码示例可作为 AWS 安全参考架构的一部分在aws-samples存储库中找到。其中许多示例都包含名为的目录中的示例`manifest.yaml`文件`customizations_for_aws_control_tower`。

有关 AWS 安全参考架构的更多信息，请参阅AWS 规范性指南页面。

AWS Control Tower (cfcT) 的自定义项概述

AWS Control Tower (cfcT) 的自定义可帮助您自定义 AWS Control Tower 着陆区，并与 AWS 最佳实践保持一致。使用 AWS CloudFormation 模板和服务控制策略 (SCP) 实现自定义。

此 cfCT 功能与 AWS Control Tower 生命周期事件集成，因此您的资源部署与着陆区保持同步。例如，通过账户工厂创建新账户时，会自动部署与该账户关联的所有资源。您可以将自定义模板和策略部署到组织内的个人账户和组织单位 (OU)。

以下视频描述了部署可扩展的 cfCT 管道和常见 cfCT 定制的最佳实践。

以下部分提供了部署适用于 AWS Control Tower (cfcT) 的自定义项的架构注意事项和配置步骤。它包括一个指向AWS CloudFormation模板的链接，该模板根据安全性和可用性 AWS 的最佳实践来启动、配置和运行所需 AWS 服务。

本主题适用于具有 AWS 云架构实践经验的 IT 基础架构架构师和开发人员。

有关 AWS Control Tower 自定义项 (cfcT) 的最新更新和变更的信息，请参阅存储库中的 changelog.md 文件。 GitHub

架构概述

部署 cfCT 将在 AWS 云中构建以下环境。

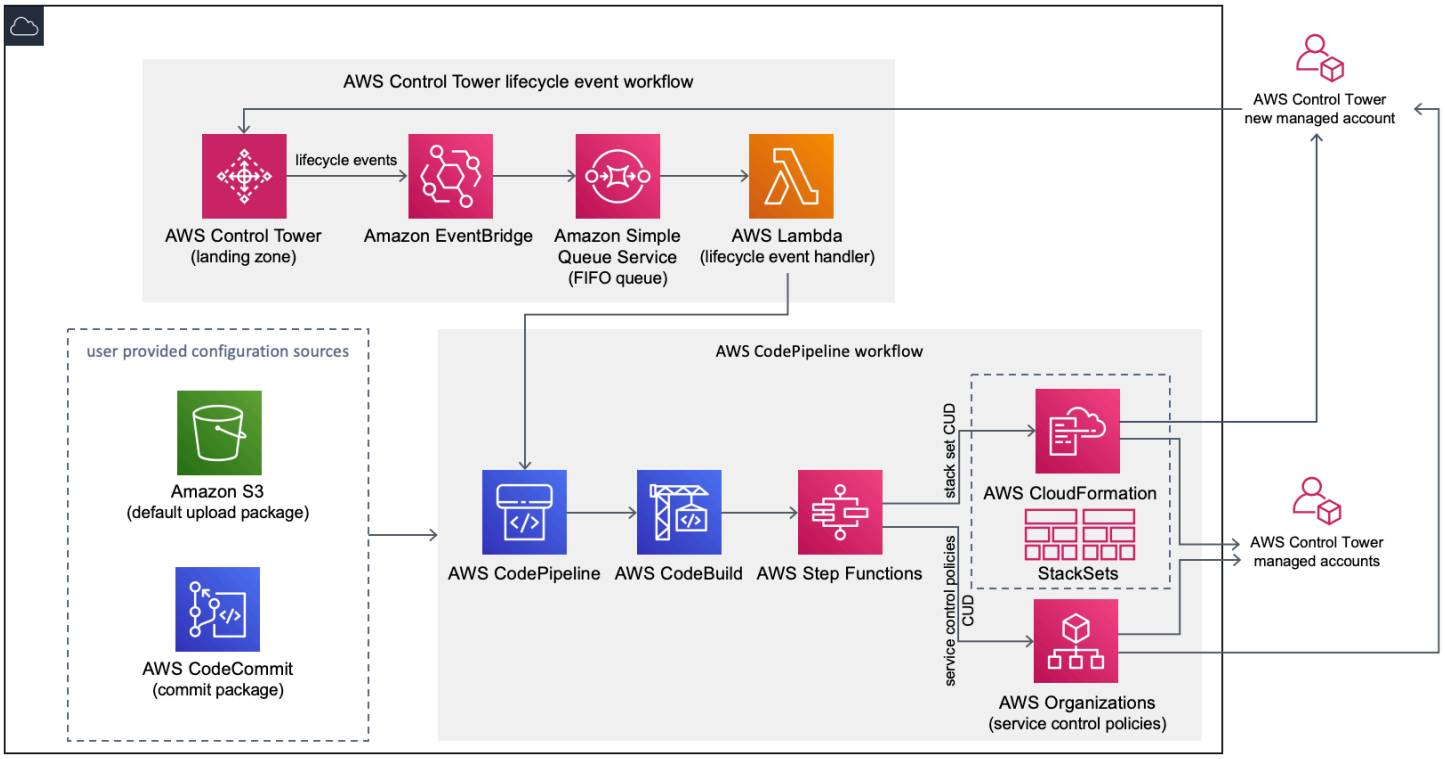


图 1：AWS Control Tower 架构的自定义设置

cfcT 包括一个您在 AWS Control Tower 管理账户中部署的 AWS CloudFormation 模板。该模板会启动构建工作流程所需的所有组件，因此您可以自定义 AWS Control Tower 着陆区。

> **备注**
>
> cfcT 必须部署在 AWS Control Tower 主区域和 AWS Control Tower 管理账户中，因为那是你的 AWS Control Tower 着陆区的部署地。有关设置 AWS Control Tower 着陆区的信息，请参阅开始使用。

在您部署 cfCT 时，它会通过亚马逊简单存储服务 (Ama zon S3) 将自定义资源打包并上传到代码管道源。上传过程会自动调用服务控制策略 (SCP) 状态机和状态机，以在 OU 级别部署 SCP，或者在 OU 或账户级别部署堆栈实例。AWS CloudFormation StackSets

> **备注**
>
> 默认情况下，cfcT 会创建一个 Amazon S3 存储桶来存储管道源，但您可以将其位置更改为AWS CodeCommit存储库。有关更多信息，请参阅将 Amazon S3 设置为配置源。

cfcT 部署了两个工作流程：

- 工作AWS CodePipeline流程
- 以及 AWS Control Tower 生命周期事件工作流程。

工作 AWS CodePipeline 流程

该 AWS CodePipeline 工作流程用于配置 AWS CodePipeline、AWS CodeBuild项目和AWS Step Functions协调组织中 SCP 的 AWS CloudFormation StackSets 管理。

当您上传配置包时，cfcT 会调用代码管道来运行三个阶段。

- 构建阶段 — 使用 AWS CodeBuild 验证配置包的内容。
- SCP Stag e — 调用服务控制策略状态机，该状态机调用 AWS Organizations API 来创建 SCP。
- AWS CloudFormation Stag e — 调用堆栈集状态机来部署您在清单文件中提供的账户或 OU 列表中指定的资源。

在每个阶段，代码管道都会调用堆栈集和 SCP 步骤函数，这些函数将自定义堆栈集和 SCP 部署到目标个人账户或整个组织单位。

> **备注**
>
> 有关自定义配置包的详细信息，请参阅。cfcT 定制指南

AWS Control Tower 生命周期事件工作流程

在 AWS Control Tower 中创建新账户时，生命周期事件可以调用 AWS CodePipeline 工作流程。您可以通过此工作流程自定义配置包，该工作流程包括亚马逊 EventBridge事件规则、亚马逊简单队列服务 (Amazon SQS) 先入先出 (FIFO) 队列和函数。AWS Lambda

当 Amazon EventBridge 事件规则检测到匹配的生命周期事件时，它会将事件传递到 Amazon SQS FIFO 队列，调用该 AWS Lambda 函数，然后调用代码管道来执行堆栈集和 SCP 的下游部署。

费用

运行 cfCT 的成本取决于运行次数、 AWS CodePipeline 运行时长、 AWS Lambda 函数的 AWS CodeBuild 数量和持续时间以及发布的 Amazon EventBridge 事件数量。例如，如果您使用 build.general1.small 在一个月内运行 100 个构建，其中每个版本运行五分钟，则运行 cfCT 的大致费用为每月 3.00 美元。有关完整详情，您可以查看您正在运行的每项 AWS 服务的定价网页。

删除模板后，将保留亚马逊简单存储服务 (Amazon S3) Service 存储桶和基于 CodeCommit AWS Git 的存储库资源，以保护您的配置信息。根据您选择的选项，将根据存储在 Amazon S3 存储桶中的数据量和 Git 请求数量（不适用于 Amazon S3 资源）向您收费。有关详情，请参阅 A mazon S3 和 AWS CodeCommit 定价。

组件服务

以下 AWS 服务是 AWS Control Tower 定制服务 (cfcT) 的组成部分。

AWS CodeCommit

根据您对 AWS CloudFormation 模板的输入，cfcT 可以创建一个AWS CodeCommit存储库，其示例配置与 Amazon 简单存储服务部分所述的配置相同。

要将 cfcT AWS CodeCommit 存储库克隆到本地计算机，必须创建凭据以允许您临时访问存储库，如AWS CodeCommit 用户指南中所述。有关版本兼容性的信息，请参阅设置 AWS CodeCommit。

AWS CodePipeline

AWS CodePipeline 根据配置包的更新验证、测试和实施更改，这些更改将在默认 Amazon S3 存储桶或存储 AWS CodeCommit 库中完成。有关将配置源控制更改为的更多信息 AWS CodeCommit，请参阅使用 Amazon S3 作为配置源。该管道包括验证和管理配置文件和模板、核心帐户、 AWS Organizations 服务控制策略的阶段，以及 AWS CloudFormation StackSets。有关管道阶段的更多信息，请参阅 cfcT 定制指南

AWS Key Management Service

cfcT 创建一个 AWS Key Management Service(AWS KMS) `CustomControlTowerKMSKey` 加密密钥。此密钥用于加密 Amazon S3 配置存储桶、Amazon SQS 队列中的对象以及 Sy AWS stems Manager 参数存储区中的敏感参数。默认情况下，只有由 cfcT 配置的角色才有权使用此密钥执行加密或解密操作。要访问配置文件、FIFO 队列或参数存储`SecureString`值，必须将管理员添加到`CustomControlTowerKMSKey`策略中。默认情况下，自动密钥轮换处于启用状态。

AWS Lambda

在 AWS Control Tower 生命周期事件期间，CfcT 使用 AWS Lambda 函数在 AWS CloudFormation StackSets 或 AWS Organizations SCP 的初始安装和部署期间调用安装组件。

Amazon Simple Notification Service

cfcT 可能会在工作流程中向亚马逊简单通知服务 (Amazon SNS) 主题发布通知，例如渠道批准。只有当您选择接收管道批准通知时，才会启动 Amazon SNS。

Amazon Simple Storage Service

当你部署 cfCT 时，cfcT 会创建一个具有唯一名称的亚马逊简单存储服务 (Amazon S3) 存储桶：

示例：亚马逊 S3 存储桶名称

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*

存储桶包含一个名为的示例配置文件 `_custom-control-tower-configuration.zip`

请注意文件名中的前导下划线。

此 zip 文件提供了示例清单和描述必要文件夹结构的相关示例模板。这些示例可帮助您开发用于自定义 AWS Control Tower 着陆区的配置包。示例清单确定了在实施自定义设置时所需的堆栈集和服务控制策略 (SCP) 的必要配置。

您可以将此示例配置包用作模型，开发和上传您的自定义包，这将自动触发 cfcT 配置管道。

有关自定义配置文件的信息，请参见cfcT 定制指南。

Amazon Simple Queue Service

cfcT 使用亚马逊简单队列服务 (Amazon SQS) Simple Queue SERVICE FIFO 队列从亚马逊捕获生命周期事件。 EventBridge它触发一个 AWS Lambda 函数，该函数调用 AWS CodePipeline 以部署 AWS CloudFormation StackSets 或 SCP。有关 SCP 的更多信息，请参阅AWS Organizations。

AWS Step Functions

cfcT 创建 Step Functions 来协调自定义部署。这些 Step Functions 会转换配置文件，以便根据需要跨环境部署自定义项。

AWS Systems Manager 参数存储

AWS Systems Manager Parameter Store 存储 cfcT 配置参数。这些参数允许您集成相关的配置模板。例如，您可以将每个账户配置为将 AWS CloudTrail 数据记录到集中式的 Amazon S3 存储桶。此外，Systems Manager Parameter Store 提供了一个集中位置，管理员可以在其中查看 cfcT 输入和参数。

部署注意事项

请务必在部署 AWS Control Tower 着陆区的同一账户和地区启动 AWS 控制塔定制 (cfcT)；也就是说，您必须将其部署在 AWS 控制塔主区域的 AWS 控制塔管理账户中。默认情况下，cfcT 通过在该账户和区域中设置配置管道来创建和运行 landing zone 配置包。

准备部署

在为初始部署准备 AWS CloudFormation 模板时，您可以选择一些选项。您可以选择配置源，也可以允许手动批准管道部署。接下来的两节将详细介绍这些选项。

选择您的配置来源

默认情况下，该模板会创建亚马逊简单存储服务 (Amazon S3) 存储桶，以将示例配置包存储为名`.zip`为的文件。`_custom-control-tower-configuration.zip`Amazon S3 存储桶受版本控制，您可以根据需要更新配置包。有关更新配置包的信息，请参阅使用 Amazon S3 作为配置源。

> **备注**
>
> 示例配置包文件名以下划线 (_) 开头， AWS CodePipeline 因此不会自动启动。完成配置包的自定义后，请务必上传`custom-control-tower-configuration.zip`不带下划线 (_) 的，以便在中开始部署。 AWS CodePipeline

通过选择 AWS CloudFormation 参数中的`AWS CodeCommit`选项，可以将配置包的存储位置从 S3 存储桶更改为 AWS CodeCommit Git 存储库。此选项使您可以轻松管理版本控制。

> **备注**
>
> 使用默认 S3 存储桶时，请确保配置包以`.zip`文件形式提供。使用 AWS CodeCommit 存储库时，请确保将配置包放在存储库中而不压缩文件。有关在中创建和存储配置包的信息 AWS CodeCommit，请参见cfcT 定制指南。

您可以使用示例配置包来创建自己的自定义配置源。当您准备好部署自定义配置时，请手动将配置包上传到 Amazon S3 存储桶或 AWS CodeCommit 存储库。当您上传配置文件时，管道会自动启动。

> **备注**
>
> 当你 AWS CodeCommit 使用存储配置包时，没有必要压缩该包。有关在中创建和存储配置包的信息 AWS CodeCommit，请参阅cfcT 定制指南。

选择您的管道配置批准参数

该 AWS CloudFormation 模板提供了手动批准部署配置更改的选项。默认情况下，不启用手动批准。有关更多信息，请参阅步骤 1。启动堆栈。

启用手动批准后，配置管道将验证对 AWS Control Tower 文件清单和模板所做的自定义，然后暂停该流程，直到获得手动批准。获得批准后，部署将根据需要继续运行剩余的管道阶段，以实施 AWS Control Tower 的自定义 (cfcT) 功能。

您可以使用手动批准参数拒绝首次尝试通过管道运行，从而阻止 AWS Control Tower 配置的自定义项运行。此参数还允许您手动验证 AWS Control Tower 配置更改的自定义，作为实施前的最终控制措施。

更新 AWS Control Tower 的自定义设置

如果您之前部署过 cfCT，则必须更新 AWS CloudFormation 堆栈才能获取 cfCT 框架的最新版本。有关详细信息，请参阅更新堆栈。

模板和源代码

AWS Control Tower (cfcT) 的自定义项将在您启动模板后部署到您的 AWS CloudFormation 管理账户中。您可以从下载模板， GitHub 然后从中启动它AWS CloudFormation。

customizations-for-aws-control-tower.template 部署了以下内容：

- 一个 AWS CodeBuild 项目
- 一个 AWS CodePipeline 项目
- 亚马逊的 EventBridge 规则
- AWS Lambda 函数
- Amazon 简单队列服务队列
- 带有示例配置包的 Amazon 简单存储服务存储桶
- AWS Step Functions

> **Note**
>
> 您可以根据自己的特定要求自定义模板。

源代码存储库

您可以访问我们的GitHub 存储库下载 cfcT 的模板和脚本，并与其他人共享您的 landing zone 自定义设置。

自动部署

在启动自动部署之前，请查看注意事项。按照本节中的 step-by-step 说明配置解决方案并将其部署到您的 AWS Control Tower 管理账户。

部署时间：大约 15 分钟

先决条件

cfcT 必须部署在您的 AWS Control Tower 管理账户和您的 AWS Control Tower 主区域中。如果您没有设置着陆区，请参阅开始使用。

部署步骤

部署 cfCT 的过程包括两个主要步骤。有关详细说明，请访问每个步骤的链接。

第 1 步。启动 堆栈

- 将 AWS CloudFormation 模板启动到您的管理账户。
- 查看模板参数，并在必要时进行调整。

第 2 步。创建自定义软件包

- 创建自定义配置包。

> **Important**
>
> 要下载正确的 AWS CloudFormation 模板并启动 cfCT，请点击本节中提供的 GitHub 链接。请勿访问任何先前指定的 S3 存储桶的旧链接。

第 1 步。启动 堆栈

本节中的 AWS CloudFormation 模板在您的账户中部署 AWS Control Tower (cfcT) 的自定义项。

> **备注**
>
> 运行cfcT时使用的 AWS 服务费用由您承担。有关更多详细信息，请参阅费用。

1. 要启动 AWS Control Tower 的自定义设置，请从下载模板， GitHub然后从中AWS CloudFormation启动该模板。
2. 默认情况下，该模板在美国东部（弗吉尼亚州北部）区域启动。要在其他 AWS 区域启动 cfcT，请使用控制台导航栏中的区域选择器。

> **Note**
>
> cfcT 必须在您部署 AWS Control Tower 着陆区（您的主区域）的同一区域和账户中启动。

3. 在创建堆栈页面上，验证 URL 文本框中显示的模板 URL 是否正确，然后选择下一步。
4. 在指定堆栈详细信息页面上，为您的 cfcT 堆栈指定一个名称。
5. 在 “参数” 下，查看以下参数并根据需要在模板中对其进行修改。

管道配置		
参数	默认值	描述
管道批准阶段	No	选择是否将管道配置从默认的自动批准阶段更改为手动批准阶段。有关更多信息，请参阅the section called “cfcT 定制指南”。
管道批准电子邮件地址	<Optional Input>	批准通知的电子邮件地址。要使用此参数，必须将 “管道批准阶段” 参数设置为Yes。
AWS CodePipeline 来源	Amazon S3	AWS 的来源 CodePipeline ，可帮助您选择存储和配置 cfcT 自定义项的位置。
AWS CodeCommit 设置		
参数	默认值	描述
现有 CodeCommit存储库？	No	选择是否使用现有 CodeCommit Git 存储库。如果选择Yes，则必须将 S CodePipeline our ce 参数设置为AWS CodeCommit 。

AWS CodeCommit 设置		
参数	默认值	描述
CodeCommit 存储库名称	`custom-control-tower-configuration`	Git 仓库名称。要使用此参数，必须将 AWS CodePipeline 来源参数设置为`AWS CodeCommit` 。此名称用于创建新的 Git 存储库，并且必须是唯一的。如果您提供现有 Git 存储库的名称，则必须设置现有 CodeCommit 存储库？ 参数设置为 “是”，然后输入该存储库的确切名称。
CodeCommit 分行名称	`main`	存储自定义包的 Git 分支。Git 存储库可以有许多分支。这是 Git 仓库中分支的默认名称。要使用此参数，必须将 S CodePipeline our ce 参数设置为`AWS CodeCommit` 。

AWS CloudFormation StackSets 配置		
参数	默认值	描述
区域并发类型	`PARALLEL`	选择在区域中部署 StackSets 操作的并发类型。此设置适用于创建、更新和删除工作流程。其他允许的值是`SEQUENTIAL` 。
最大并发百分比	`100`	一次执行此操作的账户数的最大百分比。允许的最大值为 100。有关更多信息，请参阅堆栈集操作选项。

AWS CloudFormation StackSets 配置		
参数	默认值	描述
容错百分比	10	在 AWS CloudFormation 停止该区域的操作之前，每个区域中此堆栈操作可能失败的账户百分比。允许的最小值为 0，允许的最大值为 100。有关更多信息，请参阅堆栈集操作选项。

6. 选择 Next(下一步)。
7. 在 配置堆栈选项 页面上，请选择 下一步。
8. 在 Review 页面上，审核并确认设置。务必选中确认模板将创建 AWS Identity and Access Management （IAM）资源的复选框。
9. 选择 Create stack（创建堆栈）以部署堆栈。

   您可以在 AWS CloudFormation 控制台的 “状态” 列中查看堆栈的状态。大约 15 分钟后，您应该会看到 CREATE_COMPL ETE 的状态。

第 2 步。创建自定义软件包

在启动的堆栈中，您可以通过自定义随附的配置包，为 AWS Control Tower 着陆区和服务控制策略 (SCP) 添加自定义项。有关创建自定义软件包的详细说明，请参阅cfcT 定制指南。

> **备注**
>
> 如果不上传自定义配置包，管道就无法运行。

更新堆栈

如果您之前部署了 AWS Control Tower 的自定义 (cfcT)，请按照程序更新最新版本的 cfcT 框架的 AWS CloudFormation 堆栈。

> **Important**
>
> 在完成以下步骤之前，必须将最新的模板上传 GitHub到亚马逊简单存储服务 (Amazon S3) 存储桶。有关如何开始使用 Amazon S3 的说明，请参阅《亚马逊简单存储服务用户指南》中的 Amazon S3 入门。

1. 登录 AWS CloudFormation 控制台。
2. 选择您现有的 AWS Control Tower (cfcT) CloudFormation 堆栈自定义项，然后选择 “更新”。
3. 在 “先决条件-准备模板” 下，选择 “替换当前模板”。
4. 在 “指定模板” 下，执行以下操作：
   a. 对于 “模板来源”，选择 “替换当前模板”。
   b. 对于 Amazon S3 网址，输入您之前上传 GitGub 到亚马逊 S3 的模板的模板 URL，然后选择下一步。
   c. 验证模板 URL 是否正确。然后再次选择 “下一步” 和 “下一步”。
5. 在参数下，检查模板的参数，并根据需要进行修改。请参阅步骤 1。启动堆栈以获取有关参数的详细信息。
6. 选择 Next(下一步)。
7. 在 配置堆栈选项 页面上，请选择 下一步。
8. 在 Review 页面上，审核并确认设置。请务必勾选确认模板可能会创建 AWS Identity and Access Management (IAM) 资源的复选框。
9. 选择查看更改集并验证更改。
10. 选择更新堆栈以部署堆栈。

    您可以在 AWS CloudFormation 控制台的 “状态” 列中查看堆栈的状态。大约 15 分钟后，您应该会看到 UPDATE_COM PLETE 的状态。

删除堆栈集

如果您在清单文件中启用了堆栈集删除功能，则可以删除堆栈集。默认情况下，`enable_stack_set_deletion` 参数设置为 `false`。在此配置中，从 cfcT 清单文件中删除资源时，不会采取任何操作来删除关联的堆栈集。

如果您在清单文件`true`中`enable_stack_set_deletion`将的值更改为，则当您从清单文件中移除关联资源时，cfcT 会删除堆栈集及其所有资源。

清单文件的 v2 支持此功能。

> **Important**
>
> 最初将的值设置为时`true`，下次调用 cfcT 时，所有**`enable_stack_set_deletion`**以该前缀开头`CustomControlTower-`、具有关联密钥标签`Key:AWS_Solutions, Value: CustomControlTowerStackSet`且未在清单文件中声明的资源都将被暂存以供删除。

以下是如何在`manifest.yaml`文件中设置此参数的示例：

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true   #New opt-in functionality


resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - us-west-2

  - name: demo_resource_2
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - eu-north-1
```

将 Amazon S3 设置为配置源

当您为 AWS Control Tower 设置自定义项时，它会在名为的亚马逊简单存储服务 (Amazon S3) 存储桶中存储一个名为_custom-control-tower-configuration.zip文件的初始配置文件，该文件名为Amazon S3。custom-control-tower-configuration-*account-ID*-*region*

> **备注**
>
> 如果您选择下载和修改此文件，请记得压缩更改，另存为名为的新文件custom-control-tower-configuration.zip，然后将其上传回同一 Amazon S3 存储桶。
> Amazon S3 存储桶是管道的默认来源。设置默认设置后，将文件名中不带下划线前缀的配置 zip 文件上传到 S3 存储桶将自动启动管道。

zip 文件受服务器端加密 (SSE) AWS Key Management Service (AWS KMS) 保护，并禁止使用 KMS 密钥。要访问 zip 文件，必须更新 KMS 密钥策略以指定应被授予访问权限的角色。该角色可以是管理员角色、用户或两者兼而有之。请按照以下步骤操作：

1. 导航到 AWS Key Management Service 控制台。
2. 在客户管理的密钥中，选择 CustomControlTowerkmsKe y。
3. 选择密钥策略选项卡。然后，选择 “编辑”。
4. 在 “编辑密钥策略” 页面中，找到代码中的 “允许使用密钥” 部分，然后添加以下权限之一：
   - 要添加管理角色，请执行以下操作：

     arn:aws:iam::*<account-ID>*:role/*<administrator-role>*
   - 要添加用户，请执行以下操作：

     arn:aws:iam::*<account-ID>*:user/*<username>*
5. 选择 Save Changes（保存更改）。
6. 导航到 Amazon S3 控制台，找到包含配置 zip 文件的 S3 存储桶，然后选择下载。
7. 对清单文件和模板文件进行必要的配置更改。有关自定义清单和模板文件的信息，请参阅the section called “cfcT 定制指南”。
8. 上传您的更改：

a. 压缩修改后的配置文件，并将文件命名为：`custom-control-tower-configuration.zip`。
b. 使用带有 AWS KMS 主密钥的 SSE 将文件上传到 Amazon S3：。`CustomControlTowerKMSKey`

运营指标的收集

AWS Control Tower (cfcT) 的自定义包括向其发送匿名操作指标的选项。 AWS AWS 使用这些数据来了解客户如何使用氟氯化碳以及其他相关服务和产品。启用数据收集后，以下信息将发送至 AWS：

- 解决方案 ID： AWS 解决方案标识符
- 唯一 ID (UUID)：为每个部署随机生成的唯一标识符
- 时间戳：数据收集时间戳
- 状态机执行次数：以增量方式计算此状态机运行的次数
- 清单版本：配置中使用的清单版本

> **Note**
>
> AWS 拥有它收集的数据。数据收集受AWS 隐私政策的约束。

要选择不向发送匿名操作指标 AWS，请完成以下任务之一：

- 按如下方式更新 AWS CloudFormation 模板映射部分：

  来自

```
AnonymousData:
     SendAnonymousData:
        Data: Yes
```

  到

```
AnonymousData:
     SendAnonymousData:
        Data: No
```

- 部署 cfCT 后，在参数存储控制台中找到 **/org/primary/metrics_flag** SSM 参数密钥，并将该值更新为。**No**

cfcT 定制指南

AWS Control Tower 定制 (cfcT) 指南适用于想要为公司和客户定制和扩展 AWS Control Tower 环境的管理员、 DevOps 专业人士、独立软件供应商、IT 基础设施架构师和系统集成商。它提供了有关使用 cfcT 定制包自定义和扩展 AWS Control Tower 环境的信息。

> **Note**
>
> 要部署和配置 (cfcT)，必须通过 AWS CodePipeline部署和处理配置包。以下各节详细描述了该过程。

代码管道概述

配置包需要亚马逊简单存储服务 (Amazon S3) S AWS CodePipeline ervice 和。配置包包含以下项目：

- 清单文件
- 随附的一组模板
- 其他 JSON 文件，用于描述和实现您的 AWS Control Tower 环境自定义设置

默认情况下，`_custom-control-tower-configuration.zip`配置包加载到 Amazon S3 存储桶中，命名约定如下：

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*`.`

> **Note**
>
> 默认情况下，cfcT 会创建一个 Amazon S3 存储桶来存储管道源，但您可以将源位置更改为 AWS CodeCommit 存储库。有关更多信息，请参阅《AWS CodePipeline 用户指南》CodePipeline中的编辑管道。

清单文件是一个文本文件，描述了您可以部署哪些 AWS 资源来自定义 landing zone。 CodePipeline 执行以下任务：

- 提取清单文件、随附的一组模板和其他 JSON 文件
- 执行清单和模板验证
- 调用清单文件中的部分来运行特定的管道阶段。

当您通过自定义清单文件并从配置包文件名中删除下划线 (_) 来更新配置包时，它会自动启动 AWS CodePipeline。

> **Note**
>
> 示例配置包文件名以下划线 (_) 开头， AWS CodePipeline 因此不会自动触发。完成配置包的自定义后，上传`custom-control-tower-configuration.zip`不带下划线 (_) 的文件以便在中触发部署 AWS CodePipeline。

AWS CodePipeline 阶段

cfcT 管道需要几个 AWS CodePipeline 阶段才能实施和更新您的 AWS Control Tower 环境。

1. 源阶段

   源阶段是初始阶段。您的自定义配置包将启动此工作流阶段。的源 AWS CodePipeline 可以是 Amazon S3 存储桶，也可以是 AWS CodeCommit 存储库，可以在其中托管配置包。

2. 构建阶段

   构建阶段 AWS CodeBuild 需要验证配置包的内容。这些检查包括使用 AWS CloudFormation `validate-template`和测试`manifest.yaml`文件语法和架构，以及包中包含或远程托管的所有 AWS CloudFormation 模板`cfn_nag`。如果清单文件和 AWS CloudFormation 模板通过了测试，则管道将继续进入下一阶段。如果测试失败，您可以查看 CodeBuild 日志以确定问题，并根据需要编辑配置源文件。

3. 手动批准阶段（可选）

   手动批准阶段是可选的。如果启用此阶段，它将提供对配置管道的额外控制。它会在部署期间暂停管道，直到获得批准。启动堆栈时，您可以通过将 “管道批准阶段” 参数编辑为 “是” 来选择手动批准。

4. 服务控制策略阶段

服务控制策略阶段调用服务控制策略状态机来调用创建服务控制策略 (SCP) AWS Organizations 的 API。

5. AWS CloudFormation 资源阶段

   AWS CloudFormation 资源阶段调用堆栈集状态机来部署您在清单文件中提供的账户或组织单位 (OU) 列表中指定的资源。除非指定了 AWS CloudFormation 资源依赖关系，否则状态机将按照清单文件中指定的顺序创建资源。

定义自定义配置

您将使用清单文件、随附的一组模板和其他 JSON 文件来定义您的自定义 AWS Control Tower 配置。您需要将这些文件打包成一个文件夹结构，并将它们作为`.zip`文件放入 Amazon S3 存储桶中，如以下代码示例所示。

自定义配置文件夹结构

```
- manifest.yaml
- policies/                                                [optional]
   - service control policies files (*.json)
- templates/                                               [optional]
   - template files for AWS CloudFormation Resources (*.template)
```

前面的示例描述了自定义配置文件夹的结构。无论您选择 Amazon S3 还是 AWS CodeCommit 存储库作为源存储位置，文件夹结构都保持不变。如果您选择 Amazon S3 作为源存储，请将所有文件夹和文件压缩成一个`custom-control-tower-configuration.zip`文件，然后仅将`.zip`文件上传到指定的 Amazon S3 存储桶。

> **Note**
>
> 如果您正在使用 AWS CodeCommit，请将文件放在存储库中而不压缩文件。

清单文件

该`manifest.yaml`文件是一个描述您的 AWS 资源的文本文件。以下示例显示了清单文件的结构。

```
---
```

```
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources or SCP policies
...
```

如前面的代码示例所示，清单文件的前两行指定了区域的值和版本关键字。以下是这些关键字的定义。

区域 — AWS Control Tower 默认区域的文本字符串。此值必须是有效的 AWS 区域名称（例如`us-east-1`、`eu-west-1`或`ap-southeast-1`）。创建自定义 AWS Control Tower 资源（例如 AWS CloudFormation StackSets）时，AWS Control Tower 主区域是默认区域，除非指定了更具体的资源区域。

```
region:your-home-region
```

版本-清单架构版本号。支持的最新版本是 2021-03-15。

```
version: 2021-03-15
```

> **Note**
>
> 我们强烈建议您使用最新版本。要在最新版本中更新清单属性，请参阅清单版本升级。

上一个示例中显示的下一个关键字是 resourc es 关键字。清单文件的资源部分结构化程度很高。它包含资源的详细列表，这些 AWS 资源将由 cfCT 管道自动部署。下一节将介绍这些资源及其可用参数。

清单文件的资源部分

本主题介绍清单文件的 “资源” 部分，您将在其中定义自定义所需的资源。清单文件的这一部分从关键字 resourc es 开始，一直持续到文件末尾。

清单文件的资源部分指定了 AWS CloudFormation StackSets 或 AWS Organizations SCP，cfcT 通过代码管道自动部署它们。您可以列出 OU、账户和区域以部署堆栈实例。

堆栈实例部署在账户级别，而不是 OU 级别。SCP 部署在 OU 级别。有关更多信息，请参阅创建自己的自定义项。

以下示例模板描述了清单文件资源部分中可能可用的条目。

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
        - OuName1
        - OuName2
    deploy_method: scp | stack_set
    parameters: # List of parameters [SSM, Alfred, Values]
      - parameter_key: [String]
        parameter_value: [String]
    export_outputs: # list of ssm parameters to store output values
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions: #list of strings
    - [String]
```

本主题的其余部分详细定义了上一个代码示例中显示的关键字。

名称-与关联的名称 AWS CloudFormation StackSets。 您提供的字符串为堆栈集分配了一个更便于用户使用的名称。

- 类型：字符串
- 必需：是
- 有效值：a-z、A-Z、0-9 和下划线 (_)。任何其他字符都将自动替换为下划线 (_)。

描述-资源的描述。

- 类型：字符串
- 必需：否

resource_f ile — 可以将此文件指定为清单文件、Amazon S3 URI 或指向 JSON 格式的 AWS CloudFormation 模板或 AWS Organizations 服务控制策略的 URL 的相对位置，用于创建 AWS CloudFormation 资源或 SCP。

- 类型：字符串
- 必需：是

1. 以下示例显示了resource_file，作为配置包中资源文件的相对位置给出。

```
resources:
  - name: SecurityRoles
    resource_file: templates/custom-security.template
```

2. 以下示例显示了以 Amazon S3 URI 形式提供的资源文件

```
resources:
  - name: SecurityRoles
    resource_file: s3://bucket-name/[key-name]
```

3. 以下示例显示了以 Amazon S3 HTTPS 网址形式提供的资源文件

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> 如果您提供了 Amazon S3 网址，请验证存储桶策略是否允许您从中部署 cfcT 的 AWS Control Tower 管理账户进行读取权限。如果您提供了 Amazon S3 HTTPS 网址，请验证该路径是否使用点符号。例如，S3.us-west-1。cfcT 不支持在 S3 和区域之间包含短划线的端点，例如S3-us-west-2。

4. 以下示例显示了 Amazon S3 存储桶策略和存储资源的 ARN。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::my-bucket/*”
       }
   ]
```

```
}
```

您将使用正在部署 cfcT 的管理 AWS 账户的账户 ID 替换示例中显示的*AccountId*变量。有关更多示例，请参阅《亚马逊简单存储服务用户指南》中的存储桶策略示例。

参数-指定 AWS CloudFormation 参数的名称和值。

- 类型: MapList
- 必需：否

参数部分包含成对的键/值参数。以下伪模板概述了参数部分。

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- p@@ arameter_key — 与参数关联的密钥。
  - 类型：字符串
  - 必填：是（在参数属性下）
  - 有效值：a-z、A-Z 和 0-9
- p@@ arameter_value — 与参数关联的输入值。
  - 类型：字符串
  - 必填：是（在参数属性下）

deploy_m ethod — 用于将资源部署到账户中的部署方法。目前，deploy_met hod 支持使用资源部署`stack_set`选项部署资源 AWS CloudFormation StackSets，如果您要部署 SCP，则使用该`scp`选项部署资源。

- 类型：字符串
- 有效值：`stack_set` | `scp`
- 必需：是

deplo@@ yment_t argets — 账户或组织单位 (OU) 列表，cfcT 将在其中部署 AWS CloudFormation 资源，指定为账户或组织单位。

> **Note**
>
> 如果要部署 SCP，则目标必须是 OU，而不是账户。

- 类型：字符串列表`account name`或`account number`表示此资源将部署到给定的账户列表中，或者`OU names`表示此资源将部署到给定的 OU 列表中。
- 必填：至少一个账户或组织单位
  - 账户：

    类型：字符串列表`account name`或`account number`表示此资源将部署到给定账户列表中。
  - 组织单位:

    类型：表示将此资源部署`OU names`到给定的 OU 列表的字符串列表。如果您提供的 OU 不包含账户且未添加 accounts 属性，则 cfcT 只会创建堆栈集。

    > **Note**
    >
    > 组织的管理账户 ID 不是允许的值。cfcT 不支持将堆栈实例部署到组织的管理账户中。

export_output s — 表示 SSM 参数键的名称/值对列表。这些 SSM 参数密钥允许您将模板输出存储到 SSM 参数存储中。输出仅供清单文件前面定义的其他资源参考。

```
export_outputs: # List of SSM parameters
  - name: [String]
    value: [String]
```

- 类型：名称和值键对的列表。名称包含 SSM 参数存储密钥的`name`字符串，值包含参数的`value`字符串。
- 有效值：任何字符串或`$[output_`*`CfnOutput-Logical-ID`*`]`变量，其中 *`CfnOutput-Logical-ID #####`*`输出`变量。有关 AWS CloudFormation 模板中 “输出” 部分的更多信息，请参阅AWS CloudFormation 用户指南中的输出。
- 必需：否

例如，以下代码片段将模板`VPCID`输出变量存储到名为的 SSM 参数密钥中。`/org/member/audit/vpc_id`

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

> **Note**
>
> export_output s 键名可能包含一个以外的值。output例如，如果名称为/org/environment-name，则值可能为production。

区域 — cfcT 将在其中部署 AWS CloudFormation 堆栈实例的区域列表。

- 类型：任何 AWS 商业区域名称列表，表示此资源将部署到给定的区域列表中。如果清单文件中不存在此关键字，则资源将仅部署在主区域中。
- 必需：否

root OU

cfcT 支持 Root 作为清单 V2 版本（2021-03-15）**organizational_units**中组织单位 (OU) 的值。

- 如果您选择的部署方法，则在下添加根时 scporganizational_units，AWS Control Tower 会将策略应用于根目录下的所有业务单元。如果您选择的部署方法是stack_set，则在下添加根时organizational_units，cfcT 将在根账户下注册到 AWS Control Tower 的所有账户中部署堆栈集，但管理账户除外。
- 根据 AWS Control Tower 最佳实践，管理账户仅用于管理成员账户和计费。请勿在 AWS Control Tower 管理账户中运行生产工作负载。

  根据最佳实践指南，AWS Control Tower 部署将管理账户置于根 OU 下，这样它就具有完全访问权限并且不会运行其他资源。因此，该AWSControlTowerExecution角色未部署到管理账户。
- 我们建议您遵循管理账户的这些最佳实践。如果您有需要在管理账户中部署堆栈集的特定用例，请将账户作为部署目标并指定管理账户。否则，请勿将账户作为部署目标。您必须在管理账户中创建缺失的资源，包括所需的 IAM 角色。

要在管理账户中部署堆栈集，请accounts将其添加为部署目标并指定管理帐户。否则，请勿将账户作为部署目标。

```
---
```

```
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> 只有 V2 版本的清单文件 (2021-03-15) 支持根 OU 功能。如果您将 Root 添加为下的 OU`organizational_units`，请不要添加任何其他 OU。

嵌套的 OU

cfcT 支持在清单 V2 版本 (2021-03-15) 的`organizational_units`关键字下列出一个或多个嵌套的 OU。

需要嵌套 OU 的完整路径（不包括 Root），使用冒号作为 OU 之间的分隔符。对于部署方法`scp`，AWS Control Tower 将 SCP 部署到嵌套 OU 路径中的最后一个 OU。对于部署方法`stack_set`，AWS Control Tower 会将堆栈集部署到嵌套 OU 路径中最后一个 OU 下的所有账户。

例如，考虑路径`OUName1:OUName2:OUName3`。路径中的最后一个 OU 是`OUName3`。CfcT 仅将 SCP 部署到所有直接下属`OUName3`的账户，`OUName3`并将堆栈集部署到所有账户。

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - OuName1:OUName2:OUName3
```

> **Note**
>
> 只有 V2 版本的清单文件 (2021-03-15) 支持嵌套 OU 功能。

创建自己的自定义内容

要构建自己的自定义项，您可以通过添加或更新服务控制策略 (SCP) 和 AWS CloudFormation 资源来修改`manifest.yaml`文件。对于必须部署的资源，您可以添加或删除账户和 OU。您可以添加或修改包文件夹中的模板、创建自己的文件夹，以及引用`manifest.yaml`文件中的模板或文件夹。

本节介绍构建自己的自定义项的两个主要部分：

- 如何为服务控制策略设置自己的配置包
- 如何为堆 AWS CloudFormation 栈集设置自己的配置包

为服务控制策略设置配置包

本节介绍如何为服务控制策略 (SCP) 创建配置包。此过程的两个主要部分是 (1) 准备清单文件，以及 (2) 准备您的文件夹结构。

第 1 步：编辑清单.yaml 文件

使用示例`manifest.yaml`文件作为起点。输入所有必要的配置。添加`resource_file`和`deployment_targets`详细信息。

以下代码段显示了默认的清单文件。

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

的`region`值将在部署期间自动添加。它必须与您部署 cfCT 的区域相匹配。该区域必须与 AWS Control Tower 区域相同。

要在 Amazon S3 存储桶中存储的 zip 包中的`example-configuration`文件夹中添加自定义 SCP，请打开该`example-manifest.yaml`文件并开始编辑。

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

…truncated…
```

以下代码段显示了自定义清单文件的示例。您可以在一次更改中添加多个策略。

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

步骤 2：创建文件夹结构

如果您使用 Amazon S3 URL 作为资源文件并使用带键/值对的参数，则可以跳过此步骤。

您必须包含 JSON 格式的 SCP 策略才能支持清单，因为清单文件引用了 JSON 文件。确保文件路径与清单文件中提供的路径信息相匹配。

- 策略 JSON 文件包含要部署到 OU 的 SCP。

以下代码段显示了示例清单文件的文件夹结构。

```
- manifest.yaml
- policies/
   - block-s3-public.json
```

以下片段是block-s3-public.json策略文件的示例。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

为以下各项设置配置包 AWS CloudFormation StackSets

本节介绍如何为设置配置包 AWS CloudFormation StackSets。此过程的两个主要部分是：(1) 准备清单文件，以及 (2) 更新文件夹结构。

步骤 1：编辑现有清单文件

将新 AWS CloudFormation StackSets 信息添加到您之前编辑的清单文件中。

仅供查看，以下代码段包含与之前显示的用于为 SCP 设置配置包的相同自定义清单文件。现在，您可以进一步编辑此文件，以包含有关您的资源的详细信息。

```
---
region: us-east-1
version: 2021-03-15

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
```

```
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

以下代码段显示了包含resources详细信息的经过编辑的示例清单文件。的顺序resources决定了创建resources依赖关系的执行顺序。您可以根据业务需求编辑以下示例清单文件。

```
---
region: your-home-region
version: 2021-03-15

…truncated…

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions:
      - region-name

  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
```

```
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
regions:
  - region-name
```

以下示例显示您可以在清单文件中添加多个 AWS CloudFormation 资源。

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
        - Custom
    export_outputs:
      - name: /org/network/transit-gateway-id
        value: $[output_TransitGatewayID]
    regions:
      - us-east-1
```

步骤 2：更新文件夹结构

更新文件夹结构时，可以在清单文件中包含所有支持的 AWS CloudFormation 模板文件和 SCP 策略文件。验证文件路径是否与清单文件中提供的路径相匹配。

- 模板文件包含要在 OU 和账户中部署的 AWS 资源。
- 策略文件包含模板文件中使用的输入参数。

以下示例显示了在步骤 1 中创建的示例清单文件的文件夹结构。

```
- manifest.yaml
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

“alfred” 助手和 AWS CloudFormation 参数文件

cfCT 为你提供了一种名为 alfred helper 的机制，用于获取模板中定义的 SSM 参数存储密钥的值。AWS CloudFormation 使用 alfred 助手，您可以使用存储在 SSM 参数存储中的值，而无需更新模板。 AWS CloudFormation 有关更多信息，请参阅什么是 AWS CloudFormation 模板？ 在《AWS CloudFormation 用户指南》中。

> **Important**
>
> alfred 助手有两个限制。参数仅在 AWS Control Tower 管理账户的主区域中可用。作为最佳实践，可以考虑使用堆栈实例之间不会变化的值。当 “alfred” 帮助程序检索参数时，它会从导出变量的堆栈集中随机选择一个堆栈实例。

示例

假设你有两个 AWS CloudFormation 堆栈集。堆栈集 1 有一个堆栈实例，可部署到一个区域中的一个账户。它在可用区中创建 Amazon VPC 和子网，并且`subnet ID`必须将`VPC ID`和作为参数值传递到堆栈集 2 中。在将`VPC ID`和`subnet ID`传递到堆栈集 2 之前，`subnet ID`必须使用将`VPC ID`和存储在堆栈集 1 中`AWS:::SSM::Parameter`。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的 `AWS:::SSM::Parameter`。

AWS CloudFormation 堆栈集 1：

在以下片段中，alfred 助手可以subnet ID从参数存储中获取VPC ID和的值，并将它们作为输入传递给 StackSet 状态机。

```
VpcIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/vpc/id'
      Description: Contains the VPC id
      Type: String
      Value: !Ref MyVpc

SubnetIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/subnet/id'
      Description: Contains the subnet id
      Type: String
      Value: !Ref MySubnet
```

AWS CloudFormation 堆栈集 2：

该片段显示了 AWS CloudFormation stack 2 manifest.yaml 文件中指定的参数。

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

AWS CloudFormation 堆栈集 2.1：

该片段显示您可以列出alfred_ssm属性以支持类型CommaDelimitedList参数。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的 Parameters。

```
parameters:
      - parameter_key: VpcId # Type: String
        parameter_value: $[alfred_ssm_/stack_1/vpc/id']
      - parameter_key: SubnetId # Type: String
        parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
      - parameter_key: AvailablityZones # Type: CommaDelimitedList
        parameter_value:
```

```
  - "$[alfred_ssm_/availability_zone_1]"
 - "$[alfred_ssm_/availability_zone_2]"
```

自定义包的 JSON 架构

cfcT 定制包的 JSON 架构位于上的 GitHub源代码存储库中。您可以将该架构与许多您最喜欢的开发工具一起使用，并且您可能会发现它有助于减少构建自己的`manifest.yaml`文件时的错误。

清单版本升级

有关最新版本的 AWS Control Tower 自定义项 (cfcT) 的信息，请参阅存储库中的 changelog.md 文件。 GitHub

Warning

AWS Control Tower 定制版 (cfcT) 2.2.0 版引入了清单架构（版本 2021-03-15），以与相关的服务 API 保持一致。 AWS 清单架构允许单个 manifest.yaml 文件通过分离的工作流程管理支持的资源（AWS CloudFormation 模板和 SCP）。 DevOps
我们强烈建议您将清单架构从 2020-01-01 版本更新到版本 2021- 03- 15 或更高版本。
cfcT 继续支持该文件的 2021-03-15 和 2020-01-01 版本。 `manifest.yaml`无需对现有配置进行任何更改。但是，版本 2020-01-01 已终止支持。我们不再为 2020-01-01 版本提供更新或添加增强功能。2020-01-01 版本不支持根 OU 和嵌套 OU 功能。

清单版本 202 1-03-15 中已弃用的属性：

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

强制升级步骤

升级到清单架构版本 2021-03-15 版本时，必须进行以下更改才能更新文件。接下来的章节概述了过渡期间的必修和建议的变更。

Organiations

1. 将 SCP 移至 “组织政策” 下的新属性资源下。
2. 将 policy_file 属性更改为新的属性 resource_file。
3. 将 apply_to_accounts_in_ou 更改为新的属性部署目标。OU 列表应在子属性 organial_units 下定义。组织策略不支持账户子属性。
4. 添加一个值为 scp 的新属性 deploy_met hod。

AWS CloudFormation 资源

1. 将 cloudformation_resources 下的 CloudFormation 资源移到新的属性资源下。
2. 将 template_file 属性更改为新的属性 resource_file。
3. 将 deplo y_to_ou 更改为新的属性部署目标。OU 列表应在子属性 organial_units 下定义。
4. 将 deplo y_to_accounts 更改为新的属性部署目标。账户列表应在子财产账户下定义。
5. 将 ssm_parameters 属性更改为新的属性 export_ outputs。

强烈推荐的升级步骤

AWS CloudFormation 参数

1. 将 p arameter_file 属性更改为新的属性参数。
2. 删除 p arameter_ file 属性的值中的文件路径。
3. 将现有参数 JSON 文件中的参数键和参数值复制为参数属性的新格式。这将帮助你在清单文件中管理它们。

> **Note**
>
> 清单版本 2021-03-15 支持 p arameter_file 属性。

在 AWS Control Tower 中联网

AWS Control Tower 为通过 VPC 进行联网提供基本支持。

如果 AWS Control Tower VPC 的默认配置或功能无法满足您的需求，则可以使用其他 AWS 服务来配置您的 VPC。有关如何使用 VPC 和 AWS Control Tower 的更多信息，请参阅构建可扩展且安全的多 VPC AWS 网络基础设施。

相关 主题

- 有关注册现有 VPC 的账户时 AWS Control Tower 的工作原理的信息，请参阅在 VPC 中注册现有账户。
- 使用 Account Factory，您可以配置包含 AWS Control Tower VPC 的账户，也可以配置没有 VPC 的账户。有关如何删除 AWS Control Tower VPC 或配置没有 VPC 的 AWS Control Tower 账户的信息，请参阅演练：在没有 VPC 的情况下配置 AWS Control Tower。
- 有关如何更改 VPC 账户设置的信息，请参阅有关更新账户的 Acco unt Factory 文档。
- 有关在 AWS Control Tower 中使用联网和 VPC 的更多信息，请参阅本用户指南相关信息页面上有关联网的部分。

AWS Control T AWS ower 中的 VPC 和区域

作为账户创建的标准部分，在每个区域 AWS 创建 AWS默认 VPC，即使是您不使用 AWS Control Tower 管理的区域也是如此。此默认 VPC 与 AWS Control Tower 为预配置账户创建的 VPC 不同，但是 IAM 用户可以访问非受监管区域中的 AWS 默认 VPC。

管理员可以启用区域拒绝控制，这样您的最终用户就无权连接到 AWS Control Tower 支持的区域，但在您的管辖区域之外的 VPC。要配置区域拒绝控制，请转到着陆区域设置页面，然后选择修改设置。

区域拒绝控制会阻止 API 调用大多数不受治理 AWS 区域的服务。有关更多信息，请参阅AWS 根据请求拒绝访问 AWS 区域。 。

> **Note**
>
> 在不支持 AWS Control Tower 的区域中，区域拒绝控制可能不会阻止 IAM 用户连接到 AWS 默认 VPC。

或者，您可以移除非治理 AWS 区域中的默认 VPC。要列出某个区域中的默认 VPC，您可以使用类似于以下示例的 CLI 命令：

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

AWS Control Tower 和 VPC 概述

以下是有关 AWS Control Tower VPC 的一些基本信息：

- 当您在 Account Factory 中配置账户时，AWS Control Tower 创建的 VPC 与 AWS 默认 VPC 不同。
- 当 AWS Control Tower 在支持的 AWS 区域设置新账户时，AWS Control Tower 会自动删除默认 AWS VPC，并设置由 AWS Control Tower 配置的新 VPC。
- 每个 AWS Control Tower 账户只能有一个由 AWS Control Tower 创建的 VPC。一个账户可以在账户限制内拥有其他 AWS VPC。
- 每个 AWS Control Tower VPC 在除美国西部（加利福尼亚北部）地区之外的所有地区都有三个可用区us-west-1，并在其中有两个可用区us-west-1。默认情况下，每个可用区均分配有一个公有子网和两个私有子网。因此，在美国西部（加利福尼亚北部）以外的区域，每个 AWS Control Tower VPC 默认包含九个子网，这些子网分为三个可用区。在美国西部（加利福尼亚北部），六个子网被划分为两个可用区。
- 您的 AWS Control Tower VPC 中的每个子网都被分配了一个大小相等的唯一范围。
- VPC 中的子网数量是可以配置的。有关如何更改 VPC 子网配置的更多信息，请参阅账户工厂主题。
- 由于 IP 地址不重叠，因此您的 AWS Control Tower VPC 中的六到九个子网可以不受限制地相互通信。

在使用 VPC 时，AWS Control Tower 在区域级别上没有区别。每个子网都是通过您指定的准确 CIDR 范围分配的。VPC 子网可存在于任何区域。

备注

> **管理 VPC 成本**
>
> 如果您将 Account Factory VPC 配置设置为在配置新账户时启用公有子网，则 Account Factory 会将 VPC 配置为创建 NAT 网关。Amazon VPC 将对您的用量计费。

⚠ VPC 和控制设置

如果您在启用 VPC 互联网访问设置的情况下配置 Account Factor y 账户，则该 Account Factory 设置将覆盖 “禁止客户管理的 Amazon VPC 实例访问互联网” 控件。要避免为新配置的账户启用互联网访问功能，您必须在 Account Factory 中更改设置。有关更多信息，请参阅演练：在没有 VPC 的情况下配置 AWS Control Tower。

适用于 VPC 和 AWS Control Tower 的 CIDR 和对等互连

本部分主要供网络管理员使用。贵公司的网络管理员通常是为您的 AWS Control Tower 组织选择整个 CIDR 范围的人。然后，网络管理员在该范围内分配子网，用于特定用途。

当您为 VPC 选择 CIDR 范围时，AWS Control Tower 会根据 RFC 1918 规范验证 IP 地址范围。Account Factory 允许/16的 CIDR 块不超过以下范围：

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`
- `100.64.0.0/10`（仅当您的互联网提供商允许使用此范围时）

/16 分隔符允许最多 65536 个不同的 IP 地址。

您可以分配以下范围中的任何有效的 IP 地址：

- `10.0.x.x to 10.255.x.x`
- `172.16.x.x - 172.31.x.x`
- `192.168.0.0 - 192.168.255.255`（没有 `192.168` 范围之外的 IP）

如果您指定的范围超出了这些范围，AWS Control Tower 会提供一条错误消息。

默认的 CIDR 范围为 `172.31.0.0/16`。

当 AWS Control Tower 使用您选择的 CIDR 范围创建 VPC 时，它会为您在组织单位 (OU) 内创建的每个账户的每个 VPC 分配相同的 CIDR 范围。由于 IP 地址的默认重叠，此实现最初不允许在 OU 中的任何 AWS Control Tower VPC 之间进行对等。

子网

在每个 VPC 中，AWS Control Tower 将您指定的 CIDR 范围平均划分为九个子网（美国西部（加利福尼亚北部）除外，那里有六个子网）。VPC 中的所有子网都不会重叠。因此，它们都可以在 VPC 内相互通信。

总之，默认情况下，VPC 内的子网通信不受限制。控制 VPC 子网之间通信的最佳实践（如果需要）是设置访问控制列表，其中包含定义允许流量的规则。使用安全组控制具体实例间的流量。有关在 AWS Control Tower 中设置安全组和防火墙的更多信息，请参阅演练：使用防火 AWS 墙管理器在 AWS Control Tower 中设置安全组。

对等连接

AWS Control Tower 不限制 vpc 到 VPC 的对等互连，以便在多个 VPC 之间进行通信。但是，默认情况下，所有 AWS Control Tower 虚拟私有云都具有相同的默认 CIDR 范围。要支持对等互连，您可以在 Account Factory 的设置中修改 CIDR 范围，以便 IP 地址不会重叠。

如果您在 Account Factory 的设置中更改 CIDR 范围，则随后由 AWS Control Tower（使用 Account Factory）创建的所有新账户都将分配新的 CIDR 范围。不会更新旧账户。例如，您可以创建一个账户，然后更改 CIDR 范围并创建一个新账户，那么分配给这两个账户的 VPC 就可以实现对等了。由于 IP 地址范围不同，因而可以实现对等。

所需角色和权限

AWS Control Tower 使用 IAM 角色来帮助管理对资源的访问权限。

有关角色的一般信息，请参阅用户组、角色和权限集。

关于权限

- 有关 IAM 群组及其在 AWS Control Tower 中的权限的信息，请参阅 AWS Control Tower 的 IAM 身份中心群组。
- 有关配置账户所需权限的信息，请参阅账户所需的权限。
- 有关 AWS Control Tower 所需的控制台权限的信息，请参阅使用 AWS Control Tower 控制台所需的权限。

关于角色

- 有关如何创建角色的信息，包括专为编程访问而设计的权限，请参阅创建角色和分配权限，以及 AWS Control Tower 审计账户的编程角色和信任关系。
- 有关 AWS Control Tower 用于管理您的账户的其他角色的信息，请参阅在 AWS Control Tower 中使用基于身份的策略（IAM 策略）和适用于 AWS Control Tower 的托管策略。
- 有关 AWS Control Tower 和 AWS Config 角色的信息，请参阅 AWS Control Tower ConfigRecorderRole。
- 有关 AWS Control Tower 用来汇总账户信息的角色 AWS Config 的信息，请参阅 AWS Control Tower 如何聚合非托管业务单元和账户中的 AWS Config 规则。
- 有关如何在分配角色和权限时保护资源的信息，请参阅角色信任关系的可选条件、可选配置 AWS KMS 密钥和防止跨服务模仿。
- 有关使用 IAM 角色在 AWS Control Tower 中自动配置账户的具体信息，请参阅使用 IAM 角色自动配置账户。
- 要查看保护 AWS Config SNS 主题的策略，请参阅 AWS Config SNS 主题策略。

AWS Control Tower 如何使用角色来创建和管理账户

通常，角色是中身份和访问管理 (IAM) 的一部分 AWS。有关 IAM 和中角色的一般信息 AWS，请参阅 IAM 用户指南中的AWS IAM 角色主题。

角色和账户创建

AWS Control Tower 通过调用的 `CreateAccount` API 来创建客户的账户 AWS Organizations。 AWS Organizations 创建此账户时，它会在该账户中创建一个角色，AWS Control Tower 通过向 API 传递参数来命名该角色。角色的名称为 `AWSControlTowerExecution`。

AWS Control Tower 接管了 Account Factory 创建的所有账户的`AWSControlTowerExecution`角色。AWS Control Tower 使用此角色为账户设定基准并应用强制控制（以及任何其他已启用的控件），从而创建其他角色。这些角色反过来又被其他服务使用，例如 AWS Config。

> **Note**
>
> 为账户设置基准就是设置其资源，包括Account Factory模板（有时也称为蓝图）和控件。作为模板部署的一部分，基准过程还会为账户设置集中日志和安全审计角色。AWS Control Tower 基准包含在您应用于每个注册账户的角色中。

有关账户和资源的更多信息，请参阅AWS 账户 在 AWS Control Tower 中简介。

AWSControlTowerExecution 角色解释

`AWSControlTowerExecution` 角色必须存在于所有注册的账户中。它允许 AWS Control Tower 管理您的个人账户，并将有关这些账户的信息报告给您的审计和日志存档账户。

可以通过多种方式将该`AWSControlTowerExecution`角色添加到账户中，如下所示：

- 对于安全 OU 中的账户（有时称为核心账户），AWS Control Tower 会在初始设置 AWS Control Tower 时创建角色。
- 对于通过 AWS Control Tower 控制台创建的 Account Factory 账户，AWS Control Tower 会在创建账户时创建此角色。
- 对于单一账户注册，我们要求客户手动创建角色，然后在 AWS Control Tower 中注册该账户。
- 将监管范围扩展到 OU 时，AWS Control Tower 使用 StackSet-AWSControlTowerExecutionRole 在该组织单位的所有账户中创建角色。

该`AWSControlTowerExecution`角色的目的：

- `AWSControlTowerExecution`允许您使用脚本和 Lambda 函数自动创建和注册账户。

- AWSControlTowerExecution 可帮助您配置组织的日志记录，以便每个账户的所有日志都发送到日志记录账户。
- AWSControlTowerExecution允许您在 AWS Control Tower 中注册个人账户。首先，您必须将AWSControlTowerExecution角色添加到该帐户。有关如何添加角色的步骤，请参阅手动将所需的 IAM 角色添加到现有角色 AWS 账户 并进行注册。

该AWSControlTowerExecution角色如何与 OU 配合使用：

该AWSControlTowerExecution角色可确保您选择的 AWS Control Tower 控制措施自动应用于您组织中每个 OU 中的每个个人账户，以及您在 AWS Control Tower 中创建的每个新账户。因此：

- 基于 AWS Control Tower 控件所包含的审计和日志功能，您可以更轻松地提供合规和安全报告。
- 您的安全性和合规性团队可以验证是否满足所有要求，并且没有发生组织偏差。

有关漂移的更多信息，请参阅在 AWS Control Tower 中检测和解决偏差。

总而言之，AWSControlTowerExecution 角色及其关联策略可让您灵活地控制整个组织的安全性和合规性。因此，不太可能发生违反安全或协议的情况。

角色信任关系的可选条件

您可以在角色信任策略中施加条件，以限制与 AWS Control Tower 中某些角色交互的账户和资源。我们强烈建议您限制对该AWSControlTowerAdmin角色的访问权限，因为它允许广泛的访问权限。

为帮助防止攻击者访问您的资源，请手动编辑您的 AWS Control Tower 信任策略，以便在策略声明中至少添加一个aws:SourceArn或aws:SourceAccount有条件的信任策略。作为安全最佳实践，我们强烈建议添加aws:SourceArn条件，因为它比aws:SourceAccount限制对特定账户和特定资源的访问权限更为具体。

如果您不知道资源的完整 ARN，或者要指定多个资源，则可以将带通配符 (*) 的aws:SourceArn条件用于 ARN 的未知部分。例如，如果您不想指定区域，则可以arn:aws:controltower:*:123456789012:*使用。

以下示例演示了如何将 aws:SourceArn IAM 条件与您的 IAM 角色信任策略结合使用。在您的信任关系中添加该AWSControlTowerAdmin角色的条件，因为 AWS Control Tower 服务委托人会与之交互。

如示例所示，源 ARN 的格式为：arn:aws:controltower:*${HOME_REGION}*:*${CUSTOMER_AWSACCOUNT_id}*:*

将字符串${HOME_REGION}和${CUSTOMER_AWSACCOUNT_id}替换为您自己的家庭区域和主叫账户的账户 ID。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

在示例中，指定为的源 ARN `arn:aws:controltower:us-west-2:012345678901:*` 是唯一允许执行该操作的 ARN。`sts:AssumeRole`换句话说，只有`us-west-2`在该地区能够登录账户 ID `012345678901` 的用户才可以执行需要该特定角色和信任关系的 AWS Control Tower 服务（指定为）的操作`controltower.amazonaws.com`。

下一个示例显示了应用于角色信任策略的`aws:SourceAccount`和`aws:SourceArn`条件。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

该示例说明了aws:SourceArn条件语句，并添加了aws:SourceAccount条件语句。有关更多信息，请参阅 防止跨服务模仿。

有关 AWS Control Tower 中权限策略的一般信息，请参阅管理对资源的访问权限。

建议：

我们建议您为 AWS Control Tower 创建的角色添加条件，因为这些角色由其他 AWS 服务直接担任。有关更多信息，请参阅本节前面所示的示例。AWSControlTowerAdmin对于 AWS Config 录制器角色，我们建议添加aws:SourceArn条件，将 Config 记录器 ARN 指定为允许的来源 ARN。

对于所有托管账户中的 AWS Control Tower Audit 账户可以担任的角色或其他编程角色，我们建议您在这些角色的信任策略中添加aws:PrincipalOrgID条件，以验证访问资源的委托人是否属于正确 AWS 组织中的账户。AWSControlTowerExecution不要添加aws:SourceArn条件语句，因为它无法按预期工作。

> **Note**
>
> 如果出现偏差，AWS Control Tower 角色可能会在某些情况下被重置。如果您已自定义角色，建议您定期重新检查这些角色。

AWS Control Tower 如何聚合非托管业务单元和账户中的 AWS Config 规则

AWS Control Tower 管理账户创建了一个组织级聚合器，该聚合器可帮助检测外部 AWS Config 规则，因此 AWS Control Tower 无需访问非托管账户。AWS Control Tower 控制台显示您为给定账户创建了多少条外部创建的 AWS Config 规则。您可以在账户详情页面的 External Config 规则合规性选项卡中查看有关这些外部规则的详细信息。

为了创建聚合器，AWS Control Tower 添加了一个角色，该角色具有描述组织并列出其下账户所需的权限。该AWSControlTowerConfigAggregatorRoleForOrganizations角色需要AWSConfigRoleForOrganizations托管策略和与的信任关系config.amazonaws.com。

以下是附加到该角色的 IAM 策略（JSON 工件）：

```
{
    "Version": "2012-10-17",
      "Statement": [
       {
        "Effect": "Allow",
        "Action": [
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:ListAWSServiceAccessForOrganization"
         ],
       "Resource": "*"
      }
    ]
  }
```

以下是AWSControlTowerConfigAggregatorRoleForOrganizations信任关系：

```
{
    "Version": "2012-10-17",
      "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
        "Service": "config.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}
```

要在管理账户中部署此功能，需要在托管策略中添加以下权限AWSControlTowerServiceRolePolicy，该策略由AWSControlTowerAdmin角色在创建 AWS Config 聚合器时使用：

```
{
```

```
  "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam:::role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:::config-aggregator/"
          ]
        },
      {
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
      }
    ]
}
```

已创建新资源：AWSControlTowerConfigAggregatorRoleForOrganizations和 aws-controltower-ConfigAggregatorForOrganizations

准备就绪后，您可以单独注册帐户，也可以通过注册 OU 将其注册为群组。注册账户后，如果您在中AWS Config创建规则，AWS Control Tower 就会检测到新规则。聚合器显示外部规则的数量，并提供指向 AWS Config 控制台的链接，您可以在其中查看账户的每条外部规则的详细信息。使用 AWS Config 控制台和 AWS Control Tower 控制台中的信息来确定您是否为账户启用了相应的控件。

AWS Control Tower 审计账户的编程角色和信任关系

您可以登录审计账户并扮演以编程方式审核其他账户的角色。审计账户不支持手动登录到其他账户。

通过某些仅授予 AWS Lambda 函数的角色，审计账户允许您以编程方式访问其他账户。出于安全考虑，这些角色与其他角色之间存在信任关系，这意味着使用这些角色的条件是严格定义的。

AWS Control Tower 堆栈集在审计账户中StackSet-AWSControlTowerBP-BASELINE-ROLES创建了以下仅限编程的跨账户角色：

- aws-控制塔-AdministratorExecutionRole

- aws-控制塔-AuditAdministratorRole
- aws-控制塔-ReadOnlyExecutionRole
- aws-控制塔-AuditReadOnlyRole

ReadOnlyExecutionRole:请注意，此角色允许审计账户在整个组织中读取 Amazon S3 存储桶中的对象（与仅允许访问元数据的SecurityAudit策略形成鲜明对比）。

aws-控制塔-: AdministratorExecutionRole

- 拥有管理员权限
- 无法从控制台进行假设
- 只能由审计账户中的角色担任 — aws-controltower-AuditAdministratorRole

以下构件显示了的信任关系aws-controltower-AdministratorExecutionRole。占位符号012345678901将替换为您的审计账户的Audit_acct_ID数字。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-控制塔-: AuditAdministratorRole

- 只能由 AWS Lambda 服务假设
- 有权对名称以字符串日志开头的 Amazon S3 对象执行读取 (获取) 和写入 (Put) 操作

附加政策：

1. AWSLambdaExecute— AWS 托管策略

2. AssumeRole-aws-controltower-AuditAdministratorRole — 内联策略 — 由 AWS Control Tower 创建，接下来是工件。

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
   "sts:AssumeRole"
   ],
 "Resource": [
   "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
   ],
 "Effect": "Allow"
 }
   ]
}
```

以下构件显示了以下对象的信任关系aws-controltower-AuditAdministratorRole：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-控制塔-: ReadOnlyExecutionRole

- 无法从控制台进行假设
- 只能由审计账户中的另一个角色担任 — AuditReadOnlyRole

以下构件显示了的信任关系aws-controltower-ReadOnlyExecutionRole。占位符号012345678901将替换为您的审计账户的Audit_acct_ID数字。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-控制塔-: AuditReadOnlyRole

- 只能由 AWS Lambda 服务假设
- 有权对名称以字符串日志开头的 Amazon S3 对象执行读取 (获取) 和写入 (Put) 操作

附加政策：

1. AWSLambdaExecute— AWS 托管策略

2. AssumeRole-aws-controltower-AuditReadOnlyRole — 内联策略 — 由 AWS Control Tower 创建，接下来是工件。

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
  "sts:AssumeRole"
 ],
 "Resource": [
  "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
 ],
 "Effect": "Allow"
   }
  ]
}
```

以下构件显示了以下对象的信任关系`aws-controltower-AuditAdministratorRole`：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

使用 IAM 角色自动预置账户

要以更自动化的方式配置 Account Factory 账户，您可以在 AWS Control Tower 管理账户中创建 Lambda 函数，该账户在成员账户中AWSControlTowerExecution担任该角色。然后，管理账户使用该角色在每个成员账户中执行所需的配置步骤。

如果您使用 Lambda 函数配置账户，则执行此项工作的身份除此之外还必须具有以下 IAM 权限策略。AWSServiceCatalogEndUserFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetPeregrineStatus",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
```

```
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchGroupsWithGroupName",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject",
                "organizations:describeOrganization",
                "sso:DescribeRegisteredRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS C `sso:GetPeregrineStatus` on `sso:ProvisionApplicationInstanceForAWSAccount` trol Tower A `sso:ProvisionSAMLProvide` ccount Factory 需要权限`sso:ProvisionApplicationProfileForAWSAccountInstance`、、和才能与 AWS IAM 身份中心进行交互。

AWS Control Tower 中的资源

- 有关 AWS Control Tower 中资源所有权的一般信息，请参阅管理您的 AWS Control Tower 资源的访问权限概述。
- 有关 AWS Control Tower 在共享账户中创建的资源的信息，请参阅关于共享账户。
- 有关 AWS Control Tower 在通过 Account Factory 配置账户时创建的资源的信息，请参阅Account Factory 的资源注意事项。
- 要查看有关 AWS Control Tower 定义的用于与 AWS Control Tow er API 配合使用的 AWS 资源类型的详细信息，请参阅AWS CloudFormation 用户指南中的 AWS Control Tower 资源类型参考。

AWS 区域如何与 AWS Control Tower 配合使用

目前，以下 AWS 区域支持 AWS Control Tower：

- 美国东部（弗吉尼亚州北部）
- 美国东部（俄亥俄州）
- 美国西部（俄勒冈州）
- 加拿大（中部）
- 亚太地区（悉尼）
- 亚太地区（新加坡）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- Europe (London)
- 欧洲地区（斯德哥尔摩）
- 亚太地区（孟买）
- 亚太地区（首尔）
- 亚太地区（东京)
- 欧洲地区（巴黎）
- 南美洲（圣保罗）
- 美国西部（北加利福尼亚）
- 亚太地区（香港）
- 亚太地区（雅加达）
- 亚太地区（大阪）
- 欧洲地区（米兰）
- 非洲（开普敦）
- 中东（巴林）
- 以色列（特拉维夫）
- 中东（阿联酋）
- 欧洲（西班牙）

- 亚太地区（海得拉巴）
- 欧洲（苏黎世）
- 亚太地区（墨尔本）
- 加拿大西部（卡尔加里）

关于你的家乡地区

当您创建着陆区时，您用于访问 AWS 管理控制台的区域将成为 AWS Control Tower 的主 AWS 区域。在创建过程中，一些资源是在主区域中配置的。其他资源（例如 OU 和 AWS 账户）是全球性的。

选择主区域后，您无法对其进行更改。

控件和区域

目前，所有预防性控制措施都在全球范围内发挥作用。但是，侦探和主动控制仅适用于支持 AWS Control Tower 的区域。有关在新区域激活 AWS Control Tower 时控件行为的更多信息，请参阅配置您的 AWS Control Tower 区域。

配置您的 AWS Control Tower 区域

本节介绍将您的 AWS Control Tower 着陆区扩展到新 AWS 区域或从着陆区配置中移除区域时可能出现的行为。通常，此操作是通过 AWS Control Tower 控制台的更新功能执行的。

> **Note**
>
> 我们建议您避免将 AWS Control Tower 着陆区扩展到不需要运行工作负载的 AWS 区域。选择退出某个区域并不能阻止您在该区域部署资源，但这些资源将不在 AWS Control Tower 的监管范围内。

在配置新区域期间，AWS Control Tower 会更新着陆区，这意味着它会对您的着陆区进行基准 —

- 在所有新选定的地区积极开展业务，以及
- 停止管理已取消选定地区的资源。

在此着陆区更新过程中，不会更新您的组织单位 (OU) 中由 AWS Control Tower 管理的个人账户。因此，您必须通过重新注册 OU 来更新您的帐户。

在配置 AWS Control Tower 区域时，请注意以下建议和限制：

- 选择您计划托管 AWS 资源或工作负载的区域。
- 选择退出某个区域并不能阻止您在该区域部署资源，但这些资源将不在 AWS Control Tower 的监管范围内。

当您为新区域配置着陆区时，AWS Control Tower 侦探控制将遵守以下规则：

- 存在的东西保持不变。防护机制行为（检测性以及预防性）在现有区域、现有 OU 中对于现有账户保持不变。
- 您不能对包含未更新的账户的现有 OU 应用新的侦探控制。将 AWS Control Tower 着陆区配置为新区域（通过更新着陆区）后，必须先更新现有 OU 中的现有账户，然后才能对这些 OU 和账户启用新的侦探控制。
- 更新账户后，您现有的侦探控件就会开始在新配置的区域中起作用。当您更新 AWS Control Tower 着陆区以配置新区域，然后更新账户时，已在 OU 上启用的侦探控件将开始在新配置的区域中对该账户起作用。

配置 AWS Control Tower 区域

1. 登录 AWS Control Tower 控制台，网址为 https://console.aws.amazon.com/controltower
2. 在左窗格导航菜单中，选择着陆区设置。
3. 在着陆区设置页面的详细信息部分，选择右上角的修改设置按钮。您将被引导到更新着陆区工作流程，因为管理新区域或从管理中移除区域需要您更新到最新的着陆区版本。
4. 在 “其他监管 AWS 区域” 下，搜索您想要管理（或停止治理）的区域。州/省 /市/自治区列显示您当前管理的区域，以及您不管理的区域。
5. 选中要管理的每个其他地区的复选框。取消选中要从中移除监管的每个地区的复选框。

> **Note**
>
> 如果您选择不管理某个区域，您仍然可以在该区域部署资源，但这些资源将不在 AWS Control Tower 的监管范围内。

6. 完成工作流程的其余部分，然后选择更新 landing zon e。
7. landing zone 设置完成后，重新注册 OU 以更新新区域中的账户。有关更多信息，请参阅 何时更新 AWS Control Tower 业务单元和账户。

配置新区域后，另一种配置或更新个人账户的方法是使用 S ervice Catalog 的 API 框架和批量更新账户。 AWS CLI有关更多信息，请参阅 使用自动化配置和更新账户。

配置区域时避免混合治理

在将 AWS Control Tower 管理范围扩展到新的 AWS Control Tower 管理范围之后 AWS 区域，以及从某个区域中移除 AWS Control Tower 监管之后，更新组织单位中的所有账户非常重要。

如果@@ 管理 OU 的控制与管理 OU 内每个账户的控制不完全匹配，则可能会出现混合治理的情况。如果在 AWS Control Tower 将监管范围扩展到新的或移除监管后仍未更新账户 AWS 区域，则组织单位中就会出现混合治理。

在这种情况下，与组织单位中的其他账户相比，或者与着陆区的整体治理状况相比，OU 中的某些账户在不同区域应用的控制措施可能有所不同。

在混合治理的 OU 中，如果您配置新账户，则该新账户将获得与 landing zone 相同的（更新）区域和组织单位治理状态。但是，尚未更新的现有账户不会收到更新的地区治理状况。

通常，混合治理可能会在 AWS Control Tower 控制台中创建矛盾或不准确的状态指标。例如，在混合治理期间，对于尚未更新的账户，选择加入区域在已注册的 OU 中显示为 “未受管辖” 状态。

> **Note**
>
> AWS Control Tower 不允许在混合治理状态下启用控件。

混合治理期间的控制行为

- 在混合治理期间，AWS Control Tower 无法在 OU 已显示为 “受管辖” 的区域中持续部署基于 AWS Config 规则（即侦探控件）的控件，因为 OU 中的某些账户尚未更新。您可能会收到一条`FAILED_TO_ENABLE`错误消息。
- 在混合治理期间，如果您在 OU 中的任何账户尚未更新时将着陆区域的管理范围扩展到可选区域，则在 OU 上的 `EnableControl` API 操作将失败，无法进行侦查和主动控制。您将收到一条`FAILED_TO_ENABLE`错误消息，因为 OU 中未更新的成员账户尚未被选入这些区域。
- 在混合治理期间，作为 Sec urity Hub 服务托管标准：AWS Control Tower 一部分的控制措施无法准确报告着陆区域配置与未更新的账户不匹配的区域的合规性。
- 混合治理不会改变基于 SCP 的控制（预防性控制）的行为，这些控制统一适用于每个受管辖区域中组织中的每个账户。

> **Note**
>
> 混合治理与漂移不同，也不被报告为漂移。

修复混合治理

- 为在控制台的 Organizations 页面上显示 “更新可用状态” 的 OU 中的每个账户选择 “更新账户”。
- 对于账户少于 300 的 OU，在 Organizations 页面上选择 “重新注册 OU”，这将自动更新 OU 中的所有账户。

激活 AWS 选择加入区域的注意事项

尽管默认情况下 AWS 区域 ，大多数区域都处于活动状态 AWS 账户，但某些区域只有在您手动选择时才会被激活。本文档将这些区域称为可选区域。相比之下，在创建后，默认处于活动状态的区域被称为商业区域，或者简称为 “区域”。 AWS 账户

“选择加入” 一词有其历史依据。2019 年 3 月 20 日之后 AWS 区域 推出的任何区域均被视为可选区域。在通过在选择加入区域中处于活跃状态的账户共享 IAM 数据方面，选择加入区域比商业区域具有更高的安全要求。通过 IAM 服务管理的所有数据均被视为身份数据，包括用户、群组、角色、策略、身份提供商、其关联数据（例如 X.509 签名证书或特定于上下文的证书）以及其他账户级别设置，例如密码策略和账户别名。

在设置着陆区期间，您可以通过选择选择加入区域来自动激活这些区域。您的着陆区在所有选定区域都处于活动状态。

如果您选择选择一个可选区域作为您的 AWS Control Tower 主区域，请在登录 AWS 管理控制台后，按照启用区域中的步骤先将其激活。要从选择加入的区域中引入您自己的现有日志存档和审核账户，请先手动激活该区域。

AWS 选择加入的区域包括几个可用 AWS Control Tower 的区域：

- 亚太地区（香港）区域，ap-east-1
- 亚太地区（雅加达）区域，ap-southeast-3
- 欧洲（米兰）区域，eu-south-1
- 非洲（开普敦）区域，af-south-1
- 中东（巴林）区域，me-south-1

- 以色列（特拉维夫），il-central-1
- 中东（阿联酋）区域，me-central-1
- 欧洲（西班牙）区域，eu-south-2
- 亚太地区（海得拉巴）区域，ap-south-2
- 欧洲（苏黎世）区域，eu-central-2
- 亚太地区（墨尔本）区域，ap-southeast-4
- 加拿大西部（卡尔加里）区域，ca-west-1

AWS Control Tower 有一些控件，这些控件在可选区域的工作方式与在商业区域中的工作方式不同。有关更多信息，请参阅 控制限制。在将工作负载部署到可选区域时，请记住以下注意事项。

> **治理还是激活？**
>
> 请记住，管理区域是您可以从 AWS Control Tower 控制台中选择的操作，以便在该区域中应用控制措施。激活或停用可选区域是你可以在控制台中选择的不同操作， AWS 控制台会向你的账户开放该区域，这样你就可以在该区域部署资源和工作负载。

行为注意事项

- 如果您选择管理可选区域，我们建议您不要停用（选择退出）任何受管控的选择加入区域，因为这可能会导致您的工作负载失败。AWS Control Tower 不允许从 AWS Control Tower 控制台中停用受管控区域，但请确保不要从 AWS 控制塔之外的来源（例如 AWS 账单控制台或 AWS 软件开发工具包）停用受管区域。
- 当 AWS Control Tower 将监管范围扩展到可选加入区域时，它会在所有成员账户中激活（选择加入）该区域。当您从管理中移除某个区域时，AWS Control Tower 不会在成员账户中停用（选择退出）该区域。
- 在取消选择区域期间，如果选择加入的区域已为来自 AWS Control Tower 以外的来源（例如账 AWS 单控制台或软件开发工具包）的账户手动停用该区域，AWS Control Tower 将跳过从该区域移除该资源的操作。 AWS 我们建议您从已停用的区域中移除资源，否则这些资源可能会收到意想不到的账单费用。
- 如果您的着陆区已停用，AWS Control Tower 会清理所有受监管区域（包括可选区域）中的资源。但是，AWS Control Tower 不会停用可选区域。停用后，您可以通过额外步骤停用可选区域。
- 如果您的主区域是可选区域，并且您打算将现有账户注册为日志存档和审计账户，则必须先手动激活选择加入区域，然后才能将其选择为着陆区域的主区域。请参阅启用区域。

- 如果 AWS Control Tower 设置为可选区域作为您的主区域，并且如果您从任何其他区域的控制 AWS 台访问 AWS Control Tower 服务，则控制台不会自动将您重定向到主区域。
- 底层 API 有容量限制，这可能会将延迟从几分钟增加到数小时，具体取决于区域、账户和服务负载的数量。作为最佳实践，请仅选择将要运行工作负载的 AWS 区域 区域，一次只能选择加入一个区域。

治理和控制的重要限制

- 如果您当前启用了选择加入区域不支持的 AWS Control Tower 控件，则在该区域支持该控件之前，您将无法将 AWS Control Tower 管理扩展到该选择加入区域。有关更多信息，请参阅 控制限制。
- 如果您将 AWS Control Tower 监管扩展到不支持特定控件的选择加入区域，则在您使用 AWS Control Tower 管理的所有区域都支持该控制之前，您将无法在任何区域启用该控件。有关更多信息，请参阅 控制限制
- 如果所有可用 AWS Control Tower 的 22 个商业区域（包括可选区域）都被激活，则在将监管范围扩展到 OU 时，每个组织单位 (OU) 的账户数量上限就会降低。限制为 220 个帐户，而不是 300 个帐户。这种减少是由于 StackSet局限性造成的。如果您需要将监管范围扩展到拥有超过 220 个账户的 OU，请减少激活区域的数量。

配置区域拒绝控制

AWS Control Tower 提供两种区域拒绝控制措施。激活后GRREGIONDENY，一个控件适用于整个着陆区。另一个控件在激活后CTMULTISERVICEPV1，可以应用于您指定的特定 OU。有关更多信息，请参阅AWS 根据请求拒绝访问 AWS 区域和应用于 OU 的区域拒绝控制。

Region deny 控制GRREGIONDENY是唯一的，因为它适用于整个着陆区，而不是任何特定的 OU。要配置区域拒绝控制，请转到着陆区域设置页面，然后选择修改设置。

- 此设置可以在以后更改。
- 启用后，此控件将应用于所有已注册的 OU。
- 无法为单个 OU 配置此控件。

> **Note**
>
> 在启用区域拒绝控制之前，请确保这些区域中没有现有资源，因为在应用控制后，您将无法访问您的资源。启用控件后，您将无法在被拒绝的区域部署资源。

根据您的 AWS Control Tower 区域配置，区域拒绝控制禁止访问 AWS 服务。它拒绝访问状态为 “未受管辖” 的 AWS 区域。区域拒绝控制还拒绝访问没有 AWS Control Tower 的区域。您不能拒绝访问您的家乡地区。某些全球 AWS 服务（例如 IAM 和 AWS Organizations）不受区域拒绝控制的约束。要了解更多信息，请参阅AWS 根据请求拒绝访问 AWS 区域。

启用该控件后，它将应用于层次结构中所有已注册的顶级 OU，并由链中较低的 OU 继承。当您移除控件时，所有注册的 OU 上的控件都会被移除，AWS Control Tower 中所有非受管理的区域都将保持不受管控状态，并且您可以在 AWS Control Tower 可用范围之外的区域部署资源。

- 完整控制名称： AWS 根据请求的 AWS 区域拒绝访问权限
- Guardrail 描述：禁止访问指定区域以外的全球和区域服务中的未列出的业务。
- 这是一种带有预防指导的选择性对照。

要查看区域拒绝控制 SCP 的模板，请参阅 AWS Control Tower Control 参考资料 AWS 区域中的请求拒绝访问。 AWS AWS Control Tower SCP 与 SCP 相似 AWS Organizations，但并不相同。

您可以在区域服务页面上确定区域服务终端节点。

OU 级别区域拒绝控制的注意事项

OU 级区域拒绝控制的主要考虑因素是确定如果两者都被激活，它将如何与着陆区域 Region deny 控件进行交互。有关更多信息，请参阅应用于 OU 的区域拒绝控制。

在 AWS Control Tower 中配置和管理账户

本章包括在 AWS Control Tower 着陆区中配置和管理成员账户的概述和程序。

它还包括将现有 AWS 账户注册到 AWS Control Tower 的概述和程序。

有关 AWS Control Tower 中账户的更多信息，请参阅AWS 账户 在 AWS Control Tower 中简介。有关将多个账户注册到 AWS Control Tower 的信息，请参阅。向 AWS Control Tower 注册现有组织单位

> **Note**
>
> 您最多可以同时执行五 (5) 项与账户相关的操作，包括配置、更新和注册。

资源调配方法

AWS Control Tower 提供了多种创建和更新成员账户的方法。有些方法主要是基于控制台的，有些方法主要是自动化的。

概述

创建成员账户的标准方法是通过 Account Factory，这是一款基于控制台的产品，属于服务目录。如果您的着陆区域未处于漂移状态，则可以使用创建账户作为从控制台添加新账户的方法，也可以使用注册账户将现有 AWS 账户注册到 AWS Control Tower。

借助 Account Factory，您可以依靠 AWS Control Tower 的默认设置来配置基本账户。您还可以配置满足特殊用例要求的自定义账户。

Account Factory 定制 (AFC) 是一种从 AWS Control Tower 控制台配置自定义账户的方法，它可以自动自定义和部署您的账户。它允许在执行一些一次性设置步骤后进行基于控制台的自动配置，从而无需编写脚本或设置管道。有关更多信息，请参阅 使用 Account Factory 自定义 (AFC) 自定义账户。

基于控制台的方法：

- 通过属于基本账户或自定义账户的 Accoun AWS Service Catalog t Factory 控制台。查看使用 Account Factory 配置和管理账户详情和说明。
- 如果您的着陆区未处于漂移状态，请通过 AWS Control Tower 中的注册账户功能。请参阅 注册现有账户。

- 在 AWS Control Tower 控制台中，您可以使用 Account Factory 同时创建、更新或注册最多五个账户。

自动化方法：

- Lambda 代码：使用 Lambda 代码和相应的 IAM 角色从您的 AWS Control Tower 着陆区域的管理账户中获取。请参阅使用 IAM 角色自动配置账户。
- Terraform：来自适用于 Terraform 的 AWS Control Tower Account Factory (AFT)，该工厂依靠账户工厂和 GitOps 模型来实现账户配置和更新的自动化。请参阅 使用适用于 Terraform 的 AWS Control Tower Account Factory（AFT）配置账户 。
- 在 AWS Control Tower 控制台中自定义账户：完成设置步骤后，将来配置自定义账户无需额外的配置或管道维护。账户是通过名为蓝图 AWS Service Catalog 的产品进行配置的。蓝图可以使用 AWS CloudFormation 模板或 Terraform 模板。

> **Note**
>
> AWS CloudFormation 蓝图可以将资源部署到多个区域。Terraform 蓝图只能将资源部署到单个区域。默认情况下，这是主区域。

AWS Control Tower 创建账户后会发生什么

AWS Control Tower 中的新账户是通过 AWS Control Tower、 AWS Organizations、和之间的交互创建和 AWS Service Catalog配置的。有关 AWS 账户 使用 AWS Control Tower 控制台注册现有控制台的步骤，请参阅注册现有账户。

账号创建的幕后花絮

1. 例如，您可以从 AWS Control Tower Account Factory 页面发起请求，或者直接从 AWS Service Catalog 控制台发起请求，或者通过调用 Service Catalog `ProvisionProduct` API 发起请求。
2. AWS Service Catalog 致电 AWS Control Tower。
3. AWS Control Tower 启动了一个工作流程，该工作流程作为第一步调用 AWS Organizations `CreateAccount` API。
4. AWS Organizations 创建账户后，AWS Control Tower 通过应用蓝图和控制来完成配置过程。
5. Service Catalog 继续对 AWS Control Tower 进行轮询，以检查配置过程是否已完成。

6. AWS Control Tower 中的工作流程完成后，Service Catalog 会最终确定账户的状态并将结果通知您（请求者）。

账户所需的权限

每个部分分别讨论了每种配置和更新账户的方法所需的权限。有了相应的用户组权限，供应商就可以为其组织中的任何账户指定标准化基准和网络配置。

> **Note**
>
> 配置账户时，账户申请者必须始终拥有`CreateAccount`和`DescribeCreateAccountStatus`权限。此权限集是管理员角色的一部分，当请求者担任管理员角色时，它会自动授予。如果您委托配置账户的权限，则可能需要直接为账户申请者添加这些权限。

当您通过 AWS Control Tower 控制台使用 Account Factory 创建账户时，您必须使用启用该`AWSServiceCatalogEndUserFullAccess`策略的 IAM 用户登录账户，并拥有使用 AWS Control Tower 控制台的权限，并且您不能以根用户身份登录。

有关 AWS Control Tower 所需权限的一般信息，请参阅在 AWS Control Tower 中使用基于身份的策略（IAM 策略）。有关 AWS Control Tower 中角色和账户的信息，请参阅角色和账户。

> **为您的账户提供安全保障**
>
> 您可以在 AWS Organizations 文档中找到有关保护 AWS Control Tower 管理账户和成员账户安全的最佳实践指南。
>
> - 管理账户的最佳实践
> - 成员账户的最佳实践

AWS 账户 在 AWS Control Tower 中简介

AWS 账户 是您拥有的所有资源的容器。这些资源包括账户接受的 AWS Identity and Access Management (IAM) 身份，这些身份决定了谁有权访问该账户。IAM 身份可以包括用户、群组、角色等。有关在 AWS Control Tower 中使用 IAM、用户、角色和策略的更多信息，请参阅 AWS Cont rol Tower 中的身份和访问管理。

资源和账户创建时间

当 AWS Control Tower 创建或注册账户时，它会部署该账户所需的最低资源配置，包括账户工厂模板形式的资源和着陆区中的其他资源。这些资源可能包括 IAM 角色、 AWS CloudTrail 跟踪、S ervice Catalog 预配置产品和 IAM 身份中心用户。AWS Control Tower 还根据控制配置的要求为新账户将成为成员账户的组织单位 (OU) 部署资源。

AWS Control Tower 代表您协调这些资源的部署。每个资源可能需要几分钟才能完成部署，因此请考虑创建或注册账户之前的总时间。有关管理账户资源的更多信息，请参阅创建和修改 AWS Control Tower 资源的指南。

引入现有安全账户或日志账户的注意事项

在接受 AWS 账户 作为安全账户或日志账户之前，AWS Control Tower 会检查该账户中是否有与 AWS Control Tower 要求相冲突的资源。例如，您可能有一个与 AWS Control Tower 要求的名称相同的日志存储桶。此外，AWS Control Tower 还会验证账户是否可以配置资源；例如，通过确保启用 AWS Security Token Service (AWS STS)、账户未被暂停以及 AWS Control Tower 有权在账户内配置资源。

AWS Control Tower 不会删除您提供的日志和安全账户中的任何现有资源。但是，如果您选择启用 AWS 区域 拒绝功能，则区域拒绝控制会阻止访问被拒绝区域中的资源。

查看您的账户

组织页面列出了您组织中的所有 OU 和账户，无论组织单位或在 AWS Control Tower 中的注册状态如何。如果每个账户都满足注册的先决条件，则可以单独或按组织单位组查看和注册 AWS Control Tower。

要在组织页面上查看特定账户，您可以从右上角的下拉菜单中选择 “仅限账户”，然后从表格中选择您的账户名称。或者，您可以从表格中选择父 OU 的名称，然后在该 OU 的 “详细信息” 页面上查看该 OU 内所有账户的列表。

在组织页面和账户详情页面上，您可以看到账户的状态，这是以下状态之一：

- 未注册 — 该账户是父 OU 的成员，但不完全由 AWS Control Tower 管理。如果父 OU 已注册，则该账户受为其注册的父 OU 配置的预防性控制措施的约束，但是 OU 的侦探控制不适用于此账户。如果父 OU 未注册，则没有任何控制适用于此账户。
- 注册 — AWS Control Tower 正在对该账户进行管理。我们正在使账户与父 OU 的控制配置保持一致。对于每个账户资源，此过程可能需要几分钟。
- 已注册 — 该账户受为其父 OU 配置的控件控制。它完全由 AWS Control Tower 管理。

- 注册失败 — 该账户无法在 AWS Control Tower 中注册。有关更多信息，请参阅 注册失败的常见原因。
- 更新可用-该账户有可用的更新。处于此状态的账户仍处于已注册状态，但必须更新账户以反映最近对您的环境所做的更改。要更新单个账户，请导航至账户详情页面，然后选择更新账户。

  如果您在一个 OU 下有多个处于此状态的账户，则可以选择重新注册 OU 并一起更新这些账户。

在共享账户中创建的资源

本节显示了在您设置着陆区时 AWS Control Tower 在共享账户中创建的资源。

有关成员账户资源的信息，请参阅Account Factory 的资源注意事项。

管理账户资源

设置 landing zone 时，将在您的管理账户中创建以下 AWS 资源。

AWS 服务	资源类型	资源名称
AWS Organizations	账户	audit log archive
AWS Organizations	OU	Security Sandbox
AWS Organizations	服务控制策略	aws-guardrails-*
AWS CloudFormation	堆栈	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER（在 2.6 及更高版本中）
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL（未在 3.0 及更高版本中部署）

AWS 服务	资源类型	资源名称
		AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later)
		AWSControlTowerBP-BASELINE-CLOUDWATCH
		AWSControlTowerBP-BASELINE-CONFIG
		AWSControlTowerBP-BASELINE-ROLES
		AWSControlTowerBP-BASELINE-SERVICE-ROLES
		AWSControlTowerBP-SECURITY-TOPICS
		AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED
		AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED
		AWSControlTowerLoggingResources
		AWSControlTowerSecurityResources
		AWSControlTowerExecutionRole

AWS 服务	资源类型	资源名称
AWS Service Catalog	产品	AWS Control Tower Account Factory
AWS Config	聚合器	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	试用	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch 日志	aws-controltower/CloudTrail Logs
AWS Identity and Access Management	角色	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	策略	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

AWS 服务	资源类型	资源名称
AWS IAM Identity Center	目录组	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS IAM Identity Center	权限集	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

> **Note**
>
> 未在 AWS CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL` landing zone 版本 3.0 或更高版本中部署。但是，在您更新着陆区之前，它会继续存在于早期版本的着陆区中。

日志存档账户资源

设置 landing zone 时，将在您的日志存档账户中创建以下 AWS 资源。

AWS 服务	资源类型	资源名称
AWS CloudFormation	堆栈	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-BASELINE-ROLES-

AWS 服务	资源类型	资源名称
		StackSet-AWSControlTowerLoggingResources-
AWS Config	AWS Config 规则	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT
AWS CloudTrail	跟踪	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch 赛事规则	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch 日志	/aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	角色	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution

AWS 服务	资源类型	资源名称
AWS Identity and Access Management	策略	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	主题	aws-controltower-SecurityNotifications
AWS Lambda	应用程序	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	函数	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	存储桶	aws-controltower-logs-* aws-controltower-s3-access-logs-*

审计账户资源

设置 landing zone 时，将在您的审核账户中创建以下 AWS 资源。

AWS 服务	资源类型	资源名称
AWS CloudFormation	堆栈	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED-

AWS 服务	资源类型	资源名称
		StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerSecurityResources-*
AWS Config	聚合器	aws-controltower-GuardrailsComplianceAggregator

AWS 服务	资源类型	资源名称
AWS Config	AWS Config 规则	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	试用	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch 赛事规则	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch 日志	/aws/lambda/aws-controltower-NotificationForwarder

AWS 服务	资源类型	资源名称
AWS Identity and Access Management	角色	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole aws-controltower-AuditAdministratorRole aws-controltower-AuditReadOnlyRole AWSControlTowerExecution
AWS Identity and Access Management	策略	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	主题	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications
AWS Lambda	函数	aws-controltower-NotificationForwarder

关于共享账户

三个特殊 AWS 账户 账户与 AWS Control Tower 关联：管理账户、审计账户和日志存档账户。这些账户通常被称为共享账户，有时也被称为核心账户。

- 在设置 landing zone 时，您可以为审核和日志存档帐户选择自定义名称。有关更改账户名称的信息，请参阅从外部更改 AWS Control Tower 资源名称。
- 在最初的着陆区设置过程中，您还可以将现有账户指定 AWS 账户 为 AWS Control Tower 安全账户或日志账户。此选项使得 AWS Control Tower 无需创建新的共享账户。（这是一次性选择。）

有关共享账户及其关联资源的更多信息，请参阅在共享账户中创建的资源。

管理账户

这将 AWS 账户 启动 AWS Control Tower。默认情况下，该账户的根用户和该账户的 IAM 用户或 IAM 管理员用户拥有对您的 landing zone 内所有资源的完全访问权限。

> **Note**
>
> 作为最佳实践，我们建议在 AWS Control Tower 控制台中执行管理功能时以具有管理员权限的 IAM 身份中心用户身份登录，而不是以该账户的根用户或 IAM 管理员用户身份登录。

有关管理账户中可用角色和资源的更多信息，请参阅在共享账户中创建的资源。

日志存档账户

日志存档共享账户是在您创建 landing zone 时自动设置的。

此账户包含一个中央 Amazon S3 存储桶，用于存储您的着陆区中所有其他账户的副本 AWS CloudTrail 和所有其他账户的 AWS Config 日志文件。作为最佳实践，我们建议限制负责合规和调查的团队及其相关安全或审计工具访问日志存档帐户。此账户可用于自动安全审计，也可用于托管自定义 AWS Config 规则函数（例如 Lambda 函数）以执行补救操作。

> **亚马逊 S3 存储桶政策**
>
> 对于 AWS Control Tower landing zone 版本 3.3 及更高版本，账户必须满足对审核存储桶的任何写入权限的`aws:SourceOrgID`条件。此条件可确保 CloudTrail 只有代表组织内的账户才

能将日志写入您的 S3 存储桶；它可以防止组织外部的 CloudTrail 日志写入您的 AWS Control Tower S3 存储桶。有关更多信息，请参阅 AWS Control Tower 着陆区版本 3.3。

有关日志存档账户中可用角色和资源的更多信息，请参阅 日志存档账户资源

> **Note**
>
> 这些日志无法更改。存储所有日志的目的都是为了进行与账户活动相关的审计和合规调查。

审计账户

此共享账户是在您创建着陆区时自动设置的。

审计账户应仅限于具有审核员（只读）和管理员（完全访问权限）跨账户角色的安全与合规团队，他们可以在 landing zone 中使用所有账户。这些角色旨在供安全与合规团队用于：

- 通过 AWS 机制（例如托管自定义 AWS Config 规则 Lambda 函数）执行审计。
- 执行自动安全操作，例如补救措施。

审计账户还通过亚马逊简单通知服务 (Amazon SNS) Service 服务接收通知。可以接收三类通知：

- 所有配置事件 — 本主题汇总了您的 landing zone 中所有账户的所有 CloudTrail 和 AWS Config 通知。
- 聚合安全通知-此主题汇总了来自特定 CloudWatch 事件、合 AWS Config 规则 规性状态变更事件和 GuardDuty 发现的所有安全通知。
- 漂移通知 — 本主题汇总了在您的 landing zone 中的所有账户、用户、OU 和 SCP 中发现的所有漂移警告。有关漂移的更多信息，请参阅在 AWS Control Tower 中检测并解决偏差。

在成员账户内触发的审计通知也可以向本地 Amazon SNS 主题发送提醒。此功能允许账户管理员订阅特定于个人成员账户的审计通知。因此，管理员可以解决影响个人账户的问题，同时仍可将所有账户通知汇总到您的集中审计账户。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南。

有关审计账户中可用角色和资源的更多信息，请参阅审计账户资源。

有关编程审计的更多信息，请参阅 AWS Control Tower 审计账户的编程角色和信任关系。

> **Important**
>
> 您为审计账户提供的电子邮件地址会收到来自 AWS Control Tower 所有 AWS 区域 支持者的AWS 通知-订阅确认电子邮件。要在您的审计账户中接收合规电子邮件，您必须从 AWS Control Tower AWS 区域 支持的每封电子邮件中选择 “确认订阅” 链接。

关于成员账号

成员账户是指您的用户用来执行其 AWS 工作负载的账户。这些成员账户可以在 Account Factory 中创建，也可以由具有管理员权限的 IAM Identity Center 用户在 Service Catalog 控制台中创建，也可以通过自动方法创建。创建后，这些成员账户存在于在 AWS Control Tower 控制台中创建或在 AWS Control Tower 注册的 OU 中。有关更多信息，请参阅以下相关主题：

- 使用 Account Factory 配置和管理账户
- 在 AWS Control Tower 中自动执行任务
- AWS 《AWS Organizations 用户指南》中的 Organizations 术语和概念。

另请参阅 使用适用于 Terraform 的 AWS Control Tower Account Factory（AFT）配置账户 。

> **账户和控件**
>
> 成员账户可以在 AWS Control Tower 中注册，也可以取消注册。控制措施对已注册和未注册帐户的适用方式不同，并且根据继承情况，控制措施可能适用于嵌套 OU 中的帐户。

有关 AWS Control Tower 分配的成员账户资源的信息，请参阅Account Factory 的资源注意事项。

注册现有的 AWS 账户

您可以将 AWS Control Tower 的监管范围扩展到个人， AWS 账户 当您将个人注册到已经由 AWS Control Tower 管理的组织单位 (OU) 时，该组织就存在了。符合条件的账户存在于未注册的 OU 中，这些组织与 AWS Control Tower OU 属于同一个 AWS Organizations 组织。

> **Note**
>
> 除非在初始 landing zone 设置期间，否则您无法注册现有账户作为审核或日志存档账户。

首先设置可信访问权限

在 AWS 账户 将现有账户注册到 AWS Control Tower 之前，您必须授予 AWS Control Tower 管理或监管账户的权限。具体而言，AWS Control Tower 需要获得权限才能 AWS Organizations 在您之间 AWS CloudFormation 和代表您之间建立 AWS CloudFormation 可信访问权限，这样才能将您的堆栈自动部署到所选组织中的账户。凭借这种可信访问权限，该AWSControlTowerExecution角色可以开展管理每个账户所需的活动。因此，在注册之前，您必须将此角色添加到每个账户。

启用可信访问后，只需一次操作 AWS CloudFormation 即可跨多个账户创建、更新或删除堆栈。 AWS 区域 AWS Control Tower 依靠这种信任功能，因此它可以在将现有账户转移到注册的组织单位之前，将角色和权限应用于现有账户，从而对其进行管理。

要了解有关可信访问和的更多信息 AWS CloudFormation StackSets，请参阅AWS CloudFormationStackSets和 AWS Organizations。

账户注册期间会发生什么

在注册过程中，AWS Control Tower 会执行以下操作：

- 为账户设定基准，包括部署以下堆栈集：
  - AWSControlTowerBP-BASELINE-CLOUDTRAIL
  - AWSControlTowerBP-BASELINE-CLOUDWATCH
  - AWSControlTowerBP-BASELINE-CONFIG
  - AWSControlTowerBP-BASELINE-ROLES
  - AWSControlTowerBP-BASELINE-SERVICE-ROLES
  - AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES
  - AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1

  最好查看这些堆栈集的模板，并确保它们不会与现有策略冲突。
- 通过 AWS IAM Identity Center 或识别账户 AWS Organizations。
- 将账户放入您指定的 OU 中。请确保应用当前 OU 中应用的所有 SCP，以便您的安全状况保持一致。
- 通过适用于整个选定组织单位的 SCP 对账户应用强制控制。
- 启用 AWS Config 并配置它以记录账户中的所有资源。
- 添加将 AWS Control Tower 侦探控件应用于账户的 AWS Config 规则。

账户和组织级别的跟踪 CloudTrail

无论是否注册，OU 中的所有成员账户都受该 OU 的 AWS CloudTrail 跟踪控制：

- 当您将账户注册到 AWS Control Tower 时，您的账户将受新组织的 AWS CloudTrail 跟踪管理。如果您已经部署了 CloudTrail 跟踪，则可能会看到重复的费用，除非您在将其注册到 AWS Control Tower 之前删除该账户的现有跟踪。
- 如果您将账户转移到注册的 OU（例如通过控制 AWS Organizations 台），但您没有继续将该账户注册到 AWS Control Tower，则您可能希望删除该账户的所有剩余账户级别跟踪。如果您已经部署了 CloudTrail 跟踪，则会产生重复的 CloudTrail 费用。

如果您更新了着陆区并选择退出组织级别的跟踪，或者您的着陆区版本低于 3.0，则组织级别的 CloudTrail跟踪不适用于您的账户。

在 VPC 中注册现有账户

当您在 Account Factory 中配置新账户时，AWS Control Tower 对 VPC 的处理方式与注册现有账户时不同。

- 当您创建新账户时，AWS Control Tower 会自动删除 AWS 默认 VPC 并为该账户创建一个新的 VPC。
- 当您注册现有账户时，AWS Control Tower 不会为该账户创建新的 VPC。
- 当您注册现有账户时，AWS Control Tower 不会删除与该账户关联的任何现有 VPC 或 AWS 默认 VPC。

Tip

您可以通过配置 Account Factory 来更改新账户的默认行为，因此默认情况下，它不会在 AWS Control Tower 下为您组织中的账户设置 VPC。有关更多信息，请参阅 在没有 VPC 的 AWS Control Tower 中创建账户。

注册的先决条件

要在 AWS Control Tower AWS 账户 中注册现有的，必须具备以下先决条件：

1. 要注册现有账户 AWS 账户，该AWSControlTowerExecution角色必须存在于您注册的账户中。您可以查看注册账户以了解详细信息和说明。
2. 除AWSControlTowerExecution角色外， AWS 账户 您要注册的现有角色还必须具有以下权限和信任关系。否则，注册将失败。

   角色权限:AdministratorAccess（AWS 托管策略）

   角色信任关系：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::Management Account ID:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. 我们建议该账户不应有 AWS Config 配置记录器或传送渠道。 AWS CLI 在您注册帐户之前，可以通过删除或修改这些内容。否则，请查看注册拥有现有 AWS Config 资源的账户，了解如何修改现有资源的说明。
4. 您想要注册的账户必须与 AWS Control Tower 管理账户位于同一个 AWS Organizations 组织中。存在的账户只能在已在 AWS Control Tower 注册的 OU 中注册到与 AWS Control Tower 管理账户相同的组织中。

要查看注册的其他先决条件，请参阅 AWS Control Tower 入门。

> **Note**
>
> 当您向 AWS Control Tower 注册账户时，您的账户将受 AWS Control Tower 组织的 AWS CloudTrail 跟踪管理。如果您已经部署了 CloudTrail跟踪，则可能会看到重复的费用，除非您在将其注册到 AWS Control Tower 之前删除该账户的现有跟踪。

注册现有账户

AWS Control Tower 控制台中提供了注册账户功能，用于注册现有账户， AWS 账户 使其受 AWS Control Tower 的管理。有关更多信息，请参阅注册现有的 AWS 账户。

当您的 landing zone 未处于漂移状态时，可以使用 Enrol l 账户功能。要在控制台中查看此功能，请执行以下操作：

- 导航到 AWS Control Tower 中的组织页面。
- 找到您要注册的账户的名称。要找到它，请从右上角的下拉菜单中选择 “仅限账户”，然后在筛选后的表格中找到账户名称。
- 按照注册个人账户的步骤进行操作，如注册账户的步骤部分所示。

> **Note**
>
> 注册现有电子邮件地址时 AWS 账户，请务必验证现有的电子邮件地址。否则，可能会创建一个新帐户。

某些错误可能要求您刷新页面并重试。如果您的登录区处于偏差状态，您可能无法成功使用 Enroll account (注册账户) 功能。在着陆区漂移问题得到解决之前，你需要通过 Account Factory 配置新账户。

当您从 AWS Control Tower 控制台注册账户时，您必须使用启用该`AWSServiceCatalogEndUserFullAccess`策略的用户登录账户，并拥有管理员访问权限才能使用 AWS Control Tower 控制台，并且您不能以根用户身份登录。

您注册的账户可以通过 AWS Service Catalog 和 AWS Control Tower 账户工厂进行更新，就像更新任何其他账户一样。更新过程在名为使用 AWS Control Tower 或使用 AWS Control Tower 更新和移动账户工厂账户 AWS Service Catalog的部分中给出。

注册账户的步骤

在您的现有账户中设置AdministratorAccess权限（政策）后，请按照以下步骤注册该账户：

在 AWS Control Tower 中注册个人账户

- 导航到 AWS Control Tower 组织页面。

- 在组织页面上，符合注册资格的账户允许您从该部分顶部的操作下拉菜单中选择注册。当您在账户详情页面查看这些账户时，它们还会显示注册账户按钮。
- 当你选择注册账户时，你会看到一个注册账户页面，系统会提示你将该AWSControlTowerExecution角色添加到账户。有关一些说明，请参阅手动将所需的 IAM 角色添加到现有角色 AWS 账户 并进行注册。
- 接下来，从下拉列表中选择已注册的 OU。如果该账户已在注册的 OU 中，则此列表将显示 OU。
- 选择 Enroll account (注册账户)。
- 你会看到一个模态提醒，提醒你添加AWSControlTowerExecution角色并确认操作。
- 选择 “注册”。
- AWS Control Tower 开始注册流程，您将被引导回到账户详情页面。

注册失败的常见原因

- 要注册现有账户，该AWSControlTowerExecution角色必须存在于您注册的账户中。
- 您的 IAM 委托人可能缺乏预置账户所需的权限。
- AWS Security Token Service (AWS STS) AWS 账户 在您所在的地区或 AWS Control Tower 支持的任何区域中被禁用。
- 您登录的账户可能需要添加到 Account Factory Portfolio 中 AWS Service Catalog。必须先添加账户，然后才能访问 Account Factory，这样您才能在 AWS Control Tower 中创建或注册账户。如果未将相应的用户或角色添加到 Account Factory 产品组合中，则在尝试添加账户时会收到错误消息。有关如何授予对 AWS Service Catalog 投资组合的访问权限的说明，请参阅向用户授予访问权限。
- 您可以用 root 用户身份登录。
- 您尝试注册的账户可能有剩余 AWS Config 设置。特别是，该账户可能有配置记录器或传送渠道。必须先通过删除或修改这些 AWS CLI 信息，然后才能注册账户。有关更多信息，请参阅 注册拥有现有 AWS Config 资源的账户 和 与 AWS Control Tower 使用进行交互 AWS CloudShell。
- 如果该账户属于具有管理账户的另一个 OU，包括另一个 AWS Control Tower OU，则必须先在其当前 OU 中终止该账户，然后它才能加入另一个 OU。必须移除原始 OU 中的现有资源。否则，注册将失败。
- 如果您的目标 OU 的 SCP 不允许您创建该账户所需的所有资源，则账户配置和注册将失败。例如，目标 OU 中的 SCP 可能会在没有特定标签的情况下阻止资源创建。在这种情况下，账户配置或注册会失败，因为 AWS Control Tower 不支持对资源进行标记。如需帮助，请联系您的客户代表，或 AWS Support。

有关创建新账户或注册现有账户时 AWS Control Tower 如何使用角色的更多信息，请参阅角色和账户。

> **Tip**
>
> 如果您无法确认现有组织是否 AWS 账户 满足注册先决条件，则可以设置注册 OU 并将该账户注册到该 OU。注册成功后，您可以将账户转移到所需的 OU。如果注册失败，则该失败不会影响其他账户或 OU。

如果您怀疑自己的现有账户及其配置是否与 AWS Control Tower 兼容，可以遵循下一节中推荐的最佳实践。

建议：您可以设置一个包含两个步骤的账户注册方法

- 首先，使用 AWS Config 一致性包来评估某些 AWS Con trol Tower 控制措施可能如何影响您的账户。要确定注册 AWS Control Tower 会如何影响您的账户，请参阅使用 AWS Config 一致性包扩展 AWS Control Tower 的治理。
- 接下来，您可能希望注册该账户。如果合规性结果令人满意，迁移路径会更容易，因为您可以注册账户而不会产生意外后果。
- 完成评估后，如果您决定设置 AWS Control Tower 着陆区，则可能需要移除为评估而创建的 AWS Config 交付渠道和配置记录器。然后，您将能够成功设置 AWS Control Tower。

> **Note**
>
> 合规包也适用于账户位于 AWS Control Tower 注册的 OU 中，但工作负载在不支持 AWS Control Tower 的 AWS 区域内运行的情况。您可以使用一致性包来管理未部署 AWS Control Tower 的区域中存在的账户中的资源。

如果账户不符合先决条件怎么办？

请记住，作为先决条件，有资格加入 AWS Control Tower 治理的账户必须属于同一个整体组织。要满足账户注册的这一先决条件，您可以按照以下准备步骤将账户转移到与 AWS Control Tower 相同的组织中。

将账户引入与 AWS Control Tower 相同的组织的准备步骤

1. 将该账户从其现有组织中删除。如果您使用这种方式，则必须提供单独的付款方式。
2. 邀请该账户加入 AWS Control Tower 组织。有关更多信息，请参阅AWS Organizations 用户指南中的邀请 AWS 账户加入您的组织。
3. 接受邀请。该帐户显示在组织的根目录中。此步骤将账户转移到与 AWS Control Tower 相同的组织中。并建立 SCP 和整合账单。

> **Tip**
>
> 您可以在账户退出旧组织之前，向新组织发送邀请。当该账户正式退出其现有组织时，将等待邀请。

满足其余先决条件的步骤：

1. 创建必要的`AWSControlTowerExecution`角色。
2. 清除默认 VPC。（这部分是可选的。 AWS Control Tower 不会更改您现有的默认 VPC。）
3. 通过或删除或修改任何现有的 AWS Config 配置记录器或传送渠道 AWS CloudShell。 AWS CLI 有关更多信息，请参阅资源状态的 AWS Config CLI 命令示例和注册拥有现有 AWS Config 资源的账户

完成这些准备步骤后，您可以将该账户注册到 AWS Control Tower。有关更多信息，请参阅 注册账户的步骤。此步骤使该账户进入全面的 AWS Control Tower 管理状态。

取消配置账户的可选步骤，使其可以注册并保留其堆栈

1. 要保留应用的 AWS CloudFormation 堆栈，请从堆栈集中删除堆栈实例，然后为该实例选择保留堆栈。
2. 在 Account Factory 中终止 AWS Service Catalog 账户配置的产品。（此步骤仅从 AWS Control Tower 中移除已配置的产品。 它不会删除该帐户。）
3. 根据任何不属于组织的账户的要求，使用必要的账单详细信息设置账户。然后将该账户从组织中移除。（您这样做，这样账户就不会计入您的 AWS Organizations 配额总额。）
4. 如果仍有资源，请清理账户，然后按照中的账户关闭步骤将其关闭取消账户管理。
5. 如果您有一个带有已定义控件的暂停 OU，则可以将账户移到该处，而不必执行步骤 1。

资源状态的 AWS Config CLI 命令示例

以下是一些用于确定配置记录器和传送渠道状态的 AWS Config CLI 命令示例。

查看命令：

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

正常的反应是这样的 `"name": "default"`

删除命令：

- `aws configservice stop-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-delivery-channel --delivery-channel-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*

手动将所需的 IAM 角色添加到现有角色 AWS 账户 并进行注册

如果您已经设置了 AWS Control Tower 着陆区，则可以开始将贵组织的账户注册到已在 AWS Control Tower 注册的 OU 中。如果您尚未设置着陆区，请按照 AWS Control Tower 用户指南入门步骤 2 中所述的步骤进行操作。着陆区准备就绪后，手动完成以下步骤，让 AWS Control Tower 对现有账户进行管理。

请务必阅读本章前面注册的先决条件提到的内容。

在 AWS Control Tower 注册账户之前，您必须向 AWS Control Tower 授予管理该账户的权限。为此，您需要添加一个对账户具有完全访问权限的角色，如以下步骤所示。必须对您注册的每个账户执行这些步骤。

对于每个账户：

步骤 1：以管理员权限登录当前包含您要注册的帐户的组织的管理帐户。

例如，如果您从中创建此账户， AWS Organizations 并使用跨账户 IAM 角色登录，则可以按照以下步骤操作：

1. 登录贵组织的管理账户。
2. 转到 AWS Organizations。
3. 在 “帐户” 下，选择您要注册的账户并复制其账户 ID。
4. 打开顶部导航栏上的账户下拉菜单，然后选择切换角色。
5. 在 Switch 角色表单上，填写以下字段：
   - 在 “账户” 下，输入您复制的账户 ID。
   - 在角色下，输入允许跨账户访问此账户的 IAM 角色的名称。该角色的名称是在创建账户时定义的。如果您在创建账户时未指定角色名称，请输入默认角色名称`OrganizationAccountAccessRole`。
6. 选择 Switch Role。
7. 现在，您应该以子女 AWS Management Console 身份登录帐户。
8. 完成后，请留在子女账户中进行下一部分的手术。
9. 记下管理账户 ID，因为您需要在下一步中输入它。

第 2 步：授予 AWS Control Tower 管理账户的权限。

1. 前往 IAM。
2. 转到 “角色”。
3. 选择 创建角色。
4. 当系统要求选择该角色的服务时，请选择自定义信任策略。
5. 复制此处显示的代码示例，然后将其粘贴到政策文档中。将该字符串*`Management Account ID`*替换为管理账户的实际管理账户 ID。以下是要粘贴的政策：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
      "Effect":"Allow",
      "Principal":{
         "AWS": "arn:aws:iam::Management Account ID:root"
         },
```

```
        "Action": "sts:AssumeRole",
        "Condition": {}
    }
  ]
}
```

6. 当被要求附加政策时，选择AdministratorAccess。
7. 选择下一步: 标签。
8. 您可能会看到一个标题为 “添加标签” 的可选屏幕。选择 “下一步” 暂时跳过此屏幕：Review
9. 在 “查看” 屏幕上，在 “角色名称” 字段中输入`AWSControlTowerExecution`。
10. 在描述框中输入简短描述，例如允许注册时具有完全的帐户访问权限。
11. 选择 创建角色。

第 3 步：通过将账户转移到已注册的 OU 来注册账户，然后验证注册。

通过创建角色设置必要权限后，请按照以下步骤注册账户并验证注册。

1. 再次以管理员身份登录并前往 AWS Control Tower。
2. 注册账户。
   - 在 AWS Control Tower 的组织页面中，选择您的账户，然后从右上角的操作下拉菜单中选择注册。
   - 按照注册账户的步骤页面上显示的注册个人账户的步骤进行操作。
3. 验证注册。
   - 在 AWS Control Tower 中，选择左侧导航栏中的组织。
   - 查找您最近注册的账户。其初始状态将显示为 “正在注册”。
   - 当状态更改为 “已注册” 时，移动成功。

要继续此过程，请登录贵组织中您想要在 AWS Control Tower 中注册的每个账户。对每个账户重复前提步骤和注册步骤。

自动注册 AWS Organizations 账户

您可以使用名为 “将现有 AWS 账户注册到 AWS Control Tower” 的博客文章中描述的注册方法，通过编程流程将您的 AWS Organizations 账户注册到 AWS Control Tower。

以下 YAML 模板可以帮助您在账户中创建所需的角色，以便可以通过编程方式进行注册。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: AWSControlTowerExecution
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS:
                - !Ref AdministratorAccountId
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

注册拥有现有 AWS Config 资源的账户

本主题提供了一种如何注册拥有现有 AWS Config 资源的账户 step-by-step 的方法。有关如何检查现有资源的示例，请参阅资源状态的 AWS Config CLI 命令示例。

> **Note**
>
> 如果您计划将现有 AWS 账户作为审计和日志存档账户引入 AWS Control Tower，并且这些账户具有现有 AWS Config 资源，则必须完全删除现有 AWS Config 资源，然后才能将这些账户注册到 AWS Control Tower 以实现此目的。对于不打算成为审计和日志存档帐户的帐户，您可以修改现有的 Config 资源。

AWS Config 资源示例

以下是您的账户可能已经拥有的一些 AWS Config 资源类型。可能需要对这些资源进行修改，以便您可以将您的账户注册到 AWS Control Tower。

- AWS Config 录音机
- AWS Config 配送渠道
- AWS Config 聚合授权

假设

- 您已经部署了 AWS Control Tower 着陆区
- 您的账户尚未注册 AWS Control Tower。
- 您的账户在管理账户管理的至少一个 AWS Control Tower 区域中至少有一个预先存在的 AWS Config 资源。
- 您的账户不是 AWS Control Tower 管理账户。
- 您的账户未处于治理偏离状态。

有关描述使用现有资源注册账户的自动方法的博客，请参阅使用现有 AWS Config 资源自动将账户注册到 AWS Control Tower。 AWS Config 您将能够为所有想要注册的账户提交一份支持请求，如以下所第 1 步：联系客户支持并提交工单，将该账户添加到 AWS Control Tower 允许名单述。

限制

- 只有通过使用 AWS Control Tower 工作流程来扩大监管范围才能注册该账户。
- 如果资源被修改并在账户上造成偏差，AWS Control Tower 不会更新资源。
- AWS Config 不受 AWS Control Tower 管理的区域中的资源不会发生变化。

> **Note**
>
> 如果您尝试注册拥有现有 Config 资源的账户，但未将该账户添加到允许列表，则注册将失败。此后，如果您随后尝试将该账户添加到允许列表中，AWS Control Tower 将无法验证该账户的配置是否正确。您必须先从 AWS Control Tower 取消配置账户，然后才能申请允许列表并进行注册。如果您仅将账户转移到其他 AWS Control Tower OU，则会导致监管偏差，从而也无法将该账户添加到允许列表中。

此过程有 5 个主要步骤。

1. 将该账户添加到 AWS Control Tower 允许列表中。
2. 在账户中创建新的 IAM 角色。
3. 修改先前存在的 AWS Config 资源。
4. 在不存在 AWS Config 资源的 AWS 地区创建资源。
5. 在 AWS Control Tower 注册账户。

在继续之前，请考虑有关此过程的以下期望。

- AWS Control Tower 不会在此账户中创建任何 AWS Config 资源。
- 注册后，AWS Control Tower 控件会自动保护您创建的 AWS Config 资源，包括新的 IAM 角色。
- 如果在注册后对 AWS Config 资源进行了任何更改，则必须先更新这些资源以使其与 AWS Control Tower 设置保持一致，然后才能重新注册账户。

第 1 步：联系客户支持并提交工单，将该账户添加到 AWS Control Tower 允许名单

在你的门票主题行中加入这句话：

将拥有现有 AWS Config 资源的账户注册到 AWS Control Tower

在门票正文中包含以下详细信息：

- 管理账号
- 拥有现有 AWS Config 资源的成员账号的账号
- 您为 AWS Control Tower 设置选择的主区域

> **Note**
>
> 将您的账户添加到允许列表所需的时间为 2 个工作日。

步骤 2：在成员账户中创建新的 IAM 角色

1. 打开成员账户的 AWS CloudFormation 控制台。

2. 使用以下模板创建新堆栈

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config

Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. 将堆栈的名称提供为 CustomerCreatedConfigRecorderRoleForControlTower

4. 创建堆栈。

> **Note**
>
> 您创建的任何 SCP 都应排除`aws-controltower-ConfigRecorderRole*`角色。请勿修改限制 AWS Config 规则执行评估能力的权限。
> 请遵循这些准则，这样当你的 SCP 被阻止`aws-controltower-ConfigRecorderRole*`调用 Config `AccessDeniedException` 时，你就不会收到消息。

步骤 3：确定已有资源 AWS 的地区

对于账户中的每个受管辖区域（AWS Control Tower 管辖），请识别并记下至少具有前面显示的现有 AWS Config 资源示例类型之一的区域。

步骤 4：确定没有任何 AWS Config 资源 AWS 的地区

对于账户中的每个受管辖区域（AWS Control Tower 管辖），识别并记下没有前面所示示例类型 AWS Config 资源的区域。

步骤 5：修改每个 AWS 区域的现有资源

在此步骤中，需要提供有关您的 AWS Control Tower 设置的以下信息。

- LOGGING_ACCOUNT-登录账户 ID
- AUDIT_ACCOUNT-审计账户 ID
- IAM_ROLE_ARN-在步骤 1 中创建的 IAM 角色 ARN
- ORGANIZATION_ID-管理账户的组织 ID
- MEMBER_ACCOUNT_NUMBER-正在修改的成员账户
- HOME_REGION-AWS Control Tower 设置的主区域。

按照后面第 5a 至 5c 节中给出的说明修改每个现有资源。

步骤 5a。 AWS Config 录音机资源

每个 AWS 区域只能存在一个 AWS Config 录制器。如果存在，请修改设置，如图所示。在你的家乡地区将该物品GLOBAL_RESOURCE_RECORDING替换为 true。对于存在 AWS Config 录制器的其他区域，将该项目替换为 false。

- 名称：别改变
- RoLearn： IAM_ROLE_ARN
  - RecordingGroup:
  - AllSupported: 真的
  - IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
  - ResourceTypes: 空

可以使用以下命令通过 AWS CLI 进行此修改。将该字符串RECORDER_NAME替换为现有的 AWS Config 录制器名称。

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
 allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

步骤 5b。修改 AWS Config 配送渠道资源

每个地区只能存在一个 AWS Config 配送渠道。如果存在其他设置，请修改设置，如图所示。

- 名称：别改变
- ConfigSnapshotDeliveryProperties: TwentyFour _Hou rs
- S3BucketName：来自 AWS Control Tower 日志账户的日志存储桶名称

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- S3KeyPrefix：*##_ID*
- SnsTopicARN：来自审核账户的 SNS 主题 ARN，格式如下：

  `arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-AllConfigNotifications`

可以使用以下命令通过 AWS CLI 进行此修改。将该字符串*DELIVERY_CHANNEL_NAME*替换为现有的 AWS Config 录制器名称。

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=aws-controltower-
logs-LOGGING_ACCOUNT_ID-
HOME_REGION,s3KeyPrefix="ORGANIZATION_ID",configSnapshotDeliveryProperties={deliveryFrequency=T
controltower-AllConfigNotifications --region CURRENT_REGION
```

步骤 5c。修改 AWS Config 聚合授权资源

每个区域可以存在多个聚合授权。AWS Control Tower 需要聚合授权，该授权将审计账户指定为授权账户，并将 AWS Control Tower 的主区域指定为授权区域。如果它不存在，请使用以下设置创建一个新的：

- AuthorizedAccountId: 审计账户 ID
- AuthorizedAwsRegion: AWS Control Tower 设置的主区域

可以使用以下命令通过 AWS CLI 进行此修改：

```
aws configservice put-aggregation-authorization --authorized-account-
id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region
CURRENT_REGION
```

第 6 步：在 AWS Control Tower 管理的区域中，在不存在资源的地方创建资源

修改 AWS CloudFormation 模板，使您的主区域中的IncludeGlobalResourcesTypes参数具有值GLOBAL_RESOURCE_RECORDING，如以下示例所示。还要更新模板中的必填字段，如本节所述。

在你的家乡地区将该物品GLOBAL_RESOURCE_RECORDING替换为 true。对于存在 AWS Config 录制器的其他区域，将该项目替换为 false。

1. 导航到管理账户的 AWS CloudFormation 控制台。
2. StackSet 用这个名字创建一个新的CustomerCreatedConfigResourcesForControlTower。
3. 复制并更新以下模板：

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
```

```
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

使用必填字段更新模板：

a. *# **S3 BucketName** ###### LOGGING_ACCOUNT_ID # HO ME_REGIO N*

b. 在 S3 KeyPrefix 字段中，替换 “*##* _ID”

c. *# **SnsTopicARN** ###### AUDIT_ACCOUNT*

d. 在AuthorizedAccountId字段中，替换 AUDIT_ACCOU *NT*

e. 在AuthorizedAwsRegion字段中，替换 *HOME* _REGION

4. 在 AWS CloudFormation 控制台上部署期间，添加成员账号。
5. 添加步骤 4 中确定的 AWS 区域。
6. 部署堆栈集。

第 7 步：在 AWS Control Tower 上注册 OU

在 AWS Control Tower 控制面板中，注册 OU。

> **Note**
>
> 此任务的注册账户工作流程将无法成功。您必须选择 “注册 OU” 或 “重新注册 OU”。

使用 Account Factory 配置和管理账户

本章包括使用 Account Factory 在 AWS Control Tower 着陆区中配置新成员账户的概述和程序。

配置和配置账户的权限

AWS Control Tower Account Factory 允许云管理员和用户在 AWS IAM Identity Center 您的着陆区配置账户。默认情况下，配置账户的 IAM Identity Center 用户必须属于`AWSAccountFactory`群组或管理组。

> **Note**
>
> 使用管理账户工作时要谨慎行事，就像使用任何在整个组织中拥有权限的账户时一样。

AWS Control Tower 管理账户与该`AWSControlTowerExecution`角色存在信任关系，允许通过管理账户设置账户，包括一些自动账户设置。有关该`AWSControlTowerExecution`角色的更多信息，请参阅角色和帐户。

> **Note**
>
> 要 AWS 账户 将现有账户注册到 AWS Control Tower，该账户必须启用该`AWSControlTowerExecution`角色。有关如何注册现有账户的更多信息，请参阅注册现有的 AWS 账户。

有关权限的更多信息，请参阅账户所需的权限。

使用 Account Factory 配置 AWS Service Catalog 账户

以下过程介绍如何通过在 IAM Identity Center 中以用户身份创建和配置账户 AWS Service Catalog。此过程也称为高级账户配置或手动账户配置。或者，您可以使用 AWS CLI 或 AWS Control Tower Account Factory for Terraform (AFT) 以编程方式配置账户。如果您之前设置过自定义蓝图，则可以在控制台中配置自定义账户。有关自定义的更多信息，请参阅使用 Account Factory 自定义 (AFC) 自定义账户。

以用户身份在 Account Factory 中单独配置账户

1. 从您的用户门户 URL 登录。
2. 从 “我的应用程序” 中，选择 “AWS 账户”。
3. 从账户列表中，为您的管理账户选择账户 ID。此 ID 也可能带有标签，例如 “（管理）”。

4. 从AWSServiceCatalogEndUserAccess中选择管理控制台。这将在此账户中 AWS Management Console 为该用户打开。
5. 确保您选择的账户配置正确 AWS 区域 ，该区域应该是您的 AWS Control Tower 区域。
6. 搜索并选择 S ervice Catalog 以打开服务目录控制台。
7. 在导航窗格中，选择 “产品”。
8. 选择 AWS Control Tower Account Fac tory，然后选择启动产品按钮。这一选择将启动向导以预置新账户。
9. 填写信息，并记住以下几点：
   - SSO UserEmail 可以是新的电子邮件地址，也可以是与现有 IAM 身份中心用户关联的电子邮件地址。无论您选择哪一个，此用户都将拥有您正在预置的账户的管理访问权。
   - AccountEmail必须是尚未与关联的电子邮件地址 AWS 账户。如果您在 SSO 中使用了新的电子邮件地址UserEmail，则可以在此处使用该电子邮件地址。
10. 请勿定义TagOptions和启用通知，否则可能会无法配置账户。完成后，选择 “启动产品”。
11. 检查您的账户设置，然后选择 Launch (启动)。请勿创建资源计划，否则将无法配置账户。
12. 您的账户现在正在预置中。这可能需要几分钟才能完成。您可以刷新页面以更新显示的状态信息。

> **Note**
>
> 一次最多可以配置五个账户。

在 Account Factory 中管理账户的注意事项

您可以通过 Account Factory 更新、取消管理和关闭您创建和配置的账户。您可以通过更新要重新调整用途的帐户中的用户参数来回收帐户。您也可以更改账户的组织单位 (OU)。

> **Note**
>
> 在更新与 Account Factory 出售的账户关联的预配置产品时，如果您为其指定新的用户电子邮件地址 AWS IAM Identity Center，AWS Control Tower 将在 IAM 身份中心创建一个新用户。之前创建的账户不会被删除。有关从 IAM Identity Center 中删除以前的 IAM 身份中心用户电子邮件地址的信息，请参阅禁用用户。

使用 AWS Control Tower 或使用 AWS Control Tower 更新和移动账户工厂账户 AWS Service Catalog

更新已注册账户的最简单方法是通过 AWS Control Tower 控制台。个人账户更新对于解决偏差问题很有用，例如已移动成员账户。作为完整的 landing zone 更新的一部分，还需要更新账号。

如果您将账户从一个组织单位 (OU) 转移到另一个组织单位 (OU)，请记住，新 OU 所应用的控制可能与以前的 OU 中的控制不同。请确保新 OU 中的控件符合您对账户的政策要求。

控制在账户之间移动时的行为 OU

当您在组织单元之间转移账户时，目标 OU 的控制将应用于 账户。但是，应用于前 OU 账户的控制不是 已移除。控件的确切行为因实施而异 在前 OU 和目标 OU 上处于活动状态的控件。

- 对于使用 AWS Config 规则实现的控件：来自先前 OU 的控件 未被删除。必须手动删除这些控件。
- 对于使用 SCP 实现的控件：以前的 OU 中基于 SCP 的控件是 已移除。目标 OU 的基于 SCP 的控件将对此账户生效。
- 对于使用 AWS CloudFormation 钩子实现的控件：此行为 取决于新 OU 中控件的状态。
  - 如果目标 OU 没有激活基于挂钩的控件：旧 除非您移除控件，否则已移动账户的控件仍处于活动状态 手动。
  - 如果目标 OU 激活了挂钩控件：旧的控件是 已移除，目标 OU 中的控件将应用于 账户。

在控制台中更新账户

在 AWS Control Tower 控制台中更新账户

1. 登录 AWS Control Tower 后，导航到组织页面。
2. 在 OU 和账户列表中，选择要更新的账户名称。可供更新的账户显示更新可用状态。
3. 接下来，您将看到所选账户的账户详情页面。
4. 在右上角，选择更新账户。

更新预配置的产品

以下过程将指导您通过在 Service Catalog 中更新账户的预配置产品来更新 Account Factory 中的账户或将其移至新的 OU。

通过 Service Catalog 更新 Account Factory 账户或更改其 OU

1. 登录 AWS 管理控制台，然后通过 https://console.aws.amazon.com/servicecatalog/ 打开 AWS Service Catalog 控制台。

   > **Note**
   >
   > 您必须以有权在 Service Catalog 中配置新产品的用户身份登录（例如，`AWSAccountFactory`或`AWSServiceCatalogAdmins`群组中的 IAM Identity Center 用户）。

2. 在导航窗格中，选择配置，然后选择预配置产品。
3. 对于列出的每个成员帐户，请执行以下步骤来更新所有成员帐户：

   a. 选择一个成员账户。您将被引导至该账户的预配置产品详情页面。

   b. 在预配置产品详细信息页面上，选择事件选项卡。

   c. 记下以下参数：

      - SSO UserEmail（可在预配置产品详细信息中找到）
      - AccountEmail（可在预配置产品详细信息中找到）
      - SSO UserFirstName（在 IAM 身份中心可用）
      - SSOU SerLastName（在 IAM 身份中心可用）
      - AccountName（在 IAM 身份中心可用）

   d. 从 Actions (操作) 中，选择 Update (更新)。

   e. 选择要更新的产品的 Version (版本) 旁边的按钮，并选择 Next (下一步)。

   f. 提供之前提到的参数值。

      - 如果要保留现有 OU ManagedOrganizationalUnit，请选择该账户已存在的 OU。
      - 如果要将账户迁移到新的 OU，请为ManagedOrganizationalUnit该账户选择新的 OU。

      中央云管理员可以在 AWS Control Tower 控制台的组织页面上找到这些信息。

   g. 选择下一步。

   h. 查看您的更改，然后选择 Update (更新)。对于每个账户，此过程可能需要几分钟。

更改已注册账户的电子邮件地址

要在 AWS Control Tower 中更改已注册成员账户的电子邮件地址，请按照本节中的步骤操作。

> **Note**
>
> 以下过程不允许您更改管理账户、日志存档账户或审计账户的电子邮件地址。有关这方面的更多信息，请参阅如何更改与我的 AWS 账户关联的电子邮件地址？ 或者联系 Supp AWS ort。

更改 AWS Control Tower 创建的账户的电子邮件地址

1. 恢复该帐户的 root 用户密码。您可以按照文章中的步骤操作如何恢复丢失或忘记的 AWS 密码？
2. 使用 root 用户密码登录账户。
3. 像更改其他电子邮件地址一样更改电子邮件地址 AWS 账户，然后等待更改反映出来 AWS Organizations。当电子邮件地址更改完成更新时，您可能会遇到延迟。
4. 使用先前属于该账户的电子邮件地址在 Service Catalog 中更新已配置的产品。更新预配置产品的过程包括将新的电子邮件地址与预配置产品相关联。这样，电子邮件地址的更改就会在 AWS Control Tower 中生效。使用新的电子邮件地址获取后续配置产品的更新。

要更改您创建的成员账户的密码或电子邮件地址 AWS Organizations，请参阅用户指南中的以 root 用户身份访问成员账户。AWS Organizations

更改已注册账户的名称

按照本节中的步骤更改已注册的 AWS Control Tower 账户的名称。

> **Note**
>
> 要更改 AWS 管理员帐户的名称，您必须具有管理员权限并以该帐户的 root 用户身份登录。

更改 AWS Control Tower 创建的账户的名称

1. 恢复账户的 root 密码。您可以按照本文 “如何恢复丢失或忘记的 AWS 密码？” 中概述的步骤进行操作
2. 使用 root 密码登录账户。
3. 在 AWS Billing 控制台中，导航到账户设置页面。

4. 在 “账户设置” 中更改姓名，就像更改其他名称一样 AWS 账户。
5. AWS Control Tower 会自动更新以反映名称的更改。此更新不会反映在中的预配置产品中。 AWS Service Catalog

使用亚马逊虚拟私有云设置配置 Account Factory

Account Factory 允许您为组织中的帐户创建预先批准的基准和配置选项。您可以通过 AWS Service Catalog配置和预置新账户。

在 Account Factory 页面上，您可以看到组织单位 (OU) 的列表及其允许列表状态。默认情况下，所有 OU 都在允许列表中，这意味着可以在 OU 下预置账户。您可以通过禁用某些 OU 进行账户配置 AWS Service Catalog。

您可以查看最终用户在配置新账户时可用的 Amazon VPC 配置选项。

在 Account Factory 中配置亚马逊 VPC 设置

1. 作为中央云管理员，使用管理账户中的管理员权限登录 AWS Control Tower 控制台。
2. 在控制面板的左侧，选择 Acco unt Factory 以导航到 Account Factory 网络配置页面。在该页面中，您可以看到显示的默认网络设置。要进行编辑，请选择编辑并查看 Account Factory 网络配置设置的可编辑版本。
3. 您可以根据需要修改默认设置的每个字段。选择您要为最终用户可能创建的所有新 Account Factory 账户设置的 VPC 配置选项，然后在字段中输入您的设置。

- 选择禁用或启用以在 Amazon VPC 中创建公有子网。默认情况下，禁止可通过 Internet 访问的子网。

> **Note**
>
> 如果您将账户工厂 VPC 配置设置为在配置新账户时启用公有子网，则账户工厂会将 Amazon VPC 配置为创建 NAT 网关。Amazon VPC 将对您的用量计费。有关更多信息，请参阅 VPC 定价。

- 从列表中选择 Amazon VPC 中私有子网的最大数量。默认情况下，将选择 1。每个可用区允许的最大私有子网数量为 2。
- 输入用于创建账户 VPC 的 IP 地址范围。该值必须采用无类型域间路由 (CIDR) 块的形式（例如默认为 `172.31.0.0/16`）。此 CIDR 块提供了 Account Factory 为您的账户创建的 VPC 的子网 IP 地址

的总体范围。在您的 VPC 中，将从您指定的范围中自动分配子网，并且这些子网的大小相等。默认情况下，您的 VPC 中的子网不会重叠。但是，在所有预置账户中的 VPC 中的子网 IP 地址范围可以重叠。

- 在预置账户时，选择一个区域或所有区域来创建 VPC。默认情况下，将选中所有可用区域。
- 从列表中，选择要在每个 VPC 中为其配置子网的可用区的数目。默认和推荐的数量为 3。
- 选择保存。

您可以设置这些配置选项以创建不包含 VPC 的新账户。请参阅演练。

取消账户管理

如果您在 Account Factory 中创建了一个账户或注册了一个账户 AWS 账户，但又不想让该账户在着陆区由 AWS Control Tower 管理，则可以从 AWS Control Tower 控制台取消对账户的管理。

当您取消管理 AWS Control Tower 账户时，AWS Control Tower 配置的所有资源都将被删除，包括所有蓝图。该账户将移出任何 AWS Control Tower 组织单位，进入根区域。该账户不再是已注册 OU 的一部分，也不再受 AWS Control Tower SCP 的约束。您可以通过关闭账户 AWS Organizations。

`AWSAccountFactory`群组中的 IAM Identity Center 用户也可以在 Service Catalog 控制台中通过终止预配置产品来取消对账户的管理。有关 IAM Identity Center 用户或群组的更多信息，请参阅通过管理用户和访问权限 AWS IAM Identity Center。以下过程介绍如何在 Service Catalog 中取消对成员帐户的管理。

取消管理已注册账户

1. 在 Web 浏览器中打开 Service Catalog 控制台，网址为https://console.aws.amazon.com/servicecatalog。
2. 在左侧导航窗格中，选择预配置产品列表。
3. 从预配置账户列表中，选择您希望 AWS Control Tower 不再管理的账户名称。
4. 在 Provisioned product details (预置的产品详细信息) 页面上，从 Actions (操作) 菜单中选择 Terminate (终止)。
5. 从随后显示的对话框中，选择 Terminate (终止)。

> **Important**
>
> “终止” 一词特定于 Service Catalog。当你在 Service Catalog Account Factory 中终止账户时，该账户并未关闭。此操作会将该账户从其 OU 和您的着陆区域中移除。

6. 当账户处于非托管状态时，其状态将更改为 “未注册”。
7. 如果您不再需要该帐户，请将其关闭。有关关闭 AWS 账户的更多信息，请参阅《AWS Billing 用户指南》中的关闭账户

当您取消管理自定义账户时，AWS Control Tower 会移除蓝图已部署的资源，以及 AWS Control Tower 在账户中创建的任何其他资源。取消账户管理后，您可以通过 AWS Organizations关闭账户。

> **Note**
>
> 非托管账户不会被关闭或删除。当账户处于非托管状态时，您在 Account Factory 中创建账户时选择的 IAM Identity Center 用户仍具有该账户的管理权限。如果您不希望此用户拥有管理权限，则必须在 IAM Identity Center 中更改此设置，方法是在 Account Factory 中更新账户并更改该账户的 IAM Identity Center 用户电子邮件地址。有关更多信息，请参阅 使用 AWS Control Tower 或使用 AWS Control Tower 更新和移动账户工厂账户 AWS Service Catalog。

视频演练

此视频 (3:25) 描述了如何从 AWS Control Tower 中删除账户、获得该账户的根访问权限以及最后关闭。 AWS 账户您也可以使用 AWS Organizations API 关闭账户。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

在 AWS Control Tower 中关闭账户的视频演练。

您可以在 AWS Control Tower 中观看解释常见任务的 AWS YouTube 视频列表。

关闭在 Account Factory 中创建的账户

在 Account Factory 中创建的账户是 AWS 账户。有关关闭账户的信息 AWS 账户，请参阅《账户管理参考指南》中的关闭AWS账户。

> **Note**
>
> 关闭与从 AWS AWS 账户 Control Tower 取消管理账户的操作不同，这些操作是分开的。在关闭账户之前，必须取消对账户的管理。

通过关闭 AWS Control Tower 成员账户 AWS Organizations

您可以通过以下方式从贵组织的管理账户中关闭您的 AWS Control Tower 成员账户，无需使用根证书单独登录每个成员账户 AWS Organizations。但是，您不能以这种方式关闭您的管理账户。

当您调用 AWS Organizations CloseAccountAPI 或在 AWS Organizations 控制台中关闭账户时，成员账户 AWS 账户 将像任何账户一样被隔离 90 天。该账户在 AWS Control Tower 中显示为 “已暂停” 状态，并且 AWS Organizations。如果您在这 90 天内尝试使用该账户，AWS Control Tower 会显示一条错误消息。

在 90 天到期之前，您可以恢复成员帐户，就像恢复任何成员帐户一样 AWS 账户。在这90天之后，该账户的记录将被删除。

作为最佳实践，我们建议您在关闭会员账户之前取消该账户的管理。如果您在未事先取消管理成员账户的情况下关闭该账户，AWS Control Tower 会将该账户的状态显示为已暂停，但也会显示为已注册。因此，如果您在这 90 天内尝试重新注册账户的 OU，AWS Control Tower 会生成一条错误消息。由于预先检查失败，被暂停的账户本质上会阻止重新注册的操作。如果您从 OU 中删除该账户，则可以重新注册 OU，但 AWS 可能会出现有关该账户缺少付款方式的错误。要解决此限制，请创建另一个 OU，然后在尝试重新注册之前将该账户移至该 OU。我们建议将此 OU 命名为暂停的 OU。

> **Note**
>
> 如果您在关闭账户之前未取消对账户的管理，则必须在 90 天 AWS Service Catalog 结束后删除该账户的预配置产品。

有关更多信息，请参阅有关 CloseAccountAPI 的 AWS Organizations 文档。

Account Factory 的资源注意事项

使用 Account Factory 为账户配置时，将在该账户中创建以下 AWS 资源。

AWS 服务	资源类型	资源名称
AWS CloudFormation	堆栈	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-*

AWS 服务	资源类型	资源名称
		StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	试用	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch 赛事规则	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch 日志	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder

AWS 服务	资源类型	资源名称
AWS Identity and Access Management	角色	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	策略	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	主题	aws-controltower-SecurityNotifications
AWS Lambda	应用程序	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	函数	aws-controltower-NotificationForwarder

使用 Account Factory 自定义 (AFC) 自定义账户

AWS Control Tower 允许您在从 AWS Control Tower 控制台配置新资源和现有资源 AWS 账户 时对其进行自定义。在您设置账户出厂自定义后，AWS Control Tower 会自动执行此过程以备将来配置，因此您无需维护任何管道。配置资源后，可以立即使用自定义帐户。

您的自定义账户是在账户工厂、 AWS CloudFormation 模板或 Terraform 中配置的。您将定义一个用作自定义账户蓝图的模板。您的蓝图描述了配置账户时所需的特定资源和配置。还提供由 AWS 合作伙伴构建和管理的预定义蓝图。有关合作伙伴管理的蓝图的更多信息，请参阅AWS Service Catalog 入门库。

> **Note**
>
> AWS Control Tower 包含主动控件， AWS CloudFormation 用于监控 AWS 控制塔中的资源。或者，您也可以在着陆区（Landing zone）中激活这些控件。当你应用主动控制措施时，他们会进行检查以确保你要部署到账户的资源符合贵组织的政策和程序。有关主动控制的更多信息，请参阅主动控制。

您的账户蓝图存储在中 AWS 账户，就我们而言，该账户被称为中心账户。蓝图以 Service Catalog 产品的形式存储。我们称此产品为蓝图，以将其与任何其他 Service Catalog 产品区分开来。要详细了解如何创建 Service Catalog 产品，请参阅《AWS Service Catalog 管理员指南》中的创建产品。

将蓝图应用于现有账户

您也可以按照 AWS Control Tower 控制台中的更新账户步骤将自定义蓝图应用于现有账户。有关更多信息，请参阅 在控制台中更新账户。

> **开始前的准备工作**
>
> 在开始使用 AWS Control Tower Account Factory 创建自定义账户之前，您必须部署 AWS Control Tower 着陆区环境，并且必须在 AWS Control Tower 注册一个组织单位 (OU)，您新创建的账户将存放在那里。

有关使用 AFC 的更多信息，请参阅 AWS Control Tower 中使用 AWS Control Tower 中的账户出厂自定义自动进行账户自定义。

为定制做准备

- 您可以创建一个新账户作为中心账户，也可以使用现有账户 AWS 账户。我们强烈建议您不要使用 AWS Control Tower 管理账户作为蓝图中心账户。
- 如果您计划注册 AWS 账户 AWS Control Tower 并对其进行自定义，则必须先将该`AWSControlTowerExecution`角色添加到这些账户，就像您注册到 AWS Control Tower 的任何其他账户一样。

- 如果您计划使用具有市场订阅要求的合作伙伴蓝图，则必须先从 AWS Control Tower 管理账户配置这些蓝图，然后再将合作伙伴蓝图部署为账户出厂自定义蓝图。

主题

设置为自定义

接下来的章节将介绍为自定义过程设置 Account Factory 的步骤。在开始这些步骤之前，我们建议您为中心账户设置委托管理员。

Summary

- 第 1 步。创建所需的角色。创建一个 IAM 角色，授予 AWS Control Tower 访问存储服务目录产品（也称为蓝图）的（中心）账户的权限。
- 第 2 步。创建 AWS Service Catalog 产品。创建为自定义账户设定基准所需的 AWS Service Catalog 产品（也称为 “蓝图产品”）。
- 第 3 步。查看您的自定义蓝图。检查您创建的 AWS Service Catalog 产品（蓝图）。
- 第 4 步。调用您的蓝图来创建自定义账户。创建账户时，在 AWS Control Tower 控制台的 Account Factory 的相应字段中输入蓝图产品信息和角色信息。

第 1 步。创建所需的角色

在开始自定义账户之前，您必须设置一个包含 AWS Control Tower 和您的中心账户之间信任关系的角色。担任该角色后，将授予 AWS Control Tower 管理中心账户的访问权限。必须为角色命名AWSControlTowerBlueprintAccess。

AWS Control Tower 担任此角色代表您在中创建投资组合资源 AWS Service Catalog，然后将您的蓝图作为服务目录产品添加到该产品组合中，然后在账户配置期间与您的成员账户共享此产品组合和蓝图。

您将创建AWSControlTowerBlueprintAccess角色，如以下各节所述。

导航到 IAM 控制台以设置所需的角色。

在已注册的 AWS Control Tower 账户中设置该角色

1. 在 AWS Control Tower 管理账户中加入联合账户或以委托人身份登录。
2. 从管理账户中的联合委托人代入角色或将角色切换到您选择用作蓝图中心账户的已注册 AWS Control Tower 账户中的角色。AWSControlTowerExecution
3. 使用已注册的 AWS Control Tower 账户中的AWSControlTowerExecutionAWSControlTowerBlueprintAccess角色，创建具有适当权限和信任关系的角色。

Note

为了遵守 AWS 最佳实践指南，在创建角色后立即注AWSControlTowerExecution销该角色非常重要。AWSControlTowerBlueprintAccess
为防止对资源进行意外更改，该AWSControlTowerExecution角色仅供 AWS Control Tower 使用。

如果您的蓝图中心账户未在 AWS Control Tower 中注册，则该账户中将不存在该AWSControlTowerExecution角色，在继续设置角色之前无需假设该AWSControlTowerBlueprintAccess角色。

在未注册的成员账户中设置角色

1. 使用您的首选方法，在您希望指定为中心账户的账户中进行联合或以委托人身份登录。

2. 以账户委托人身份登录后，创建具有适当权限和信任关系的`AWSControlTowerBlueprintAccess`角色。

必须将该AWSControlTowerBlueprintAccess角色设置为向两位委托人授予信任：

- 在 AWS Control Tower 管理账户中运行 AWS Control Tower 的委托人（用户）。
- `AWSControlTowerAdmin`在 AWS Control Tower 管理账户中指定的角色。

以下是信任策略示例，类似于你需要为自己的角色加入的信任策略。此策略演示了授予最低权限访问权限的最佳实践。当您制定自己的策略时，请将该术语*`YourManagementAccountId`*替换为您的 AWS Control Tower 管理账户的实际账户 ID，并将该术语*`YourControlTowerUserRole`*替换为管理账户的 IAM 角色标识符。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",
                "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

必需的权限策略

AWS Control Tower 要求`AWSServiceCatalogAdminFullAccess`必须将名为的托管策略附加到该`AWSControlTowerBlueprintAccess`角色。此策略提供的权限适用于何时允许 AWS Control Tower 管理您的产品组合和 AWS Service Catalog 产品资源。 AWS Service Catalog 在 IAM 控制台中创建角色时，您可以附加此策略。

可能需要其他权限

- 如果您将蓝图存储在 Amazon S3 中，AWS Control Tower 还需要该`AWSControlTowerBlueprintAccess`角色的`AmazonS3ReadOnlyAccess`权限策略。
- 如果您不使用默认的管理员策略， AWS Service Catalog Terraform 类型的产品要求您向 AFC 自定义 IAM 策略添加一些额外的权限。除了创建您在 terraform 模板中定义的资源所需的权限外，它还需要这些权限。

第 2 步。创建 AWS Service Catalog 产品

要创建 AWS Service Catalog 产品，请按照《AWS Service Catalog 管理员指南》中创建产品中的步骤进行操作。创建 AWS Service Catalog 产品时，您需要将账户蓝图添加为模板。

Important

由于更新 HashiCorp了 Terraform 许可，将对 Terrafor m 开源产品和预配置产品的支持 AWS Service Catalog 更改为一种名为 Exter nal 的新产品类型。要详细了解此次变更对 AFC 的影响，包括如何将现有账户蓝图更新为外部产品类型，请查看过渡到外部产品类型。

创建蓝图的步骤摘要

- 创建或下载 AWS CloudFormation 模板或 Terraform tar.gz 配置文件，该文件将成为您的账户蓝图。本节稍后将给出一些模板示例。
- 登录您存储 Account Factory 蓝图 AWS 账户 的地方（有时称为中心账户）。
- 导航到 AWS Service Catalog 控制台。选择 “商品列表”，然后选择 “上传新商品”。
- 在产品详细信息窗格中，输入蓝图产品的详细信息，例如名称和描述。
- 选择 “使用模板文件”，然后选择 “选择文件”。选择或粘贴您开发或下载的模板或配置文件以用作蓝图。
- 选择控制台页面底部的创建产品。

您可以从 AWS Service Catalog 参考架构存储库下载 AWS CloudFormation 模板。该存储库中的一个示例有助于为您的资源制定备份计划。

这是一家名为B es t Pets的虚构公司的示例模板。它可以帮助他们建立与宠物数据库的连接。

```
Resources:
  ConnectionStringGeneratorLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - lambda.amazonaws.com
            Action:
              - "sts:AssumeRole"
  ConnectionStringGeneratorLambda:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
 ['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]]
      Description: Retrieves the connection string for this account to access the Pet
 Database
      Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
      Runtime: nodejs16.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
          const response = require("cfn-response");
          exports.handler = function (event, context) {
            const awsAccountId = context.invokedFunctionArn.split(":")[4]
            const connectionString= "fake connection string that's specific to account
 " + awsAccountId;
            const responseData = {
              Value: connectionString,
            }
            response.send(event, context, response.SUCCESS, responseData);
            return connectionString;
          };

  ConnectionString:
    Type: Custom::ConnectionStringGenerator
    Properties:
      ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn
```

```
  PetDatabaseConnectionString:
    DependsOn: ConnectionString
    # For example purposes we're using SSM parameter store.
    # In your template, use secure alternatives to store
    # sensitive values such as connection strings.
    Type: AWS::SSM::Parameter
    Properties:
      Name: pet-database-connection-string
      Description: Connection information for the BestPets pet database
      Type: String
      Value: !GetAtt ConnectionString.Value
```

第 3 步。查看您的自定义蓝图

您可以在 AWS Service Catalog 控制台中查看您的蓝图。有关更多信息，请参阅《S ervice Catalog 管理员指南》中的管理产品。

第 4 步。调用你的蓝图创建自定义账户

在 AWS Control Tower 控制台中执行创建账户工作流程时，您将看到一个可选部分，您可以在其中输入有关要用于自定义账户的蓝图的信息。

> **Note**
>
> 您必须先设置自定义中心账户并添加至少一个蓝图（Service Catalog 产品），然后才能将该信息输入到 AWS Control Tower 控制台并开始配置自定义账户。

在 AWS Control Tower 控制台中创建或更新自定义账户。

1. 输入包含您的蓝图的账户的账户 ID。
2. 从该账户中选择现有的 Service Catalog 产品（现有蓝图）。
3. 如果您有多个版本，请选择蓝图的正确版本（Service Catalog 产品）。
4. （可选）您可以在此过程中添加或更改蓝图配置策略。蓝图配置策略以 JSON 格式编写并附加到 IAM 角色，因此它可以配置蓝图模板中指定的资源。AWS Control Tower 在成员账户中创建此角色，这样 Service Catalog 就可以使用 AWS CloudFormation 堆栈集部署资源。该角色命名为 `AWSControlTower-BlueprintExecution-bp-xxxx`。默认情况下，此`AdministratorAccess`策略在此处应用。
5. 根据此蓝图选择您要在其中部署账户的 AWS 区域 或区域。

6. 如果您的蓝图包含参数，则可以在 AWS Control Tower 工作流程的其他字段中输入参数值。其他值可能包括： GitHub 存储库名称、 GitHub 分支、Amazon ECS 集群名称和存储库所有者的 GitHub 身份。
7. 如果您的中心账户或蓝图尚未准备就绪，则可以稍后按照账户更新流程自定义账户。

有关更多详细信息，请参阅根据蓝图创建自定义账户。

根据蓝图创建自定义账户

创建自定义蓝图后，您可以开始在 AWS Control Tower 账户工厂中创建自定义账户。

创建新 AWS 账户时，请按照以下步骤部署自定义蓝图：

1. 前往中的 AWS Control Tower AWS Management Console。
2. 选择 “账户工厂” 和 “创建账户”。
3. 输入账户详情，例如账户名和电子邮件地址。
4. 使用电子邮件地址和用户名配置 IAM 身份中心详细信息。
5. 选择要在其中添加账户的已注册 OU。
6. 展开 “账户出厂自定义” 部分。
7. 输入包含您的 Service Catalog 产品的蓝图中心账户的账户 ID，然后选择验证。有关蓝图中心账户的更多信息，请参阅使用 Account Factory 自定义 (AFC) 自定义账户。
8. 选择包含您的 Service Catalog 产品列表中所有蓝图（所有定制蓝图和合作伙伴蓝图）的下拉菜单。选择要部署的蓝图和相应的版本。
9. 如果您的蓝图包含参数，则会显示这些字段供您填充。默认值已预先填充。
10. 最后，选择要部署蓝图的位置，即主区域或所有受管辖区域。诸如 Route 53 或 IAM 之类的全球资源可能只需要部署到单个区域。区域资源（例如 Amazon EC2 实例或 Amazon S3 存储桶）可以部署到所有受管控的区域
11. 填写完所有字段后，选择创建账户。

> **Note**
>
> 使用 Terraform 创建的蓝图只能部署到一个区域，不能部署到多个区域。

您可以在组织页面上查看账户配置进度。账户配置完成后，蓝图中指定的资源已经部署在蓝图中。要查看账户和蓝图的详细信息，请前往账户详情页面。

注册和自定义账户

在 AWS Control Tower 控制台中注册和自定义账户。

1. 导航到 AWS Control Tower 控制台，然后从左侧导航栏中选择 “组织”。
2. 您将看到可用账户的列表。使用自定义蓝图确定您要注册的账户。该账户的 “州” 列应反映该账户处于 “未注册” 状态。
3. 选择账户左侧的单选按钮，然后选择屏幕右上角的 “操作” 下拉菜单。在这里，您将选择 “注册” 选项。
4. 使用账户的 IAM 身份中心信息完成访问配置部分。
5. 选择您的账户将成为成员的已注册 OU。
6. 使用与创建账户过程中的 7-12 相同的步骤完成账户出厂自定义部分。有关更多信息，请参阅 Provision A ccount Factory 账户 AWS Service Catalog。

您可以在组织页面上查看您的账户进度状态。账户注册完成后，蓝图中指定的资源已经部署在蓝图中。

向 AWS Control Tower 账户添加蓝图

要向现有 AWS Control Tower 成员账户添加蓝图，请按照 AWS Control Tower 控制台中的更新账户工作流程进行操作，然后选择要添加到账户的新蓝图。有关更多信息，请参阅使用 AWS Control T ower 或使用 AWS Control Tower 更新和移动 Account Factory 账户 AWS Service Catalog。

> **Note**
>
> 如果您向账户添加新蓝图，则现有蓝图将被覆盖。

> **Note**
>
> 每个 AWS Control Tower 账户可以部署一个蓝图。

更新蓝图

以下过程描述了如何更新自定义蓝图以及如何部署它们。

更新您的自定义蓝图

1. 使用新的配置更新你的 AWS CloudFormation 模板或 Terraform tar.gz 文件（蓝图）。
2. 将更新的蓝图另存为新版本 AWS Service Catalog。

部署更新后的蓝图

1. 在 AWS Control Tower 控制台中导航到 “组织” 页面。
2. 按蓝图名称和版本筛选 “组织” 页面。
3. 按照更新账户流程进行操作，并在您的账户中部署最新的蓝图版本。

如果蓝图更新不成功

当预配置的产品`AVAILABLE`处于状态时，AWS Control Tower 允许更新蓝图。如果您的预配置产品处于`TAINTED`状态，则更新将失败。我们建议采用以下解决方法：

1. 在 AWS Service Catalog 控制台中，手动更新`TAINTED`已配置产品以将状态更改为`AVAILABLE`。有关更多信息，请参阅更新预配置产品。
2. 然后，按照 AWS Control Tower 中的更新账户流程修复蓝图部署错误。

我们建议您手动执行此步骤，因为：移除蓝图时，可能会导致成员账户中的资源被移除。移除资源可能会影响您的现有工作负载。因此，我们建议使用这种方法，而不是更新蓝图的替代方法，即移除并替换原始蓝图，尤其是在运行生产工作负载的情况下。

从账户中移除蓝图

要从账户中移除蓝图，请按照更新账户工作流程移除蓝图并将该账户恢复为 AWS Control Tower 的默认配置。

当您在控制台中进入更新账户工作流程时，您将看到所有账户详细信息均已填充，自定义详细信息未填充。如果您将这些 AFC 详细信息留空，AWS Control Tower 将从账户中移除蓝图。在操作开始之前，您将看到一条警告消息。

> **Note**
>
> 仅当您在创建账户或更新账户过程中选择蓝图时，AWS Control Tower 才会向账户添加蓝图。

合作伙伴蓝图

AWS Control Tower 账户工厂定制 (AFC) 允许访问由 AWS 合作伙伴构建和管理的预定义自定义蓝图。这些合作伙伴蓝图可帮助您针对特定用例自定义账户。每个合作伙伴的蓝图都可帮助您建立定制账户，这些账户已预先配置为与该特定合作伙伴提供的产品配合使用。

要查看 AWS Control Tower 合作伙伴蓝图的完整列表，请在控制台中导航到服务目录入门库。搜索源类型 AWS Control Tower 蓝图。

Account Factory 定制注意事项 (AFC)

- AFC 仅支持使用单个 AWS Service Catalog 蓝图产品进行自定义。
- AWS Service Catalog 蓝图产品必须在中心账户中创建，并且必须与 AWS Control Tower 着陆区主区域位于同一区域。
- 必须使用正确的名称、权限和信任策略创建 `AWSControlTowerBlueprintAccess` IAM 角色。
- AWS Control Tower 支持蓝图的两个部署选项：仅部署到主区域，或者部署到受 AWS Control Tower 管理的所有区域。无法选择区域。
- 在成员账户中更新蓝图时，无法更改蓝图中心账户 ID 和 AWS Service Catalog 蓝图产品。
- AWS Control Tower 不支持在单个蓝图更新操作中移除现有蓝图和添加新蓝图。您可以移除蓝图，然后通过单独的操作添加新蓝图。
- AWS Control Tower 会根据您是在创建或注册自定义账户还是非自定义账户来改变行为。如果您没有使用蓝图创建或注册自定义账户，AWS Control Tower 会在 AWS Control Tower 管理账户中创建账户出厂预配置的产品（通过服务目录）。如果您在使用蓝图创建或注册账户时指定了自定义，则 AWS Control Tower 不会在 AWS Control Tower 管理账户中创建账户出厂预配置的产品。

如果出现蓝图错误

应用蓝图时出错

如果在将蓝图应用于账户（无论是新账户还是注册到 AWS Control Tower 的现有账户）的过程中出现错误，则恢复过程相同。该账户将存在，但它不是自定义的，也不会注册到 AWS Control Tower 中。要继续，请按照步骤将账户注册到 AWS Control Tower，并在注册时添加蓝图。

创建**`AWSControlTowerBlueprintAccess`**角色时出错及解决方法

当您通过 AWS Control Tower 账户创建AWSControlTowerBlueprintAccess角色时，必须使用该AWSControlTowerExecution角色以委托人身份登录。如果您以任何其他方式登录，则CreateRole操作会被 SCP 阻止，如以下构件所示：

```
{
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:role/AWSControlTowerExecution",
                        "arn:aws:iam::*:role/stacksets-exec-*"
                    ]
                }
            },
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePermissionsBoundary",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:PutRolePermissionsBoundary",
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-controltower-*",
                "arn:aws:iam::*:role/*AWSControlTower*",
                "arn:aws:iam::*:role/stacksets-exec-*"
            ],
            "Effect": "Deny",
            "Sid": "GRIAMROLEPOLICY"
        }
```

有以下解决方法可用：

- （最推荐）代入AWSControlTowerExecution角色并创建AWSControlTowerBlueprintAccess角色。如果您选择此变通方案，请务必在之后立即退出该AWSControlTowerExecution角色，以防止对资源进行意外更改。
- 登录一个未在 AWS Control Tower 中注册、因此不受此 SCP 约束的账户。

- 临时编辑此 SCP 以允许该操作。
- （强烈不推荐）使用您的 AWS Control Tower 管理账户作为中心账户，这样它就不受 SCP 的约束。

根据以下内容为亚足联蓝图定制您的政策文件 CloudFormation

当您通过账户工厂启用蓝图时，AWS Control Tower 会指示 AWS CloudFormation 您 StackSet 代表您创建蓝图。 AWS CloudFormation 需要访问您的托管账户才能在中创建 AWS CloudFormation 堆栈。StackSet尽管 AWS CloudFormation 已通过该`AWSControlTowerExecution`角色在托管账户中拥有管理员权限，但该角色不能由 AWS CloudFormation担任。

作为启用蓝图的一部分，AWS Control Tower 在成员账户中创建一个角色，该角色 AWS CloudFormation 可以假设该角色完成 StackSet 管理任务。通过账户工厂启用自定义蓝图的最简单方法是使用 allow-all 策略，因为这些策略与任何蓝图模板兼容。

但是，最佳实践建议您必须限制目标账户 AWS CloudFormation 中的权限。您可以提供自定义策略，AWS Control Tower 将其应用于其创建的角色 AWS CloudFormation 以供使用。例如，如果您的蓝图创建了一个名为重要内容的 SSM 参数，则可以提供以下策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFormationActionsOnStacks",
            "Effect": "Allow",
            "Action": "cloudformation:*",
            "Resource": "arn:aws:cloudformation:*:*:stack/*"
        },
        {
            "Sid": "AllowSsmParameterActions",
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                 "ssm:DeleteParameter",
                 "ssm:GetParameter",
                 "ssm:GetParameters"
            ],
            "Resource": "arn:*:ssm:*:*:parameter/something-important"
        }
    ]
}
```

所有 AFC 自定义策略都需要该AllowCloudFormationActionsOnStacks声明； AWS CloudFormation 使用此角色创建堆栈实例，因此需要权限才能对堆栈执行 AWS CloudFormation 操作。该AllowSsmParameterActions部分特定于正在启用的模板。

解决权限问题

使用受限策略启用蓝图时，您可能会发现没有足够的权限来启用该蓝图。要解决这些问题，请修改您的政策文件并更新成员账户的蓝图偏好以使用更正后的政策。要检查该策略是否足以启用蓝图，请确保已授予 AWS CloudFormation 权限，并且您可以使用该角色直接创建堆栈。

创建基于 Terraform 的 Service Catalog 产品所需的额外权限

使用适用于 AFC 的 Terraform 配置文件创建 AWS Service Catalog 外部产品时，除了创建模板中定义的资源所需的权限外，还 AWS Service Catalog 需要向 AFC 自定义 IAM 策略添加某些权限。如果您选择默认的完整管理员策略，则无需添加这些额外权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "s3:GetObject",
```

```
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        }
    ]
}
```

有关使用中的 “外部” 产品类型创建 Terraform 产品的更多信息 AWS Service Catalog，请参阅《Service Catalog 管理员指南》中的 “步骤 5：创建启动角色”。

使用适用于 Terraform 的 AWS Control Tower Account Factory（AFT）配置账户

AWS Control Tower Account Factory for Terraform (AFT) 采用一种 GitOps 模型，可以自动在 AWS Control Tower 中配置和更新账户。

> **Note**
>
> AFT 不会影响 AWS Control Tower 中的工作流程性能。如果您通过 AFT 或 Account Factory 配置账户，则会出现相同的后端工作流程。

使用 AFT，您可以创建一个账户请求 Terraform 文件，其中包含调用 AFT 工作流程的输入。账户配置和更新完成后，AFT 工作流程继续运行 AFT 账户配置框架和账户自定义步骤。

先决条件

在开始使用 AFT 之前，必须创建以下内容：

- 全面部署的 AFT 环境。有关更多信息，请参阅适用于 Terraform 的 AWS Control Tower 账户工厂 (AFT) 概述和部署适用于 Terraform 的 AWS Control Tower 账户工厂 (AFT)
- 完全部署的 AFT 环境中的一个或多个 AFT `git` 存储库。有关更多信息，请参阅 AFT 的部署后步骤。

> **Tip**
>
> 或者，您可以在aft-account-customizations存储库中创建账户模板文件夹。

有关 AFT AWS 区域 在哪些地方有部署限制的信息，请参见AWS Control Tower 中的限制和配额和控制限制。

在 AFT 开设一个新账户

要使用 AFT 配置新账户，请创建一个账户请求 Terraform 文件。此文件包含aft-account-request存储库中参数的输入。创建账户请求 Terraform 文件后，通过运行开始处理您的账户请求。`git push`此命令调用中的`ct-aft-account-request`操作 AWS CodePipeline，该操作是在账户配置完成后在 AFT 管理账户中创建的。有关更多信息，请参阅 AFT 账户配置管道。

账户请求 Terraform 文件参数

您必须在账户请求 Terraform 文件中包含以下参数。你可以在上查看 Terraform 账户请求文件示例。GitHub

- 的值`module name`必须是每个 AWS 账户 请求的唯一值。
- 的值`module source`是 AFT 提供的账户请求 Terraform 模块的路径。
- 的值`control_tower_parameters`捕获创建 AWS Control Tower 账户所需的输入。该值包括以下输入字段：
  - `AccountEmail`
  - `AccountName`
  - `ManagedOrganizationalUnit`
  - `SSOUserEmail`
  - `SSOUserFirstName`
  - `SSOUserLastName`

> **Note**
>
> 在账户配置期间，`control_tower_parameters`无法更改您提供的输入。
> 支持在aft-account-request存储库`ManagedOrganizationalUnit`中指定的格式包括`OUName`和`OUName (OU-ID)`。

- account_tags捕获用户定义的密钥和值，这些密钥和值可以 AWS 账户 根据业务标准进行标记。有关更多信息，请参阅《AWS Organizations 用户指南》中的为AWS Organizations 资源添加标签。
- 的值会change_management_parameters捕获其他信息，例如创建账户请求的原因以及谁发起了账户请求。该值包括以下输入字段：
  - change_reason
  - change_requested_by
- custom_fields使用密钥和值捕获其他元数据，这些密钥和值作为 SSM 参数部署在 /aft/account-request-request/custom-fields/ 下的销售账户中。您可以在账户自定义期间引用此元数据以部署适当的控件。例如，受监管合规约约束的账户可能会额外部署 AWS Config 规则。在账户配置和更新期间，您收集的元数据custom_fields可能会调用其他处理。如果从账户请求中删除了自定义字段，则该自定义字段将从销售账户的 SSM Parameter Store 中删除。
- （可选）account_customizations_name捕获aft-account-customizations存储库中的账户模板文件夹。有关更多信息，请参阅账户自定义。

提交多个账户申请

AFT 一次处理一个账户申请，但您可以向 AFT 管道提交多个账户请求。当您向 AFT 管道提交多个账户请求时，AFT 会按先入先出的顺序对账户请求进行排队和处理。

> **Note**
>
> 您可以为希望 AFT 配置的每个账户创建一个账户请求 Terraform 文件，或者在单个账户请求 Terraform 文件中级联多个账户请求。

更新现有账户

您可以通过编辑先前提交的账户请求并运行来更新 AFT 提供的账户git push。此命令调用账户配置工作流程并可以处理账户更新请求。您可以更新账户请求 Terraform 文件中其他参数的control_tower_parameters输入（这是所需值的一部分）。ManagedOrganizationalUnit有关更多信息，请参阅使用 AFT 开通新账户。

> **Note**
>
> 在账户配置期间，control_tower_parameters无法更改您提供的输入。

支持在aft-account-request存储库ManagedOrganizationalUnit中指定的格式包括OUName和OUName (OU-ID)。

更新 AFT 未配置的账户

您可以通过在aft-account-request存储库中指定账户来更新在 AFT 之外创建的 AWS Control Tower 账户。

> **Note**
>
> 确保所有账户详情正确无误，并与 AWS Control Tower 组织和相应的 AWS Service Catalog 预配置产品保持一致。

使用 AFT 更新现有版本 AWS 账户 的先决条件

- AWS 账户 必须在 AWS Control Tower 中注册。
- AWS 账户 必须是 AWS Control Tower 组织的一部分。

部署 AWS Control Tower Account Factory for Terraform (AFT)

本节适用于希望在现有环境中设置 Terraform Account Factory (AFT) 的 AWS Control Tower 环境管理员。它描述了如何使用新的专用 AFT 管理账户设置 Account Factory for Terraform (AFT) 环境。

> **Note**
>
> Terraform 模块部署了 AFT。此模块在 AFT 存储库中可用 GitHub，整个 AFT 存储库被视为该模块。
>
> 我们建议您参考上的 AFT 模块， GitHub 而不是克隆 AFT 存储库。这样，您就可以在可用时控制和使用模块的更新。

有关最新版本的 AWS Control Tower Account Factory for Terraform (AFT) 功能的详细信息，请参阅此 GitHub 存储库的版本文件。

部署先决条件

在配置和启动 AFT 环境之前，必须具备以下条件：

- AWS Control Tower 着陆区。有关更多信息，请参阅规划您的 AWS Control Tower 着陆区。
- AWS Control Tower 着陆区域的主区域。有关更多信息，请参阅如何 AWS 区域 使用 AWS Control Tower。
- 一个 Terraform 版本和发行版。有关更多信息，请参阅 Terraform 和 AFT 版本。
- 一个 VCS 提供商，用于跟踪和管理代码和其他文件的更改。默认情况下，AFT 使用 AWS CodeCommit。有关更多信息，请参阅什么是 AWS CodeCommit？ 在《AWS CodeCommit 用户指南》中。如果您想选择其他版本控制系统（VCS）提供商，请参阅 AFT 中源代码版本控制的替代方案。
- 一个运行时环境，你可以在其中运行安装 AFT 的 Terraform 模块。
- AFT 功能选项。有关更多信息，请参阅启用功能选项。

配置并启动适用于 Terraform 的 AWS Control Tower Account Factory

以下步骤假设你熟悉 Terraform 工作流程。您还可以通过关注 Worksho AWS p Studio 网站上的 A FT 实验室简介来了解有关部署 AFT 的更多信息。

第 1 步：启动你的 AWS Control Tower 着陆区

完成 AWS Control Tower 入门中的步骤。在这里，您可以创建 AWS Control Tower 管理账户并设置 AWS Control Tower 着陆区。

> **Note**
>
> 请务必为 AWS Control Tower 管理账户创建一个具有AdministratorAccess证书的角色。有关更多信息，请参阅下列内容：
>
> - 用户指南中的 IAM 身份（用户、AWS Identity and Access Management 用户组和角色）
> - AdministratorAccess在《AWS 托管策略参考指南》中

第 2 步：为 AFT 创建新的组织单位（推荐）

我们建议您在 AWS 组织中创建单独的 OU。这是您部署 AFT 管理帐户的地方。使用您的 AWS Control Tower 管理账户创建新的 OU。有关更多信息，请参阅创建新 OU。

步骤 3：配置 AFT 管理账户

AFT 要求您配置一个专门用于 AFT 管理操作的 AWS 账户。与您的 AWS Control Tower 着陆区关联的 AWS Control Tower 管理账户出售 AFT 管理账户。有关更多信息，请参阅使用 Account Factory 配置 AWS Service Catalog 账户。

> **Note**
>
> 如果您为 AFT 创建了单独的 OU，请务必在创建 AFT 管理账户时选择此 OU。

最长可能需要 30 分钟才能完全配置 AFT 管理账户。

步骤 4：验证 Terraform 环境是否可供部署

此步骤假设你有使用 Terraform 的经验，并且已经准备好了执行 Terraform 的程序。有关更多信息，请参阅 HashiCorp 开发者网站上的 Command: in it。

> **Note**
>
> AFT 支持 Terraform 版本`1.2.0`或更高版本。

第 5 步：调用 Account Factory for Terraform 模块部署 AFT

使用您为拥有AdministratorAccess证书的 AWS Control Tower 管理账户创建的角色调用 AFT 模块。AWS Control Tower 通过 AWS Control Tower 管理账户配置 Terraform 模块，该账户建立了编排 AWS Control Tower Account Factory 请求所需的所有基础设施。

您可以在上查看 AFT 存储库中的 AFT 模块 GitHub。整个 GitHub 存储库被视为 AFT 模块。有关运行 AFT 模块和部署 AFT 所需的输入的信息，请参阅自述文件。或者，您可以在 Terraform 注册表中查看 AFT 模块。

AFT 模块包含一个`aft_enable_vpc`参数，用于指定 AWS Control Tower 是否在中央 AFT 管理账户的虚拟私有云 (VPC) 中配置账户资源。默认情况下，该参数设置为`true`。如果您将此参数设置为`false`，AWS Control Tower 将在不使用 VPC 和私有网络资源（例如 NAT 网关或 VPC 终端节点）的情况下部署 AFT。在某些使用模式下，禁用*`aft_enable_vpc`*可能有助于降低 AFT 的运营成本。

> **Note**
>
> 重新启用`aft_enable_vpc`参数（将值从切换`false`为`true`）可能需要您连续运行`terraform apply`命令两次。

如果您的环境中有用于管理 Terraform 的管道，则可以将 AFT 模块集成到现有的工作流程中。否则，请从任何使用所需凭据进行身份验证的环境中运行 AFT 模块。

超时会导致部署失败。我们建议使用 AWS Security Token Service (STS) 凭证来确保您的超时时间足以进行完整部署。 AWS STS 证书的最小超时时间为 60 分钟。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的 IAM 中的临时安全证书。

> **Note**
>
> 你可能需要等待 30 分钟，AFT 才能完成通过 Terraform 模块的部署。

第 6 步：管理 Terraform 状态文件

部署 AFT 时会生成一个 Terraform 状态文件。这个构件描述了 Terraform 创建的资源的状态。如果你计划更新 AFT 版本，请确保保留 Terraform 状态文件，或者使用 Amazon S3 和 DynamoDB 设置 Terraform 后端。AFT 模块不管理后端 Terraform 状态。

> **Note**
>
> 你有责任保护 Terraform 状态文件。某些输入变量可能包含敏感值，例如私`ssh`钥或 Terraform 令牌。根据您的部署方法，这些值可以在 Terraform 状态文件中以纯文本形式查看。有关更多信息，请参阅 HashiCorp 网站上的状态敏感数据。

部署后步骤

AFT 基础设施部署完成后，请按照以下额外步骤完成设置过程并准备好配置账户。

第 1 步：（可选）CodeConnections 与您想要的 VCS 提供商一起填写

如果您选择第三方 VCS 提供商，AFT 将建立 CodeConnections，并由您进行确认。请参阅AFT 中源代码版本控制的替代方案，了解如何使用首选 VCS 设置 AFT。

建立 AWS CodeStar 连接的第一步由 AFT 完成。您必须确认连接。

第 2 步：（必填）填充每个存储库

AFT 要求您管理四个存储库：

1. 账户请求-此存储库处理账户的放置或更新请求。可用的示例。有关 AFT 账户请求的更多信息，请参阅在 AFT 开设一个新账户。
2. AFT 账户配置自定义 — 在开始全局自定义阶段之前，此存储库管理应用于 AFT 创建和管理的所有账户的自定义。可用的示例。要创建 AFT 账户配置自定义项，请参阅创建您的 AFT 账户配置自定义状态机。
3. 全局自定义 — 此存储库管理应用于由 AFT 创建和管理的所有账户的自定义。可用的示例。要创建 AFT 全局自定义项，请参阅应用全局自定义。
4. 账户自定义 — 此存储库管理的自定义设置仅适用于由 AFT 创建和使用 AFT 管理的特定帐户。可用的示例。要创建 AFT 账户自定义设置，请参阅应用账户自定义。

AFT 希望这些存储库中的每一个都遵循特定的目录结构。用于填充存储库的模板和描述如何填充模板的说明可在 AFT github 存储库的 Account Factory for Terraform 模块中找到。

适用于 Terraform 的 AWS Control Tower Account Factory (AFT) 概述

Account Factory for Terraform (AFT) 设置了 Terraform 管道，以帮助你在 AWS Control Tower 中配置和自定义账户。AFT 为您提供基于 Terraform 的账户配置的优势，同时允许您使用 AWS Control Tower 管理您的账户。

使用 AFT，您可以创建一个账户请求 Terraform 文件以获取触发 AFT 账户配置工作流程的输入。账户配置阶段完成后，AFT 会在账户自定义阶段开始之前自动运行一系列步骤。有关更多信息，请参阅 AFT 账户配置管道。

AFT 支持 Terraform Cloud、Terraform Enterprise 和 Terraform 社区版。使用 AFT，您可以使用输入文件和简单`git push`命令启动账户创建，并自定义新账户或现有账户。账户创建包括 AWS Control Tower 的所有 AWS Control Tower 管理权益和账户自定义，可帮助您满足组织的标准安全程序和合规准则。

AFT 支持账户自定义请求跟踪。每次您提交账户自定义请求时，AFT 都会生成一个唯一的跟踪令牌，该令牌通过 AFT 自定义 AWS Step Functions 状态机传递，该状态机将令牌作为其执行的一部分进行记录。然后，您可以使用 Amazon CloudWatch Logs 见解查询来搜索时间戳范围并检索请求令牌。因此，您可以看到令牌附带的有效负载，因此您可以在整个 AFT 工作流程中跟踪您的账户自定义请求。有关 CloudWatch 日志和 Step Functions 的信息，请参阅以下内容：

- 什么是 Amazon CloudWatch 日志？ 在 Amazon CloudWatch 日志用户指南中
- 什么是 AWS Step Functions？ 在《AWS Step Functions 开发者指南》中

AFT 将构建框架等其他 AWS 服务的功能与部署 Terraform 基础设施即代码 (IaC) 的管道相结合。组件服务AFT 使您能够：

- 在 GitOps 模型中提交账户配置和更新请求
- 存储账户元数据和审计历史记录
- 应用账户级标签
- 为所有账户、一组账户或个人账户添加自定义设置
- 启用功能选项

AFT 创建了一个名为 AFT 管理账户的单独账户来部署 AFT 功能。在设置 AFT 之前，您必须拥有现有的 AWS Control Tower 着陆区。AFT 管理账户与 AWS Control Tower 管理账户不同。

AFT 提供了灵活性

- 平台的灵活性：AFT 支持任何 Terraform 发行版，用于初始部署和持续运行：社区版、云端和企业版。
- 版本控制系统的灵活性：AFT 本机依赖于 AWS CodeCommit，但它支持其他来源。CodeConnections

AFT 提供功能选项

您可以根据最佳实践启用多个功能选项：

- 创建 CloudTrail 用于记录数据事件的组织级别
- 删除账户的 AWS 默认 VPC
- 将已配置的账户注册到 Enterprise Su AWS pport 计划中

> **Note**
>
> AFT 管道不适用于部署您的账户运行应用程序所需的资源，例如 Amazon EC2 实例。它仅用于自动配置和自定义 AWS Control Tower 账户。

视频演练

这段视频 (7:33) 描述了如何使用适用于 Terraform 的 AWS Control Tower Account Factory 部署账户。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

AWS Control Tower 中自动配置账户的视频演练。

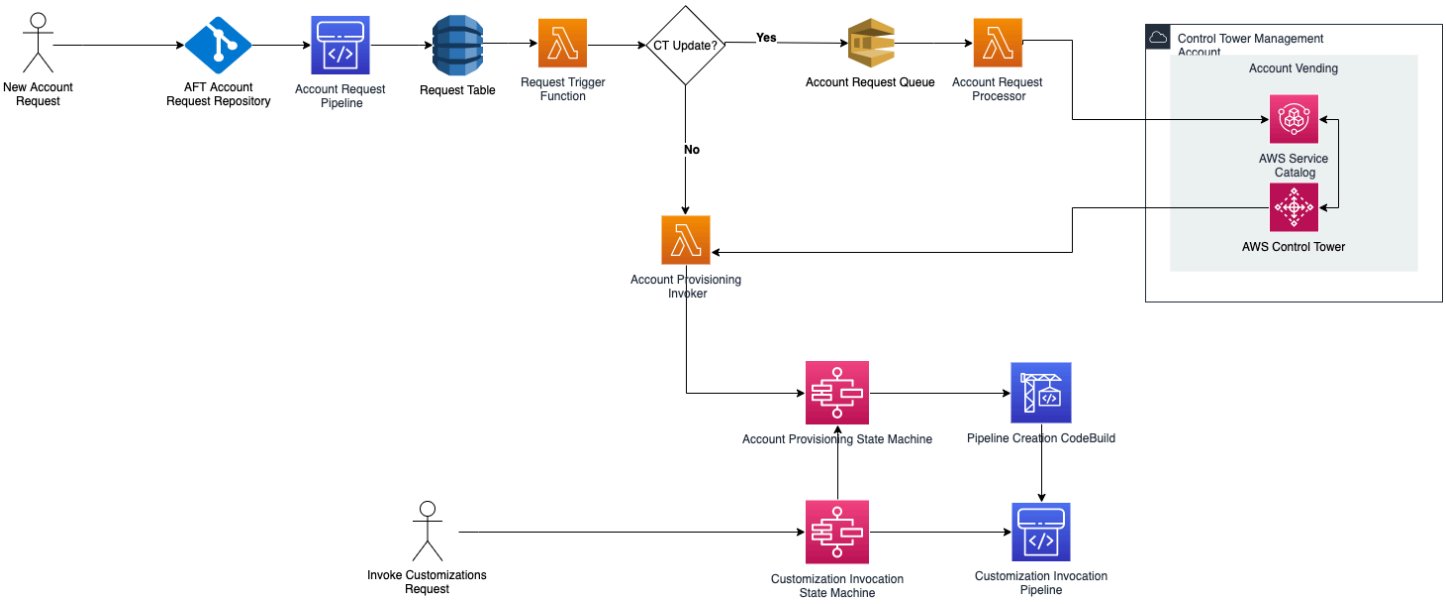
AFT 架构

操作顺序

您在 AFT 管理账户中运行 AFT 操作。对于完整的账户配置工作流程，图中从左到右的阶段顺序如下：

1. 账户请求已创建并提交给管道。您一次可以创建和提交多个账户申请。Account Factory 处理 first-in-first-out 订单中的请求。有关更多信息，请参阅提交多个账户申请。
2. 每个账户都已预配置。此阶段在 AWS Control Tower 管理账户中运行。
3. 全局自定义项在为每个已售账户创建的管道中运行。
4. 如果在初始账户配置请求中指定了自定义，则自定义仅在目标账户上运行。如果您的账户已配置完毕，则必须在该账户的管道中手动启动进一步的自定义设置。

适用于 Terraform 的 AWS Control Tower Account Factory — 账户配置工作流程



费用

AFT 不收取任何额外费用。您只需为 AFT 部署的资源、AFT 启用的 AWS 服务以及在 AFT 环境中部署的资源付费。

默认 AFT 配置包括 AWS PrivateLink 端点分配（用于增强数据保护和安全性）以及需要支持的 NAT 网关 AWS CodeBuild。有关此基础设施定价的详细信息，请参阅 NA T 网关的AWS PrivateLink 定价和 Amazon VPC 定价。有关管理这些费用的更多具体信息，请联系您的 AWS 客户代表。您可以更改 AFT 的这些默认设置。

Terraform 和 AFT 版本

Account Factory for Terraform (AFT) 支持 Terraform 版本或更高版本。`1.2.0`您必须提供 Terraform 版本作为 AFT 部署过程的输入参数，如以下示例所示。

```
terraform_version = "1.2.0"
```

Terraform 分布

AFT 支持三种 Terraform 发行版：

- Terraform 社区版
- terraform Cloud
- Terraform Enter

以下各节将对这些分布进行说明。在 AFT 引导过程中，提供您选择的 Terraform 分布作为输入参数。有关 AFT 部署和输入参数的更多信息，请参阅部署 AWS Control Tower Account Factory for Terraform (AFT)。

如果您选择 Terraform Cloud 或 Terraform Enterprise 发行版，则指定的 API 令牌`terraform_token`必须是用户或团队 API 令牌。并非所有必需的 API 都支持组织令牌。出于安全考虑，您必须避免通过分配 terraform 变量来将此令牌的值签入版本控制系统 (VCS)，如以下示例所示。

```
# Sensitive variable managed in Terraform Cloud:
terraform_token = var.terraform_cloud_token
```

Terraform 社区版

当你选择 Terraform 社区版作为发行版时，AFT 会在 AFT 管理账户中为你管理 Terraform 后端。AFT 会`terraform-cli`下载您指定的 Terraform 版本以在 AFT 部署和 AFT 管道阶段运行。生成的 Terraform 状态配置存储在 Amazon S3 存储桶中，其命名形式如下：

```
aft-backend-[account_id]-primary-region
```

AFT 还会创建一个 Amazon S3 存储桶，用于将您的 Terraform 状态配置复制到另一个存储桶 AWS 区域，用于灾难恢复，其命名形式如下：

```
aft-backend-[account_id]-secondary-region
```

我们建议您在这些 Terraform 状态的 Amazon S3 存储桶上为删除功能启用多重身份验证 (MFA)。要了解有关 Terraform 社区版的更多信息，请参阅 Terraform 文档。

要选择 Terraform OSS 作为您的发行版，请提供以下输入参数：

```
terraform_distribution = "oss"
```

terraform Cloud

当你选择 Terraform Cloud 作为发行版时，AFT 会为你的 Terraform Cloud 组织中的以下组件创建工作空间，从而启动 API 驱动的工作流程。

- 账户申请
- AFT 提供的账户的 AFT 自定义
- 为 AFT 提供的账户进行账户自定义
- AFT 提供的账户的全球自定义

Terraform Cloud 管理生成的 Terraform 状态配置。

当您选择 Terraform Cloud 作为发行版时，请提供以下输入参数：

- `terraform_distribution = "tfc"`
- `terraform_token`— 此参数包含 Terraform Cloud 令牌的值。AFT 将标记为敏感，并将该值作为安全字符串存储在 AFT 管理账户的 SSM 参数存储中。我们建议您根据公司的安全政策和合规准则定期轮换 Terraform 代币的价值。Terraform 令牌应该是用户或团队级别的 API 令牌。不支持组织令牌。
- `terraform_org_name`— 此参数包含你的 Terraform Cloud 组织的名称。

> **Note**
>
> 不支持在单个 Terraform Cloud 组织中部署多个 AFT。

有关如何设置 Terraform Cloud 的信息，请参阅 Terra form 文档。

Terraform Enter

当你选择 Terraform Enterprise 作为发行版时，AFT 会为你的 Terraform Enterprise 组织中的以下组件创建工作空间，并触发 API 驱动的工作流程，用于生成的 Terraform 运行。

- 账户申请
- AFT 为由 AFT 配置的账户进行账户配置自定义
- AFT 为账户配置的账户进行账户自定义
- AFT 提供的账户的全局自定义

生成的 Terraform 状态配置由你的 Terraform Enterprise 设置管理。

要选择 Terraform Enterprise 作为发行版，请提供以下输入参数：

- `terraform_distribution = "tfe"`
- `terraform_token`— 此参数包含您的 Terraform Enterprise 代币的值。AFT 将其值标记为敏感值，并将其作为安全字符串存储在 SSM 参数存储区的 AFT 管理账户中。我们建议您根据公司的安全政策和合规准则，定期轮换 Terraform 代币的价值。
- `terraform_org_name`— 此参数包含您的 Terraform Enterprise 组织的名称。
- `terraform_api_endpoint`— 此参数包含你的 Terraform Enterprise 环境的网址。此参数的值必须采用以下格式：

```
https://{fqdn}/api/v2/
```

有关如何设置 Terraform Enterprise 的更多信息，请参阅 Terraform 文档。

查看 AFT 版本

您可以通过查询 AWS SSM 参数存储区密钥来检查已部署的 AFT 版本：

```
/aft/config/aft/version
```

如果您使用注册表方法，则可以固定版本。

```
module "control_tower_account_factory" {
```

```
  source  = "aws-ia/control_tower_account_factory/aws"
  version = "1.3.2"
  # insert the 6 required variables here
}
```

您可以在 AFT 存储库中查看有关 AFT 版本的更多信息。

更新 AFT 版本

您可以通过从main存储库分支中提取已部署的 AFT 版本来更新该版本：

```
terraform get -update
```

拉取完成后，您可以重新运行 Terraform 计划或运行 apply 以使用最新更改更新 AFT 基础架构。

启用功能选项

AFT 根据最佳实践提供功能选项。在 AFT 部署期间，您可以通过功能标志选择使用这些功能。有关 在 AFT 开设一个新账户 AFT 输入配置参数的更多信息，请参阅。

默认情况下，这些功能未启用。您必须在您的环境中明确启用每个选项。

主题

- AWS CloudTrail 数据事件
- AWS 企业 Support 计划
- 删除 AWS 默认 VPC

AWS CloudTrail 数据事件

启用后， AWS CloudTrail 数据事件选项将配置这些功能。

- 在 AWS Control Tower 管理账户中创建组织跟踪，用于 CloudTrail
- 开启亚马逊 S3 和 Lambda 数据事件的日志记录
- 使用加密功能加密所有 CloudTrail 数据事件并将其导出到 AWS Control Tower 日志存档账户中的 `aws-aft-logs-*` S3 存储桶 AWS KMS
- 开启日志文件验证设置

要启用此选项，请在您的 AFT 部署输入配置中将以下功能标志设置为 True。

```
aft_feature_cloudtrail_data_events
```

先决条件

在启用此功能选项之前，请确保在您的组织中 AWS CloudTrail 启用了的可信访问权限。

要检查以下各项的可信访问状态，请执行 CloudTrail 以下操作：

1. 导航到 AWS Organizations 控制台。
2. 选择 “服务” > CloudTrail。
3. 然后根据需要选择右上角的 “启用可信访问”。

您可能会收到一条警告消息，建议您使用 AWS CloudTrail 控制台，但在这种情况下，请忽略该警告。在您允许可信访问之后，AFT 会创建跟踪，作为启用此功能选项的一部分。如果未启用可信访问，则当 AFT 尝试为数据事件创建跟踪时，您将收到一条错误消息。

> **Note**
>
> 此设置适用于组织级别。启用此设置会影响中的所有账户 AWS Organizations，无论这些账户是否由 AFT 管理。启用时 AWS Control Tower 日志存档账户中的所有存储桶都将排除在 Amazon S3 数据事件之外。要了解更多信息，请参阅《 AWS CloudTrail 用户指南》CloudTrail。

AWS 企业 Support 计划

启用此选项后，AFT 管道将为由 AFT 配置的账户开启 AWS 企业支持计划。

AWS 默认情况下，账户已启用 B AWS asic Support 计划。AFT 为由 AFT 提供的账户自动注册到企业支持级别。配置过程会为该账户打开支持请求，请求将其添加到 E AWS nterprise Support 计划中。

要启用 Enterprise Support 选项，请在 AFT 部署输入配置中将以下功能标志设置为 True。

```
aft_feature_enterprise_support=false
```

要了解有关AWS 支持计划的更多信息，请参阅比较 AWS 支持计划。

> **Note**
>
> 要允许此功能运行，您必须将付款人账户注册到 Enterprise Support 计划中。

删除 AWS 默认 VPC

启用此选项后，AFT 会删除管理账户中的所有 AWS 默认 VPC 以及所有默认 VPC AWS 区域，即使这些 AWS 区域虚拟私有云中尚未部署 AWS Control Tower 资源也是如此。

AFT 不会自动删除 AFT 配置的任何 AWS Control Tower 账户或您通过 AFT 在 AWS Control Tower 中注册的现有 AWS 账户的 AWS 默认 VPC。

默认情况下，创建新 AWS 账户时每个 AWS 区域账户都设置了 VPC。您的企业可能有创建 VPC 的标准做法，这要求您删除 AWS 默认 VPC 并避免将其启用，尤其是对于 AFT 管理账户。

要启用此选项，请在您的 AFT 部署输入配置中将以下功能标志设置为 True。

```
aft_feature_delete_default_vpcs_enabled
```

要了解有关默认 VPC 的更多信息，请参阅默认 VPC 和默认子网。

适用于 Terraform 的 AWS Control Tower Account Factory 的资源注意事项

当您使用适用于 Terraform 的 AWS Control Tower Account Factory 设置着陆区时，会在您的 AWS 账户中创建多种类型的 AWS 资源。

搜索资源

- 您可以使用标签搜索最新的 AFT 资源列表。您搜索的键值对是：

```
Key: managed_by | Value: AFT
```

- 对于不支持标签的组件服务，您可以通过在资源名称`aft`中搜索来查找资源。

按账户分列的初始创建的资源表

适用于 Terraform 的 AWS Control Tower Account Factory 管理账户

AWS service	资源类型	资源名称
AWS Identity and Access Management	角色	AWSAFTAdministrator AWSAFTExecution AWSAFTService aws-ct-aft-*
AWS Identity and Access Management	策略	aws-ct-aft-*
CodeCommit	Repositories	aws-ct-aft-*
CodeBuild	构建项目	aws-ct-aft-*
代码管道	管线	*-baseline-*
Amazon S3	存储桶	*-aws-ct-aft-* aws-ct-aft-*
Lambda	函数	aws-ct-aft-*
Lambda	图层	aws-ct-aft-common-layer
DynamoDB	表	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	状态机	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline

AWS service	资源类型	资源名称
		aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc
Amazon SNS	主题	aws-ct-aft-notifications aws-ct-aft-failure-notifications
Amazon EventBridge	事件总线	aws-ct-aft-events-from-ct-management
Amazon EventBridge	赛事规则	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor
密钥管理服务 (KMS)	客户托管密钥	*-aws-ct-aft-* aws-ct-aft-*
AWS Systems Manager	参数存储	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	队列	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	日志组	/aws/*/aws-ct-aft-* aws-ct-aft-*
AWS Support Center（可选）	Support 计划	Enterprise

AWS 通过 AWS Control Tower Account Factory 为 Terraform 配置的账户

AWS service	资源类型	资源名称
AWS Identity and Access Management	角色	AWSAFTExecution
AWS Support Center（可选）	Support 计划	Enterprise

AWS Control Tower 管理账户

AWS service	资源类型	资源名称
AWS Identity and Access Management	角色	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-controltower-events-rule
AWS Systems Manager	参数存储	/aws-ct-aft/account/aws-ct-aft-management/account-id
AWS Organizations （可选）	服务控制策略	aws-ct-aft-protect-resources
CloudTrail （可选）	跟踪	aws-ct-aft-BaselineCloudTrail
AWS Support 中心（可选）	Support 计划	Enterprise

AWS Control Tower 日志存档账户

AWS service	资源类型	资源名称
AWS Identity and Access Management	角色	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-cloudtrail-data-events-role

AWS service	资源类型	资源名称
密钥管理服务 (KMS)	客户托管密钥	*-aws-ct-aft-kms-gd-findings
Amazon S3	存储桶	*-aws-ct-aft-logs* aws-ct-aft-s3-access-logs*
AWS Support Center（可选）	Support 计划	Enterprise

AWS Control Tower 审计账户

AWS service	资源类型	资源名称
AWS Identity and Access Management	角色	AWSAFTExecutionRole AWSAFTExecution
AWS Support Center（可选）	Support 计划	Enterprise

必填角色

一般而言，角色和策略是中身份和访问管理 (IAM) 的一部分 AWS。有关更多信息，请参阅 AWS IAM 用户指南。

AFT 在 AFT 管理账户和 AWS Control Tower 管理账户中创建了多个 IAM 角色和策略，以支持 AFT 管道的运营。这些角色是根据最低权限访问模型创建的，该模型将权限限制为每个角色和策略所需的最低限度操作和资源集。为这些角色和策略分配了一`key:value`对 AWS 标签， `managed_by:AFT`以便识别。

除了这些 IAM 角色外，AFT 还创建了三个基本角色：

- `AWSAFTAdmin`角色
- `AWSAFTExecution`角色
- `AWSAFTService`角色

以下各节将对这些角色进行说明。

AWSAFTAdmin 角色解释

部署 AFT 时，AWSAFTAdmin角色将在 AFT 管理账户中创建。此角色允许 AFT 管道担任 AWS Control Tower 和 AFT 预配置账户中的AWSAFTExecution角色，从而执行与账户配置和自定义相关的操作。

以下是附加到AWSAFTAdmin角色的内联策略（JSON 工件）：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::*:role/AWSAFTExecution",
                "arn:aws:iam::*:role/AWSAFTService"
            ]
        }
    ]
}
```

以下 JSON 构件显示了该AWSAFTAdmin角色的信任关系。占位符号被 012345678901 AFT 管理账户 ID 号所取代。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTExecution 角色解释

部署 AFT 时，AWSAFTExecution角色将在 AFT 管理账户和 AWS Control Tower 管理账户中创建。稍后，AFT 管道在 AFT 账户配置阶段在每个 AFT 预配置账户中创建AWSAFTExecution角色。

AFT 最初使用该AWSControlTowerExecution角色在指定账户中创建AWSAFTExecution角色。该AWSAFTExecution角色允许 AFT 管道运行在 AFT 框架的配置和配置自定义阶段执行的步骤，适用于已置备的 AFT 账户和共享账户。

> **不同的角色可以帮助你限制范围**
>
> 最佳做法是，将自定义权限与资源初始部署期间允许的权限分开。请记住，该AWSAFTService角色用于账户配置，该AWSAFTExecution角色用于账户自定义。这种分离限制了管道每个阶段允许的权限范围。如果您要自定义 AWS Control Tower 共享账户，这种区别尤其重要，因为共享账户可能包含敏感信息，例如账单详情或用户信息。

AWSAFTExecution角色权限：AdministratorAccess— AWS 托管策略

以下 JSON 构件显示了附加到该AWSAFTExecution角色的 IAM 策略（信任关系）。占位符号被 012345678901 AFT 管理账户 ID 号所取代。

的信任政策 AWSAFTExecution

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTService 角色解释

该AWSAFTService角色在所有已注册和托管账户（包括共享账户和管理账户）中部署 AFT 资源。以前的资源只能由该AWSAFTExecution角色部署。

该AWSAFTService角色旨在供服务基础架构用于在配置阶段部署资源，而该AWSAFTExecution角色仅用于部署自定义项。通过以这种方式担任角色，您可以在每个阶段保持更精细的访问控制。

AWSAFTService角色权限：AdministratorAccess— AWS 托管策略

以下 JSON 构件显示了附加到该AWSAFTService角色的 IAM 策略（信任关系）。占位符号被 012345678901 AFT 管理账户 ID 号所取代。

的信任政策 AWSAFTService

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

组件服务

部署 AFT 时，会将每项 AWS 服务中的组件添加到您的 AWS 环境中。

- AWS Control Tower — AFT 使用 AWS Control Tower 管理账户中的 AWS Control Tower Account Factory 来配置账户。
- Amazon DynamoDB — AFT 在 AFT 管理账户中创建亚马逊 DynamoDB 表，用于存储账户请求、账户更新的审计历史记录、账户元数据和 AWS Control Tower 生命周期事件。AFT 还会创建 DynamoDB Lambda 触发器来启动下游流程，例如启动 AFT 账户配置工作流程。
- 亚马逊简单存储服务 — AFT 在 AFT 管理账户和 AWS Control Tower 日志存档账户中创建亚马逊简单存储服务 (S3) 存储桶，后者存储 AFT 管道所需的 AWS 服务生成的日志。AFT 还在主要和次要 AWS 区域中创建一个 Terraform 后端 S3 存储桶，用于存储 AFT 管道工作流程期间生成的 Terraform 状态。
- 亚马逊简单通知服务 — AFT 在 AFT 管理账户中创建亚马逊简单通知服务 (SNS) Simple Notification Service 主题，该账户在处理每个 AFT 账户请求后存储成功和失败通知。您可以使用您选择的协议来接收这些消息。
- 亚马逊简单队列服务 — AFT 在 AFT 管理账户中创建亚马逊简单队列服务 (Amazon SQS) FIFO 队列。该队列允许您并行提交多个账户请求，但它一次只能向 AWS Control Tower Account Account Factory 发送一个请求进行顺序处理。

- AWS CodeBuild — AFT 在 AFT 管理账户中创 CodeBuild 建 AWS 构建项目，以便在各个构建阶段初始化、编译、测试和应用 AFT 源代码的 Terraform 计划。
- AWS CodePipeline — AFT 在 AFT 管理账户中创建 AWS CodePipeline 管道，以便与您选择的、支持的 AWS CodeStar 连接提供商集成 AFT 源代码，并在 AWS 中触发构建任务 CodeBuild。
- AWS Lambda — AFT 在 AFT 管理账户中创建 AWS Lambda 函数和层，以便在账户请求、AFT 账户配置和账户自定义过程中执行步骤。
- AWS Systems Manager Parameter Stor e — AFT 在 AFT 管理账户中设置 AWS Systems Manager Parameter Store，用于存储 AFT 管道流程所需的配置参数。
- 亚马逊 CloudWatch — A FT 在 AFT 管理账户中创建亚马逊 CloudWatch 日志组，用于存储 AFT 管道使用的 AWS 服务生成的日志。 CloudWatch 日志的保留期限设置为`Never Expire`。
- Amazon VPC — AFT 创建亚马逊虚拟私有云 (VPC)，将 AFT 管理账户中的服务和资源隔离到单独的网络环境中，从而增强安全性。
- AWS KMS — AFT 在 AFT 管理账户和 AWS Control Tower 日志存档账户中使用 AWS 密钥管理服务 (KMS)。AFT 创建密钥来加密 Terraform 状态、存储在 DynamoDB 表中的数据和 SNS 主题。这些日志和项目是在 AFT 部署 AWS 资源和服务时生成的。默认情况下，AFT 创建的 KMS 密钥已启用年度轮换。
- AWS Identity and Access Management (IAM) — AFT 遵循推荐的最低权限模型。它根据需要在 AFT 管理账户、AWS Control Tower 账户和 AFT 预配置账户中创建 AWS Identity and Access Management (IAM) 角色和策略，以执行 AFT 管道工作流程中所需的操作。
- AWS Step Fun ctions — AFT 在 AFT 管理账户中创建 AWS Step Functions 状态机。这些状态机协调和自动化 AFT 账户配置框架和自定义的流程和步骤。
- 亚马逊 EventBridge — AFT 在 AFT 和 AWS Control Tower 管理账户中创建亚马逊 EventBridge事件总线，用于在 AFT 管理账户的 DynamoDB 表中长期捕获和存储 AWS 控制塔生命周期事件。AFT 在 AFT 管理账户和 AWS Control Tower 管理账户中创建 AWS CloudWatch 事件规则，这些规则会触发 AFT 管道工作流程运行期间所需的多个步骤
- AWS CloudTrail （可选）— 启用此功能后，AFT 将在 AWS Control Tower 管理账户中创建 AWS CloudTrail 组织跟踪，用于记录 Amazon S3 存储桶和 AWS Lambda 函数的数据事件。AFT 将这些日志发送到 AWS Control Tower 日志存档账户中的中央 S3 存储桶。
- AWS Support（可选）— 启用此功能后，AFT 将为 AFT 预配置的账户启用 AWS 企业支持计划。默认情况下，AWS 账户是在启用 AWS Basic Support 计划的情况下创建的。

AFT 账户配置管道

管道的账户配置阶段完成后，AFT 框架将继续。它会自动运行一系列步骤，以确保在账户自定义阶段开始之前，新配置的账户已准备就绪。

以下是 AFT 管道运行的后续步骤。

1. 验证账户请求输入。
2. 检索有关已配置账户的信息，例如账户 ID。
3. 将账户元数据存储在 AFT 管理账户的 DynamoDB 表中。
4. 在新配置的账户中创建 AWSAFTExecutionIAM 角色。AFT 担任此角色是为了执行账户自定义阶段，因为该角色授予对账户工厂投资组合的访问权限。
5. 应用您在账户请求输入参数中提供的账户标签。
6. 应用您在部署 AFT 时选择的 AFT 功能选项。
7. 应用您提供的 AFT 账户配置自定义。下一节将详细介绍如何在`git`存储库中使用 AWS Step Functions 状态机设置这些自定义项。此阶段有时被称为账户配置框架阶段。这是核心配置过程的一部分，但是您之前已经设置了一个框架，该框架将自定义集成作为账户配置工作流程的一部分，然后在下一阶段向账户添加其他自定义项。
8. 对于配置的每个账户，它都会 AWS CodePipeline 在 AFT 管理账户中创建一个账户，该账户将运行以执行（下一个全局）账户自定义阶段。
9. 为已配置（和定向）的每个账户调用账户自定义管道。
10. 向 SNS 主题发送成功或失败通知，您可以从中检索消息。

使用状态机设置账户配置框架自定义

如果您在配置账户之前设置了自定义的非 TerraForm 集成，则这些自定义项将包含在您的 AFT 账户配置工作流程中。例如，您可能需要进行某些自定义，以确保AFT创建的所有账户都符合您组织的标准和政策，例如安全标准，并且可以在进行其他自定义之前将这些标准添加到帐户中。在接下来的全局账户自定义阶段开始之前，将在每个已配置的账户上实施这些账户配置框架自定义。

> **Note**
>
> 本节中描述的 AFT 功能适用于了解 AWS Step Functions 功能的高级用户。作为替代方案，我们建议您在账户自定义阶段与全球助手合作。

AFT 账户配置框架调用由您定义的 AWS Step Functions 状态机来实现您的自定义。请参阅 AWS Step Functions 文档，详细了解可能的状态机集成。

以下是一些常见的集成。

- AWS Lambda 以您选择的语言运行
- 使用 Docker 容器的 AWS ECS 或 AWS Fargate 任务
- 使用自定义工作程序的 AWS Step Functions 活动，托管在 AWS 或本地
- 亚马逊 SNS 或 SQS 集成

如果未定义 AWS Step Functions 状态机，则该阶段将在空操作的情况下通过。要创建 AFT 账户配置自定义状态机，请按照中的说明进行操作。创建您的 AFT 账户配置自定义状态机在添加自定义项之前，请确保已具备先决条件。

这些类型的集成不是 AWS Control Tower 的一部分，也不能在 AFT 账户定制的全球 API 之前阶段添加它们。相反，AFT 管道允许您将这些自定义设置设置为配置过程的一部分，并在配置工作流程中运行。如以下各节所述，在开始 AFT 账户配置阶段之前，您必须通过提前创建状态机来实现这些自定义。

创建状态机的先决条件

- 全面部署的 AFT。有关 AFT 部署部署 AWS Control Tower Account Factory for Terraform (AFT)的更多信息，请参阅。
- 在您的环境中为 AFT 账户配置自定义设置`git`存储库。请参阅部署后步骤了解更多信息。

创建您的 AFT 账户配置自定义状态机

步骤 1：修改状态机定义

修改`customizations.asl.json`状态机定义示例。该示例可在您为存储 AFT 账户配置自定义项而设置的存储`git`库中、部署后步骤中找到。要了解有关状态机定义的更多信息，请参阅 AWS Step Functions 开发人员指南。

第 2 步：包括相应的 Terraform 配置

将带有`.tf`扩展名的 Terraform 文件与自定义集成的状态机定义放在同一个`git`存储库中。例如，如果您选择在状态机任务定义中调用 Lambda 函数，则需要将该`lambda.tf`文件包含在同一目录中。确保包含自定义配置所需的 IAM 角色和权限。

当您提供适当的输入时，AFT 管道会自动调用您的状态机并将您的自定义设置作为 AFT 账户配置框架阶段的一部分进行部署。

重新启动 AFT 账户配置框架和自定义

AFT 为通过 AFT 管道出售的每个账户运行账户配置框架和自定义步骤。要重新启动账户配置自定义，您可以使用以下两种方法之一：

1. 在账户请求存储库中对现有账户进行任何更改。
2. 在 AFT 开设一个新账户。

账户自定义

AFT 可以在已配置的账户中部署标准或自定义配置。在 AFT 管理账户中，AFT 为每个账户提供一个管道。通过此渠道，您可以在所有账户、一组账户或个人账户中实现自定义。您可以运行 Python 脚本、bash 脚本和 Terraform 配置，也可以在账户自定义阶段与 AWS CLI 进行交互。

概述

在您选择的`git`存储库（存储全局自定义项或存储账户自定义项的存储库）中指定自定义项后，AFT 管道将自动完成账户自定义阶段。要追溯自定义帐户，请参阅重新调用自定义。

全局自定义（可选）

您可以选择将某些自定义设置应用于 AFT 配置的所有账户。例如，如果您需要创建特定的 IAM 角色或在每个账户中部署自定义控件，AFT 管道中的全局自定义阶段允许您自动执行此操作。

账户自定义（可选）

要以不同于其他 AFT 预配置账户的方式自定义个人账户或一组账户，您可以利用 AFT 管道的账户自定义部分来实现特定于账户的配置。例如，只有特定的账户可能需要访问互联网网关。

自定义先决条件

在开始自定义账户之前，请确保满足这些先决条件。

- 全面部署的 AFT。有关如何部署的信息，请参阅配置并启动适用于 Terraform 的 AWS Control Tower Account Factory。
- 预先填充的`git`存储库，用于在您的环境中进行全局自定义和账户自定义。有关更多信息，请参阅中的部署后步骤步骤 3：填充每个存储库。

应用全局自定义

要应用全局自定义，必须将特定的文件夹结构推送到所选存储库。

- 如果您的自定义配置采用 Python 程序或脚本的形式，请将其放在存储库中的 api_helpers/ python 文件夹下。
- 如果您的自定义配置采用 Bash 脚本的形式，请将其放在存储库中的 api_helpers 文件夹下。
- 如果您的自定义配置采用 Terraform 的形式，请将其放在存储库中的 terraform 文件夹下。
- 有关创建自定义配置的更多详细信息，请参阅全局自定义 README 文件。

> **Note**
>
> 在 AFT 管道的 AFT 账户配置框架阶段之后，会自动应用全局定制。

应用账户自定义

您可以通过将特定的文件夹结构推送到所选存储库来应用账户自定义。账户自定义在 AFT 管道中和全球定制阶段之后自动应用。您还可以在账户自定义存储库中创建多个包含不同账户自定义项的文件夹。对于您需要的每个账户自定义，请使用以下步骤。

应用账户自定义

1. 步骤 1：为账户自定义创建文件夹

   在您选择的存储库中，将 AFT 提供的ACCOUNT_TEMPLATE文件夹复制到新文件夹。新文件夹的名称应与您在账户申请中提供的名称一致。account_customizations_name

2. 将配置添加到您的特定账户自定义文件夹

   您可以根据配置的格式将配置添加到您的账户自定义文件夹。

   - 如果你的自定义配置采用 Python 程序或脚本的形式，请将其放在存储库中的 ***[account_customizations_name] /api_*** helpers/p ython 文件夹下。
   - 如果您的自定义配置采用 Bash 脚本的形式，请将其放在存储库中的 ***[account_customizations_name] /api_*** helpers 文件夹下。
   - 如果你的自定义配置采用 Terraform 的形式，请将其放在存储库中的 ***[account_customizations_name]*** /terraform 文件夹下。

有关创建自定义配置的更多信息，请参阅账户自定义 README 文件。

3. 请参阅账户请求文件中的特定**account_customizations_name**参数

   AFT 账户请求文件包含输入参数account_customizations_name。输入您的账户自定义名称作为此参数的值。

> **Note**
>
> 您可以为环境中的账户提交多个账户申请。如果您想应用不同或相似的账户自定义设置，请使用账户请求中的account_customizations_name输入参数指定账户自定义。有关更多信息，请参阅提交多个账户申请。

重新调用自定义

AFT 提供了一种在 AFT 管道中重新调用自定义项的方法。当您添加了新的自定义步骤或对现有自定义项进行更改时，此方法非常有用。当您重新调用时，AFT 会启动自定义管道以对 AFT 配置的账户进行更改。 event-source-based 重新调用允许您对个人账户、所有账户、根据其 OU 对账户或根据标签选择的账户应用自定义设置。

按照以下三个步骤重新调用 AFT 配置的账户的自定义设置。

第 1 步：将更改推送到全局或账户自定义存储库 **git**

您可以根据需要更新您的全局和账户自定义设置，并将更改推送回您的git存储库。此时，什么也没发生，自定义管道必须由事件源调用，如接下来的两个步骤所述。

步骤 2：启动 AWS Step 函数运行以重新调用自定义项

AFT 提供在 AFT 管理账户aft-invoke-customizations中调用的 AWS 步骤函数。该功能的目的是重新调用 AFT 配置的账户的自定义管道。

以下是您可以创建的事件架构（JSON 格式）的示例，用于将输入传递给 aft-invoke-customizations AWS Step 函数。

```
{
```

```
  "include": [
    {
      "type": "all"
    },
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ],

  "exclude": [
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ]
}
```

示例事件架构显示，您可以选择要在重新调用过程中包含或排除的帐户。您可以按组织单位 (OU)、账户标签和账户 ID 进行筛选。如果您未应用任何筛选条件并添加声明`"type":"all"`，则会重新调用所有 AFT 配置账户的自定义设置。

> **Note**
>
> 如果您的 AWS Control Tower 版本是 1.6.5 或更高版本，则可以使用语法将嵌套的 OU 作为目标`OU Name (ou-id-1234)`。有关更多信息，请参阅以下主题GitHub。

填写事件参数后，Step Functions 会运行并调用相应的自定义设置。AFT 一次最多可以调用 5 个自定义。Step Functions 会等待并循环，直到所有符合事件标准的账户都完成为止。

步骤 3：监控 AWS 步骤函数输出并观察 AWS 的 CodePipeline 运行情况

- 生成的 Step Function 输出包含与 Step Function 输入事件源匹配的账户 ID。
- 在 “开发者工具” CodePipeline 下导航到 AWS，查看账户 ID 的相应自定义渠道。

使用 AFT 账户自定义请求跟踪进行故障排除

基于包含目标账户和自定义请求 ID 的 AWS Lambda 发射日志的账户自定义工作流程。AFT 允许您使用 Amazon CloudWatch Logs 跟踪自定义请求并对其进行故障排除，方法是向您提供 L CloudWatch ogs Insights 查询，您可以使用这些查询按目标账户或自定义请求 ID 筛选与您的自定义请求相关的 CloudWatch 日志。有关更多信息，请参阅《亚马逊日志用户指南》中的使用 Amaz CloudWatch on Logs 分析 CloudWatch 日志数据。

使用 AFT 的 CloudWatch 日志见解

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择日志，然后选择日志见解。
3. 选择 “查询”。
4. 在 “示例查询” 下，选择 Terraform 的 Account Factor y，然后选择以下查询之一：

    - 按账户 ID 排列的自定义日志

    > **Note**
    >
    > 请务必将 *“#### ID” ####### ID*。

    ```
    fields @timestamp, log_message.account_id as target_account_id,
     log_message.customization_request_id as customization_request_id,
     log_message.detail as detail, @logStream
    | sort @timestamp desc
    | filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /
    customization_request_id/
    ```

    - 按自定义请求 ID 排列的自定义日志

> **Note**
>
> 请务必将 *“#########” ############*您可以在 AFT 账户配置框架 AWS Step Functions 状态机的输出中找到您的自定义请求 ID。有关 AFT 账户配置框架的更多信息，请参阅 AFT 账户配置管道

```
fields @timestamp, log_message.account_id as target_account_id,
 log_message.customization_request_id as customization_request_id,
 log_message.detail as detail, @logStream
| sort @timestamp desc
| filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
```

5. 选择查询后，请确保选择时间间隔，然后选择 “运行查询”。

AFT 中源代码版本控制的替代方案

AFT 原生使用 AWS CodeCommit 源代码版本控制系统 (VCS)，但它允许其他CodeConnections满足您的业务需求或现有架构的系统。您可以指定第三方 VCS 作为 AFT 部署先决条件的一部分。

AFT 支持以下源代码控制替代方案：

- GitHub
- GitHub 企业服务器
- BitBucket

如果您选择 AWS CodeCommit 作为 VCS，则无需执行其他步骤。默认情况下，AFT 使用默认名称在您的环境中创建必要的`git`存储库。但是，您可以根据需要覆盖默认存储库名称，以符合您的组织标准。 CodeCommit

使用 AFT 设置备用源代码版本控制系统（自定义 VCS）

要为 AFT 部署设置备用源代码版本控制系统，请按照以下步骤操作。

步骤 1：在支持的第三方版本控制系统 (VCS) 中创建**`git`**存储库。

如果您不使用 AWS CodeCommit，则必须在 AFT 支持的第三方 VCS 提供商环境中为以下项目创建`git`存储库。

- AFT 账户申请。提供示例代码。有关 AFT 账户请求的更多信息，请参阅在 AFT 开设一个新账户。
- AFT 账户配置自定义。提供示例代码。有关 AFT 账户配置自定义的更多信息，请参阅创建您的 AFT 账户配置自定义状态机。
- AFT 全球定制。提供示例代码。有关 AFT 全局自定义的更多信息，请参阅账户自定义。
- AFT 账户自定义。提供示例代码。有关 AFT 账户自定义的更多信息，请参阅账户自定义。

步骤 2：指定 AFT 部署所需的 VCS 配置参数

作为 AFT 部署的一部分，需要以下输入参数来配置 VCS 提供商。

- vcs_provid er：如果您未使用 AWS CodeCommit，请根据您的用例将 VCS 提供程序指定为"bitbucket""github""githubenterprise"、或。
- github_enterprise_url：仅适用于 GitHub 企业客户，请指定 URL。 GitHub
- account_request_repo_name：默认情况下，对于用户，此值设置为。aft-account-request AWS CodeCommit 如果您在 AFT 支持的第三方 VCS 提供商环境中 CodeCommit 或环境中使用新名称创建存储库，请使用您的实际存储库名称更新此输入值。对于 BitBucket Github 和 GitHub Enterprise，存储库名称的格式必须为[Org]/[Repo]。
- account_customizations_repo_name：默认情况下，对于用户，此值设置为。aft-account-customizations AWS CodeCommit 如果您在 AFT 支持的第三方 VCS 提供商环境中 CodeCommit 或环境中使用新名称创建了存储库，请使用您的存储库名称更新此输入值。对于 BitBucket Github 和 GitHub Enterprise，存储库名称的格式必须为[Org]/[Repo]。
- account_provisioning_customizations_repo_name：默认情况下，对于用户，此值设置为。aft-account-provisioning-customizations AWS CodeCommit 如果您在支持 AFT 的第三方 VCS 提供商环境中 AWS CodeCommit 或环境中使用新名称创建了存储库，请使用您的存储库名称更新此输入值。对于 BitBucket Github 和 GitHub Enterprise，存储库名称的格式必须为[Org]/[Repo]。
- global_customizations_repo_name：默认情况下，对于用户，此值设置为。aft-global-customizations AWS CodeCommit 如果您在 AFT 支持的第三方 VCS 提供商环境中 CodeCommit 或环境中使用新名称创建了存储库，请使用您的存储库名称更新此输入值。对于 BitBucket Github 和 GitHub Enterprise，存储库名称的格式必须为[Org]/[Repo]。
- account_request_repo_bran ch：main默认情况下是分支，但可以覆盖该值。

默认情况下，AFT 来自每个git存储库的main分支。您可以使用其他输入参数覆盖分支名称值。有关输入参数的更多信息，请参阅 AFT Terraform 模块中的自述文件。

步骤 3：完成第三方 VCS 提供商的 AWS CodeStar 连接

部署运行时，AFT 要么创建所需的 AWS CodeCommit 存储库，要么为您选择的第三方 VCS 提供商创建 AWS CodeStar 连接。如果是后者，则必须手动登录 AFT 管理账户的控制台才能完成待处理的 AWS CodeStar 连接。有关完成 AWS CodeStar 连接的更多说明，请参阅AWS CodeStar 文档。

数据保护

分AWS 担责任模型适用于AFT中的数据保护。出于数据保护的目的，我们建议采用以下最佳安全实践。

- 遵守 AWS Control Tower 提供的数据保护指南。有关更多信息，请参阅 AWS Control Tower 中的数据保护。
- 保留 AFT 部署时生成的 Terraform 状态配置。有关更多信息，请参阅 部署 AWS Control Tower Account Factory for Terraform (AFT)。
- 按照组织安全策略的指示，定期轮换敏感凭证。机密的例子有 Terraform 代`git`币、代币等。

静态加密

AFT 创建使用密钥管理服务密钥进行静态加密的 Amazon S3 存储桶、亚马逊 SNS 主题、亚马逊 SQS 队列和亚马逊 DynamoDB 数据库。 AWS 默认情况下，AFT 创建的 KMS 密钥已启用年度轮换。如果你选择 Terraform 的 Terraform Cloud 或 Terraform Enterprise 发行版，AFT 会包含一个 Systems Manager SecureString 参数来存储 AWS 敏感的 Terraform 令牌值。

AFT 使用中描述的 AWS 服务组件服务，这些服务在默认情况下是静态加密的。有关详细信息，请参阅 AFT 每个组件 AWS 服务的 AWS 文档，并了解每项服务所遵循的数据保护实践。

传输中加密

默认情况下，AFT 依赖于组件服务中描述的在传输中使用加密的 AWS 服务。有关详细信息，请参阅 AFT 每个组件 AWS 服务的 AWS 文档，并了解每项服务所遵循的数据保护实践。

对于 Terraform Cloud 或 Terraform Enterprise 发行版，AFT 会调用 HTTPS 端点 API 来访问你的 Terraform 组织。如果您选择 AWS CodeStar 连接支持的第三方 VCS 提供商，AFT 会调用 HTTPS 端点 API 来访问您的 VCS 提供商组织。

从 AFT 中删除一个账户

本主题介绍如何从 AFT 中删除账户，以便 AFT 管道停止部署和更新该账户。

> **Important**
>
> 从 AFT 管道中删除账户是不可逆的，并且可能导致状态丢失。

当你想要关闭已停用应用程序的账户、隔离被盗的账户或将账户从一个组织转移到另一个组织时，你可以从 AFT 中删除一个账户。

> **Note**
>
> 从 AFT 中删除账户不同于删除 AWS Control Tower 账户或 AWS 账户。当您从 AFT 中删除账户时，AWS Control Tower 仍会管理该账户。要删除 AWS Control Tower 账户或 AWS 账户，请参阅以下内容：
>
> - 在 AWS Control Tower 用户指南中取消账户管理。
> - 在《AWS Billing 用户指南》中@@ 关闭账户。

从 AFT 管道中删除账户

以下过程描述了如何从 AFT 中删除帐户。

1. 从**`git`**存储账户请求的存储库中移除账户

   在`git`存储账户请求的存储库中，删除要从 AFT 中删除的账户的账户请求。

   当您从账户请求存储库中删除账户请求时，AFT 会删除自定义管道和账户元数据。有关更多信息，请参阅上的 AFT 1.8.0 版本说明。 GitHub
2. 删除 Terraform 工作区（仅适用于 Terraform Cloud 和 Terraform Enterprise 客户）

   删除要从 AFT 中移除的账户的全局自定义和账户自定义工作区。
3. 从亚马逊 S3 后端删除 Terraform 状态

   在 AFT 管理账户中，删除要从 AFT 中删除的账户的 Amazon S3 存储桶内的所有相关文件夹。

   > **Tip**
   >
   > 在以下示例中，*`012345678901`*替换为 AFT 管理账户 ID 号。

示例：Terraform OSS

当你选择 Terraform OSS 时，你会在`aft-backend-012345678901-primary-region`和`aft-backend-012345678901-secondary-region` Amazon S3 存储桶中找到每个账户的 3 个文件夹。这些文件夹与账户自定义状态、自定义管道状态和全局自定义状态相关

示例：Terraform Cloud 或 Terraform Enter

当你选择 Terraform Cloud 或 Terraform Enterprise 时，你会在`aft-backend-012345678901-primary-region`和 Amazon S3 存储桶`aft-backend-012345678901-secondary-region`中为每个账户找到一个文件夹。这些文件夹与自定义管道状态相关。

运营指标

默认情况下，Acco unt Factory for Terraform（AFT）会向发送匿名的运营指标。 AWS我们使用这些数据来了解客户如何使用 AFT，这样我们就可以提高解决方案的质量和功能。您可以通过在 AFT 部署期间更改参数来选择退出数据收集。启用收集后，以下数据将发送到 AWS：

- 解决方案：AFT 特定的标识符
- 版本：AFT 的版本
- 通用唯一标识符 (UUID)：为每个 AFT 部署随机生成的唯一标识符
- 时间戳：数据收集时间戳
- 数据：AFT 配置和客户采取的行动

AWS 拥有收集的数据。数据收集受AWS 隐私政策的约束。

> **Note**
>
> 1.6.0 之前的 AFT 版本不会向报告使用量指标。 AWS

要选择退出报告指标，请执行以下操作：

- 如以下示例所示`aft_metrics_reporting`，`false`在 Terraform 输入配置文件中将的输入值设置为，然后重新部署 AFT。如果您未明确设置此值，则`true`默认情况下会将其设置为。

如果您复制示例，请记住用您的实际 ID 和 Region 值代替字符串中给出的项目x。

```
module "control_tower_account_factory" {
source = "aws-ia/control_tower_account_factory/aws"

# Required Vars
ct_management_account_id    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
audit_account_id            = "xxxxxxxxxxx"
aft_management_account_id   = "xxxxxxxxxxx"
ct_home_region              = "xx-xxxx-x"
tf_backend_secondary_region = "xx-xxxx-x"

# Optional Vars
aft_metrics_reporting = false    # to opt out, set this value to false
}
```

Account Factory for Terraform (AFT) 故障排除指南

本节可以帮助你解决在使用 Account Factory for Terraform (AFT) 时可能遇到的常见问题。

主题

一般性问题

- 已超过 AWS 资源配额

  如果您的日志组显示您已超出 AWS 资源配额，请联系 Supp AWS ort。Account Factory 使用的资源 AWS 服务 配额包括 AWS CodeBuild AWS Organizations、和 AWS Systems Manager。有关更多信息，请参阅下列内容：

  - 什么是 AWS CodeBuild？ 在《CodeBuild 用户指南》中。
  - 什么是 AWS Organizations？ 在 Organi zations 用户指南中。
  - 什么是 AWS Systems Manager？ 在 S ystems Manager 用户指南中。

- Account Factory 的过时版本

  如果您遇到问题并认为问题是错误，请确保您使用的是最新版本的 Account Factory。有关更多信息，请参阅更新 Account Factory 版本。

- 对 Account Factory 源代码进行了本地更改

  Account Factory 是一个开源项目。AWS Control Tower 支持 Account Factory 核心代码。如果您在本地对 Account Factory 核心代码进行更改，AWS Control Tower 仅在尽力而为的基础上支持您的账户工厂部署。

- Account Factory 角色权限不足

  Account Factory 创建 IAM 角色和策略来管理付费账户的部署和自定义。如果您更改这些角色或政策，Account Factory 渠道可能无法执行某些操作。有关更多信息，请参阅必填角色。

- 账户存储库未正确填充

  在配置账户之前，请务必按照部署后的步骤进行操作。

- 手动更改 OU 后未检测到偏差

  > **Note**
  >
  > AWS Control Tower 会自动检测偏差。有关解决偏差的信息，请参阅在 AWS Control Tower 中检测和解决偏差。

  手动更改组织单位 (OU) 时，不会检测到偏差。这是由于 Account Factory 的事件驱动性质所致。提交账户请求时，Terraform 管理的资源是亚马逊 DynamoDB 项目，而不是直接账户。更改项目后，请求将被放入队列，AWS Control Tower 通过服务目录（管理账户详细信息的服务）处理这些请求。如果您手动更改 OU，则不会检测到偏差，因为账户请求未更改。

与账户配置/注册有关的问题

- 账户申请（电子邮件地址/姓名）已存在

  该问题通常会导致 Service Catalog 产品在置备期间出现故障`ConditionalCheckFailedException`。

  您可以通过执行以下任一操作来找到有关该问题的更多信息：

  - 查看你的 Terraform 或 Lo CloudWatch gs 日志组。

  - 查看 Amazon SNS `aft-failure-notifications` 主题中出现的故障。
- 账号请求格式不正确

  请确保您的账户请求符合预期架构。有关示例，请参阅上的 terraform-aws-control_tower_account_factory。 GitHub
- 超过 AWS Organizations

  确保您的账户请求不超过 AWS Organizations 资源配额。有关更多信息，请参阅 Organizati ons 的 AWS 配额。

与调用自定义相关的问题

- 目标账户未加入 Account Factory

  确保自定义请求中包含的所有账户都已登录到 Account Factory。有关更多信息，请参阅更新现有账户。
- 自定义请求目标的账户存在于 DynamoDB **`aft-request-metadata`** 表中，但不存在于账户请求存储库中

  通过执行以下任一操作，格式化您的自定义调用请求以排除违规账户：

  - 在 DynamoDB `aft-request-metadata` 表中，删除引用已不在账户请求存储库中的账户的条目。
  - 不使用 “全部” 作为目标。
  - 不定位账户所属的 OU。
  - 不直接定位该账户。
- 为 Terraform Cloud 使用了错误的代币

  确保您设置了正确的令牌。Terraform Cloud 仅支持基于团队的代币，不支持基于组织的代币。
- 在创建账户自定义渠道之前创建账户失败；无法自定义账户

  在账户请求存储库中更改账户规范。当您进行更改（例如更改帐户的标签值）时，即使管道不存在，Account Factory 也会遵循尝试创建管道的路径。

与账户自定义工作流程相关的问题

如果您遇到与账户自定义工作流程相关的问题，请确保您的 AFT 版本为 1.8.0 或更高版本，并从 DynamoDB 请求表中删除所有与账户相关的元数据实例。

有关 AFT 1.8.0 版本的信息，请参阅上的 1.8.0 版本。 GitHub

有关如何检查和更新 AFT 版本的信息，请参阅以下内容：

- 查看 AFT 版本
- 更新 AFT 版本

您还可以使用 Amazon L CloudWatch ogs Insights 查询筛选包含目标账户和自定义请求 ID 的日志，从而跟踪自定义请求并对其进行故障排除。有关更多信息，请参阅使用 AFT 账户自定义请求跟踪进行故障排除。

在 AWS Control Tower 中检测并解决偏差

识别和解决偏差问题是 AWS Control Tower 管理账户管理员的一项常规操作任务。解决偏差问题有助于确保您遵守治理要求。

创建着陆区时，着陆区以及所有组织单位 (OU)、账户和资源都符合您选择的控件强制执行的管理规则。当您和您的组织成员使用 landing zone 时，这种合规状态可能会发生变化。有些更改可能是偶然的，而有些更改可能会故意响应对时间敏感的操作事件。

偏差检测帮助您标识需要更改或配置更新的资源以消除偏差。

检测漂移

AWS Control Tower 会自动检测偏差。要检测偏差，该`AWSControlTowerAdmin`角色需要持续访问您的管理账户，这样 AWS Control Tower 才能对进行只读 API 调用 AWS Organizations。这些 API 调用显示为 AWS CloudTrail 事件。

漂移出现在审计账户中汇总的亚马逊简单通知服务 (Amazon SNS) Simple Notification 中。每个成员账户中的通知都会向本地 Amazon SNS 主题和 Lambda 函数发送提醒。

对于属于 AWS Security Hub 服务管理标准：AWS Control Tower 的控件，在 AWS Control Tower 控制台的账户和账户详情页面以及亚马逊 SNS 通知中显示偏差。

成员账户管理员可以（作为最佳实践，他们应该）订阅特定账户的 SNS 偏差通知。例如，`aws-controltower-AggregateSecurityNotifications`SNS 主题提供偏差通知。当出现偏差时，AWS Control Tower 控制台会向管理账户管理员发出指示。有关偏差检测和通知的 SNS 主题的更多信息，请参阅漂移防护和通知。

漂移通知重复数据删除

如果同一组资源多次出现相同类型的偏移，AWS Control Tower 将仅针对初始偏移实例发送 SNS 通知。如果 AWS Control Tower 检测到该偏差实例已得到修复，则仅当这些相同的资源再次出现偏移时，它才会再次发送通知。

示例：账户漂移和 SCP 漂移按以下方式处理

- 如果您多次修改同一个托管 SCP，则首次修改该托管 SCP 时会收到通知。
- 如果您修改托管 SCP，然后修复偏差，然后再次对其进行修改，您将收到两条通知。

- 如果一个账户在同一个源和目标 OU 之间多次移动，而没有先修复偏移，则会发送一条通知，即使该账户在这些 OU 之间移动了不止一次。

账户漂移的类型

- 账户在 OU 之间移动
- 已从组织中移除账户

> **Note**
>
> 当您将账户从一个 OU 转移到另一个 OU 时，之前的 OU 中的控制不会被移除。如果您在目标 OU 上启用任何新的基于挂钩的控件，则旧的 OU 基于挂钩的控件已从账户中移除，新控件取而代之。当账户更改 OU 时，必须手动移除使用 SCP 和 AWS Config 规则实施的控件。

政策偏差的类型

- SCP 已更新
- SCP 已连接到 OU
- SCP 已与 OU 分离
- SCP 已绑定到账户

有关更多信息，请参阅治理偏差的类型。

解决漂移问题

虽然检测是自动进行的，但消除偏差的步骤必须通过控制台来完成。

- 许多类型的漂移可以通过着陆区域设置页面来解决。您可以在 “版本” 部分中选择 “重置” 按钮来解决这些类型的偏差。
- 如果您的 OU 的账户少于 300 个，则可以通过在 “组织” 页面或 OU 详细信息页面上选择 “重新注册 OU” 来解决 Account Factory 预配置账户中的偏差或 SCP 偏差。
- 您可以解决账户偏差问题已移动成员账户，例如更新个人账户。有关更多信息，请参阅 在控制台中更新账户。

⚠ 当你采取措施解决 landing zone 版本上的漂移问题时，可能有两种行为。

- 如果您使用的是最新的着陆区版本，则当您选择 “重置” 然后选择 “确认” 时，您的漂移着陆区资源将重置为保存的 AWS Control Tower 配置。landing zone 版本保持不变。
- 如果您使用的不是最新版本，则必须选择 “更新”。着陆区已升级到最新的着陆区版本。漂移问题已作为此过程的一部分得到解决。

关于漂移和 SCP 扫描的注意事项

AWS Control Tower 每天都会扫描您的托管 SCP，以验证相应的控制措施是否正确应用并且没有偏差。为了检索 SCP 并对其进行检查，AWS Control Tower 使用您的管理账户中的角色代表您致电 AWS Organizations 。

如果 AWS Control Tower 扫描发现偏差，您将收到通知。对于每个漂移问题，AWS Control Tower 只发送一条通知，因此，如果您的着陆区已经处于漂移状态，则除非找到新的漂移物品，否则您将不会收到其他通知。

AWS Organizations 限制其每个 API 的调用频率。此限制以每秒事务数 (TPS) 表示，称为 TPS 限制、限制速率或 API 请求速率。当 AWS Control Tower 通过调用来审核您的 SCP 时 AWS Organizations，AWS Control Tower 发出的 API 调用将计入您的 TPS 限制，因为 AWS Control Tower 使用管理账户进行调用。

在极少数情况下，无论是通过第三方解决方案还是通过您编写的自定义脚本重复调用相同的 API，都可能达到此限制。例如，如果您和 AWS Control Tower 在同一时间（1 秒内）调用相同的 AWS Organizations API，并且达到 TPS 限制，则后续调用会受到限制。也就是说，这些调用会返回错误，例如`Rate exceeded`。

如果超过 API 请求速率

- 如果 AWS Control Tower 达到限制并受到限制，我们会暂停执行审计，稍后再恢复。
- 如果您的工作负载达到限制并受到限制，则结果可能从轻微的延迟一直到工作负载中的致命错误，具体取决于工作负载的配置方式。这种边缘情况值得注意。

每日 SCP 扫描包括

1. 正在检索您最近处于活动状态的 OU。

2. 对于每个注册的 OU，检索所有由 AWS Control Tower 管理的、附加到该 OU 的 SCP。托管 SCP 的标识符以开头。`aws-guardrails`
3. 对于 OU 上启用的每项预防性控制，验证该控制的策略声明是否存在于 OU 的托管 SCP 中。

一个 OU 可能有一个或多个托管 SCP。

需要立即解决的漂移类型

大多数类型的偏差可以由管理员解决。必须立即解决一些类型的偏差，包括删除 AWS Control Tower 着陆区所需的组织单位。以下是一些您可能希望避免的重大偏差示例：

- 不要删除安全 OU：不应删除 AWS Control Tower 在设置着陆区期间最初名为 “安全” 的组织单位。如果将其删除，则会看到一条错误消息，指示您立即重置着陆区。在重置完成之前，您将无法在 AWS Control Tower 中执行任何其他操作。
- 不要删除必需的角色：当您登录控制台时，AWS Control Tower 会检查某些 AWS Identity and Access Management (IAM) 角色是否存在 IAM 角色偏差。如果缺少这些角色或无法访问这些角色，您将看到一个错误页面，指示您重置着陆区。这些角色是`AWSControlTowerAdminAWSControlTowerCloudTrailRoleAWSControlTowerStackSetRole`。

  有关这些角色的更多信息，请参阅使用 AWS Control Tower 控制台所需的权限。
- 不要删除所有其他 OU：如果您在 AWS Control Tower 设置着陆区期间删除了最初名为 Sandbox 的组织单位，则您的着陆区将处于漂移状态，但您仍然可以使用 AWS Control Tower。AWS Control Tower 至少需要一个额外的 OU 才能运行，但它不一定是沙盒 OU。
- 不要删除共享帐户：如果您从 Foundational OU 中删除共享帐户，例如从安全 OU 中删除登录帐户，则您的着陆区域将处于漂移状态。必须先重置着陆区，然后才能继续使用 AWS Control Tower 控制台。

可修复的资源变更

以下是允许对 AWS Control Tower 资源进行更改的列表，尽管这些更改会造成可解决的偏差。这些允许的操作的结果可以在 AWS Control Tower 控制台中查看，但可能需要刷新。

有关如何解决由此产生的偏差的更多信息，请参阅在 AWS Control Tower 之外管理资源。

允许在 AWS Control Tower 控制台之外进行更改

- 更改已注册 OU 的名称。

- 更改安全 OU 的名称。
- 更改非基础 OU 中成员帐户的名称。
- 在安全 OU 中更改 AWS Control Tower 共享账户的名称。
- 删除非基础 OU。
- 从非基础 OU 中删除已注册的账户。
- 在安全 OU 中更改共享账户的电子邮件地址。
- 更改已注册 OU 中成员账户的电子邮件地址。

> **Note**
>
> 在 OU 之间转移账户被视为漂移，必须解决这个问题。

偏差和新账户预配置

如果您的着陆区处于漂移状态，AWS Control Tower 中的注册账户功能将无法使用。在这种情况下，您必须通过 AWS Service Catalog 配置新账户。有关说明，请参阅使用 Account Factory 配置 AWS Service Catalog 账户 。

特别是，如果您通过 Service Catalog 对账户进行了某些更改，例如更改投资组合的名称，则注册账户功能将无法使用。

监管偏差类型

当 OU、SCP 和成员账户发生更改或更新时，就会发生治理漂移，也称为组织漂移。在 AWS Control Tower 中可以检测到的治理偏差类型如下：

- 已移动成员账户
- 已删除成员账户
- 托管 SCP 的计划外更新
- SCP 已附加到成员账户
- SCP 已附加到托管 OU
- SCP 已从托管 OU 分离
- 已删除基础 OU
- Security Hub 控制偏差

- 已禁用可信访问

另一种类型的漂移是 l anding zone 漂移，可以通过管理账户找到。着陆区域漂移包括 IAM 角色偏移或任何类型的组织偏移，具体影响基础 OU 和共享账户。

landing zone 漂移的一个特殊情况是角色漂移，当所需角色不可用时，就会检测到角色漂移。如果出现这种偏差，控制台将显示警告页面和一些有关如何恢复角色的说明。在角色偏差问题得到解决之前，你的着陆区域不可用。有关漂移的更多信息，请参阅名为 “不要删除必需角色” 一节中的需要立即解决的漂移类型。

AWS Control Tower 不会寻找与管理账户配合使用的其他服务的偏差，包括 CloudTrail CloudWatch、、IAM 身份中心 AWS CloudFormation AWS Config、、等。儿童账户中没有偏差检测功能，因为这些账户受预防性强制控制措施的保护。

但是，它确实报告了与AWS Security Hub 服务托管标准：AWS Control Tower 一部分的控件存在偏差。

已移动成员账户

这种类型的偏差发生在账户上，而不是OU上。当 AWS Control Tower 成员账户、审计账户或日志存档账户从注册的 AWS Control Tower 组织单位转移到任何其他 OU 时，可能会发生这种偏差。以下是检测到此类偏差时的 Amazon SNS 通知示例。

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more
 than 300 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

解决方法

当 OU 中设置的 Account Factory 账户出现这种偏差时，您可以通过以下方式解决：

- 在 AWS Control Tower 控制台中导航到组织页面，选择账户，然后选择右上角的更新账户（个人账户的最快选项）。
- 在 AWS Control Tower 控制台中导航到 “组织” 页面，然后为包含该账户的 OU 选择 “重新注册”（多个账户的最快选项）。有关更多信息，请参阅 向 AWS Control Tower 注册现有组织单位。
- 在 Account Factory 中更新预配置的产品。有关更多信息，请参阅 使用 AWS Control Tower 或使用 AWS Control Tower 更新和移动账户工厂账户 AWS Service Catalog。

> **Note**
>
> 如果您有多个个人帐户要更新, 另请参阅此使用脚本进行更新的方法:使用自动化配置和更新账户.

- 当这种类型的漂移发生在拥有超过 300 个账户的 OU 中时，漂移解决方案可能取决于转移了哪种类型的账户，如下文所述。有关更多信息，请参阅 更新您的登录区。
  - 如果 Account Factory 配置的账户被移动 — 在账户少于 300 的 OU 中，您可以通过更新 Account Factory 中的预配置产品、重新注册 OU 或更新您的着陆区域来解决账户偏移问题。

    在拥有超过 300 个账户的 OU 中，您必须通过 AWS Control Tower 控制台或预配置产品更新每个已转移的账户，从而解决偏差问题，因为重新注册 OU 不会执行更新。有关更多信息，请参阅 使用 AWS Control Tower 或使用 AWS Control Tower 更新和移动账户工厂账户 AWS Service Catalog。
  - 如果共享帐户被移动 — 您可以通过更新 landing zone 来解决移动审核或日志存档帐户的偏差。有关更多信息，请参阅 更新您的登录区。

> **⚠ 已弃用的字段名称**
>
> 为了符合 AWS 指导方针`ManagementAccountID`，字段名称`MasterAccountID`已更改。旧名称已被弃用。从 2022 年开始，包含已弃用字段名称的脚本将不再起作用。

已删除成员账户

当从注册的 AWS Control Tower 组织单位中删除成员账户时，可能会发生这种偏差。以下示例显示了检测到此类偏差时的 Amazon SNS 通知。

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has
 been removed from organization o-123EXAMPLE. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-
account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory
 provisioned product",
  "AccountId" : "012345678909"
}
```

解决方案

- 当成员账户出现此类偏差时，您可以通过在 AWS Control Tower 控制台或 Account Factory 中更新账户来解决偏移问题。例如，您可以通过 Account Factory 更新向导将该账户添加到另一个已注册的 OU。有关更多信息，请参阅 使用 AWS Control Tower 或使用 AWS Control Tower 更新和移动账户工厂账户 AWS Service Catalog。
- 如果共享帐户已从基础组织单位中移除，则必须通过重置着陆区来解决这个问题。在此问题得到解决之前，您将无法使用 AWS Control Tower 控制台。
- 有关解决账户和 OU 的偏差的更多信息，请参阅如果您在 AWS Control Tower 之外管理资源。

> **Note**
>
> 在 Service Catalog 中，代表账户的 Account Factory 预配置产品不会更新以删除该账户。相反，预配置产品显示为 TAINTED 且处于错误状态。要进行清理，请转至 Service Catalog，选择已配置的产品，然后选择 “终止”。

托管 SCP 的计划外更新

当在控制 AWS Organizations 台中更新控件的 SCP 时，或者使用 AWS CLI 或其中一个 AWS 开发工具包以编程方式更新控件的 SCP 时，可能会发生这种偏差。以下是检测到此类偏差时的 Amazon SNS 通知示例。

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit
 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
update-scp'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

解决方案

当在拥有多达 300 个账户的 OU 中出现这种偏差时，您可以通过以下方式解决：

- 在 AWS Control Tower 控制台中导航到 “组织” 页面以重新注册 OU（最快的选项）。有关更多信息，请参阅 向 AWS Control Tower 注册现有组织单位。
- 更新您的着陆区（速度较慢的选项）。有关更多信息，请参阅 更新您的登录区。

当拥有超过 300 个账户的 OU 中发生此类偏移时，请通过更新 landing zone 来解决这个问题。有关更多信息，请参阅 更新您的登录区。

SCP 已附加到托管 OU

当控件的 SCP 连接到任何其他 OU 时，可能会发生这种偏差。当您从 AWS Control Tower 控制台之外处理业务单元时，这种情况尤其常见。以下是检测到此类偏差时的 Amazon SNS 通知示例。

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the registered
```

```
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

解决方案

当在拥有多达 300 个账户的 OU 中出现这种偏差时，您可以通过以下方式解决：

- 在 AWS Control Tower 控制台中导航到 “组织” 页面以重新注册 OU（最快的选项）。有关更多信息，请参阅 向 AWS Control Tower 注册现有组织单位。
- 更新您的着陆区（速度较慢的选项）。有关更多信息，请参阅 更新您的登录区。

当拥有超过 300 个账户的 OU 中发生此类偏移时，请通过更新 landing zone 来解决这个问题。有关更多信息，请参阅 更新您的登录区。

SCP 已从托管 OU 分离

当控制的 SCP 与 AWS Control Tower 管理的 OU 分离时，可能会发生这种偏差。当您在 AWS Control Tower 控制台之外工作时，这种情况尤其常见。以下是检测到此类偏差时的 Amazon SNS 通知示例。

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_DETACHED_FROM_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
```

```
}
```

解决方案

当在拥有多达 300 个账户的 OU 中出现这种偏差时，您可以通过以下方式解决：

- 在 AWS Control Tower 控制台中导航到 OU 以重新注册 OU（最快的选项）。有关更多信息，请参阅 向 AWS Control Tower 注册现有组织单位。
- 更新您的着陆区（速度较慢的选项）。如果偏移影响了强制控制，则更新过程会创建一个新的服务控制策略 (SCP) 并将其附加到 OU 以解决偏移问题。有关如何更新 landing zone 的更多信息，请参阅更新您的登录区。

当拥有超过 300 个账户的 OU 中发生此类偏移时，请通过更新 landing zone 来解决这个问题。如果偏移影响了强制控制，则更新过程会创建一个新的服务控制策略 (SCP) 并将其附加到 OU 以解决偏移问题。有关如何更新 landing zone 的更多信息，请参阅更新您的登录区。

SCP 已附加到成员账户

当控件的 SCP 附加到 Organizations 控制台中的账户时，可能会发生这种偏差。可以通过 AWS Control Tower 控制台在 OU 上启用护栏及其 SCP（从而应用于 OU 的所有注册账户）。以下是检测到此类偏差时的 Amazon SNS 通知示例。

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the member account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_ACCOUNT",
  "RemediationStep" : "Re-register this organizational unit (OU)",
  "AccountId" : "012345678909",
  "PolicyId" : "p-tEXAMPLE"
}
```

解决方案

这种类型的偏差发生在账户上，而不是OU上。

当基础组织单元（例如安全 OU）中的帐户出现这种偏差时，解决方案是更新您的着陆区。有关更多信息，请参阅 更新您的登录区。

当在拥有最多 300 个账户的非基础 OU 中发生此类偏差时，您可以通过以下方式解决：

- 将 AWS Control Tower SCP 与账户工厂账户分离。
- 在 AWS Control Tower 控制台中导航到 OU 以重新注册 OU（最快的选项）。有关更多信息，请参阅 向 AWS Control Tower 注册现有组织单位。

当拥有超过 300 个账户的 OU 中出现这种偏差时，您可以尝试通过更新该账户的账户出厂配置来解决该问题。可能无法成功解决这个问题。有关更多信息，请参阅 更新您的登录区。

已删除基础 OU

这种偏差仅适用于 AWS Control Tower 基础业务单元，例如安全 OU。如果在 AWS Control Tower 控制台之外删除了基础 OU，则可能会发生这种情况。如果不创建这种类型的偏移，就无法移动基础 OU，因为移动 OU 与将其删除然后将其添加到其他位置相同。当您通过更新着陆区来解决偏差问题时，AWS Control Tower 会取代原始位置的基础 OU。以下示例显示了检测到此类偏差时您可能会收到的 Amazon SNS 通知。

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit
 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-
ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

解决方案

由于这种偏差仅发生在基础 OU 中，因此解决方法是更新 landing zone。删除其他类型的 OU 时，AWS Control Tower 会自动更新。

有关解决账户和 OU 的偏差的更多信息，请参阅如果您在 AWS Control Tower 之外管理资源。

Security Hub 控制偏差

当属于AWS Security Hub 服务管理标准：AWS Control Tower 的控件报告偏差状态时，就会发生这种偏差。该 AWS Security Hub 服务本身不会报告这些控件的偏移状态。相反，该服务将其调查结果发送给 AWS Control Tower。

如果 AWS Control Tower 在 24 小时内没有收到来自 Security Hub 的状态更新，也可以检测到 Security Hub 控制偏差。如果未按预期收到这些发现，AWS Control Tower 会验证控制是否处于偏离状态。以下示例显示了检测到此类偏差时您可能会收到的 Amazon SNS 通知。

```
{
"Message" : "AWS Control Tower has detected that an AWS Security Hub control
 was removed in your account example-account@amazon.com <mailto:example-
account@amazon.com>. The artifact deployed on the target OU and accounts does not match
 the expected template and configuration for the control. This mismatch indicates that
 configuration changes were made outside of AWS Control Tower. For more information,
 view Security Hub standard",
"MasterAccountId" : "123456789XXX",
"ManagementAccountId" : "123456789XXX",
"OrganizationId" : "o-123EXAMPLE",
"DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
"RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
 and enable it again. If the problem persists, contact AWS support.",
"AccountId" : "7876543219XXX",
"ControlId" : "PYBETSAGNUZB",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"Region" : "us-east-1"
}
```

解决方案

对于账户少于 300 个的 OU，解决方案是重新注册 OU，这会将控件重置为原始状态。对于任何 OU，您可以通过控制台或 AWS Control Tower API 删除并重新启用控件，这也会重置控件。

有关解决账户和 OU 的偏差的更多信息，请参阅如果您在 AWS Control Tower 之外管理资源。

已禁用可信访问

这种偏差适用于 AWS Control Tower 着陆区。当您在设置 AWS Control Tower 着陆区 AWS Organizations 后禁用对 AWS Control Tower 的可信访问时，就会发生这种情况。

禁用可信访问后，AWS Control Tower 将不再接收来自的变更事件 AWS Organizations。AWS Control Tower 依靠这些变更事件来与之保持同步 AWS Organizations。因此，AWS Control Tower 可能会错过账户和 OU 的组织变动。因此，每次更新 landing zone 时，都必须重新注册每个 OU。

示例：亚马逊 SNS 通知

以下是发生此类偏差时您收到的 Amazon SNS 通知的示例。

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
 AWS Organizations. For more information, including steps to resolve this issue, see
 https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
}
```

解决方案

当 AWS Control Tower 控制台中出现此类偏差时，AWS Control Tower 会通知您。解决方案是重置您的 AWS Control Tower 着陆区。有关更多信息，请参阅解决偏差。

如果您在 AWS Control Tower 之外管理资源

AWS Control Tower 代表您设置账户、组织单位和其他资源，但您是这些资源的所有者。您可以在 AWS Control Tower 内部或外部更改这些资源。在 AWS Control Tower 之外更改资源的最常见位置是 AWS Organizations 控制台。本主题介绍当您在 AWS Control Tower 之外进行更改时，如何协调对 AWS Control Tower 资源的更改。

在 AWS Control Tower 控制台之外重命名、删除和移动资源会导致控制台不同步。许多更改都可以自动调节。某些更改需要重置您的着陆区，才能更新 AWS Control Tower 控制台中显示的信息。

通常，您在 AWS Control Tower 控制台之外对 AWS Control Tower 资源所做的更改会在您的着陆区中造成一种可解析的漂移状态。有关这些更改的更多信息，请参阅可修复的资源变更。

需要重置 landing zone 的任务

- 删除安全 OU（这是一种特殊情况，不能轻易完成。）

- 从安全 OU 中移除共享帐户（不推荐。）
- 更新、附加或分离与安全 OU 关联的 SCP。

由 AWS Control Tower 自动更新的更改

- 更改已注册账户的电子邮件地址
- 重命名已注册的账户
- 创建新的顶级组织单位 (OU)
- 重命名已注册的 OU
- 删除已注册的 OU（安全 OU 除外，需要更新。）
- 删除已注册的账户（安全 OU 中的共享账户除外。）

> **Note**
>
> AWS Service Catalog 处理变更的方式与 AWS Control Tower 不同。 AWS Service Catalog 当它协调您的更改时，可能会改变治理态势。有关更新预配置产品的更多信息，请参阅文档中的更新预配置产品。 AWS Service Catalog

引用 AWS Control Tower 之外的资源

当您在 AWS Control Tower 之外创建新的 OU 和账户时，它们不受 AWS Control Tower 的管辖，即使它们可能会显示出来。

创建 OU

在 AWS Control Tower 之外创建的组织单位 (OU) 被称为未注册。它们显示在组织页面中，但它们不受 AWS Control Tower 控件的约束。

创建账户

在 AWS Control Tower 之外创建的账户被称为未注册。属于在 AWS Control Tower 注册的 OU 的已注册账户和未注册账户将显示在组织页面上。可以使用 AWS Organizations 控制台邀请不属于已注册 OU 的账户。此加入邀请不会在 AWS Control Tower 中注册账户，也不会将 AWS 控制塔的管理范围扩展到该账户。要通过注册账户来扩大监管范围，请前往 AWS Control Tower 中的组织页面或账户详情页面，然后选择注册账户。

在外部更改 AWS Control Tower 资源名称

您可以在 AWS Control Tower 控制台之外更改组织单位 (OU) 和账户的名称，控制台会自动更新以反映这些更改。

重命名 OU

在中 AWS Organizations，您可以使用 AWS Organizations API 或控制台更改 OU 的名称。当您在 AWS Control Tower 之外更改 OU 名称时，AWS Control Tower 控制台会自动反映名称的更改。但是，如果您使用配置账户，则还必须重置您的着陆区 AWS Service Catalog，以确保 AWS Control Tower 与保持一致 AWS Organizations。重置工作流程可确保基础和附加 OU 的服务之间的一致性。您可以从着陆区设置页面解决此类偏移问题。请参阅中名为 “解决偏差” 的部分在 AWS Control Tower 中检测并解决偏差。

AWS Control Tower 在 AWS 控制塔控制面板的组织页面上显示 OU 的名称。你可以看到你的 landing zone 重置操作何时成功。

重命名已注册的账户

每个 AWS 账户都有一个显示名称，该账户的 root 用户可以在 AWS Billing and Cost Management 控制台中更改该名称。当您重命名已在 AWS Control Tower 中注册的账户时，名称更改会自动反映在 AWS Control Tower 中。有关更改账户名称的更多信息，请参阅AWS 账单用户指南中的管理 AWS 账户。

删除安全 OU

此类偏差是一种特殊情况。如果您删除 Sec urit y OU，则会看到一个错误消息页面，提示您重置着陆区。您必须先重置着陆区，然后才能在 AWS Control Tower 中执行任何其他操作。

- 在重置完成 AWS Service Catalog 之前，您将无法在 AWS Control Tower 控制台中执行任何操作，也无法在中创建任何新账户。
- 您将无法查看着陆区域设置页面以查看那里的 “重置” 按钮。

在这种情况下，landing zone 重置过程会创建一个新的安全 OU，并将两个共享帐户移至新的安全 OU。AWS Control Tower 将日志存档和审计账户标记为已移动。同样的过程可以解决这些账户中的偏差。

如果您确定必须删除安全 OU，则需要了解以下内容：

在删除安全 OU 之前，必须确保它不包含任何帐户。具体而言，您必须从 OU 中移除日志存档和审核帐户。建议您将这些账户移至另一个 OU。

> **Note**
>
> 未经适当考虑，不得执行删除您的安全 OU 的操作。如果暂时暂停日志记录，并且某些控制措施可能无法强制执行，则该操作可能会引起合规性问题。

有关偏差的一般信息，请参阅在 AWS Control Tower 中检测并解决偏差中的“解决偏差”。

从安全 OU 中删除账户

我们不建议您从组织中删除任何共享帐户或将其移出安全 OU。如果您意外删除了共享帐户，则可以按照本节中的补救步骤恢复该帐户。

- 在 AWS Control Tower 控制台中：要开始修复过程，请按照半手动修复步骤进行操作。确保您用于访问 AWS Control Tower 控制台的用户或角色拥有运行权限`organizations:InviteAccountToOrganization`。如果您没有此类权限，请按照手动修复步骤操作，这些步骤同时使用 AWS Control Tower 控制台和 AWS Organizations 控制台。
- 从 AWS Organizations 控制台开始：此修复过程稍长一些，完全手动完成。执行手动修复步骤时，您将在 AWS Organizations 控制台和 AWS Control Tower 控制台之间切换。在中工作时 AWS Organizations，您需要具有`AWSOrganizationsFullAccess`托管策略或等效策略的用户或角色。在 AWS Control Tower 控制台中工作时，您需要具有`AWSControlTowerServiceRolePolicy`托管策略或同等策略的用户或角色，以及运行所有 AWS Control Tower 操作的权限（controltower：*）。
- 如果补救步骤未恢复账户，请联系 AWS Support。

通过 AWS Organizations以下方式删除共享账户的结果：

- 该账户不再受服务控制策略 (SCP) 的 AWS Control Tower 强制控制措施的保护。结果：AWS Control Tower 在账户中创建的资源可能会被修改或删除。
- 该账户已不在 AWS Organizations 管理账户下。结果： AWS Organizations 管理账户的管理员无法再查看账户的支出。
- 不再保证该账户会受到监控 AWS Config。结果： AWS Organizations 管理账户的管理员可能无法检测到资源变化。
- 该账户已不在组织中。结果：AWS Control Tower 更新和重置将失败。

使用 AWS Control Tower 控制台恢复共享账户（半手动程序）

1. 登录 AWS Control Tower 控制台，网址为 https://console.aws.amazon.com/controltower。您必须以 IAM 用户、IAM 身份中心用户或具有运行权限的角色身份登录`organizations:InviteAccountToOrganization`。如果您没有此类权限，请使用本主题后面介绍的手动修复程序。
2. 在 “检测到着陆区域漂移” 页面上，选择 “重新邀请”，通过重新邀请共享帐户加入组织来修复已删除的共享帐户。自动生成的电子邮件将发送到该账户的电子邮件地址。
3. 接受邀请，将共享账户重新带回组织。请执行以下操作之一：
   - 登录已删除的共享账户，然后前往 https://console.aws.amazon.com/organizations/home#/invites
   - 如果您有权访问再次邀请账户时发送的电子邮件，请登录已删除的账户，然后点击邮件中的链接直接导航到账户邀请。
   - 如果被删除的共享账户不在其他组织中，请登录该账户，打开 AWS Organizations 控制台并导航到邀请。
4. 再次登录管理账户，或者重新加载 AWS Control Tower 控制台（如果该控制台已打开）。你会看到着陆区漂移页面。选择 “重置” 以修复着陆区。
5. 等待重置过程完成。

如果修复成功，则共享账户将显示为正常状态和合规状态。

如果补救步骤未恢复账户，请联系 AWS Support。

使用 AWS Control Tower 和控制 AWS Organizations 台恢复共享账户（手动修复）

1. 登录 AWS Organizations 控制台，网址为https://console.aws.amazon.com/organizations/。您必须以 IAM 用户、IAM 身份中心用户或具有`AWSOrganizationsFullAccess`托管策略或等效策略的角色身份登录。
2. 邀请共享账号返回组织。有关邀请账户加入的要求、先决条件和程序的信息 AWS Organizations，请参阅AWS Organizations 用户指南中的邀请 AWS 账户加入您的组织。
3. 登录已删除的共享账户，然后前往 https://console.aws.amazon.com/organizations/home#/invites 接受邀请。
4. 再次登录管理账户。
5. 以具有`AWSControlTowerServiceRolePolicy`托管策略或等效策略并具有运行所有 AWS Control Tower 操作的权限的用户或角色登录 AWS Control Tower 控制台（controltower：*）。

6. 您将看到着陆区漂移页面，其中包含重置着陆区的选项。选择 “重置” 以修复着陆区。
7. 等待重置过程完成。

如果修复成功，则共享账户将显示为正常状态和合规状态。

如果补救步骤未恢复账户，请联系 AWS Support。

自动更新的外部更改

AWS Control Tower 会自动更新您对账户电子邮件地址所做的更改，但是 Account Factory 不会自动更新这些更改。

更改受监管账户的电子邮件地址

AWS Control Tower 根据控制台体验的要求检索和显示电子邮件地址。因此，共享账户和其他账户的电子邮件地址会在您更改后更新并一致地显示在 AWS Control Tower 中。

> **Note**
>
> 在中 AWS Service Catalog，Account Factory 显示了您在创建预配置产品时在控制台中指定的参数。但是，当账户电子邮件地址更改时，原始账户电子邮件地址不会自动更新。这是因为该账户在概念上包含在预配置产品中；它与预配置产品不同。要更新此值，您必须更新预配置的产品，这可能会导致监管状态发生变化。

应用外部 AWS Config 规则

AWS Control Tower 显示部署到在 AWS Control Tower 注册的组织单位中的所有 AWS Config 规则的合规状态，包括在 AWS Control Tower 控制台之外激活的规则。

删除 AWS 控制塔外的 AWS Control Tower 资源

您可以在 AWS Control Tower 中删除 OU 和账户，无需采取任何进一步的操作即可查看更新。当您删除 OU 时，Account Factory 会自动更新，但在您删除帐户时不会自动更新。

删除已注册的 OU（安全 OU 除外）

在内部 AWS Organizations，您可以使用 API 或控制台移除空的组织单位 (OU)。无法删除包含账户的 OU。

当组织单位被删除 AWS Organizations 时，AWS Control Tower 会收到通知。它会更新 Account Factory 中的 OU 列表，以便注册的 OU 列表保持一致。

> **Note**
>
> 在中 AWS Service Catalog，Account Factory 已更新，将已删除的 OU 从可用 OU 列表中移除，您可以在其中配置帐户。

从 OU 中删除已注册的账户

当您删除已注册账户时，AWS Control Tower 会收到通知并进行更新，以便信息保持一致。

> **Note**
>
> 在中 AWS Service Catalog，代表受监管账户的 Account Factory 预配置产品未更新为删除该账户。相反，预配置产品显示为 TAINTED 且处于错误状态。要清理，请转到 AWS Service Catalog，选择预配置产品，然后选择 Terminate (终止)。

使用 AWS Control Tower 管理组织和账户

您在 AWS Control Tower 中创建的所有组织单位 (OU) 和账户均由 AWS Control Tower 自动管理。此外，如果您有在 AWS Control Tower 之外创建的现有业务实体和账户，则可以将其纳入 AWS Control Tower 的监管中。

对于现有 AWS Organizations 和 AWS 账户，大多数客户更愿意通过注册包含账户的整个组织单位 (OU) 来注册账户组。您也可以单独注册帐户。有关注册个人账户的更多信息，请参阅注册现有的 AWS 账户。

术语

- 当您将现有组织引入 AWS Control Tower 时，这称为注册该组织或将管理范围扩大到该组织。
- 当您将 AWS 账户带入 AWS Control Tower 时，这称为注册该账户。

查看您的 OU 和账户

在 AWS Control Tower 组织页面上，您可以查看您的所有 OU AWS Organizations，包括在 AWS Control Tower 注册的 OU 和未注册的 OU。您可以将嵌套的 OU 作为层次结构的一部分进行查看。在“组织” 页面上查看组织单位的一种简单方法是仅从右上角的下拉列表中选择 “组织单位”。

组织页面列出了您组织中的所有账户，无论组织单位或在 AWS Control Tower 中的注册状态如何。在组织页面上查看账户的一种简单方法是从右上角的下拉列表中选择 “仅限账户”。如果账户满足注册的先决条件，则可以在 OU 中单独查看、更新和注册账户。

如果您未选择任何筛选，则组织页面会按层次结构显示您的账户和 OU。它是监控您的所有 AWS Control Tower 资源并对其采取操作的中心位置。有关组织页面的更多信息，您可以观看视频演练。

视频演练

此视频 (4:01) 介绍了如何在 AWS Control Tower 中使用组织页面。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

在 AWS Control Tower 中使用组织页面的视频演练。

主题

- 向 AWS Control Tower 注册现有组织单位

- 注册现有的 AWS 账户

将治理范围扩展到现有组织

您可以按照 AWS Control Tower 用户指南入门第 2 步中概述的设置着陆区 (LZ)，为现有组织添加 AWS Control Tower 治理。

以下是您在现有组织中设置 AWS Control Tower 着陆区时的期望。

- 每个 AWS Organizations 组织可以有一个着陆区。
- AWS Control Tower 使用您现有 AWS Organizations 组织的管理账户作为其管理账户。无需新的管理账户。
- AWS Control Tower 在注册的 OU 中设置了两个新账户：一个审计账户和一个日志账户。
- 您组织的服务限制必须允许创建这两个附加账户。
- 在您启动着陆区或注册了 OU 后，AWS Control Tower 控制将自动应用于该 OU 中的所有注册账户。
- 您可以将其他现有 AWS 账户注册到受 AWS Control Tower 管理的 OU 中，以便控制适用于这些账户。
- 您可以在 AWS Control Tower 中添加更多 OU，也可以注册现有 OU。

要查看注册和注册的其他先决条件，请参阅 AWS Control Tower 入门。

以下是关于 AWS Control Tower 控制如何不适用于您在未设置 AWS Control Tower 着陆区的 AWS 组织中的 OU 的更多详细信息：

- 在 AWS Control Tower Account Factory 之外创建的新账户不受注册组织单位控制的约束。
- 在 OU 中创建的未在 AWS Control Tower 注册的新账户不受控制约束，除非您专门将这些账户注册到 AWS Control Tower。有关注册账户的更多信息，请参阅注册现有的 AWS 账户。
- 其他现有组织、现有账户、任何新的 OU 或您在 AWS Control Tower 之外创建的任何账户均不受 AWS Control Tower 控制的约束，除非您单独注册组织单位或注册账户。

有关如何将 AWS Control Tower 应用于现有 OU 和账户的更多信息，请参阅向 AWS Control Tower 注册现有组织单位。

有关在现有组织中设置 AWS Control Tower 着陆区的过程的概述，请观看下一节中的视频。

> **Note**
>
> 在设置过程中，AWS Control Tower 会进行预检查以避免出现常见问题。但是，如果您目前正在使用 AWS 着陆区解决方案 AWS Organizations，请在尝试在组织中启用 AWS Control Tower 之前，请咨询您的 AWS 解决方案架构师，以确定 AWS Control Tower 是否会干扰您当前的着陆区部署。另请参阅，了解如果账户不符合先决条件怎么办？有关将账户从一个着陆区转移到另一个着陆区的信息。

视频：在现有区域中启用着陆区 AWS Organizations

该视频 (7:48) 描述了如何在现有 AWS Organizations 结构中设置和启用 AWS Control Tower 着陆区。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

为现有组织启用 AWS Control Tower

IAM 身份中心和现有组织的注意事项

- 如果已经设置 AWS IAM Identity Center （ IAM 身份中心 ），则 AWS Control Tower 主区域必须与 IAM 身份中心区域相同。
- AWS Control Tower 不会删除现有配置。
- 如果 IAM 身份中心已启用，并且您正在使用 IAM 身份中心目录，AWS Control Tower 会添加权限集、群组等资源并照常进行。
- 如果设置了另一个目录（外部、AD、托管 AD），AWS Control Tower 不会更改现有配置。有关更多详细信息，请参阅AWS IAM Identity Center （ IAM 身份中心 ）客户的注意事项。

访问其他 AWS 服务

将您的组织引入 AWS Control Tower 监管后，您仍然可以通过 AWS Organizations AWS Organizations 控制台和 API 访问任何可用的 AWS 服务。有关更多信息，请参阅 相关 AWS 服务。

AWS Control Tower 中嵌套的 OU

本章列出了在 AWS Control Tower 中使用嵌套 OU 时需要注意的期望和注意事项。在大多数情况下，使用嵌套的 OU 与使用扁平的 OU 结构相同。注册和重新注册功能适用于嵌套的 OU，但本章中提到的更改行为除外。

视频演练

此视频 (4:46) 描述了如何在 AWS Control Tower 中管理嵌套的 OU 部署。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

在 AWS Control Tower 中管理嵌套业务单元的视频演练。

有关嵌套 OU 和着陆区的最佳实践的指导，请参阅博客文章使用嵌套的 OU 组织您的 AWS Control Tower 着陆区。

从扁平的 OU 结构扩展到嵌套的 OU 结构

如果您使用扁平的 OU 结构创建了 AWS Control Tower 着陆区，则可以将其扩展为嵌套的 OU 结构。

此过程有四个主要步骤：

1. 在 AWS Control Tower 中创建所需的嵌套 OU 结构。
2. 进入 AWS Organizations 控制台，使用其批量移动功能将账户从源 OU（平面）移动到目标 OU（嵌套）。方法如下：
   a. 转到要从中转移账户的 OU。
   b. 选择 OU 中的所有账户。
   c. 选择移动。

   > **Note**
   >
   > 此步骤必须在 AWS Organizations 控制台中完成，因为 AWS Control Tower 没有移动功能。

3. 前往 AWS Control Tower 中嵌套的 OU 并对其进行注册或重新注册。嵌套 OU 中的所有账户都将被注册。
   - 如果您在 AWS Control Tower 中创建了 OU，请重新注册该组织单元。
   - 如果您在中创建了 OU AWS Organizations，请首次注册 OU。
4. 在您的账户移动和注册后，从 AWS Organizations 控制台或 AWS Control Tower 控制台中删除空的顶层 OU。

嵌套 OU 注册预检

为了支持成功注册嵌套 OU 及其成员账户，AWS Control Tower 会执行一系列预检查。注册任何顶层 OU 或嵌套 OU 时，也会执行相同的预检查。有关更多信息，请参阅注册或重新注册期间的常见失败原因。

- 如果所有预检查均通过，AWS Control Tower 将自动开始注册您的 OU。
- 如果任何预检查失败，AWS Control Tower 将停止注册流程，并为您提供在注册 OU 之前必须修复的项目清单。

嵌套的 OU 和角色

AWS Control Tower 会将`AWSControlTowerExecution`角色部署到目标 OU 下的账户，以及嵌套在目标 OU 下的所有 OU 中的账户，即使您只打算注册目标 OU 也是如此。此角色向管理账户中的任何用户授予任何具有该`AWSControlTowerExecution`角色的账户的管理员权限。该角色可用于执行 AWS Control Tower 控件通常不允许的操作。

您可以从不打算注册的已取消注册账户中删除此角色。如果您删除此角色，则无法在 AWS Control Tower 中注册该账户，也无法注册直系父 OU，除非您将该角色恢复到该账户。要从账户中删除该`AWSControlTowerExecution`角色，您必须使用该`AWSControlTowerExecution`角色登录，因为不允许其他 IAM 委托人删除由 AWS Control Tower 管理的角色。

有关如何限制角色访问权限的信息，请参阅角色信任关系的可选条件。

在注册和重新注册嵌套 OU 和账户期间会发生什么

当您注册或重新注册嵌套 OU 时，AWS Control Tower 会注册目标 OU 的所有未注册账户，并更新所有已注册的账户。以下是可以期待的。

AWS Control Tower 执行以下任务

- 将该`AWSControlTowerExecution`角色添加到此 OU 下的所有未注册帐户以及其嵌套 OU 中的所有未注册帐户。
- 注册未注册的成员账户。
- 重新注册已注册的会员账户。
- 为新注册的成员账户创建 IAM 身份中心登录名。
- 更新现有已注册的会员账户，以反映您的 landing zone 变更。

- 更新为此 OU 及其成员账户配置的控件。

嵌套 OU 注册的注意事项

- 您不能在核心 OU（安全 OU）下注册 OU。
- 嵌套的 OU 必须单独注册。
- 除非注册了 OU 的父 OU，否则您无法注册 OU。
- 除非树中的所有 OU 在某个时候都已成功注册（有些可能已被删除），否则您无法注册 OU。
- 您可以注册位于漂移较高的 OU 之下的 OU，但该操作无法修复漂移。

嵌套 OU 限制

- OU 最多可以在根深处嵌套 5 个级别。
- 必须单独注册或重新注册目标 OU 下的嵌套 OU。
- 如果目标 OU 在层次结构中位于 2 级或以下，也就是说，如果它不是顶级 OU，则会自动对此 OU 及其下所有 OU 实施在更高 OU 上启用的预防性控制。
- OU 注册失败不会在层次结构树中向上传播。您可以在父组织单元的详细信息页面上查看有关嵌套 OU 状态的详细信息。
- OU 注册失败不会在层次结构树中向下传播。
- AWS Control Tower 不会修改任何新账户或现有账户的 VPC 设置。

嵌套 OU 和合规性

在 AWS Control Tower 控制台中，您可以在组织页面中查看不合规的 OU 和账户，这样您就可以更全面地了解合规情况。

有关嵌套 OU 和账户合规性的注意事项

- OU 的合规性不是根据嵌套在其下的 OU 的合规性来确定的。
- 控件的合规性状态是根据启用控件的所有 OU（包括嵌套的 OU）计算的。查看 AWS Control Tower 业务单元和账户的合规状态 w。
- 只有当 OU 的账户不合规时，OU 才会显示为不合规，而不管 OU 在 OU 层次结构中的位置如何。
- 如果嵌套 OU 不合规，则其父 OU 不会自动被视为不合规。

- 在 OU 详情或账户详情页面上，您可以查看可能导致您的 OU 或账户显示不合规状态的不合规资源列表。

嵌套 OU 和偏移

在某些情况下，漂移可能会阻止嵌套 OU 的注册。

对漂移和嵌套 OU 的期望

- 您可以对具有漂移父级的 OU 启用控制，但不能直接在漂移的 OU 上启用控制。
- 只要漂移的 OU 不是顶级漂移 OU，你就可以在漂移的 OU 下启用侦探控制。
- 强制控制仅在顶层 OU 上启用。注册嵌套 OU 时会跳过强制控件。
- 一个强制性控件可以保护 AWS Config 资源；因此，该控件必须处于非漂移状态才能注册嵌套的 OU。如果存在偏差，AWS Control Tower 会阻止嵌套业务单元的注册。
- 如果顶层 OU 处于漂移状态，则保护 AWS Config 资源的控制可能处于偏离状态。在这种情况下，AWS Control Tower 会阻止任何需要创建或更新 AWS Config 资源的操作，包括应用侦探控制。

嵌套的 OU 和控件

当您在已注册的 OU 上启用控件时，预防和侦测控件的行为会有所不同。对于嵌套的 OU，主动控制的行为类似于侦探控件。

预防性控制

- 对嵌套的 OU 实施预防性控制。
- 对组织单位及其嵌套业务单元下的所有账户实施强制性预防性控制。
- 预防性控制会影响嵌套在目标 OU 下的所有账户和 OU，即使这些账户和 OU 尚未注册。

Detective 和主动控制

- 嵌套的 OU 不会自动继承侦探或主动控制；这些控制必须单独启用。
- Detective 和主动控制仅部署到您的着陆区运营区域的注册账户。

启用控制状态和继承

您可以在 OU 详细信息页面上查看每个 OU 的继承控件。

> **Tip**
>
> 你可以利用控制继承来帮助保持在 OU 的 SCP 配额之内。例如，您可以在 OU 层次结构的顶层 OU 中启用控件，而不是直接为嵌套的 OU 启用。

继承状态

- “继承” 状态表示该控件仅通过继承启用，并且尚未直接应用于 OU。
- 状态为 “已启用” 表示无论其他 OU 上的控制状态如何，都将在此 OU 上强制执行控制。
- 状态为 “失败” 表示无论其他 OU 上的控制状态如何，都不会对此 OU 强制执行控制。

> **Note**
>
> “继承” 状态表示控件已应用于树中更高的 OU，并且已在此 OU 上强制执行，但未直接添加到此 OU 中。

> **如果你的 landing zone 不是当前版本**
>
> “已启用的控件” 表中的每一行代表一个单独的 OU 上已启用的控件。

嵌套的 OU 和根

根不是 OU，因此无法注册或重新注册。您也无法直接在根目录中创建账户。根目录不能不合规，也不能处于生命周期状态，例如已注册或处于偏移状态。

但是，根是所有账户和 OU 的顶级容器。在嵌套 OU 的上下文中，它是所有其他 OU 嵌套在其下的节点。

向 AWS Control Tower 注册现有组织单位

将多个现有 AWS 账户引入 AWS Control Tower 的一种有效方法是将 AWS Control Tower 的管理范围扩展到整个组织单位 (OU)。

要启用 AWS Control Tower 对使用 AWS Organizations其账户创建的现有 OU 及其账户进行管理，请在您的 AWS Control Tower 着陆区注册该 OU。您可以注册最多包含 300 个账户的 OU。如果一个 OU 包含的账户超过 300 个，则无法在 AWS Control Tower 中对其进行注册。

当您注册 OU 时，其成员账户将注册到 AWS Control Tower 着陆区。他们受适用于其 OU 的控制措施的约束。

> **Note**
>
> 如果您还没有 AWS Control Tower 着陆区，请先在 AWS Control Tower 创建的新组织中或现有 AWS Organizations 组织中设置一个着陆区。有关如何设置着陆区的更多详细信息，请参阅AWS Control Tower 入门。

当我注册 OU 时，我的账户会怎样？

AWS Control Tower 需要获得权限才能 AWS Organizations 在您之间 AWS CloudFormation 以及代表您之间建立 AWS CloudFormation 可信访问权限，这样才能自动将您的堆栈部署到您组织中的账户。

- 该`AWSControlTowerExecution`角色将添加到所有状态为 “未注册” 的账户。
- 当您注册 OU 时，默认情况下会对您的 OU 及其所有账户启用强制控制。

在 OU 注册后注册部分账户

成功注册 OU 是可能的，但某些账户可能仍处于未注册状态。如果是，则这些账户不符合注册的某些先决条件。如果作为注册 OU 流程一部分的账户注册失败，则账户页面上的账户状态将显示注册失败。您还可以在您的 OU 页面上看到账户信息，例如账户字段中的 5 个中的 4 个。

例如，如果您看到 5 个账户中的 4 个，则表示您的 OU 总共有 5 个账户，其中 4 个已成功注册，但有一个账户在注册 OU 过程中注册失败。在确保账户满足注册先决条件后，您可以选择 “重新注册 OU” 来注册账户。

IAM 用户注册 OU 的先决条件

在执行注册 OU 操作时，您 AWS Identity and Access Management 的 (IAM) 身份（用户或角色）或 IAM Identity Center 用户身份必须包含在相应的 Account Factory 产品组合中，即使您已经拥有`Admin`权限。否则，预配置产品的创建将在注册过程中失败。之所以出现故障，是因为 AWS Control Tower 在注册 OU 时依赖于 IAM 用户的证书或 IAM 身份中心用户身份。

相关的投资组合由 AWS Control Tower 创建，名为 AWS Control Tower Account Factory Factory Portfolio。通过选择 “服务目录” > “账户工厂” > “AWS Control Tower 账户工厂投资组合” 导航到该目录。然后选择名为 “群组、角色和用户” 的选项卡，查看您的 IAM 或 IAM 身份中心身份。有关如何授予访问权限的更多信息，请参阅文档 AWS Service Catalog。

注册现有 OU

在 AWS Control Tower 控制台的组织页面上，您可以按层次结构查看组织的所有业务实体和账户，包括在 AWS Control Tower 注册的 OU 和未注册的 OU。

通常，未注册的 OU 是在中创建的 AWS Organizations，并且不受任何其他 landing zone 的管辖。您可以注册最多包含 300 个账户的现有 OU。如果一个 OU 包含的账户超过 300 个，则无法在 AWS Control Tower 中对其进行注册。

注册现有 OU

1. 登录 AWS Control Tower 控制台，网址为 https://console.aws.amazon.com/controltower。
2. 在左窗格导航菜单中，选择组织。
3. 在 “组织” 页面上，选择要注册的 OU 旁边的单选按钮，然后从右上角的 “操作” 下拉菜单中选择 “注册组织单位”，或者选择 OU 的名称，以便您可以查看该 OU 的 OU 详细信息页面。
4. 在 OU 详细信息页面上，您可以从右上角的操作下拉菜单中选择 “注册 OU”。

注册过程至少需要 10 分钟才能将监管范围扩展到 OU，每增加一个账户，最多需要 2 分钟。

注册现有 OU 的结果

在您注册现有 OU 后，该`AWSControlTowerExecution`角色允许 AWS Control Tower 将监管范围扩展到其个人账户。强制执行防护措施，并将有关账户活动的信息报告给您的审计和日志账户。

其他结果包括以下内容：

- `AWSControlTowerExecution`允许通过 AWS Control Tower 审计账户进行审计。
- `AWSControlTowerExecution`帮助您配置组织的日志记录，以便将每个账户的所有日志发送到日志帐户。
- `AWSControlTowerExecution`确保您选择的 AWS Control Tower 控制措施自动应用于您的 OU 中的每个个人账户以及您在 AWS Control Tower 中创建的每个新账户。

对于注册的 OU，您可以根据 AWS Control Tower 控件所包含的审计和日志功能提供合规和安全报告。您的安全性和合规性团队可以验证是否满足所有要求，并且没有发生组织偏差。有关漂移的更多信息，请参阅在 AWS Control Tower 中检测并解决偏差。

> **Note**
>
> 当 AWS Control Tower 显示 OU 及其账户时，可能会出现一种异常情况。如果您在已注册的 OU 中创建了一个账户，然后又将该注册账户转移到另一个未注册的 OU 中，特别是如果您使用 AWS Organizations 转移账户，则可以在您的 OU 详细信息页面中看到 “0 个账户中的 1 个” 的结果。此外，您可能在该未注册的 OU 中创建了另一个未注册的帐户。如果有未注册的帐户，主机可能会显示 OU 的 “1 of 1”。看来单个（新创建的）账户已注册，但事实并非如此。您必须注册新账户。

创建新的 OU

在 AWS Control Tower 中创建新的 OU

1. 导航至 “组织” 页面。
2. 从右上角的 “创建资源” 下拉菜单中选择 “创建组织单位”。
3. 在 OU 名称字段中指定名称。
4. 在父 OU 下拉列表中，您可以看到已注册 OU 的层次结构。为您正在创建的新 OU 选择父 OU。
5. 选择 添加。

> **Tip**
>
> 要以更少的步骤添加嵌套的 OU，请选择 “组织” 页面表格中显示的父 OU 的名称，查看该父 OU 的 OU 页面，然后从右上角的 “操作” 下拉菜单中选择 “添加 OU”。新的 OU 会自动创建为所选 OU 下的嵌套 OU。

> **Note**
>
> 如果你的 landing zone 不是最新的，你将在下拉菜单中看到一个平面列表而不是层次结构。即使您的着陆区域包含嵌套的 OU，您也不会在下拉列表中看到 L5 OU，因为您无法在 L5 OU

下创建新的 OU。有关 AWS Control Tower 中嵌套业务单元的更多信息，请参阅AWS Control Tower 中嵌套的 OU。

注册或重新注册期间失败的常见原因

如果 OU 或其任何成员账户的注册（或重新注册）失败，您可以下载包含详细报告的文件，该报告显示哪些预检查未通过。您可以通过选择注册区域右上角的下载按钮来完成下载。

本节列出了预检查失败时可能收到的错误类型以及如何更正错误。

通常，当您注册或重新注册一个 OU 时，该 OU 中的所有账户都将在 AWS Control Tower 中注册。但是，即使OU作为一个整体成功注册，某些帐户也可能无法注册。在这种情况下，您必须解决与该账户相关的预检查失败问题，然后尝试重新注册该账户或 OU。

着陆区错误

- 着陆区还没准备好

  重置您当前的着陆区，或将其更新到最新版本。

OU 错误

- 超过 SCP 的最大数量

  您可能已超过每个 OU 的服务控制策略 (SCP) 限制，或者可能已达到其他配额。每个 OU 上限 5 个 SCP 适用于您的 AWS Control Tower 着陆区中的所有 OU。如果您的 SCP 超过了配额允许的数量，则必须删除或合并这些 SCP。
- 相互冲突的 SCP

  现有 SCP 可能会应用于 OU 或账户，这会阻止 AWS Control Tower 注册该账户。检查已应用的 SCP 中是否存在任何可能阻止 AWS Control Tower 运行的策略。请务必检查从层次结构中较高的 OU 继承的 SCP。
- 超过堆栈集配额

  可能已超过堆栈集配额。如果您的实例数超过了配额允许的数量，则必须删除一些堆栈实例。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的 AWS CloudFormation 配额。
- 超过账户限制

AWS Control Tower 在注册期间将每个 OU 限制在 300 个账户以内。

账户错误

- 禁止对账户进行预先检查

  OU 中的现有 SCP 会阻止 AWS Control Tower 对您的 OU 成员账户进行预检查。要解决此预检查失败，请更新或从 OU 中删除 SCP。

- 电子邮件地址错误

  您为该账户指定的电子邮件地址不符合命名标准。以下是指定允许使用哪些字符的正则表达式 (regex)：`[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- 已启用 Config 记录器或传送渠道

  该账户可能有现有的 AWS Config 配置记录器或传送渠道。在注册账户之前，必须通过 AWS CLI 在 AWS Control Tower 管理账户管理资源的所有 AWS 区域中删除或修改这些内容。

- 已禁用 STS

  AWS Security Token Service (AWS STS) 可能会在账户中被禁用。 AWS 必须在 AWS Control Tower 支持的所有区域的账户中激活 STS 终端节点。

- IAM 身份中心冲突

  AWS Control Tower 主区域与 AWS IAM Identity Center （IAM 身份中心）区域不同。如果已经设置了 IAM 身份中心，则 AWS Control Tower 的主区域必须与 IAM 身份中心区域相同。

- 相互冲突的 SNS 话题

  该账户有一个亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题名称，AWS Control Tower 需要使用该名称。AWS Control Tower 创建具有特定名称的资源（例如 SNS 主题）。如果已经使用了这些名称，AWS Control Tower 的设置就会失败。如果您重复使用之前在 AWS Control Tower 中注册的账户，则可能会出现这种情况。

- 检测到已暂停的账户

  该账户已被暂停。它无法注册到 AWS Control Tower。请从此 OU 中移除账户，然后重试。

- IAM 用户不在投资组合中

  在注册 OU 之前，将 AWS Identity and Access Management (IAM) 用户添加到 Service Catalog 产品组合中。此错误仅与管理账户有关。

- 账户不符合先决条件

  该账户不符合账户注册的先决条件。例如，该账户可能缺少在 AWS Control Tower 中注册所需的角色和权限。中提供了添加角色的说明手动将所需的 IAM 角色添加到现有角色 AWS 账户 并进行注册。

提醒一下，当您在 AWS AWS CloudTrail Control Tower 中注册您的所有 AWS 账户时，系统会自动启用这些账户。 CloudTrail 如果在注册之前已在账户上启用，则除非您在开始注册流程 CloudTrail 之前停用，否则您可能会遇到双重计费的情况。

更新组织

更新组织单位 (OU) 或更新 OU 内的多个帐户的最快方法是重新注册 OU。

何时更新 AWS Control Tower 业务单元和账户

在执行 landing zone 更新时，必须更新已注册的账户才能对这些账户应用新的控制措施。

- 您可以使用 “重新注册” 选项对 OU 下的所有账户进行更新。
- 如果您的 landing zone 中有多个已注册的 OU，请重新注册所有 OU 以更新您的所有账户。
- 要更新单个账户，您可以从 AWS Control Tower 控制台进行更新，也可以在中选择更新预配置产品选项。 AWS Service Catalog请参阅 在控制台中更新账户。

更新同一 OU 中的多个账户

要在一个 OU 中更新多个账户，只需一个操作即可

1. 登录 AWS Control Tower 控制台，网址为 https://console.aws.amazon.com/controltower。
2. 在左窗格导航菜单中，选择组织。
3. 在组织页面上，选择任意 OU 以查看 OU 详细信息页面。
4. 在右上角的 “操作” 下，选择 “重新注册 OU”。

如果您需要更新所有账户和 OU，请对您的 AWS Control Tower 组织中的每个 OU 重复这些步骤。

或者，您可以选择任何显示更新可用状态的账户，然后根据需要为任意数量的账户选择 “更新账户”。

重新注册期间会发生什么

当您重新注册 OU 时：

- “州” 字段显示该账户当前是否已注册 AWS Control Tower（已注册）、该账户是否从未注册过（未注册），或者之前是否注册失败（注册失败）。
- 重新注册 OU 时，该`AWSControlTowerExecution`角色将添加到状态为 “未注册” 或 “注册失败” 的所有账户中。
- AWS Control Tower 为这些新注册的账户创建单点登录（IAM 身份中心）登录名。
- 已注册的账户将重新注册到 AWS Control Tower。
- 应用于 OU 的任何预防性控制措施的偏差都已修复，因为 SCP 会恢复其默认定义。
- 所有账户均已更新，以反映最新的 landing zone 变更。

有关更多信息，请参阅注册现有的 AWS 账户。

> **Tip**
>
> 当你重新注册一个 OU 时，或者当你更新你的 landing zone 版本和多个成员账户时，你可能会看到一条提及 StackSet-AWSControlTowerExecutionRole 的失败消息。管理账户 StackSet 中的此操作可能会失败，因为所有已注册的成员账户中都已存在 AWSControlTowerExecutionIAM 角色。此错误消息是预期行为，可以忽略。

更新单个账户

您可以在 AWS Control Tower 控制台或服务目录控制台中更新单个 AWS Control Tower 账户。

要在 AWS Control Tower 控制台中更新单个账户，请参阅在控制台中更新账户。

要在中更新单个账户 AWS Service Catalog

1. 转到 AWS Service Catalog。
2. 在左窗格导航菜单中，选择预配置产品。
3. 在预配置产品页面上，选择要更新的预配置产品旁边的单选按钮。
4. 在右上角，选择操作下拉列表进行更新。

要了解有关更新的更多信息 AWS Service Catalog，请参阅《S ervice Catalog 管理员指南》中的更新预配置的产品和更新产品。

集成服务

AWS Control Tower 是一项建立在其他 AWS 服务之上的服务，可帮助您设置架构良好的环境。本章简要概述了这些服务，包括有关底层服务的配置信息以及它们在 AWS Control Tower 中的工作方式。

有关如何测量架构良好的环境的更多信息，请了解 Well-Architected 工具AWS 。另请参阅《管理和治理云环境指南》。

主题

使用部署环境 AWS CloudFormation

AWS CloudFormation 使您能够以可预测的方式重复创建和配置 AWS 基础架构部署。它可以帮助您利用 AWS 产品在云中构建高度可靠、高度可扩展、经济实惠的应用程序，而不必担心创建和配置底层 AWS 基础架构。 AWS CloudFormation 允许您使用模板文件将资源集合作为一个单元（堆栈）一起创建和删除。有关更多信息，请参阅《AWS CloudFormation 用户指南》。

AWS Control Tower 使用 AWS CloudFormation 堆栈集对账户进行控制。有关如何 AWS CloudFormation 与 AWS Control Tower 协同工作的更多信息，请参阅 使用创建 AWS Control Tower 资源 AWS CloudFormation。

使用监控事件 CloudTrail

AWS Control Tower 配置 AWS CloudTrail 为启用集中式日志记录和审计。借 CloudTrail助，管理账户可以查看成员账户的管理操作和生命周期事件。

CloudTrail 通过保存账户的 AWS API 调用历史记录，帮助您监控云端 AWS 环境。例如，您可以识别为支持的服务调用 AWS API 的用户和账户 CloudTrail、发出呼叫的源 IP 地址以及呼叫发生的时间。您可以使用 API CloudTrail 集成到应用程序中，为您的组织自动创建跟踪，检查跟踪的状态，并控制管理员如何开启和关闭 CloudTrail 登录功能。有关更多信息，请参阅《AWS CloudTrail 用户指南》。

使用监控资源和服务 CloudWatch

Amazon CloudWatch 提供了可靠、可扩展且灵活的监控解决方案，您可以在几分钟内开始使用。您不再需要设置、管理和扩展监控系统和基础设施了。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

有关亚马逊如何 CloudWatch 使用 AWS Control Tower 的更多信息，请参阅监控。

使用管理资源配置 AWS Config

AWS Config 提供了与您的 AWS 账户关联的资源的详细视图，包括它们的配置方式、它们之间的关系以及配置及其关系如何随着时间的推移而发生变化。有关更多信息，请参阅 AWS Config 开发人员指南。

AWS Config 由 AWS Control Tower 配置的资源会自动标记为`aws-control-tower`且值为。`managed-by-control-tower`

有关如何 AWS Config 监控和记录 AWS Control Tower 中的资源以及如何向您收取费用的更多信息，请参阅使用监控资源变化 AWS Config。

AWS Control Tower 用于 AWS Config 规则 实施侦探控制。有关更多信息，请参阅关于 AWS Control Tower 中的控件。

使用 IAM 管理实体的权限

AWS Identity and Access Management (IAM) 是一项 AWS 用于控制对其他 AWS 服务的访问的服务。借助 IAM，您可以集中管理用户、安全证书（例如访问密钥和权限），这些证书指定您的用户和应用程序有权访问的 AWS 资源。

在设置 landing zone 时，如果您选择 IAM 作为身份提供商，则可以 AWS IAM Identity Center 自动为其创建多个群组。这些群组的权限集是 IAM 中预定义的权限策略。您的最终用户还可以使用 IAM 来定义 IAM 用户和成员账户内其他实体的权限范围。

AWS Identity and Access Management (IAM) 简化了您管理 AWS 账户和业务应用程序访问权限的方式。您可以在 AWS Control Tower 中控制所有 AWS 账户的 IAM 身份中心访问权限和用户权限。

有关更多信息，请参阅《AWS IAM Identity Center 用户指南》。

如果您所在的所在地 AWS 区域 不支持 IAM，则可以让其他身份提供商手动设置和维护自己的用户和群组。

AWS Key Management Service

AWS Key Management Service (AWS KMS) 允许您创建和控制保护数据的密钥。AWS Control Tower（可选）允许您使用 AWS KMS 加密密钥对数据进行加密。有关的信息 AWS KMS，请参阅 AWS KMS 开发人员指南。

有关如何使用 AWS Control Tower 设置 AWS KMS 密钥的信息，请参阅可选配置 AWS KMS 密钥。

使用 Lambda 运行无服务器计算函数

使用 AWS Lambda，您无需预置或管理服务器即可运行代码。您可以为多种类型的应用程序或后端服务运行代码，而无需额外的管理开销。当您上传代码时，Lambda 可以在高可用性下运行和扩展代码。您可以将代码设置为自动从其他 AWS 服务触发，也可以直接从任何网络或移动应用程序调用。

例如，可以通过编程方式担任 AWS Control Tower 审计账户中的某些角色，这样您就可以使用 Lambda 审核其他账户。此外，您还可以使用 AWS Control Tower 生命周期事件来触发 Lambda 函数。

通过以下方式管理账户 AWS Organizations

AWS Organizations 是一项账户管理服务，可让您将多个 AWS 账户整合到一个由您创建和集中管理的组织中。通过 Organizations，您可以创建成员账户并邀请现有账户加入您的组织。您可以将这些账户分到不同的组中，然后应用基于策略的控制。有关更多信息，请参阅《AWS Organizations 用户指南》。

在 AWS Control Tower 中，Organizations 可帮助集中管理账单；控制访问权限、合规性和安全；并在您的成员 AWS 账户之间共享资源。账户被分为各个逻辑组，这些逻辑组称为组织部门 (OU)。有关 Organizations 的更多信息，请参阅《AWS Organizations 用户指南》。

AWS Control Tower 使用以下 OU：

- Root — 着陆区域中所有账户和所有其他 OU 的父容器。
- 安全-此 OU 包含日志存档帐户、审核帐户及其拥有的资源。
- Sandbox — 此 OU 是在您设置着陆区时创建的。它和你的 landing zone 中的其他子 OU 包含你的成员账户。这些是您的最终用户访问的用于执行 AWS 资源工作的帐户。

> **Note**
>
> 您可以通过组织单位页面上的 AWS Control Tower 控制台在着陆区域中添加其他 OU。

注意事项

通过 AWS Control Tower 创建的 OU 可以对其应用控制措施。默认情况下，在 AWS Control Tower 之外创建的 OU 不能。但是，您可以注册这样的 OU。一旦您注册了 OU，就可以对其及其账户进行控制。有关注册 OU 的信息，请参阅向 AWS Control Tower 注册现有组织单位。

使用 Amazon S3 存储对象

Amazon Simple Storage Service (Amazon S3) 是一种面向 Internet 的存储服务。您可以通过 Amazon S3 随时在 Web 上的任何位置存储和检索的任意大小的数据。您可以使用 AWS Management Console 的简单直观的 Web 界面来完成这些任务。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南。

设置着陆区时，会在您的日志存档账户中创建一个 Amazon S3 存储桶，用于包含着陆区中所有账户的所有日志。

使用 Security Hub 监控您的环境

AWS Control Tower 通过名为 “服务管理标准：AWS Control Tower” 的安全中心标准与 AWS Securit y Hub 集成。有关更多信息，请参阅 S ecurity Hub 标准。

通过以下方式配置账户 AWS Service Catalog

AWS Service Catalog 使 IT 管理员能够创建、管理和向最终用户分发经批准的产品组合，然后最终用户可以在个性化门户中访问所需的产品。典型产品包括使用 AWS 资源部署的服务器、数据库、网站或应用程序。

您可以控制有权访问特定产品的用户，这使您可以强制遵守组织业务标准，管理产品生命周期，并帮助用户放心地查找和发布产品。有关更多信息，请参阅《S ervice Catalog 管理员指南》。

在 AWS Control Tower 中，您的中央云管理员和最终用户可以使用名为 “自定义蓝图” AWS Service Catalog 的产品在您的着陆区配置自定义账户。有关更多信息，请参阅步骤 2。创建 AWS Service Catalog 产品。

AWS Control Tower 还可以利用服务目录 API 来进一步自动配置和更新账户。有关详细信息，请参阅《 AWS Service Catalog 开发人员指南》。

过渡到 AWS Service Catalog 外部产品类型

AWS Service Catalog 将对 Terraform 开源产品的支持更改为一种名为 External 的新产品类型。要了解有关此过渡的更多信息，请查看管理员指南中的将现有 Terraform 开源产品和预配置产品更新为外部产品类型。AWS Service Catalog

此更改会影响您创建或注册的 AWS Control Tower 账户出厂自定义的现有账户。要将这些账户过渡到外部产品类型，您需要同时在 AWS Control Tower AWS Service Catalog 和 AWS Control Tower 中进行更改。

过渡到外部产品类型

1. 升级现有的 Terraform 参考引擎 AWS Service Catalog ，使其包括对外部和 Terraform 开源产品类型的支持。有关更新 Terraform 参考引擎的说明，请查看存储库。AWS Service Catalog GitHub
2. 在中 AWS Service Catalog，复制任何现有的 Terraform 开源产品（蓝图），副本使用新的外部产品类型。不要终止现有的 Terraform 开源蓝图。
3. 在 AWS Control Tower 中，使用 Terraform 开源蓝图更新每个账户，以使用新的外部蓝图。
    a. 要更新蓝图，必须先完全移除 Terraform 开源蓝图。有关更多详细信息，请查看从账户中移除蓝图。
    b. 将新的外部蓝图添加到同一个账户。有关更多详细信息，请查看向 AWS Control Tower 账户添加蓝图。

4. 在所有使用 Terraform 开源蓝图的账户更新为外部蓝图后，返回 AWS Service Catalog 并终止所有使用 Terraform 开源作为产品类型的产品。
5. 今后，所有使用 AWS Control Tower 账户出厂自定义创建或注册的账户都必须使用AWS CloudFormation或外部产品类型引用蓝图。

   对于使用外部产品类型创建的蓝图，AWS Control Tower 仅支持使用 Terraform 模板和 Terraform 参考引擎进行账户自定义。要了解更多信息，请查看设置为自定义。

> **Note**
>
> 创建新账户时，AWS Control Tower 不支持 Terraform 开源作为产品类型。要了解有关这些变更的更多信息，请查看管理员指南中的将现有 Terraform 开源产品和预配置产品更新为外部产品类型。AWS Service Catalog AWS Service Catalog 将根据需要支持客户完成此产品类型过渡。如需帮助，请联系您的客户代表。

通过 Amazon 简单通知服务跟踪警报

亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 是一项网络服务，它使应用程序、最终用户和设备能够立即从云端发送和接收通知。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南。

AWS Control Tower 使用 Amazon SNS 向您的管理账户和审计账户的电子邮件地址发送编程提醒。这些警报可帮助您防止在着陆区内漂移。有关更多信息，请参阅 在 AWS Control Tower 中检测并解决偏差。

我们还使用 Amazon 简单通知服务从发送合规通知 AWS Config。

> **Tip**
>
> 接收 AWS Control Tower 控制合规通知（在您的审计账户中）的最佳方式之一是订阅`AggregateConfigurationNotifications`。它是一项可帮助您检查合规性的服务。它为您提供有关不合规 AWS Config 规则的真实数据。 AWS Config 自动维护您的 OU 中的账户列表。
> 您必须使用电子邮件或 SNS 允许的任何类型的订阅方式手动订阅。该账单将`arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications`引导到您的审计账户。

使用构建分布式应用程序 AWS Step Functions

AWS Step Functions 可以轻松地将分布式应用程序的组件作为可视化工作流程中的一系列步骤进行协调。您可以快速构建和运行状态机，以可靠和可扩展的方式执行应用程序的步骤。有关更多信息，请参阅 AWS Step Functions 开发人员指南。

AWS Control Tower 中的身份和访问管理

要在着陆区域中执行任何操作，例如在 Account Factory 中配置账户或在 AWS Control Tower 控制台中创建新的组织单位 AWS Identity and Access Management (OU)，请使用 (IAM) 或 AWS IAM Identity Center 要求您验证自己是经批准的 AWS 用户。例如，如果您使用的是 AWS Control Tower 控制台，则可以通过提供管理员提供的 AWS 证书来验证您的身份。

在您对身份进行身份验证后，IAM 会 AWS 使用一组针对特定操作和资源的定义权限来控制您的访问权限。如果您是账户管理员，则可以使用 IAM 来控制其他 IAM 用户对与您的账户关联的资源的访问权限。

主题

身份验证

您可以访问 AWS 以下任何类型的身份：

- AWS 账户 root 用户 — 首次创建 AWS 账户时，首先要有一个可以完全访问账户中所有 AWS 服务和资源的身份。此身份称为 AWS 账户 root 用户。当使用创建账户所用的电子邮件地址和密码登录时，您可以获得此身份。强烈建议您不使用根用户执行日常任务，即使是管理任务。相反，请遵循最佳实践，即仅使用根用户来创建您的第一个 IAM Identity Center 用户（推荐）或 IAM 用户（在大多数用例中不是最佳实践）。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。有关更多信息，请参阅 何时以 root 用户身份登录。
- IAM 用户 — I AM 用户是您的 AWS 账户中具有特定自定义权限的身份。您可以使用 IAM 用户证书登录安全 AWS 网页，例如 AWS 管理控制台、 AWS 讨论论坛或 Su AWS pport Center。 AWS 最佳实践建议您创建 IAM Identity Center 用户而不是 IAM 用户，因为当您创建具有长期证书的 IAM 用户时，安全风险更大。

  如果您必须为特定目的创建 IAM 用户，那么除了登录凭证之外，您还可以为每个 IAM 用户生成访问密钥。在以编程方式调用 AWS 服务时，您可以使用这些密钥，无论是通过多个 SDK 中的一个还是

使用 AWS 命令行界面 (CLI)。SDK 和 CLI 工具使用访问密钥对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。AWS Control Tower 支持签名版本 4，这是一种用于对入站 API 请求进行身份验证的协议。有关对请求进行身份验证的更多信息，请参阅《 AWS 一般参考》中的 “签名版本 4 签名流程”。

- IAM 角色 – IAM 角色是可在账户中创建的一种具有特定权限的 IAM 身份。IAM 角色与 IAM 用户类似，因为它是一个 AWS 身份，它具有权限策略，用于确定该身份可以做什么和不能做什么 AWS。但是，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。此外，角色没有关联的标准长期凭证（如密码或访问密钥）。相反，当您代入角色时，它会为您提供角色会话的临时安全凭证。具有临时凭证的 IAM 角色在以下情况下很有用：
  - 联合用户访问权限 — 您可以使用来自 AWS Directory Service企业用户目录或 Web 身份提供商的现有身份，而不是创建 IAM 用户。这些用户被称为联合用户。 AWS 当通过身份提供者请求访问权限时，将角色分配给联合用户。有关联合用户的更多信息，请参阅《IAM 用户指南》中的联合用户和角色。
  - AWS 服务访问权限 — 服务角色是一个 IAM 角色，由服务代为代表您在账户中执行操作。在设置某些 AWS 服务环境时，必须为服务定义一个要扮演的角色。此服务角色必须包含服务访问其所需 AWS 资源所需的所有权限。服务角色因服务而异，但只要您满足服务记录在案的要求，许多服务都允许您选择权限。服务角色只在您的账户内提供访问权限，不能用于为访问其它账户中的服务授权。您可以从 IAM 中创建、修改和删除服务角色。例如，您可以创建一个角色以允许 Amazon Redshift 代表您访问 Amazon S3 存储桶，然后将该存储桶中的数据加载到 Amazon Redshift 集群中。有关更多信息，请参阅 IAM 用户指南中的创建角色以向 AWS 服务委派权限。
  - 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 Amazon EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 Amazon EC2 实例中存储访问密钥。要向 Amazon EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 Amazon EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。
- IAM Identit y Center 用户对 IAM 身份中心用户门户的身份验证由您连接到 IAM 身份中心的目录控制。但是，对用户门户中可供最终用户使用的 AWS 账户的授权由两个因素决定：
  - 在 AWS IAM Identity Center 控制台中，谁被分配了对这些 AWS 账户的访问权限。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的单点登录访问权限。
  - 在 AWS IAM Identity Center 控制台中向最终用户授予了什么级别的权限，以允许他们对这些 AWS 账户进行适当的访问权限。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。

访问控制

要创建、更新、删除或列出 AWS Control Tower AWS 资源或着陆区中的其他资源，您需要执行操作的权限，并且需要访问相应资源的权限。此外，要以编程方式执行该操作，您需要有效的访问密钥。

以下各节介绍如何管理 AWS Control Tower 的权限：

主题

- 管理您的 AWS Control Tower 资源的访问权限概述
- 在 AWS Control Tower 中使用基于身份的策略（IAM 策略）

与 AWS IAM 身份中心和 AWS Control Tower 合作

在 AWS Control Tower 中，IAM 身份中心允许中央云管理员和最终用户管理对多个 AWS 账户和业务应用程序的访问权限。默认情况下，AWS Control Tower 使用此服务来设置和管理对通过 Account Factory 创建的账户的访问权限，除非您选择了自行管理身份和访问控制的选项。

有关选择身份提供者的更多信息，请参阅IAM 身份中心指南。

有关如何在 AWS Control Tower 中设置 IAM 身份中心用户和权限的简短教程，您可以观看此视频 (6:23)。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

在 AWS Control Tower 中设置 AWS IAM 身份中心的视频演练。

关于使用 IAM 身份中心设置 AWS Control Tower

最初设置 AWS Control Tower 时，只有根用户用户和具有正确权限的任何 IAM 用户才能添加 IAM 身份中心用户。但是，将最终用户添加到AWSAccountFactory群组后，他们可以通过 Account Factory 向导创建新的 IAM Identity Center 用户。有关更多信息，请参阅使用 Account Factory 配置和管理账户。

如果您选择推荐的默认设置，AWS Control Tower 会使用预先配置的目录来设置您的着陆区，该目录可帮助您管理用户身份和单点登录，这样您的用户就可以跨账户进行联合访问。设置 landing zone 时，会创建此默认目录以包含用户组和权限集。

> **Note**
>
> 您可以使用 IAM I AWS IAM Identity Center dentity Center 的委托管理员功能，将组织中的管理委托给管理账户以外的账户。如果您选择使用此功能，请注意，有权管理群组成员资格的管

理员也可以管理分配给管理帐户的群组。有关更多信息，请参阅这篇题为 “AWS SSO 委托管理入门” 的博客文章

用户组、角色和权限集

用户组管理在共享账户中定义的专用角色 。角色建立同属一组的权限集。组的所有成员继承与组关联的权限集或角色。您可以为成员账户的最终用户创建新组，以便您只能自定义分配某个组所执行的特定任务所需的角色。

可用的权限集涵盖了各种不同的用户权限要求，例如只读访问权限、AWS Control Tower 管理权限和 Service Catalog 访问权限。这些权限集使您的最终用户能够在您的着陆区（Landing zone）中快速配置自己的 AWS 帐户，同时遵守企业的指导方针。

有关规划用户、组和权限分配的提示，请参阅 设置群组、角色和策略的建议

有关如何在 AWS Control Tower 环境中使用此服务的更多信息，请参阅AWS IAM Identity Center 用户指南中的以下主题。

- 要添加用户，请参阅添加用户。
- 要将用户添加到组，请参阅将用户添加到组。
- 要编辑用户属性，请参阅编辑用户属性。
- 要添加组，请参阅添加组。

Warning

AWS Control Tower 在您所在的地区设置您的 IAM 身份中心目录。如果您在另一个区域设置了着陆区，然后导航到 IAM Identity Center 控制台，则必须将该区域更改为您的主区域。请勿删除您所在地区的 IAM 身份中心配置。

关于 IAM 身份中心账户和 AWS Control Tower 的注意事项

以下是在 AWS Control Tower 中使用 IAM 身份中心用户账户时需要了解的一些好消息。

- 如果您的 AWS IAM Identity Center 用户账户被禁用，则在尝试在 Account Factory 中配置新账户时，您将收到一条错误消息。您可以在 IAM 身份中心控制台中重新启用您的 IAM 身份中心用户。

- 如果您在更新与 Account Factory 出售的账户关联的预配置产品时指定了新的 IAM Identity Center 用户电子邮件地址，AWS Control Tower 会创建一个新的 IAM 身份中心用户账户。之前创建的用户账户不会被删除。如果您希望从 IAM Identity Center 中删除之前 AWS 的 IAM 身份中心用户电子邮件地址，请参阅禁用用户。
- AWS IAM 身份中心已与 Azure 活动目录集成，你可以将现有的 Azure 活动目录连接到 AWS Control Tower。
- 有关 AWS Control Tower 行为如何与 AWS IAM 身份中心和不同身份源交互的更多信息，请参阅 AWS IAM 身份中心文档中的更改身份源的注意事项。

适用于 AWS Control Tower 的 IAM 身份中心群组

AWS Control Tower 提供预配置的群组，用于组织在您的账户中执行特定任务的用户。您可以直接在 IAM Identity Center 中添加用户并将其分配到这些群组。这样做会将权限集与账户中的组用户进行匹配。在设置 landing zone 时，会创建以下群组。

AWSAccountFactory

账户	权限集	描述
管理账户	AWSServiceCatalogEndUserAccess	此组仅用于此账户中使用 Account Factory 配置新账户。

AWSServiceCatalogAdmins

账户	权限集	描述
管理账户	AWSServiceCatalogAdminFullAccess	该组仅在该账户中用于对 Account Factory 进行管理更改。除非该群组中的用户也加入群AWSAccountFactory组，否则他们无法配置新帐户。

AWSControlTowerAdmins

账户	权限集	描述
管理账户	AWSAdministratorAccess	该账户中该群组的用户是唯一有权访问 AWS Control Tower 控制台的用户。
日志存档账户	AWSAdministratorAccess	用户拥有此账户的管理员访问权限。
审计账户	AWSAdministratorAccess	用户拥有此账户的管理员访问权限。
成员账户	AWSOrganizationsFullAccess	用户在此账户中拥有对 Organizations 的完全访问权限。

AWSSecurityAuditPowerUsers

账户	权限集	描述
管理账户	AWSPowerUserAccess	用户可以执行应用程序开发任务，也可以创建和配置支持有 AWS 意识的应用程序开发的资源和服务。
日志存档账户	AWSPowerUserAccess	用户可以执行应用程序开发任务，也可以创建和配置支持有 AWS 意识的应用程序开发的资源和服务。
审计账户	AWSPowerUserAccess	用户可以执行应用程序开发任务，也可以创建和配置支持有 AWS 意识的应用程序开发的资源和服务。
成员账户	AWSPowerUserAccess	用户可以执行应用程序开发任务，也可以创建和配置支持有

账户	权限集	描述
		AWS 意识的应用程序开发的资源和服务。

AWSSecurityAuditors

账户	权限集	描述
管理账户	AWSReadOnlyAccess	用户对该账户中的所有 AWS 服务和资源具有只读访问权限。
日志存档账户	AWSReadOnlyAccess	用户对该账户中的所有 AWS 服务和资源具有只读访问权限。
审计账户	AWSReadOnlyAccess	用户对该账户中的所有 AWS 服务和资源具有只读访问权限。
成员账户	AWSReadOnlyAccess	用户对该账户中的所有 AWS 服务和资源具有只读访问权限。

AWSLogArchiveAdmins

账户	权限集	描述
日志存档账户	AWSAdministratorAccess	用户拥有此账户的管理员访问权限。

AWSLogArchiveViewers

账户	权限集	描述
日志存档账户	AWSReadOnlyAccess	用户对该账户中的所有 AWS 服务和资源具有只读访问权限。

AWSAuditAccountAdmins

账户	权限集	描述
审计账户	AWSAdministratorAccess	用户拥有此账户的管理员访问权限。

管理您的 AWS Control Tower 资源的访问权限概述

每个 AWS 资源都归人所有 AWS 账户，创建资源或获取资源访问权限的权限受权限策略的约束。账户管理员可以向 IAM 身份（即：用户、组和角色）附加权限策略。某些服务（例如 AWS Lambda）还支持为资源附加权限策略。

> **Note**
>
> 账户管理员（或管理员）是具有管理员权限的用户。有关更多信息，请参阅《IAM 用户指南》中的 IAM 最佳实操。

当你负责向用户或角色授予权限时，你必须知道并跟踪需要权限的用户和角色、每个用户和角色需要权限的资源，以及操作这些资源必须允许的特定操作。

主题

- AWS Control Tower 资源和操作
- 关于资源所有权
- 管理对资源的访问权限
- 指定策略元素：操作、效果和主体
- 在策略中指定条件

AWS Control Tower 资源和操作

在 AWS Control Tower 中，主要资源是着陆区。AWS Control Tower 还支持另一种资源类型，即控件，有时也称为护栏。但是，对于 AWS Control Tower，您只能在现有着陆区的环境中管理控件。控件可以称为子资源。

中的资源和子资源 AWS 具有与之关联的唯一 Amazon 资源名称 (ARN)，如下例所示。

AWS Control Tower 提供了一组 API 操作，用于处理 AWS Control Tower 资源。有关可用操作的列表，请参阅 AWS Control Tower 《AWS Control Tower API 参考》。

有关 AWS Control Tower 中 AWS CloudFormation 资源的更多信息，请参阅 AWS CloudFormation 用户指南。

关于资源所有权

该 AWS 账户拥有在账户中创建的资源，无论谁创建了这些资源。具体而言，资源所有者是对资源创建请求进行身份验证的委托人实体（即 AWS 账户 根用户、IAM 身份中心用户、IAM 用户或 IAM 角色）的 AWS 账户。以下示例说明了它的工作原理：

- 如果您使用 AWS 账户的账户根用户凭证来设置着陆区，则您的 AWS 账户就是该资源的所有者。AWS
- 如果您在自己的 AWS 账户中创建 IAM 用户并向该用户授予设置着陆区的权限，则只要其账户满足先决条件，该用户就可以设置着陆区。但是，该用户所属的您的 AWS 账户拥有着陆区资源。
- 如果您在 AWS 账户中创建具有设置着陆区的权限的 IAM 角色，则任何能够担任该角色的人都可以设置着陆区。该角色所属的 AWS 账户拥有着陆区资源。

管理对资源的访问权限

权限策略规定谁可以访问哪些内容。下一节介绍创建权限策略时的可用选项。

> **Note**
>
> 本节讨论在 AWS Control Tower 的背景下使用 IAM。这里不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅《IAM 用户指南》中的什么是 IAM？。有关 IAM 策略语法和说明的信息，请参阅《IAM 用户指南》中的 AWS IAM 策略参考。

附加到 IAM 身份的策略称为基于身份的策略（IAM 策略）。附加到资源的策略称为基于资源的策略。

> **Note**
>
> AWS Control Tower 仅支持基于身份的策略（IAM 策略）。

主题

关于基于身份的策略（IAM 策略）

您可以向 IAM 身份附加策略。例如，您可以执行以下操作：

- 将@@ 权限策略附加到您账户中的用户或群组 — 要向用户授予创建 AWS Control Tower 资源（例如设置着陆区）的权限，您可以将权限策略附加到该用户所属的用户或群组。
- 向角色附加权限策略（授予跨账户权限）– 您可以向 IAM 角色附加基于身份的权限策略，以授予跨账户的权限。例如，一个 AWS 账户（账户 A）的管理员可以创建一个向另一个账户（账户 B）授予跨 AWS 账户权限的角色，或者管理员可以创建一个向其他 AWS 服务授予权限的角色。
  1. 账户 A 管理员创建一个 IAM 角色并向该角色附加权限策略，该策略授予管理账户 A 中资源的权限。
  2. 账户 A 管理员为该角色附加信任策略。该策略将账户 B 标识为可担任该角色的主体。
  3. 作为委托人，账户 B 管理员可以向账户 B 中的任何用户授予担任该角色的权限。通过担任该角色，账户 B 中的用户可以创建账户 A 中的资源或获得对这些资源的访问权限。
  4. 要向 AWS 服务授予担任该角色的能力（权限），您在信任策略中指定的委托人可以是 AWS 服务。

创建角色并分配权限

角色和权限允许您访问 AWS Control Tower 和其他 AWS 服务中的资源，包括以编程方式访问资源。

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。

- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

有关使用 IAM 委托权限的更多信息，请参阅 IAM 用户指南中的访问权限管理。

> **Note**
>
> 设置 AWS Control Tower 着陆区时，您需要具有AdministratorAccess托管策略的用户或角色。(arn: aws: iam:: aws: policy/) AdministratorAccess

为 AWS 服务（IAM 控制台）创建角色

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。
3. 对于 Trusted entity type（可信实体类型），选择 AWS 服务。
4. 对于服务或使用案例，请选择服务，然后选择使用案例。用例由服务定义以包含服务要求的信任策略。
5. 选择下一步。
6. 对于权限策略，选项取决于您选择的使用案例：
   - 如果服务定义了角色的权限，则您无法选择权限策略。
   - 从一组有限的权限策略中进行选择。
   - 从所有权限策略中进行选择。
   - 不选择任何权限策略，创建角色后创建策略，然后将这些策略附加到该角色。
7. （可选）设置权限边界。这是一项高级特征，可用于服务角色，但不可用于服务相关角色。

   a. 打开设置权限边界部分，然后选择使用权限边界控制最大角色权限。

IAM 包含您账户中的 AWS 托管策略和客户托管策略列表。

b. 选择要用于权限边界的策略。

8. 选择下一步。
9. 对于角色名称，选项取决于服务：

- 如果服务定义角色名称，则您无法编辑角色名称。
- 如果服务定义角色名称的前缀，您可以输入可选的后缀。
- 如果服务未定义角色名称，您可以为该角色命名。

> **Important**
>
> 命名角色时，请注意以下事项：
>
> - 角色名称在您内部必须是唯一的 AWS 账户，并且不能因大小写而变得唯一。
>
> 例如，不要同时创建名为 **PRODROLE** 和 **prodrole** 的角色。当角色名称在策略中使用或者作为 ARN 的一部分时，角色名称区分大小写，但是当角色名称在控制台中向客户显示时（例如，在登录期间），角色名称不区分大小写。
> - 创建角色后，您无法编辑该角色的名称，因为其他实体可能会引用该角色。

10. （可选）对于描述，输入角色的描述。
11. （可选）要编辑角色的使用案例和权限，请在步骤 1：选择可信实体或步骤 2：添加权限部分中选择编辑。
12. （可选）为了帮助识别、组织或搜索角色，请以键值对形式添加标签。有关在 IAM 中使用标签的更多信息，请参阅《IAM 用户指南》中的标记 IAM 资源。
13. 检查该角色，然后选择创建角色。

使用 JSON 策略编辑器创建策略

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在左侧的导航窗格中，选择策略。

   如果这是您首次选择策略，则会显示欢迎访问托管式策略页面。选择开始使用。
3. 在页面的顶部，选择创建策略。
4. 在策略编辑器部分，选择 JSON 选项。

5. 输入或粘贴一个 JSON 策略文档。有关 IAM 策略语言的详细信息，请参阅 IAM JSON 策略参考。
6. 解决策略验证过程中生成的任何安全警告、错误或常规警告，然后选择下一步。

> **Note**
>
> 您可以随时在可视化和 JSON 编辑器选项卡之间切换。不过，如果您进行更改或在可视化编辑器中选择下一步，IAM 可能会调整策略结构以针对可视化编辑器进行优化。有关更多信息，请参阅《IAM 用户指南》中的调整策略结构。

7. （可选）在中创建或编辑策略时 AWS Management Console，可以生成可在模板中使用的 JSON 或 YAML 策略 AWS CloudFormation 模板。

   为此，请在策略编辑器中选择操作，然后选择生成 CloudFormation模板。要了解更多信息 AWS CloudFormation，请参阅AWS CloudFormation 用户指南中的AWS Identity and Access Management 资源类型参考。
8. 向策略添加完权限后，选择下一步。
9. 在查看并创建页面上，为您要创建的策略键入策略名称和描述（可选）。查看此策略中定义的权限以查看策略授予的权限。
10. （可选）通过以密钥值对的形式附加标签来向策略添加元数据。有关在 IAM 中使用标签的更多信息，请参阅 《IAM 用户指南》 中的标记 IAM 资源。
11. 选择创建策略可保存您的新策略。

使用可视化编辑器创建策略

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在左侧的导航窗格中，选择策略。

   如果这是您首次选择策略，则会显示欢迎访问托管式策略页面。选择开始使用。
3. 选择创建策略。
4. 在 “策略编辑器” 部分，找到 “选择服务” 部分，然后选择 AWS 服务。您可以使用顶部的搜索框限制服务列表中的结果。您只能在一个可视化编辑器权限块中选择一个服务。要为多个服务授予访问权限，请选择添加更多权限以添加多个权限块。
5. 对于允许的操作，选择要添加到策略的操作。您可以使用以下方法选择操作：

   - 选中所有操作的复选框。

- 选择添加操作以输入特定操作的名称。您可以使用通配符 (*) 来指定多个操作。
- 选择访问级别组之一以选择访问级别的所有操作（例如，读取、写入或列出）。
- 展开每个访问级别组以选择单独的操作。

预设情况下，您创建的策略允许执行选择的操作。要拒绝选择的操作，请选择切换到拒绝权限。由于 IAM 默认拒绝，作为安全最佳实践，我们建议您仅允许用户所需的操作和资源的权限。创建一个 JSON 语句以仅在您想要覆盖其他语句或策略单独允许的权限时才拒绝权限。我们建议您将拒绝权限数限制为最低，因为它们可能会增加解决权限问题的难度。

6. 对于资源，如果您在前面步骤中选择的服务和操作不支持选择特定资源，则允许使用所有资源，并且您无法编辑此部分。

   如果您选择了一个或多个操作支持资源级权限，可视化编辑器会列出这些资源。然后，展开资源以指定您的策略的资源。

   您可以通过以下方式指定资源：

   - 选择添加 ARN，通过 Amazon 资源名称（ARN）指定资源。您可以使用可视化 ARN 编辑器或手动列出 ARN。有关 ARN 语法的更多信息，请参阅 IA M 用户指南中的亚马逊资源名称 (ARN)。有关在策略Resource元素中使用 ARN 的信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：资源。
   - 选择资源旁边的此账户中的任意项以授予对该类型的任何资源的权限。
   - 选择所有以选择该服务的所有资源。

7. （可选）选择请求条件 – 可选，以在创建的策略中添加条件。条件限制 JSON 策略语句的效果。例如，您可以指定仅在以下情况下允许用户对资源执行操作：该用户的请求发生在特定的时间范围内。您还可以使用常用条件来限制是否必须使用多重身份验证 (MFA) 设备对用户进行身份验证。或者，您可以要求请求来自特定范围的 IP 地址。有关可在策略条件中使用的所有上下文密钥的列表，请参阅《服务授权参考》中的AWS 服务操作、资源和条件密钥。

   您可以使用以下方法选择条件：

   - 使用复选框选择常用的条件。
   - 选择添加其他条件以指定其他条件。选择条件的条件键、限定词和运算符，然后输入值。要添加多个值，请选择添加。您可以将这些值视为通过逻辑OR运算符连接的。完成后，选择添加条件。

要添加多个条件，请再次选择添加其他条件。根据需要重复上述步骤。每个条件仅适用于该可视化编辑器权限块。所有条件都必须为 true，才会将权限块视为匹配项。换句话说，考虑要通过逻辑AND运算符连接的条件。

有关条件元素的更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：条件。

8. 要添加更多权限块，请选择添加更多权限。对于每个块，重复步骤 2 到步骤 5。

> **Note**
>
> 您可以随时在可视化和 JSON 编辑器选项卡之间切换。不过，如果您进行更改或在可视化编辑器中选择下一步，IAM 可能会调整策略结构以针对可视化编辑器进行优化。有关更多信息，请参阅《IAM 用户指南》中的调整策略结构。

9. （可选）在中创建或编辑策略时 AWS Management Console，可以生成可在模板中使用的 JSON 或 YAML 策略 AWS CloudFormation 模板。

   为此，请在策略编辑器中选择操作，然后选择生成 CloudFormation模板。要了解更多信息 AWS CloudFormation，请参阅AWS CloudFormation 用户指南中的AWS Identity and Access Management 资源类型参考。

10. 向策略添加完权限后，选择下一步。
11. 在查看并创建页面上，为您要创建的策略键入策略名称和描述（可选）。查看此策略中定义的权限，确保您授予了所需的权限。
12. （可选）通过以密钥值对的形式附加标签来向策略添加元数据。有关在 IAM 中使用标签的更多信息，请参阅 《IAM 用户指南》 中的标记 IAM 资源。
13. 选择创建策略可保存您的新策略。

授予编程访问权限

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS Management Console。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
人力身份 （在 IAM Identity Center 中管理的用户）	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中的 “配置 AWS CLI 要使用”。 • 有关 AWS 软件开发工具包、工具和 AWS API，请参阅《软件开发工具包和AWS 工具参考指南》中的 IAM 身份中心身份验证。
IAM	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照 IAM 用户指南中的将临时证书与 AWS 资源配合使用中的说明进行操作。
IAM	（不推荐使用） 使用长期凭证签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface • 有关 AWS SDK 和工具，请参阅 S AWS DK 和工具参考指南中的使用长期凭证进行身份验证。 • 有关 AWS API，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。

防范攻击者

有关在向其他 AWS 服务主体授予权限时如何帮助防范攻击者的更多信息，请参阅角色信任关系的可选条件。通过在策略中添加某些条件，您可以帮助防止一种特定类型的攻击，即混淆副手攻击，这种攻击发生在实体强迫权限更高的实体执行操作（例如跨服务模仿）时发生。有关政策条件的一般信息，另请参阅在策略中指定条件。

有关在 AWS Control Tower 中使用基于身份的策略的更多信息，请参阅。在 AWS Control Tower 中使用基于身份的策略（IAM 策略）有关用户、组、角色和权限的更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html中的身份（用户、组和角色）。

基于资源的策略

其他服务（如 Amazon S3）还支持基于资源的权限策略。例如，您可以将策略附加到 S3 存储桶以管理对该存储桶的访问权限。AWS Control Tower 不支持基于资源的策略。

指定策略元素：操作、效果和主体

您可以通过 AWS Control Tower 控制台或着陆区 API 来设置和管理您的着陆区。要设置您的着陆区，您必须是具有 IAM 策略中定义的管理权限的 IAM 用户。

以下是您可以在策略中识别的最基本的元素：

- 资源 - 在策略中，您可以使用 Amazon 资源名称（ARN）标识策略应用到的资源。有关更多信息，请参阅 AWS Control Tower 资源和操作。
- 操作 – 您可以使用操作关键字标识要允许或拒绝的资源操作。有关可供执行的操作类型的信息，请参阅 AWS Control Tower 定义的操作。
- 效果：您可以指定当用户请求特定操作（可以是允许或拒绝）时的效果。如果没有显式授予（允许）对资源的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问，这样可确保用户无法访问该资源，即使有其他策略授予了访问权限的情况下也是如此。
- 委托人 — 在基于身份的策略（IAM 策略）中，策略所关联的用户是隐式委托人。对于基于资源的策略，您可以指定要接收权限的用户、账户、服务或其他实体（仅适用于基于资源的策略）。AWS Control Tower 不支持基于资源的策略。

有关 IAM 策略语法和介绍的更多信息，请参阅《IAM 用户指南》中的 AWS IAM 策略参考。

在策略中指定条件

当您授予权限时，可使用 IAM 策略语言来指定规定策略何时生效的条件。例如，您可能希望策略仅在特定日期后应用。有关使用策略语言指定条件的更多信息，请参阅《IAM 用户指南》中的条件。

要表达条件，您可以使用预定义的条件键。没有特定于 AWS Control Tower 的条件密钥。但是，您可以根据需要使用 AWS范围内的条件键。有关 AWS范围密钥的完整列表，请参阅 IAM 用户指南中的条件可用密钥。

防止跨服务模仿

在中 AWS，跨服务模仿可能会导致混乱的副手问题。当一个服务调用另一个服务时，如果一个服务操纵另一个服务，使用其权限以其他方式不允许的方式对客户的资源进行操作，则会发生跨服务模仿。为了防止这种攻击，我们 AWS 提供了一些工具来帮助您保护数据，以便只有拥有合法权限的服务才能访问您账户中的资源。

我们建议使用策略中的`aws:SourceArn`和`aws:SourceAccount`条件来限制 AWS Control Tower 授予其他服务访问您的资源的权限。

- `aws:SourceArn`如果您只想将一个资源与跨服务访问相关联，请使用。
- `aws:SourceAccount`如果您想允许该账户中的任何资源与跨服务使用相关联，请使用。
- 如果该`aws:SourceArn`值不包含账户 ID，例如 Amazon S3 存储桶的 ARN，则必须同时使用这两个条件来限制权限。
- 如果您同时使用这两个条件，并且该`aws:SourceArn`值包含账户 ID，则该`aws:SourceAccount`值和`aws:SourceArn`值中的账户在同一政策声明中使用时必须显示相同的账户 ID

有关更多信息以及示例，请参阅 https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html。

在 AWS Control Tower 中使用基于身份的策略（IAM 策略）

本主题提供了基于身份的策略示例，这些示例演示了账户管理员如何将权限策略附加到 IAM 身份（即用户、群组和角色），从而授予对 AWS Control Tower 资源执行操作的权限。

> **Important**
>
> 我们建议您先阅读介绍性主题，这些主题解释了管理您的 AWS Control Tower 资源访问权限的基本概念和选项。有关更多信息，请参阅 管理您的 AWS Control Tower 资源的访问权限概述。

使用 AWS Control Tower 控制台所需的权限

当您设置着陆区时，AWS Control Tower 会自动创建三个角色。所有这三个角色都需要允许访问控制台。作为最佳实践，AWS Control Tower 将权限分为三个角色，以限制对最少量的操作和资源的访问。

三个必填角色

- AWS ControlTowerAdmin 角色
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

我们建议您限制对这些角色的角色信任策略的访问权限。有关更多信息，请参阅角色信任关系的可选条件。

AWS ControlTowerAdmin 角色

此角色为 AWS Control Tower 提供了访问对维护着陆区至关重要的基础设施的权限。该AWS ControlTowerAdmin角色需要附加的托管策略和 IAM 角色的角色信任策略。角色信任策略是一种基于资源的策略，用于指定哪些委托人可以担任该角色。

以下是此角色信任策略的示例片段：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

要从 AWS CLI 创建此角色并将其放入名为的文件中`trust.json`，以下是 CLI 命令示例：

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://trust.json
```

此角色需要两个 IAM 策略。

1. 内联策略，例如：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
```

2. 随后的托管策略，即`AWS ControlTowerServiceRolePolicy`。

AWS ControlTowerServiceRolePolicy

AWS ControlTowerServiceRolePolicy是一项 AWS托管策略，它定义了创建和管理 AWS Control Tower 资源的权限，例如堆栈 AWS CloudFormation 集和堆栈实例、 AWS CloudTrail 日志文件、AWS Control Tower 的配置聚合器以及受 AWS Control Tower 管理的 AWS Organizations 账户和组织单位 (OU)。

表中汇总了此托管策略的更新[AWS Control Tower 的托管策略](#)。

有关更多信息，请参阅 [AWSControlTowerServiceRolePolicy](#)AWS 托管策略参考指南。

托管策略名称：`AWS ControlTowerServiceRolePolicy`

的 JSON 构`AWS ControlTowerServiceRolePolicy`件如下所示：

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:ListRegions",
                "account:GetRegionOptStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
```

```
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
                "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:PutEventSelectors",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
                "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-controltower*/*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution",
                "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "ec2:DescribeAvailabilityZones",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "organizations:CreateAccount",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListRoots",
                "organizations:MoveAccount",
                "servicecatalog:AssociatePrincipalWithPortfolio"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:GetRolePolicy"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
                "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
                "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:DeleteConfigurationAggregator",
                "config:PutConfigurationAggregator",
                "config:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "config.amazonaws.com",
                        "cloudtrail.amazonaws.com"
                    ]
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloudtrail.amazonaws.com"
                }
            }
        }
    ]
}
```

角色信任政策：

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

内联策略是AWSControlTowerAdminPolicy：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
```

```
}
```

AWS ControlTowerStackSetRole

AWS CloudFormation 担任此角色是为了在 AWS Control Tower 创建的账户中部署堆栈集。内联策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

信任策略

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerCloudTrailRole

AWS Control Tower CloudTrail 作为最佳实践启用，并将此角色提供给 CloudTrail。 CloudTrail担任此角色来创建和发布 CloudTrail 日志。内联策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
```

信任策略

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerBlueprintAccess 角色要求

AWS Control Tower 要求您在同一组织内的指定蓝图中心账户中创建`AWSControlTowerBlueprintAccess`角色。

角色名称

角色名称必须为 `AWSControlTowerBlueprintAccess`。

角色信任政策

必须将该角色设置为信任以下委托人：

- 在管理账户中使用 AWS Control Tower 的委托人。
- 管理账户中的AWSControlTowerAdmin角色。

以下示例显示了最低权限的信任策略。当您制定自己的策略时，请将该术语*YourManagementAccountId*替换为您的 AWS Control Tower 管理账户的实际账户 ID，并将该术语*YourControlTowerUserRole*替换为管理账户的 IAM 角色标识符。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

角色权限

您需要将托管策略附加AWSServiceCatalogAdminFullAccess到该角色。

AWSServiceRoleForAWSControlTower

此角色为 AWS Control Tower 提供了访问日志存档账户、审计账户和成员账户的权限，用于对维护着陆区至关重要的操作，例如通知您有关资源漂移的情况。

该AWSServiceRoleForAWSControlTower角色需要附加的托管策略和 IAM 角色的角色信任策略。

此角色的托管策略：AWSControlTowerAccountServiceRolePolicy

角色信任政策：

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerAccountServiceRolePolicy

此 AWS托管策略允许 AWS Control Tower 代表您调用提供自动账户配置和集中管理的 AWS 服务。

该策略包含 AWS Control Tower 对由 Security Hub 控件管理的资源实施 AWS Security Hub 调查结果转发的最低权限，这些资源是 Sec urity Hub 服务托管标准：AWS Control Tower 的一部分，并且它可以防止限制客户账户管理能力的更改。它是背景 AWS Security Hub 漂移检测过程的一部分，不是由客户直接启动的。

该策略允许在每个成员账户中创建 Amazon EventBridge 规则，特别是针对 Security Hub 控件的规则，并且这些规则必须指定确切的规则 EventPattern。此外，规则只能对我们的服务主体管理的规则起作用。

服务负责人：`controltower.amazonaws.com`

的 JSON 构`AWSControlTowerAccountServiceRolePolicy`件如下所示：

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
  //For creating the managed rule
   "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "events:source": "aws.securityhub"
    },
    "Null": {
```

```
      "events:detail-type": "false"
     },
     "StringEquals": {
      "events:ManagedBy": "controltower.amazonaws.com",
      "events:detail-type": "Security Hub Findings - Imported"
     }
    }
   },
   // Other operations to manage the managed rule
   {
    "Sid": "AllowOtherOperationsOnRulesManagedByControlTower",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
    "Condition": {
     "StringEquals": {
      "events:ManagedBy": "controltower.amazonaws.com"
     }
    }
   },
   // More managed rule permissions
   {
    "Sid": "AllowDescribeOperationsOnRulesManagedByControlTower",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:ListTargetsByRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/*ControlTower*"
   },
   // Add permission to publish the security notifications to SNS
   {
    "Sid": "AllowControlTowerToPublishSecurityNotifications",
    "Effect": "Allow",
    "Action": "sns:publish",
    "Resource": "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
    "Condition": {
     "StringEquals": {
```

```
      "aws:PrincipalAccount": "${aws:ResourceAccount}"
     }
    }
   },
   // For drift verification
   {
    "Sid": "AllowActionsForSecurityHubIntegration",
    "Effect": "Allow",
    "Action": [
     "securityhub:DescribeStandardsControls",
     "securityhub:GetEnabledStandards"
    ],
    "Resource": "arn:aws:securityhub:*:*:hub/default"
   }
  ]
}
```

表中汇总了此托管策略的更新AWS Control Tower 的托管策略。

AWS Control Tower 的托管策略

AWS 通过提供由创建和管理的独立 IAM 策略来解决许多常见用例 AWS。托管式策略可授予常用案例的必要权限，因此，您可以免去调查都需要哪些权限的工作。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略。

更改	描述	日期
AWSControlTowerAccountServiceRolePolicy— 一项新政策	AWS Control Tower 添加了一个新的服务相关角色，允许 AWS Control Tower 创建和管理事件规则，并根据这些规则管理与 Security Hub 相关的控件的偏差检测。 当这些资源与 Security Hub 服务托管标准：AWS Control Tower 中的 Security Hub 控件相关时，需要进行此项更改，以便客户可以在控制台中查看漂移的资源。	2023 年 5 月 22 日

更改	描述	日期
AWS ControlTowerServiceRolePolicy – 更新了现有策略	AWS Control Tower 添加了新的权限`EnableRegion` ，`ListRegions` 允许 AWS Control Tower 调用 AWS 账户管理服务实施的、和 `GetRegionOptStatus` API，从而使登录区域中的客户账户（管理账户、日志存档账户、审计账户、OU 成员账户）AWS 区域 可以使用选择加入。 需要进行此项更改，以便客户可以选择将 AWS Control Tower 的区域管理扩展到可选择加入的区域。	2023 年 4 月 6 日

更改	描述	日期
AWS ControlTowerServiceRolePolicy – 更新了现有策略	AWS Control Tower 添加了新的权限，允许 AWS Control Tower 在蓝图（中心）账户中担任`AWSControlTowerBlueprintAccess` 角色，该账户是组织中的专用账户，包含存储在一个或多个服务目录产品中的预定义蓝图。AWS Control Tower 负责执行三项任务：创建服务目录组合，添加请求的蓝图产品，并在账户配置时将产品组合共享到请求的成员账户。`AWSControlTowerBlueprintAccess` 需要进行此项更改，以便客户可以通过 AWS Control Tower Account Factory 配置自定义账户。	2022 年 10 月 28 日
AWS ControlTowerServiceRolePolicy – 更新了现有策略	从着陆区版本 3.0 开始，AWS Control Tower 添加了新的权限，允许客户设置组织级别的 AWS CloudTrail 跟踪。 基于组织的 CloudTrail 功能要求客户为 CloudTrail 服务启用可信访问权限，并且 IAM 用户或角色必须有权在管理账户中创建组织级跟踪。	2022 年 6 月 20 日

更改	描述	日期
AWS ControlTowerServiceRolePolicy – 更新了现有策略	AWS Control Tower 添加了新的权限，允许客户使用 KMS 密钥加密。 KMS 功能允许客户提供自己的 KMS 密钥来加密 CloudTrail 日志。客户还可以在着陆区更新或修复期间更改 KMS 密钥。更新 KMS 密钥时，AWS CloudFormation 需要调用 AWS CloudTrail `PutEventSelector` API 的权限。此政策的更改是允许该AWS ControlTowerAdmin角色调用 AWS CloudTrail `PutEventSelector` API。	2021 年 7 月 28 日
AWS Control Tower 开始跟踪变更	AWS Control Tower 开始跟踪其 AWS 托管策略的变更。	2021 年 5 月 27 日

AWS Control Tower 中的安全

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 AWS Control Tower 的合规计划，请参阅按合规计划划分的范围内AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

本文档可帮助您了解在使用 AWS Control Tower 时如何应用分担责任模型。以下主题向您展示了如何配置 AWS Control Tower 以满足您的安全与合规目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 AWS Control Tower 资源。

AWS Control Tower 中的数据保护

责任共担模式 AWS 分担责任模型适用于 AWS Control Tower 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。

- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API 或软件开发工具包 AWS 服务 使用 AWS Control Tower 或其他 AWS 软件开发工具包的情况。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

> **Note**
>
> 设置着陆区时 AWS CloudTrail ，AWS Control Tower 会自动处理用户活动记录。

有关数据保护的更多信息，请参阅AWS 安全性博客 上的AWS 责任共担模式和 GDPR 博客文章。AWS Control Tower 提供了以下选项，您可以使用这些选项来帮助保护您的着陆区中存在的内容：

主题

静态加密

AWS Control Tower 使用亚马逊 S3 存储桶和亚马逊 DynamoDB 数据库，这些存储桶和使用亚马逊 S3 托管密钥 (SSE-S3) 进行静态加密以支持您的着陆区。这种加密是在您设置 landing zone 时默认配置的。或者，您可以将 landing zone 配置为使用 KMS 加密密钥对资源进行加密。您还可以为在 landing zone 中使用的服务为支持该服务的服务建立静态加密。有关更多信息，请参阅该服务在线文档的安全章节。

传输中加密

AWS Control Tower 使用传输层安全 (TLS) 和客户端加密在传输中进行加密，以支持您的着陆区。此外，访问 AWS Control Tower 需要使用控制台，控制台只能通过 HTTPS 终端节点进行访问。这种加密是在您设置 landing zone 时默认配置的。

限制对内容的访问

作为最佳实践，您应限制对适当的用户子集的访问。借助 AWS Control Tower，您可以确保您的中央云管理员和最终用户拥有正确的 IAM 权限，或者对于 IAM Identity Center 用户，确保他们属于正确的群组。

- 有关 IAM 实体角色和策略的更多信息，请参阅 IAM 用户指南。
- 有关在设置 landing zone 时创建的 IAM Identity Center 群组的更多信息，请参阅适用于 AWS Control Tower 的 IAM 身份中心群组。

AWS Control Tower 的合规性验证

AWS Control Tower 是一项架构完善的服务，可通过控制和最佳实践帮助您的组织满足您的合规需求。此外，作为多个合规计划的一部分，第三方审计师还会评估您可以在着陆区中使用的许多服务的安全 AWS 性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规计划范围内的 AWS 服务列表，请参阅按合规计划划分的范围内的AWS 服务。有关一般信息，请参阅 AWS 合规性计划。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅《AWS Artifact 用户指南》中的“在 A AWS rtifact 中下载报告”。

您在使用 AWS Control Tower 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在上部署以安全性和合规性为重点的基准环境的步骤。 AWS
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规性 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 标准的应用程序。
- AWS 合规资源 — 此工作簿和指南集可能适用于您所在的行业和所在地。
- AWS Config— 该 AWS 服务评估您的资源配置在多大程度上符合内部实践、行业指导方针和法规。
- AWS Security Hub— 此 AWS 服务可全面了解您的安全状态 AWS ，帮助您检查是否符合安全行业标准和最佳实践。

AWS Control Tower 中的弹性

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。

AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接起来。利用可用区，您可以设计和运行在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础架构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS Con AWS 区域 trol Tower 可用区域的列表，请参阅AWS 区域如何与 AWS Control Tower 配合使用。

您的家乡区域被定义为设置着陆区的区域。 AWS

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

AWS Control Tower 中的基础设施安全

AWS Control Tower 受亚马逊网络服务：安全流程概述白皮书中描述的 AWS 全球网络安全程序的保护。

您可以使用 AWS 已发布的 API 调用通过网络访问您的 landing zone 内的 AWS 服务和资源。我们需要传输层安全 (TLS) 1.2，建议使用传输层安全 (TLS) 1.3 或更高版本。客户端还必须支持具有完全向前保密（PFS）的密码套件，例如 Ephemeral Diffie-Hellman（DHE）或 Elliptic Curve Ephemeral Diffie-Hellman（ECDHE）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

您可以设置安全组，为您的 AWS Control Tower 着陆区工作负载提供额外的网络基础设施安全。有关更多信息，请参阅 演练：使用 AWS Firewall Manager 在 AWS Control Tower 中设置安全组。

在 AWS Control Tower 中进行日志记录和监控

通过监控，您可以对潜在事件进行规划和响应。监控活动的结果存储在日志文件中。因此，日志和监控是密切相关的概念，它们是 AWS Control Tower 架构完善的重要组成部分。

设置 landing zone 时，创建的共享账户之一就是日志存档账户。它专门用于集中收集所有日志，包括所有共享账户和成员账户的日志。日志文件存储在 Amazon S3 存储桶中。通过这些日志文件，管理员和审核员可查看已发生的操作和事件。

作为最佳实践，您应该将 AWS 设置中所有部分的监控数据收集到日志中，以便在出现多点故障时可以更轻松地进行调试。 AWS 提供了多种用于监控您在 landing zone 中的资源和活动的工具。

例如，您的控件状态会受到持续监控。您可以在 AWS Control Tower 控制台中一目了然地查看它们的状态，也可以通过 AWS Contro l Tower API 以编程方式查看它们的状态。您在 Account Factory 中配置的账户的运行状况和状态也会受到持续监控。

从 “活动” 页面查看记录的操作

在 AWS Control Tower 控制台中，活动页面概述了 AWS Control Tower 管理账户的操作。要导航到 AWS Control Tower 活动页面，请从左侧导航栏中选择 “活动”。

活动页面中显示的活动与 AWS Control Tower AWS CloudTrail 事件日志中报告的活动相同，但它们以表格形式显示。要了解有关特定活动的更多信息，请从表中选择该活动，然后选择查看详细信息。

您可以在日志存档文件中查看成员账户的操作和事件。

以下各节详细介绍了 AWS Control Tower 中的监控和日志记录：

主题

关于登录 AWS Control Tower

AWS Control Tower 通过与和的集成自动完成操作 AWS CloudTrail 和事件的记录 AWS Config，并将它们记录在中 CloudWatch。所有操作都将被记录下来，包括来自 AWS Control Tower 管理账户和贵

组织成员账户的操作。管理账户的操作和事件可在控制台的 “活动” 页面上查看。您可以在日志存档文件中查看成员账户的操作和事件。

组织级别的跟踪

当你设置着陆区时，AWS Control Tower 会设置 CloudTrail 一条新的路线。它是组织级别的跟踪，这意味着它记录管理账户和组织中所有成员账户的所有事件。此功能依靠可信访问权限为管理账户授予在每个成员账户上创建跟踪的权限。

有关 AWS Control Tower 和 CloudTrail 组织跟踪的更多信息，请参阅为组织创建跟踪。

> **Note**
>
> 在登陆区版本 3.0 之前的 AWS Control Tower 版本中，AWS Control Tower 在每个账户中创建了成员账户跟踪。当你更新到 3.0 版本时，你的 CloudTrail 跟踪将变成组织跟踪。有关在轨迹之间移动的最佳实践，请参阅《CloudTrail 用户指南》中的更改轨迹的最佳实践。

当您向 AWS Control Tower 注册账户时，您的账户将受 AWS Control Tower 组织的 AWS CloudTrail 跟踪管理。如果您已在该账户中部署了 CloudTrail 跟踪，则可能会看到重复的费用，除非您在将该账户注册到 AWS Control Tower 之前删除该账户的现有跟踪。

> **Note**
>
> 当您更新到着陆区版本 3.0 时，AWS Control Tower 会代表您删除您注册账户中的账户级跟踪（AWS Control Tower 已创建）。您现有的账户级日志文件将保留在其 Amazon S3 存储桶中。

审计账户中的 Amazon S3 存储桶策略

在 AWS Control Tower 中，只有当请求来自您的组织或组织单位 (OU) 时， AWS 服务才能访问您的资源。任何写入权限都必须满足一个`aws:SourceOrgID`条件。

您可以在 Amazon S3 存储桶策略的条件元素中使用条件键并将该值设置为您的组织 ID。`aws:SourceOrgID`此条件可确保 CloudTrail 只有代表组织内的账户才能将日志写入您的 S3 存储桶；它可以防止组织外部的 CloudTrail 日志写入您的 AWS Control Tower S3 存储桶。

此政策不会影响您现有工作负载的功能。该策略如以下示例所示。

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
            Condition:
              Bool:
                aws:SecureTransport: false
          - Sid: AWSBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSBucketDeliveryForConfig
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - Fn::Join:
```

```
                  - ""
                  -
                    - !Sub "arn:${AWS::Partition}:s3:::"
                    - !Ref "S3AuditBucket"
                    - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
              Condition:
                StringEquals:
                  aws:SourceOrgID: !Ref OrganizationId
            - Sid: AWSBucketDeliveryForOrganizationTrail
              Effect: Allow
              Principal:
                Service:
                  - cloudtrail.amazonaws.com
              Action: s3:PutObject
              Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                  [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                  !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
              Condition:
                StringEquals:
              aws:SourceOrgID: !Ref OrganizationId
```

有关此条件键的更多信息，请参阅 IAM 文档和 IAM 博客文章，标题为 “对访问您的资源的 AWS 服务使用可扩展的控制”。

用于监控的集成工具

监控是维护 AWS Control Tower 和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。AWS 提供了以下监控工具，用于监视 AWS Control Tower，在出现问题时进行报告，并在适当时自动采取措施：

- Amazon 会实时 CloudWatch监控您的 AWS 资源和您运行 AWS 的应用程序。您可以收集和跟踪指标，创建自定义的控制平面，以及 设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon CloudWatch Events 提供近乎实时的系统事件流，这些事件描述了 AWS 资源的变化。CloudWatch 事件支持事件驱动的自动计算，因为您可以编写规则来监视某些事件，并在这些事件发生时在其他 AWS 服务中触发自动操作。有关更多信息，请参阅 Amazon Ev CloudWatch ents 用户指南。

- Amazon CloudWatch Logs 允许您监控、存储和访问来自 Amazon EC2 实例和其他来源的日志文件。 CloudTrail CloudWatch 日志可以监视日志文件中的信息，并在达到特定阈值时通知您。您还可以在高持久性存储中检索您的日志数据。有关更多信息，请参阅 Amazon CloudWatch 日志用户指南。
- AWS CloudTrail捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。

提示：您可以通过 “日志和 CloudWatch CloudWatch 日志见解” 查看和查询账户 CloudTrail 的活动。本活动包括 AWS Control Tower 生命周期事件。 CloudWatch日志的功能使您可以执行比平时更精确、更精确的查询。 CloudTrail

有关更多信息，请参阅 使用记录 AWS Control Tower 操作 AWS CloudTrail。

使用记录 AWS Control Tower 操作 AWS CloudTrail

AWS Control Tower 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 AWS Control Tower 中执行的操作的记录。 CloudTrail 将 AWS Control Tower 的操作捕获为事件。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 AWS Control Tower 的事件。

如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。通过收集的信息 CloudTrail，您可以确定向 AWS Control Tower 发出的请求、发出请求的 IP 地址、谁提出了请求、何时提出请求以及其他详细信息。

要了解更多信息 CloudTrail，包括如何配置和启用它，请参阅《AWS CloudTrail 用户指南》。

AWS Control Tower 中的信息 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 AWS Control Tower 中出现支持的事件活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

> **Note**
>
> 在着陆区版本 3.0 之前的 AWS Control Tower 版本中，AWS Control Tower 创建了成员账户跟踪。当您更新到 3.0 版本时，您的 CloudTrail 跟踪将更新为组织跟踪。有关在跟踪之间移动的最佳实践，请参阅《 CloudTrail 用户指南》中的创建组织跟踪。

推荐：创建跟踪

要持续记录您的 AWS 账户中的事件，包括 AWS Control Tower 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析 CloudTrail 日志中收集的事件数据并对其采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- 为创建跟踪做准备
- 管理 CloudTrail 成本
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail日志文件

AWS Control Tower 将以下操作作为事件 CloudTrail 记录在日志文件中：

公共 API

- `DisableControl`
- `EnableControl`
- `GetControlOperation`
- `ListEnabledControls`

其他 API

- `SetupLandingZone`
- `UpdateAccountFactoryConfig`

- ManageOrganizationalUnit
- CreateManagedAccount
- EnableGuardrail
- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService
- GetAvailableUpdates

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。

- 请求是否由其他 AWS 服务发出。
- 请求是因访问被拒绝而被拒绝还是成功处理。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

示例：AWS Control Tower 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 事件在日志文件中不按任何特定顺序出现。

以下示例显示了一个 CloudTrail 日志条目，该条目显示了 SetupLandingZone AWS Control Tower 事件的典型日志文件条目的结构，包括发起该操作的用户的身份记录。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE;:assumed-role/AWSControlTowerTestAdmin/backend-
test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
```

```
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```

使用监控资源变化 AWS Config

AWS C AWS Config ontrol Tower 启用所有注册账户，因此它可以通过侦探控制来监控合规性、记录资源变化并将资源变更日志传送到日志存档账户。

如果您的 landing zone 版本低于 3.0：对于您注册的账户， AWS Config 记录账户运营所在的所有地区的资源的所有更改。每项更改都建模为配置项目 (CI)，其中包含资源标识符、区域、记录每项更改的日期以及更改是与已知资源还是新发现的资源相关等信息。

如果您的着陆区域版本为 3.0 或更高版本：AWS Control Tower 将全球资源（例如 IAM 用户、群组、角色和客户托管策略）的记录仅限于您的主区域。并非每个区域都存储全球资源变更的副本。资源记录的这种限制符合 AWS Config 最佳实践。全球资源的完整列表可在 AWS Config 文档中找到。

- 要了解更多信息 AWS Config，请参阅AWS Config 工作原理。
- 有关 AWS Config 可以支持的资源列表，请参阅支持的资源类型。
- 要了解如何在 AWS Control Tower 环境中自定义资源跟踪，请参阅标题为 “在 AWS Cont rol Tower 中自定义 AWS Config 资源跟踪” 的博客文章。

AWS Control Tower 在所有注册账户中设置了 AWS Config 配送渠道。通过此传送渠道，它会记录日志存档账户 AWS Config 中记录的所有更改，这些更改存储在亚马逊简单存储服务存储桶中的文件夹中。

在 AWS Control Tower 中管理 AWS Config 成本

本节介绍如何 AWS Config 记录您的 AWS Control Tower 账户中的资源变更并向您开具账单。这些信息可以帮助您了解在使用 AWS Control Tower 时如何管理与 AWS Config之相关的成本。AWS Control Tower 不会增加任何额外费用。

> **Note**
>
> 如果您的着陆区域版本为 3.0 或更高版本：AWS Control Tower 将全球资源（例如 IAM 用户、群组、角色和客户管理的策略）的 AWS Config 记录仅限于您的主区域。因此，本节中的某些信息可能不适用于您的着陆区。

AWS Config 旨在将账户运营所在的每个区域中每项资源的每项更改记录为配置项目 (CI)。 AWS Config 根据它生成的每个配置项目向您开具账单。

如何 AWS Config 运作

AWS Config 分别记录每个区域的资源。某些全球资源（例如 IAM 角色）在每个区域记录一次。例如，如果您在五个区域运营的注册账户中创建了一个新的 IAM 角色，则 AWS Config 会生成五个 CI，每个区域一个 CI。其他全球资源（例如 Route 53 托管区域）在所有区域中仅记录一次。例如，如果您在注册的账户中创建了一个新的 Route 53 托管区域，则无论为该账户选择了多少个区域，都会 AWS Config 生成一个 CI。有关可帮助您区分这些类型的资源的列表，请参阅同一资源会被记录多次。

> **Note**
>
> 当 AWS Control Tower 与之合作时 AWS Config，一个区域可能受 AWS Control Tower 管辖，也可以不受管辖，如果账户在该区域运营，则 AWS Config 仍会记录更改。

AWS Config 检测资源中的两种关系

AWS Config 区分了资源之间的直接关系和间接关系。如果资源在其他资源的 Describe AP I 调用中返回，则这些资源将记录为直接关系。当您更改与另一种资源有直接关系的资源时， AWS Config 不会为这两个资源创建 CI。

例如，如果您创建了一个 Amazon EC2 实例，而 API 要求您创建网络接口，则 AWS Config 认为该 Amazon EC2 实例与网络接口有直接关系。因此，仅 AWS Config 生成一个 CI。

AWS Config 记录属于间接关系的资源关系的单独更改。例如，如果您创建一个安全组并添加属于安全组的关联 Amazon EC2 实例，则 AWS Config 会生成两个 CI。

有关直接关系和间接关系的更多信息，请参阅什么是与资源的直接关系和间接关系？

您可以在 AWS Config 文档中找到资源关系列表。

查看已注册账户的 AWS Config 记录器数据

AWS Config 已与集成， CloudWatch 因此您可以在控制面板中查看 AWS Config CI。有关更多信息，请参阅标题为 “AWS Config 支持 Amazon CloudWatch 指标” 的博客文章。

通过编程方式，要查看 AWS Config 数据，您可以使用 AWS CLI，也可以使用其他 AWS 工具。

查询特定资源上的 AWS Config 记录器数据

您可以使用 C AWS LI 来检索资源的最新更改列表。

资源历史记录命令：

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

要了解更多信息，请参阅的 API 文档get-config-history。

使用 Amazon 实现 AWS Config 数据可视化 QuickSight

您可以对整个组织中记录的资源进行 AWS Config 可视化和查询。有关更多信息，请参阅使用亚马逊 Athen QuickSight a 和亚马逊可视化 AWS Config 数据。

AWS Config 在 AWS Control Tower 中进行故障排除

本节提供有关您在使用 AWS Config AWS Control Tower 时可能遇到的一些问题的信息。

AWS Config 成本高

如果您的工作流包括频繁创建、更新或删除资源的流程，或者如果它处理大量资源，则该工作流可能会生成大量 CI。如果您在非生产账户中运行这些流程，请考虑取消注册该账户。您可能需要手动停用该帐户的 AWS Config 录制器。

> **Note**
>
> 取消账户注册后，AWS Control Tower 无法对该账户中的资源实施侦探控制或记录账户事件（例如 AWS Config 活动）。

有关更多信息，请参阅取消管理已注册账户。要了解如何停用 AWS Config 录制器，请参阅管理配置记录器。

同一资源会被记录多次

检查该资源是否为全局资源。对于 3.0 版之前的 AWS Control Tower 着陆区， AWS Config 可以为每个运营区域记录一次某些全球资源。 AWS Config 例如，如果 AWS Config 在八个区域上启用，则每个角色将被记录八次。

对于每个运营区域，以下资源 AWS Config 仅记录一次：

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

其他全球资源仅记录一次。以下是一些仅记录一次的资源示例：

- `AWS::Route53::HostedZone`
- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

AWS Config 没有记录资源

某些资源与其他资源存在依赖关系。这些关系可能是直接的，也可以是间接的。您可以在AWS Config 常见问题解答中找到已弃用的间接关系列表。

AWS Control Tower 中的生命周期事件

AWS Control Tower 记录的某些事件是生命周期事件。生命周期事件的目的是标记某些改变资源状态的 AWS Control Tower 操作的完成。生命周期事件适用于 AWS Control Tower 创建或管理的资源，例如组织单位 (OU)、账户和控制权。

AWS Control Tower 生命周期事件的特征

- 对于每个生命周期事件，事件日志均显示发端 Control Tower 操作是成功完成，还是失败。
- AWS CloudTrail 自动将每个生命周期事件记录为非 API AWS 服务事件。有关更多信息，请参阅《 AWS CloudTrail 用户指南》。
- 每个生命周期事件还会发送到亚马逊 EventBridge 和亚马逊 CloudWatch 活动服务。

AWS Control Tower 中的生命周期事件具有两个主要优势：

- 由于生命周期事件记录了 AWS Control Tower 操作的完成，因此您可以根据生命周期 CloudWatch 事件的状态创建可触发自动化工作流程后续步骤的 Amazon EventBridge 规则或 Amazon Events 规则。
- 日志提供了其他详细信息，以帮助管理员和审核员查看组织中的某些类型的活动。

生命周期事件的工作原理

AWS Control Tower 依靠多种服务来实施其操作。因此，只有在一系列操作完成后，才会记录每个生命周期事件。例如，当您在 OU 上启用控件时，AWS Control Tower 会启动一系列实现请求的子步骤。整个子步骤系列的最终结果将作为生命周期事件的状态记录在日志中。

- 如果每个基础子步骤都成功完成，则生命周期事件状态将记录为 Succeeded (已成功)。
- 如有任何基础子步骤未成功完成，则生命周期事件状态将记录为 Failed (已失败)。

每个生命周期事件都包含一个记录的时间戳，该时间戳显示 AWS Control Tower 操作的启动时间，以及另一个显示生命周期事件何时完成（标记成功或失败）的时间戳。

在 Control Tower 中查看生命周期事件

您可以从 AWS Control Tower 控制面板的 “活动” 页面查看生命周期事件。

- 要导航到 Activities (活动) 页面，请从左侧导航窗格中选择 Activities (活动)。

- 要获取有关特定事件的更多详细信息，请选择该事件，然后选择右上角的 View details (查看详细信息) 按钮。

有关如何将 AWS Control Tower 生命周期事件集成到您的工作流程中的更多信息，请参阅这篇博客文章《使用生命周期事件跟踪 AWS Control Tower 操作并触发自动工作流程》。

CreateManagedAccount 和 UpdateManagedAccount生命周期事件的预期行为

当您在 AWS Control Tower 中创建账户或注册账户时，这两个操作会调用相同的内部 API。如果在此过程中出现错误，则通常发生在账户创建但尚未完全配置之后。当您在错误发生后重试创建账户或尝试更新预配置产品时，AWS Control Tower 会看到该账户已经存在。

由于账户存在，AWS Control Tower 会在重试请求结束时记录`CreateManagedAccount`生命周期事件，而不是生命周期事件。`UpdateManagedAccount`由于该错误，您可能希望看到另一个`CreateManagedAccount`事件。但是，`UpdateManagedAccount`生命周期事件是预期和期望的行为。

如果您计划使用自动方法在 AWS Control Tower 中创建账户或将账户注册到 AWS Control Tower，请编程 Lambda 函数以查找UpdateManagedAccount生命周期事件和CreateManagedAccount生命周期事件。

生命周期事件名称

每个生命周期事件的命名使其与最初的 AWS Control Tower 操作相对应，该操作也由 AWS 记录 CloudTrail。因此，例如，由 AWS Control Tower 事件发起的生命周期`CreateManagedAccount` CloudTrail 事件被命名为`CreateManagedAccount`。

以下列表中的每个名称都是一条指向记录详细信息（JSON 格式）示例的链接。这些示例中显示的其他详细信息取自 Amazon CloudWatch 事件日志。

虽然 JSON 不支持注释，但为了便于解释，还是在示例中添加了一些注释。注释显示在示例的右侧，前面带有“//”。

在这些示例中，某些账户名称和组织名称被遮盖。`accountId` 始终是由 12 个数字组成的序列，在示例中已替换为“xxxxxxxxxxxx”。`organizationalUnitID` 是由字母和数字组成的唯一字符串。它的形式在示例中保留下来。

- `CreateManagedAccount`：该日志记录 AWS Control Tower 是否成功完成了使用账户工厂创建和配置新账户的所有操作。

- UpdateManagedAccount：该日志记录 AWS Control Tower 是否成功完成了更新与您之前使用账户工厂创建的账户关联的预配置产品的所有操作。
- EnableGuardrail：该日志记录 AWS Control Tower 是否成功完成了在 AWS Control Tower 创建的 OU 上启用控制的所有操作。
- DisableGuardrail：该日志记录 AWS Control Tower 是否成功完成了禁用 AWS Control Tower 创建的 OU 上的控件的所有操作。
- SetupLandingZone：日志记录 AWS Control Tower 是否成功完成了设置着陆区的所有操作。
- UpdateLandingZone：日志记录 AWS Control Tower 是否成功完成了更新现有着陆区的所有操作。
- RegisterOrganizationalUnit：该日志记录了 AWS Control Tower 是否成功完成了在 OU 上启用其监管功能的所有操作。
- DeregisterOrganizationalUnit：该日志记录 AWS Control Tower 是否成功完成了在组织单位上禁用其监管功能的所有操作。
- PrecheckOrganizationalUnit：日志记录 AWS Control Tower 是否检测到任何会阻碍扩展管理操作成功完成的资源。

以下各节提供了 AWS Control Tower 生命周期事件的列表，以及每种生命周期事件记录的详细信息示例。

CreateManagedAccount

此生命周期事件记录 AWS Control Tower 是否使用账户工厂成功创建和配置了新账户。此事件与 AWS Control Tower CreateManagedAccount CloudTrail 事件相对应。该生命周期事件日志包含新创建账户的 accountName 和 accountId，以及账户所在 OU 的 organizationalUnitName 和 organizationalUnitId。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
```

```
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                    // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "CreateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "createManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"

                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully created a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

UpdateManagedAccount

此生命周期事件记录 AWS Control Tower 是否成功更新了与之前使用账户工厂创建的账户关联的预配置产品。此事件与 AWS Control Tower UpdateManagedAccount CloudTrail 事件相对应。该生命周期事件日志包含关联账户的 accountName 和 accountId，以及更新账户所在 OU 的 organizationalUnitName 和 organizationalUnitId。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // AWS Control Tower
 organization management account.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"624281831893"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully updated a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
```

```
    }
}
```

EnableGuardrail

此生命周期事件记录 AWS Control Tower 是否成功启用了对由 AWS Control Tower 管理的 OU 的控件。此事件与 AWS Control Tower EnableGuardrail CloudTrail 事件相对应。生命周期事件日志包括控件guardrailBehavior的guardrailId和，organizationalUnitName以及organizationalUnitId启用控件的 OU 的和。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",                                    // End-time of action.
 Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "us-east-1",                                             // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
```

```
                ],
                "guardrails": [
                  {
                    "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                    "guardrailBehavior": "DETECTIVE"
                  }
                ],
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully enabled a guardrail on an
 organizational unit.",
                "requestTimestamp": "2019-11-12T09:01:07+0000",
                "completedTimestamp": "2019-11-12T09:01:54+0000"
              }
        }
    }
}
```

DisableGuardrail

此生命周期事件记录 AWS Control Tower 是否成功禁用了由 AWS Control Tower 管理的 OU 上的控件。此事件与 AWS Control Tower DisableGuardrail CloudTrail 事件相对应。生命周期事件日志包括控件guardrailBehavior的guardrailId和，以及禁用控件的 OU 的organizationalUnitName和organizationalUnitId。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DisableGuardrail",
        "awsRegion": "us-east-1",
```

```
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "disableGuardrailStatus": {
                   "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully disabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
            }
        }
    }
```

SetupLandingZone

此生命周期事件记录 AWS Control Tower 是否成功设置了着陆区。此事件与 AWS Control Tower SetupLandingZone CloudTrail 事件相对应。生命周期事件日志包括rootOrganizationalId，这是 AWS Control Tower 通过管理账户创建的组织的 ID。日志条目还包括在 organizationalUnitName AWS Control Tower 设置着陆区时创建的每个 OU 的accountName和accountId，以及每个账户的和。organizationalUnitId

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
```

```
   "account": "XXXXXXXXXXXX",                                    // Management account
ID.
   "time": "2018-08-30T21:42:18Z",                                // Event time from
CloudTrail.
   "region": "us-east-1",                                         // Management account
CloudTrail region.
   "resources": [ ],
   "detail": {
       "eventVersion": "1.05",
       "userIdentity": {
           "accountId": "XXXXXXXXXXXX",                           // Management-account
ID.
           "invokedBy": "AWS Internal"
       },
       "eventTime": "2018-08-30T21:42:18Z",                       // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
       "eventSource": "controltower.amazonaws.com",
       "eventName": "SetupLandingZone",
       "awsRegion": "us-east-1",                                  // AWS Control Tower
home region.
       "sourceIPAddress": "AWS Internal",
       "userAgent": "AWS Internal",
       "eventID": "CloudTrail_event_ID",                          // This value is
generated by CloudTrail.
       "readOnly": false,
       "eventType": "AwsServiceEvent",
       "serviceEventDetails": {
           "setupLandingZoneStatus": {
               "state": "SUCCEEDED",                               // Status of entire
lifecycle operation.
               "message": "AWS Control Tower successfully set up a new landing zone.",

               "rootOrganizationalId" : "r-1234",
               "organizationalUnits" : [                           // Use a list.
                 {
                   "organizationalUnitName": "Security",             // Security OU
name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                 },
                 {
                   "organizationalUnitName": "Custom",           // Custom OU name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Custom OU ID.
                 },
               ],
```

```
               "accounts": [                                        // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

UpdateLandingZone

此生命周期事件记录 AWS Control Tower 是否成功更新了您的现有着陆区。此事件与 AWS Control Tower UpdateLandingZone CloudTrail 事件相对应。生命周期事件日志包括rootOrganizationalId，这是受 AWS Control Tower 管理的（已更新）组织的 ID。日志条目还包括每个 OU organizationalUnitId 的organizationalUnitName和，以及之前在 AWS Control Tower 最初设置着陆区时创建的每个账户的accountName和accountId。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
```

```
            "accountId": "XXXXXXXXXXXX",                          // Management account
ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateLandingZone",
        "awsRegion": "us-east-1",                                 // AWS Control Tower
home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                         // This value is
generated by CloudTrail.

        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateLandingZoneStatus": {
                "state": "SUCCEEDED",                             // Status of entire
operation.
                "message": "AWS Control Tower successfully updated a landing zone.",


                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                          // Use a list.
                  {
                    "organizationalUnitName": "Security",             // Security OU
name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",            // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                  },
                ],
               "accounts": [                                       // All created
accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
```

```
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXX"
                }
            ],
            "requestedTimestamp": "2018-08-30T21:42:18Z",
            "completedTimestamp": "2018-08-30T21:42:18Z"
        }
    }
}
```

RegisterOrganizationalUnit

此生命周期事件记录 AWS Control Tower 是否成功地在 OU 上启用了其监管功能。此事件与 AWS Control Tower `RegisterOrganizationalUnit` CloudTrail 事件相对应。生命周期事件日志包括 AWS C `organizationalUnitId` ontrol Tower 对其管理的 OU 的`organizationalUnitName`和。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "123456789012",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "RegisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
```

```
                "state": "SUCCEEDED",

                "message": "AWS Control Tower successfully registered an organizational
 unit.",

                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
                  }
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

DeregisterOrganizationalUnit

此生命周期事件记录 AWS Control Tower 是否成功禁用了 OU 上的监管功能。此事件与 AWS Control Tower `DeregisterOrganizationalUnit` CloudTrail 事件相对应。生命周期事件日志包括 AWS C `organizationalUnitId` ontrol Tower 已禁用其监管功能的 OU 的`organizationalUnitName`和。

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
```

```
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "deregisterOrganizationalUnitStatus": {
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully deregistered an
organizational unit, and enabled mandatory guardrails on the new organizational
unit.",
                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",                    // Foundational
OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"           // Foundational
OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
            }
        }
    }
```

PrecheckOrganizationalUnit

此生命周期事件记录 AWS Control Tower 是否成功对 OU 进行了预检查。此事件与 AWS Control Tower PrecheckOrganizationalUnit CloudTrail 事件相对应。生命周期事件日志包含、和failedPrechecks值字段 IdName，对应于 AWS Control Tower 在 OU 注册过程中对其执行预检查的每个资源。

事件日志还包含有关对其执行预检查的嵌套账户的信息，包括accountNameaccountId、和failedPrechecks字段。

如果该failedPrechecks值为空，则表示该资源的所有预检查均成功通过。

- 只有在预检查失败时才会发出此事件。
- 如果您注册的是空的 OU，则不会触发此事件。

事件示例：

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "precheckOrganizationalUnitStatus": {
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
            "SCP_CONFLICT"
          ]
      },
      "accounts": [
        {
          "accountName": "Child Account 1",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Child Account 2",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Management Account",
```

```
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
          ]
        },
        {
          "accountName": "Child Account 3",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": []
        },
        ...
      ],
      "state": "FAILED",
      "message": "AWS Control Tower failed to register an organizational unit due to
 pre-check failures. Go to the OU details page to download a list of failed pre-checks
 for the OU and accounts within.",
      "requestedTimestamp": "2021-09-20T22:44:02+0000",
      "completedTimestamp": "2021-09-20T22:45:43+0000"
    }
  },
  "eventCategory": "Management"
}
```

将 AWS 用户通知与 AWS Control Tower

您可以使用AWS 用户通知来设置发送渠道以接收有关 AWS Control Tower 事件的通知。当事件与指定的规则匹配时，会收到通知。您可以通过多种渠道接收事件通知，包括电子邮件、AWS Chatbot聊天通知或 Cons AWS ole Mobile App 推送通知。还可以在控制台通知中心中查看通知。

AWS 用户通知支持聚合，这可以减少您在特定事件期间收到的通知数量。通知也可以在控制台通知中心中看到。

通过用户通知而不是通过 AWS 用户通知订阅通知的好处 EventBridge 包括：

- 更友好的用户界面 (UI)。
- 与 AWS 控制台集成，在全局导航栏的铃声/通知区域中。
- 原生支持电子邮件通知，无需设置 Amazon SNS。
- 最值得注意的是，支持移动推送通知，仅限于 AWS 用户通知。

例如，您可能希望收到的一种通知是在 Security Hub 发现严重和严重性高的情况下。JSON 中用于设置该通知订阅的代码片段可能如下所示：

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

事件过滤

- 您可以使用 AWS 用户通知控制台上提供的过滤器按服务和名称筛选事件。
- 如果您根据 JSON 代码创建自己的 EventBridge 过滤器，则可以按特定属性筛选事件。

示例 AWS Control Tower 事件

以下是的通用示例事件。 AWS Control Tower

- 这是个 EventBridge 事件。
- 您可以使用 AWS 用户通知订阅 EventBridge 事件（例如此事件）。

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
```

```
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "<event name>", // one of the 9 event names in https://
docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
        "awsRegion": "<region>",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "<id>",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            // the contents of this object vary depending on the event subtype and
 event state
        }
    }
}
```

演练

本章包含可帮助您使用 AWS Control Tower 的演练程序。

主题

演练：从 ALZ 移动到 AWS Control Tower

许多 AWS 客户已采用 AWS 着陆区解决方案 (ALZ) 来设置安全、合规的多账户环境 AWS 。为了减轻管理着陆区的负担， AWS 创建了名为 AWS Control Tower 的托管服务。

ALZ 没有计划提供其他功能；它仅提供长期支持。因此，我们建议您从 ALZ 迁移到 AWS Control Tower 服务。本章中链接的博客将引导您了解该迁移的不同注意事项，并说明了如何规划从 ALZ 成功迁移到 AWS Control Tower。

博客：将 AWS 着陆区解决方案迁移到 AWS Control Tower

AWS 规范性指南提供了更广泛的文档，包括从 ALZ 过渡到 AWS Control Tower 的步骤。从本质上讲，您将在运行 ALZ 的现有组织中启用 AWS Control Tower 治理，前提是许多先决条件。有关信息，请参阅从 AWS 着陆区过渡到 AWS Control Tower。

演练：通过 Service Catalog API 在 AWS Control Tower 中自动配置账户

AWS Control Tower 与其他几项 AWS 服务集成，例如 AWS Service Catalog。您可以使用这些 API 在 AWS Control Tower 中创建和配置您的成员账户。

该视频向您展示了如何通过调用 AWS Service Catalog API 以自动化的批量方式配置账户。要进行配置，您需要从 AWS 命令行界面 (CLI) 调用 `ProvisionProduct`API，然后指定一个 JSON 文件，其

中包含您要设置的每个账户的参数。该视频说明了如何安装和使用 AWS Cloud9 开发环境来执行这项工作。如果你使用 Clouds AWS hell 而不是 Cloud AWS 9，CLI 命令将是一样的。

> **Note**
>
> 您还可以通过为每个账户调用的 `UpdateProvisionedProduct`API 来调整这种方法 AWS Service Catalog 以实现账户自动更新。您可以编写一个脚本来逐个更新账户。

作为一种完全不同的自动化方法，如果你熟悉 Terraform，你可以使用 AWS Control Tower Account Factory for Terraform (AFT) 配置账户。

自动化管理角色示例

以下示例模板可用于帮助您在管理账户中配置自动化管理角色。你需要在管理账户中配置这个角色，这样它就可以在目标账户中使用管理员访问权限执行自动化。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
```

```
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

自动化执行角色示例

以下是一个示例模板，可帮助您设置自动化执行角色。您将在目标账户中配置此角色。

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
  SessionDurationInSecs:
    Type: "Number"
    Description: "Maximum session duration in seconds."
    Default: 14400

Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
```

```
      Path: "/"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

配置这些角色后，您可以调用 AWS Service Catalog API 来执行自动任务。视频中给出了 CLI 命令。

Service Catalog API 的配置输入示例

以下是您在使用 Service Catalog `ProvisionProduct` API 预配置 AWS Control Tower 账户时可以向该服务目录 API 提供的输入示例：

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
    {
      key: "AccountName",
      value: "ABC"
    },
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
    },
    {
      key: "SSOUserFirstName",
      value: "John"
    },
    {
      key: "SSOUserLastName",
      value: "Smith"
    }
  ],
  provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
```

```
}
```

有关更多信息，请参阅 S ervice Catalog 的 API 参考。

> **Note**
>
> 请注意，值的输入字符串的格式`ManagedOrganizationalUnit`已从变`OU_NAME`为`OU_NAME (OU_ID)`。接下来的视频没有提及这一变化。

视频演练

此视频 (6:58) 介绍了如何在 AWS Control Tower 中自动部署账户。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

AWS Control Tower 中自动配置账户的视频演练。

演练：在没有 VPC 的情况下配置 AWS Control Tower

本主题介绍如何在没有 VPC 的情况下配置您的 AWS Control Tower 账户。

如果您的工作负载不需要 VPC，可以执行以下操作：

- 您可以删除 AWS Control Tower 虚拟私有云 (VPC)。此 VPC 是在您设置登录区域时创建的。
- 您可以更改您的 Account Factory 设置，以便在没有关联 VPC 的情况下创建新的 AWS Control Tower 账户。

> **Important**
>
> 如果您在启用 VPC 互联网访问设置的情况下配置 Account Factor y 账户，则该 Account Factory 设置将覆盖 “禁止客户管理的 Amazon VPC 实例访问互联网” 控件。要避免为新配置的账户启用互联网接入，您必须在 Account Factory 中更改设置。

删除 AWS Control Tower VPC

在 AWS Control Tower 之外，每位 AWS 客户都有一个默认 VPC，您可以在亚马逊虚拟私有云（亚马逊 VPC）控制台上查看，网址为 https://console.aws.amazon.com/vpc/。您可以识别出默认 VPC，因为其名称的末尾位置总是包含（默认值）字样。

在您设置 AWS Control Tower 着陆区时，AWS Control Tower 会删除您的 AWS 默认 VPC 并创建一个新的 AWS 控制塔默认 VPC。新的 VPC 已与您的 AWS Control Tower 管理账户关联。本主题将新的 VPC 称为 Cont rol Tower VPC。

当您在亚马逊 VPC 控制台中查看 AWS Control Tower VPC 时，名称末尾不会看到（默认）字样。如果您有多个 VPC，则必须使用分配的 CIDR 范围来识别正确的 AWS Control Tower VPC。

您可以删除 AWS Control Tower VPC，但是如果您以后需要在 AWS Control Tower 中建一个 VPC，则必须自己创建。

删除 AWS Control Tower VPC

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 在 Service Catalog 选项中搜索**VPC**或选择 VPC。然后，您可以看到 VPC 控制面板。
3. 从左侧的菜单中，选择 Your VPCs (您的 VPC)。然后，您可以看到您的所有 VPC。
4. 通过 CIDR 范围识别 AWS Control Tower VPC。
5. 要删除 VPC，请选择 Actions (操作)，然后选择 Delete VPC (删除 VPC)。

AWS Control Tower 管理账户的每个区域中都已存在一个 AWS （默认）VPC。为了遵循最佳安全实践，如果您选择删除 AWS Control Tower VPC，最好同时从所有 AWS 区域中删除与该管理账户关联的 AWS 默认 VPC。因此，为了保护管理账户的安全，请从每个区域移除默认 VPC，并移除 Control Tower 在您的 AWS Control Tower 主区域中创建的 VPC。

在没有 VPC 的 AWS Control Tower 中创建账户

如果您的最终用户工作负载不需要 VPC，则可以使用此方法来设置未自动为其创建 VPC 的最终用户帐户。

在 AWS Control Tower 控制面板中，您可以查看和编辑您的网络配置设置。在您更改设置以便在没有关联 VPC 的情况下创建 AWS Control Tower 账户后，所有新账户都是在没有 VPC 的情况下创建的，直到您再次更改设置为止。

配置 Account Factory 以创建没有 VPC 的账户

1. 打开网络浏览器，然后导航到 AWS Control Tower 控制台，网址为 https://console.aws.amazon.com/controltower。
2. 从左侧菜单中选择 Ac count Fac tory。
3. 然后，您将看到带有网络配置部分的 Account Factory 页面。
4. 请记录当前设置（如果您打算以后恢复设置的话）。
5. 在 “网络配置” 部分中选择 “编辑” 按钮。
6. 在 Edit account factory network configuration (编辑账户工厂网络配置) 页面中，转到 VPC Configuration options for new accounts (新账户的 VPC 配置选项) 部分。

   您可以按照选项 1 或选项 2 或两者兼而有之，确保 AWS Control Tower 在配置账户时不会创建 VPC。

   a. 选项 1-移除子网

      - 关闭 Internet-accessible subnet (可访问 Internet 的子网) 切换开关。
      - 将 Maximum number of private subnets (最大私有子网数) 值设置为 0。

   b. 选项 2-移除 AWS 区域

      - 清除 Regions for VPC creation (VPC 创建区域) 列中的每个复选框。
7. 选择保存。

可能的错误

请注意，当您删除 AWS Control Tower VPC 或重新配置 Account Factory 以创建没有 VPC 的账户时，可能会出现这些错误。

- 您的现有管理账户可能在 AWS Control Tower VPC 中存在依赖关系或资源，这可能会导致删除失败错误。
- 如果您在设置时保留默认 CIDR，以便启动不含 VPC 的新账户，则您的请求将失败并出现 the CIDR is not valid (该 CIDR 无效) 错误。

演练：使用 AWS Firewall Manager 在 AWS Control Tower 中设置安全组

该视频向您展示了如何使用 Fi AWS rewall Manager 服务来改进 AWS Control Tower 的网络安全。可以指定已启用的安全管理员账户来设置安全组。您将了解如何为 AWS Control Tower 组织配置安全策略和强制执行安全规则，以及如何通过自动应用策略来修复不合规的资源。您可以查看组织中每个账户和资源（例如 Amazon EC2 实例）有效的安全组。

可以创建自己的防火墙策略，也可以从受信任的供应商处订阅规则。

使用 Fi AWS rewall Manager 设置安全组

此视频 (8:02) 介绍如何在 AWS Control Tower 中为您的资源和工作负载设置更好的网络基础设施安全性。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

在 AWS Control Tower 中设置防火墙的视频演练。

有关更多信息，请参阅有关如何设置 AWS WAF 的文档。

演练：停用 AWS Control Tower 着陆区

AWS Control Tower 允许您设置和管理安全的多账户 AWS 环境，即着陆区。清理 AWS Control Tower 分配的所有资源的过程称为停用着陆区。

如果您不想再使用 AWS Control Tower，则自动停用工具会清理 AWS Control Tower 分配的资源。要开始自动停用流程，请导航至 “着陆区设置” 页面，选择 “停用” 选项卡，然后选择 “停用” 着陆区。

有关停用期间执行的操作的列表，请参阅退役过程概述。

> **Warning**
>
> 手动删除您的所有 AWS Control Tower 资源与停用不同。它不允许你设置新的着陆区。

停用过程不会通过以下方式更改您的数据和现有 AWS Organizations 数据。

- AWS Control Tower 不会删除您的数据，它只会删除它创建的部分着陆区。
- 停用过程完成后，仍有一些资源项目，例如 Amazon S3 存储桶和 Amazon Lo CloudWatch gs 日志组。在设置另一个登录区之前，必须手动删除这些资源，以避免产生与维护某些资源相关的可能成本。

- 您无法使用自动停用功能来删除部分设置的登录区。如果登录区设置过程失败，则必须解析故障状态并将其设置为可以自动停用，或者必须手动逐个删除资源。

停用登录区是一个具有重大后果的过程且无法撤消。以下各节将介绍 AWS Control Tower 采取的停用操作以及停用后剩余的工件。

> **Important**
>
> 我们强烈建议您仅在打算停止使用登录区时才执行此停用过程。在您停用现有的登录区后，无法重新创建此登录区。

退役过程概述

当您请求停用您的着陆区时，AWS Control Tower 会执行以下操作。

- 禁用 landing zone 中启用的每个侦探控件。AWS Control Tower 会删除支持该控件的 AWS CloudFormation 资源。
- 通过从中删除服务控制策略 (SCP) 来禁用每项预防性控制。 AWS Organizations如果策略为空（应该在移除 AWS Control Tower 管理的所有 SCP 之后该策略为空），则 AWS Control Tower 会分离并完全删除该策略。
- 删除所有部署为 AWS CloudFormation StackSets的蓝图。
- 删除所有区域中作为 CloudFormation 堆栈部署的所有蓝图。
- 对于每个已配置的账户，AWS Control Tower 会在停用过程中执行以下操作。
  - 删除每个账户工厂账户的记录。
  - 通过移除 AWS Control Tower 创建的 IAM 角色（除非已向其添加了其他策略）来撤销账户的 AWS Control Tower 权限，然后重新创建标准 `OrganizationsFullAccessRole` IAM 角色。
  - 从中删除该账户的记录 AWS Service Catalog。
  - 从 AWS Service Catalog中删除账户工厂产品和产品组合。
- 删除共享（审计和日志存档）账户的蓝图。
- 通过移除 AWS Control Tower 创建的 IAM 角色（除非已向其添加了其他策略），撤消共享账户的 AWS Control Tower 权限，然后重新创建 `OrganizationsFullAccessRole` IAM 角色。
- 删除与共享账户相关的记录。
- 删除与客户创建的 OU 相关的记录。

- 删除标识主区域的内部记录。

> **Note**
>
> 停用后，如果您的 VPC 不为空，您可能希望删除账户工厂 VPC 蓝图 (BP_ACCOUNT_FACTORY_VPC) 以清理路由和 NAT 网关。

停用期间未移除资源

停用着陆区并不能完全逆转 AWS Control Tower 的设置过程。某些资源仍然存在，可以手动将其删除。

AWS Organizations

对于没有现有 AWS Organizations 组织的客户，AWS Control Tower 会建立一个由两个组织单位 (OU) 组成的组织，分别命名为安全和沙盒。当您停用登录区时，将保留组织的层次结构，如下所示：

- 您通过 AWS Control Tower 控制台创建的组织单位 (OU) 不会被删除。
- 未移除安全 OU 和沙盒 OU。
- 该组织未从中删除 AWS Organizations。
- 中的任何帐户 AWS Organizations （共享、已配置或管理）都不会被移动或删除。

AWS IAM Identity Center (SSO)

对于没有现有 IAM 身份中心目录的客户，AWS Control Tower 会设置 IAM 身份中心并配置初始目录。当您停用着陆区时，AWS Control Tower 不会对 IAM 身份中心进行任何更改。如果需要，您可以手动删除存储在您的管理账户中的 IAM 身份中心信息。特别是，停用不更改以下这些方面：

- 不会删除使用账户工厂创建的用户。
- 由 AWS Control Tower 设置创建的群组不会被删除。
- AWS Control Tower 创建的权限集不会被删除。
- AWS 账户与 IAM 身份中心权限集之间的关联不会被删除。
- IAM 身份中心目录未更改。

角色

在设置过程中，如果您使用控制台，AWS Control Tower 会为您创建某些角色；如果您通过 API 设置着陆区，AWS Control Tower 会要求您创建这些角色。当你停用 landing zone 时，以下角色不会被移除：

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Amazon S3 存储桶

在设置过程中，AWS Control Tower 会在日志账户中创建用于记录和访问日志的存储桶。当您停用登录区时，不会删除以下资源：

- 不会删除日志记录账户中的日志记录和日志记录访问 S3 存储桶。
- 不会删除日志记录和日志记录访问存储桶的内容。

共享账户

在 AWS Control Tower 设置期间，在安全 OU 中创建了两个共享账户（审计和日志存档）。当您停用登录区时：

- 在 AWS Control Tower 设置期间创建的共享账户不会关闭。
- 重新创建 `OrganizationAccountAccessRole` IAM 角色以符合标准 AWS Organizations 配置。
- 删除 `AWSControlTowerExecution` 角色。

预配置账户

AWS Control Tower 客户可以使用账户工厂创建新的 AWS 账户。当您停用登录区时：

- 不会关闭您使用账户工厂创建的预配置账户。
- 中的预配置产品不会 AWS Service Catalog 被移除。如果你通过终止它们来清理它们，他们的账户就会被移到根 OU。
- AWS Control Tower 创建的 VPC 不会被移除，关联的 AWS CloudFormation 堆栈集 (`BP_ACCOUNT_FACTORY_VPC`) 也不会被移除。

- 重新创建 OrganizationAccountAccessRole IAM 角色以符合标准 AWS Organizations 配置。
- 删除 AWSControlTowerExecution 角色。

CloudWatch 日志日志组

作为名为的蓝图的一部分aws-controltower/CloudTrailLogs，创建了一个 CloudWatch 日志日志组AWSControlTowerBP-BASELINE-CLOUDTRAIL-MANAGEMENT。不会删除此日志组。相反，将删除蓝图并保留资源。

- 在设置其他登录区之前，必须手动删除此日志组。

> **Note**
>
> landing zone 3.0 及更高版本的客户无需删除其个人注册账户的 CloudTrail CloudTrail 日志和日志角色，因为这些角色仅在管理账户中为组织级别的跟踪创建。
> 从着陆区版本 3.2 开始，AWS Control Tower 创建了一条名为的亚马逊 EventBridge 规则AWSControlTowerManagedRule。此规则是在所有受管辖区域的每个成员账户中创建的。在停用期间，该规则不会自动删除，因此您必须先从所有受管辖区域的共享账户和成员账户中手动将其删除，然后才能在新区域中设置着陆区。

中给出了如何删除 AWS Control Tower 资源的程序管理 AWS Control Tower 资源。

管理 AWS Control Tower 资源

本文档提供了有关如何在日常维护和管理任务中单独删除 AWS Control Tower 资源的说明。本章中给出的程序仅用于在需要时移除单个资源或少量资源。这与停用你的着陆区不同。

有两种类型的任务可能需要您移除资源：

- 在常规情况下管理登录区时删除资源。
- 清理自动停用后剩余的资源。

> **Warning**
>
> 手动移除资源将不允许您设置新的着陆区。这与退役不同。如果您打算停用 AWS Control Tower 着陆区，请在采取本章所述的任何操作演练：停用 AWS Control Tower 着陆区之前按照

中的说明进行操作。本章中的说明可以帮助您清理自动停用完成后剩余的资源。即使您手动删除了所有着陆区资源，也与停用着陆区不同，并且可能会产生意想不到的费用。

如果您需要从 AWS Control Tower 中移除账户，请参阅以下章节来关闭账户：

- 取消账户管理
- 关闭在 Account Factory 中创建的账户

我需要停用而不是删除吗？

如果您不再打算在企业中使用 AWS Control Tower，或者需要重新部署组织资源，则可能需要停用最初设置着陆区时创建的资源。

- 停用过程完成后，仍有一些资源项目，例如 Amazon S3 存储桶和 Amazon Lo CloudWatch gs 日志组。
- 在设置另一个 landing zone 之前，您必须手动清理账户中的剩余资源，以免产生意外费用。有关更多信息，请参阅停用期间未移除资源。

⚠ Warning

我们强烈建议您仅在打算停止使用着陆区时才执行退役流程。此过程无法撤消。

关于移除 AWS Control Tower 资源

本章中的各个步骤将指导您完成移除 AWS Control Tower 资源的手动方法。当您需要从 landing zone 中删除特定资源时，可以按照以下步骤操作。

在执行这些程序之前，除非另有说明，否则您必须登录到着陆区域的主区域，并且必须以 IAM 用户或用户身份登录 IAM Identity Center，并拥有包含您的着陆区的管理账户的管理权限。 AWS Management Console

⚠ Warning

这些破坏性行为可能会给您的 AWS Control Tower 设置带来治理偏差。这些操作无法撤消。

主题

删除 SCP

AWS Control Tower 使用服务控制策略 (SCP) 进行控制。此过程介绍如何删除与 AWS Control Tower 特别相关的 SCP。

删除 S AWS Organizations CP

1. 通过以下网址打开 Organizations 控制台：https://console.aws.amazon.com/organizations/。
2. 打开 Policies (策略) 选项卡，找到前缀为 aws-guardrails- 的服务控制策略 (SCP) 并对每个 SCP 执行以下操作：
   a. 将 SCP 与关联的 OU 分离。
   b. 删除 SCP。

删除 StackSets 和堆叠

AWS Control Tower 使用 StackSets 和堆栈来部署 AWS Config 规则 与您的着陆区中的控件相关的控件。以下过程演练如何删除这些特定资源。

要删除 AWS CloudFormation StackSets

1. 打开 AWS CloudFormation 控制台，网址为 https://console.aws.amazon.com/cloudformation。
2. 从左侧导航菜单中选择StackSets。
3. 对于每个 StackSet 带有前缀的内容 AWSControlTower，请执行以下操作。如果您在 a 中有多个帐户 StackSet，则可能需要一些时间。
   a. StackSet 从仪表板的表格中选择具体的。这将打开其属性页面 StackSet。
   b. 在页面底部的堆栈表中，记录表格中所有 AWS 账户的账户 ID。复制所有账户的列表。

c. 在操作中，选择从中删除堆栈。 StackSet

d. 在设置部署选项上，从部署位置中选择在账户中部署堆栈。

e. 在文本字段中，输入您在步骤 3.b 中记录的 AWS 账户 ID，用逗号分隔。例如：*123456789012*、*098765431098* 等。

f. 从 Specify regions (指定区域) 中，选择 Add all (全部添加)，将页面上的其余参数保留其默认值，然后选择 Next (下一步)。

g. 在 Review (查看) 页面上，查看您的选择，然后选择 Delete stacks (删除堆栈)。

h. 在StackSet 属性页面上，您可以为其他人重新开始此过程 StackSets。

4. 当不同StackSets 属性页面的 Stacks 表中的记录为空时，该过程即告完成。

5. 当 “堆栈” 表中的记录为空时，选择 “删除 StackSet”。

删除 AWS CloudFormation 堆栈

1. 打开 AWS CloudFormation 控制台，网址为 https://console.aws.amazon.com/cloudformation。

2. 在堆栈控制面板中，搜索所有带有前缀的堆栈。AWSControlTower

3. 对于表中的每个堆栈，执行以下操作：

   a. 选中堆栈名称旁边的复选框。

   b. 从 Actions (操作) 菜单中选择 Delete Stack (删除堆栈)。

   c. 在打开的对话框中，查看相关信息以确保其准确，然后选择 Yes, Delete (是，删除)。

删除日志存档账户中的 Amazon S3 存储桶

以下过程将指导您完成如何以 IAM 身份中心用户身份登录日志存档账户，然后删除日志存档账户中的 Amazon S3 存储桶。AWSControlTowerExecution

使用适当权限登录日志存档账户

1. 通过以下网址打开 Organizations 控制台：https://console.aws.amazon.com/organizations/。

2. 从 Accounts (账户) 选项卡中，找到 Log archive (日志存档) 账户。

3. 从打开的右窗格中，记录日志存档账号。

4. 从导航栏中，选择您的账户名称以打开账户菜单。

5. 选择 Switch Role。

6. 在打开的页面上，提供 Account (账户) 中日志存档账户的账号。

7. 对于 “角色”，输入AWSControlTowerExecution。
8. 这将向 Display Name (显示名称) 填充文本。
9. 选择您喜爱的 Color (颜色)。
10. 选择 Switch Role。

删除 Amazon S3 存储桶

1. 打开 Amazon S3 控制台，网址为：https://console.aws.amazon.com/s3/。
2. 搜索包含 aws-controltower 的存储桶名称。
3. 对于表中的每个存储桶，执行以下操作：
   a. 选中表中存储桶的复选框。
   b. 选择 Delete （ 删除)。
   c. 在打开的对话框中，查看相应信息以确保其准确，输入存储桶名称以进行确认，然后选择 Confirm (确认)。

移除 Account Factory 产品组合和产品

以下过程将指导您完成如何在AWSServiceCatalogAdmins群组中以 IAM 身份中心用户身份登录，然后清理您的 Account Factory 产品组合和产品。

使用相应权限登录您的管理账户

1. 转到用户门户 URL，即 *directory-id*.awsapps.com/start
2. 在AWS 账户中，找到管理账户。
3. 从AWSServiceCatalogAdminFullAccess中选择管理控制台 AWS Management Console 以此角色登录。

清理 Account Factory

1. 通过以下网址打开 Service Catalog 控制台：https://console.aws.amazon.com/servicecatalog/。
2. 从左侧导航菜单中，选择 Portfolios list (产品组合列表)。
3. 在本地投资组合表中，搜索名为 Cont AWS rol Tower Account Factory Portfolio 的投资组合。
4. 选择该产品组合的名称以转至其详细信息页面。

5. 展开页面的 “约束” 部分，然后选择产品名称为 Cont AWS rol Tower Account Fac tory 的约束条件的单选按钮。
6. 选择 REMOVE CONSTRAINTS (删除约束)。
7. 在打开的对话框中，查看相应信息以确保其准确，然后选择 CONTINUE (继续)。
8. 从页面的 “产品” 部分，为名为 Cont AWS rol Tower Account Fac tory 的产品选择单选按钮。
9. 选择 REMOVE PRODUCT (删除产品)。
10. 在打开的对话框中，查看相应信息以确保其准确，然后选择 CONTINUE (继续)。
11. 展开页面的 Users, Groups, and Roles (用户、组和角色) 部分，并选中此表中所有记录的复选框。
12. 选择 REMOVE USERS, GROUP OR ROLE (删除用户、组或角色)。
13. 在打开的对话框中，查看相应信息以确保其准确，然后选择 CONTINUE (继续)。
14. 从左侧导航菜单中，选择 Portfolios list (产品组合列表)。
15. 在本地投资组合表中，搜索名为 Cont AWS rol Tower Account Factory Portfolio 的投资组合。
16. 选择该产品组合的单选按钮，然后选择 DELETE PORTFOLIO (删除产品组合)。
17. 在打开的对话框中，查看相应信息以确保其准确，然后选择 CONTINUE (继续)。
18. 从左侧导航菜单中，选择 Product list (产品列表)。
19. 在管理产品页面上，搜索名为 Cont AWS rol Tower Account Factory 的产品。
20. 选择产品以打开 Admin product details (管理产品详细信息) 页。
21. 从 Actions (操作) 中，选择 Delete product (删除产品)。
22. 在打开的对话框中，查看相应信息以确保其准确，然后选择 CONTINUE (继续)。

移除 AWS Control Tower 角色和策略

这些程序将引导您了解如何清理 AWS Control Tower 在设置您的着陆区时或之后创建的角色和策略。

删除 IAM 身份中心 AWSServiceCatalogEndUserAccess 角色

1. 打开 AWS IAM Identity Center 控制台，网址为 https://console.aws.amazon.com/singlesignon/。
2. 将您的 AWS 区域更改为您的主区域，即您最初设置 AWS Control Tower 的区域。
3. 从左侧导航菜单中选择 “AWS 帐户”。
4. 选择您的管理账户链接。
5. 选择 “权限集” 的下拉列表，选择 AWSServiceCatalogEndUserAccess，然后选择 “删除”。
6. 从左侧面板中选择AWS 账户。
7. 打开 Permission sets (权限集) 选项卡。

8. 选择AWSServiceCatalogEndUserAccess并删除它。

删除 IAM 角色

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 从左侧导航菜单中，选择 Roles (角色)。
3. 在表格中，搜索名称为的角色AWSControlTower。
4. 对于表中的每个角色，执行以下操作：
   a. 选中角色的复选框。
   b. 选择删除角色。
   c. 在打开的对话框中，查看相关信息以确保其准确，然后选择 Yes, delete (是，删除)。

删除 IAM 策略

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 从左侧导航菜单中，选择 Policies (策略)。
3. 从表中搜索名称为的策略AWSControlTower。
4. 对于表中的每个策略，执行以下操作：
   a. 选中策略的复选框。
   b. 选择 Policy actions (策略操作)，然后从下拉菜单中选择 Delete (删除)。
   c. 在打开的对话框中，查看相关信息以确保其准确，然后选择 Delete (删除)。

AWS Control Tower 资源帮助

如果您在移除 AWS Control Tower 资源时遇到任何无法解决的问题，请联系AWS 支持部门。

如何停用着陆区

要停用您的 AWS Control Tower 着陆区，请按照此处给出的步骤进行操作。

> **Note**
>
> 我们建议您在停用之前取消对已注册账户的管理。

1. 在 AWS C ontrol Tower 控制台中导航到着陆区域设置页面。
2. 在 “停用您的着陆区” 部分中选择 “停用您的着陆区”。
3. 此时将显示一个对话框，说明您将要执行的操作，并提供必要的确认流程。要确认您的停用意图，您必须选择每个框并按要求键入确认。

> **Important**
>
> 停用过程无法撤销。

4. 如果您确认打算停用您的着陆区，则在停用期间，您将被重定向到 AWS Control Tower 主页。该过程可能需要长达两个小时。
5. 成功停用后，您必须手动删除剩余资源，然后才能从 AWS Control Tower 控制台设置新的着陆区。这些剩余资源包括一些特定的 Amazon S3 存储桶、组织和 CloudWatch 日志组。

> **Note**
>
> 这些行为可能会对您的账单和合规活动产生重大影响。例如，未能删除这些资源可能会导致意外费用。

有关如何手动删除资源的更多信息，请参阅关于移除 AWS Control Tower 资源。

6. 如果您打算在新区域中设置新的着陆 AWS 区，请按照此额外步骤操作。通过 CLI 输入以下命令：

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

停用后需要手动执行清理任务

- 如果您在停用日志存档和审核帐户后创建新的登录区域，或者按照程序创建自己的现有日志存档或审核帐户，则必须为日志存档和审核帐户指定不同的电子邮件地址。
- 在设置另一个 landing zone 之前`aws-controltower/CloudTrailLogs`，必须手动删除 Log CloudWatch s 日志组。
- 必须手动移除或重命名两个带有日志保留名称的 Amazon S3 存储桶。
- 您必须手动删除或重命名现有的安全和沙盒组织单位。

> **Note**
>
> 在删除 AWS Control Tower Sec urity OU 组织之前，必须先删除日志和审计账户，但不能删除管理账户。要删除这些账户，您必须何时以 root 用户身份登录到审核账户和日志记录账户，然后单独删除它们。

- 您可能希望手动删除 AWS Control Tower 的 AWS IAM Identity Center （ IAM 身份中心）配置，但您可以继续使用现有的 IAM 身份中心配置。
- 您可能希望移除由 AWS Control Tower 创建的 VPC，并移除关联的 AWS CloudFormation 堆栈集。
- 在新 AWS 区域中设置新的着陆区之前，必须执行以下额外步骤。
  - 通过 CLI 输入以下命令：

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

  - 从所有受管辖区域的共享账户和成员账户中删除剩余的名AWSControlTowerManagedRule为的托管规则。 AWSControlTowerManagedRule是 Amazon 的 EventBridge 规则。

停用 landing zone 后进行设置

停用您的登录区后，在手动清理完成之前，您无法再次成功执行设置。此外，如果不手动清理这些剩余资源，您可能会产生意外的账单费用。您必须注意以下问题：

- AWS Control Tower 管理账户是 AWS Control Tower 根组织单位的一部分。请务必从管理账户中移除这些 IAM 角色和 IAM 策略：
  - 角色：
    - AWSControlTowerAdmin
    - AWSControlTowerCloudTrailRole
    - AWSControlTowerStackSetRole
  - 策略：
    - AWSControlTowerAdminPolicy
    - AWSControlTowerCloudTrailRolePolicy

  - AWSControlTowerStackSetRolePolicy

- 在再次进入着陆区之前，您可能希望删除或更新 AWS Control Tower 的现有 IAM 身份中心配置，但无需将其删除。
- 您可能希望移除 AWS Control Tower 创建的 VPC。
- 如果为日志或审计帐户指定的电子邮件地址与现有 AWS 帐户相关联，则安装将失败。您可以关闭 AWS 账户，也可以使用不同的电子邮件地址重新设置着陆区。或者，您可以重复使用这些现有的共享帐户，该功能允许您自带日志和审计帐户。有关更多信息，请参阅 引入现有安全账户或日志账户的注意事项。
- 如果日志账户中已存在具有以下保留名称的 Amazon S3 存储桶，则安装将失败：
  - aws-controltower-logs-*{accountId}*-*{region}*（用于日志记录存储桶）。
  - aws-controltower-s3-access-logs-*{accountId}*-*{region}*（用于日志记录访问存储桶）。

  您必须重命名或删除这些存储桶，或者为日志记录账户使用其他账户。
- 如果管理账户在“日志”中 CloudWatch 拥有现有的日志组aws-controltower/CloudTrailLogs，则安装将失败。您必须重命名或删除日志组。

在设置新版本之前 AWS 区域

如果您打算在新区域中设置新的着陆 AWS 区，请按照以下额外步骤操作。

- 通过 CLI 输入以下命令：

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- 从所有受管辖区域的共享账户和成员账户中删除剩余的名AWSControlTowerManagedRule为的托管规则。

> **Note**
>
> 您无法在拥有名为 Sec ur ity 或 S andbox 的顶级 OU 的组织中设置新的着陆区。您必须重命名或删除这些 OU 才能再次设置登录区。

故障排除

如果您在使用 AWS Control Tower 时遇到问题，可以根据我们的最佳实践使用以下信息来解决这些问题。如果您遇到的问题超出了以下信息的范围，或者在您尝试解决这些问题后仍然存在，请联系 Su AWS pport。

登录区启动失败

登录区启动失败的常见原因：

- 缺少对确认电子邮件的回复。
- AWS CloudFormation StackSet 失败。

确认电子邮件：如果您的管理账户使用时间不到一小时，则在创建其他账户时可能会遇到问题。

要采取的操作

如果您遇到此问题，请查收电子邮件。您可能已经收到了一封等待回应的确认电子邮件。或者，我们建议您等待一个小时，然后重试。如果问题仍然存在，请联系 Supp AWS ort。

失败 StackSets：landing zone 启动失败的另一个可能原因是 AWS CloudFormation StackSet 失败。AWS 必须在 AWS Control Tower 管理的所有 AWS 区域的管理账户中启用安全令牌服务 (STS) 区域，这样配置才能成功；否则，堆栈集将无法启动。

要采取的操作

在启动 AWS Control Tower 之前，请务必启用所有必需 AWS 的安全令牌服务 (STS) 终端节点区域。

要查看 AWS Con AWS 区域 trol Tower 支持的列表，请参阅AWS 区域如何与 AWS Control Tower 配合使用。

着陆区不是最新的错误

如果您最近没有更新着陆区，则在尝试重新获得 AWS Control Tower 访问权限时可能会收到错误消息。您可能会看到类似于以下内容的错误消息：

```
Unable to access Control Tower
```

您的账户已经停用了太长时间。由于处于非活动状态，您必须更新着陆区才能访问 AWS Control Tower。

但是，您的 landing zone 更新可能会失败。

要采取的步骤

登录您组织的管理帐户，然后以 root 用户身份登录。您的 IAM 用户或在 IAM 身份中心的用户必须拥有 AWS Control Tower 管理员权限并且是该AWSControlTowerAdmins群组的一员。然后再次尝试更新。

新账户预置失败

如果遇到此问题，请检查以下常见原因。

当填写账户预置表单时，您可能已经：

- 指定 tagOption，
- 启用 SNS 通知，
- 启用预置产品通知。

请在不指定上述任何选项的情况下重新尝试预置账户。有关更多信息，请参阅 使用 Account Factory 配置 AWS Service Catalog 账户 。

失败的其他常见原因：

- 如果您创建了预置产品计划（以查看资源更改），则您的账户预置可能会无限期地保持 In progress (正在进行) 状态。
- 当其他 AWS Control Tower 配置更改正在进行时，在 Account Factory 中创建新账户将失败。例如，在运行向 OU 添加控件的流程时，如果您尝试配置帐户，Account Factory 将显示一条错误消息。

在 AWS Control Tower 中查看先前操作的状态

- 导航到 AWS CloudFormation > StackSets
- 检查与 AWS Control Tower 相关的每个堆栈集（前缀：AWSControlTower“”）
- 查找仍在运行的 AWS CloudFormation StackSets 操作。

如果您的账户预置用时超过一小时，最好终止预置过程并重试。

无法注册现有账户

如果您尝试注册现有 AWS 账户但注册失败，则再次尝试时，错误消息可能会告诉您堆栈集存在。要继续操作，您必须在账户工厂中删除预置的产品。

如果首次注册失败的原因是您忘了提前在账户中创建 `AWSControlTowerExecution` 角色，您将收到的错误消息会正确地告诉您创建此角色。但是，当您尝试创建角色时，您可能会收到另一条错误消息，指出 AWS Control Tower 无法创建该角色。出现此错误的原因是该过程已部分完成。

在这种情况下，您必须执行两个恢复步骤，然后才能继续注册现有账户。首先，您必须通过 AWS Service Catalog 控制台终止 Account Factory 配置的产品。接下来，您必须使用 AWS Organizations 控制台手动将账户移出 OU 并移回根目录。完成此操作后，在账户中创建 `AWSControlTowerExecution` 角色，然后再次填写 Enroll account (注册账户) 表单。

注册失败的另一个可能原因是该账户拥有现有 AWS Config 资源。在这种情况下，请参阅注册拥有现有 AWS Config 资源的账户，了解如何修改现有资源的说明。

无法更新账户工厂账户

当账户处于不一致状态时，无法从 Account Factory 或 Account Factory 成功更新该账户 AWS Service Catalog。

案例 1：您可能会遇到类似以下错误消息：

```
AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.
```

常见原因：AWS Control Tower 在初始配置期间总是删除 AWS 默认 VPC。要在账户中拥有 AWS 默认 VPC，您必须在创建账户后添加该默认 VPC。AWS Control Tower 有自己的默认 VPC，可以取代 AWS 默认 VPC，除非你按照演练中显示的方式设置 Account Factory，这样 AWS Control Tower 就不会预置 VPC，这样 AWS Control Tower 就根本不会配置 VPC。这样，该账户没有 VPC。如果您想使用 AWS 默认 VPC，则必须重新添加该默认 VPC。

但是，AWS Control Tower 不支持 AWS 默认 VPC。部署一个此 VPC 会导致账户进入 `Tainted` 状态。当账户处于该状态时，您无法通过更新账户 AWS Service Catalog。

要执行的操作：您必须删除您添加的默认 VPC，然后才能更新账户。

> **Note**
>
> 该Tainted状态会导致后续问题：未更新的账户可能会阻止对其所属的 OU 启用控制。

案例 2：您可能会看到类似以下错误消息：

```
AWS Control Tower detects that your enrolled account has been moved to a
new organizational unit.
```

常见原因：您试图将账户从一个注册的 OU 转移到另一个 OU，但旧的 AWS Config 规则仍然存在。该账户处于不一致的状态。

要采取的行动：

如果有意转移账户：

- 在 Service Catalog 中终止账户。
- 再次注册。
- 上下文/影响：已部署的 AWS Config 规则与目标 OU 规定的配置不匹配。
- AWS Config 规则可能会保留之前的 OU，从而导致意外支出。
- 由于资源命名冲突，重新注册或更新账户的尝试将失败。

如果账户转移是意外的：

- 将账户恢复到其原来的 OU。
- 从 Service Catalog 更新账户。
- 在启动参数中，输入账户最初所在的 OU。
- 上下文/影响：如果账户未返回其原始 OU，则其状态将与其所在的新 OU 所规定的控制不一致。
- 更新账户不是有效的补救措施，因为它不会删除与其先前的 OU 关联的 AWS Config 规则。

无法更新着陆区

如果更新失败，AWS Control Tower 不会回滚到之前的着陆区版本。你可能会发现你的着陆区处于不确定状态。如果是，请联系 AWS 支持人员。

着陆区更新可能由于多种原因而失败。

- 未满足先决条件
- AWS Config 某些账户中存在资源
- 存在已关闭的账户

未满足先决条件

着陆区更新必须满足与着陆区设置相同的先决条件。在更新之前，请查看发布前检查。

AWS Config 资源存在于安全 OU 账户中

请勿在您的审核和日志存档账户中添加 AWS Config 资源。如果存在这些资源，则无法完成 landing zone 更新过程。这些限制与首次注册账号或设置 landing zone 的限制类似。有关更多信息，请参阅注册拥有现有 AWS Config 资源的账户。

存在已关闭的账户

当账户处于 “已关闭” 或 “已暂停” 状态时，您在尝试更新 landing zone 时可能会遇到问题。在对 landing zone 进行更新之前，您必须删除每个已关闭账户上的预配置产品。

在 AWS Service Catalog 预配置产品页面上，您可能会看到类似于以下内容的错误消息：

```
AWSControlTowerExecution role can't be assumed on the account.
```

常见原因：您在未删除预配置产品的情况下暂停了账户。

要采取的措施：如果您看到此错误，则有两种选择：

1. 联系 S AWS upport 并重新打开账户，删除预配置的产品，然后再次关闭该账户。
2. 从中移除因账户关闭而成为孤立的资源。 StackSets （此选项仅在您未移除的 StackSets 实例处于 “当前” 状态时才可用。 ）

要从中移除资源 StackSets，请对每个已关闭的账户执行以下操作：

- 进入每个 AWS Control Tower， StackSets 然后 StackInstances 从每个区域中删除已关闭的账户。
- 重要：选择 “保留堆栈” 选项，以便仅 StackSet 删除堆栈实例。 StackSet 无法从已关闭的账户中担任角色，因此如果它尝试代入该`AWSControlTowerExecution`角色，它将失败，这会导致您收到错误消息。

提及的失败错误 AWS Config

如果 AWS Config 在 AWS Control Tower 支持的任何 AWS 区域中启用，则由于预检查失败，您可能会收到一条错误消息。由于某些潜在的行为，该消息似乎无法充分解释问题 AWS Config。

您可能会收到一条错误消息，类似于以下内容之一：

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again .`
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again .`

常见原因：在 AWS 账户上启用该 AWS Config 服务时，它会使用默认命名创建配置记录器和传送渠道。如果您通过控制台禁用该 AWS Config 服务，它不会删除配置记录器或传送渠道。您必须通过 CLI 将其删除，或者对其进行修改以供 AWS Control Tower 使用。如果在 AWS Control Tower 支持的任何一个区域启用了该 AWS Config 服务，则可能会导致此故障。

如果该账户已有 AWS Config 资源，请参阅注册拥有现有 AWS Config 资源的账户，了解如何修改现有资源的说明。

要执行的操作：删除所有受支持区域中的配置记录器和传递通道。仅仅禁用 AWS Config 是不够的，必须通过 CLI 删除配置记录器和传送渠道。从 CLI 中删除配置记录器和交付渠道后，您可以再次尝试启动 AWS Control Tower 并注册账户。

如果您正在部署预配置产品，则必须先删除预配置产品，然后再重试。否则，您可能会看到类似以下错误消息：

- `An error occurred (InvalidParametersException) when calling the ProvisionProduct operation: A stack named Stackname already exists.`

在消息中，*Stackname*指定堆栈的名称。

以下是一些用于确定配置记录器和传送渠道状态的 AWS Config CLI 命令示例。

查看命令：

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

删除命令：

- `aws configservice stop-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-delivery-channel --delivery-channel-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*

有关更多信息，请参阅 AWS Config 文档

- 管理配置记录器 (AWS CLI)
- 管理传递通道

未找到启动路径错误

当您尝试创建新账户时，您可能会看到类似以下内容的错误消息：

```
No launch paths found for resource: prod-dpqqfywxxxx
```

此错误消息由生成 AWS Service Catalog，这是一项帮助在 AWS Control Tower 中配置账户的集成服务。

常见原因：

- 您可能以 root 用户身份登录。AWS Control Tower 不支持在您以根用户身份登录时创建账户。
- 您的 IAM Identity Center 用户尚未添加到相应的权限组。您可能需要将您的 IAM Identity Center 用户添加到以下权限组之一：AWSAccountFactory（用于最终用户访问）或 AWSServiceCatalogAdmins（用于管理员访问权限）。

- 如果您以 IAM 用户身份通过身份验证，则必须将其添加到 AWS Service Catalog 产品组合中，这样它才具有正确的权限。
- 如果您拥有正确的权限，但检测到 AWS Control Tower 偏差，因此需要进行漂移修复，也会出现此问题。要修复大多数类型的漂移，请在着陆区域设置页面上选择重置。

收到权限不足错误

在某些情况下，您的账户可能不具备执行某些工作的必要权限 AWS Organizations。如果您遇到以下类型的错误，请检查所有权限区域，例如 IAM 或 IAM Identity Center 权限，以确保这些地方没有拒绝您的权限：

```
You have insufficient permissions to perform AWS Organizations API actions.
```

如果您认为自己的工作需要您正在尝试的操作，但找不到任何相关的限制，请联系您的系统管理员或 Su AWS pport。

Detective 控制未对账户生效

如果您最近将 AWS Control Tower 部署扩展到一个新 AWS 区域，则在更新受 AWS Control Tower 管理的 OU 中的个人账户之前，新应用的侦探控制不会对您在任何地区创建的新账户生效。对现有账户的现有侦查控制措施仍然有效。

如果您在更新帐户之前尝试启用侦探控件，则可能会看到类似以下错误消息：

```
AWS Control Tower can't enable the selected control on this OU. AWS Control
Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, because child
accounts have dependencies that are missing. Update all child accounts
under the OU, then try again.
```

要采取的操作：更新账户。

要通过 AWS Control Tower 控制台更新您的账户，请参阅何时更新 AWS Control Tower 业务单元和账户。

要以编程方式更新多个个人账户，您可以使用中的 API AWS Service Catalog 和 AWS CLI 来自动更新。有关如何处理更新过程的更多信息，请参阅此视频演练。 你可以用 UpdateProvisionedProductAPI 代替视频中显示的 ProvisionProductAPI。

如果您在为账户启用侦探控制方面遇到更多困难，请联系 Su AWS pport。

AWS Organizations API 返回的超出速率错误

可能的原因

您的工作负载正在运行，而 AWS Control Tower 正在运行每日扫描以检查您的 SCP 是否存在偏差。

要遵循的步骤

如果您遇到 API 限制或`rate exceeded`错误，请尝试以下步骤：

- 在不同的时间运行您的工作负载。（请参阅按地区划分的 AWS Control Tower SCP 不变性扫描时间表，了解 AWS Control Tower 何时运行审计扫描。）
- 如果您直接通过 HTTP 调用 API：请使用 AWS SDK，它会自动重试失败的操作
- 通过 Service Quotas 和 Su AWS pport 申请提高限额

可以在此处找到 Elastic Beanstalk 中 API 限制的疑难解答说明示例：`https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

无法将 Account Factory 账户直接从一个 AWS Control Tower 着陆区转移到另一个 AWS Control Tower 着陆区

> **Warning**
>
> 这种做法不符合注册合格账户的先决条件，因为符合条件的账户必须属于同一个整体 AWS 组织，而且每个组织可能只有一个 landing zone。如果您尝试执行此操作，但发现自己收到了多条错误消息，那么以下信息可能会有所帮助。

要将您通过 Account Factory 配置的账户转移到另一个由 AWS Control Tower 管理的着陆区，在另一个管理账户下，您必须从原始 OU 中移除所有 IAM 角色和与该账户关联的堆栈。从部署账户的每个区域中移除这些资源。

> **Note**
>
> 移除资源的最佳方法是，在尝试移动账户之前，先取消其原始 OU 中的账户配置。

如果你不移除资源，那么注册新 OU 就会失败，这有点惊人。您可能会遇到一条或多条错误消息，并且会一直收到类似的错误消息，直到剩余的角色和堆栈从部署账户的每个区域中移除。

每次收到错误消息时，都必须将该账户从新 OU 中移除，删除作为错误消息主题的旧资源，然后尝试将该账户移回新 OU。对于部署账户的每个区域， removing-and-deleting 必须对所有剩余资源重复此过程，可能是 10 或 20 次。之所以出现这些反复出现的错误，是因为该账户被配置到具有防止 IAM 角色删除的 SCP 的 OU。在重试之前，您可以删除账户的所有资源，从而缩短恢复过程。

以下示例显示了如果仍有未删除的角色和堆栈，您可能会收到的失败消息类型。只要保留旧资源，每次尝试注册账户时，您很可能会一次看到其中一条消息。

已针对示例修改了资源 ID 字符串的值。在您可能收到的错误消息中，它们的值将不相同。您可能会看到一条类似于以下示例的消息：

- AWS Control Tower cannot create the IAM role *aws-controltower-AdministratorExecutionRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ConfigRecorderRole* because the role already exists. To continue, delete the existing IAM role and try again.
- AWS Control Tower cannot create the IAM role *aws-controltower-ForwardSnsNotificationRole* because the role already exists. To continue, delete the existing IAM role and try again.

或者你可能会看到一条关于堆栈集失败的错误消息，类似于以下内容：

```
"Error\":\"StackSetFailState\",
\"Cause\":\"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
```

```
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.
```

从第一个 OU 中移除所有剩余资源后，您将能够成功邀请、配置账户或将该账户注册到新 OU。

AWS Support

如果要将现有成员账户移动到其他支持计划中，您可以使用根账户凭证登录各个账户，比较计划，然后根据您的意愿设置支持级别。

我们建议您在更改支持计划时更新 MFA 和账户安全联系人。

基线的类型

AWS Control Tower 中的基准是您可以应用于目标的一组资源和特定配置。最常见的基准目标可能是组织单位 (OU)。例如，您可以启用一个选定组织单位作为目标的基准，将该 OU 注册到 AWS Control Tower 中。

在设置着陆区期间，基准目标可能是共享账号或整个着陆区。根据您的 landing zone 设置和配置，可能会启用和更新某些基准。AWS Control Tower 按照基准指定的方式创建资源并将其部署到目标。

为目标启用基线时，该基线将表示为一种 AWS CloudFormation 资源，称为`EnabledBaseline`资源。

AWS Control Tower 包括四种基本类型的基准：

- 一种类型可以应用于在 AWS Control Tower 注册的 OU，也可以适用于您打算通过应用基准进行注册的 OU。
- 在初始设置期间或着陆区更新期间，三种基准类型可以应用于着陆区或共享账户。

适用于 OU 级别的基准类型，用于注册和更新 OU

- 名称：`AWSControlTowerBaseline`

  描述：为目标 OU 中的成员账户设置资源和强制控制措施，这是 AWS Control Tower 治理所必需的。

  注意事项：此基线保留了 landing zone 区域拒绝控制的设置。换句话说，如果一个区域不允许进入着陆区级别，那么当你调用 `EnableBaseline` API 注册 OU 时，该区域就不允许该组织进入该 OU。

  > **Note**
  >
  > OU 级别的 Region deny 控制无法允许着陆区域 Region deny 控制不允许的区域。

  有关更多信息，请参阅 AWS Organizations 文档中的 SCP 如何使用 deny。

  建议：我们建议您在调用 OU 的 `EnableBaseline` API 之前，确认目标 OU 可能在哪些区域运行工作负载，并根据着陆区域 Region deny 控制检查结果，否则您可能会无法访问某些区域的资源。

> **Note**
>
> 着陆区基线的行为与 OU 级别的基线不同。

作为着陆区设置和更新过程的一部分，AWS Control Tower 会自动启用在着陆区级别应用的基准。当你更改着陆区设置时，着陆区的基线可能会发生变化。例如，如果您选择加入 IAM 身份中心，AWS Control Tower 可以在您的着陆区启用最新版本的`IdentityCenterBaseline`基准。

您可以通过 `ListEnabledBaselines` API 调用查看您的着陆区已启用的基线。

可能适用于您的 landing zone 或共享账号的基准类型

- 名称：`AuditBaseline`

  描述：设置资源以监控组织中账户的安全性和合规性。您无法更改此基准，它是由 AWS Control Tower 部署的。
- 名称：`LogArchiveBaseline`

  描述：设置一个中央存储库，用于存储组织中账户的 API 活动和资源配置日志。您无法更改此基准，它是由 AWS Control Tower 部署的。
- 名称：`IdentityCenterBaseline`

  描述：为 IAM Identity Center 设置共享资源，这会`AWSControlTowerBaseline`为账户设置身份中心访问权限做好准备。

  注意事项：只有当您在最初设置着陆区时选择 IAM Identity Center 作为身份提供商，或者随后更改着陆区设置以为着陆区启用 IAM Identity Center 时，此基准才有效。如果您使用的是其他身份提供商，则无权启用此基准。

部分注册账户

当你使用基准时，可以将账户置于名为 “部分注册” 的状态。

如果您通过调用 `ResetEnabledBaseline` API 重新注册 OU，则可能会出现这种状态，因为 AWS Control Tower 仅将必需资源应用于目标 OU 中的账户。缺少其父 OU 的可选资源（控件）的账户将被标记为 “部分注册”。

如果您将未注册的账户转移到已注册的 OU 中，然后调用 OU 上的 `ResetEnabledBaseline` API 注册该账户，AWS Control Tower 会将与之关联的资源应用于新注册的账户。`AWSControlTowerBaseline`但是，为此 OU 启用的可选控件不适用于该账户。该账户仍处于“部分注册” 状态。

要完全注册账户，请在控制台中选择 “重新注册” 或 “更新账户”。当您从控制台中选择这些操作时，AWS Control Tower 会将该 OU 的所有资源应用到新注册的账户，包括为该 OU 激活的可选控件。

AWS Control Tower 控制台和用于基准的 API 之间的操作差异

当您更改 OU 的监管状态时，AWS Control Tower 控制台会自动为您执行更多操作，而不是通过基准 API 来更改治理。

差异

- 注册和配置产品

  当您通过控制台注册 OU 时，AWS Control Tower 会在注册每个账户的过程中为该组织成员账户创建服务目录产品。当您通过 `EnableBaseline` API 和注册组织单位时`AWSControlTowerBaseline`，AWS Control Tower 不会为组织单位中的成员账户创建预配置产品。
- 注销 OU

  每次注销 OU 时，都必须先移除所有成员账户和嵌套的 OU。然后，AWS Control Tower 会移除应用于 OU 的所有控件。
  - 如果您从控制台中选择 “删除 OU”，AWS Control Tower 会继续取消注册，然后从您的组织中删除 OU。
  - 但是，如果您通过调用 `DisableBaseline` API `AWSControlTowerBaseline` 从 OU 中移除 OU 来注销 OU，AWS Control Tower 不会从您的组织中删除 OU，则该组织仍存在于组织中，且未注册。

基准和版本控制默认值

如果您的 AWS Control Tower 着陆区已经设置完毕，然后您选择启用着陆区基准，那么 AWS Control Tower 会启用与您的着陆区版本兼容的最新版本的基准。如果您选择为尚未在 AWS Control Tower 注册的 OU 启用基准，AWS Control Tower 会自动为该 OU 提供最新兼容版本的基准。

OU 基准和 landing zone 版本的兼容性

如果您的业务需要，AWS Control Tower 基准允许您在 OU 级别而不是着陆区级别设置监管标准。所调用的基准可用于帮助您`AWSControlTowerBaseline`在 AWS Control Tower 中注册组织单元。

> **Note**
>
> 基准是一组控件和资源，它们协同工作，在您的 landing zone 中建立稳定的治理环境。

当您在 OU 上启用基准时，通过在 AWS Control Tower 中调用 `EnableBaseline` API，您必须指定与您当前 AWS Control Tower 着陆区版本兼容的基准版本。指定基准后，OU 中的所有成员账户都将遵循为 OU 提供的基准。换句话说，新账户使用更新的基准进行配置，现有成员账户将根据新的基准进行管理。

如果您没有为现有 OU 和账户选择基准，则默认情况下，landing zone 版本将决定整个治理状态。但是，您的 landing zone 中每个注册的 OU 都会被分配一个基准版本，这是与您当前着陆区版本兼容的最新基准。因此，即使您从未专门指定基准，每个 OU 和注册的成员账户都有一个关联的基准。

对于 OU 级别的基准`AWSControlTowerBaseline`，下表显示了基准与 AWS Control Tower 着陆区版本的兼容性。

基准版本	着陆区版本	内含蓝图	内含控件	与之前的基线相比的变化	
1.0	2.0 到 2.7	BP_BASELINE_CLOUDTRAIL、BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_ROLES、IAM 资源	所有强制性控制措施	无	

基准版本	着陆区版本	内含蓝图	内含控件	与之前的基线相比的变化	
2.0	2.8 到 2.9	BP_BASELINE_CLOUDTRAIL、BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM 资源	所有强制性控制措施	添加了 AWS Config 服务相关角色 (SLR) 和新的 Config 蓝图以使用 SLR	
3.0	3.0 到 3.1	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_ROLES、Config SLR、IAM 资源	所有强制性控制措施	新 AWS Config 蓝图。更改为仅在本地区记录全球资源。已移除 CloudTrail 蓝图	

基准版本	着陆区版本	内含蓝图	内含控件	与之前的基线相比的变化	
4.0	3.2 到 3.3	BP_BASELINE_CLOUDWATCH、BP_BASELINE_CONFIG、BP_BASELINE_ROLES、BP_BASELINE_SERVICE_LINKE_ROLES、Config SLR、IAM 资源	所有强制性控制措施	全新 SLR 蓝图	

有关设置 landing zone 时在账户中创建的特定资源的更多信息，请参阅在共享账户中创建的资源。

如果您将着陆区更新为支持更新的AWSControlTowerBaseline基准版本的版本，并且新的着陆区域版本与您现有的基准版本兼容，则您的组织单位状态将更改为更新可用。

- 除了从 2.x 更新到 3.x 的 landing zone 之外，您无需立即更新 OU 基准即可继续使用账号工厂和其他功能。
- 在基准版本更新之前，在此 OU 中注册的新账户将根据现有基准版本获得资源（使用控制台中的扩展监管功能或通过 UpdateEnabledBaseline API）。
- 更新基准版本后，该 OU 中的所有账户都会收到基于新基准版本的资源。

> **Note**
>
> 如果您将 AWS Control Tower 着陆区从任何 2.X 版本更新为任何 3.X 版本，则还必须更新 OU 上的基准版本，因为从账户级别更改为组织级跟踪。 AWS CloudTrail 在控制台中，您的 OU 将显示 “需要更新” 状态。

基准注意事项

- 如果您的 OU 需要更新基准，则无法配置新账户或将现有账户注册到该 OU。
- landing zone 更新后，如果您还计划更新 OU 基准，则必须重新注册 OU 或以编程方式更新 OU 基准版本。
- 我们建议你更新到你正在使用的着陆区版本的最高兼容基准，这样你就可以获得着陆区和基线组合在一起的所有好处。例如，如果您更新到着陆区版本 3.3，则可以继续使用基准 3.0，但除非您同时更新到基准 4.0，否则您无法获得着陆区 3.3 版本的所有好处。
- 基准更新无法回滚。
- 基准启用以每次一个 OU 为目标。因此，更新父 OU 时，嵌套 OU 不会自动更新。我们建议您在更新嵌套的 OU 之前先更新父 OU。
- 当您从控制台调用 `UpdateEnabledBaseline` API 或重新注册 OU 时，OU 会保留基准更新之前启用的所有控件。
- 当多个基准版本与您的 landing zone 版本兼容时，如果您在非托管 OU 上启用基准，则必须使用最新的基准版本。

示例：仅使用 API 注册 AWS Control Tower 组织单位

本示例演练是一份配套文档。有关解释、注意事项和更多信息，请参阅。基线的类型

先决条件

您必须有一个未在 AWS Control Tower 注册且想要注册的现有组织单位。或者，您必须拥有想要重新注册的已注册OU，以便进行更新。

注册 OU

1. 检查是否已`IdentityCenterBaseline`为着陆区启用。如果是，请获取启用身份中心的基准标识符。

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. 获取目标 OU 的 ARN。

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. 获取基线的 ARN。AWSControlTowerBaseline

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. 在目标 OU 上创建AWSControlTowerBaseline基准。

   如果启用了身份中心基准：

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"<Identity Center Enabled
 Baseline ARN>"}]'
```

   如果未启用身份中心基准，请省略该*parameters*标志，如下所示：

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

重新注册 OU

更新着陆区设置或更新着陆区版本后，必须重新注册 OU 才能向他们提供最新更改。按照以下步骤通过重置关联的资源，以编程方式重新注册 OU。EnabledBaseline

1. 获取要重新注册的目标 OU 的 ARN。

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. 获取目标 OU 的EnabledBaseline资源的 ARN。

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. 重置已启用的基准。

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

基准 API 用法示例

本节包含 AWS Control Tower 基准 API 的输入和输出参数示例。

DisableBaseline

有关此 API 操作的更多信息，请参阅DisableBaseline。

DisableBaseline输入:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

DisableBaseline输出：

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

DisableBaselineCLI 示例：

```
aws controltower disable-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
    --region us-west-2
```

EnableBaseline

有关此 API 操作的更多信息，请参阅EnableBaseline。

EnableBaseline输入:

```
{
```

```
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

EnableBaseline输出：

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
}
```

EnableBaselineCLI 示例：

此示例演示如何为一个 AWS Organizations 组织启用基准，该着陆区已选择接入 AWS Control Tower 管理的 IA AWS M 身份中心访问权限。要检索您的身份中心EnabledBaseline标识符，您可以调用 ListEnabledBaselines API，根据身份中心基准进行筛选：(arn:aws:controltower:*Region*::baseline/LN25R72TTG6IGPTQ)

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

响应将显示EnabledBaseline详细信息，其中显示其标识符。

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
            "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
```

```
            "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
            "statusSummary": {
                "status": "SUCCEEDED"
            }
        }
    ]
}
```

> **Note**
>
> 记下响应中的 ARN 值，并将此值作为参数传递以启用默认基准。

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

对于选择退出 AWS Control Tower 对 IAM Identity Center 管理的组织，请启用不带参数的基准。

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --region us-west-2
```

GetBaseline

有关此 API 操作的更多信息，请参阅GetBaseline。

GetBaseline输入:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
```

```
}
```

GetBaseline输出：

```
{
    "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",
    "name": "AWSControlTowerBaseline",
    "description": "Sets up resources and mandatory controls for member accounts within
 the target OU, required for AWS Control Tower governance.",
}
```

GetBaselineCLI 示例：

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

GetBaselineOperation

有关此 API 操作的更多信息，请参阅GetBaselineOperation。

GetBaselineOperation输入:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

GetBaselineOperation输出：

```
{
    "baselineOperation": {
        "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
        "operationType": "DISABLE_BASELINE",
        "status": "FAILED",
        "startTime": "2023-01-12T19:05:00Z",
        "endTime": "2023-01-12T19:45:00Z",
        "statusMessage": "Can't perform DisableBaseline on a parent target with
 governed child OUs"
    }
}
```

GetBaselineOperationCLI 示例：

```
aws controltower get-baseline-operation \
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

GetEnabledBaseline

有关此 API 操作的更多信息，请参阅GetEnabledBaseline。

GetEnabledBaseline输入:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

GetEnabledBaseline输出：

```
{
    "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
        "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
        "baselineVersion": "3.0",
        "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
            }
        ]
    }
}
```

GetEnabledBaselineCLI 示例：

```
aws controltower get-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

ListBaselines

有关此 API 操作的更多信息，请参阅ListBaselines。

ListBaselines输入（使用可选输入）：

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

ListBaselines输出：

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/J8HX46AHS5MIKQPD",
            "name": "LogArchiveBaseline",
            "description": "Sets up a central repository for logs of API activities and
 resource configurations from accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/LN25R72TTG6IGPTQ",
            "name": "IdentityCenterBaseline",
            "description": "Sets up shared resources for AWS Identity Center, which
 prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/17BSJV3IGJ2QSGA2",
```

```
            "name": "AWSControlTowerBaseline",
            "description": "Sets up resources and mandatory controls for member
 accounts within the target OU, required for AWS Control Tower governance."
        }
    ]
}
```

ListBaselinesCLI 示例：

```
aws controltower list-baselines \
    --region us-west-2
```

ListEnabledBaselines

有关此 API 操作的更多信息，请参阅ListEnabledBaselines。

ListEnabledBaselines输入（无过滤器）：

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines输入（仅限baselineIdentifiers过滤器）：

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines输入（仅限targetIdentifiers过滤器）：

```
{
    "filter": {
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
```

```
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 2
}
```

ListEnabledBaselines输入（baselineIdentifiers和targetIdentifiers过滤器）：

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2']
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

ListEnabledBaselines输出：

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjql",
            "statusSummary": {
                "status": "SUCCEEDED",
                "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
            }
        },
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "4.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
```

```
            "statusSummary": {
            "status": "FAILED",
                "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
            }
        }
    ],
    "nextToken": "e2bXXXXX6cab"
}
```

使用一种过滤器（baselineIdentifiers过滤器）的 CLI 示例：

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

使用多个筛选器（baselineIdentifiers和targetIdentifiers过滤器）的 CLI 示例：

```
aws controltower list-enabled-baselines \
    --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

ResetEnabledBaseline

有关此 API 操作的更多信息，请参阅ResetEnabledBaseline。

ResetEnabledbaseline输入:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

ResetEnabledBaseline输出：

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

ResetEnabledBaselineCLI 示例：

```
aws controltower reset-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

UpdateEnabledBaseline

有关此 API 操作的更多信息，请参阅UpdateEnabledBaseline。

UpdateEnabledBaseline输入:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
    "baselineVersion": "4.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

UpdateEnabledBaseline输出：

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

UpdateEnabledBaselineCLI 示例：

```
aws controltower update-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --baseline-version 4.0
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
```

```
    --region us-west-2
```

相关信息

本主题列出了 AWS Control Tower 功能和其他增强功能的常见用例和最佳实践。本主题还包括相关博客文章、技术文档和相关资源的链接，这些资源可以在您使用 AWS Control Tower 时为您提供帮助。

教程和实验

- AWS Control Tower 实验室 — 这些实验提供了与 AWS Control Tower 相关的常见任务的高级概述。
- 如果您想到了用例，但不确定从哪里开始，请在 AWS Control Tower 控制面板上选择获取个性化指导。
- 请尝试访问精选的 YouTube 视频列表，这些视频详细介绍了如何使用 AWS Control Tower 功能。

联网

为中的 AWS网络设置可重复且易于管理的模式。详细了解客户常用的设计、自动化和设备。

- AWS VPC 架构快速入门 — 本快速入门指南根据您的 AWS 云基础设施 AWS 的最佳实践提供了网络基础。它构建了一个包含公有和私有子网的 AWS Virtual Private Network 环境，您可以在其中启动 AWS 服务和其他资源。
- 使用 AWS Service Catalog 在 AWS Control Tower 中使用自助服务 VPC — 这篇博客文章描述了一种设置 Account Factory 的方法，这样您就可以为账户配置自定义 VPC。
- 在 AWS Control Tower 中实现无服务器传输网络协调器 (STNO) — 这篇博客文章演示了如何自动跨账户访问网络连接。本博客面向 AWS Control Tower 管理员或负责管理其 AWS 环境中网络的管理人员。

安全、身份和日志

扩展您的安全态势，与外部或现有身份提供商集成，并集中管理日志系统。

安全性

- 使用 AWS Control Tower 生命周期事件自动 AWS Security Hub 发出警报 — 这篇博客文章介绍了如何在 AWS Control Tower 多账户环境中对现有账户和新账户自动启用和配置 Security Hub。

- 启用 AWS Identity and Access Management— 这篇博客文章介绍了如何通过启用和集中管理 IAM Access Analyzer 的调查结果来增强组织的安全可见性。
- AWS Systems Manager Parameter Store 提供安全的分层存储，用于配置数据管理和密钥管理。您可以使用它在安全位置共享配置信息，供 AWS Systems Manager 和 AWS 使用 CloudFormation。例如，您可以存储要在其中部署一致性包的区域列表。

身份

- 将 Azure AD 用户身份关联到 AWS 账户和应用程序以进行单点登录 — 这篇博客文章介绍了如何将 Azure AD 与 IAM 身份中心和 AWS Control Tower 配合使用。
- 通过@@ 集中管理 Okta 用户对 AWS 的访问权限 AWS IAM Identity Center — 这篇博客文章介绍了如何将 Okta 与 IAM 身份中心和 AWS Control Tower 配合使用。

日志记录

- AWS 集中式日志解决方案 — 这篇解决方案文章描述了集中式日志解决方案，该解决方案使组织能够 AWS 跨多个账户和 AWS 地区收集、分析和显示日志。

部署资源和管理工作负载

部署和管理资源和工作负载。

- 入门库集成 — 这篇博客文章描述了你可以使用的入门作品集。
- 将云托管人持续部署到 AWS Control Tower

与现有组织和账户合作

与现有 AWS 组织和账户合作。

- 注册账户 — 本用户指南主题介绍如何在 AWS Control Tower 中注册现有 AWS 账户。
- 在 AWS Control Tower 下开设账户 — 这篇博客文章介绍了如何在现有 AWS 组织中部署 AWS Control Tower。
- 使用 AWS Config 一致性包扩展 AWS Control Tower 治理 — 这篇博客文章介绍了如何部署 AWS Config 一致性包以帮助将现有账户和组织纳入 AWS Control Tower 的治理。

- 如何使用 AWS Control Tower 检测和缓解护栏违规行为 — 这篇博客文章介绍了如何添加控件以及如何订阅 SNS 通知，以便您可以通过电子邮件收到有关控制合规违规行为的通知。

自动化和集成

自动创建账户并将生命周期事件与 AWS Control Tower 集成。

- 生命周期事件 — 这篇博客文章介绍了如何在 AWS Control Tower 中使用生命周期事件。
- 自动创建账户 — 这篇博客文章介绍了如何在 AWS Control Tower 中设置自动创建账户。
- Amazon VPC 流日志自动化 — 这篇博客文章介绍了如何在多账户环境中自动执行和集中管理 Amazon VPC 流日志。
- 使用 AWS Control Tower 生命周期事件自动标记 VPC — 这篇博客文章介绍了如何通过 AWS Control Tower 中的生命周期事件自动为 VPC 添加资源标签。
- 自动账户管理 — 这篇博客文章介绍如何在设置 AWS Control Tower 环境后自动执行账户管理任务。

迁移工作负载

在 AWS C AWS ontrol Tower 中使用其他服务来协助工作负载迁移。

- CloudEndure 迁移 — 这篇博客文章介绍了如何将 CloudEndure 和其他 AWS 服务与 AWS Control Tower 相结合以协助工作负载迁移。

相关 AWS 服务

AWS Control Tower 充当的编排层。 AWS Organizations因此，通过 AWS Organizations 控制台和 API，您可以访问其他 20 多种与 AWS Control Tower 配合使用的 AWS 服务。这些附加服务无法直接通过 AWS Control Tower 控制台进行访问。

- 有关通过 AWS 组织向 AWS Control Tower 提供的服务的完整列表，请参阅您可以在 AWS 组织中使用的 AWS 服务。
- 要为这些相关的 AWS 服务启用多账户功能，您必须启用可信访问。有关更多信息，请参阅 将 AWS Organizations 与其他 Amazon Web Services 结合使用。

> **Note**
>
> 请记住，AWS IAM 身份中心 AWS Config、和 AWS CloudTrail 是在 AWS Control Tower 中为您设置的，并且已完全集成。您无需修改这些服务的可信访问权限或委托管理设置。

- 通过提供的某些 AWS 服务 AWS Organizations 可以使用委托管理，包括 AWS Systems Manager 和 AWS Firewall Manager。有关更多信息，请参阅配置委派管理员和为 Fi rewall Manager 启用委派管理员帐户。另请观看此视频 “使用 AWS Firewall Manager 设置安全组”。

AWS Marketplace 解决方案

从中探索解决方案 AWS Marketplace。

- AWS Control Tower Marketplace — 为 AWS Control Tower AWS Marketplace 提供广泛的解决方案，以帮助您集成第三方软件。这些解决方案有助于解决关键基础设施和运营用例，包括身份管理、多账户环境安全、集中式联网、运营情报以及安全信息和事件管理 (SIEM)。

AWS Control Tower 发行说明

以下各节详细介绍了需要更新 AWS Control Tower 着陆区的 AWS Control Tower 版本，以及自动整合到该服务中的版本。

功能和版本根据正式向公众发布的日期按时间倒序列出（最新的优先顺序）。由于记录功能或版本的时间与正式发布之间可能存在延迟，因此此处列出的功能或版本的日期可能与中的日期略有不同文档历史记录。

2024 年 1 月——至今

自 2024 年 1 月以来，AWS Control Tower 发布了以下更新：

- AWS Control Tower 支持多达 100 个并发控制操作
- AWS Control Tower 已在 AWS 加拿大西部（卡尔加里）上市
- AWS Control Tower 支持自助服务配额调整
- AWS Control Tower 发布了控制参考指南
- AWS Control Tower 更新并重命名了两个主动控件
- 已弃用的控件不再可用
- AWS Control Tower 支持在以下位置标记`EnabledControl`资源 AWS CloudFormation
- AWS Control Tower 支持用于 OU 注册和使用基准进行配置的 API

AWS Control Tower 支持多达 100 个并发控制操作

2024年5月20日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在支持具有更高并发度的多个控制操作。您可以通过控制台或通过 API 同时跨多个组织单位 (OU) 提交最多 100 个 AWS Control Tower 控制操作。最多可以同时运行十 (10) 个操作，其他操作将排队。通过这种方式，您可以跨多个设置更加标准化的配置 AWS 账户，而不必承担重复控制操作的操作负担。

要监控正在进行的和排队的控制操作的状态，您可以在 AWS Control Tower 控制台中导航到新的 “近期操作” 页面，也可以调用新`ListControlOperations`的 API。

AWS Control Tower 库包含 500 多个控件，这些控件对应于不同的控制目标、框架和服务。对于特定的控制目标，例如加密静态数据，您可以通过单个控制操作启用多个控件，以帮助您实现目标。此功能有助于加快开发速度，允许更快地采用最佳实践控制措施，并降低运营复杂性。

AWS Control Tower 已在 AWS 加拿大西部（卡尔加里）上市

2024年5月3日

（AWS Control Tower 着陆区无需更新。）

从今天开始，您可以在加拿大西部（卡尔加里）地区激活 AWS Control Tower。如果您已经部署了 AWS Control Tower，并且想要将其监管功能扩展到该区域，则可以使用 AWS Control Tower 着陆区 API 来实现。或者在控制台中，前往 AWS Control Tower 控制面板中的设置页面，选择您的区域，然后更新您的着陆区。

加拿大西部（卡尔加里）区域不支持 AWS Service Catalog。因此，AWS Control Tower 的某些功能有所不同。最显著的功能变化是 Account Factory 不可用。如果您选择加拿大西部（卡尔加里）作为您的主区域，则更新账户、设置账户自动化以及任何其他涉及 Service Catalog 的流程将与其他地区不同。

配置账户

要在加拿大西部（卡尔加里）地区创建和配置新账户，我们建议您在 AWS Control Tower 之外创建一个账户，然后将其注册到注册的 OU。有关更多信息，请参阅注册现有账户和注册账户的步骤。

Service Catalog API 不适用于加拿大西部（卡尔加里）区域。Serv ice Catalog API 在 AWS Control Tower 中自动配置账户中显示的示例脚本不可行。

由于 AWS Control Tower 缺乏其他底层依赖关系，加拿大西部（卡尔加里）不提供账户工厂定制 (AFC)、Terraform 账户工厂 (AFT) 和 AWS 控制塔定制 (cfcT)。如果您将监管范围扩展到加拿大西部（卡尔加里）地区，则只要您所在的地区提供服务目录，您就可以继续管理 AWS Control Tower 支持的所有区域的 AFC 蓝图。

控件

AWS Security Hub 服务管理标准：AWS Control Tower 的主动控制和控制在加拿大西部（卡尔加里）地区不可用。加拿大西部（卡尔加里）CT.CLOUDFORMATION.PR.1不提供预防性控制，因为只有激活基于挂钩的主动控制才需要预防性控制。基于的某些侦探控制 AWS Config 不可用。有关更多信息，请参阅 控制限制。

身份提供商

加拿大西部（卡尔加里）不提供 IAM 身份中心。最佳实践建议是在提供 IAM 身份中心的区域设置您的着陆区。或者，如果您在加拿大西部（卡尔加里）使用外部身份提供商，则可以选择自行管理您的账户访问配置。

加拿大西部（卡尔加里）地区的 Service Catalog 不可用对由 AWS Control Tower 支持的其他区域没有影响。仅当您的家乡地区为加拿大西部（卡尔加里）时，这些差异才适用。

有关提供 AWS Control Tower 的区域的完整列表，请参阅AWS 区域表。

AWS Control Tower 支持自助服务配额调整

2024年4月25日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在支持通过服务配额控制台进行自助配额调整。有关更多信息，请参阅 请求提高限额。

AWS Control Tower 发布了控制参考指南

2024年4月21日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 发布了《控制参考指南》，这是一份新文档，您可以在其中找到有关特定于 AWS Control Tower 环境的控件的详细信息。此前，该材料已包含在 AWS Control Tower 用户指南中。《控件参考指南》涵盖了扩展格式的控件。有关更多信息，请参阅 AWS Control Tower 控件参考指南。

AWS Control Tower 更新并重命名了两个主动控件

2024年3月26日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 重命名了两个主动控制措施，以适应亚马逊 OpenSearch 服务的更新。

- [CT.OPENSEARCH.PR.8] 需要一个 Elasticsearch 服务域才能使用 TLSv1.2
- [CT.OPENSEARCH.PR.16] 需要亚马逊 OpenSearch服务域才能使用 TLSv1.2

我们更新了这两个控件的控件名称和构件，以与 Amazon S OpenSearch ervice 的最新版本保持一致。Amazon Service 现在支持传输层安全 (TLS) 1.3 版作为域终端节点安全的传输安全选项。

为了增加对这些控件的 TLSv1.3 的支持，我们更新了控件的构件和名称以反映控件的意图。他们现在评估服务域的最低 TLS 版本。要在您的环境中进行此更新，必须禁用并启用控件以部署最新的构件。

此变更不会影响其他主动控制措施。我们建议您查看这些控制措施，以确保它们符合您的控制目标。

如有疑问或疑虑，请联系 Supp AWS ort。

已弃用的控件不再可用

2024年3月12日

（ AWS Control Tower 着陆区无需更新。 ）

AWS Control Tower 已弃用某些控件。这些控件不再可用。

- CT.ATHENA.PR.1
- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

AWS Control Tower 支持在以下位置标记**EnabledControl**资源 AWS CloudFormation

2024年2月22日

（ AWS Control Tower 着陆区无需更新。 ）

此 AWS Control Tower 版本更新了EnabledControl资源的行为，以更好地与可配置控件保持一致，并提高了通过自动化管理您的 AWS Control Tower 环境的能力。在此版本中，您可以通过 AWS CloudFormation 模板向可配置EnabledControl资源添加标签。以前，您只能通过 AWS Control Tower 控制台和 API 添加标签。

AWS Control Tower GetEnabledControl 和 ListTagsforResource API 操作在此版本中进行了更新，因为它们依赖于EnabledControl资源功能。EnableControl

有关更多信息，请参阅 AWS Control Tower 中的标记EnabledControl资源和AWS CloudFormation 用户指南*EnabledControl*中的内容。

AWS Control Tower 支持用于 OU 注册和使用基准进行配置的 API

2024年2月14日

（AWS Control Tower 着陆区无需更新。）

这些 API 支持通过EnableBaseline调用进行编程 OU 注册。当您在组织单位上启用基准时，组织单位内的成员账户将注册到 AWS Control Tower 管理中。某些注意事项可能适用。例如，通过 AWS Control Tower 控制台注册 OU 可以启用可选控件和强制控件。调用 API 时，您可能需要完成一个额外的步骤才能启用可选控件。

AWS Control Tower 基准体现了 AWS Control Tower 管理组织单位和成员账户的最佳实践。例如，当您在 OU 上启用基准时，OU 内的成员账户会收到一组已定义的资源，包括、 AWS CloudTrail AWS Config、IAM Identity Center 和所需 AWS 的 IAM 角色。

特定的基准与特定的 AWS Control Tower 着陆区版本兼容。当您更改着陆区设置时，AWS Control Tower 可以将最新的兼容基准应用于您的着陆区。有关更多信息，请参阅 OU 基准和 landing zone 版本的兼容性。

此版本包括四个基本内容 基线的类型

- AWSControlTowerBaseline
- AuditBaseline
- LogArchiveBaseline
- IdentityCenterBaseline

借助新的 API 和定义的基准，您可以注册 OU 并自动执行 OU 配置工作流程。这些 API 还可以管理已受 AWS Control Tower 管理的 OU，因此您可以在着陆区更新后重新注册 OU。这些 API 包括对 AWS CloudFormation EnabledBaseline资源的支持，允许您使用基础设施即代码 (IaC) 管理组织单元。

基准 API

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: 对 OU 的基线采取行动。
- GetEnabledBaseline，ListEnabledBaselines: 发现已启用的基准的配置。
- GetBaselineOperation：查看特定基线操作的状态。
- ResetEnabledBaseline：使用已启用的基准修复 OU 上的资源偏移（包括嵌套的 OU 和强制控制偏差）。还修复了 landing-zone-level 区域拒绝控制的偏差
- GetBaseline，ListBaselines: 发现 AWS Control Tower 基准的内容。

要了解有关这些 API 的更多信息，请查看 AWS Control Tower 用户指南中的基准和 API 参考。除 GovCloud （美国）地区外，新 API 可在可用 AWS Control Tower AWS 区域 的地方使用。有关 AWS Con AWS 区域 trol Tower 可用区域的列表，请参阅 AWS 区域 表。

2023 年 1 月——至今

自 2023 年 1 月以来，AWS Control Tower 发布了以下更新：

- 过渡到新的 AWS Service Catalog 外部产品类型（第 3 阶段）
- AWS Control Tower 着陆区版本 3.3
- 过渡到新的 AWS Service Catalog 外部产品类型（第 2 阶段）
- AWS Control Tower 宣布了辅助数字主权的控制措施
- AWS Control Tower 支持着陆区 API
- AWS Control Tower 支持为已启用的控件添加标签
- AWS Control Tower 已在亚太地区（墨尔本）区域上线
- 过渡到新的 AWS Service Catalog 外部产品类型（第 1 阶段）
- 新的控制 API 可用
- AWS Control Tower 添加了其他控件
- 报告了新的漂移类型：已禁用可信访问
- 另外四个 AWS 区域
- AWS Control Tower 已在特拉维夫地区上市
- AWS Control Tower 推出了 28 种新的主动控制措施
- AWS Control Tower 弃用了两个控件
- AWS Control Tower 着陆区 3.2 版

- AWS Control Tower 根据 ID 处理账户
- AWS Control Tower 控件库中提供了其他 Security Hub 侦探控件
- AWS Control Tower 发布控制元数据表
- Terraform 支持 Account Factory 定制
- AWS 可用于 landing zone 的 IAM 身份中心自我管理
- AWS Control Tower 解决了 OU 的混合治理问题
- 还提供其他主动控制措施
- 更新了 Amazon EC2 主动控制措施
- 另外七个 AWS 区域 可用
- Account Factory for Terraform（AFT）账户自定义请求跟踪
- AWS Control Tower 着陆区版本 3.1
- 主动控制措施普遍可用

过渡到新的 AWS Service Catalog 外部产品类型（第 3 阶段）

2023年12月14日

（AWS Control Tower 着陆区无需更新。）

在创建新产品时，AWS Control Tower 不再支持 Terraform 开源作为产品类型（蓝图）。 AWS 账户有关更新账户蓝图的更多信息以及有关更新账户蓝图的说明，请查看过渡到 AWS Service Catalog 外部产品类型。

如果您不更新账户蓝图以使用外部产品类型，则只能更新或终止使用 Terraform 开源蓝图配置的帐户。

AWS Control Tower 着陆区版本 3.3

2023年12月14日

（需要将 AWS Control Tower 着陆区更新到 3.3 版。 有关信息，请参阅更新您的登录区）。

AWS Control Tower 审计账户中 S3 存储桶策略的更新

我们修改了 AWS Control Tower 在账户中部署的 Amazon S3 审计存储桶策略，因此任何写入权限都必须满足`aws:SourceOrgID`条件。在此版本中，只有当请求来自您的组织或组织单位 (OU) 时，AWS 服务才能访问您的资源。

您可以在 S3 存储桶策略的aws:SourceOrgID条件元素中使用条件键并将该值设置为您的组织 ID。此条件可确保 CloudTrail 只能代表组织内的账户将日志写入您的 S3 存储桶；它可以防止组织外部的 CloudTrail 日志写入您的 AWS Control Tower S3 存储桶。

我们进行此项更改是为了在不影响现有工作负载功能的情况下修复潜在的安全漏洞。要查看更新的政策，请参阅审计账户中的 Amazon S3 存储桶策略。

有关新条件密钥的更多信息，请参阅 IAM 文档和 IAM 博客文章，标题为 “对访问资源的 AWS 服务使用可扩展的控制”。

AWS Config SNS 主题中对政策的更新

我们在 SNS 主题的策略中添加了新的aws:SourceOrgID条件密钥。要查看更新的政策，请参阅 AWS Config SNS 主题政策。 AWS Config

着陆区 “Region Deny” 控件的更新

- 已移除discovery-marketplace:。此项行动属于aws-marketplace:*豁免范围。
- 新增了 quicksight:DescribeAccountSubscription

更新了 AWS CloudFormation 模板

我们更新了名为的堆栈的 AWS CloudFormation 模板，BASELINE-CLOUDTRAIL-MASTER使其在不使用 AWS KMS 加密时不会显示偏差。

过渡到新的 AWS Service Catalog 外部产品类型（第 2 阶段）

2023年12月7日

（AWS Control Tower 着陆区无需更新。）

HashiCorp 更新了他们的 Terraform 许可。因此，将对 Terraform 开源产品的支持 AWS Service Catalog 更改为一种名为 Exter nal 的新产品类型。

为避免中断您账户中的现有工作负载和 AWS 资源，请在 2023 年 12 月 14 日之前按照过渡到 AWS Service Catalog 外部产品类型中的 AWS Control Tower 过渡步骤进行操作。

AWS Control Tower 宣布了辅助数字主权的控制措施

2023年11月27日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 宣布推出 65 种新的 AWS托管控件，以帮助您满足数字主权要求。在此版本中，您可以在 AWS Control Tower 控制台的新数字主权组下发现这些控件。您可以使用这些控制措施来帮助防止数据驻留、精细访问限制、加密和弹性功能方面的操作并检测资源变化。这些控制措施旨在让您更轻松地满足大规模需求。有关数字主权控制的更多信息，请参阅增强数字主权保护的控件。

例如，您可以选择启用有助于强制执行加密和弹性策略的控件，例如要求 AWS AppSync API 缓存启用传输中的加密或要求跨多个可用区域部署 AWS Network Firew all。您还可以自定义 AWS Control Tower 区域拒绝控制，以应用最适合您独特业务需求的区域限制。

此版本带来了增强的 AWS Control Tower 区域拒绝功能。您可以在 OU 级别应用新的参数化区域拒绝控制，以提高治理的精度，同时在 landing zone 级别维持额外的区域治理。这种可自定义的区域拒绝控制可帮助您应用最适合您独特业务需求的区域限制。有关新的可配置区域拒绝控制的更多信息，请参阅应用于 OU 的区域拒绝控制。

作为新区域拒绝增强功能的新工具，此版本包括一个新的 APIUpdateEnabledControl，允许您将启用的控件重置为默认设置。在需要快速解决漂移问题或以编程方式保证控件不处于漂移状态的用例中，此 API 特别有用。有关新 API 的更多信息，请参阅 AWS Control Tower API 参考

新的主动控制措施

- CT.APIGATEWAY.PR.6: 要求 Amazon API Gateway REST 域使用指定最低 TLSv1.2 的 TLS 协议版本的安全策略
- CT.APPSYNC.PR.2: 要求将 AWS AppSync GraphQL API 配置为私有可见性
- CT.APPSYNC.PR.3: 要求不使用 API 密 AWS AppSync 钥对 GraphQL API 进行身份验证
- CT.APPSYNC.PR.4：需要 AWS AppSync GraphQL API 缓存才能启用传输中加密。
- CT.APPSYNC.PR.5：需要 AWS AppSync GraphQL API 缓存才能启用静态加密。
- CT.AUTOSCALING.PR.9: 需要通过 Amazon EC2 Auto Scaling 启动配置配置配置的 Amazon EBS 卷来加密静态数据
- CT.AUTOSCALING.PR.10: 要求 Amazon EC2 Auto Scaling 组在覆盖启动模板时仅使用 AWS Nitro 实例类型
- CT.AUTOSCALING.PR.11：在覆盖启动模板时，仅要求将支持实例间网络流量加密的 AWS Nitro 实例类型添加到 Amazon EC2 Auto Scaling 组中
- CT.DAX.PR.3：需要 DynamoDB 加速器集群使用传输层安全 (TLS) 对传输中的数据进行加密
- CT.DMS.PR.2: 需要 D AWS atabase Migration Service (DMS) 端点来加密源端点和目标端点的连接
- CT.EC2.PR.15：要求 Amazon EC2 实例在使用该`AWS::EC2::LaunchTemplate`资源类型创建实例时使用 AWS Nitro 实例类型

- CT.EC2.PR.16：要求 Amazon EC2 实例在使用`AWS::EC2::Instance`资源类型创建时使用 AWS Nitro 实例类型
- CT.EC2.PR.17: 需要一台 Amazon EC2 专用主机才能使用 AWS Nitro 实例类型
- CT.EC2.PR.18: 要求 Amazon EC2 队列仅覆盖那些具有 AWS Nitro 实例类型的启动模板
- CT.EC2.PR.19：要求 Amazon EC2 实例在使用资源类型创建时使用支持实例之间传输加密的 nitro 实例类型 `AWS::EC2::Instance`
- CT.EC2.PR.20：要求 Amazon EC2 队列仅覆盖那些支持实例之间传输加密的 AWS Nitro 实例类型的启动模板
- CT.ELASTICACHE.PR.8: 需要一个包含更高版本 Redis 的 Amazon ElastiCache 复制组才能激活 RBAC 身份验证
- CT.MQ.PR.1: 要求 Amazon MQ ActiveMQ 代理使用主动/备用部署模式以实现高可用性
- CT.MQ.PR.2: 要求 Amazon MQ Rabbit MQ 代理使用多可用区集群模式以实现高可用性
- CT.MSK.PR.1: 需要适用于 Apache Kafka 的亚马逊托管流媒体 Kafka (MSK) 集群才能在集群代理节点之间传输时强制加密
- CT.MSK.PR.2: 要求将适用于 Apache Kafka 的亚马逊托管流媒体 Kafka (MSK) 集群配置为禁用 PublicAccess
- CT.NETWORK-FIREWALL.PR.5: 要求在多个可用区域之间部署 AWS Network Firewall 防火墙
- CT.RDS.PR.26：需要 Amazon RDS 数据库代理才能要求传输层安全 (TLS) 连接
- CT.RDS.PR.27：需要 Amazon RDS 数据库集群参数组才能要求支持的引擎类型具有传输层安全 (TLS) 连接
- CT.RDS.PR.28：要求 Amazon RDS 数据库参数组要求支持的引擎类型需要传输层安全 (TLS) 连接
- CT.RDS.PR.29：要求未通过 “PubliclyAccessible” 属性将 Amazon RDS 集群配置为可公开访问
- CT.RDS.PR.30：要求 Amazon RDS 数据库实例将静态加密配置为使用您为支持的引擎类型指定的 KMS 密钥
- CT.S3.PR.12：要求 Amazon S3 接入点具有阻止公共访问 (BPA) 配置，并将所有选项都设置为 true

新的预防性控制措施

- CT.APPSYNC.PV.1要求将 AWS AppSync GraphQL API 配置为私有可见性
- CT.EC2.PV.1要求使用加密的 EC2 卷创建 Amazon EBS 快照
- CT.EC2.PV.2要求将连接的 Amazon EBS 卷配置为加密静态数据
- CT.EC2.PV.3要求 Amazon EBS 快照不能公开恢复

- CT.EC2.PV.4要求不调用 Amazon EBS 直接 API
- CT.EC2.PV.5禁止使用 Amazon EC2 虚拟机导入和导出
- CT.EC2.PV.6禁止使用已弃用的 Amazon EC2 RequestSpotFleet 和 API 操作 RequestSpotInstances
- CT.KMS.PV.1要求 AWS KMS 密钥政策中包含一项声明，将 AWS KMS 补助金的创建限制在 AWS 服务范围内
- CT.KMS.PV.2要求带有用于加密的 RSA 密钥材料的 AWS KMS 非对称密钥的密钥长度不能为 2048 位
- CT.KMS.PV.3要求在启用绕过策略锁定安全检查的情况下配置 AWS KMS 密钥
- CT.KMS.PV.4要求使用源自 Cl AWS KMS oudHSM 的密钥材料配置客户管理的密钥 (CMK) AWS
- CT.KMS.PV.5要求使用导入的密钥材料配置 AWS KMS 客户管理的密钥 (CMK)
- CT.KMS.PV.6要求使用来自外部密钥存储库 (XKS) 的密钥材料配置 AWS KMS 客户管理的密钥 (CMK)
- CT.LAMBDA.PV.1需要 AWS Lambda 函数 URL 才能使用 AWS 基于 IAM 的身份验证
- CT.LAMBDA.PV.2要求将 AWS Lambda 函数 URL 配置为仅供您内部的委托人访问 AWS 账户
- CT.MULTISERVICE.PV.1： AWS 根据对组织单位的请求拒绝访问权限 AWS 区域

增强您的数字主权治理态势的新侦探控制措施是 AWS Security Hub 服务托管标准 AWS Control Tower 的一部分。

新的侦探控件

- SH.ACM.2: 由 ACM 管理的 RSA 证书应使用至少 2,048 位的密钥长度
- SH.AppSync.5: AWS AppSync GraphQL API 不应使用 API 密钥进行身份验证
- SH.CloudTrail.6: 确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问：
- SH.DMS.9: DMS 端点应使用 SSL
- SH.DocumentDB.3: Amazon DocumentDB 手动集群快照不应公开
- SH.DynamoDB.3: DynamoDB 加速器 (DAX) 集群应进行静态加密
- SH.EC2.23: EC2 传输网关不应自动接受 VPC 连接请求
- SH.EKS.1: EKS 集群终端节点不应公开访问
- SH.ElastiCache.3： ElastiCache 复制组应启用自动故障转移
- SH.ElastiCache.4: ElastiCache 复制组应该已 encryption-at-rest 启用
- SH.ElastiCache.5: ElastiCache 复制组应该已 encryption-in-transit 启用

- SH.ElastiCache.6: 早期 Redis 版本的 ElastiCache 复制组应启用 Redis 身份验证
- SH.EventBridge.3: EventBridge 自定义事件总线应附加基于资源的策略
- SH.KMS.4: 应启用 AWS KMS 密钥轮换
- SH.Lambda.3: Lambda 函数应位于 VPC 中
- SH.MQ.5: ActiveMQ 代理应使用主动/备用部署模式
- SH.MQ.6: RabbitMQ 代理应使用集群部署模式
- SH.MSK.1: MSK 集群应在代理节点之间传输时进行加密
- SH.RDS.12: 应为 RDS 集群配置 IAM 身份验证
- SH.RDS.15：应为多个可用区配置 RDS 数据库集群
- SH.S3.17: S3 存储桶应使用密钥进行静态加 AWS KMS 密

有关添加到 AWS Security Hub 服务托管标准 AWS Control Tower 中的控件的更多信息，请参阅文档中适用于服务管理标准：AWS Control Tower 的 AWS Security Hub 控件。

有关不支持 AWS Security Hub 服务托管标准 AWS Control Tower 中某些控件的列表，请参阅不支持的区域。 AWS 区域

OU 级别的区域拒绝新增可配置控件

CT.MULTISERVICE.PV.1：此控件接受参数来指定豁免区域、IAM 委托人和允许在 OU 级别而不是整个 AWS Control Tower 着陆区执行的操作。它是一种预防性控制，由服务控制策略 (SCP) 实施。

有关更多信息，请参阅应用于 OU 的区域拒绝控制。

`UpdateEnabledControl` API

此 AWS Control Tower 版本为控件增加了以下 API 支持：

- 更新后的 `EnableControl` API 可以配置可配置的控件。
- 更新后的 `GetEnabledControl` API 显示已启用的控件上已配置的参数。
- 新 `UpdateEnabledControl` API 可以更改已启用的控件上的参数。

有关更多信息，请参阅 AWS Control Tower API 参考。

AWS Control Tower 支持着陆区 API

2023 年 11 月 26 日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在支持使用 API 配置和启动着陆区。您可以使用 API 创建、更新、获取、列出、重置和删除着陆区。

以下 API 使您能够使用 AWS CloudFormation 或以编程方式设置和管理着陆区。 AWS CLI

AWS Control Tower 支持以下 API 用于着陆区：

- `CreateLandingZone`—此 API 调用使用着陆区版本和清单文件创建着陆区。
- `GetLandingZoneOperation`— 此 API 调用返回指定着陆区操作的状态。
- `GetLandingZone`—此 API 调用返回有关指定 landing zone 的详细信息，包括版本、清单文件和状态。
- `UpdateLandingZone`—此 API 调用会更新 landing zone 版本或清单文件。
- `ListLandingZone`— 此 API 调用返回管理账户中设置的着陆区的一个着陆区标识符 (ARN)。
- `ResetLandingZone`—此 API 调用将着陆区重置为最新更新中指定的参数，这样可以修复漂移。如果着陆区尚未更新，则此调用会将着陆区重置为创建时指定的参数。
- `DeleteLandingZone`— 此 API 调用会停用着陆区。

要开始使用 landing zone API，请参阅使用 API 开始使用 AWS Control Tower。

AWS Control Tower 支持为已启用的控件添加标签

2023年11月10日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在支持通过 AWS Control Tower 控制台或通过 API 对已启用的控件进行资源标记。您可以为已启用的控件添加、移除或列出标签。

随着以下 API 的发布，您可以为在 AWS Control Tower 中启用的控件配置标签。标签帮助您管理、识别、组织、搜索和筛选资源。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。

AWS Control Tower 支持以下用于控制标签的 API：

- `TagResource`— 此 API 调用向 AWS Control Tower 中启用的控件添加标签。
- `UntagResource`— 此 API 调用会从 AWS Control Tower 中启用的控件中删除标签。
- `ListTagsForResource`— 此 API 调用返回在 AWS Control Tower 中启用的控件的标签。

AWS Control Tower 控制 API 可在提供 AWS Control Tower AWS 区域 的地方使用。有关可用 AWS Control Tower 的完整列表，请参阅AWS 区域表。 AWS 区域 有关 AWS Control Tower API 的完整列表，请参阅 API 参考。

AWS Control Tower 已在亚太地区（墨尔本）区域上线

2023年11月3日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 已在亚太地区（墨尔本）区域推出。

如果您已经在使用 AWS Control Tower，并且想要在您的账户中将其监管功能扩展到该区域，请前往 AWS Control Tower 控制面板中的设置页面，选择该区域，然后更新您的着陆区。在着陆区域更新后，您必须更新受 AWS Control Tower 管理的所有账户，以使您的账户和 OU 处于新区域的管理之下。有关更多信息，请参阅关于更新。

有关提供 AWS Control Tower 的区域的完整列表，请参阅AWS 区域 表。

过渡到新的 AWS Service Catalog 外部产品类型（第 1 阶段）

2023年10月31日

（AWS Control Tower 着陆区无需更新。）

HashiCorp 更新了他们的 Terraform 许可。因此， AWS Service Catalog 更新了对 Terraform 开源产品的支持，并将产品配置为一种名为 Exter nal 的新产品类型。

AWS Control Tower 不支持依赖于 AWS Service Catalog 外部产品类型的账户 Factory 自定义。为避免中断您账户中的现有工作负载和 AWS 资源，请在 2023 年 12 月 14 日之前按照以下建议顺序执行 AWS Control Tower 过渡步骤：

1. 升级现有的 Terraform 参考引擎 AWS Service Catalog ，使其包括对外部和 Terraform 开源产品类型的支持。有关更新 Terraform 参考引擎的说明，请查看存储库。AWS Service Catalog GitHub
2. 转到 AWS Service Catalog 并复制任何现有的 Terraform 开源蓝图，以使用新的外部产品类型。不要终止现有的 Terraform 开源蓝图。
3. 继续使用您现有的 Terraform 开源蓝图在 AWS Control Tower 中创建或更新账户。

新的控制 API 可用

2023年10月14日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在支持其他 API，您可以使用它来大规模部署和管理您的 AWS 控制塔控件。有关 AWS Control Tower 控制 API 的更多信息，请参阅 API 参考。

AWS Control Tower 添加了一个新的控制 API。

- `GetEnabledControl`— API 调用提供有关已启用控件的详细信息。

我们还更新了这个 API：

`ListEnabledControls`—此 API 调用列出了 AWS Control Tower 对指定组织单位及其包含的账户启用的控制措施。现在，它会在`EnabledControlSummary`对象中返回其他信息。

使用这些 API，您可以通过编程方式执行几种常见操作。例如：

- 从 AWS Control Tower 控件库中获取您已启用的所有控件的列表。
- 对于任何已启用的控件，您可以获取有关支持该控件的区域、控件的标识符 (ARN)、控件的偏移状态以及控件的状态摘要的信息。

AWS Control Tower 控制 API 可在提供 AWS Control Tower AWS 区域 的地方使用。有关可用 AWS Control Tower 的完整列表，请参阅AWS 区域表。 AWS 区域 有关 AWS Control Tower API 的完整列表，请参阅 API 参考。

AWS Control Tower 添加了其他控件

2023年10月5日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 宣布推出新的主动和侦查控制措施。

AWS Control Tower 中的主动控制是通过 Hook 实现的， AWS CloudFormation 挂钩可以在配置不合规的资源之前识别和屏 AWS CloudFormation 蔽它们。主动控制是对 AWS Control Tower 中现有的预防和侦查控制功能的补充。

新的主动控制措施

- [CT.ATHENA.PR.1] 要求亚马逊 Athena 工作组对静态的 Athena 查询结果进行加密
- [CT.ATHENA.PR.2] 要求亚马逊 Athena 工作组使用 (KMS) 密钥对静态的 Athena 查询结果进行加密 AWS Key Management Service

- [CT.CLOUDTRAIL.PR.4] 需要 AWS CloudTrail Lake 事件数据存储才能使用密 AWS KMS 钥启用静态加密
- [CT.DAX.PR.2] 要求 Amazon DAX 集群将节点部署到至少三个可用区
- [CT.EC2.PR.14] 需要通过 Amazon EC2 启动模板配置的 Amazon EBS 卷来加密静态数据
- [CT.EKS.PR.2] 要求将 Amazon EKS 集群配置为使用密 AWS 钥管理服务 (KMS) 密钥进行秘密加密
- [CT.ELASTICLOADBALANCING.PR.14] 需要 Network Load Balancer 才能激活跨区域负载平衡
- [CT.ELASTICLOADBALANCING.PR.15] 要求 Elastic Load Balancing v2 目标组不要明确禁用跨区域负载平衡
- [CT.EMR.PR.1] 要求将亚马逊 EMR (EMR) 安全配置配置为加密 Amazon S3 中的静态数据
- [CT.EMR.PR.2] 要求将 Amazon EMR (EMR) 安全配置配置为使用密钥对 Amazon S3 中的静态数据进行加密 AWS KMS
- [CT.EMR.PR.3] 要求将 Amazon EMR (EMR) 安全配置配置为使用密钥的 EBS 卷本地磁盘加密 AWS KMS
- [CT.EMR.PR.4] 要求将 Amazon EMR (EMR) 安全配置配置为对传输中的数据进行加密
- [CT.GLUE.PR.1] 需要 AWS Glue 作业才能关联安全配置
- [CT.GLUE.PR.2] 需要使用 AWS Glue 安全配置才能使用 AWS KMS 密钥对 Amazon S3 目标中的数据进行加密
- [CT.KMS.PR.2] 要求带有用于加密的 RSA 密钥材料的 AWS KMS 非对称密钥的密钥长度必须大于 2048 位
- [CT.KMS.PR.3] 要求 AWS KMS 密钥政策包含一项声明，将 AWS KMS 补助金的创建仅限于 AWS 服务
- [CT.LAMBDA.PR.4] 需要 AWS Lambda 图层权限才能向 AWS 组织或特定 AWS 账户授予访问权限
- [CT.LAMBDA.PR.5] 需要 AWS Lambda 函数 URL 才能使用 AWS 基于 IAM 的身份验证
- [CT.LAMBDA.PR.6] 需要 AWS Lambda 函数 URL CORS 策略来限制对特定来源的访问
- [CT.NEPTUNE.PR.4] 需要 Amazon Neptune 数据库集群才能为审计 CloudWatch 日志启用亚马逊日志导出功能
- [CT.NEPTUNE.PR.5] 要求 Amazon Neptune 数据库集群将备份保留期设置为大于或等于七天
- [CT.REDSHIFT.PR.9] 要求将 Amazon Redshift 集群参数组配置为使用安全套接字层 (SSL) 对传输中的数据进行加密

这些新的主动控制措施可在提供 AWS Control Tower 的商业 AWS 区域 版中使用。有关这些控制的更多详细信息，请参阅主动控制。有关控件可用位置的更多详细信息，请参阅控件限制。

新的侦探控件

在 Sec urity Hub 服务托管标准：AWS Control Tower 中添加了新的控件。这些控制措施可帮助您增强治理状况。在任何特定 OU 上启用它们后，它们将作为 Sec urity Hub 服务托管标准：AWS Control Tower 的一部分。

- [SH.Athena.1] Athena 工作组应进行静态加密
- [SH.Neptune.1] 应对 Neptune 数据库集群进行静态加密
- [SH.Neptune.2] Neptune 数据库集群应将审核日志发布到日志 CloudWatch
- [SH.Neptune.3] Neptune 数据库集群快照不应公开
- [SH.Neptune.4] Neptune 数据库集群应启用删除保护
- [SH.Neptune.5] Neptune 数据库集群应启用自动备份
- [SH.Neptune.6] 应对 Neptune 数据库集群快照进行静态加密
- [SH.Neptune.7] Neptune 数据库集群应启用 IAM 数据库身份验证
- [SH.Neptune.8] 应将 Neptune 数据库集群配置为将标签复制到快照
- [SH.RDS.27] RDS 数据库集群应进行静态加密

大多数提供 AWS Control Tower AWS 区域 的地方都可以使用新的 AWS Security Hub 侦探控件。有关这些控制措施的更多详细信息，请参阅适用于服务托管标准的控制措施：AWS Control Tower。有关控件可用位置的更多详细信息，请参阅控制限制。

报告了新的漂移类型：已禁用可信访问

2023年9月21日

（AWS Control Tower 着陆区无需更新。）

设置 AWS Control Tower 着陆区后，您可以在中禁用对 AWS Control Tower 的可信访问 AWS Organizations。但是，这样做会导致漂移。

对于禁用可信访问的漂移类型，AWS Control Tower 会在发生此类漂移时通知您，因此您可以修复 AWS Control Tower 着陆区。有关更多信息，请参阅治理偏差的类型。

另外四个 AWS 区域

2023年9月13日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现已在亚太地区（海得拉巴）、欧洲（西班牙和苏黎世）和中东（阿联酋）上市。

如果您已经在使用 AWS Control Tower，并且想要在您的账户中将其监管功能扩展到该区域，请前往 AWS Control Tower 控制面板中的设置页面，选择该区域，然后更新您的着陆区。在着陆区域更新后，您必须更新受 AWS Control Tower 管理的所有账户，以使您的账户和 OU 处于新区域的管理之下。有关更多信息，请参阅关于更新。

有关提供 AWS Control Tower 的区域的完整列表，请参阅AWS 区域 表。

AWS Control Tower 已在特拉维夫地区上市

2023年8月28日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 宣布在以色列（特拉维夫）地区上市。

如果您已经在使用 AWS Control Tower，并且想要在您的账户中将其监管功能扩展到该区域，请前往 AWS Control Tower 控制面板中的设置页面，选择该区域，然后更新您的着陆区。在着陆区域更新后，您必须更新受 AWS Control Tower 管理的所有账户，以使您的账户和 OU 处于新区域的管理之下。有关更多信息，请参阅关于更新。

有关提供 AWS Control Tower 的区域的完整列表，请参阅AWS 区域 表。

AWS Control Tower 推出了 28 种新的主动控制措施

2023年7月24日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 正在添加 28 个新的主动控制措施，以帮助您管理 AWS 环境。

主动控制通过在配置不合规的资源之前将其阻止，从而增强多账户 AWS 环境中 AWS Control Tower 的治理能力。这些控件有助于管理亚马逊、亚马逊 Neptune CloudWatch、亚马逊和亚马逊 Docum ElastiCache entDB AWS Step Functions等 AWS 服务。新的控制措施可帮助您实现控制目标，例如建立日志和监控、加密静态数据或提高弹性。

以下是新控件的完整列表：

- [CT.APPSYNC.PR.1] 需要 G AWS AppSync raphQL API 才能启用日志记录

- [CT.CLOUDWATCH.PR.1] 要求 CloudWatch亚马逊警报为警报状态配置操作
- [CT.CLOUDWATCH.PR.2] 要求 CloudWatch亚马逊日志组保留至少一年
- [CT.CLOUDWATCH.PR.3] 要求使用 KMS 密钥对 CloudWatch亚马逊日志组进行静态加密 AWS
- [CT.CLOUDWATCH.PR.4] 需要激活亚马逊警报操作 CloudWatch
- [CT.DOCUMENTDB.PR.1] 要求对亚马逊文档数据库集群进行静态加密
- [CT.DOCUMENTDB.PR.2] 要求亚马逊 DocumentDB 集群启用自动备份
- [CT.DYNAMODB.PR.2] 要求使用密钥对亚马逊 DynamoDB 表进行静态加密 AWS KMS
- [CT.EC2.PR.13] 要求亚马逊 EC2 实例启用详细监控
- [CT.EKS.PR.1] 要求将 Amazon EKS 集群配置为禁用对集群 Kubernetes API 服务器终端节点的公共访问权限
- [CT.ELASTICACHE.PR.1] 要求 ElastiCache 亚马逊版 R edis 集群激活自动备份
- [CT.ELASTICACHE.PR.2] 要求 ElastiCache 亚马逊版 Redis 集群激活自动次要版本升级
- [CT.ELASTICACHE.PR.3] 要求 ElastiCache 亚马逊版 Redis 复制组激活自动故障转移
- [CT.ELASTICACHE.PR.4] 要求亚马逊 ElastiCache 复制组激活静态加密
- [CT.ELASTICACHE.PR.5] 要求 ElastiCache 亚马逊版 Redis 复制组激活传输中的加密
- [CT.ELASTICACHE.PR.6] 要求亚马逊 ElastiCache 缓存集群使用自定义子网组
- [CT.ELASTICACHE.PR.7] 要求由早期 Redis 版本组成的 ElastiCache 亚马逊复制组进行 Redis AUTH 身份验证
- [CT.ELASTICBEANSTALK.PR.3] 需要 Elastic Beanstalk 环境才能进行日志 AWS 配置
- [CT.LAMBDA.PR.3] 要求 AWS Lambda 函数位于客户管理的亚马逊虚拟私有云 (VPC) 中 Amazon Virtual Private Cloud
- [CT.NEPTUNE.PR.1] 要求亚马逊 Ne ptune 数据库集群具有 (IAM) 数据库身份验证 AWS Identity and Access Management
- [CT.NEPTUNE.PR.2] 要求亚马逊 Neptune 数据库集群启用删除保护
- [CT.NEPTUNE.PR.3] 要求亚马逊 Ne ptune 数据库集群启用存储加密
- [CT.REDSHIFT.PR.8] 要求对亚马逊 Red shift 集群进行加密
- [CT.S3.PR.9] 要求亚马逊 S3 存储桶激活 S3 对象锁
- [CT.S3.PR.10] 要求 Amazon S 3 存储桶使用密钥配置服务器端加密 AWS KMS
- [CT.S3.PR.11] 要求 Amazon S 3 存储桶启用版本控制
- [CT.STEPFUNCTIONS.PR.1] 要求状态机激活日志 AWS Step Functions 记录

- [CT.STEPFUNCTIONS.PR.2] 要求状态机激活跟 AWS Step Functions 踪 AWS X-Ray

AWS Control Tower 中的主动控制是通过 Hook 实现的， AWS CloudFormation 挂钩可以在配置不合规的资源之前识别和屏 AWS CloudFormation 蔽它们。主动控制是对 AWS Control Tower 中现有的预防和侦查控制功能的补充。

这些新的主动控制措施在 AWS Control Tower 的所有 AWS 区域 可用区域都可用。有关这些控制的更多详细信息，请参阅主动控制。

AWS Control Tower 弃用了两个控件

2023年7月18日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 会定期审查其安全控制措施，以确保它们是最新的，并且仍被视为最佳实践。以下两个控件已被弃用，自 2023 年 7 月 18 日起生效，并将从 2023 年 8 月 18 日起从控件库中删除。您无法再对任何组织单位启用这些控件。您可以选择在移除日期之前停用这些控件。

- [SH.S3.4] S3 存储桶应启用服务器端加密
- [CT.S3.PR.7] 要求 Amazon S3 存储桶配置服务器端加密

弃用原因

自 2023 年 1 月起，Amazon S3 在所有新的和现有的未加密存储桶上配置了默认加密，以应用服务器端加密，将 S3 托管密钥 (SSE-S3) 作为上传到这些存储桶的新对象的基本加密级别。未对已有 SSE-S3 或配置了密 AWS 钥管理服务 (AWS KMS) 密钥 (SSE-KMS) 的服务器端加密的现有存储桶的默认加密配置进行任何更改。

AWS Control Tower 着陆区 3.2 版

2023 年 6 月 16 日

（需要将 AWS Control Tower 着陆区更新到 3.2 版。 有关信息，请参阅更新您的登录区）。

AWS Control Tower 着陆区版本 3.2 将 AWS Security Hub 服务管理标准：AWS Control Tower 中的控件全面推出。它引入了在 AWS Control Tower 控制台中查看属于该标准的控件的偏移状态的功能。

此更新包括一个新的服务相关角色 (SLR)，名为。AWSServiceRoleForAWSControlTower该角色通过创建 EventBridge 托管规则来协助 AWS Control Tower，该规则AWSControlTowerManagedRule在每

个成员账户中名为。该托管规则收集 AWS Security Hub 查找事件，通过 AWS Control Tower 可以确定控制偏差。

该规则是 AWS Control Tower 创建的第一条托管规则。该规则不是由堆栈部署的；而是直接从 EventBridge API 部署的。您可以在 EventBridge 控制台中或通过 EventBridge API 查看规则。如果该`managed-by`字段已填充，它将显示 AWS Control Tower 的服务主体。

以前，AWS Control Tower 负责在成员账户中执行操作。AWSControlTowerExecution这一新的角色和规则更符合在多账户 AWS 环境中执行操作时允许最低权限的最佳实践原则。新角色提供范围缩小权限，这些权限特别允许：在成员账户中创建托管规则、维护托管规则、通过 SNS 发布安全通知以及验证偏差。有关更多信息，请参阅 AWSServiceRoleForAWSControlTower。

landing zone 3.2 更新还在管理账户中加入了一个新 StackSet 资源`BP_BASELINE_SERVICE_LINKED_ROLE`，该账户最初部署的是服务相关角色。

在报告 Security Hub 控制偏差（在着陆区 3.2 及更高版本中）时，AWS Control Tower 会收到来自 Security Hub 的每日状态更新。尽管控件在每个受管控区域都处于活动状态，但 AWS Control Tower 仅向 AWS Control Tower 主区域发送 AWS Security Hub 发现事件。有关更多信息，请参阅 S ecurity Hub 控制偏差报告。

更新 “区域拒绝” 控件

此 landing zone 版本还包括对 “区域拒绝” 控件的更新。

已添加全球服务和 API

- AWS Billing and Cost Management (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) 以允许在成员账户中查看全球事件。
- AWS 整合账单 (`consolidatedbilling:*`)
- AWS 管理控制台 Mobile Application (`consoleapp:*`)
- AWS 免费套餐 (`freetier:*`)
- AWS 开票 (`invoicing:*`)
- AWS IQ (`iq:*`)
- AWS 用户通知 (`notifications:*`)
- AWS 用户通知联系人 (`notifications-contacts:*`)
- Amazon Payments (`payments:*`)
- AWS 税务设置 (`tax:*`)

已移除全球服务和 API

- 已移除，`s3:GetAccountPublic`因为它不是有效的操作。
- 已移除，`s3:PutAccountPublic`因为它不是有效的操作。

AWS Control Tower 根据 ID 处理账户

2023年6月14日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在通过跟踪账户 ID 而不是账户的电子邮件地址来创建和管理您在 Account Factory 中创建的账户。 AWS

配置账户时，账户申请者必须始终拥有`CreateAccount`和`DescribeCreateAccountStatus`权限。此权限集是管理员角色的一部分，当请求者担任管理员角色时，它会自动授予。如果您委托配置账户的权限，则可能需要直接为账户申请者添加这些权限。

AWS Control Tower 控件库中提供了其他 Security Hub 侦探控件

2023年6月12日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 在 AWS Control Tower 控件库中添加了十个新的 AWS Security Hub 侦探控件。这些新控件针对的是诸如 API Gateway AWS CodeBuild、Amazon Elastic Compute Cloud (EC2)、亚马逊弹性负载均衡器、亚马逊 Redshift、亚马逊和。 SageMaker AWS WAF这些新控件通过实现控制目标（例如建立日志记录和监控、限制网络访问和加密静态数据）来帮助您增强治理状态。

在任何特定 OU 上启用这些控件后，这些控件将作为 Sec urity Hub 服务托管标准：AWS Control Tower 的一部分。

- [sh.account.1] 应为以下人员提供安全联系信息 AWS 账户
- [sh.apiGateway.8] API Gateway.8] API Gateway 路由应指定授权类型
- [sh.apigateway.9] 应该为 API Gat eway V2 Stages 配置访问日志
- [SH。 CodeBuild.3] 应 CodeBuild 对 S3 日志进行加密
- [SH.EC2.25] EC2 启动模板不应为网络接口分配公有 IP
- [SH.ELB.1] 应将 Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS

- [sh.redshift.10] Reds hift 集群应该在静态状态下进行加密
- [SH。 SageMaker.2] SageMaker 笔记本实例应在自定义 VPC 中启动
- [SH。 SageMaker.3] 用户不应拥有 SageMaker 笔记本实例的 root 访问权限
- [SH.WAF.10] WAFV2 Web ACL 应至少有一个规则或规则组

新的 AWS Security Hub 侦探控件可在所有可用 AWS Control Tower AWS 区域 的地方使用。有关这些控制措施的更多详细信息，请参阅适用于服务托管标准的控制措施：AWS Control Tower。

AWS Control Tower 发布控制元数据表

2023年6月7日

（ AWS Control Tower 着陆区无需更新。 ）

AWS Control Tower 现在在已发布的文档中提供了完整的控制元数据表。在使用控件 API 时，您可以查找每个控件的 API Control Identifier，这是与每个控件关联的唯一 ARN。 AWS 区域这些表格包括每项控制措施所涵盖的框架和控制目标。以前，此信息仅在控制台中可用。

这些表还包括属于AWS Security Hub 服务管理标准：AWS Control Tower 的 Security Hub 控件的元数据。有关完整详细信息，请参阅控件元数据表。

有关控件标识符的简短列表和一些用法示例，请参阅 API 和控件的资源标识符。

Terraform 支持 Account Factory 定制

2023年6月6日

（ AWS Control Tower 着陆区无需更新。 ）

AWS Control Tower 通过账户工厂定制 (AFC) 为 Terraform 提供单区域支持。从本版本开始，您可以在 Terraform 开源中同时使用 AWS Control Tower 和 Service Catalog 来定义 AFC 账户蓝图。在 AWS Control Tower 中配置资源之前 AWS 账户，您可以自定义您的新资源和现有资源。默认情况下，此功能允许您使用 Terraform 在 AWS Control Tower 主区域部署和更新账户。

账户蓝图描述了置备时所需的特定资源和配置。 AWS 账户 您可以将蓝图用作模板来大规模创建多个 AWS 账户 蓝图。

要开始使用 Terraform 参考引擎，请开启。 GitHub参考引擎配置了 Terraform 开源引擎与 Service Catalog 配合使用所需的代码和基础架构。此一次性设置过程需要几分钟。之后，您可以在 Terraform 中定义您的自定义账户要求，然后使用定义明确的 AWS Control Tower 账户出厂工作流程部署您的账

户。更喜欢使用 Terraform 的客户可以通过 AFC 大规模使用 AWS Control Tower 账户自定义功能，并在每个账户配置完毕后立即访问该账户。

要了解如何创建这些自定义项，请参阅 Service Catalog 文档中的创建产品和 Terraform 开源入门。此功能在所有可用 AWS Control Tower AWS 区域 的地方都可用。

AWS 可用于 landing zone 的 IAM 身份中心自我管理

2023年6月6日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在支持为 AWS Control Tower 着陆区选择身份提供商，您可以在设置或更新期间对其进行配置。根据使用多个账户组织 AWS 环境中定义的最佳实践指南，默认情况下，着陆区域选择使用 AWS IAM Identity Center。你现在有三种选择：

- 您可以接受默认设置并允许 AWS Control Tower 为您设置和管理 AWS IAM 身份中心。
- 您可以选择自行管理 AWS IAM 身份中心，以反映您的特定业务需求。
- 如果需要，您可以选择通过IAM Identity Center连接第三方身份提供商并对其进行自我管理。如果您的监管环境要求您使用特定的提供商，或者如果您在 AWS IAM Identity Center 不可用的 AWS 区域地区开展业务，则应使用身份提供商可选性。

有关更多信息，请参阅 IAM 身份中心指南。

不支持在账户级别选择身份提供商。此功能仅适用于整个着陆区。AWS Control Tower 身份提供商选项在所有可用 AWS Control Tower AWS 区域 的地方都可用。

AWS Control Tower 解决了 OU 的混合治理问题

2023年6月1日

（AWS Control Tower 着陆区无需更新。）

在此版本中，如果组织单位 (OU) 处于混合治理状态，AWS Control Tower 将阻止控制部署到该组织单位 (OU)。如果在 AWS Control Tower 将监管范围扩展到新的或移除监管后仍未更新账户 AWS 区域，则组织单位中就会出现混合治理。此版本可帮助您使该 OU 的成员账户保持统一合规。有关更多信息，请参阅 配置区域时避免混合治理。

还提供其他主动控制措施

2023年5月19日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 正在添加 28 个新的主动控制措施，以帮助您管理多账户环境并实现特定的控制目标，例如静态数据加密或限制网络访问。主动控制是通过 AWS CloudFormation 挂钩实现的，挂钩可以在配置资源之前检查您的资源。新的控件可以帮助管理亚马逊 AWS OpenSearch 服务、Amazon EC2 Auto Scaling、亚马逊 SageMaker、Amazon API Gateway 和亚马逊关系数据库服务 (RDS) 等服务。

所有提供 AWS Control Tower AWS 区域 的商业版都支持主动控制。

亚马逊 OpenSearch 服务

- [CT.OPENSEARCH.PR.1] 需要 Elasticsearch 域来加密静态数据
- [CT.OPENSEARCH.PR.2] 要求在用户指定的亚马逊 VPC 中创建 Elasticsearch 域
- [CT.OPENSEARCH.PR.3] 需要一个 Elasticsearch 域来加密节点之间发送的数据
- [CT.OPENSEARCH.PR.4] 需要 Elasticsearch 域才能将错误日志发送到亚马逊日志 CloudWatch
- [CT.OPENSEARCH.PR.5] 需要 Elasticsearch 域才能将审核日志发送到亚马逊日志 CloudWatch
- [CT.OPENSEARCH.PR.6] 要求一个 Elasticsearch 域具有区域感知能力和至少三个数据节点
- [CT.OPENSEARCH.PR.7] 要求一个 Elasticsearch 域至少有三个专用的主节点
- [CT.OPENSEARCH.PR.8] 需要一个 Elasticsearch 服务域才能使用 TLSv1.2
- [CT.OPENSEARCH.PR.9] 要求使用 OpenSearch 亚马逊服务域来加密静态数据
- [CT.OPENSEARCH.PR.10] 要求在用户指定的 OpenSearch 亚马逊 VPC 中创建亚马逊服务域
- [CT.OPENSEARCH.PR.11] 需要 OpenSearch 亚马逊服务域来加密节点之间发送的数据
- [CT.OPENSEARCH.PR.12] 需要亚马逊服务域才能将错误日志发送到 OpenSearch 亚马逊日志 CloudWatch
- [CT.OPENSEARCH.PR.13] 需要亚马逊服务域才能将审核日志发送到 OpenSearch 亚马逊日志 CloudWatch
- [CT.OPENSEARCH.PR.14] 要求 OpenSearch 亚马逊服务域具有区域感知能力和至少三个数据节点
- [CT.OPENSEARCH.PR.15] 要求 OpenSearch 亚马逊服务域名使用精细的访问控制
- [CT.OPENSEARCH.PR.16] 需要亚马逊服务域名才能使用 TLSv1.2 OpenSearch

Amazon EC2 Auto Scaling

- [CT.AUTOSCALING.PR.1] 要求一个 Amazon EC2 Auto Scaling 组拥有多个可用区

- [CT.AUTOSCALING.PR.2] 需要亚马逊 EC2 Auto Scaling 组启动配置才能为 imdsv2 配置亚马逊 EC2 实例
- [CT.AUTOSCALING.PR.3] 需要 Amazon EC2 Auto Scaling 启动配置才能设置单跳元数据响应限制
- [CT.AUTOSCALING.PR.4] 要求与亚马逊 Elastic Load Balancing (ELB) 关联的 Amazon EC2 Auto Scaling 组激活 ELB 运行状况检查
- [CT.AUTOSCALING.PR.5] 要求亚马逊 EC2 Auto Scaling 组启动配置中没有带有公有 IP 地址的亚马逊 EC2 实例
- [CT.AUTOSCALING.PR.6] 要求任何 Amazon EC2 Auto Scaling 组使用多种实例类型
- [CT.AUTOSCALING.PR.8] 要求亚马逊 EC2 Auto Scaling 组配置 EC2 启动模板

Amazon SageMaker

- [CT.SAGEMAKER.PR.1] 需要亚马逊 SageMaker 笔记本实例以防止直接访问互联网
- [CT.SAGEMAKER.PR.2] 要求在自定义 Amazon VPC 中 SageMaker 部署亚马逊笔记本实例
- [CT.SAGEMAKER.PR.3] 要求禁止亚马逊 SageMaker 笔记本实例具有根访问权限

Amazon API Gateway

- [CT.APIGATEWAY.PR.5] 要求亚马逊 API Gateway V2 Websocket 和 HTTP 路由来指定授权类型

Amazon Relational Database Service (RDS)

- [CT.RDS.PR.25] 要求 Amazon RDS 数据库集群配置日志记录

有关更多信息，请参阅主动控制。

更新了 Amazon EC2 主动控制措施

2023年5月2日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 更新了两个主动控制措施：CT.EC2.PR.3和CT.EC2.PR.4。

对于更新的CT.EC2.PR.3控件，除非是端口 80 或 443，否则任何 AWS CloudFormation 引用安全组资源前缀列表的部署都将被禁止部署。

对于更新的CT.EC2.PR.4控件，如果端口为
3389、20、23、110、143、3306、8080、1433、9200、9300、25、445、135、21、1434、433、434、43
则任何引用安全组资源前缀列表的 AWS CloudFormation 部署都将被阻止。

另外七个 AWS 区域 可用

2023年4月19日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现已在另外七个地区推出 AWS 区域：北加州（旧金山）、亚太地区（香港、雅加达和大阪）、欧洲（米兰）、中东（巴林）和非洲（开普敦）。AWS Control Tower 的这些其他区域（称为选择加入区域）默认处于非活动状态，但美国西部（加利福尼亚北部）区域除外，该区域默认处于活动状态。

AWS Control Tower 中的某些控件在 AWS 区域 其中一些提供 AWS Control Tower 的额外区域中不起作用，因为这些区域不支持所需的基础功能。有关更多信息，请参阅 控制限制。

在这些新区域中，亚太地区（雅加达和大阪）不提供氟氯化碳。其他版本的可用性保持 AWS 区域 不变。

有关 AWS Control Tower 如何管理区域和控制的限制的更多信息，请参阅激活 AWS 选择加入区域的注意事项。

AFT 所需的 vPCE 终端节点在中东（巴林）区域不可用。在该区域部署 AFT 的客户需要使用参数进行部署`aft_vpc_endpoints=false`。有关更多信息，请参阅自述文件中的参数。

由于亚马逊 EC2 的限制，AWS Control Tower VPC 在美国西部（加利福尼亚北部）地区有两个可用区。`us-west-1`在美国西部（加利福尼亚北部），六个子网被划分为两个可用区。有关更多信息，请参阅 AWS Control Tower 和 VPC 概述。

AWS Control Tower 为`AWSControlTowerServiceRolePolicy`其添加了新的权限`EnableRegion`，允许 AWS Control Tower 调用 AWS 账户管理服务实施的`ListRegions`、和`GetRegionOptStatus` API，从而使这些额外权限 AWS 区域 可用于您在着陆区域中的共享账户（管理账户、日志存档账户、审计账户）和您的 OU 成员账户。有关更多信息，请参阅 AWS Control Tower 的托管策略。

Account Factory for Terraform（AFT）账户自定义请求跟踪

2023年2月16日

AFT 支持账户自定义请求跟踪。每次您提交账户自定义请求时，AFT 都会生成一个唯一的跟踪令牌，该令牌通过 AFT 自定义 AWS Step Functions 状态机传递，该状态机将令牌记录为其执行的一部分。您可以使用 Amazon CloudWatch Logs 见解查询来搜索时间戳范围并检索请求令牌。因此，您可以看到令牌附带的有效负载，因此您可以在整个 AFT 工作流程中跟踪您的账户自定义请求。有关 AFT 的更多信息，请参阅适用于 T erraform 的 AWS Control Tower Account Factory 概述。有关 CloudWatch 日志和 Step Functions 的信息，请参阅以下内容：

- 什么是 Amazon CloudWatch 日志？ 在 Amazon CloudWatch 日志用户指南中
- 什么是 AWS Step Functions？ 在《AWS Step Functions 开发者指南》中

AWS Control Tower 着陆区版本 3.1

2023 年 2 月 9 日

（需要将 AWS Control Tower 着陆区更新到 3.1 版。 有关信息，请参阅更新您的登录区）

AWS Control Tower 着陆区版本 3.1 包括以下更新：

- 在此版本中，AWS Control Tower 会停用访问日志存储桶（访问日志存档账户中存储访问日志的 Amazon S3 存储桶）的不必要访问日志记录，同时继续为 S3 存储桶启用服务器访问日志记录。此版本还包括对 “区域拒绝” 控件的更新，允许对全球服务执行其他操作，例如 AWS Support 计划和 AWS Artifact。
- 停用 AWS Control Tower 访问日志存储桶的服务器访问日志会导致 Security Hub 为日志存档账户的访问日志存储桶创建调查结果， AWS Security Hub 根据规则，应启用 [S3.9] S3 存储桶服务器访问日志记录。为了与 Security Hub 保持一致，我们建议您按照 Security Hub 对此规则的描述中所述，取消此特定发现。有关其他信息，请参阅有关隐藏查找结果的信息。
- 在 3.1 版本中，日志存档账户中（常规）日志存储桶的访问日志记录保持不变。根据最佳实践，该存储桶的访问事件将作为日志条目记录在访问日志存储桶中。有关访问日志的更多信息，请参阅 Amazon S3 文档中的使用服务器访问日志记录请求。
- 我们更新了 “区域拒绝” 控件。此更新允许更多全球服务执行操作。有关此 SCP 的详细信息，请参阅AWS 根据请求拒绝访问 AWS 区域和增强数据驻留保护的控制措施。

  添加了全球服务：

  - AWS Account Management (`account:*`)
  - AWS 激活 (`activate:*`)
  - AWS Artifact (`artifact:*`)
  - AWS Billing Conductor (`billingconductor:*`)

- AWS Compute Optimizer (compute-optimizer:*)
- AWS Data Pipeline (datapipeline:GetAccountLimits)
- AWS Device Farm(devicefarm:*)
- AWS Marketplace (discovery-marketplace:*)
- 亚马逊 ECR () ecr-public:*
- AWS License Manager (license-manager:ListReceivedLicenses)
- AWS Lightsail () lightsail:Get*
- AWS 资源探索器 (resource-explorer-2:*)
- 亚马逊 S3 (s3:CreateMultiRegionAccessPoint,s3:GetBucketPolicyStatus,s3:PutMultiRegionAcc
- AWS Savings Plans (savingsplans:*)
- IAM 身份中心 (sso:*)
- AWS Support App (supportapp:*)
- AWS Support 计划 (supportplans:*)
- AWS 可持续发展 (sustainability:*)
- AWS Resource Groups Tagging API (tag:GetResources)
- AWS Marketplace 供应商见解 (vendor-insights:ListEntitledSecurityProfiles)

主动控制措施普遍可用

2023年1月24日

（AWS Control Tower 着陆区无需更新。）

之前宣布的预览状态下的可选主动控制现已正式推出。这些控制措施之所以被称为主动控制，是因为它们会在部署资源之前检查您的资源，以确定新资源是否符合在您的环境中激活的控制措施。有关更多信息，请参阅 全面的控制有助于 AWS 资源调配和管理。

2022 年 1 月至 12 月

2022 年，AWS Control Tower 发布了以下更新：

- 并发账户操作
- Account Factory 定制 (AFC)

- 全面的控制有助于 AWS 资源调配和管理
- 所有规则的合规性状态均 AWS Config 可查看
- 控件和新 AWS CloudFormation 资源的 API
- cfCT 支持删除堆栈集
- 自定义日志保留
- 角色偏差修复可用
- AWS Control Tower 着陆区 3.0 版
- 组织页面结合了 OU 和账户的视图
- 更轻松地注册和更新个人会员账户
- AFT 支持对共享的 AWS Control Tower 账户进行自动定制
- 所有可选控件的并行操作
- 现有的安全和日志账户
- AWS Control Tower 着陆区版本 2.9
- AWS Control Tower 着陆区 2.8 版

并发账户操作

2022年12月16日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在支持账户工厂中的并发操作。您一次最多可以创建、更新或注册五 (5) 个账户。连续提交最多五个操作并查看每个请求的完成状态，同时您的账户将在后台完成构建。例如，在更新其他账户或重新注册整个组织单位 (OU) 之前，您不必再等待每个流程完成。

Account Factory 定制 (AFC)

2022年11月28日

（AWS Control Tower 着陆区无需更新。）

账户出厂自定义允许您在 AWS Control Tower 控制台中自定义新账户和现有账户。这些新的自定义功能使您可以灵活地定义账户蓝图，这些蓝图是包含在专门的 Service Catalog 产品中的 AWS CloudFormation 模板。蓝图提供完全自定义的资源和配置。您也可以选择使用由 AWS 合作伙伴构建和管理的预定义蓝图，以帮助您针对特定用例自定义账户。

以前，AWS Control Tower 账户工厂不支持在控制台中自定义账户。通过此次账户工厂更新，您可以预定义账户要求并将其作为明确定义的工作流程的一部分来实施。您可以应用蓝图来创建新账户、将其他 AWS 账户注册到 AWS Control Tower 以及更新现有的 AWS Control Tower 账户。

在账户工厂中配置、注册或更新账户时，您将选择要部署的蓝图。蓝图中指定的资源是在您的账户中配置的。当您的账户完成构建后，所有自定义配置均可立即使用。

要开始自定义帐户，您可以在 Service Catalog 产品中为预期用例定义资源。您也可以从 AWS 入门库中选择合作伙伴管理的解决方案。有关更多信息，请参阅 使用 Account Factory 自定义 (AFC) 自定义账户。

全面的控制有助于 AWS 资源调配和管理

2022年11月28日

（ AWS Control Tower 着陆区无需更新。 ）

AWS Control Tower 现在支持全面的控制管理，包括通过 AWS CloudFormation 挂钩实现的全新、可选的主动控制。这些控制措施之所以被称为主动控制，是因为它们会在部署资源之前检查您的资源，以确定新资源是否符合在您的环境中激活的控制措施。

130 多种新的主动控制措施可帮助您实现 AWS Control Tower 环境的特定政策目标；满足行业标准合规框架的要求；以及管理其他二十多项 AWS 服务之间的 AWS Control Tower 交互。

AWS Control Tower 控件库根据相关的 AWS 服务和资源对这些控件进行分类。有关更多详细信息，请参阅主动控制。

在此版本中，AWS Control Tower 还通过新的安全中心服务托管标准：AWS Control Tower 与 AWS Security Hub支持 AWS 基础安全最佳实践 (FSBP) 标准的AWS Control Tower集成。您可以在控制台中查看 160 多个 Security Hub 控件和 AWS Control Tower 控件，还可以获取 AWS Control Tower 环境的 Security Hub 安全评分。有关更多信息，请参阅 S ecurity Hub 控件。

所有规则的合规性状态均 AWS Config 可查看

2022年11月18日

（ AWS Control Tower 着陆区无需更新。 ）

AWS Control Tower 现在可以显示部署到在 AWS Control Tower 注册的组织单位中的所有 AWS Config 规则的合规状态。您无需在 AWS Control Tower 控制台之外导航即可查看影响您在 AWS Control Tower 中的账户的所有 AWS Config 规则的合规状态，无论是已注册还是取消注册。客户可以

选择在 AWS Control Tower 中设置名为侦探控制的配置规则，也可以直接通过该 AWS Config 服务进行设置。显示了部署的 AWS Config 规则以及 AWS Control Tower 部署的规则。

以前，通过该 AWS Config 服务部署的 AWS Config 规则在 AWS Control Tower 控制台中不可见。客户必须导航到该 AWS Config 服务才能识别不合规的 AWS Config 规则。现在，您可以在 AWS Control Tower 控制台中识别任何不合规的 AWS Config 规则。要查看所有配置规则的合规性状态，请导航到 AWS Control Tower 控制台中的账户详情页面。您将看到一个列表，其中显示了由 AWS Control Tower 管理的控制和部署在 AWS 控制塔之外的配置规则的合规状态。

控件和新 AWS CloudFormation 资源的 API

2022 年 9 月 1 日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在支持通过一组 API 调用对控件（也称为护栏）进行编程管理。新 AWS CloudFormation 资源支持控件的 API 功能。有关更多详细信息，请参阅 在 AWS Control Tower 中自动执行任务 和 使用创建 AWS Control Tower 资源 AWS CloudFormation。

这些 API 允许您启用、禁用和查看 AWS Control Tower 库中控件的应用程序状态。这些 API 包括对的支持 AWS CloudFormation，因此您可以以 infrastructure-as-code (IaC) 的身份管理 AWS 资源。AWS Control Tower 提供可选的预防和侦查控制措施，以表达您对整个组织单位 (OU) 和 OU 内每个 AWS 账户的政策意图。当您创建新账户或更改现有账户时，这些规则仍然有效。

此版本中包含的 API

- EnableControl— 此 API 调用激活控件。它启动异步操作，在指定的组织单位及其包含的帐户上创建 AWS 资源。
- DisableControl— 此 API 调用会关闭控件。它启动异步操作，删除指定组织单位中的 AWS 资源及其包含的帐户。
- GetControlOperation— 返回特定EnableControl或DisableControl操作的状态。
- ListEnabledControls— 列出 AWS Control Tower 对指定组织单位及其包含的账户启用的控件。

要查看可选控件的控件名称列表，请参阅 AWS Control Tower 用户指南中的 API 和控件的资源标识符。

cfCT 支持删除堆栈集

2022年8月26日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower (cfcT) 的自定义功能现在支持通过在文件中设置参数来删除堆栈集。`manifest.yaml`有关更多信息，请参阅 删除堆栈集。

> **Important**
>
> 最初将的值设置为时`true`，下次调用 cfcT 时，所有**`enable_stack_set_deletion`**以该前缀开头`CustomControlTower-`、具有关联密钥标签`Key:AWS_Solutions, Value: CustomControlTowerStackSet`且未在清单文件中声明的资源都将被暂存以供删除。

自定义日志保留

2022年8月15日

（AWS Control Tower 着陆区需要更新。 有关信息，请参阅更新您的登录区）

AWS Control Tower 现在可以为存储 AWS 控制塔 CloudTrail 日志的 Amazon S3 存储桶自定义保留策略。您可以自定义 Amazon S3 日志保留策略，以天或年为增量，最长不超过 15 年。

如果您选择不自定义日志保留期，则标准账户日志记录的默认设置为 1 年，访问日志记录的默认设置为 10 年。

当您更新或修复着陆区时，现有客户可通过 AWS Control Tower 使用此功能，也可以通过 AWS Control Tower 设置流程向新客户提供此功能。

角色偏差修复可用

2022年8月11日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在支持修复角色偏移。无需完全修复 landing zone，即可恢复所需的角色。如果需要这种类型的漂移修复，控制台错误页面会提供恢复角色的步骤，以便您的着陆区再次可用。

AWS Control Tower 着陆区 3.0 版

2022年7月29日

（AWS Control Tower 着陆区需要更新到 3.0 版。 有关信息，请参阅更新您的登录区）

AWS Control Tower 着陆区版本 3.0 包括以下更新：

- 可以选择组织级别的 AWS CloudTrail 跟踪，也可以选择退出由 AWS Control T CloudTrail ower 管理的跟踪。
- 两个新的侦探控件用于确定您的账户中 AWS CloudTrail 是否有记录活动。
- 仅在您所在地区汇总有关全球资源 AWS Config 信息的选项。
- 区域拒绝控制的更新。
- 托管策略的更新，AWSControlTowerServicePolicy。
- 我们不再在每个注册账户`aws-controltower/CloudTrailLogs`中创建 IAM 角色`aws-controltower-CloudWatchLogsRole`和 CloudWatch 日志组。以前，我们在每个账户中为其账户跟踪创建了这些账户。对于组织跟踪，我们只在管理账户中创建一个。

以下各节提供了有关每项新功能的更多详细信息。

AWS Control T CloudTrail ower 中的组织级跟踪

在 landing zone 3.0 版本中，AWS Control Tower 现在支持组织级别的 AWS CloudTrail 跟踪。

当您将 AWS Control Tower 着陆区更新到 3.0 版本时，您可以选择组织级别的 AWS CloudTrail 跟踪作为日志记录首选项，也可以选择退出由 AWS Control Tower 管理的 CloudTrail 跟踪。当您更新到版本 3.0 时，AWS Control Tower 会在等待 24 小时后删除已注册账户的现有账户级别跟踪。AWS Control Tower 不会删除未注册账户的账户级别跟踪。如果您的着陆区域更新失败，但失败发生在 AWS Control Tower 已创建组织级跟踪之后，则在更新操作能够成功完成之前，您可能会为组织级别和账户级别的跟踪支付重复费用。

从着陆区 3.0 开始，AWS Control Tower 不再支持可管理的账户级跟踪。 AWS 相反，AWS Control Tower 会根据您的选择创建组织级别的跟踪，该跟踪处于活动状态或非活动状态。

> **Note**
>
> 更新到 3.0 或更高版本后，您将无法选择继续使用由 AWS Control Tower 管理的账户级 CloudTrail 跟踪。

您的汇总账户日志不会丢失任何日志数据，因为这些日志仍保留在存储它们的现有 Amazon S3 存储桶中。仅删除跟踪，不删除现有日志。如果您选择添加组织级跟踪的选项，AWS Control Tower 会在

Amazon S3 存储桶中打开一条指向新文件夹的新路径，并继续向该位置发送日志信息。如果您选择退出由 AWS Control Tower 管理的跟踪，则您的现有日志将保留在存储桶中，保持不变。

日志存储的路径命名约定

- 账户跟踪日志以以下格式存储路径：`/org id/AWSLogs/…`
- 组织跟踪日志以以下格式存储路径：`/org id/AWSLogs/org id/…`

AWS Control Tower 为您的组织级 CloudTrail 跟踪创建的路径与手动创建的组织级跟踪的默认路径不同，后者的格式如下：

- `/AWSLogs/org id/…`

有关 CloudTrail 路径命名的更多信息，请参阅查找 CloudTrail 日志文件。

> **Tip**
>
> 如果您计划创建和管理自己的账户级跟踪，我们建议您在完成 AWS Control Tower 着陆区版本 3.0 的更新之前创建新的跟踪，以便立即开始记录。

您可以随时选择创建新的账户级或组织级 CloudTrail跟踪并自行管理。在 3.0 或更高版本的任何着陆区更新期间，都可以选择由 AWS Control Tower 管理的组织级 CloudTrail路线。每当你更新 landing zone 时，你都可以选择加入和选择退出组织级别的路线。

如果您的日志由第三方服务管理，请务必为您的服务指定新的路径名。

> **Note**
>
> 对于 3.0 或更高版本的着陆区，AWS Control Tower 不支持账户级别的 AWS CloudTrail 跟踪。您可以随时创建和维护自己的账户级跟踪，也可以选择加入由 AWS Control Tower 管理的组织级跟踪。

仅在主区域录制 AWS Config 资源

在着陆区版本 3.0 中，AWS Control Tower 更新了的基准配置， AWS Config 使其仅记录所在区域的全球资源。更新到 3.0 版后，仅在您所在的地区启用全球资源的资源记录。

此配置被认为是最佳实践。它由 AWS Security Hub 和推荐 AWS Config，它通过减少创建、修改或删除全局资源时创建的配置项的数量来节省成本。以前，无论是客户还是 AWS 服务，每次创建、更新或删除全球资源时，都会为每个受管辖区域中的每个项目创建一个配置项目。

两个用于 AWS CloudTrail 记录的新侦探控件

作为组织级 AWS CloudTrail 跟踪变更的一部分，AWS Control Tower 推出了两个新的侦探控件，用于检查 CloudTrail 是否已启用。第一个控件具有强制性指导，在 3.0 及更高版本的设置或 landing zone 更新期间，它会在安全 OU 上启用。第二种控件具有强烈推荐的指导方针，可以选择将其应用于除安全 OU 之外的任何 OU，该组织已经强制实施了强制性控制保护。

强制控制：检测安全组织单位下的共享账户是否已启用 AWS CloudTrail 或启用 CloudTrail Lake

强烈建议进行控制：检测账户是否已启用 AWS CloudTrail 或启用 CloudTrail Lake

有关新控件的更多信息，请参阅 AWS Control Tower 控件库。

区域拒绝控制的更新

我们更新了区域拒绝控制中的NotAction列表，以包括一些其他服务的操作，如下所示：

```
        “chatbot:*”,
        "s3:GetAccountPublic",
        "s3:DeleteMultiRegionAccessPoint",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListMultiRegionAccessPoints",
        "s3:GetStorageLensConfiguration",
        “s3:GetStorageLensDashboard",
        “s3:ListStorageLensConfigurations”
        “s3:GetAccountPublicAccessBlock“,,
        “s3:PutAccountPublic",
        “s3:PutAccountPublicAccessBlock“,
```

视频演练

此视频 (3:07) 描述了如何将现有的 AWS Control Tower 着陆区更新到版本 3。为了更好地观看，请选择视频右下角的图标以将其放大为全屏。可以使用字幕。

将现有 AWS Control Tower 着陆区更新为着陆区 3 的视频演练。

组织页面结合了 OU 和账户的视图

2022年7月18日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 中的新组织页面显示了所有组织单位 (OU) 和账户的分层视图。它结合了以前存在的 OU 和 A c counts 页面的信息。

在新页面上，您可以看到父 OU 与其嵌套 OU 和账户之间的关系，您可以对资源分组采取操作。您可以配置页面视图。例如，您可以展开或折叠分层视图，筛选视图以仅查看账户或 OU，选择仅查看您的注册账户和注册的 OU，或者您可以查看相关资源组。可以更轻松地确保您的整个组织都得到正确更新。

更轻松地注册和更新个人会员账户

2022年5月31日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在可以提高您单独更新和注册成员账户的能力。每个账户都会显示何时可以更新，因此您可以更轻松地确保您的成员账户包含最新配置。只需几个简化的步骤，您就可以更新您的 landing zone、纠正账户偏差或将账户注册到已注册的 OU。

更新账户时，无需在每次更新操作中都包含账户的整个组织单位 (OU)。因此，更新个人账户所需的时间大大缩短。

在 AWS Control Tower 控制台的更多帮助下，您可以在 AWS Control Tower OU 中注册账户。您在 AWS Control Tower 中注册的现有账户仍必须满足账户的先决条件，并且您必须添加该`AWSControlTowerExecution`角色。然后，您可以选择任何已注册的 OU，然后通过选择 “注册” 按钮将该帐户注册到该组织中。

我们已将注册账户功能与账户工厂中的创建账户工作流程分开，以进一步区分这些类似的流程，并帮助避免在输入账户信息时出现设置错误。

AFT 支持对共享的 AWS Control Tower 账户进行自动定制

2022年5月27日

（AWS Control Tower 着陆区无需更新）

Account Factory for Terraform (AFT) 现在可以通过编程方式自定义和更新您由 AWS Control Tower 管理的任何账户，包括管理账户、审计账户和日志存档账户，以及您的注册账户。您可以集中进行账户自定义和更新管理，同时保护账户配置的安全，因为您可以确定执行工作的角色范围。

现有AWSAFTExecution角色现在可以在所有账户中部署自定义设置。您可以根据您的业务和安全要求设置带有限制AWSAFTExecution角色访问权限的 IAM 权限。您还可以通过编程方式为可信用户委派该角色中已批准的自定义权限。作为最佳实践，我们建议您将权限限制为部署所需自定义项所必需的权限。

AFT 现在创建了在所有托管账户（包括共享账户和管理账户）中部署 AFT 资源的新AWSAFTService角色。之前的资源是由该AWSAFTExecution角色部署的。

AWS Control Tower 共享账户和管理账户不是通过账户工厂配置的，因此它们中没有相应的预配置产品。 AWS Service Catalog因此，您无法更新 Service Catalog 中的共享账户和管理账户。

所有可选控件的并行操作

2022年5月18日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在支持预防性控制和侦探控制的并行操作。

有了这项新功能，现在可以同时应用或删除任何可选控件，从而提高了所有可选控件的易用性和性能。您可以启用多个可选控件，而无需等待单个控制操作完成。唯一的限制时间是 AWS Control Tower 正在设置着陆区或将监管范围扩展到新组织时。

支持的预防性控制功能：

- 在同一 OU 上应用和移除不同的预防控制措施。
- 同时在不同的 OU 上应用和移除不同的预防控制措施。
- 同时对多个 OU 应用和移除相同的预防控制。
- 您可以同时应用和移除任何预防和侦查控制。

您可以在所有已发布的 AWS Control Tower 版本中体验这些控制并发性改进。

当您对嵌套的 OU 应用预防性控制措施时，预防性控制会影响嵌套在目标 OU 下的所有账户和 OU，即使这些账户和 OU 未在 AWS Control Tower 中注册也是如此。预防性控制是使用服务控制策略 (SCP)

实施的，服务控制策略是其中的一部分。 AWS Organizations Detective 控制是使用 AWS Config 规则实现的。当您创建新账户或更改现有账户时，护栏仍然有效，AWS Control Tower 会提供一份摘要报告，说明每个账户如何遵守您启用的策略。有关可用控件的完整列表，请参阅 AWS Control Tower 控件库。

现有的安全和日志账户

2022年5月16日

（在初始设置期间可用。）

AWS Control Tower 现在为您提供了在初始着陆区设置过程中将现有 AWS 账户指定为 AWS Control Tower 安全账户或日志账户的选项。此选项使得 AWS Control Tower 无需创建新的共享账户。安全账户（默认为审核账户）是一个受限账户，允许您的安全和合规团队访问您的 landing zone 中的所有账户。日志帐户（默认情况下称为日志存档帐户）用作存储库。它存储您的 landing zone 中所有账户的 API 活动和资源配置日志。

通过引入现有的安全和日志账户，可以更轻松地将 AWS Control Tower 管理扩展到现有组织，或者从备用着陆区迁移到 AWS Control Tower。在最初的 landing zone 设置过程中，会显示您使用现有账户的选项。它包括在设置过程中进行检查，以确保成功部署。AWS Control Tower 对您的现有账户实施必要的角色和控制。它不会删除或合并这些账户中存在的任何现有资源或数据。

限制：如果您计划将现有 AWS 账户作为审计和日志存档账户引入 AWS Control Tower，并且这些账户有现有 AWS Config 资源，则必须先删除现有 AWS Config 资源，然后才能将这些账户注册到 AWS Control Tower。

AWS Control Tower 着陆区版本 2.9

2022年4月22日

（需要将 AWS Control Tower 着陆区更新到 2.9 版。 有关信息，请参阅更新您的登录区）

AWS Control Tower 着陆区版本 2.9 将通知转发器 Lambda 更新为使用 Python 版本 3.9 运行时。此更新解决了 Python 3.6 版本的弃用问题，该版本计划于 2022 年 7 月发布。有关最新信息，请参阅 Python 弃用页面。

AWS Control Tower 着陆区 2.8 版

2022年2月10日

（需要将 AWS Control Tower 着陆区更新到 2.8 版。 有关信息，请参阅更新您的登录区）

AWS Control Tower landing zone 版本 2.8 添加的功能与AWS 基础安全最佳实践的最新更新保持一致。

在此版本中：

- 已为日志存档账户中的访问日志存储桶配置访问日志记录，以跟踪对现有 S3 访问日志存储桶的访问权限。
- 添加了对生命周期策略的 Support 支持。现有 S3 访问日志存储桶的访问日志的默认保留时间设置为 10 年。
- 此外，此版本更新了 AWS Control Tower AWS Config，使其在所有托管账户（不包括管理账户）中使用由提供的 AWS 服务关联角色 (SLR)，这样您就可以设置和管理符合 AWS Config 最佳实践的配置规则。不升级的客户将继续使用其现有角色。
- 此版本简化了用于加密 AWS Config 数据的 AWS Control Tower KMS 配置流程，并改进了中的相关状态消息。 CloudTrail
- 该版本包括对区域拒绝控件的更新，以允许在中`route53-application-recovery`使用该功能`us-west-2`。
- 更新：2022 年 2 月 15 日，我们删除了 AWS Lambda 函数的死信队列。

其他详细信息：

- 如果您停用着陆区，AWS Control Tower 不会移除 AWS Config 与服务相关的角色。
- 如果您取消配置 Account Factory 账户，AWS Control Tower 不会删除该 AWS Config 服务相关角色。

要将着陆区更新到 2.8，请导航到着陆区域设置页面，选择 2.8 版本，然后选择更新。更新着陆区域后，您必须更新受 AWS Control Tower 管理的所有账户，如中所示AWS Control Tower 中的配置更新管理。

2021 年 1 月至 12 月

2021 年，AWS Control Tower 发布了以下更新：

- 区域拒绝功能
- 数据驻留功能
- AWS Control Tower 推出了 Terraform 账户配置和自定义

- 新的生命周期事件可用
- AWS Control Tower 支持嵌套业务单元
- Detective 控制并发性
- 两个新区域可用
- 取消区域选择
- AWS Control Tower 可与 AWS 密钥管理系统配合使用
- 控件已重命名，功能未更改
- AWS Control Tower 每天扫描 SCP 以检查是否存在偏差
- OU 和账户的自定义名称
- AWS Control Tower 着陆区版本 2.7
- 三个新 AWS 区域可用
- 仅管理选定区域
- AWS Control Tower 现在将监管范围扩展到您 AWS 组织中的现有 OU
- AWS Control Tower 提供批量账户更新

区域拒绝功能

2021年11月30日

（AWS Control Tower 着陆区无需更新。）

AWS Control Tower 现在提供区域拒绝功能，可帮助您限制注册账户在 AWS Control Tower 环境中访问 AWS 服务和操作。区域拒绝功能补充了 AWS Control Tower 中现有的区域选择和区域取消选择功能。这些功能共同帮助您解决合规和监管问题，同时平衡与扩展到其他地区相关的成本。

例如，德国的 AWS 客户可以拒绝访问法兰克福地区以外地区的 AWS 服务。您可以在 AWS Control Tower 设置过程中或在着陆区域设置页面中选择受限区域。当您更新 AWS Control Tower 着陆区版本时，区域拒绝功能可用。部分 AWS 服务不受区域拒绝功能的约束。要了解更多信息，请参阅配置区域拒绝控制。

数据驻留功能

2021年11月30日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在提供专门构建的控件，以帮助确保您上传到 AWS 服务的任何客户数据仅位于您 AWS 指定的区域。您可以选择存储和处理客户数据的一个或多个区域。 AWS 有关提供 AWS Control Tower 的 AWS 区域的完整列表，请参阅AWS 区域表。

为了实现精细控制，您可以应用其他控制措施，例如禁止亚马逊虚拟专用网络 (VPN) 连接或禁止亚马逊 VPC 实例访问互联网。您可以在 AWS Control Tower 控制台中查看控件的合规性状态。有关可用控件的完整列表，请参阅 AWS Control Tower 控件库。

AWS Control Tower 推出了 Terraform 账户配置和自定义

2021年11月29日

（AWS Control Tower 着陆区的可选更新）

现在，您可以使用 Terraform 通过 AWS Control Tower 以及适用于 Ter raform 的 AWS Control Tower Account Factory (AFT) 来配置和更新自定义账户。

AFT 提供单个 Terraform 基础设施即代码 (IaC) 管道，用于配置由 AWS Control Tower 管理的账户。在将帐户提供给最终用户之前，在配置期间进行自定义有助于满足您的业务和安全策略的要求。

AFT 自动账户创建管道会监控直到账户配置完成，然后继续运行，触发额外的 Terraform 模块，通过任何必要的自定义来增强账户。作为自定义过程的另一部分，您可以将管道配置为安装自己的自定义 Terraform 模块，也可以选择添加任何 AFT 功能选项，这些选项由提供， AWS 用于常见自定义。

按照 AWS Control Tower 用户指南中提供的步骤开始使用适用于 Terraform 的 AWS Control Tower Account Factory部署 AWS Control Tower Account Factory for Terraform (AFT)，然后为你的 Terraform 实例下载 AFT。AFT 支持 Terraform Cloud、Terraform Enterprise 和 Terraform 开源发行版。

新的生命周期事件可用

2021年11月18日

（AWS Control Tower 着陆区无需更新）

该`PrecheckOrganizationalUnit`事件记录是否有任何资源阻止 Ex tend 管理任务成功，包括嵌套 OU 中的资源。有关更多信息，请参阅 `PrecheckOrganizationalUnit`。

AWS Control Tower 支持嵌套业务单元

2021年11月16日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在允许您将嵌套的 OU 作为着陆区的一部分。

AWS Control Tower 为嵌套组织单位 (OU) 提供支持，允许您将账户组织为多个层次结构级别，并按层次实施预防性控制。您可以注册包含嵌套 OU 的 OU，在父 OU 下创建和注册 OU，以及对任何已注册的 OU 启用控制，无论深度如何。为了支持此功能，控制台会显示受管理的账户和 OU 的数量。

借助嵌套 OU，您可以将 AWS Control Tower OU 与 AWS 多账户策略保持一致，还可以通过在父 OU 级别实施控制来缩短在多个 OU 上启用控制所需的时间。

重要注意事项：

1. 您可以一次向 AWS Control Tower 注册一个组织单元，从顶层 OU 开始，然后沿着树向下注册现有多级 OU。有关更多信息，请参阅 从扁平的 OU 结构扩展到嵌套的 OU 结构。
2. 直接注册的 OU 下的账户将自动注册。再往下走，可以通过注册其直系父OU来注册账户。
3. 预防性控制 (SCP) 会自动沿着层次结构向下继承；应用于父级的 SCP 由所有嵌套的 OU 继承。
4. Detective 控件（AWS Config 规则）不会自动继承。
5. 每个 OU 都要报告遵守侦探控制的情况。
6. OU 上的 SCP 漂移会影响其下的所有账户和 OU。
7. 您无法在安全 OU（核心 OU）下创建新的嵌套 OU。

Detective 控制并发性

2021年11月5日

（AWS Control Tower 着陆区的可选更新）

AWS Control Tower 侦探控件现在支持侦探控制的并行操作，从而提高了易用性和性能。您可以启用多个侦测控件，而无需等待单个控制操作完成。

支持的功能：

- 在同一 OU 上启用不同的侦测控件（例如，检测根用户的 MFA 是否已启用，检测是否允许对 Amazon S3 存储桶进行公开写入访问）。
- 同时在不同的 OU 上启用不同的探测控件。
- Guardrail 错误消息已得到改进，可以为支持的控制并发操作提供更多指导。

此版本不支持：

- 不支持同时在多个 OU 上启用相同的侦测控制。
- 不支持@@ 预防性控制并发。

您可以在所有版本的 AWS Control Tower 中体验侦探控制并发性的改进。建议当前未使用 2.7 版本的客户执行着陆区更新，以利用最新版本中提供的其他功能，例如区域选择和取消选择。

两个新区域可用

2021年7月29日

（AWS Control Tower 着陆区需要更新）

AWS Control Tower 现已在另外两个 AWS 地区推出：南美（圣保罗）和欧洲（巴黎）。此更新将 AWS Control Tower 的可用性扩展到 15 个 AWS 区域。

如果您不熟悉 AWS Control Tower，则可以在任何支持的区域立即启动它。在启动期间，您可以选择希望 AWS Control Tower 在其中构建和管理您的多账户环境的区域。

如果您已经拥有 AWS C ontrol Tower 环境，并且想要在一个或多个支持区域中扩展或移除 AWS Control Tower 治理功能，请前往 AWS 控制塔控制面板中的着陆区域设置页面，然后选择区域。更新您的着陆区域后，您必须更新受 AWS Control Tower 管理的所有账户。

取消区域选择

2021年7月29日

（AWS Control Tower 着陆区的可选更新）

取消选择 AWS Control Tower 区域可以增强您管理 AWS Control Tower 资源的地理足迹的能力。您可以取消选择您不再希望 AWS Control Tower 管理的区域。此功能使您能够解决合规性和监管问题，同时平衡与扩展到其他地区相关的成本。

当您更新 AWS Control Tower 着陆区版本时，可以取消选择区域。

当您使用 Account Factory 创建新账户或注册先前存在的成员账户时，或者当您选择 “扩展治理” 在先前存在的组织单位中注册账户时，AWS Control Tower 会在您选择的账户区域部署其治理功能，包括集中记录、监控和控制。选择取消选择某个区域并从该区域移除 AWS Control Tower 监管会移除该监管功能，但这不会限制您的用户将 AWS 资源或工作负载部署到这些区域的能力。

AWS Control Tower 可与 AWS 密钥管理系统配合使用

2021年7月28日

（AWS Control Tower 着陆区的可选更新）

AWS Control Tower 为您提供使用 AWS 密钥管理服务 (AWS KMS) 密钥的选项。密钥由您提供并管理，用于保护 AWS Control Tower 部署的服务，包括 AWS CloudTrail AWS Config、和关联的 Amazon S3 数据。 AWS 与 AWS Control Tower 默认使用的 SSE-S3 加密相比，KMS 加密是一种增强的加密级别。

将 AWS KMS 支持集成到 AWS Control Tower 符合AWS 基础安全最佳实践，后者建议为您的敏感日志文件增加一层安全保护。您应该使用 AWS KMS 托管密钥 (SSE-KMS) 进行静态加密。 AWS 当您设置新的着陆区或更新现有的 AWS Control Tower 着陆区时，KMS 加密支持可用。

要配置此功能，您可以在初始着陆区设置期间选择 KMS 密钥配置。您可以选择现有的 KMS 密钥，也可以选择将您定向到 AWS KMS 控制台的按钮来创建新密钥。您还可以灵活地从默认加密更改为 SSE-KMS，或者更改为其他 SSE-KMS 密钥。

对于现有的 AWS Control Tower 着陆区，您可以执行更新以开始使用 AWS KMS 密钥。

控件已重命名，功能未更改

2021年7月26日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 正在修改某些控件名称和描述，以更好地反映控件的政策意图。修改后的名称和描述可帮助您更直观地了解控件如何体现您的账户政策。例如，我们将部分侦探控件的名称从 “不允许” 更改为 “检测”，因为侦探控件本身不会停止特定的操作，它只会检测违反策略的行为并通过控制面板提供警报。

控制功能、指导和实现保持不变。仅修改了控件名称和描述。

AWS Control Tower 每天扫描 SCP 以检查是否存在偏差

2021年5月11日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在每天都会对您的托管 SCP 执行自动扫描，以验证相应的控制措施是否正确应用以及它们是否存在偏差。如果扫描发现偏差，您将收到通知。对于每个漂移问题，AWS Control

Tower 只发送一条通知，因此，如果您的着陆区已经处于漂移状态，则除非找到新的漂移物品，否则您将不会收到其他通知。

OU 和账户的自定义名称

2021年4月16日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在允许您自定义着陆区的命名。您可以保留 AWS Control Tower 为组织单位 (OU) 和核心账户推荐的名称，也可以在最初的着陆区设置过程中修改这些名称。

AWS Control Tower 为业务单元和核心账户提供的默认名称与 AWS 多账户最佳实践指南相符。 但是，如果您的公司有特定的命名政策，或者您已经拥有现有的 OU 或具有相同推荐名称的账户，则新的 OU 和账户命名功能可让您灵活地解决这些限制。

除了设置期间的工作流程更改外，以前称为核心 OU 的 OU 现在被称为安全 OU，而以前称为自定义 OU 的 OU 现在称为沙盒 OU。我们进行此项更改是为了更好地与命名方面的总体 AWS 最佳实践指南保持一致。

新客户将看到这些新的 OU 名称。现有客户将继续看到这些 OU 的原始名称。在我们将文档更新为新名称时，您可能会在 OU 命名中遇到一些不一致之处。

要从 AWS 管理控制台开始使用 AWS Control Tower，请前往 AWS Control Tower 控制台，然后选择右上角的设置着陆区。有关更多信息，您可以阅读有关规划 AWS Control Tower 着陆区的信息。

AWS Control Tower 着陆区版本 2.7

2021年4月8日

（需要将 AWS Control Tower 着陆区更新到 2.7 版。 有关信息，请参阅更新您的登录区）

在 AWS Control Tower 2.7 版本中，AWS Control Tower 引入了四个新的强制性预防性日志存档控件，这些控件仅在 AWS Control Tower 资源上实施策略。我们已将四个现有日志存档控制措施的指导从强制性调整为选择性，因为它们为 AWS Control Tower 之外的资源设定了策略。通过这种控制变更和扩展，可以将 AWS Control Tower 内资源的日志存档管理与 AWS Control Tower 外部资源的管理区分开来。

更改后的四个控件可以与新的强制性控制措施结合使用，为更广泛的 AWS 日志存档提供管理。为了保持环境一致性，现有的 AWS Control Tower 环境将自动启用这四个已更改的控件；但是，现在可以禁用这些选修控件。新的 AWS Control Tower 环境必须启用所有可选控件。在向未由 AWS Control Tower 部署的 Amazon S3 存储桶添加加密功能之前，现有环境必须禁用以前必需的控件。

新的强制性控制措施：

- 不允许在日志存档中更改 AWS Control Tower 创建的 S3 存储桶的加密配置
- 不允许在日志存档中更改 AWS Control Tower 创建的 S3 存储桶的日志配置
- 不允许更改 AWS Control Tower 在日志存档中创建的 S3 存储桶的存储桶策略
- 不允许在日志存档中更改 AWS Control Tower 创建的 S3 存储桶的生命周期配置

指导从必修课改为选修课：

- 不允许更改所有 Amazon S3 存储桶的加密配置 [以前：为日志存档启用静态加密]
- 不允许更改所有 Amazon S3 存储桶的日志配置 [以前：为日志存档启用访问日志记录]
- 不允许更改所有 Amazon S3 存储桶的存储桶策略 [以前：不允许对日志存档进行策略更改]
- 不允许更改所有 Amazon S3 存储桶的生命周期配置 [以前：为日志存档设置保留策略]

AWS Control Tower 版本 2.7 包括对 AWS Control Tower 着陆区蓝图的更改，在升级到 2.7 之后，这些更改可能会导致与之前的版本不兼容。

- 特别是，AWS Control Tower 2.7 版本在 AWS Control Tower 部署的 S3 存储桶上`BlockPublicAccess`自动启用。如果您的工作负载需要跨账户访问权限，则可以关闭此默认设置。有关`BlockPublicaccess`启用后会发生什么情况的更多信息，请参阅阻止公众访问您的 Amazon S3 存储。
- AWS Control Tower 版本 2.7 包括对 HTTPS 的要求。发送到由 AWS Control Tower 部署的 S3 存储桶的所有请求都必须使用安全套接字层 (SSL)。只允许通过 HTTPS 请求。如果您使用 HTTP（不带 SSL）作为发送请求的终端节点，则此更改会给您一个拒绝访问的错误，这可能会中断您的工作流程。在您的 landing zone 2.7 更新之后，此更改将无法恢复。

  我们建议您将请求更改为使用 TLS 而不是 HTTP。

三个新 AWS 区域可用

2021年4月8日

（AWS Control Tower 着陆区需要更新）

AWS Control Tower 在另外三个 AWS 区域推出：亚太地区（东京）区域、亚太地区（首尔）地区和亚太地区（孟买）区域。要将监管扩展到这些区域，需要将 landing zone 更新到 2.7 版。

当您对版本 2.7 进行更新时，您的着陆区域不会自动扩展到这些区域，您必须在 Regions 表中查看并选择它们才能包含在内。

仅管理选定区域

2021年2月19日

（AWS Control Tower 着陆区无需更新）

选择 AWS Control Tower 区域可以更好地管理您的 AWS Control Tower 资源的地理足迹。为了扩大托管 AWS 资源或工作负载的区域数量（出于合规性、监管、成本或其他原因），您现在可以选择其他区域进行管理。

当您设置新的着陆区或更新 AWS Control Tower 着陆区版本时，可以选择区域。当您使用 Account Factory 创建新账户或注册先前存在的成员账户时，或者当您使用 Extend Governance 在先前存在的组织单位中注册账户时，AWS Control Tower 会在您选择的账户区域部署集中记录、监控和控制的监管功能。有关选择区域的更多信息，请参阅配置您的 AWS Control Tower 区域。

AWS Control Tower 现在将监管范围扩展到您 AWS 组织中的现有 OU

2021年1月28日

（AWS Control Tower 着陆区无需更新）

在 AWS Control Tower 控制台中将管理范围扩展到现有组织单位 (OU)（不在 AWS Control Tower 中的组织单位）。借助此功能，您可以将顶级 OU 和包含的账户置于 AWS Control Tower 的监管之下。有关将监管扩展到整个 OU 的信息，请参阅向 AWS Control Tower 注册现有组织单位。

当您注册 OU 时，AWS Control Tower 会执行一系列检查，以确保成功延长管控范围并在 OU 内注册账户。有关与 OU 初始注册相关的常见问题的更多信息，请参阅注册或重新注册期间失败的常见原因。

您也可以访问 AWS Control Tower 产品网页或 YouTube 访问观看这段关于 AWS Control Tower 入门的视频 AWS Organizations。

AWS Control Tower 提供批量账户更新

2021年1月28日

（AWS Control Tower 着陆区无需更新）

借助批量更新功能，您现在只需在 AWS Control Tower 控制面板中单击一下即可更新包含最多 300 个账户的注册 AWS Organizations 组织单位 (OU) 中的所有账户。这在您更新 AWS Control Tower 着陆区并且还必须更新注册账户以使其与当前着陆区版本保持一致的情况下特别有用。

当您更新 AWS Control Tower 着陆区以扩展到新区域时，或者当您想要重新注册 OU 以确保该 OU 中的所有账户都应用了最新控制措施时，此功能还可以帮助您将账户保持最新状态。批量账户更新无需一次更新一个账户或使用外部脚本对多个账户执行更新。

有关更新着陆区的信息，请参阅更新您的登录区。

有关注册或重新注册 OU 的信息，请参阅向 AWS Control Tower 注册现有组织单位。

2020 年 1 月至 12 月

2020 年，AWS Control Tower 发布了以下更新：

- AWS Control Tower 控制台现在链接到外部 AWS 配置规则
- AWS Control Tower 现已在其他区域推出
- 护栏更新
- AWS Control Tower 控制台显示了有关 OU 和账户的更多详细信息
- 使用 AWS Control Tower 在中设置新的多账户 AWS 环境 AWS Organizations
- AWS Control Tower 解决方案的自定义
- AWS Control Tower 2.3 版本正式上市
- 在 AWS Control Tower 中进行单步账户配置
- AWS Control Tower 停用工具
- AWS Control Tower 生命周期事件通知

AWS Control Tower 控制台现在链接到外部 AWS 配置规则

2020年12月29日

（AWS Control Tower 着陆区需要更新到 2.6 版。 有关信息，请参阅更新您的登录区）

AWS Control Tower 现在包括一个组织级聚合器，可帮助检测外部配置 AWS 规则。这使您可以在 AWS AWS Control Tower 控制台中查看除了 AWS Control Tower 创建的 AWS 配置规则之外是否存在外部创建的配置规则。该聚合器允许 AWS Control Tower 检测外部规则并提供指向 AWS 配置控制台的链接，而无需 AWS Control Tower 获得对非托管账户的访问权限。

借助此功能，您现在可以统一查看应用于您账户的侦探控制措施，因此您可以跟踪合规性并确定是否需要对账户进行其他控制。有关信息，请参阅 AWS Control Tower 如何聚合非托管业务单元和账户中的 AWS Config 规则。

AWS Control Tower 现已在其他区域推出

2020年11月18日

（AWS Control Tower 着陆区需要更新到 2.5 版。 有关信息，请参阅更新您的登录区）

AWS Control Tower 现已在另外 5 个 AWS 区域推出：

- 亚太地区（新加坡）区域
- 欧洲地区（法兰克福）区域
- 欧洲地区（伦敦）区域
- 欧洲地区（斯德哥尔摩）区域
- 加拿大（中部）区域

添加这 5 个 AWS 区域是 AWS Control Tower 2.5 版本中引入的唯一变更。

AWS Control Tower 还可在美国东部（弗吉尼亚北部）区域、美国东部（俄亥俄州）区域、美国西部（俄勒冈）区域、欧洲（爱尔兰）地区和亚太地区（悉尼）区域使用。此次发布后，AWS Control Tower 现已在 10 个 AWS 区域推出。

此 landing zone 更新包括列出的所有区域，无法撤消。将您的着陆区域更新到版本 2.5 后，您必须手动更新 AWS Control Tower 的所有注册账户，以便在 10 个受支持 AWS 区域中进行管理。有关信息，请参阅 配置您的 AWS Control Tower 区域。

护栏更新

2020年10月8日

（AWS Control Tower 着陆区无需更新）

强制性控制的更新版本已经发布`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED`。

必须对控制进行此项更改，因为自动注册到 AWS Control Tower 的账户必须启用该`AWSControlTowerExecution`角色。该控件的先前版本禁止创建此角色。

有关更多信息，请参阅 “禁止更改 AWS Control Tower 设置的 IA AWS M 角色” 和 AWS CloudFormation “AWS 控制塔控件参考指南”。

AWS Control Tower 控制台显示了有关 OU 和账户的更多详细信息

2020年7月22日

（AWS Control Tower 着陆区无需更新）

您可以查看未在 AWS Control Tower 中注册的组织和账户，以及已注册的组织和账户。

在 AWS Control Tower 控制台中，您可以查看有关您的 AWS 账户和组织单位 (OU) 的更多详细信息。账户页面现在会列出您组织中的所有账户，无论组织单位或在 AWS Control Tower 中的注册状态如何。现在，您可以对所有表格进行搜索、排序和筛选。

使用 AWS Control Tower 在中设置新的多账户 AWS 环境 AWS Organizations

2020年4月22日

（AWS Control Tower 着陆区无需更新）

AWS Organizations 客户现在可以使用 AWS Control Tower 通过利用以下新功能来管理新创建的组织单位 (OU) 和账户：

- 现有 AWS Organizations 客户现在可以在其现有管理账户中为新的组织单位 (OU) 设置新的着陆区。您可以在 AWS Control Tower 中创建新的 OU，也可以通过 AWS Control Tower 管理在这些业务单元中创建新账户。
- AWS Organizations 客户可以使用账户注册流程或通过脚本来注册现有账户。

AWS Control Tower 提供使用其他服务的编排 AWS 服务。它专为拥有多个账户和团队的组织而设计，他们正在寻找最简单的方法来设置新的或现有的多账户 AWS 环境并进行大规模治理。对于由 AWS Control Tower 管理的组织，云管理员知道组织中的账户符合既定政策。建筑商之所以受益，是因为他们可以快速配置新 AWS 账户，而不必过分担心合规性。

有关设置着陆区的信息，请参阅规划你的 AWS Control Tower 着陆区。您也可以访问 AWS Control Tower 产品网页或 YouTube 访问观看这段关于 AWS Control Tower 入门的视频 AWS Organizations。

除此更改外，AWS Control Tower 中的快速账户配置功能已重命名为注册账户。现在，它允许注册现有 AWS 账户和创建新账户。有关更多信息，请参阅 注册现有账户。

AWS Control Tower 解决方案的自定义

2020年3月17日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在包含一个新的参考实现，可让您轻松地将自定义模板和策略应用于 AWS Control Tower 着陆区。

通过 AWS Control Tower 的自定义设置，您可以使用 AWS CloudFormation 模板将新资源部署到组织内的现有账户和新账户。除了 AWS Control Tower 已经提供的 SCP 之外，您还可以将自定义服务控制策略 (SCP) 应用于这些账户。AWS Control Tower 管道的自定义设置与 AWS Control Tower 生命周期事件和通知 (AWS Control Tower 中的生命周期事件) 集成，以确保资源部署与您的着陆区保持同步。

此 AWS Control Tower 解决方案架构的部署文档可通过AWS 解决方案网页获得。

AWS Control Tower 2.3 版本正式上市

2020年3月5日

（AWS Control Tower 着陆区需要更新。 有关信息，请参阅更新您的登录区。）

除了美国东部（俄亥俄州）、美国东部（弗吉尼亚北部）、美国西部（俄勒冈）和欧洲（爱尔兰）AWS 地区外，AWS Control Tower 现已在亚太地区（悉尼）推出。亚太地区（悉尼）区域的加入是 AWS Control Tower 2.3 版本中引入的唯一变更。

如果您之前没有使用过 AWS Control Tower，则可以立即在任何受支持的区域启动它。如果您已经在使用 AWS Control Tower，并希望在自己的账户中将其监管功能扩展到亚太地区（悉尼）地区，请前往 AWS Control Tower 控制面板中的设置页面。从那里，将你的 landing zone 更新到最新版本。然后，单独更新您的账户。

> **Note**
>
> 更新您的 landing zone 不会自动更新您的账号。如果您有多个帐户，则所需的更新可能很耗时。因此，我们建议您避免将 AWS Control Tower 着陆区扩展到不需要运行工作负载的区域。

有关在部署到新区域后侦探控制的预期行为的信息，请参阅配置您的 AWS Control Tower 区域。

在 AWS Control Tower 中进行单步账户配置

2020年3月2日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在支持通过 AWS Control Tower 控制台进行单步账户配置。此功能允许您从 AWS Control Tower 控制台中配置新账户。

要使用简化的表格，请导航到 AWS Control Tower 控制台中的 “账户工厂”，然后选择 “快速账户配置”。AWS Control Tower 将相同的电子邮件地址分配给已配置的账户和为该账户创建的单点登录（IAM 身份中心）用户。如果您要求这两个电子邮件地址不同，则必须通过 Service Catalog 配置您的帐户。

通过使用 Service Catalog 和 AWS Control Tower 账户工厂快速配置账户来更新您创建的账户，就像更新任何其他账户一样。

> **Note**
>
> 2020 年 4 月，快速账户配置功能更名为 “注册账户”。2022 年 6 月，在 AWS Control Tower 控制台中创建和更新账户的功能与注册 AWS 账户的功能分开。有关更多信息，请参阅 注册现有账户。

AWS Control Tower 停用工具

2020年2月28日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在支持自动停用工具，可帮助您清理 AWS Control Tower 分配的资源。如果您不再打算在企业中使用 AWS Control Tower，或者需要重新部署组织资源，则可能需要清理最初设置着陆区时创建的资源。

要使用基本上是自动化的流程来停用您的着陆区，请联系 AWS Support 以获取有关所需其他步骤的帮助。有关停用的更多信息，请参阅演练：停用 AWS Control Tower 着陆区。

AWS Control Tower 生命周期事件通知

2020年1月22日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 宣布推出生命周期事件通知。生命周期事件标志着 AWS Control Tower 操作的完成，该操作可以更改由 AWS Control Tower 创建和管理的组织单位 (OU)、账户和控制等资源的状态。生命周期事件被记录为 AWS CloudTrail 事件，并作为事件发送给 Amazon EventBridge 。

AWS Control Tower 会在使用该服务执行的以下操作完成后记录生命周期事件：创建或更新着陆区；创建或删除 OU；启用或禁用 OU；启用或禁用 OU 上的控件；使用账户工厂创建新账户或将账户转移到另一个 OU。

AWS Control Tower 使用多种 AWS 服务来构建和管理最佳实践的多账户 AWS 环境。AWS Control Tower 操作可能需要几分钟才能完成。您可以在 CloudTrail 日志中跟踪生命周期事件，以验证最初的 AWS Control Tower 操作是否成功完成。您可以创建一条 EventBridge 规则，以便在 CloudTrail 记录生命周期事件时通知您，或者自动触发自动化工作流程的下一步。

2019 年 1 月至 12 月

从 2019 年 1 月 1 日到 12 月 31 日，AWS Control Tower 发布了以下更新：

- AWS Control Tower 2.2 版正式上市
- AWS Control Tower 中的新选修控件
- AWS Control Tower 中的新侦探控件
- AWS Control Tower 接受与管理账户不同的域名的共享账户的电子邮件地址
- AWS Control Tower 2.1 版本正式上市

AWS Control Tower 2.2 版正式上市

2019年11月13日

（AWS Control Tower 着陆区需要更新。 有关信息，请参阅更新您的登录区。）

AWS Control Tower 2.2 版本提供了三种新的预防性控制措施，可防止账户流失：

- 不允许对 AWS Control Tower 设置的亚马逊 CloudWatch 日志组进行更改
- 不允许删除由 AWS Control Tower 创建的 AWS Config 聚合授权
- 不允许删除日志存档

控制是一条高级规则，可为您的整体 AWS 环境提供持续的治理。当您创建 AWS Control Tower 着陆区时，着陆区和所有组织单位 (OU)、账户和资源都将遵守您选择的控件所执行的监管规则。当您和您的组织成员使用 landing zone 时，这种合规状态可能会发生变化（意外或故意）。偏差检测可帮助您识别需要更改或更新配置以解决偏差问题的资源。有关更多信息，请参阅 在 AWS Control Tower 中检测并解决偏差。

AWS Control Tower 中的新选修控件

2019年9月5日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在包括以下四个新的选修控件：

- 不允许在没有 MFA 的情况下对 Amazon S3 存储桶执行删除操作
- 不允许更改 Amazon S3 存储桶的复制配置
- 不允许以 root 用户身份执行操作
- 不允许为 root 用户创建访问密钥

控制是一条高级规则，可为您的整体 AWS 环境提供持续的治理。防护机制使您能够表达您的策略意向。有关更多信息，请参阅关于 AWS Control Tower 中的控件。

AWS Control Tower 中的新侦探控件

2019年8月25日

（AWS Control Tower 着陆区无需更新）

AWS Control Tower 现在包括以下八个新的侦探控件：

- 检测 Amazon S3 存储桶的版本控制是否已启用
- 检测控制台上的 IAM 用户是否已启用 MFA AWS
- 检测 IAM 用户是否已启用 MFA
- 检测是否为亚马逊 EC2 实例启用了亚马逊 EBS 优化
- 检测 Amazon EBS 卷是否已连接到亚马逊 EC2 实例
- 检测是否已启用对 Amazon RDS 数据库实例的公共访问权限
- 检测是否已启用对 Amazon RDS 数据库快照的公共访问权限

- 检测是否已为 Amazon RDS 数据库实例启用存储加密

控制是一条高级规则，可为您的整体 AWS 环境提供持续的治理。侦探控件可检测您账户中资源的违规行为，例如违反政策，并通过控制面板提供警报。有关更多信息，请参阅关于 AWS Control Tower 中的控件。

AWS Control Tower 接受与管理账户不同的域名的共享账户的电子邮件地址

2019年8月1日

（AWS Control Tower 着陆区无需更新）

在 AWS Control Tower 中，您现在可以为域名与管理账户的电子邮件地址不同的共享账户（日志存档和审计成员）和子账户（使用账户工厂出售）提交电子邮件地址。此功能仅在您创建新的 landing zone 和配置新的儿童帐户时可用。

AWS Control Tower 2.1 版本正式上市

2019年6月24日

（AWS Control Tower 着陆区需要更新。 有关信息，请参阅更新您的着陆区。）

AWS Control Tower 现已正式上市，并支持生产使用。AWS Control Tower 适用于拥有多个账户和团队的组织，他们正在寻找最简单的方法来设置新的多账户 AWS 环境并进行大规模治理。借助 AWS Control Tower，您可以帮助确保组织中的账户符合既定政策。分布式团队的最终用户可以快速配置新 AWS 帐户。

使用 AWS Control Tower，您可以设置一个采用最佳实践的着陆区，例如使用配置多账户结构 AWS Organizations、使用管理用户身份和联合访问 AWS IAM Identity Center、通过 Service Catalog 启用账户配置，以及使用 AWS CloudTrail 和 AWS Config创建集中式日志档案。

为了进行持续监管，您可以启用预配置的控制措施，这些控件是针对安全、运营和合规性的明确定义规则。防护栏有助于防止部署不符合策略的资源，并持续监控已部署的资源是否存在不合规情况。AWS Control Tower 控制面板提供对 AWS 环境的集中可见性，包括已配置的账户、启用的控制以及账户的合规状态。

只需在 AWS Control Tower 控制台中单击一下，即可设置新的多账户环境。使用 AWS Control Tower 无需支付额外费用或预先承诺。您只需为为设置着陆区和实施选定控制而启用的 AWS 服务付费。

文档历史记录

- 最新文档更新：2024 年 5 月 20 日

下表描述了 AWS Control Tower 用户指南的重要更改。如需有关文档更新的通知，您可以订阅 RSS 源。

变更	说明	日期
AWS Control Tower 支持多达 100 个并发控制操作	将并发控制操作配额增加到 100。	2024年5月20日
AWS Control Tower 已在 AWS 卡尔加里西部（加拿大）地区上线	AWS Control Tower 已在加拿大西部（卡尔加里）区域推出。	2024 年 5 月 3 日
AWS Control Tower 支持自助服务配额调整	AWS Control Tower 已与控制台中的 AWS 服务配额集成。	2024 年 4 月 25 日
将控件文档移至新指南	AWS Control Tower 发布了《控制参考指南》。	2024年4月21日
在中标记EnabledControl 资源 AWS CloudFormation	AWS Control Tower 支持通过 AWS CloudFormation 模板向EnabledControl 资源添加标签。	2024年2月22日
基准 API 可用	AWS Control Tower 发布了用于以编程方式注册 OU 的新 API。	2024年2月14日
AWS Control Tower 着陆区版本 3.3	AWS Control Tower 着陆区 3.3 版已推出。	2023 年 12 月 14 日
AWS Control Tower 宣布了辅助数字主权的控制措施	AWS Control Tower 发布了一组控制措施，以帮助客户满足数字主权要求。	2023 年 11 月 27 日

AWS Control Tower 支持着陆区 API	AWS Control Tower 支持使用新的 API 配置和启动着陆区。	2023 年 11 月 26 日
AWS Control Tower 支持启用标记的控件	AWS Control Tower 支持在控制台中使用新 API 为启用标签的控件添加标签。	2023 年 11 月 10 日
AWS Control Tower 已在亚太地区（墨尔本）上市 AWS 区域	在亚太地区（墨尔本）地区可用。	2023 年 11 月 3 日
新的控制 API 可用	AWS Control Tower 发布了一个新的控制 API。	2023 年 10 月 14 日
AWS Control Tower 推出新的控件	AWS Control Tower 发布了新的主动式和侦查型控件。	2023 年 10 月 5 日
AWS Control Tower 报告了禁用可信访问的偏差	如果客户在中关闭了对 AWS Control Tower 的可信访问权限，AWS Control Tower 会在发生偏差时通知客户。 AWS Organizations	2023 年 9 月 21 日
AWS Control Tower 还有四款可供选择 AWS 区域	在亚太地区（海得拉巴）、欧洲（西班牙和苏黎世）和中东（阿联酋）上市。	2023 年 9 月 13 日
AWS Control Tower 已在特拉维夫地区上市	AWS Control Tower 已在特拉维夫地区 il-central-1 上市。	2023 年 8 月 28 日
AWS Control Tower 推出了 28 种新的主动控制措施	AWS Control Tower 发布了 28 种新的主动控制措施。	2023 年 7 月 24 日
AWS Control Tower 弃用了 2 个控件	自 2023 年 8 月 18 日起，AWS Control Tower 将从控件库中移除两个控件。	2023 年 7 月 18 日
AWS Control Tower 着陆区 3.2 上线	AWS Control Tower 着陆区 3.2 版已上市。	2023 年 6 月 16 日

AWS Control Tower 根据 ID 处理账户	AWS Control Tower 会跟踪 AWS 账户 ID，而不是账户的电子邮件地址。	2023 年 6 月 14 日
提供其他 Security Hub 侦探控件	AWS Control Tower 在控件库中添加了十个新控件，用于安全中心服务托管标准：AWS Control Tower。	2023 年 6 月 12 日
AWS Control Tower 发布控制元数据表	AWS Control Tower 现在在已发布的文档中提供了控制元数据表。	2023 年 6 月 7 日
Terraform 支持 Account Factory 定制	AFC 中对 Terraform 开源蓝图的单区域支持。	2023 年 6 月 6 日
AWS IAM 自我管理可用于 landing zone	AWS Control Tower 现在支持客户为着陆区选择身份提供商。	2023 年 6 月 6 日
新角色已添加	AWS Control Tower 添加了一个新的服务相关角色和相关策略。AWSServiceRoleForAWSControlTowerAWSControlTowerAccountServiceRolePolicy	2023 年 6 月 1 日
混合治理更新	更新以向客户提供有关混合治理的建议。	2023 年 6 月 1 日
还提供其他主动控制措施	新的主动控制可帮助您管理多账户环境并实现特定的控制目标。	2023 年 5 月 19 日

另外七个区域可用	AWS Control Tower 现已在另外七个地区推出 AWS 区域：北加州（旧金山）、亚太地区（香港、雅加达和大阪）、欧洲（米兰）、中东（巴林）和非洲（开普敦）。	2023 年 4 月 19 日
更改为托管策略	我们更改了，以AWSControlTowerServiceRolePolicy便 AWS Control Tower 可以调用 AWS 账户管理服务实现的ListRegions 、、GetRegionOptStatus API。EnableRegion	2023 年 4 月 6 日
账户自定义请求追踪现已上线	AWS Control Tower 现在支持使用 Account Factory for Terraform (AFT) 工作流程跟踪账户自定义请求。	2023 年 2 月 16 日
IAM 最佳实践更新	更新了指南，使其与 IAM 最佳实践建议保持一致。有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 2 月 15 日
AWS Control Tower 着陆区 3.1 上线	AWS Control Tower 着陆区 3.1 已上线。	2023 年 2 月 9 日
现已推出主动控制措施	主动控制从预览状态启动到正式发布。	2023 年 1 月 24 日
并发账户操作	AWS Control Tower 现在支持账户工厂中最多五 (5) 个并发操作。您一次最多可以创建、更新或注册五个账户。	2022 年 12 月 16 日

主动控制有助于资源调配	AWS Control Tower 现在支持通过 AWS CloudFormation 挂钩实现的主动控制。	2022 年 11 月 28 日
账户出厂自定义可用	AWS Control Tower 现在支持直接从 AWS Control Tower 控制台使用可自定义的账户模板（称为蓝图）进行账户配置。	2022 年 11 月 28 日
所有规则的合规性状态均 AWS Config 可查看	AWS Control Tower 现在可以显示部署到在 AWS Control Tower 注册的组织单位中的所有 AWS Config 规则的合规状态。	2022 年 11 月 18 日
更改为托管策略	我们进行了更改，以 AWSControlTowerServiceRolePolicy便 AWS Control Tower 可以代入该`AWSControlTowerBlueprintAccess` 角色，这是 Account Factory 自定义所必需的。	2022 年 10 月 28 日
用于控件、 AWS CloudFormation 资源的 API	AWS Control Tower 现在支持通过一组 API 调用和新 AWS CloudFormation 资源激活和停用控件。	2022 年 9 月 1 日
cfCT 支持删除堆栈集	CfcT 支持通过在清单文件中设置参数来删除堆栈集。	2022 年 8 月 26 日
自定义日志保留	您可以为存储您的 AWS Control Tower CloudTrail 日志的 Amazon S3 存储桶自定义保留策略，以天或年为增量，最长不超过 15 年。	2022 年 8 月 15 日

角色偏差修复可用	AWS Control Tower 支持修复角色偏移，无需对着陆区进行全面修复。	2022 年 8 月 11 日
3.0 版本可用	AWS Control Tower 着陆区版本 3.0 从基于账户的 AWS CloudTrail 跟踪更改为基于组织的跟踪，它更新了托管策略以启用组织级跟踪。它使您只能在自己的家乡聚合 AWS Config 信息。3.0 版本还包括区域拒绝控制的更新和两个新的侦探控件。	2022 年 7 月 29 日
组织页面结合了 OU 和账户的视图	AWS Control Tower 中的新组织页面显示了所有组织单位 (OU) 和账户的分层视图。	2022 年 7 月 18 日
更改为托管策略	我们更改了，AWSControlTowerServiceRolePolicy这样客户就可以通过组织级别的 AWS CloudTrail 跟踪来汇总 AWS CloudTrail 日志。	2022 年 6 月 20 日
更轻松地注册和更新会员账户	AWS Control Tower 现在允许您在着陆区内单独注册和更新成员账户。每个账户都会显示何时可以进行更新。我们将注册账户按钮与 Account Factory 中的 “创建账户” 工作流程分开。	2022 年 5 月 31 日
AFT 支持对共享账户进行自定义	AWS Control Tower Account Factory for Terraform 现在支持自定义 AWS Control Tower 管理账户、日志存档和审计账户。	2022 年 5 月 27 日

所有可选控件的并行操作	AWS Control Tower 现在允许您同时应用和移除可选的预防性监护以及侦探控制措施。	2022 年 5 月 18 日
现有的安全账户和日志账户	AWS Control Tower 现在支持引入现有安全账户和日志账户，而不是在设置着陆区期间创建新账户。	2022 年 5 月 16 日
2.9 版本可用	AWS Control Tower 着陆区版本 2.9 将通知转发器 Lambda 更新为使用 Python 版本 3.9 运行时。	2022 年 4 月 22 日
更新了对 AWS 最佳实践的支持，2.8 版本已推出	AWS Control Tower landing zone 版本 2.8 提供了额外支持，以确保您的工作负载和 AWS 账户符合 AWS 最佳实践。	2022 年 2 月 10 日
区域拒绝控制	AWS Control Tower 现在包含一项控件，可帮助您限制对 AWS 区域的访问，以解决合规和监管问题。	2021 年 11 月 30 日
数据驻留控制	AWS Control Tower 现在支持控制功能，可帮助您通过精细控制来管理数据驻留。	2021 年 11 月 30 日
适用于 Terraform 的 AWS Control Tower 账户工厂	AWS Control Tower 现在支持 Terraform，用于自动配置和更新账户。	2021 年 11 月 29 日
新的生命周期事件可用	该`PrecheckOrganizationalUnit` 事件记录是否有任何资源阻止 Ex tend 管理任务成功，包括嵌套 OU 中的资源。	2021 年 11 月 18 日

嵌套 OU 可用	AWS Control Tower 现在允许您的着陆区包含嵌套的 OU 结构。	2021 年 11 月 16 日
Detective 控制并发性	AWS Control Tower 侦探控件现在支持并行启用和禁用操作。	2021 年 11 月 5 日
两个新区域可用	AWS Control Tower 现已在两个新 AWS 区域推出，即欧洲（巴黎）区域和南美洲（圣保罗）区域。	2021 年 7 月 29 日
取消区域选择	您可以取消选择您不想再通过 AWS Control Tower 管理的 AWS 区域。	2021 年 7 月 29 日
KMS 密钥可用	您可以选择创建或选择自己管理的 KMS 密钥来加密您的数据和资源。	2021 年 7 月 28 日
更改为托管策略	我们更改了，AWSControlTowerServiceRolePolicy以便客户可以将自己的 KMS 加密密钥用于 AWS CloudTrail 日志。	2021 年 7 月 28 日
控件名称已更改，功能未更改	某些控件名称和描述已更新，以更好地反映控件的策略意图，但功能没有变化。	2021 年 7 月 26 日
自动扫描托管 SCP	AWS Control Tower 每天对托管 SCP 执行自动扫描，以检查是否存在偏差。	2021 年 5 月 11 日
OU 和账户的自定义名称	AWS Control Tower 允许您在着陆区设置过程中为必要 OU 和账户提供自定义名称，而不会造成偏差。	2021 年 4 月 16 日

停用 landing zone 是自助服务	AWS Control Tower 现在允许您停用着陆区，而无需联系 AWS 支持部门。退役是一个半自动化的过程，无法撤消。这与手动删除所有 AWS Control Tower 资源不同。	2021 年 4 月 9 日
另外三个区域	AWS Control Tower 现已在另外三个 AWS 区域推出：亚太地区（东京）区域、亚太地区（首尔）地区和亚太地区（孟买）区域。	2021 年 4 月 8 日
新的日志存档控件，landing zone 2.7 版本已推出	四个新的日志存档控件提供了对 AWS Control Tower 资源的日志存档管理，与 AWS Control Tower 之外的资源管理是分开的。关于四项现有控制措施的指导已从强制性改为选择性。AWS Control Tower 着陆区 2.7 版包括对 HTTPS 的要求，更新后无法撤消该要求。	2021 年 4 月 8 日
区域选择	选择 AWS Control Tower 区域可以更好地管理您的 AWS Control Tower 资源的地理足迹。为了扩大托管 AWS 资源或工作负载的区域数量（出于合规性、监管、成本或其他原因），您现在可以选择其他区域进行管理。	2021 年 2 月 19 日
注册一个 OU 并同时使用 AWS Control Tower 管理其所有账户	AWS Control Tower 增加了注册 OU 的功能，这是一种同时将多个账户纳入管理的方式。	2021 年 1 月 28 日

已注册 OU 中的多个账户更新	现在，您只需在 AWS Control Tower 控制面板中单击一下即可更新任何注册 AWS Organizations 组织单位 (OU) 中包含最多 300 个账户的所有账户。多账户更新功能（也称为批量更新）使您无需一次更新一个账户，也无需使用外部脚本同时对多个账户执行更新。	2021 年 1 月 28 日
用于聚合非托管 OU 和账户的新角色	新角色有助于检测外部 AWS Config 规则，因此 AWS Control Tower 无需获得对非托管账户的访问权限。	2020 年 12 月 29 日
AWS Control Tower 已在更多 AWS 地区推出。	AWS Control Tower 现已可在亚太地区（新加坡）区域、欧洲（法兰克福）区域、欧洲（伦敦）区域、欧洲（斯德哥尔摩）地区和加拿大（中部）地区部署。此次发布后，AWS Control Tower 现已在 10 个 AWS 区域推出。此 landing zone 更新包括列出的所有区域，且无法撤消。将您的着陆区域更新到版本 2.5 后，您必须手动更新 AWS Control Tower 的所有注册账户，以便在 10 个受支持 AWS 区域中进行管理。	2020 年 11 月 18 日
控件更新	强制性控制的更新版本已经发布`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED` 。更新的控件允许更轻松地自动注册帐户。	2020 年 10 月 8 日

AWS Control Tower 的相关信息页面现已上线	通过相关信息页面，您可以更轻松地找到在设置 AWS Control Tower 着陆区后可能有所帮助的常见任务。	2020 年 9 月 18 日
AWS Control Tower 控制台显示了有关 OU 和账户的更多详细信息。	在 AWS Control Tower 控制台中，您可以查看有关您的 AWS 账户和组织单位 (OU) 的更多详细信息。“账户” 页面现在会列出您组织中的所有账户，无论组织单位或在 AWS Control Tower 中的注册状态如何。现在，您可以对所有表格进行搜索、排序和筛选。	2020 年 7 月 22 日
AWS Control Tower 允许现有组织设置着陆区	现在，您可以在现有组织中启动 AWS Control Tower 的着陆区，将该组织纳入治理。AWS Control Tower 中的快速账户配置功能已重命名为注册 AWS 账户，现在允许注册现有账户和创建新账户。	2020 年 4 月 16 日
AWS Control Tower 现已在亚太地区上市	AWS Control Tower 现已可在亚太地区（悉尼） AWS 地区部署。此版本要求对销售账户进行手动更新，仅当您计划在亚太地区（悉尼）运行工作负载时才进行更新。	2020 年 3 月 3 日
可以停用 AWS Control Tower 着陆区	AWS 尽管需要进行一些手动清理，但Support可以通过一种基本自动化的流程来帮助您永久停用着陆区，从而保护您的组织。	2020 年 2 月 27 日

AWS Control Tower 中提供了快速账户配置功能	通过快速账户预配置，您可以在您的登录区为最新时，使用 Enroll account (注册账户) 功能更轻松地启动新成员账户。	2020 年 2 月 20 日
生命周期事件在 AWS Control Tower 中进行跟踪	生命周期事件为某些 AWS Control Tower 事件提供了更多详细信息，以简化某些工作流程自动化。	2019 年 12 月 12 日
AWS Control Tower 提供了设置和活动页面	通过“设置”和“活动”页面，可以更轻松地更新您的登录区和查看记录的事件。	2019年11月30日
AWS Control Tower 还提供了其他预防性控制措施	AWS Control Tower 中的预防性控制可使您的组织和资源与您的环境保持一致。	2019 年 9 月 6 日
AWS Control Tower 还提供了其他侦探控件	AWS Control Tower 中的侦探控件提供有关您的组织和资源状态的信息。	2019 年 8 月 27 日
AWS Control Tower 现已正式上市	AWS Control Tower 是一项服务，它为大规模设置和管理多账户 AWS 环境提供了最简单的方法。	2019 年 6 月 24 日

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。

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。