AWS 决策指南

选择 AWS 云治理服务

选择 AWS 云治理服务: AWS 决策指南

Table of Contents

选择 AWS 云治理服务

迈出第一步

目的	帮助确定哪些 AWS 云治理服务最适合您的组织。
上次更新	2024年12月23日
承保服务	• AWS Artifact • AWS Audit Manager • CloudFormation • AWS CloudTrail • AWS Config • AWS Control Tower • AWS Organizations • AWS Security Hub CSPM • AWS Service Catalog • AWS Systems Manager • AWS Trusted Advisor

AWS 云治理简介

云治理是一组规则、流程和报告，可帮助您将 AWS Cloud 使用与业务目标保持一致。

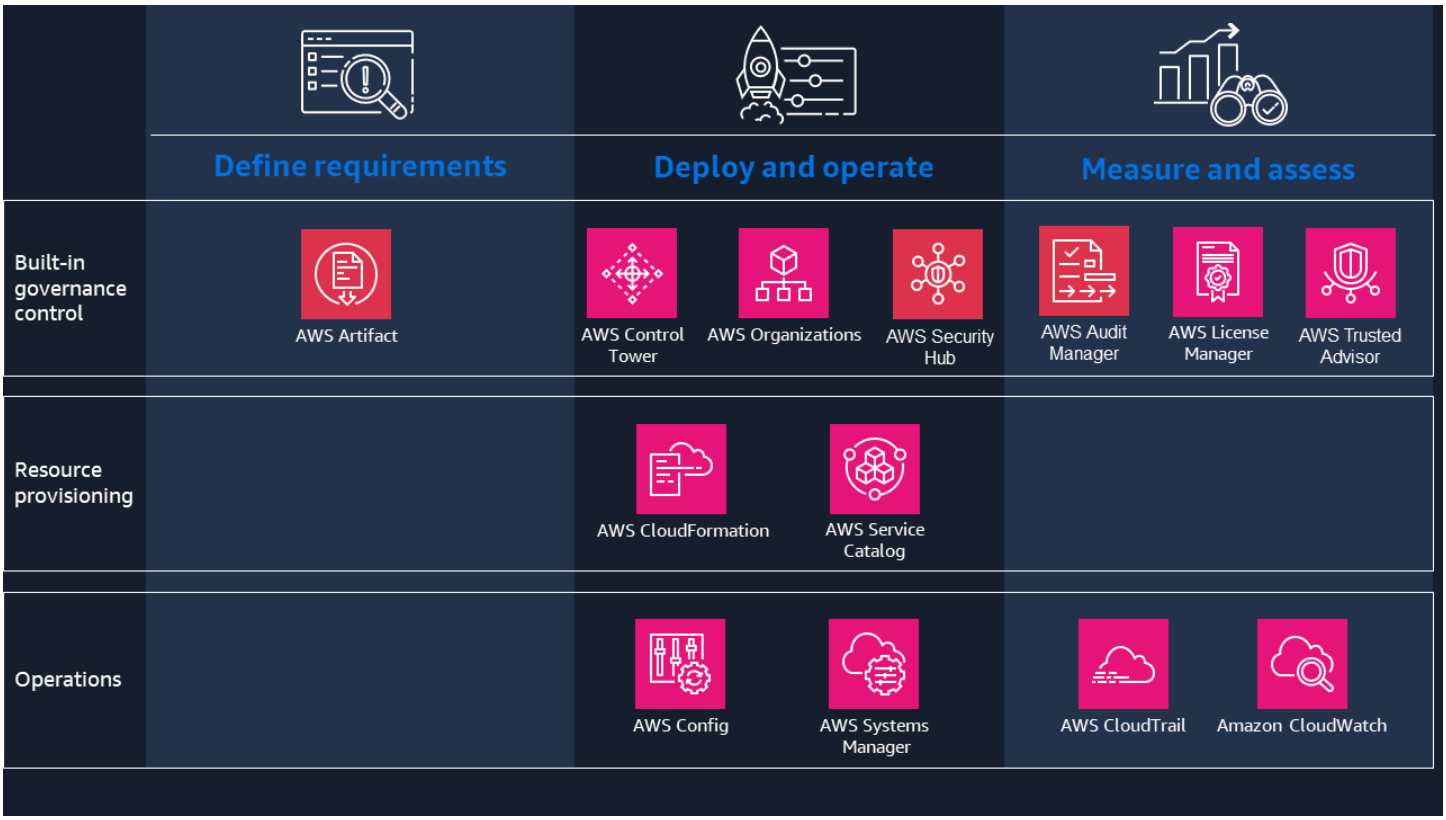
这包括通过启用多账户策略、持续监控和控制策略来实现安全性。它通过自动检查、报告和补救来涵盖合规性。它通过在企业范围内应用控制来涵盖运营。它通过大规模集中身份和访问管理来涵盖身份。它通过促进使用情况报告和政策执行来支付成本。它还通过帮助将评估和测试整合到 CI/CD 管道中进行验证，从而涵盖了弹性。

我们提供一系列服务，帮助您设置、管理、监控和控制云中账户、服务和资源的使用，从而实施云治理最佳实践。

该指南旨在帮助您确定哪些 AWS 云治理服务最适合您的组织，增强运营弹性，优化成本，并建立控制措施以帮助遵守法规或公司标准，同时保持开发速度并加快创新。

本视频是介绍云治理最佳实践的演示文稿的六分钟片段。

了解 AWS 云治理



上图显示了云治理如何利用多个云治理 AWS 服务，这使您可以定义治理需求，部署和操作系统，以及衡量和评估其性能。这些服务提供内置的治理控制、与您的治理策略保持一致的资源调配，以及帮助您监控和管理环境的操作工具。

利用 AWS 云治理服务可以帮助您确保云的使用支持您的业务目标，具体而言，它们使您能够提高开发人员的速度和敏捷性，在动态监管环境中运营，简化合并和收购，并增强运营弹性：

- 提高开发人员的速度和敏捷性 — 通过确保您的开发人员不必等待长达数周的配置周期， APIs 从而快速打造新环境，并加快 CI/CD 管道的配置。使用预先构建的控件和规则以及用于高效配置公共资源的 infrastructure-as-code模板，在软件交付过程的早期发现和预防缺陷。
- 在动态监管环境中运营 — 创建始终在线的边界，以保护和控制对数据的访问 AWS，整理您的合规性要求，并自动评估整个组织的资源配置。
- 简化合并和收购 — 通过构建安全、架构良好的多账户环境，更快地迁移工作负载。轻松快速地集中账户创建、分配资源、对账户进行分组以及应用治理策略和控制。采用程序化方法进行大规模的多账户管理。

- 增强运营弹性 — 快速建立一个安全、架构完善、有弹性的多账户环境。对您的工作负载进行评估，以发现与弹性相关的潜在弱点。根据五个关键领域（成本优化、性能、安全性、容错能力和服务限制）进行自动检查，并获得建议，使您能够遵循已知的最佳实践。
- 优化成本- 可视化、了解和管理一段时间内的成本和使用情况。持续分析资源利用率，识别未充分利用的资源，并终止闲置的资源。

在设置和操作工作负载时，可以有效地内置云治理最佳实践 AWS。互操作服务可帮助您对包括 AWS 第三方产品在内的 IT 资产实现一致、集中的治理。控制的广度和深度 AWS 服务 可帮助您满足不断变化的监管要求并最大限度地降低安全风险。

考虑 AWS 云治理标准

以下部分概述了选择云治理策略时需要考虑的一些关键标准。特别是，它讨论了可能适用于您的组织和业务目标的不同类型的云环境、控制制度和开发人员支持机会。

Multi-account strategy

它是什么：实施云环境最佳实践取决于采用安全的多账户策略。使用帐户作为构建块，并将其分组为组织单位 (OUs)，例如 OUs 用于安全和基础架构的基础部门，以及 OUs 用于沙盒和工作负载的其他单位。

为何重要：多账户策略为您的云环境提供了自然界限和隔离。这反过来又允许您管理配额和账户限制，自动配置和自定义账户，并通过限制对管理账户的访问来应用最低权限原则。它可以实现可见性，以跟踪整个环境中的用户活动和风险。您的多账户策略是您为迁移项目或兼并和收购等组织变革进行构建的基础。

用于 AWS 账户 将多个账户整合AWS Organizations到一个组织中，您可以使用该组织来分配资源、对账户进行分组和应用治理策略。

AWS Control Tower用作编排服务，层叠在上面 AWS Organizations，以帮助构建您的资 AWS 产，并将治理扩展到您的多账户环境。 OUs

Controls management best practices

它是什么：实施控制管理最佳实践可以包括一系列方法。Detective 控制违反既定安全策略的 catch 资源。预防性控制通过阻止特定操作来保护安全基准。主动控制会在资源配置之前对其进行扫描，阻止部署不合规的代码，并指导开发人员对其进行补救。随着您进入新市场，Interoperable 可 AWS 服务 让您集中管理和控制整个 IT 资产，包括 AWS 第三方产品。

为何重要：控制管理最佳实践允许您以编程方式大规模实施控制，并自动配置合规性或纠正不合规行为。如果您的组织在受监管的行业（例如医疗保健、生命科学、金融服务或公共部门）运营，在这些行业中适用特定的监管框架，或者遵守特定的公司标准或数据驻留和数字主权要求，则这一点尤其重要。

考虑是否有机会协调多个配置设置 AWS 服务 以确保组织的安全性和合规性需求，使用AWS Control Tower、定义配置设置并检测与这些设置的偏差 AWS Config，使用和审核 AWS 使用情况以及对法规和行业标准的遵守情况。AWS Audit Manager

Cloud governance for developers

它是什么：为开发人员实施云治理最佳实践可能包括使用基础设施即代码 (IaC) 来确保其工作的可重复性和一致性，以及建立检测安全漏洞的流程。

为何重要：这可以帮助团队快速行动，同时对自己的治理流程充满信心。它为开发人员提供了可以部署到整个堆栈的单一事实来源，他们可以复制、重新部署和重新调整用途的基础架构，能够同时控制基础架构和应用程序的版本控制，以及自助操作的选择。

开发人员的云治理还可能涉及检测代码中的安全漏洞。这可以帮助他们提高代码质量，识别关键问题，确保发布渠道一致，并使用蓝图启动项目。

考虑一下如何使用 AWS 服务 类似 Service Catalog 的服务目录为构建者提供预先批准的 infrastructure-as-code模板，以及相应的 IAM 政策，这些政策规定了使用对象、地点和方式。

Scalability and flexibility

它是什么：选择 AWS 服务 能够帮助您的云治理措施与您的基础架构无缝增长并适应不断变化的需求的产品。考虑一下您的组织将如何发展，以及发展速度有多快。

为何重要：考虑可扩展性和灵活性可以帮助您确保云治理安排强大、响应迅速，并且能够支持动态业务环境。

为了帮助您快速扩展，我们 AWS Control Tower 精心策划了其他几项功能 AWS 服务，包括 AWS Organizations 和 AWS IAM Identity Center，以便在不到一小时的时间内建造一个着陆区。Control Tower 代表您设置和管理资源。

AWS Organizations 使您能够跨多个账户管理 40 多个服务资源。这为各个应用程序团队提供了灵活性和可见性，可以管理特定于其工作负载的云治理需求，同时还为他们提供了集中式团队的可见性。

选择 AWS 云治理服务

现在，您知道了评估云治理选项所依据的标准，就可以选择哪种 AWS 云治理服务最适合您的组织需求了。下表突出显示了哪些服务针对哪些情况进行了优化。使用它来帮助确定最适合您的组织和用例的服务。

用例类型	你什么时候会用它？	推荐服务
定义需求	提供按需下载 AWS 安全与合规性文件。	AWS Artifact
部署和操作	使用基础架构即代码加速云配置。	AWS CloudFormation
	代表您的理想配置设置并检测 AWS 资源是否偏离了该设置。	AWS Config
	代表您设置和协调多个 AWS 服务 项目，同时帮助您满足组织的安全性和合规性需求。	AWS Control Tower
	要 AWS 账户 将多个组织整合到一个组织中，您可以使用该组织来分配资源、对账户进行分组、应用治理策略以及集中和大规模管理。	AWS Organizations
	根据一组受支持的安全标准中的规则运行自动和持续的检查。	AWS Security Hub CSPM
	为构建者提供预先批准的 infrastructure-as-code模板和相应的 IAM 政策，这些政策规定了使用对象、地点和方式。	服务目录

用例类型	你什么时候会用它？	推荐服务
	为多云 AWS 和混合环境中的资源提供安全 end-to-end管理。	AWS Systems Manager
测量和评估	审计 AWS 使用情况，评估风险以及对法规和行业标准的遵守情况。	AWS Audit Manager
	启用您的运营和风险审计、治理和合规性 AWS 账户。	AWS CloudTrail
	实时监控您的 AWS 资源和您运行 AWS 的应用程序。	Amazon CloudWatch
	在您的本地环境中 AWS 集中管理供应商提供的软件许可证。	AWS License Manager
	根据最佳实践评估使用情况和配置。	AWS Trusted Advisor

使用 AWS 云治理服务

现在，您应该清楚地了解每种 AWS 云治理服务的用途，以及哪些服务可能适合您。

为了探索如何使用每种可用的 AWS 云治理服务并了解有关这些服务的更多信息，我们提供了探索每种服务的工作原理的途径。以下部分提供了指向深入文档、动手教程和其他资源的链接，以帮助您入门。

AWS Artifact

- 入门 AWS Artifact

  下载安全与合规报告、管理法律协议和管理通知。

  浏览指南”
- 管理中的协议 AWS Artifact

使用 AWS 管理控制台 来查看、接受和管理您的账户或组织的协议。

浏览指南”

- 为 AWS 第 1 部分中的审计做准备 — AWS Audit Manager AWS Config、和 AWS Artifact

  使用 AWS 服务 服务来帮助您自动收集用于审计的证据。

  阅读博客”

AWS Audit Manager

- 入门 AWS Audit Manager

  使用 AWS 管理控制台、Audit Manager API 或启用 Audit Manager AWS CLI。

  浏览指南”

- 审计所有者教程：创建评估

  使用 Audit Manager 示例框架创建评估。

  开始阅读本教程”

- 代表教程：审阅控件集

  在 Audit Manager 中查看审计责任人与您共享的控制集。

  开始阅读本教程”

AWS CloudTrail

- 查看事件历史记录

  查看你的 AWS API 活动 ， AWS 账户 了解支持的服务 CloudTrail。

  开始阅读本教程”

- 创建记录管理事件的跟踪

  创建跟踪以记录所有区域的管理事件。

  开始阅读本教程”

AWS Config

- AWS Config features

  探索的资源跟踪功能 AWS Config，从配置历史记录和快照到可自定义的规则和一致性包。

  浏览指南”

- AWS Config 工作原理

  深入了解并了解该服务如何发现和跟踪资源，以及如何通过各种渠道交付配置项目。 AWS Config

  浏览指南”

- 风险与合规研讨会

  使用 AWS Config 和 AWS 托管 Config 规则自动进行控制。

  探索工作坊”

- AWS Config 规则开发套件库：大规模构建和操作规则

  使用规则开发套件 (RDK) 构建自定义 AWS Config 规则并使用进行部 RDKLib署。

  阅读博客”

AWS Control Tower

- 入门 AWS Control Tower

  了解如何使用 AWS Control Tower 主机设置着陆区，或者 APIs.

  浏览指南”

- AWS Control Tower 控制管理研讨会

  了解如何在多账户环境中设置治理，使其与 AWS 最佳实践和常见合规框架保持一致。

  探索工作坊”

- 利用 Amazon Bedrock 实现账户管理现代化和 AWS Control Tower

  配置安全工具账户，利用生成式 AI 来加快 AWS 账户 设置和管理流程。

阅读博客”

- 使用以下方法构建精心设计的环境 AWS GovCloud (US) AWS Control Tower

  在 AWS GovCloud (US) 区域中设置您的治理，包括使用组织单位 (OUs) 和来管理您的 AWS 工作负载 AWS 账户。

  阅读博客”

AWS Organizations

- 入门 AWS Organizations

  了解如何开始使用 AWS Organizations，包括查看术语和概念、使用整合账单以及应用组织政策。

  浏览指南”
- 创建和配置组织

  创建您的组织并使用两个 AWS 成员帐户对其进行配置。

  开始阅读本教程”
- 使用多个账户组织您的 AWS 环境

  了解如何使用多个 AWS 账户 功能来帮助隔离和管理您的业务应用程序和数据，并在 Well-Architecte AWS d Framework 支柱之间进行优化。

  阅读白皮书”
- 与之配合使用的服务 AWS Organizations

  了解您可以与哪些 AWS 服务 服务一起使用， AWS Organizations 以及在整个组织范围内使用每项服务的好处。

  浏览指南”
- Best Practices for Organizational Units with AWS Organizations

  深入研究构建组织时推荐 AWS 的最佳实践架构、OU 结构和具体的实施示例。

  阅读博客”
- 通过设计考虑实现卓越运营 AWS Organizations SCPs

了解如何 SCPs 帮助控制组织内创建的多个账户的访问权限 AWS 服务 和资源配置。

阅读博客”

AWS Security Hub CSPM

- 正在启用 AWS Security Hub CSPM

  AWS Security Hub CSPM 使用 AWS Organizations 或在独立账户中启用。

  浏览指南”
- 跨区域聚合

  AWS 区域 将多个聚合区域的 AWS Security Hub CSPM 发现结果汇总到单个聚合区域。

  浏览指南”
- AWS Security Hub CSPM 工作坊

  学习如何使用 AWS Security Hub CSPM 、管理和改善 AWS 环境的安全状况。

  探索工作坊”
- 三种反复出现的 Security Hub 使用模式以及如何部署它们

  了解三种最常见的 AWS Security Hub CSPM 使用模式，以及如何改进识别和管理发现的策略。

  阅读博客”

探索 AWS 云治理资源

架构图

浏览参考架构图，帮助您制定安全、身份和治理策略。

浏览架构图

白皮书

浏览白皮书，了解更多关于选择、实施和使用最适合您组织的安全、身份和治理服务的见解和最佳实践。

浏览白皮书

解决方案

使用这些解决方案进一步制定和完善您的安全、身份和治理策略。

探索解决方案

文档历史记录

下表描述了本决策指南的重要更改。要获取有关本指南更新的通知，您可以订阅 RSS feed。

变更	说明	日期
初次发布	指南首次出版。	2024 年 10 月 4 日

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