AWS 安全参考架构 (AWS SRA)-核心架构

AWS 规范性指导

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 规范性指导: AWS 安全参考架构 (AWS SRA)-核心架构

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

AWS 安全参考架构 (AWS SRA)-核心架构

亚马逊 Web Services 全球服务安全团队（贡献者）

2025 年 12 月（文档历史记录）

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

Amazon Web Services (AWS) 安全参考架构 (AWS SRA) 是一套完整的指南，用于在多账户环境中部署全套 AWS 安全服务。使用它来帮助设计、实施和管理 AWS 安全服务，使其符合 AWS 建议的做法。这些建议是围绕单页架构构建的，该架构包括 AWS 安全服务，它们如何帮助实现安全目标，在哪里可以最好地部署和管理这些服务 AWS 账户，以及它们如何与其他安全服务交互。本总体架构指南补充了详细的、特定于服务的建议，例如AWS 安全文档网站上的建议。

架构和随附的建议基于我们与 AWS 企业客户的集体经验。本文档是一份参考资料，一套用于保护特定环境的全面指南，而 AWS SRA 代码存储库中的解决方案模式是针对本参考文献中说明的特定架构设计的。 AWS 服务 每个客户都有不同的要求。因此，您的 AWS 环境设计可能与此处提供的示例有所不同。您需要修改和定制这些建议，以适应您的个人环境和安全需求。 在整篇文档中，我们会酌情为经常出现的替代方案提出建议。

AWS SRA 是一套活生动的指南，会根据新的服务和功能发布、客户反馈以及不断变化的威胁形势定期更新。每次更新都将包括修订日期和相关的变更日志。

尽管我们依赖单页图表作为基础，但该架构比单个方框图更深入，并且必须建立在基础和安全原则的结构良好的基础之上。您可以通过两种方式使用本文档：作为叙述或作为参考。这些主题以故事形式组织，因此您可以从头到尾（基础安全指南）阅读它们（讨论可以实现的代码示例）。或者，您可以浏览文档，重点介绍与您的需求最相关的安全原则、服务、账户类型、指南和示例。

本文档分为以下各节和附录：

- Ab@@ out the AWS SRA 图书馆概述了 AWS SRA 出版物集中包含的技术指南和代码。
- AWS SRA 的价值讨论了构建 SR AWS A 的动机，描述了如何使用它来帮助提高安全性，并列出了关键要点。
- 安全基础回顾了 AWS 云采用框架 (AWS CAF)、Well-Ar AWS chitected 框架和 AWS 责任共担模型，并重点介绍了与 SRA 特别相关的元素。 AWS
- AWS Organizations、账户和 IAM guardrails 介绍了该 AWS Organizations 服务，讨论了基础安全功能和防护措施，并概述了我们推荐的多账户策略。

- AWS 安全参考架构是一个单页架构图，显示了功能 AWS 账户以及普遍可用的安全服务和功能。
- 用于安全的 AI/ML 描述了如何在后台 AWS 服务 使用人工智能和机器学习 (AI/ML) 来帮助您实现特定的安全目标。您可以将它们包含 AWS 服务 在设计中，以利用高级安全功能。
- 构建安全架构 – 根据 AWS SRA 提供的参考资料，分阶段的方法提供了有关如何分六个迭代阶段构建自己的安全架构的指导。
- AWS SRA 最佳实践清单将整个指南中讨论的建议提炼成一份清单，您可以在构建安全架构版本时遵循该清单。
- IAM 资源提供了一份摘要和一组指导 AWS Identity and Access Management (IAM) 指南，这些指南对您的安全架构很重要。
- AWS SRA 示例的代码存储库提供了相关GitHub 存储库的概述，该存储库将帮助开发人员和工程师部署本文档中介绍的一些指导和架构模式。你可以使用 AWS CloudFormation 或 Terraform 来部署示例。 HashiCorp它们同时支持 AWS Control Tower 和非AWS Control Tower 环境。

附录包含各个 AWS 安全、身份和合规服务的列表，并提供了指向有关每项服务的更多信息的链接。“文档历史记录” 部分提供了用于跟踪此文档版本的变更日志。您也可以订阅 RSS 提要以获取变更通知。

关于 AWS SRA 图书馆

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

本指南是库的一部分，该库为设计和构建安全架构提供了架构蓝图和技术指导。 AWS该库由实现代码（AWS SRA 代码库）、验证工具（SRA Verify）以及涵盖核心架构和深入研究架构的两类补充指南组成。

AWS SRA — 核心架构（本指南）

本指南为推荐 AWS 的安全架构奠定了基础。它是适用于所有组织的起点，无论其行业、应用程序类型或任何其他考虑因素如何。该基础可帮助您构建强大且可扩展的架构， AWS 并有助于创建强大的 AWS 多账户安全基准，该基准可随着业务的增长而安全扩展。

AWS SRA — 深入研究架构

AWS SRA — 核心架构指南由其他出版物作为补充，这些出版物提供了与特定安全功能、应用程序类型以及合规性或监管要求相一致的架构模式。这些模式扩展了核心架构，应与 AWS SRA（核心架构指南）结合使用。

以下指南提供了与特定安全功能相对应的架构模式：

- AWS SRA — 身份管理提供了有关如何实施可扩展、强大且集中的身份和访问管理解决方案的 AWS 指导。
- AWS SRA — 外围安全讨论架构模式以及在 AWS 服务 中央账户或个人账户中实施边缘安全。
- AWS SRA — 网络取证描述了如何将 AWS 取证帐户配置为起点，以此来发展组织的取证能力并帮助改善安全事件响应 (IR) 的准备工作。

以下指南提供了特定应用程序类型的架构模式。在构建基准安全架构之后，您可能需要重点关注以下内容：

- AWS SRA — AI sec urity 为使用 AWS 生成式 AI 服务设计和构建包含生成式 AI 功能的应用程序提供安全架构建议。
- AWS SRA — IoT 为设计和构建物联网应用程序提供安全架构建议。 AWS

此外，以下指南还描述了符合特定合规性或监管框架的架构模式：

- AWS 隐私参考架构 (AWS PRA) 为处理个人数据的应用程序提供了安全架构，并且必须支持广泛的隐私合规要求，例如《通用数据保护条例》(GDPR)、《加州消费者隐私法》(CCPA) 或《巴西通用数据保护法》(LGPD)。 AWS PRA提供了一套专门针对中隐私控制的设计和配置的指导方针。 AWS 服务

我们建议您从 AWS SRA（核心架构指南）入手，了解基础架构，然后查阅补充指南以利用高级功能和实现。有关此内容集的更多信息，请参阅AWS 安全参考架构。

> **架构图**
>
> 要根据业务需求自定义 AWS SRA 库中的参考架构图，您可以下载以下.zip 文件并提取其内容。
>
> 下载图表源文件（微软 PowerPoint格式）

AWS SRA 的价值

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

AWS 拥有大量（而且还在不断增长）的安全和安全相关服务。客户对通过我们的服务文档、博客文章、教程、峰会和会议提供的详细信息表示感谢。他们还告诉我们，他们希望更好地了解大局并从战略角度看待 AWS 安全服务。当我们与客户合作以更深入地了解他们的需求时，会出现三个优先事项：

- 客户需要更多信息和推荐模式，以了解他们如何全面部署、配置和运营 AWS 安全服务。应在哪些账户中部署和管理服务，以实现哪些安全目标？ 是否有一个安全账户可以运行所有或大多数服务？ 地点（组织单位或 AWS 账户）的选择如何为安全目标提供依据？ 客户应该注意哪些权衡取舍（设计注意事项）？
- 客户有兴趣看到逻辑组织许多 AWS 安全服务的不同视角。除了每项服务（例如身份服务或日志服务）的主要功能外，这些替代观点还可以帮助客户规划、设计和实施其安全架构。本文档稍后分享的一个示例根据与您的 AWS 环境推荐结构一致的保护层对服务进行分组。
- 客户正在寻找指导和示例，以最有效的方式集成安全服务。例如，他们应该如何最好地 AWS Config 与其他服务协调和连接，以完成自动化审计和监控管道中的繁重工作？ 客户正在寻求有关每项 AWS 安全服务如何依赖或支持其他安全服务的指导。

我们在 AWS SRA中逐一解决了这些问题。列表中的第一要务（事情进展如何）是主架构图的重点以及本文档中随附的讨论。我们提供了推荐的 AWS Organizations 架构，并 account-by-account描述了哪些服务的去向。要开始了解列表中的第二个优先级（如何考虑全套安全服务），请阅读在整个 AWS 组织中应用安全服务一节。本节介绍一种根据 AWS 组织中元素的结构对安全服务进行分组的方法。此外，同样的想法也反映在关于应用程序账户的讨论中，其中重点介绍了如何运营安全服务以专注于账户的某些层：亚马逊弹性计算云 (Amazon EC2) 实例、亚马逊虚拟私有云 (Amazon VPC) 网络以及更广泛的账户。最后，第三个优先事项（服务集成）反映在整个指南中，尤其是在SRA库的深入研究指南中对单个服务的讨论以及 AWS SRA代码库中的代码中 AWS 。

如何使用 AWS SRA

根据您在云采用之旅中所处的阶段，有不同的使用 AWS SRA 的方法。以下列出了从 AWS SRA 资产中获得最大洞察力的方法（架构图、书面指南和代码示例）。

- 为自己的安全架构@@ 定义目标状态。

无论您是刚刚开始 AWS Cloud 旅程（设置第一组帐户），还是计划增强已建立的 AWS 环境，AWS SRA 都是开始构建安全架构的地方。从全面的账户结构和安全服务基础开始，然后根据您的特定技术堆栈、技能、安全目标和合规性要求进行调整。如果您知道自己将构建和启动更多工作负载，则可以采用自定义版本的 AWS SRA，将其用作组织安全参考架构的基础。要了解如何实现 AWS SRA 描述的目标状态，请参阅 “构建您的安全架构 — 分阶段方法” 一节。

- 审查（并修改）您已经实施的设计和功能。

  如果你已经有了安全设计和实现，那么值得花点时间将你所拥有的与 AWS SRA进行比较。 AWS SRA 的设计非常全面，可为审查您自己的安全性提供诊断基准。如果您的安全设计符合 AWS SRA，则可以更有信心在使用 AWS 服务时遵循最佳实践。如果你的安全设计与 AWS SRA 中的指导意见存在分歧甚至不一致，这不一定表明你做错了什么。相反，这个观察结果为你提供了回顾决策过程的机会。出于正当的业务和技术原因，您可能会偏离 AWS SRA 最佳实践。也许您的特定合规性、监管或组织安全要求需要特定的服务配置。或者，您可能不使用 AWS 服务，而是对自己构建和管理的自定义应用程序中的产品 AWS Partner Network 或自定义应用程序有功能偏好。有时，在这次审查中，您可能会发现您之前的决定是基于已不再适用的旧技术、 AWS 功能或业务限制做出的。这是一个很好的机会，可以查看所有更新，确定其优先顺序，并将它们添加到工程待办事项列表的相应位置。无论您在根据 AWS SRA评估安全架构时发现什么，都将发现记录该分析很有价值。拥有决策及其理由的历史记录可以帮助为未来的决策提供信息并确定其优先顺序。

- 引导您自己的安全架构的实现。

  AWS SRA 基础设施即代码 (IaC) 模块提供了一种快速、可靠的方式来开始构建和实施您的安全架构。代码存储库部分和公共 GitHub 存储库中对这些模块进行了更深入的描述。它们不仅使工程师能够在 AWS SRA 指南中的高质量模式示例基础上再接再厉，而且还纳入了推荐的安全控制措施，例如 IAM 密码策略、亚马逊简单存储服务 (Amazon S3) Simple Storage 封锁账户公开访问、亚马逊 EC2 默认亚马逊弹性区块存储 (Amazon EBS) Elastic Block Store 加密以及与之 AWS Control Tower 集成，以便在新控制措施上线时应用或移除控件退役。 AWS 账户

- 了解有关 AWS 安全服务和功能的更多信息。

  AWS SRA 中的指导和讨论包括个人 AWS 安全和安全相关服务的重要功能以及部署和管理注意事项。 AWS SRA 的一个特点是，它提供了对 AWS 安全服务的广泛性以及它们如何在多账户环境中协同工作的高级介绍。这补充了对其他来源中每项服务的功能和配置的深入研究。这方面的一个例子是关于 AWS Security Hub 云安全态势管理 (AWS Security Hub CSPM) 如何从各种 AWS Partner 产品甚至你自己的应用程序中提取安全发现的AWS 服务讨论。

- 推动关于组织治理和安全责任的讨论。

设计和实施任何安全架构或策略的一个重要因素是了解组织中谁负有哪些与安全相关的责任。例如，在何处汇总和监控安全调查结果的问题与哪个小组将负责该活动有关。整个组织的所有调查结果是否都由需要访问专用安全工具帐户的中央团队监控？ 还是个别应用团队（或业务部门）负责某些监控活动，因此需要访问某些警报和监控工具？ 再举一个例子，如果你的组织有一个集中管理所有加密密钥的群组，那将影响谁有权创建 AWS Key Management Service (AWS KMS) 密钥以及这些密钥将在哪些账户中进行管理。了解组织的特征（不同的团队和职责）将有助于您量身定制最适合您需求的 AWS SRA。相反，有时对安全架构的讨论会成为讨论现有组织职责和考虑潜在变化的动力。AWS 建议采用分散决策流程，由工作量小组负责根据其工作量职能和要求确定安全控制措施。集中式安全和治理团队的目标是构建一个系统，使工作负载所有者能够做出明智的决策，并使所有各方都能了解配置、发现和事件。 AWS SRA可以成为识别和通报这些讨论的工具。

AWS SRA 的关键实施指南

在设计和实施安全措施时，请记住以下 AWS SRA的八个关键要点。

- AWS Organizations 适当的多账户策略是您的安全架构的必要元素。正确分离工作负载、团队和职能为职责和 defense-in-depth策略的分离奠定了基础。本指南将在后面的章节中对此进行进一步介绍。
- Defense-in-depth 是为组织选择安全控制措施的重要设计考虑因素。它可以帮助您在 AWS Organizations 结构的不同层面注入适当的安全控制措施，这有助于最大限度地减少问题的影响：如果某一层存在问题，则有控制措施可以隔离其他宝贵的 IT 资源。 AWS SRA 演示了 AWS 技术堆栈不同层次的不同 AWS 服务 功能，以及组合使用这些服务如何帮助您实现目标 defense-in-depth。后面的章节将进一步讨论这个 defense-in-depth概念，并在应用程序帐户下显示设计示例。 AWS
- 使用涵盖多个 AWS 服务 和功能的各种安全构建块来构建强大而有弹性的云基础架构。在根据您的特定需求定制 AWS SRA 时，不仅要考虑其主要功能 AWS 服务 和功能（例如身份验证、加密、监控、权限策略），还要考虑它们如何融入您的架构结构。本指南的后面部分将介绍某些服务在整个 AWS 组织中的运行方式。其他服务最好在一个账户内运行，有些服务旨在向个人委托人授予或拒绝许可。考虑这两个角度可以帮助您构建更灵活、更分层的安全方法。
- 在可能的情况下（详见后面的章节），利用可在每个账户（分布式而不是集中式）中部署的功能，并构建一组一致的共享护栏，以帮助保护您的工作负载免遭滥用，并帮助减少安全事件的影响。 AWS 服务 AWS SRA 使用 AWS Security Hub CSPM （集中式发现监控和合规性检查）、Amazon GuardDuty（威胁检测和异常检测）、 AWS Config （资源监控和变更检测）、IAM Access Analyzer AWS CloudTrail （资源访问监控）、（记录环境中的服务 API 活动）和 Amazon Macie（数据分类）作为在每个环境中部署的基础集 AWS 服务 。 AWS 账户
- 使用支持的委托管理功能 AWS Organizations，如本指南的委托管理部分稍后所述。这样，您就可以将 AWS 成员帐户注册为受支持服务的管理员。委托管理为企业内的不同团队提供了灵活性，允许他

们根据自己的职责使用不同的账户来管理 AWS 服务 整个环境。此外，使用委派管理员可以帮助您限制对管理账户的访问权限并 AWS Organizations 管理其权限开销。

- 在整个 AWS 组织中实施集中式监控、管理和治理。通过使用 AWS 服务 支持多账户（有时还有多区域）聚合以及委托管理功能，您可以让中央安全、网络和云工程团队对适当的安全配置和数据收集拥有广泛的可见性和控制力。此外，可以将数据提供给工作负载团队，使他们能够在软件开发生命周期 (SDLC) 的早期做出有效的安全决策。
- 使用预先构建的安全控制 AWS Control Tower 来设置和管理您的多账户 AWS 环境，从而引导您的安全参考架构构建。 AWS Control Tower 提供了一个蓝图，用于提供身份管理、账户联合访问权限、集中式日志记录以及用于配置其他账户的已定义工作流程。然后，您可以使用 “定制” AWS Control Tower (cfcT) 解决方案，通过其他安全控制、服务配置和监管来对所 AWS Control Tower 管理的账户进行基准，如 AWS SRA 代码存储库所示。账户工厂功能可根据已批准的账户配置，使用可配置的模板自动配置新账户，以标准化 AWS 组织内的账户。您还可以将管理范围扩展到已受其管理的组织单位 (OU)， AWS 账户 从而将治理范围扩大到现有个人。 AWS Control Tower
- AWS SRA 代码示例演示了如何使用基础设施即代码 (IaC) 在 AWS SRA 指南中自动实现模式。通过编纂模式，您可以像对待组织中的其他应用程序一样对待 IaC，并在部署代码之前自动进行测试。IaC 还通过在多个（例如 SDLC 或特定区域）环境中部署护栏，帮助确保一致性和可重复性。SRA 代码示例可以在带或不带的 AWS Organizations 多账户环境中部署。 AWS Control Tower 此存储库中需要的解决方案 AWS Control Tower 已通过使用和定制 AWS Control Tower (cfCT) 在 AWS Control Tower环境中进行部署 AWS CloudFormation和测试。不需要的解决方案 AWS Control Tower 已在AWS Organizations环境中使用进行了测试AWS CloudFormation。如果您不使用 AWS Control Tower，则可以使用AWS Organizations基于的部署解决方案。

安全基础知识

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

AWS SRA与三个 AWS 安全基础保持一致： AWS 云采用框架（AWS CAF）、Well-Architected和责任 AWS 共担模型。 AWS

AWS Professional Services 创建了 AWS CAF，旨在帮助公司设计并加快成功采用云的道路。该框架提供的指导和最佳实践可帮助您在整个企业和整个 IT 生命周期中构建全面的云计算方法。 AWS CAF 将指导分为六个重点领域，称为视角。每个视角都涵盖与职能相关的利益相关者拥有或管理的不同职责。一般而言，业务、人员和治理视角侧重于业务能力；而平台、安全和运营视角侧重于技术能力。

AWS CAF 的安全视角可帮助您在整个企业中组织控制措施的选择和实施。遵循安全支柱中的当前 AWS 建议可以帮助您满足业务和监管要求。

AWS Wel l-Architected 帮助云架构师为其应用程序和工作负载构建安全、高性能、弹性和高效的基础架构。该框架基于六大支柱（卓越运营、安全性、可靠性、性能效率、成本优化和可持续性），为 AWS 客户和合作伙伴提供了一种一致的方法来评估架构和实施可随时间推移而扩展的设计。我们相信，拥有架构完善的工作负载能够大大提高实现业务成功的可能性。

Wel l-Architected Framework 安全支柱描述了如何利用云技术来帮助保护数据、系统和资产，从而改善您的安全状况。通过遵循当前 AWS 的建议，这将帮助您满足业务和监管要求。Well-Architected Framework 还有其他重点领域，可以为治理、无服务器、人工智能/机器学习和游戏等特定领域提供更多背景信息。这些镜头被称为 Well-Arch AWS itected 镜头。

安全和合规是客户共同承担 AWS 的责任。这种共享模型可以帮助您减轻运营负担，因为您可以 AWS 操作、管理和控制从主机操作系统和虚拟化层到服务运行设施的物理安全的组件。例如，您负责并管理客户机操作系统（包括更新和安全补丁）、应用程序软件、服务器端数据加密、网络流量路由表以及 AWS提供的安全组防火墙的配置。对于 Amazon S3 和 Amazon AWS DynamoDB 等抽象服务，运行基础设施层、操作系统和平台，您可以访问终端节点来存储和检索数据。您负责管理数据（包括加密选项）、对资产进行分类以及使用 IAM 工具应用适当的权限。这种共享模式通常被描述 AWS 为负责云的安全（即保护运行云中提供的所有服务的基础架构 AWS Cloud），而您对云中的安全负责（由您选择的 AWS Cloud 服务决定）。

在这些基础文档提供的指导中，有两组概念与 AWS SRA的设计和理解特别相关：安全功能和安全设计原则。

安全能力

AWS CAF 的安全视角概述了九项功能，可帮助您实现数据和云工作负载的机密性、完整性和可用性。

- 安全治理，用于在组织 AWS 环境中制定和沟通安全角色、职责、政策、流程和程序。
- 安全保障，用于监控、评估、管理和提高您的安全和隐私计划的有效性。
- 身份和访问管理，用于大规模管理身份和权限。
- 威胁检测，用于了解和识别潜在的安全配置错误、威胁或意外行为。
- 漏洞管理可持续识别、分类、修复和缓解安全漏洞。
- 基础设施保护，可帮助验证工作负载中的系统和服务是否受到保护。
- 数据保护可保持对数据的可见性和控制力，以及对组织中访问和使用数据的方式。
- 应用程序安全，可帮助检测和解决软件开发过程中的安全漏洞。
- 事件响应，通过有效应对安全事件来减少潜在伤害。

安全设计原则

Well-Architected Framework 的安全支柱包含一组七项设计原则，这些原则将特定的安全领域转化为实用指南，可以帮助您增强工作负载安全。在安全功能构成整体安全策略的地方，这些 Well-Architected Framework 原则描述了你可以开始做什么。它们非常谨慎地反映在本 AWS SRA中，包括以下内容：

- 建立坚实的身份基础 – 实施最小权限原则，在每次与 AWS 资源的互动中都要有适当的授权，强制执行职责分离。集中进行身份管理，并努力消除对长期静态凭证的依赖。
- 启用可追溯性 – 实时监控、生成警报并审核环境的操作和更改。为系统集成日志和指标收集功能，以自动调查并采取行动。
- 在所有层面应用安全性 – defense-in-depth 采用具有多种安全控制的方法。将多种类型的控制措施（例如预防和检测控制）应用于所有层，包括网络边缘、虚拟私有云 (VPC)、负载平衡、实例和计算服务、操作系统、应用程序配置和代码。
- 自动化安全最佳实践-基于软件的自动化安全机制可提高您更快、更经济地安全扩展的能力。创建安全的架构，并在版本控制的模板中实现以代码形式定义和管理的控件。
- 保护传输中的数据和静态数据 – 将您的数据按敏感度级别进行分类，并酌情使用加密、标记化和访问控制等机制。
- 让人们远离数据-使用机制和工具来减少或消除直接访问或手动处理数据的需求。这样可以降低处理敏感数据时数据处理不当、被修改以及人为错误的风险。

- 为安全事件做好准备 – 制定符合组织要求的事件管理和调查政策及流程，为事件做好准备。开展意外事件响应模拟演练，并使用具有自动化功能的工具来提高检测、调查和恢复的速度。

如何在 CAF 和 Well- AWS Architected F AWS ramework 中使用 SRA AWS

AWS CAF、Well-Ar AWS chitected Framewor AWS k 和 SRA 是互补的框架，它们共同支持您的云迁移和现代化工作。

- AWS CAF 利用 AWS 经验和最佳实践来帮助您将云采用的价值与所需的业务成果保持一致。使用 AWS CAF 来识别转型机会并确定其优先级，评估和改善云就绪性，并迭代发展您的转型路线图。
- Wel AWS l-Architected Framework 为各种应用程序和工作负载构建安全、高性能、弹性和高效的基础架构 AWS 提供了建议，以满足您的业务成果。
- AWS SRA 可帮助您了解如何以符合 CAF 和 Well- AWS Architected Framework 建议的方式部署和管理安全服务。 AWS

例如， AWS CAF 安全视角建议您评估如何集中管理员工身份及其身份验证。 AWS根据这些信息，您可以决定为此目的使用新的或现有的企业身份提供商 (IdP) 解决方案，例如 Okta、Active Directory 或 Ping Identity。您按照 Well-Architect AWS ed Framework 中的指导进行操作，并决定将您的 IdP 与 AWS IAM Identity Center 集成，为您的员工提供单点登录体验，使其群组成员资格和权限同步。您可以查看 AWS SRA 建议，在 AWS 组织的管理账户中启用 IAM Identity Center，并通过安全运营团队使用的安全工具账户对其进行管理。此示例说明 AWS 了 AWS CAF 如何帮助您就所需的安全态势做出初步决策，Well-Architected Framework 提供了有关如何评估 AWS 服务 可用于实现该目标的指导，然后 SRA 就如何部署和管理您选择的安全服务提供了建议。 AWS

SRA 的基石 — AWS Organizations、账户和护栏

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

AWS 最好在 AWS多账户策略以及身份和访问管理护栏的基础上使用安全服务、其控制和交互。这些护栏设置了您实施最低权限、职责分离和隐私的能力，并为决定需要哪些类型的控制、每项安全服务的管理位置以及它们如何在 SRA 中共享数据和权限提供了支持。 AWS

为您的 AWS 资源 AWS 账户 提供安全性、访问权限和计费界限，使您能够实现资源独立和隔离。如使用多个账户组织环境白皮书的 “使用多个账户组织 AWS 环境” 的 “使用多个账户的好处 AWS 账户” 部分所述，使用多个账户在满足安全要求方面 AWS 账户 起着重要作用。例如，您可以根据职能、合规性要求或一组常用控件将工作负载组织到单独的账户中，并对组织单位 (OU) 内的账户进行分组，而不是镜像企业的报告结构。请牢记安全和基础架构，使您的企业能够随着工作负载的增长设置共同的护栏。这种方法在工作负载之间提供了强大的界限和控制。账户级分离与之相结合，用于将生产环境与 AWS Organizations开发和测试环境隔离开来，或者在处理不同分类（例如支付卡行业数据安全标准 (PCI DSS) 或《健康保险便携性与责任法案》(HIPAA)）等不同类别的数据的工作负载之间提供强大的逻辑界限。尽管您可能从一个账户开始您的 AWS 旅程，但 AWS 建议您随着工作负载规模和复杂性的增加而设置多个帐户。

权限允许您指定对 AWS 资源的访问权限。权限被授予被称为委托人（用户、群组和角色）的 IAM 实体。默认情况下，委托人一开始就没有权限。在您向他们授予权限 AWS 之前，IAM 委托人无法在其中执行任何操作，并且您可以设置防护栏，其范围与整个 AWS 组织一样广泛，也可以像委托人、操作、资源和条件的个人组合一样精细地适用。

AWS Organizations 出于安全考虑

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

AWS Organizations随着 AWS 资源的增长和扩展，可以帮助你集中管理和治理环境。通过使用 AWS Organizations，您可以以编程方式创建新账户 AWS 账户、分配资源、对账户进行分组以组织工作负载，以及将策略应用于账户或账户组进行管理。一个 AWS 组织会整合你的， AWS 账户 这样你就可以把它们当作一个单位来管理。它有一个管理账户以及零个或多个成员账户。您的大部分工作负载都驻留在成员账户中，但某些集中管理的流程除外，这些流程必须位于管理账户或指定为委托管理员的账户中

AWS 服务。您可以从中心位置为安全团队提供工具和访问权限，以代表 AWS 组织管理安全需求。您可以通过在 AWS 组织内共享关键资源来减少资源重复。您可以将帐户分组为 AWS 组织单位 (OUs)，这些单位可以根据工作负载的要求和目的代表不同的环境。 AWS Organizations 还提供了多项策略，使您能够对组织中的所有成员帐户集中应用额外的安全控制。本节重点介绍服务控制策略 (SCPs)、资源控制策略 (RCPs) 和声明性策略。

使用 AWS Organizations，您可以在 AWS 组织、OU 或账户级别使用SCPs和RCPs应用权限护栏。SCPs 是适用于组织账户内委托人的护栏，但管理账户除外（这是不在此账户中运行工作负载的原因之一）。当您将 SCP 附加到 OU 时，该 SCP 将由该组织下的子女 OUs 和账户继承。 SCPs 不要授予任何权限。相反，它们会指定您的委托人在 AWS 组织、组织单位或账户中可用的最大权限。您仍然需要将基于身份或基于资源的策略附加到您的委托人或资源，才能实际 AWS 账户 向他们授予权限。例如，如果 SCP 拒绝访问所有 Amazon S3，则即使通过 IAM 策略明确授予访问权限，受 SCP 影响的委托人也无法访问 Amazon S3。有关如何评估 IAM 策略、角色以及最终如何授予或拒绝访问权限的更多信息，请参阅 IAM 文档中的策略评估逻辑。 SCPs

RCPs 是适用于组织账户内资源的护栏，无论这些资源是否属于同一个组织。比如 SCPs， RCPs不要影响管理账户中的资源，也不要授予任何权限。当您将 RCP 附加到 OU 时，RCP 将由子项 OUs 和 OU 下的帐户继承。 RCPs 提供对组织中资源的最大可用权限的集中控制，目前支持其中的一部分 AWS 服务。在 SCPs 为您的设计时 OUs，我们建议您使用 IAM 策略模拟器评估更改。您还应查看 IAM 中上次访问的服务数据，AWS CloudTrail 并用于在 API 级别记录服务使用情况，以了解 SCP 更改的潜在影响。

SCPs 并且 RCPs 是独立的控制机构。您可以根据要实施的访问控制选择仅启用 SCPs 或 RCPs，或者同时使用这两种策略类型。例如，如果您想阻止组织的委托人访问组织外部的资源，则可以通过使用 SCPs来强制执行此控制。如果您想限制或阻止外部身份访问您的资源，则可以使用来强制执行此控制 RCPs。有关和的更多 RCPs 信息和用例 SCPs，请参阅 AWS Organizations 文档 RCPs中的使用 SCPs 和。

您可以使用 AWS Organizations 声明性策略 AWS 服务 在整个组织中大规模地集中声明和强制执行所需的配置。例如，您可以屏蔽整个组织中对 Amazon VPC 资源的公共互联网访问权限。与 SCPs 和等授权策略不同 RCPs，声明式策略是在 AWS 服务的控制平面中强制执行的。授权策略规范对访问的访问 APIs，而声明性策略则直接应用于服务级别以强制执行持久意图。 这些策略有助于确保始终保持的 AWS 服务 基准配置，即使服务引入了新功能或 APIs。当向组织添加新账户或创建新的主体和资源时，也会保持基准配置。声明式策略可以应用于整个组织或特定 OUs 或帐户。

每个用户 AWS 账户 都有一个 root 用户，默认情况下该用户对所有 AWS 资源拥有完全权限。 作为安全最佳实践，我们建议您不要使用 root 用户，只有少数任务明确需要 root 用户。如果您 AWS 账户 通过管理多个 AWS Organizations，则可以集中禁用 root 登录，然后代表所有成员账户执行 root 权限操作。集中管理成员账户的根访问权限后，您可以删除根用户密码、访问密钥和签名证书，并停用成员账

户的多因素身份验证 (MFA)。默认情况下，在集中管理的 root 访问权限下创建的新账户没有 root 用户证书。成员账户无法使用其根用户登录或为其根用户执行密码恢复。

AWS Control Tower提供了一种设置和管理多个帐户的简化方法。它可以自动设置 AWS 组织中的帐户，自动进行配置，应用控制措施（包括预防和侦查控制），并为您提供可见性的仪表板。附加的 IAM 管理策略（权限边界）附加到特定的 IAM 委托人（用户或角色），用于设置基于身份的策略可以向 IAM 委托人授予的最大权限。

AWS Organizations 帮助您进行适用于AWS 服务所有账户的配置。例如，您可以使用配置在 AWS 组织中执行的所有操作的集中日志记录 CloudTrail，并防止成员帐户禁用日志记录。您还可以集中汇总您通过使用定义的规则的数据 AWS Config，这样您就可以审计工作负载的合规性并对变化做出快速反应。您可以使用AWS CloudFormation StackSets集中管理各个账户和 AWS 组织 OUs 中的 CloudFormation 堆栈，这样您就可以自动配置一个新帐户以满足您的安全要求。

AWS Organizations 支持使用 SCPs 作为拒绝列表的默认配置。通过使用拒绝列表策略，成员账户管理员可以委托所有服务和操作，直到您创建并附加拒绝特定服务或一组操作的 SCP 为止。与允许列表相比，拒绝语句需要更少的维护，因为在 AWS 添加新服务时您不必更新它们。拒绝语句的字符长度通常较短，因此更容易保持在最大长度以内 SCPs。在`Effect`元素值为的语句中`Deny`，您还可以限制对特定资源的访问权限，或者定义何时生效 SCPs 的条件。相比之下，SCP 中的`Allow`语句适用于所有资源 ("*")，并且不能受条件限制。有关更多信息和示例，请参阅 AWS Organizations 文档 SCPs中的使用策略。

设计注意事项

- 或者，要 SCPs 用作允许列表，您必须将 AWS 托管 `FullAWSAccess` SCP 替换为明确仅允许您想要允许的服务和操作的 SCP。要为指定账户启用权限，每个 SCP（从根目录到账户直接路径中的每个 OU，甚至附加到账户本身）都必须允许该权限。这种模式本质上更具限制性，可能适合高度监管和敏感的工作负载。这种方法要求您明确允许从到 OU 的路径中的每个 IAM 服务或操作。 AWS 账户
- 理想情况下，您可以结合使用拒绝列表和允许列表策略。使用允许列表定义允许在 AWS 组织内使用的 AWS 服务 已批准列表，并将此 SCP 附加到 AWS 组织的根目录。如果您的开发环境允许使用不同的服务集，则需要 SCPs 在每个 OU 中附加相应的服务。然后，您可以使用拒绝列表通过明确拒绝特定的 IAM 操作来定义企业护栏。
- RCPs 适用于其子集的资源 AWS 服务。有关更多信息，请参阅 AWS Organizations 文档 RCPs中的支持列表。 AWS 服务 默认配置 AWS Organizations 支持使用 RCPs 作为拒绝列表。当您在组织 RCPs 中启用时，名`RCPFullAWSAccess`为的 AWS 托管策略将自动附加到组织根目录、每个 OU 和组织中的每个账户。您无法分离此策略。此默认 RCP 允许所有

委托人和操作访问权限通过 RCP 评估。这意味着，在您开始创建和附加之前 RCPs，您的所有现有 IAM 权限将继续按原样运行。此 AWS 托管策略不授予访问权限。然后，您可以创 RCPs 作新的拒绝语句列表，以阻止对组织中资源的访问。

管理账户、可信访问权限和委派管理员

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

管理账户（也称为 AWS 组织管理账户或组织管理账户）是独一无二的，不同于中的所有其他账户 AWS Organizations。创建 AWS 组织的是账户。通过此账户，您可以在 AWS 组织 AWS 账户 中创建、邀请其他现有账户加入 AWS 组织（两种类型均被视为成员账户）、从 AWS 组织中移除账户以及将 IAM 策略应用于 AWS 组织内的根账户或账户。 OUs

管理账户通过 SCPs、 RCPs和服务部署（例如 CloudTrail）部署通用安全防护栏，这将影响组织中的所有成员账户。 AWS 为了进一步限制管理账户中的权限，可以尽可能将这些权限委托给其他相应的账户，例如安全账户。

管理账户具有付款人账户的责任，并负责支付成员账户产生的所有费用。您无法切换 AWS 组织的管理帐户。一个 AWS 账户 人一次只能是一个 AWS 组织的成员。

由于管理账户的功能和影响范围，我们建议您限制对该账户的访问权限，并仅向需要权限的角色授予权限。可帮助您实现此目的的两个功能是可信访问权限和委派管理员。您可以使用可信访问权限来启用您指定的名为 AWS 服务 可信服务的可信服务，以代表您执行 AWS 组织及其账户中的任务。这涉及向信任服务授予权限，但不会以其他方式影响 IAM 用户或角色的权限。您可以使用可信访问权限来指定您希望受信任的服务代表您保留在 AWS 组织账户中的设置和配置详细信息。例如， AWS SRA 的组织管理账户部分说明了如何向 CloudTrail 服务授予可信访问权限，以便在 CloudTrail 组织中的所有账户中创建 AWS 组织跟踪。

有些 AWS 服务 支持中的委托管理员功能 AWS Organizations。使用此功能，兼容的服务可以将 AWS 组织中的 AWS成员帐户注册为该服务中 AWS 组织帐户的管理员。此功能为企业内的不同团队提供了灵活性，使他们能够根据自己的职责使用不同的账户来管理 AWS 服务 整个环境。 AWS SRA 中目前支持委托管理员 AWS 的安全服务包括 IAM 身份中心、、、亚马逊、IAM Access Analyzer AWS Config AWS Firewall Manager、Amazon Macie GuardDuty、云安全态势管理AWS Security Hub CSPM()、Amazon Detective AWS Security Hub 、Amazon Inspector、Amazon Inspector 和。 AWS Audit Manager AWS Systems Manager作为最佳实践， AWS SRA 强调使用委派管理员功能，我们将安全相关服务的管理委托给安全工具账户。

专用账户结构

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

为您的 AWS 资源 AWS 账户 提供安全性、访问权限和计费界限，并使您能够实现资源独立和隔离。默认不允许在账户之间进行访问。

在设计 OU 和账户结构时，首先要考虑安全性和基础架构。我们建议 OUs 为这些特定功能创建一组基础知识，分为 “基础架构” 和 “安全 OUs”。这些 OU 和账户建议包含了我们更广泛、更全面的 AWS Organizations 多账户结构设计指南中的一部分。有关全套建议，请参阅 AWS 文档中的使用多个账户组织 AWS 环境，以及博客文章《组织单位最佳实践》 AWS Organizations。

AWS SRA利用以下帐户来实现有效的安全操作。 AWS这些专用账户有助于确保职责分工，为不同的应用程序和数据敏感度支持不同的治理和访问策略，并有助于减轻安全事件的影响。在接下来的讨论中，我们将重点介绍生产（生产）客户及其相关的工作负载。软件开发生命周期 (SDLC) 帐户（通常称为开发和测试帐户）用于暂存可交付成果，并且可以在与生产帐户不同的安全策略下运行。

Account	OU	安全角色
管理	—	对所有人和账户进行中央治理 AWS 区域 和管理。 AWS 账户 承载 AWS 组织根的。
安全工具	安全性	专门 AWS 账户 用于运营广泛适用的安全服务（例如 Security Hub CSPM GuardDuty、Audit Manager、Detective、Amazon Inspector 和 AWS Config）AWS 账户、监控和自动发送安全警报和响应。（在中 AWS Control Tower，安全 OU 下帐户的默认名称为 “审核帐户”。）
日志存档	安全性	专门 AWS 账户 用于接收和存档所有和的所有日志记录和备

		份。 AWS 区域 AWS 账户这应该设计为不可变的存储。
Network	Infrastructure	您的应用程序和更广泛的互联网之间的网关。网络帐户将更广泛的网络服务、配置和操作与单个应用程序工作负载、安全和其他基础设施隔离开来。
共享服务	Infrastructure	此账户支持多个应用程序和团队用来交付成果的服务。示例包括身份中心目录服务（Active Directory）、邮件服务和元数据服务。
应用程序	工作负载	AWS 账户 托管 AWS 组织的应用程序并执行工作负载。（这些帐户有时被称为工作负载帐户。）应创建应用程序帐户以隔离软件服务，而不是映射到您的团队。这使得部署的应用程序更能适应组织变革。

AWS AWS SRA 的组织和账户结构

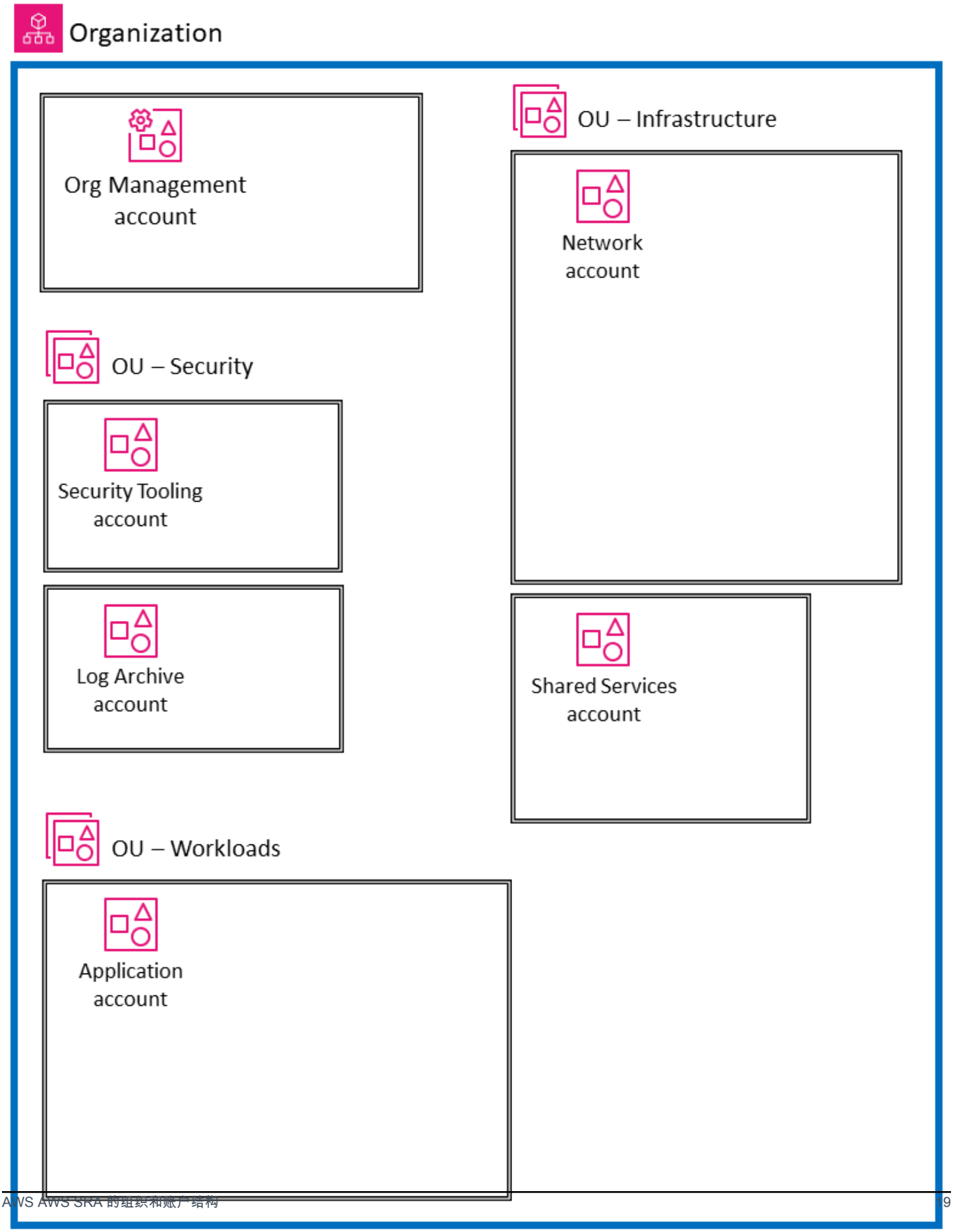
通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

下图捕捉了 AWS SRA 的高级结构，但不显示特定的服务。它反映了上一节中讨论的专用账户结构，我们在此处加入了图表，以围绕架构的主要组件进行讨论：

- 图中显示的所有账户都属于一个 AWS 组织。
- 图的左上角是组织管理账户，用于创建 AWS 组织。
- 组织管理账户下方是具有两个特定帐户的安全 OU：一个用于安全工具，另一个用于日志存档。
- 右侧是带有网络帐户和共享服务帐户的基础架构 OU。
- 图的底部是工作负载 OU，它与存放企业应用程序的应用程序帐户相关联。

在本指南中，所有账户都被视为在单个 AWS 区域账户中运行的生产（生产）账户。大多数 AWS 服务（全球服务除外）都是按区域划分的，这意味着服务的控制平面和数据平面独立存在于每个服务中。AWS 区域因此，您必须在计划使用的所有 AWS 区域 内容中复制此架构，以确保覆盖整个 AWS 景观。如果您在特定区域中没有任何工作负载 AWS 区域，则应使用SCPs或使用日志和监控机制禁用该区域。您可以使用 Security Hub CSPM 将多个聚合区域的发现结果和安全评分汇总 AWS 区域 到单个聚合区域，以实现集中可见性。

在托管拥有大量账户的 AWS 组织时，拥有一个便于账户部署和账户管理的协调层是有益的。 AWS Control Tower 提供了一种设置和管理 AWS 多账户环境的简单方法。GitHub 存储库中的 AWS SRA 代码示例演示了如何使用定制 AWS Control Tower (cfcT) 解决方案来部署 AWS SRA 推荐的结构。

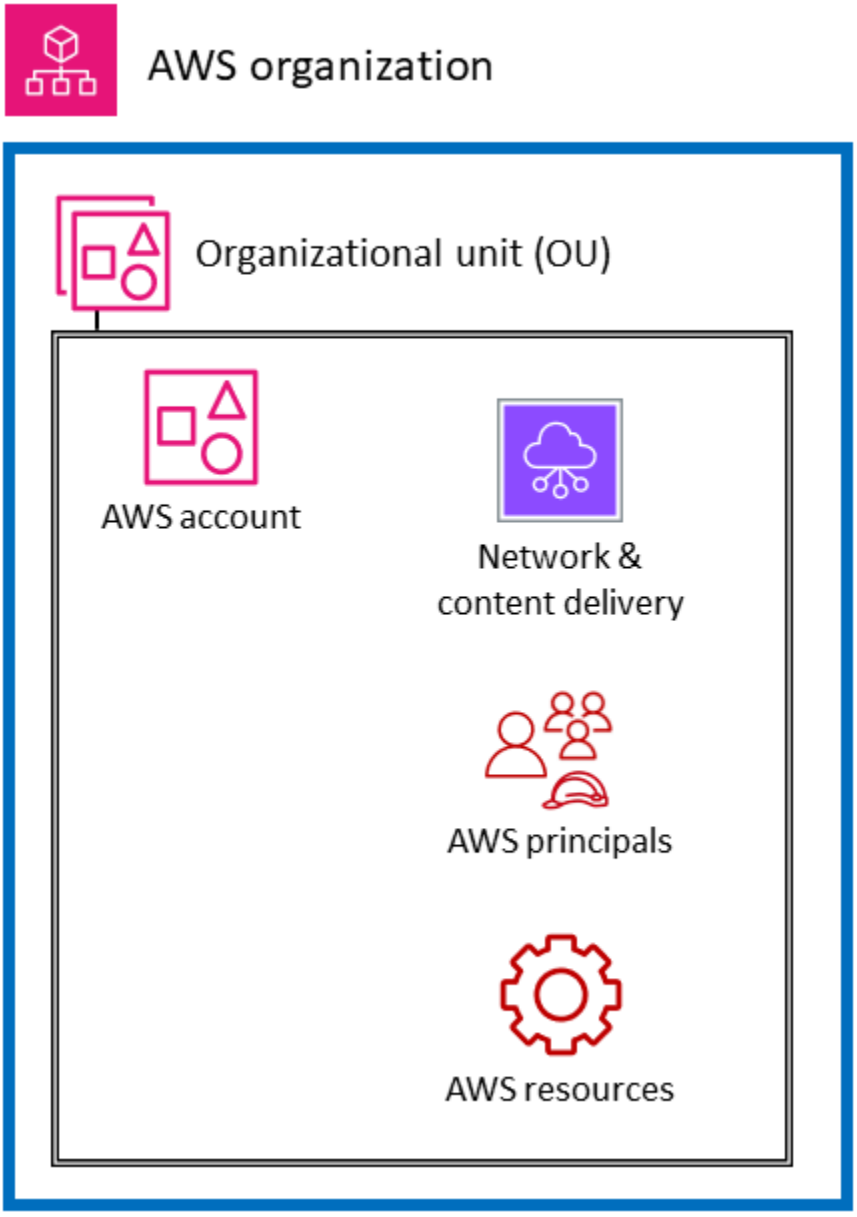

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

在整个 AWS 组织中应用安全服务

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

如前一节所述，客户正在寻找另一种方法来思考和战略性地组织全套 AWS 安全服务。当今最常见的组织方法是按主要职能对安全服务进行分组，具体取决于每项服务的用途。 AWS CAF 的安全视角列出了九项功能，包括身份和访问管理、基础设施保护、数据保护和威胁检测。 AWS 服务 与这些功能能力相匹配是在每个领域做出实施决策的实用方法。例如，在考虑身份和访问管理时，IAM 和 IAM 身份中心是需要考虑的服务。在设计威胁检测方法时， GuardDuty 可能是您的首要考虑因素。

作为此功能视图的补充，您还可以使用跨领域的结构视图来查看您的安全性。也就是说，除了问 “我 AWS 服务 应该用哪个来控制和保护我的身份、逻辑访问或威胁检测机制？”，你也可以问：“我 AWS 服务 应该在整个 AWS 组织中申请哪个？ 我应该设置哪些防御层来保护作为应用程序核心的 Amazon EC2 实例？” 在此视图中，您可以将地图 AWS 服务 和要素映射到 AWS 环境中的图层。有些服务和功能非常适合在整个 AWS 组织中实施控制措施。例如，阻止公众访问 Amazon S3 存储桶是该层的特定控制措施。最好在根组织中完成，而不是作为个人账户设置的一部分。最好使用其他服务和功能来帮助保护内部的个人资源 AWS 账户。此类别的一个例子是，在需要私有 TLS 证书的账户中实现从属证书颁发机构 (CA)。另一个同样重要的分组包括对 AWS 基础架构的虚拟网络层产生影响的服务。下图显示了典型 AWS 环境中的六个层： AWS 组织、组织单位 (OU)、帐户、网络基础架构、委托人和资源。



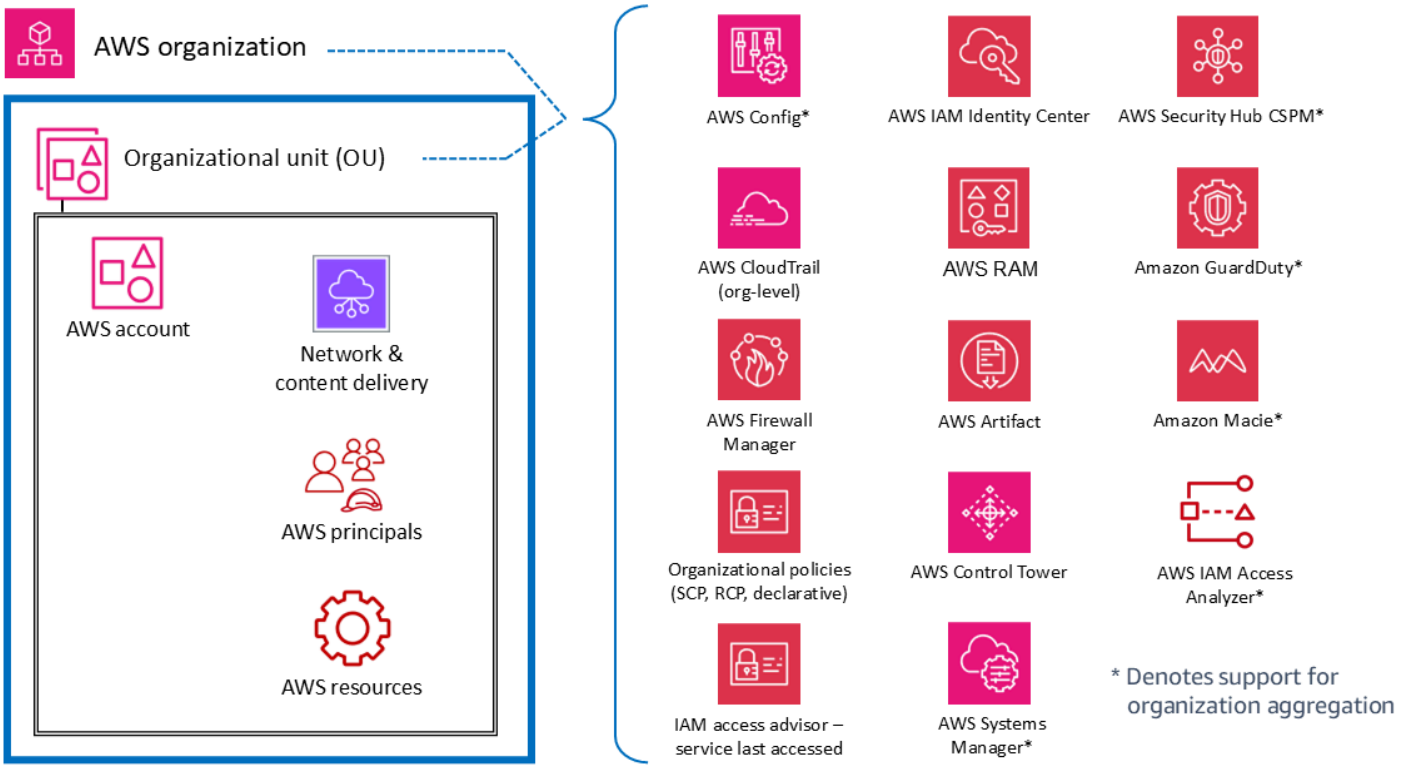
了解这种结构环境中的服务，包括每层的控制和保护，可以帮助您在整个 AWS 环境中规划和实施 defense-in-depth策略。从这个角度来看，你可以自上而下地回答两个问题（例如，“我使用哪些服务在整个 AWS 组织中实施安全控制？”）并自下而上（例如，“哪些服务管理对此 EC2 实例的控制？”）。在本节中，我们将介绍 AWS 环境的各个要素，并确定相关的安全服务和功能。当然，有些 AWS 服务具有广泛的功能集并支持多个安全目标。这些服务可能支持您 AWS 环境的多个元素。

为清楚起见，我们简要描述了某些服务如何符合既定目标。下一节将进一步讨论每项服务中的各项服务 AWS 账户。

组织范围的账户或多个账户

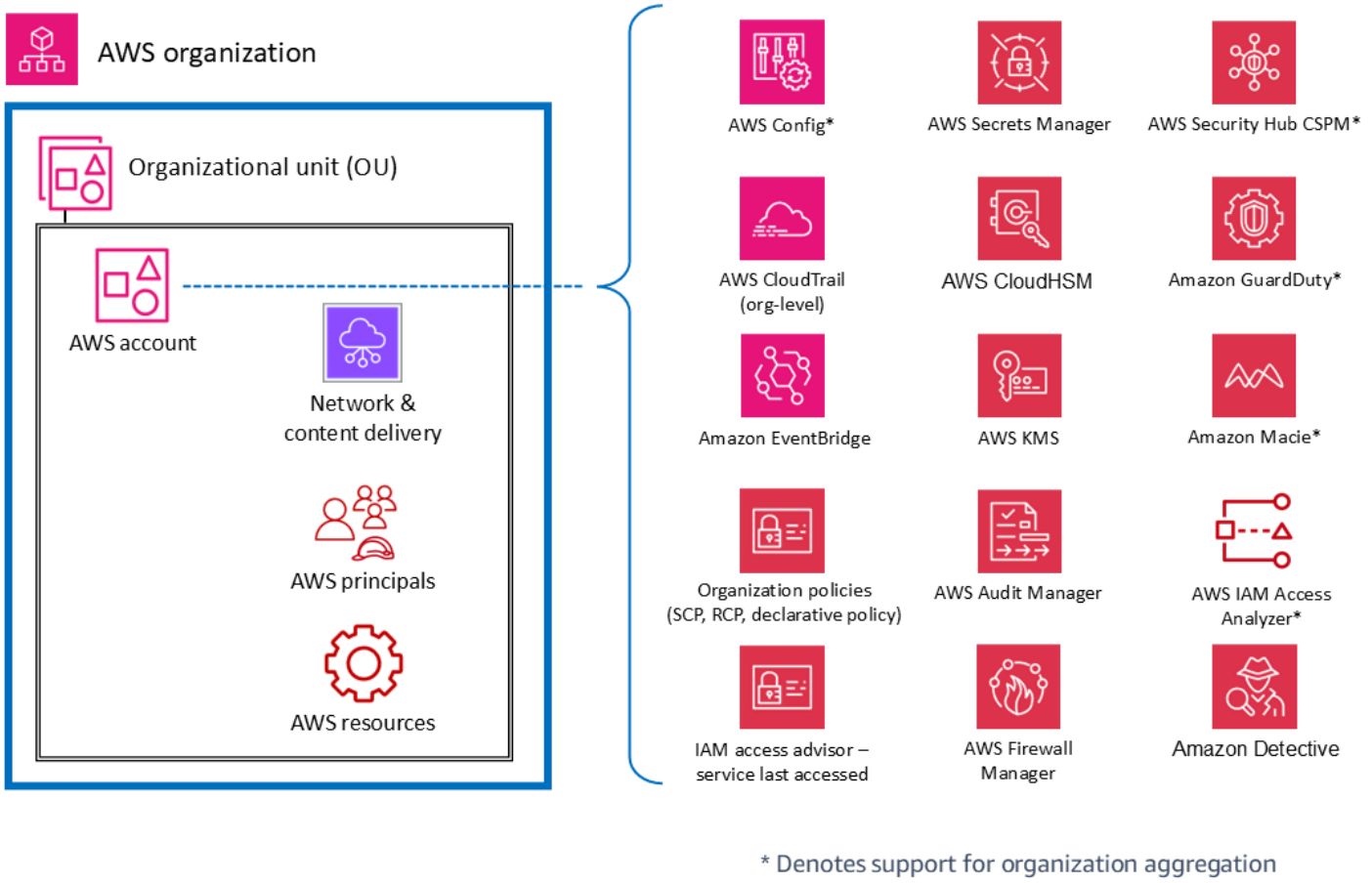
在顶层，有 AWS 服务 一些功能旨在将治理和控制能力或护栏应用于组织中的多个帐户（包括整个 AWS 组织或特定 OUs组织）。服务控制策略 (SCPs) 和资源控制策略 (RCPs) 是 IAM 功能的良好示例，这些功能为 AWS 整个组织提供预防性护栏。 AWS Organizations 还提供了一个声明性策略，用于集中定义和强制执行大规模的基准 AWS 服务 配置。另一个例子是 CloudTrail，它通过组织跟踪提供监控，该跟踪记录了该 AWS 组织 AWS 账户 中所有人的所有事件。这种全面的跟踪不同于可能在每个账户中创建的单个跟踪。第三个示例是 AWS Firewall Manager，您可以使用它来配置、应用和管理 AWS 组织中所有账户的多种资源： AWS WAF 规则、 AWS WAF 经典规则、 AWS Shield Advanced 保护、Amazon Virtual Private Cloud (Amazon VPC) 安全组、 AWS Network Firewall 策略和 Amazon Route 53 Resolver DNS 防火墙策略。

下图中标有星号 (*) 的服务具有双重范围：组织范围和以客户为中心。这些服务从根本上监控或帮助控制个人账户的安全性。但是，它们还支持将多个账户的结果汇总到一个组织范围的账户中，以实现集中可见性和管理。为清楚起见 SCPs ，请考虑这适用于整个 OU 或 AWS 组织。 AWS 账户相比之下，您可以在账户级别（生成个人调查结果的地方）和 AWS 组织级别（使用委托管理员功能）配置和管理 GuardDuty ，在这些级别上，可以聚合查看和管理调查结果。



AWS 账户

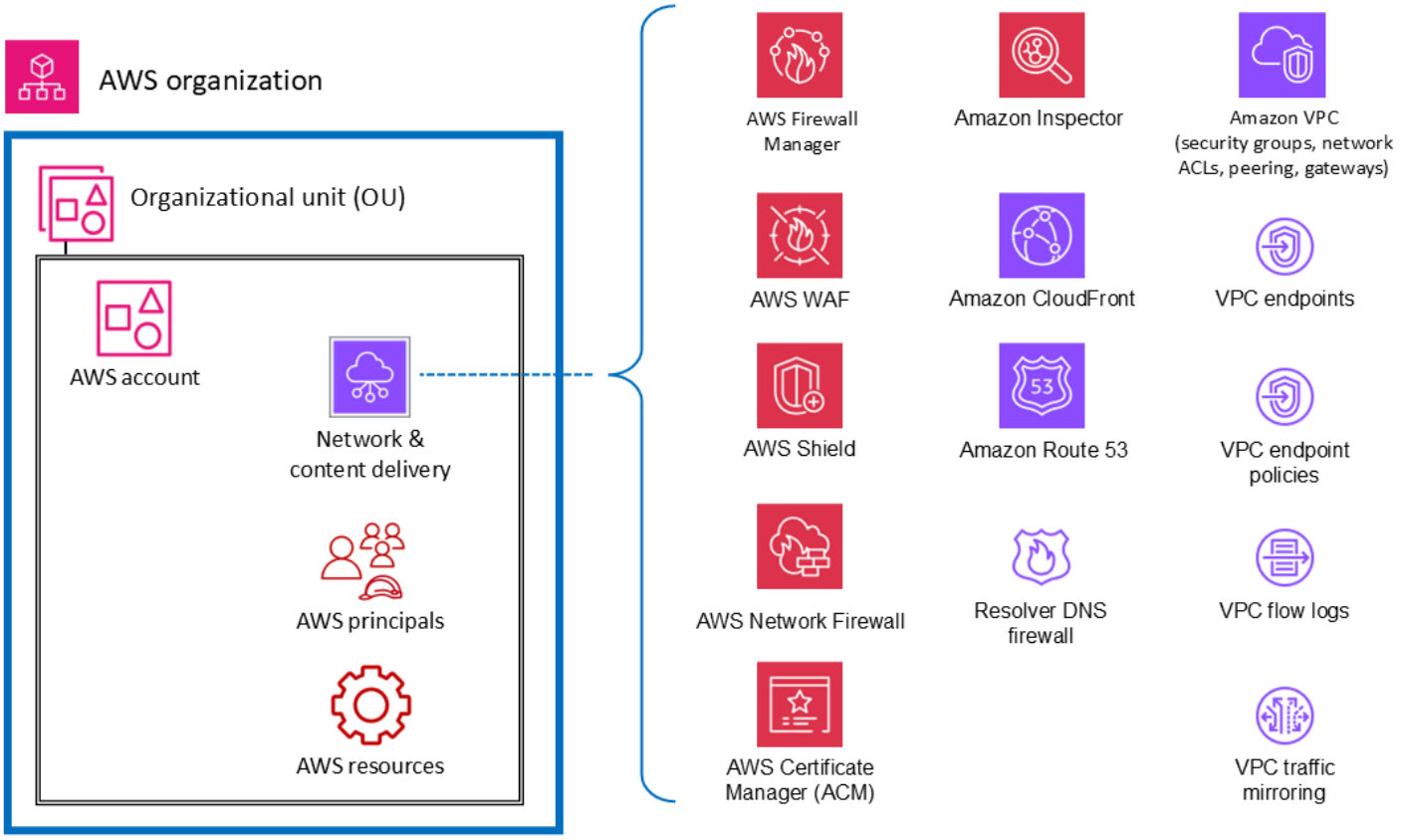
在内部 OUs，有一些服务可以帮助保护其中多种类型的元素 AWS 账户。例如，通常 AWS Secrets Manager 由特定账户进行管理，并保护该账户中的资源（例如数据库凭据或身份验证信息）、应用程序和该账户 AWS 服务 中的资源。可以将 IAM Access Analyzer 配置为在外部委托人可以访问指定资源时生成调查结果。 AWS 账户如上一节所述，其中许多服务也可以在其中配置和管理 AWS Organizations，因此可以跨多个账户进行管理。这些服务在图中标有星号 (*)。它们还可以更轻松地汇总来自多个账户的结果并将其发送到单个账户。这为各个应用程序团队提供了灵活性和可见性，以管理特定于其工作负载的安全需求，同时还允许集中式安全团队进行管理和可见性。 GuardDuty 就是此类服务的一个例子。 GuardDuty 监控与单个账户关联的资源和活动，并且可以通过委派的管理员账户收集、查看和管理来自多个成员账户（例如 AWS 组织中的所有账户）的 GuardDuty 调查结果。



虚拟网络、计算和内容交付

由于网络访问对安全至关重要，而计算基础设施是许多 AWS 工作负载的基本组成部分，因此有许多 AWS 安全服务和功能专用于这些资源。例如，Amazon Inspector 是一项漏洞管理服务，可以持续扫描您的 AWS 工作负载中是否存在漏洞。这些扫描包括网络可访问性检查，这些检查表明您的环境中允许

通往 Amazon EC2 实例的网络路径。Amazon VPC 允许您定义一个可以在其中启动 AWS 资源的虚拟网络。该虚拟网络与传统网络非常相似，具有多种功能和优点。VPC 终端节点使您能够私密地将您的 VPC 连接到支持的终端节点服务 AWS 服务 以及由其提供支持的终端节点服务 ， AWS PrivateLink 而无需访问互联网的路径。下图说明了以网络、计算和内容交付基础设施为重点的安全服务。



校长和资源

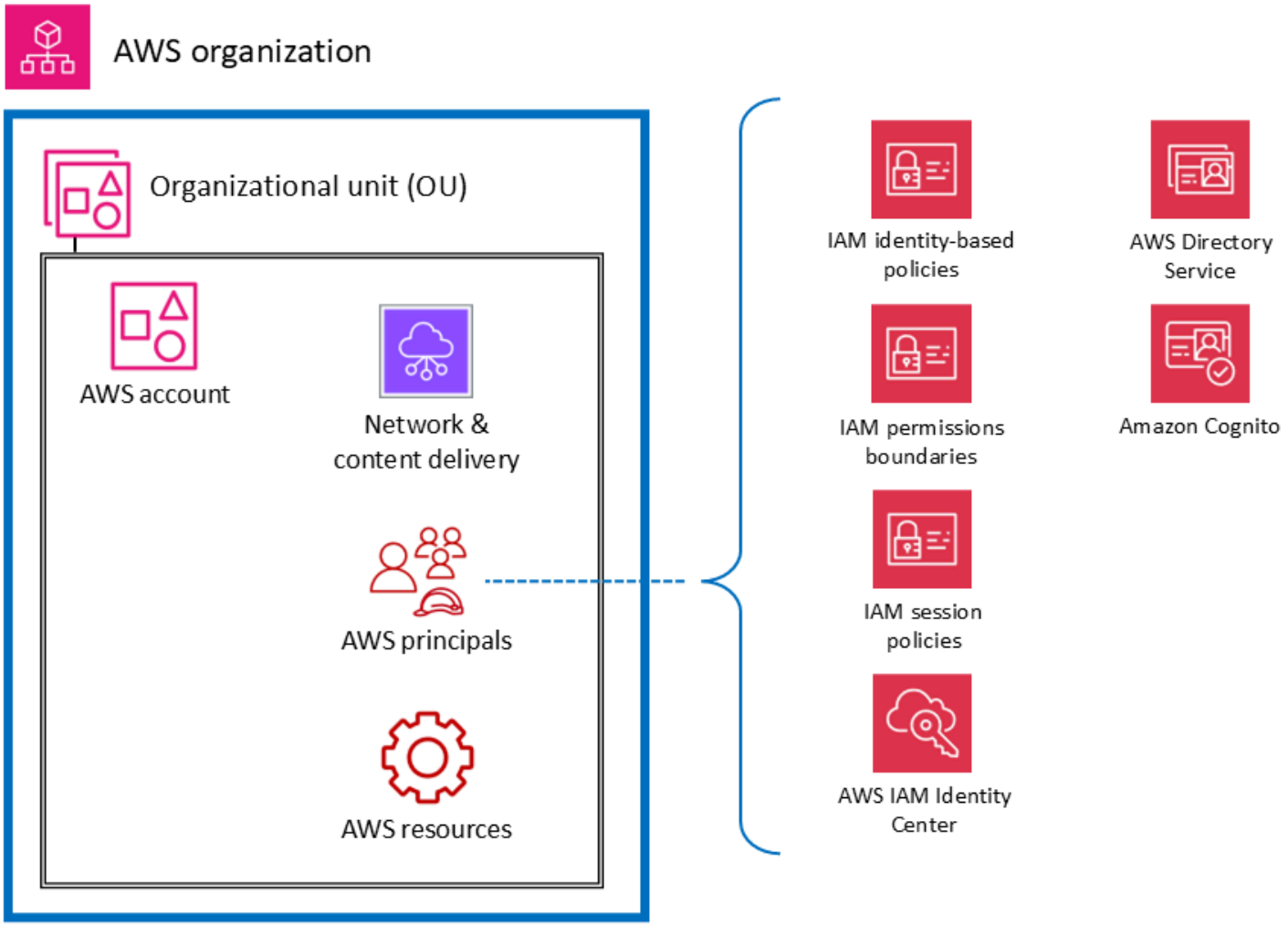
AWS 委托人和 AWS 资源（以及 IAM 策略）是上 AWS身份和访问管理的基本要素。中经过身份验证的委托人 AWS 可以执行操作和访问 AWS 资源。委托人可以作为 AWS 账户 根用户和 IAM 用户进行身份验证，也可以通过担任角色进行身份验证。

> **Note**
>
> 请勿创建与 AWS 根用户账户关联的永久性 API 密钥。root 用户帐户的访问权限应仅限于需要 root 用户的任务，并且只能通过严格的例外和批准流程进行访问。有关保护账户根用户的最佳实践，请参阅 IAM 文档。

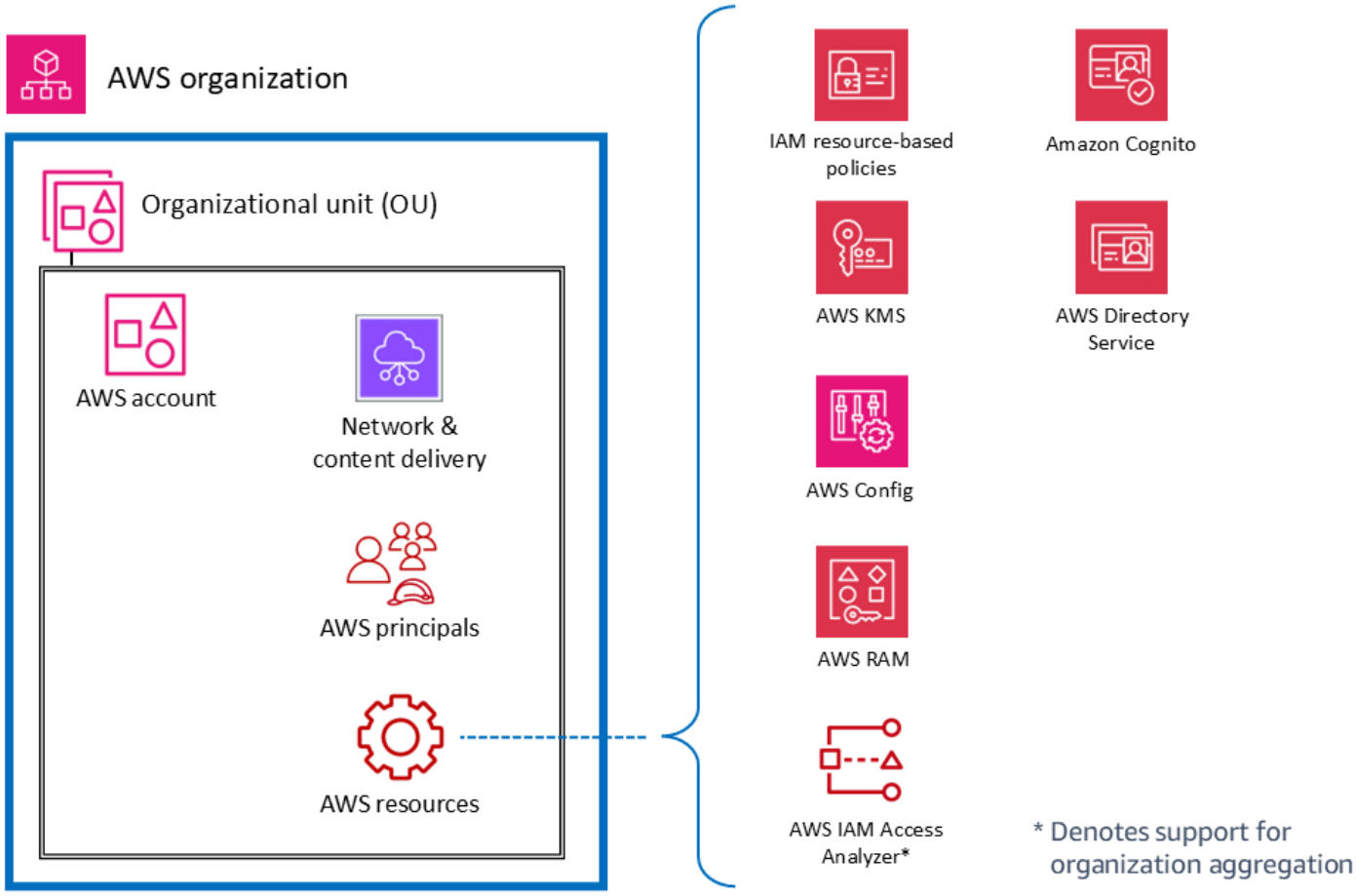
AWS 资源是存在于中的一个对象 AWS 服务 ，可供您使用。示例包括 EC2 实例、 CloudFormation 堆栈、亚马逊简单通知服务 (Amazon SNS) Service 主题和 S3 存储桶。IAM 策略是在与 IAM 委托人（用户、群组或角色）或 AWS 资源关联时定义权限的对象。基于身份的策略是您附加到委托人（角色、用户和用户组）的策略文档，用于控制委托人可以执行哪些操作、对哪些资源以及在哪些条件下执行哪些操作。基于资源的策略是您附加到资源（例如 S3 存储桶）的策略文档。这些策略向指定的委托人授予对该资源执行特定操作的权限，并定义该权限的条件。基于资源的策略是内联策略。I AM 资源部分深入探讨了 IAM 策略的类型及其使用方式。

为了简化本次讨论，我们列出了面向以账户委托人操作或申请账户委托人为主要目的的 IAM 委托人的 AWS 安全服务和功能。我们保持这种简单性，同时承认 IAM 权限策略的灵活性和影响广度。策略中的单个声明可以对多种类型的 AWS 实体产生影响。例如，尽管基于 IAM 身份的策略与 IAM 委托人关联并定义了该委托人的权限（允许、拒绝），但该策略还隐式定义了对指定操作、资源和条件的权限。这样，基于身份的策略可以成为定义资源权限的关键要素。

下图说明了为 AWS 委托人提供的 AWS 安全服务和功能。基于身份的策略附加到 IAM 用户、组或角色。这些策略可让您指定该身份可执行哪些操作（其权限）。IAM 会话策略是用户代入角色时在会话中传递的内联权限策略。您可以自己传递策略，也可以将身份代理配置为在您的身份联合到 AWS时插入策略。这使您的管理员能够减少必须创建的角色数量，因为多个用户可以扮演相同的角色，但具有唯一的会话权限。IAM Identity Center 服务与 AWS Organizations AWS API 操作集成，可帮助您管理 SSO 访问权限和用户权限。 AWS 账户 AWS Organizations



下图说明了账户资源的服务和功能。基于资源的策略附加到某个资源。例如，您可以将基于资源的策略附加到 S3 存储桶、亚马逊简单队列服务 (Amazon SQS) Simple Queue SQUEE 队列、VPC 终端节点和加密密钥。 AWS KMS 您可以使用基于资源的策略来指定谁有权访问资源以及他们可以对资源执行哪些操作。S3 存储桶策略、 AWS KMS 密钥策略和 VPC 终端节点策略是基于资源的策略的类型。IAM Access Analyzer帮助您标识企业和账户中与外部实体共享的资源，例如 S3 存储桶或 IAM 角色。这使您可以识别对您的资源和数据的意外访问，这是一种安全风险。 AWS Config 使您能够评估、审核和评估中受支持 AWS 资源的配置 AWS 账户。 AWS Config 持续监控和记录 AWS 资源配置，并根据所需的配置自动评估记录的配置。


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

AWS 安全参考架构

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

下图说明了 AWS SRA。此架构图汇集了所有与 AWS 安全相关的服务。它围绕一个简单的三层 Web 架构构建，可以放在单个页面上。在这样的工作负载中，有一个 Web 层，用户通过该层与应用程序层进行连接和交互，应用程序层处理应用程序的实际业务逻辑：从用户那里获取输入、进行一些计算和生成输出。应用程序层存储和检索来自数据层的信息。该架构专门采用模块化设计，为许多现代 Web 应用程序提供了高级抽象。

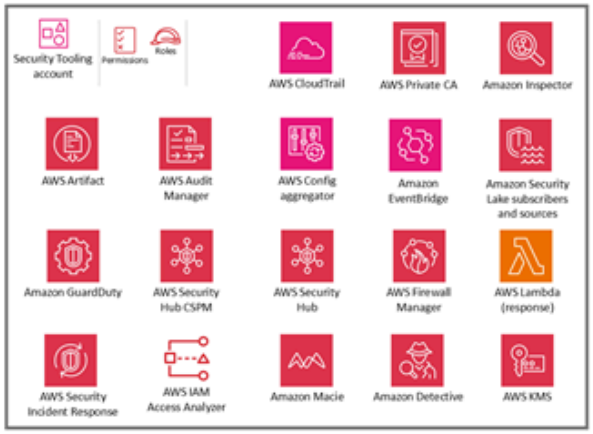
架构图

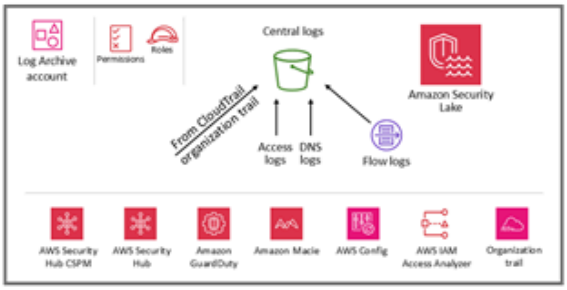
要根据您的业务需求自定义本指南中的参考架构图，您可以下载以下.zip 文件并提取其内容。

下载图表源文件（微软 PowerPoint 格式）

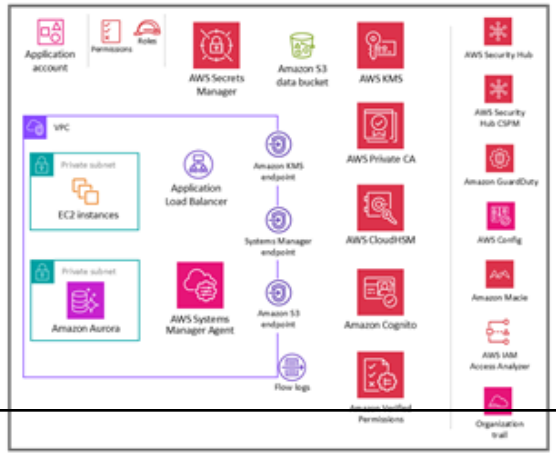
Organization

OU – Security

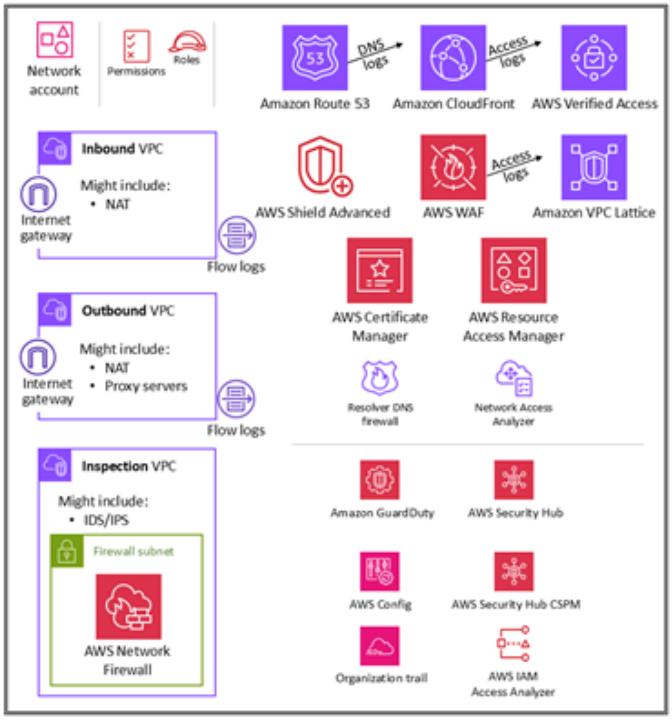


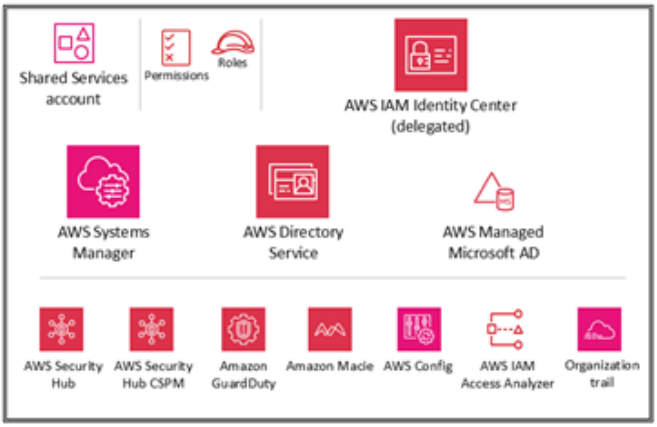


OU – Workloads



OU – Infrastructure





对于此参考架构，我们特意分别通过 Amazon EC2 实例和 Amazon Aurora 数据库尽可能简单地表示实际的 Web 应用程序和数据层。大多数架构图都侧重并深入研究 Web、应用程序和数据层。为了便于阅读，它们通常会省略安全控制。此图表将重点转移到尽可能地显示安全性，并使应用程序和数据层尽可能简单，以有意义地显示安全功能。

AWS SRA 包含发布时可用的所有 AWS 与安全相关的服务。（请参阅文档历史记录。）但是，并非每个工作负载或环境都必须根据其独特的威胁暴露情况部署每项安全服务。我们的目标是为一系列选项提供参考，包括描述这些服务在架构上是如何组合在一起的，以便您的企业可以根据风险做出最适合您的基础架构、工作负载和安全需求的决策。

以下各节将介绍每个 OU 和帐户，以了解其目标以及与之相关的各个 AWS 安全服务。对于每个元素（通常是 AWS 服务），本文档提供以下信息：

- 该元素及其在 AWS SRA 中的安全目的的简要概述。有关各项服务的更多详细描述和技术信息，请参阅附录。
- 建议放置位置，以最有效地启用和管理服务。这在每个账户和 OU 的单独架构图中捕捉到。
- 配置、管理和数据共享链接到其他安全服务。此服务如何依赖或支持其他安全服务？
- 设计注意事项。首先，本文档重点介绍了具有重要安全影响的可选功能或配置。其次，如果我们团队的经验包括我们提出的建议中的常见差异（通常是由于其他要求或限制），则文档描述了这些选项。

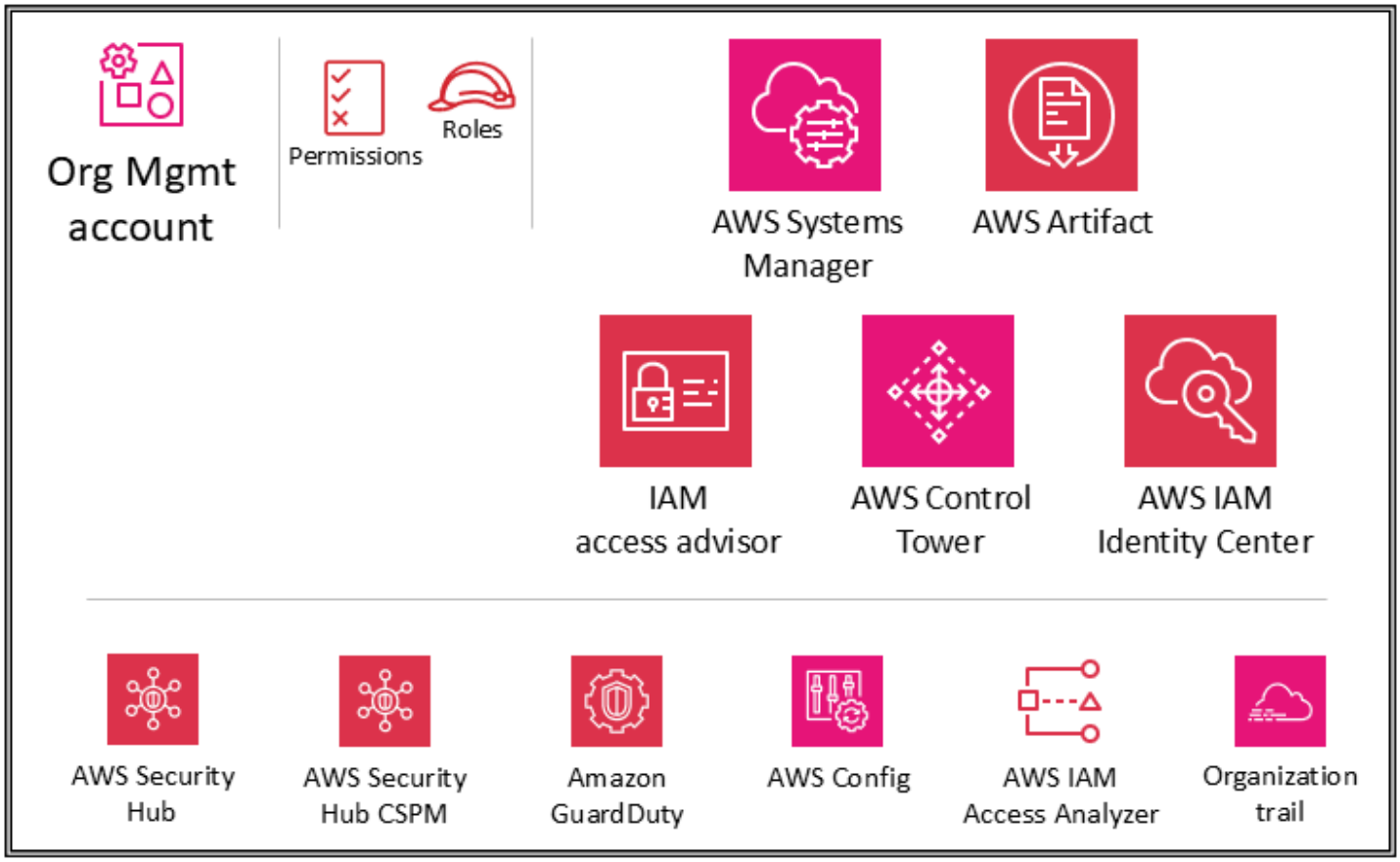
OUs 和账户

- 组织管理账户
- 安全 OU – 安全工具账户
- 安全 OU – 日志存档账户
- 基础设施 OU – 网络账户
- 基础架构 OU — 共享服务账户
- 工作负载 OU — 应用程序帐户

组织管理账户

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

下图说明了在组织管理账户中配置 AWS 的安全服务。



本指南前面的 “AWS Organizations 用于安全性” 和 “管理账户、可信访问权限和委派管理员” 部分深入讨论了组织管理账户的目的和安全目标。请遵循组织管理账户的安全最佳实践。其中包括使用由您的企业管理的电子邮件地址、维护正确的管理和安全联系信息（例如，在 AWS 需要联系账户所有者时向账户添加电话号码）、为所有用户启用多因素身份验证 (MFA)，以及定期查看谁有权访问组织管理账户。在组织管理账户中部署的服务应配置适当的角色、信任策略和其他权限，这样这些服务的管理员（必须使用组织管理账户访问这些服务）也不会不当访问其他服务。

服务控制策略

借AWS Organizations助，您可以集中管理多个策略 AWS 账户。例如，您可以将服务控制策略 (SCPs) 应用 AWS 账户 于多个组织成员。 SCPs 允许您定义哪些 AWS 服务 APIs 可以和不能由组织成员AWS 账户中的 IAM 委托人（例如 IAM 用户和角色）运行。 SCPs 是通过组织管理账户创建和应用的，组织管理账户 AWS 账户 是您在创建组织时使用的账户。 SCPs 在本参考文献前面的 “AWS Organizations 用于安全性” 一节中阅读更多相关信息。

如果您使用 AWS Control Tower 来管理您的 AWS 组织，它将部署一套 SCPs 作为预防性护栏（分为必填项、强烈建议或选择性）。这些护栏通过在组织范围内实施安全控制来帮助您管理资源。它们 SCPs 会自动使用值为的 aws-control-tower标签 managed-by-control-tower。

设计注意事项

SCPs 仅影响 AWS 组织中的成员帐户。尽管它们是从组织管理账户应用的，但它们对该账户中的用户或角色没有影响。要了解 SCP 评估逻辑的工作原理以及推荐结构的示例，请参阅中的 AWSAWS Organizations博客文章 “如何使用服务控制策略”。

资源控制策略

资源控制策略 (RCPs) 提供对组织中资源的最大可用权限的集中控制。RCP 定义了权限护栏或对身份可以对组织中的资源采取的操作设置限制。您可以使用 RCPs 来限制谁可以访问您的资源，并强制要求组织成员如何访问您的资源 AWS 账户。您可以 RCPs 直接关联到个人账户或组织根帐户。 OUs有关 RCPs 工作原理的详细说明，请参阅 AWS Organizations 文档中的 RCP 评估。 RCPs 在本参考文献前面的 “AWS Organizations 用于安全性” 一节中阅读更多相关信息。

如果您使用 AWS Control Tower 来管理您的 AWS 组织，它将部署一套 RCPs 作为预防性护栏（分为必填项、强烈建议或选择性）。这些护栏通过在组织范围内实施安全控制来帮助您管理资源。它们 SCPs 会自动使用值为的`aws-control-tower`标签`managed-by-control-tower`。

设计注意事项

- RCPs 仅影响组织中成员账户中的资源。对管理账户中的资源没有任何影响。这也意味着这 RCPs 适用于被指定为授权管理员的成员账户。
- RCPs 适用于其子集的资源 AWS 服务。有关更多信息，请参阅 AWS Organizations 文档 RCPs中的支持列表。 AWS 服务 您可以使用AWS Config 规则和AWS Lambda 函数来监控和自动执行对当前不支持的资源的安全控制 RCPs。

声明式策略

声明式策略是一种 AWS Organizations 管理策略，可帮助您在整个组织中大规模地集中声明和强制执行给定 AWS 服务 配置所需的配置。声明性政策目前支持亚马逊 EC2、亚马逊 VPC 和亚马逊 EBS 服务。可用的服务属性包括强制执行实例元数据服务版本 2 (imdsv2)、允许通过 EC2 串行控制台进行故障排除、允许亚马逊系统映像 (AMI) 设置以及阻止公众访问亚马逊 EBS 快照、亚马逊 EC2 和 Amazon VPC 资源。 AMIs有关最新支持的服务和属性，请参阅 AWS Organizations 文档中的声明式策略。

您可以 AWS 服务 通过在 AWS Organizations 和 AWS Control Tower 控制台上进行一些选择或使用几个 AWS Command Line Interface (AWS CLI) 和 AWS SDK 命令来强制执行基准配置。声明式策略是

在服务的控制平面中强制执行的，这意味着即使服务引入了新功能，或者向组织添加了新帐户 APIs，或者创建了新的委托人和资源，也始终保持了的基准配置。 AWS 服务 声明式策略可以应用于整个组织或特定 OUs 或帐户。有效的策略是继承自组织根目录的一组规则， OUs 以及直接关联到账户的策略。 如果分离声明性策略，则该属性状态将回滚到附加声明性策略之前的状态。

您可以使用声明性策略来创建自定义错误消息。例如，如果 API 操作因声明性策略而失败，则可以设置错误消息或提供自定义 URL，例如指向内部 wiki 的链接或描述失败的消息的链接。这有助于为用户提供更多信息，以便他们可以自己解决问题。您还可以使用来审核创建声明性策略、更新声明性策略和删除声明性策略的过程。 AWS CloudTrail

声明式策略提供账户状态报告，使您能够查看范围内账户的声明性策略支持的所有属性的当前状态。您可以选择 OUs 要包含在报告范围内的帐户，也可以通过选择根目录来选择整个组织。此报告通过提供细分 AWS 区域 并指定属性的当前状态是跨账户（通过值）一致还是不同账户（通过*numberOfMatchedAccounts*值）不一致（通过*numberOfUnmatchedAccounts*值）来帮助您评估准备情况。

> **设计注意事项**
>
> 使用声明性策略配置服务属性时，该策略可能会影响多个 APIs属性。任何不合规的操作都将失败。账户管理员将无法在个人账户级别修改服务属性的值。

集中式根访问权限

中的所有成员账户 AWS Organizations 都有自己的根用户，该用户可以完全访问该成员账户中的所有资源 AWS 服务 和资源。IAM 提供集中式根访问管理，以管理所有成员账户的根访问权限。这有助于防止使用成员 root 用户，并有助于提供大规模恢复。集中式根访问功能具有两项基本功能：根凭据管理和根会话。

- 根凭证管理功能允许集中管理，并有助于保护所有管理账户的 root 用户。此功能包括删除长期根证书、防止成员账户恢复根凭证，以及默认情况下配置没有根凭证的新成员账户。它还提供了一种证明合规性的简便方法。在集中管理根用户时，您可以删除根用户密码、访问密钥和签名证书，并停用所有成员账户的多因素身份验证 (MFA)。
- 根会话功能使您能够使用来自组织管理账户或委托管理员账户的成员账户的短期凭证来执行特权根用户操作。此功能可帮助您启用短期 root 访问权限，该权限仅限于特定的操作，同时遵循最低权限原则。

要进行集中式根凭据管理，您需要通过组织管理账户或委派管理员账户在组织级别启用根凭证管理和根会话功能。按 AWS 照 SRA 最佳实践，我们将此功能委托给安全工具账户。有关配置和使用集中根用户访问权限的信息，请参阅 S AWS ecurity 博客文章《使用集中管理客户的根访问权限》 AWS Organizations。

IAM Identity Center

AWS IAM Identity Center是一项身份联合服务，可帮助您集中管理对所有工作负载 AWS 账户、委托人和云工作负载的 SSO 访问权限。IAM Identity Center 还可以帮助您管理对常用的第三方软件即服务 (SaaS) 应用程序的访问和权限。身份提供商使用 SAML 2.0 与 IAM 身份中心集成。批量 just-in-time 配置可以通过使用跨域身份管理系统 (SCIM) 来完成。IAM 身份中心还可以通过使用与本地或 AWS托管的 Microsoft Active Directory (AD) 域集成，作为身份提供商。 AWS Directory Service IAM Identity Center 包括一个用户门户，您的最终用户可以在其中一处查找和访问他们分配的 AWS 账户 IAM 身份中心、角色、云应用程序和自定义应用程序。

默认情况下，IAM Identity Center AWS Organizations 与组织管理账户进行原生集成并在组织管理账户中运行。但是，为了行使最低权限并严格控制对管理账户的访问权限，可以将 IAM Identity Center 的管理委托给特定的成员账户。在 AWS SRA 中，共享服务账户是 IAM 身份中心的委派管理员账户。在 IAM Identity Center 启用委托管理之前，请查看以下注意事项。您可以在共享服务帐户部分找到有关委托的更多信息。即使您启用了委托，IAM Identity Center 仍需要在组织管理账户中运行才能执行某些与 IAM Identity Center 相关的任务，包括管理在组织管理账户中配置的权限集。

在 IAM Identity Center 控制台中，账户按其封装 OU 显示。这使您能够快速发现自己的权限 AWS 账户，应用常用权限集，并从中央位置管理访问权限。

IAM Identity Center 包括一个身份存储，必须存储特定的用户信息。但是，IAM 身份中心不必是员工信息的权威来源。如果您的企业已经拥有权威来源，则 IAM Identity Center 支持以下类型的身份提供商 (IdPs)。

- IAM Identity Center 身份存储 — 如果以下两个选项不可用，请选择此选项。在身份存储中创建用户、进行群组分配和分配权限。即使您的权威来源位于 IAM Identity Center 之外，委托人属性的副本也将与身份存储一起存储。
- Microsoft Active Directory (AD) — 如果要继续管理活动目录中的用户 AWS Directory Service for Microsoft Active Directory 或自己管理的目录中的用户，请选择此选项。
- 外部身份提供商- 如果您更喜欢在基于 SAML 的外部第三方 IdP 中管理用户，请选择此选项。

您可以依赖企业中已经存在的现有 IdP。这样可以更轻松地管理跨多个应用程序和服务的访问权限，因为您可以从一个位置创建、管理和撤消访问权限。例如，如果有人离开你的团队，你可以撤消他们从一

个地点对所有应用程序和服务（包括 AWS 账户）的访问权限。这减少了对多个证书的需求，并为您提供了与人力资源 (HR) 流程集成的机会。

> **设计注意事项**
>
> 如果您的企业可以使用外部 IdP 选项，请使用该选项。如果您的 IdP 支持跨域身份管理系统 (SCIM)，请利用 IAM Identity Center 中的 SCIM 功能自动配置用户、群组和权限（同步）。这样，新员工、要调到其他团队的员工以及即将离开公司的员工都可以 AWS 访问与您的公司工作流程保持同步。在任何给定时间，您只能将一个目录或一个 SAML 2.0 身份提供商连接到 IAM 身份中心。但是，您可以切换到其他身份提供商。

IAM 访问顾问

IAM 访问顾问以您 AWS 账户 和的服务上次访问信息的形式提供可追溯性数据 OUs。使用此侦探控件为最低权限策略做出贡献。对于 IAM 委托人，您可以查看两种类型的上次访问信息：允许的 AWS 服务 信息和允许的操作信息。此信息包括进行尝试的日期和时间。

通过组织管理账户中的 IAM 访问权限，您可以查看 AWS 组织管理账户、OU、成员账户或 IAM 策略的上次访问服务数据。此信息可在管理账户的 IAM 控制台中找到，也可以通过使用中的 IAM 访问顾问 APIs AWS CLI 或编程客户端以编程方式获取。该信息指明组织或账户中的哪些主体上次尝试访问该服务以及尝试访问的时间。上次访问的信息提供了对实际服务使用情况的见解（参见示例场景），因此您可以将 IAM 权限减少到仅限实际使用的服务。

AWS Systems Manager

Quick Setup 和 Explorer 是的功能 AWS Systems Manager，既支持 AWS Organizations 组织管理账户，也可通过组织管理账户进行操作。

快速设置是 S ystems Manager 的一项自动化功能。它使组织管理帐户能够轻松定义配置，让 Systems Manager 代表您 AWS 组织中的多个账户进行互动。您可以在整个 AWS 组织中启用快速设置，也可以选择特定的 OUs。快速设置可以安排 AWS Systems Manager 代理（SSM 代理）在您的 EC2 实例上每两周运行一次更新，并且可以设置对这些实例的每日扫描以识别缺失的补丁。

Explorer 是一个可自定义的操作仪表板，用于报告有关您的 AWS 资源的信息。Explorer 会显示您 AWS 账户及各个账户的运营数据的汇总视图 AWS 区域。这包括有关您的 EC2 实例的数据和补丁合规性详细信息。在中完成集成设置（其中还包括 Systems Manager OpsCenter）后 AWS Organizations，您可以按组织单位在 Explorer 中聚合数据，也可以聚合整个 AWS 组织的数据。在资源管理器中显示数据之前，Systems Manager 会将数据聚合到 AWS 组织管理帐户中。

本指南后面的工作负载 OU 部分讨论了在应用程序账户的 EC2 实例上使用 SSM 代理的情况。

AWS Control Tower

AWS Control Tower提供了一种设置和管理安全的多账户 AWS 环境（称为 landing zon e）的简单方法。 AWS Control Tower 使用创建您的 landin AWS Organizations g zone，并提供持续的账户管理和治理以及实施最佳实践。只需几个步骤 AWS Control Tower 即可使用配置新帐户，同时确保这些帐户符合您的组织政策。您甚至可以将现有账户添加到新 AWS Control Tower 环境中。

AWS Control Tower 具有广泛而灵活的功能集。一项关键功能是它能够协调其他几个（包括AWS 服务 AWS Organizations AWS Service Catalog、和 IAM Identity Center）的功能，以构建着陆区。例如，默认情况下， AWS Control Tower 使用服务控制策略 () AWS CloudFormation 来建立基准，使用 AWS Organizations 服务控制策略 (SCPs) 来防止配置更改，使用 AWS Config 规则 规则来持续检测不合格情况。 AWS Control Tower 采用蓝图，帮助您快速调整多账户 AWS 环境与 W AWS ell Architected 安全基础设计原则。在监管功能中， AWS Control Tower 它提供了防护，可防止部署不符合所选策略的资源。

您可以通过以下方式开始实施 AWS SRA 指南。 AWS Control Tower例如，使用推荐的多账户架构 AWS Control Tower 建立一个 AWS 组织。它提供了蓝图，用于提供身份管理、提供账户联合访问权限、集中日志记录、建立跨账户安全审计、定义配置新账户的工作流程，以及使用网络配置实施账户基准。

在 AWS SRA 中， AWS Control Tower 位于组织管理账户中，因为 AWS Control Tower 使用此账户自动设置 AWS 组织并将该账户指定为管理账户。此账户用于在整个 AWS 组织中进行计费。它还用于 Account Factory 配置账户 OUs、管理和管理护栏。如果您 AWS Control Tower 在现有 AWS 组织中启动，则可以使用现有的管理账户。 AWS Control Tower 将使用该账户作为指定的管理账户。

> **设计注意事项**
>
> 如果您想对账户中的控制和配置进行额外的基准化，则可以使用 “定制” AWS Control Tower (cfcT)。使用 cfcT，您可以使用 CloudFormation 模板自定义 AWS Control Tower 着陆区，然后。 SCPs您可以将自定义模板和策略部署到个人账户和组织 OUs 内部。cfcT 与 AWS Control Tower 生命周期事件集成，确保资源部署与您的 landing zone 保持同步。

AWS Artifact

AWS Artifact提供按需访问 AWS 安全与合规报告以及精选在线协议。中提供的报告 AWS Artifact 包括系统和组织控制 (SOC) 报告、支付卡行业 (PCI) 报告，以及来自不同地区和合规垂直领域的认证机构

的认证，这些认证机构验证了安全控制的实施和运营有效性。 AWS AWS Artifact 帮助您进行尽职调查 AWS ，提高我们安全控制环境的透明度。它还允许您持续监控安全性和合规性，并 AWS 可立即访问新报告。

AWS Artifact 协议使您能够查看、接受和跟踪 AWS 协议的状态，例如个人账户和属于您组织中的 AWS Organizations账户的商业伙伴附录 (BAA)。

您可以向 AWS 审计师或监管机构提供审计工件作为 AWS 安全控制的证据。您还可以使用某些 AWS 审计工件提供的责任指南来设计您的云架构。本指南有助于确定您可以采取哪些其他安全控制措施来支持系统的特定用例。

AWS Artifact 托管在组织管理账户中，提供一个中心位置，您可以在其中查看、接受和管理与之达成的协议 AWS。这是因为管理账户接受的协议会向下流向成员账户。

> **设计注意事项**
>
> 应限制组织管理账户中的用户只能使用的 “协议” 功能 AWS Artifact ，不得使用其他任何功能。为了实现职责分离，还托管在 Security Too AWS Artifact ls 账户中，您可以在其中向合规利益相关者和外部审计师委派访问审计工件的权限。您可以通过定义精细的 IAM 权限策略来实现这种分离。有关示例，请参阅 AWS 文档中的 IAM 策略示例。

分布式和集中式安全服务护栏

在 AWS SRA 中，、 AWS Security Hub AWS Security Hub CSPM、Amazon GuardDuty、 AWS Config、IAM Access Analyzer、 AWS CloudTrail 组织跟踪和 Amazon Macie 通常都部署了跨账户的适当委托护栏，还为整个组织提供集中监控、管理和治理。 AWS 你可以在 AWS SRA中代表的每种账户类型中找到这组服务。这些应该是 AWS 服务 必须作为账户入职和基准制定流程的一部分进行配置的一部分。GitHub 代码存储库提供了跨账户（包括 AWS 组织管理账户）实施 AWS 以安全为重点的服务的示例。

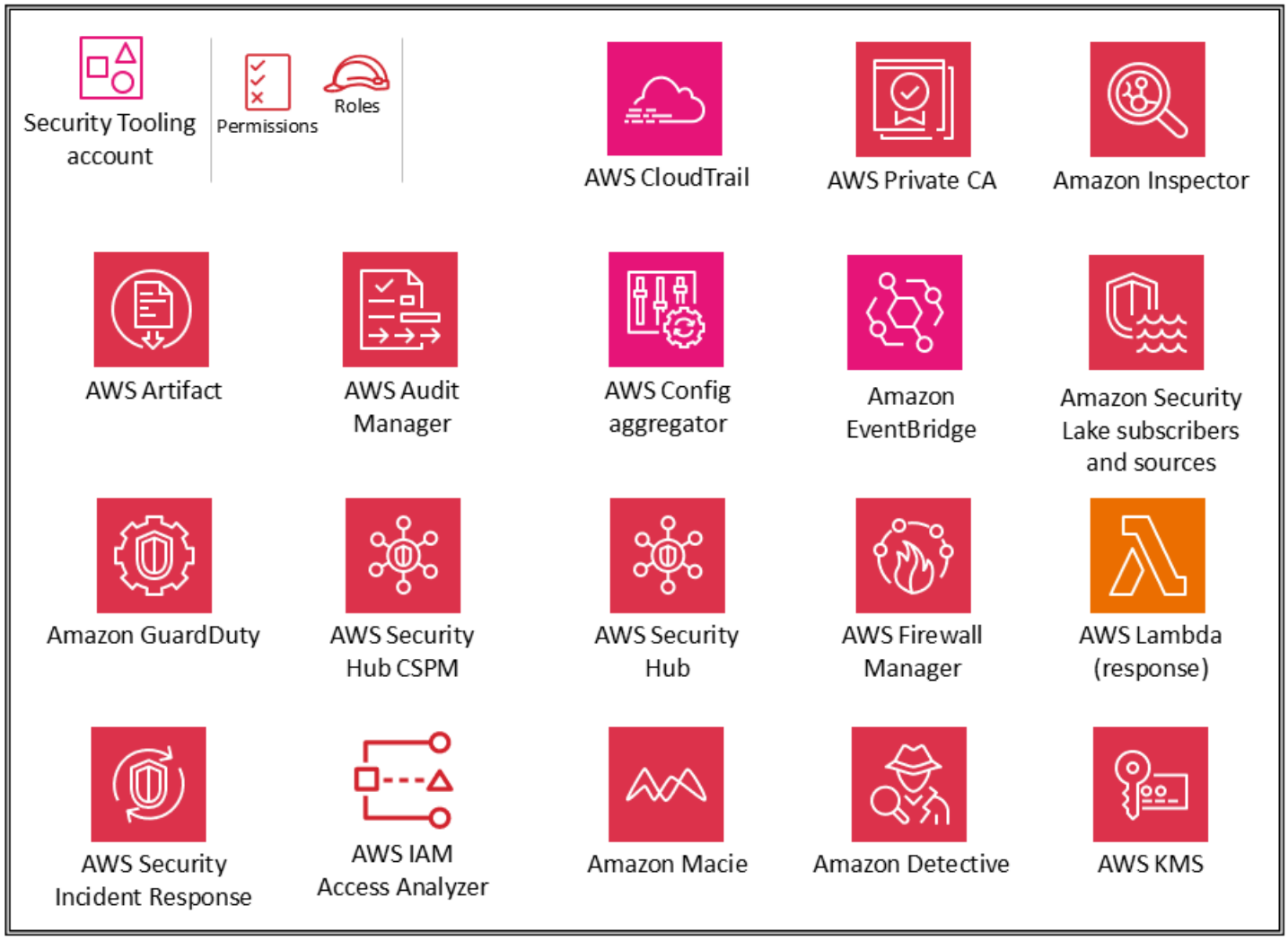
除了这些服务外， AWS SRA 还包括两项以安全为重点的服务，即 Amazon Detective 和 AWS Audit Manager，它们支持中的集成和委托管理员功能。 AWS Organizations但是，这些不包括在账户基准的推荐服务中。我们已经看到，这些服务最适合在以下场景中使用：

- 您有一个专门的团队或一组资源来执行这些数字取证和 IT 审计职能。安全分析团队最能利用 Detective，而 Audit Manager 对您的内部审计或合规团队很有帮助。
- 您希望在项目开始 AWS Security Hub CSPM 时专注于一组核心工具 AWS Config，例如 Amazon GuardDuty 和 AWS Security Hub，然后使用提供额外功能的服务在这些工具的基础上再接再厉。

安全 OU – 安全工具账户

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

下图说明了在 AWS 安全工具账户中配置的安全服务。



Security Tooling 账户专门用于操作安全服务 AWS 账户、监控以及自动发送安全警报和响应。安全目标包括以下内容：

- 提供具有受控访问权限的专用帐户，以管理对安全护栏的访问权限、监控和响应。
- 维护适当的集中式安全基础架构，以监控安全运营数据并保持可追溯性。检测、调查和响应是安全生命周期的重要组成部分，可用于支持质量流程、法律或合规义务以及威胁识别和响应工作。

- 通过保持对适当安全配置和操作（例如加密密钥和安全组设置）的另一层控制，进一步支持defense-in-depth组织战略。这是安全操作员工作的账户。查看 AWS 组织范围信息的只读/审计角色是典型的，而 write/modify 角色数量有限，受到严格控制、监控和记录。

> 设计注意事项
>
> - AWS Control Tower 默认情况下，将安全 OU 下的帐户命名为审计帐户。您可以在 AWS Control Tower 设置过程中重命名该帐户。
> - 拥有多个安全工具帐户可能是合适的。例如，安全事件的监控和响应通常分配给一个专门的团队。网络安全可能需要与云基础架构或网络团队合作使用自己的帐户和角色。这种分裂保留了分离集中式安全飞地的目标，并进一步强调了职责分离、最低权限和团队分配的潜在简单性。如果您正在使用 AWS Control Tower，则它会限制在安全 OU AWS 账户 下创建其他内容。

安全服务的委派管理员

Security Tools 帐户充当安全服务的管理员帐户，这些服务在整个 administrator/member 结构中进行管理 AWS 账户。如前所述，这是通过 AWS Organizations 委派管理员功能来处理的。 AWS SRA 中目前支持委派管理员的服务包括 IAM 对根访问权限的集中管理、、、Amazon、IAM Access Analyzer AWS Config AWS Firewall Manager、Amazon Macie GuardDuty、、、Amazon Detective、AWS Security Hub、Amazon Inspector AWS Security Hub CSPM、 AWS Audit Manager、Amazon Inspector AWS CloudTrail和。 AWS Systems Manager您的安全团队管理这些服务的安全功能，并监控任何特定于安全的事件或发现。

AWS IAM Identity Center 支持对成员账户进行委托管理。 AWS SRA 使用共享服务账户作为 IAM 身份中心的委托管理员账户，如共享服务账户的 IAM 身份中心部分稍后所述。

集中式根访问权限

Security Tooling 账户是 IAM 集中管理根访问权限的委托管理员账户。 必须在组织级别启用此功能，方法是在成员账户中启用凭据管理和特权 root 操作。必须明确向授权管理员提供`sts:AssumeRoot`权限，才能代表成员账户执行特权 root 操作。只有在组织管理账户或委托管理员账户中启用成员账户中的特权 root 操作后，此权限才可用。有了此权限，用户可以从 Security Tooling 账户集中对成员账户执行特权 root 用户任务。启动特权会话后，您可以删除配置错误的 S3 存储桶策略、删除配置错误的 SQS 队列策略、删除成员账户的根用户证书，以及重新启用成员账户的根用户证书。您可以使用 AWS Command Line Interface (AWS CLI) 或通过，从控制台执行这些操作 APIs。

AWS CloudTrail

AWS CloudTrail是一项支持对您的活动进行治理、合规和审计的服务 AWS 账户。借 CloudTrail助，您可以记录、持续监控和保留与整个 AWS 基础架构中的操作相关的账户活动。 CloudTrail 已与集成 AWS Organizations，并且该集成可用于创建单个跟踪，用于记录 AWS 组织中所有账户的所有事件。这称为组织跟踪。您只能通过组织的管理账户或委派的管理员账户创建和管理组织跟踪。创建组织跟踪时，将在属于您的 AWS 组织的每个跟踪中创建具有您指定名称 AWS 账户 的跟踪。跟踪记录 AWS 组织中所有账户（包括管理账户）的活动，并将日志存储在单个 S3 存储桶中。由于此 S3 存储桶的敏感性，您应遵循本指南后面的 Amazon S3 作为中央日志存储部分中概述的最佳实践来保护它。 AWS 组织中的所有账户都可以在其跟踪列表中看到组织跟踪。但是 AWS 账户 ，成员只能查看此路径。默认情况下，当您在 CloudTrail 控制台中创建组织跟踪时，该跟踪是多区域跟踪。有关其他安全最佳实践，请参阅CloudTrail文档。

在 AWS SRA 中，安全工具帐户是用于管理 CloudTrail的委派管理员帐户。存储组织跟踪日志的相应的 S3 存储桶是在日志存档账户中创建的。这是为了区分 CloudTrail日志权限的管理和使用。有关如何创建或更新 S3 存储桶以存储组织跟踪的日志文件的信息，请参阅CloudTrail 文档。作为安全最佳实践，将组织跟踪的`aws:SourceArn`条件密钥添加到 S3 存储桶（以及任何其他资源，例如 KMS 密钥或 SNS 主题）的资源策略中。这可确保 S3 存储桶仅接受与特定跟踪关联的数据。该跟踪配置了日志文件验证，以验证日志文件完整性。使用 SSE-KMS 对日志和摘要文件进行加密。组织跟踪还与 Logs 中的 CloudWatch 日志组集成，用于发送事件以进行长期保留。

> **Note**
>
> 您可以通过管理帐户和委派管理员帐户创建和管理组织跟踪。但是，作为最佳实践，您应限制对管理账户的访问权限，并在可用的情况下使用委派管理员功能。

> **设计注意事项**
>
> - CloudTrail 默认情况下不记录数据事件，因为这些事件通常是高容量活动。但是，您应该捕获特定关键 AWS 资源的数据事件，例如 S3 存储桶、Lambda 函数、从 AWS 外部发送到湖中的日志事件以及 S CloudTrail NS 主题。为此，请通过指定每个单独的资源来配置组织跟踪，使其包含来自特定资源的数据事件。 ARNs
> - 如果成员账户需要访问自己账户的 CloudTrail 日志文件，则可以选择性地共享中央 S3 存储桶中的组织 CloudTrail 日志文件。但是，如果成员账户需要使用本地 Amazon CloudWatch 日志组来存储其账户的 CloudTrail 日志，或者想要配置与组织跟踪不同的日志管理和数据事

件（只读、只写、管理事件、数据事件），则他们可以创建具有适当控件的本地跟踪。特定于本地账户的跟踪会产生额外费用。

AWS Security Hub CSPM

AWS Security Hub Cloud Security Posture Managem ent (AWS Security Hub CSPM)（以前称为 AWS Security Hub）可为您提供安全态势的全面视图， AWS 并帮助您根据安全行业标准和最佳实践检查您的环境。Security Hub CSPM 从各种 AWS 集成服务、支持的第三方产品以及您可能使用的其他自定义安全产品中收集安全数据。它可以帮助您持续监控和分析安全趋势，并确定最高优先级的安全问题。除了摄取的来源外，Security Hub CSPM 还会生成自己的发现，这些发现由映射到一个或多个安全标准的安全控制来表示。这些标准包括 AWS 基础安全最佳实践 (FSBP)、互联网安全中心 (CIS) AWS 基金会基准 v1.20 和 v1.4.0、美国国家标准与技术研究所 (NIST) SP 800-53 Rev. 5、支付卡行业数据安全标准 (PCI DSS) 和服务管理标准。有关当前安全标准列表和特定安全控制的详细信息，请参阅 Security Hub CSPM 文档中的 S ecurity Hub CSPM 标准参考。

Security Hub CSPM 与 AWS Organizations 集成，可简化组织中所有现有和未来账户的安全态势管理。 AWS 您可以使用委派管理员帐户（在本例中为安全工具）中的 Security Hub CSPM 中央配置功能来指定如何在您的组织账户和组织单位 (OUs) 中跨区域配置 Security Hub CSPM 服务、安全标准和安全控制。 您可以通过几个步骤从一个主区域（即主区域）配置这些设置。如果您不使用中央配置，则必须在每个账户和区域中分别配置 Security Hub CSPM。委托管理员可以将账户指定 OUs 为自我管理，成员可以在每个区域中单独配置设置，也可以指定为集中管理，委托管理员可以跨区域配置成员账户或 OU。您可以将组织 OUs 中的所有账户指定为集中管理、全部自我管理或两者兼而有之。这简化了执行一致性配置的过程，同时提供了为每个 OU 和账户修改配置的灵活性。

Security Hub CSPM 委托管理员账户还可以查看所有成员账户的调查结果、查看见解和控制详细信息。此外，您还可以在委托管理员账户中指定一个聚合区域，以便在您的账户和关联区域中集中您的调查结果。您的发现将在聚合器区域与所有其他区域之间持续双向同步。

Security Hub CSPM 支持与多个集成。 AWS 服务亚马逊 GuardDuty、亚马逊 Macie AWS Config、IAM Access Analyzer、 AWS Firewall Manager Amazon Inspector、 Amazon Route 53 Resolver DNS 防火墙和 AWS Systems Manager 补丁管理器可以将调查结果提供给 Security Hub CSPM。Security Hub CSPM 使用一种称为AWS 安全调查结果格式 (ASFF) 的标准格式来处理调查结果。Security Hub CSPM 将集成产品的发现关联起来，确定最重要的产品的优先级。您可以丰富 Security Hub CSPM 发现的元数据，以帮助更好地对安全发现进行情境化、优先级排序和采取行动。这种扩充功能为采集到 Security Hub CSPM 的每个发现添加了资源标签、新的 AWS 应用程序标签和账户名信息。这可以帮助您微调自动化规则的发现，搜索或筛选发现结果和见解，并按应用程序评估安全态势状态。此外，您还可以使用自动化规则自动更新调查结果。当 Security Hub CSPM 摄取发现结

果时，它可以应用各种规则操作，例如抑制搜索结果、更改其严重性以及在发现结果中添加注释。当搜索结果符合您的指定标准（例如与查找结果关联的资源或帐户 IDs 或其标题）时，这些规则操作就会生效。您可以使用自动化规则更新 ASFF 中的选定查找字段。规则适用于新的和更新的发现。

在调查安全事件期间，您可以从 Security Hub CSPM 导航到 Amazon Detective 以调查调查结果。GuardDuty Security Hub CSPM 建议调整诸如 Detective（如果存在）之类的服务的委托管理员帐户，以便更顺畅地集成。例如，如果您不在 Detective 和 Security Hub CSPM 之间调整管理员帐户，则无法从调查结果导航到 Detective。有关完整列表，请参阅 Security Hub CSPM 文档中的 Security Hub CSPM AWS 服务 集成概述。

您可以将 Security Hub CSPM 与 Amazon VPC 的网络访问分析器功能配合使用，以帮助持续监控 AWS 网络配置的合规性。这将帮助您阻止不需要的网络访问，并有助于防止外部访问您的关键资源。有关架构和实施的更多细节，请参阅 AWS 博客文章使用 Amazon VPC 网络访问分析器持续验证网络合规性和 AWS Security Hub CSPM。

除了监控功能外，Security Hub CSPM 还支持与亚马逊集成 EventBridge ，以自动修复特定发现。您可以定义在收到调查结果时要采取的自定义操作。例如，您可以配置自定义操作，将结果发送到票证系统或自动修复系统。有关其他讨论和示例，请参阅 AWS 博客文章使用 AWS Security Hub CSPM自动响应和补救以及如何部署 Security Hub CSPM 自动响应和补救 AWS 解决方案。

Security Hub CSPM 使用服务关联 AWS Config 规则 来执行其大部分安全控制检查。要支持这些控制，AWS Config 必须在每个启用 Security AWS 区域 Hub CSPM 的账户（包括管理员（或委托管理员）账户和成员账户）上启用这些控制。

设计注意事项

- 如果 Security Hub CSPM 中已经存在合规标准，例如 PCI-DSS，那么完全托管的 Security Hub CSPM 服务是实现该标准的最简单方法。但是，如果您想制定自己的合规性或安全标准，其中可能包括安全、运营或成本优化检查，则 AWS Config 一致性包提供了简化的自定义流程。（有关 AWS Config 和一致性包的更多信息，请参阅一AWS Config节。）
- Security Hub CSPM 的常见用例包括以下内容：
  - 作为仪表板，让应用程序所有者可以查看其 AWS 资源的安全和合规状况
  - 作为安全运营部门、事件响应者和威胁猎人使用的安全调查结果的中心视图，用于对跨地区和地区的 AWS 安全与合规调查结果进行分类并采取行动 AWS 账户
  - 汇总来自各个地区的安全与合规性调查结果， AWS 账户 并将其发送到集中式安全信息和事件管理 (SIEM) 或其他安全协调系统

有关这些用例的更多指导，包括如何进行设置，请参阅博客文章《三种反复出现的 Security Hub CSPM 使用模式以及如何部署它们》。

实现示例

AWS SRA 代码库提供了 Security Hub CSPM 的示例实现。它包括自动启用服务、将管理委托给成员账户（安全工具），以及为组织中所有现有和未来账户启用 Security Hub CSPM 的配置。 AWS

AWS Security Hub

AWS Security Hub是一款统一的云安全解决方案，可对您的关键安全威胁进行优先级排序，并帮助您大规模做出响应。Security Hub 通过自动关联和丰富来自多个来源的安全信号，例如状态管理 (AWS Security Hub CSPM)、漏洞管理 (Amazon Inspector)、敏感数据 (Amazon Macie) 和威胁检测 (亚马逊)，近乎实时地检测安全问题。 GuardDuty这使得安全团队能够通过自动化分析和上下文见解优先处理云环境中的活跃风险。Security Hub 直观地呈现了潜在的攻击路径，攻击者可以利用这些路径来访问与暴露发现相关的资源。这将复杂的安全信号转化为切实可行的见解，因此您可以快速就自己的安全做出明智的决策。

Security Hub 经过了战略重新设计，以简化相关安全服务构建块的启用流程，从而实现安全成果。通过近乎实时地关联不同安全信号的威胁矩阵中的安全发现，您可以先确定最关键的风险的优先级。这些发现与检测与 AWS 资源相关的暴露相关。风险暴露代表了安全控制、配置错误或其他可能被主动威胁利用的领域中更广泛的弱点。例如，漏洞可能是可从互联网访问的 EC2 实例，该实例具有很可能被利用的软件漏洞。

Security Hub 和 Security Hub CSPM 是互补服务。Sec@@ urity Hub CSPM 可全面了解您的安全状况，并帮助您根据安全行业标准和最佳实践评估您的云环境。 Security Hub 提供统一的体验，可帮助您确定关键安全问题的优先顺序并做出响应。Security Hub CSPM 调查发现会自动路由到 Security Hub，在那里它们与其他安全服务（例如 Amazon Inspector）的调查发现相关联，从而产生暴露。这有助于您识别自己环境中最严重的风险。

Security Hub 还按类型和相关发现提供 AWS 环境中资源的摘要。资源按照暴露和攻击序列确定优先级。选择资源类型时，您可以查看与该资源类型关联的所有资源。

为了获得最佳体验，我们建议启用 Security Hub 和 Security Hub CSPM，并启用其他安全服务：亚马逊 GuardDuty、Amazon Insp ector 和 Amazon Mac ie。通过使用 Security Hub Coverage 调查结果，您可以了解这些服务和功能是否已在组织的所有成员账户中统一启用。

在 AWS SRA 中，安全工具账户充当 Security Hub、Security Hub CSPM 和其他 AWS 安全服务的委托管理员。在 Security Tooling 账户中，您可以查看与成员账户关联的所有资源。您还可以通过链接查看家 AWS 区域 中的所有资源 AWS 区域。

实施说明

启用 Security Hub 需要三个步骤，包括考虑您之前是否启用过 Security Hub CSPM 的过程。Security Hub 与原生集成 AWS Organizations，这简化了配置和实施过程，并将所有发现集中并汇总到一个位置。根据 AWS SRA 最佳实践，使用安全工具帐户作为委托管理员帐户来管理和配置 Security Hub。使用 Security Hub 配置设置自动启用所有区域和账户，包括未来的区域和账户。 OUs您还应该设置跨区域聚合，将来自多个区域的调查结果、资源和趋势聚合 AWS 区域 到一个主区域中。在配置过程中，您还可以启用任何原生集成，例如 Jira Cloud 或。 ServiceNow

设计注意事项

- Security Hub 的调查结果采用开放网络安全架构框架 (OCSF) 进行格式化。Security Hub 在 OCSF 中生成调查结果，并在 OCSF 中接收来自 Security Hub CSPM 和其他机构的调查结果。 AWS 服务这些 OCSF 调查结果可以通过 Amazon 发送 EventBridge 以实现自动化，也可以存储在中央日志聚合账户中以执行安全日志分析和保留。
- AWS 组织管理账户无法在 Security Hub 中将自己指定为 “委托管理员”。这符合 AWS SRA 将安全工具帐户指定为授权管理员的最佳实践。另请注意：
  - Security Hub CSPM 的指定管理员帐户自动成为 Security Hub 的指定管理员。
  - 通过 Security Hub 移除委托管理也会移除 Security Hub CSPM 的委托管理。同样，通过 Security Hub CSPM 移除委托管理也会移除 Security Hub 的委托管理。
- Security Hub 包括根据您的规格自动修改发现结果并对其采取措施的功能，Security Hub 支持以下类型的自动化：
  - 自动化规则，可根据定义的标准自动更新调查结果、抑制发现结果并将结果近乎实时地发送到工单工具。
  - 自动响应和补救，可创建自定义 EventBridge 规则，定义针对特定发现和见解采取的自动行动。

- Security Hub 可以通过策略在所有成员账户和区域中配置 Amazon Inspector，也可以通过部署配置 GuardDuty 和 Security Hub CSPM。 AWS Organizations 策略为账户和地区生成策略。部署是一次性操作，可在选定的账户和地区启用安全功能。部署不适用于新启用的账户。或者，你可以在 GuardDuty和 Security Hub CSPM 中为新成员账户自动启用功能。

Amazon GuardDuty

Amazon GuardDuty 是一项威胁检测服务，可持续监控恶意活动和未经授权的行为，以保护您的 AWS 账户 和工作负载。您必须始终捕获和存储适当的日志以进行监控和审计，但要直接从 AWS CloudTrail Amazon VPC 流日志和 AWS DNS 日志中 GuardDuty 提取独立的数据流。您无需管理 Amazon S3 存储桶策略或修改收集和存储日志的方式。 GuardDuty权限作为服务相关角色进行管理，您可以随时通过禁用来撤消这些角色。 GuardDuty这使得无需复杂配置即可轻松启用服务，并且消除了 IAM 权限修改或 S3 存储桶策略更改会影响服务运行的风险。

除了提供基础数据源外，还 GuardDuty 提供用于识别安全发现的可选功能。这些保护包括 EKS 保护、RDS 保护、S3 保护、恶意软件防护和 Lambda 防护。对于新的探测器，这些可选功能默认处于启用状态，但 EKS 防护除外，必须手动启用。

- 借助 GuardDuty S3 保护，除了默认 CloudTrail 管理事件外，还可以 GuardDuty 监控 Amazon S3 数据事件。 CloudTrail 监控数据事件使您 GuardDuty 能够监控对象级 API 操作，以防您的 S3 存储桶中的数据面临潜在的安全风险。
- GuardDuty 恶意软件保护通过对连接的 Amazon Elastic Block Store (Amazon EBS) 卷启动无代理扫描来检测 Amazon EC2 实例或容器工作负载上是否存在恶意软件。 GuardDuty 还可以通过扫描新上传的对象或现有对象的新版本来检测 S3 存储桶中的潜在恶意软件。
- GuardDuty RDS 保护旨在在不影响数据库性能的情况下分析和监控 Amazon Aurora 数据库的访问活动。
- GuardDuty EKS 保护包括 EKS 审核日志监控和 EKS 运行时监控。通过 EKS 审核日志监控，GuardDuty 监控来自 Amazon EKS 集群的 Kubernetes 审计日志，并分析这些日志中是否存在潜在的恶意和可疑活动。EKS 运行时监控使用 GuardDuty 安全代理（这是一个 Amazon EKS 附加组件）来提供对各个 Amazon EKS 工作负载的运行时可见性。 GuardDuty 安全代理可帮助识别您的 Amazon EKS 集群中可能遭到入侵的特定容器。它还可以检测有人企图将权限从单个容器升级到底层 Amazon EC2 主机或更广泛的 AWS 环境。

GuardDuty 还提供一项名为 “扩展威胁检测” 的功能，该功能可自动检测跨越数据源、多种 AWS 资源类型和时间段的多阶段攻击。 AWS 账户 GuardDuty关联这些事件（称为信号），以识别对您的 AWS

环境构成潜在威胁的场景，然后生成攻击序列发现。这涵盖了涉及与 AWS 证书滥用相关的泄露以及您的中的数据泄露企图的威胁场景 AWS 账户。 GuardDuty 将所有攻击序列查找类型视为 “严重”。默认情况下，此功能处于启用状态，并且不会产生任何额外费用。

在 AWS SRA 中，通过在所有账户中启 GuardDuty 用 AWS Organizations，并且所有发现均可由相应的安全团队在 GuardDuty 委派的管理员帐户（在本例中为安全工具帐户）中查看和采取行动。GuardDuty 活动调查结果将导出到日志存档账户中的中央 S3 存储桶中，因此您可以将发现的保留时间超过 90 天。调查结果从委托管理员账户导出，还包括来自同一区域关联成员账户的所有调查结果。S3 存储桶中的结果使用 AWS KMS 客户托管密钥进行加密。S3 存储桶策略和 KMS 密钥策略配置GuardDuty为仅允许使用资源。

启用后 AWS Security Hub CSPM ，搜索 GuardDuty 结果会自动流向 Security Hub CSPM 和 Security Hub。启用 Amazon Detective 后， GuardDuty 发现的结果将包含在 Detective 日志采集流程中。GuardDuty 和 Detective 支持跨服务用户工作流程，其中 GuardDuty 提供来自控制台的链接，可将您从选定的发现重定向到包含一组精选的可视化效果的 Detective 页面，用于调查该发现。例如，您还可以 GuardDuty 与 Amazon EventBridge 集成，自动执行最佳实践 GuardDuty，例如自动回复新 GuardDuty 发现。

> 实现示例
>
> AWS SRA 代码库提供了一个实现示例。GuardDuty它包括加密的 S3 存储桶配置、委托管理以及 GuardDuty 对 AWS 组织中所有现有和未来账户的启用。

AWS Config

AWS Config是一项使您能够评估、审核和评估中受支持 AWS 资源的配置的服务 AWS 账户。 AWS Config 持续监控和记录 AWS 资源配置，并根据所需的配置自动评估记录的配置。您还可以 AWS Config 与其他服务集成，在自动审计和监控管道中完成繁重的工作。例如， AWS Config 可以监视中各个密钥的变化 AWS Secrets Manager。

您可以使用来评估 AWS 资源的配置设置AWS Config 规则。 AWS Config 提供了一个名为托管规则的可自定义预定义规则库，您也可以编写自己的自定义规则。您可以在主动模式（部署资源之前）或侦探模式（部署资源之后）下运行 AWS Config 规则 。当配置发生更改时，可以按定期计划或按选择的频率对资源进行评估。

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在账户和区域中 AWS Organizations，也可以跨组织部署。一致性包是通过创作一个 YAML 模板来创建的，该模板包含 AWS

Config 托管或自定义规则和补救操作的列表。要开始评估您的 AWS 环境，请使用其中一个样本一致性包模板。

AWS Config 与集成 AWS Security Hub CSPM ，将 AWS Config 托管和自定义规则评估的结果作为结果发送到 Security Hub CSPM。

AWS Config 规则 可以与结合使用， AWS Systems Manager 以有效修复不合规的资源。您可以使用 Systems Manager Explorer 收集 AWS 账户 跨界中AWS Config规则的合规性状态， AWS 区域 然后使用 S ystems Manager 自动化文档（运行手册）来解决您的不合规 AWS Config 规则。有关实施的详细信息，请参阅博客文章《使用 AWS Systems Manager 自动化运行手册修复不合规 AWS Config 规则》。

AWS Config 聚合器在中收集多个账户、地区和组织的配置和合规性数据。 AWS Organizations聚合器仪表板显示聚合资源的配置数据。库存和合规性仪表板提供有关组织中 AWS 账户、跨 AWS 区域组织或 AWS 组织内部的 AWS 资源配置和合规性状态的重要和最新信息。它们使您无需编写 AWS Config 高级查询即可对 AWS 资源库存进行可视化和评估。 您可以获得基本见解，例如按资源划分的合规性摘要、拥有不合规资源的前 10 个账户、按类型比较正在运行和已停止 EC2 实例以及按卷类型和大小划分的 EBS 卷。

如果您使用 AWS Control Tower 管理您的 AWS 组织，它将部署一组 AWS Config 规则作为侦探护栏（分为必修规则、强烈推荐规则或选修规则）。这些护栏可帮助您管理资源并监控组织中各个账户的合规性。 AWS 这些 AWS Config 规则将自动使用值为的`aws-control-tower`标签`managed-by-control-tower`。

AWS Config 必须为 AWS 组织中包含要保护的资源的每个成员帐户启用。 AWS 区域 您可以集中管理（例如，创建、更新和删除）AWS 组织内所有账户的 AWS Config 规则。通过 AWS Config 委派管理员帐户，您可以在所有账户中部署一组通用的 AWS Config 规则，并指定不应在其中创建 AWS Config 规则的帐户。 AWS Config 委派的管理员账户还可以汇总来自所有成员账户的资源配置和合规性数据，以提供单一视图。使用 APIs 来自委派管理员账户的，通过确保 AWS 组织中的成员账户无法修改基础 AWS Config 规则来强制治理。 AWS Config 如果启用了 Security Hub CSPM 并且至少存在一条 AWS Config 托管或自定义规则，则本机集成可将发现结果发送到 AWS Security Hub CSPM。

在 AWS SRA 中， AWS Config 委托的管理员帐户是安全工具帐户。 AWS Config 传输通道配置为在日志存档账户的集中式 S3 存储桶中传送资源配置快照。由于日志存档帐户是中央日志存储库，因此它用于存储资源配置。

设计注意事项

- AWS Config 将配置和合规性变更通知流向 Amazon EventBridge。这意味着您可以使用中的本机筛选功能 EventBridge 来筛选AWS Config 事件，以便可以将特定类型的通知路由到特定的目标。例如，您可以将特定规则或资源类型的合规性通知发送到特定的电子邮件地址，或者将配置更改通知发送到外部 IT 服务管理 (ITSM) 或配置管理数据库 (CMDB) 工具。有关更多信息，请参阅博客文章AWS Config 最佳实践。
- 除了使用 AWS Config 主动规则评估外，您还可以使用 AWS CloudFormation Guard，这是一种可以主动检查资源配置合规性的 policy-as-code评估工具。 AWS CloudFormation Guard 命令行界面 (CLI) 为您提供了一种声明性的、特定于域的语言 (DSL)，您可以使用该语言将策略表示为代码。此外，您可以使用 AWS CLI 命令来验证 JSON 格式或 YAML 格式的结构化数据，例如 CloudFormation 变更集、基于 JSON 的 Terraform 配置文件或 Kubernetes 配置。您可以在创作过程中使用 AWS CloudFormation Guard CLI 在本地运行评估，也可以在部署管道中运行评估。如果您有AWS Cloud Development Kit (AWS CDK)应用程序，则可以使用 cdk-nag 主动检查最佳实践。

实现示例

AWS SRA 代码库提供了一个示例实现，可将 AWS Config 一致性包部署到组织内的所有 AWS 账户 区域和区域。 AWS Agg AWS Config regator 模块可帮助您配置 AWS Config 聚合器，方法是将管理委托给组织管理账户中的成员账户（安全工具），然后在委派的管理员账户中为组织中所有现有和未来的账户配置 Agg AWS Config regator。 AWS 您可以使用 Cont AWS Config rol Tower 管理帐户模块在组织管理帐户 AWS Config 中启用，但该模块不是由启用的。 AWS Control Tower

Amazon Security Lake

Amazon Secur ity Lake 是一项完全托管的安全数据湖服务。您可以使用 Security Lake 自动集中来自 AWS 环境、软件即服务 (SaaS) 提供商、本地和第三方来源的安全数据。Security Lake 可帮助您构建标准化数据源，简化分析工具而不是安全数据的使用，因此您可以更全面地了解整个组织的安全状况。数据湖由 Amazon Simple Storage Service (Amazon S3) 存储桶提供支持，您保留数据的所有权。Security Lake 会自动收集日志 AWS 服务，包括 AWS CloudTrail亚马逊 VPC、Amazon Route 53、Amazon S3 AWS Lambda、Amazon EKS 审计日志、 AWS Security Hub CSPM 调查结果和 AWS WAF 日志。

AWS SRA 建议您使用日志存档帐户作为 Security Lake 的委托管理员帐户。有关设置委托管理员账户的更多信息，请参阅安全 OU — 日志存档账户部分中的 Amazon Security Lak e。想要访问 Security Lake 数据或需要能够使用自定义提取、转换和加载 (ETL) 函数将非原生日志写入 Security Lake 存储桶的安全团队应在 Security Tools 账户中操作。

Security Lake 可以收集来自不同云提供商的日志、来自第三方解决方案的日志或其他自定义日志。我们建议您使用安全工具帐户执行 ETL 函数，将日志转换为开放网络安全架构框架 (OCSF) 格式，并以 Apache Parquet 格式输出文件。Security Lake 创建跨账户角色，该角色对安全工具账户和由 Lambda 函数 AWS Glue 或爬虫支持的自定义源具有适当权限，用于向 Security Lake 的 S3 存储桶写入数据。

Security Lake 管理员应配置使用安全工具帐户并需要访问 Security Lake 作为订阅者收集的日志的安全小组。 Security Lake 支持两种类型的订阅者访问：

- 数据访问 — 订阅者可以直接访问安全湖的 Amazon S3 对象。Security Lake 管理基础设施和权限。当您将安全工具账户配置为安全湖数据访问订阅者时，该账户将通过亚马逊简单队列服务 (Amazon SQS) Simple SQUEE Service 收到有关安全湖存储桶中的新对象的通知，安全湖会创建访问这些新对象的权限。
- 查询访问权限 — 订阅者可以使用诸如 Amazon Athena 之类的服务从您的 S3 存储桶中的 AWS Lake Formation 表中查询源数据。使用 Lake Formation 可以自动设置跨账户访问以进行查询访问。当您将 Security Tooling 账户配置为 Security Lake 查询访问订阅者时，该账户将获得对 Security Lake 账户中日志的只读访问权限。当您使用此订阅者类型时，Security Lake Log Archive 账户中的 Athena AWS Glue 和表将通过 () 与安全工具帐户 AWS Resource Access Manager 共享。AWS RAM要启用此功能，您必须将跨账户数据共享设置更新到版本 3。

有关创建订阅者的更多信息，请参阅 Security Lake 文档中的订阅者管理。

有关提取自定义源的最佳实践，请参阅 Security Lake 文档中的从自定义来源收集数据。

你可以使用 Amazon Quick Sight、Amazon S OpenSearch er vic e 和 Amazon SageMaker 对存储在 Security Lake 中的安全数据进行分析。

> **设计注意事项**
>
> 如果应用程序团队需要查询Security Lake数据以满足业务需求，则Security Lake管理员应将该应用程序帐户配置为订阅者。

Amazon Macie

Amazon Macie 是一项完全托管的数据安全和数据隐私服务，它使用机器学习和模式匹配来发现和帮助保护您的敏感数据。 AWS您需要确定您的工作负载正在处理的数据的类型和分类，以确保实施适当的控制措施。您可以使用 Macie 通过两种方式自动发现和报告敏感数据：执行自动敏感数据发现以及创建和运行敏感数据发现任务。通过自动发现敏感数据，Macie 每天都会评估您的 S3 存储桶清单，并使用采样技术从您的存储桶中识别和选择具有代表性的 S3 对象。然后，Macie 检索并分析所选对象，检查它们是否有敏感数据。敏感数据发现工作可提供更深入、更有针对性的分析。使用此选项，您可以定义分析的广度和深度，包括要分析的 S3 存储桶、采样深度以及源自 S3 对象属性的自定义标准。如果 Macie 检测到存储桶的安全性或隐私存在潜在问题，它会为您创建策略调查发现。默认情况下，所有新的 Macie 客户都将启用自动数据发现，现有的 Macie 客户只需点击一下即可启用自动数据发现。

Macie 已通过 AWS Organizations以下方式在所有账户中启用。在委托管理员账户（在本例中为 Security Tooling 账户）中拥有相应权限的委托人可以在任何账户中启用或暂停 Macie，为成员账户拥有的存储分区创建敏感数据发现任务，以及查看所有成员账户的所有策略结果。只有创建敏感发现任务的账户才能查看敏感数据调查结果。有关更多信息，请参阅 Macie 文档中的作为一个组织管理多个 Macie 帐户。

Macie 的调查结果将提交给 AWS Security Hub CSPM 进行审查和分析。Macie 还与 Amazon 集成，EventBridge 以促进对警报、安全信息和事件管理 (SIEM) 系统的馈送以及自动补救等发现的自动响应。

设计注意事项

- 如果 S3 对象使用您管理的 AWS Key Management Service (AWS KMS) 密钥加密，则可以将 Macie 服务相关角色作为密钥用户添加到该 KMS 密钥中，以允许 Macie 扫描数据。
- Macie 已针对扫描 Amazon S3 中的对象进行了优化。因此，可以扫描任何可放入 Amazon S3（永久或临时）的 MacIE 支持的对象类型，以查找敏感数据。这意味着来自其他来源的数据（例如，亚马逊关系数据库服务 (Amazon RDS) 或亚马逊 Aurora 数据库的定期快照导出、导出的亚马逊 DynamoDB 表或从本机或第三方应用程序提取的文本文件）可以移动到 A mazon S3 并由 Macie 进行评估。

实现示例

AWS SRA 代码库提供了 Amazon Macie 的示例实现。它包括将管理委托给成员账户，以及在委托管理员账户中为组织中所有现有和将来的账户配置 Macie。 AWS Macie 还配置为将调查结果发送到使用客户托管密钥加密的中央 S3 存储桶。 AWS KMS

IAM 访问分析器

随着您加快 AWS Cloud 采用过程并继续创新，保持对细粒度访问权限（权限）的严格控制、遏制访问激增并确保有效使用权限至关重要。过多和未使用的访问权限会带来安全挑战，并使企业更难执行最小权限原则。该原则是一个重要的安全架构支柱，它涉及不断调整IAM权限的大小，以平衡安全要求与运营和应用程序开发需求。这项工作涉及多个利益相关者角色，包括中央安全和云卓越中心 (CCoE) 团队以及去中心化开发团队。

AWS Identity and Access Management A@@ ccess Analyzer 提供的工具可以有效地设置细粒度权限、验证预期权限，并通过删除未使用的访问权限来优化权限，从而帮助您满足企业安全标准。它使您可以通过仪表板和控制面板查看外部和内部对 AWS 资源的访问以及未使用的访问结果AWS Security Hub CSPM。此外，它还支持 Amazon 基于事件 EventBridge的自定义通知和补救工作流程。

IAM Access Analyzer 外部访问分析器发现结果功能可帮助您识别 AWS 组织和账户中与外部实体共享的资源，例如 A mazon S3 存储桶或 IAM 角色。您选择的 AWS 组织或账户被称为信任区域。分析器使用自动推理来分析信任区域内所有支持的资源，并为可以从信任区域之外访问资源的委托人生成调查结果。这些发现有助于识别与外部实体共享的资源，并帮助您在部署资源权限之前预览您的政策如何影响公共和跨账户访问您的资源。此项服务无需额外付费。

同样，IAM Access Analyzer 内部访问分析器查找功能可帮助您识别 AWS 组织中的资源以及与组织或账户内部委托人共享的账户。此分析通过确保只有组织内的目标委托人才能访问您的指定资源，从而支持最低权限原则。这是一项付费功能，需要明确配置资源才能进行检查。谨慎地使用此功能来监视特定的敏感资源，根据设计，即使在内部也需要锁定这些资源。

IAM Access Analyzer 的调查结果还可以帮助您识别您的 AWS 组织和账户中授予的未使用访问权限，包括：

- 未使用的 IAM 角色 — 在指定的使用窗口内没有访问活动的角色。
- 未使用的 IAM 用户、证书和访问密钥 — 属于 IAM 用户并用于访问 AWS 服务 和资源的证书。
- 未使用的 IAM 策略和权限 — 角色在指定使用窗口内未使用的服务级别和操作级权限。IAM Access Analyzer 使用附加到角色的基于身份的策略来确定这些角色可以访问的服务和操作。分析器可以查看所有服务级别权限的未使用权限。

您可以使用 IAM Access Analyzer 生成的调查结果，根据贵组织的策略和安全标准，了解并修复任何意外或未使用的访问。修复后，下次运行分析器时，这些发现将被标记为已解决。如果发现是故意的，您可以在 IAM Access Analyzer 中将其标记为已存档，并优先考虑其他存在更大安全风险的发现。此外，您可以设置存档规则以自动存档特定的调查结果。例如，您可以创建一个存档规则，来自动存档您定期为其授予访问权限的特定 Amazon S3 存储桶的调查发现。

作为构建者，您可以使用 IAM Access Analyzer 在开发和部署 (CI/CD) 流程的早期自动执行 IAM 策略检查，以遵守您的企业安全标准。作为开发团队 CI/CD 管道的一部分，您可以将 IAM Access Analyzer 自定义策略检查和策略审查与 AWS CloudFormation 集成，从而自动执行策略审查。这包括：

- IAM 策略验证 — IAM Access Analyzer 会根据 IAM 策略语法和 AWS 最佳实践验证您的策略。您可以查看策略验证检查的结果，包括安全警告、错误、一般警告和策略建议。目前有 100 多项策略验证检查可用，可以使用 AWS Command Line Interface (AWS CLI) 和自动执行这些检查 APIs。
- IAM 自定义策略检查 — IAM Access Analyzer 自定义策略检查根据您指定的安全标准验证您的策略。自定义策略检查使用自动推理，为满足企业安全标准提供更高级别的保证。自定义策略检查的类型包括：
  - 根据@@ 参考策略进行核对：编辑策略时，可以将其与参考策略（例如策略的现有版本）进行比较，以检查更新是否授予了新的访问权限。CheckNoNewAccessAPI 比较两个策略（更新后的策略和参考策略），以确定更新后的策略是否通过引用策略引入了新的访问权限，并返回通过或失败的响应。
  - 对照 IAM 操作列表进行核对：您可以使用 CheckAccessNotGrantedAPI 来确保策略不会授予对安全标准中定义的关键操作列表的访问权限。此 API 采用策略和最多 100 个 IAM 操作的列表来检查该策略是否允许至少一个操作，并返回通过或失败的响应。

安全团队和其他 IAM 策略作者可以使用 IAM Access Analyzer 来编写符合 IAM 策略语法和安全标准的策略。手动编写大小合适的策略可能容易出错且耗时。IAM Access Analyzer 策略生成功能可帮助编写基于委托人访问活动的 IAM 策略。IAM Access Analyzer 会查看支持的服务的 AWS CloudTrail日志，并生成一个策略模板，其中包含委托人在指定日期范围内使用的权限。然后，您可以使用此模板创建具有精细权限的策略，该策略仅授予必要的权限。

- 您必须为账户启用 CloudTrail 跟踪，才能根据访问活动生成策略。
- IAM Access Analyzer 不会在生成的策略中识别数据事件的操作级活动，例如 Amazon S3 数据事件。
- 该`iam:PassRole`操作不会被跟踪 CloudTrail ，也不会包含在生成的策略中。

IAM Access Analyzer 是通过中的委托管理员功能在安全工具账户中部署的 AWS Organizations。授权的管理员有权创建和管理以 AWS 组织为信任区的分析器。

> **设计注意事项**
>
> 要获得账户范围内的调查结果（其中账户作为可信边界），您可以在每个成员账户中创建一个账户范围的分析器。这可以作为账户渠道的一部分来完成。账户范围内的调查结果将在成员账户级别流入 Security Hub CSPM。从那里，它们会流向 Security Hub CSPM 委托管理员账户（安全工具）。

> **实施示例**
>
> - AWS SRA 代码库提供了 IAM Access Analyzer 的示例实现。它演示了如何在委派的管理员账户中配置组织级分析器，在每个账户中配置账户级分析器。
> - 有关如何将自定义策略检查集成到构建器工作流程的信息，请参阅 AWS 博客文章 IAM Access Analyzer 自定义策略检查简介。

AWS Firewall Manager

AWS Firewall Manager通过简化跨多个账户和资源对 AWS WAF、 AWS Shield Advanced、Amazon VPC 安全组和 Amazon Route 53 Resolver DNS 防火墙的管理和维护任务 AWS Network Firewall，帮助保护您的网络。使用 Firewall Manager，您只需设置一次 AWS WAF 防火墙规则、Shield 高级保护、Amazon VPC 安全组、网络防火墙和 DNS 防火墙规则组关联。即使您添加新资源，该服务也会自动跨账户和资源应用您的规则和保护。

当您想要保护整个 AWS 组织而不是少数特定帐户和资源，或者您经常添加想要保护的新资源时，Firewall Manager 特别有用。Firewall Manager 使用安全策略允许您定义一组配置，包括必须部署的相关规则、保护和操作，以及要包含或排除的帐户和资源（由标签指示）。您可以创建精细而灵活的配置，同时仍然能够将控制范围扩展到大量帐户和 VPCs. 即使创建了新账户和资源，这些策略也会自动一致地强制执行您配置的规则。Firewall Manager 通过在所有帐户中启用 AWS Organizations，配置和管理由相应的安全团队在 Firewall Manager 委派的管理员帐户（在本例中为安全工具帐户）中执行。

您必须 AWS Config 为 AWS 区域 包含要保护的资源的每个资源启用该选项。如果您不想 AWS Config 为所有资源启用该功能，则必须为与您所使用的 Firewall Manager 策略类型关联的资源启用该功能。

当你同时使用两者 AWS Security Hub CSPM 以及防火墙管理器时，Firewall Manager 会自动将你的发现发送到 Security Hub CSPM。Firewall Manager 会为不合规的资源及其检测到的攻击创建调查结果，并将发现结果发送到 Security Hub CSPM。为设置 Firewall Manager 策略时 AWS WAF，可以集中启用所有范围内帐户的 Web 访问控制列表 (Web ACLs) 上的登录功能，并将日志集中在一个帐户下。

使用 Firewall Manager，您可以有一个或多个管理员来管理组织的防火墙资源。当您分配多个管理员时，您可以应用限制性的管理范围条件来定义每个管理员可以管理的资源（帐户 OUs、区域、策略类型）。这使您可以灵活地在组织中使用不同的管理员角色，并帮助您保持最低权限访问的原则。 AWS SRA 使用一名管理员，其全部管理权限委托给安全工具帐户。

设计注意事项

AWS 组织中个人成员账户的客户经理可以根据自己的特定需求在 Firewall Manager 托管服务中配置其他控件（例如 AWS WAF 规则和 Amazon VPC 安全组）。

实现示例

AWS SRA 代码库提供了 Fi rewall Manager 的实现示例。它演示委托管理（Security Tools）、部署允许的最大安全组、配置安全组策略以及配置多个策略。 AWS WAF

Amazon EventBridge

Amazon EventBridge 是一项无服务器事件总线服务，可以直接将您的应用程序与来自各种来源的数据连接起来。它经常用于安全自动化。您可以设置路由规则来确定将数据发送到何处，从而构建能够实时响应所有数据源的应用程序架构。除了在每个账户中使用默认事件总线外，您还可以创建自定义事件总线来接收来自自定义应用程序的事件。您可以在 Security Tools 账户中创建事件总线，该总线可以接收来自 AWS 组织中其他账户的安全特定事件。例如，通过链接 AWS Config 规则 GuardDuty、Amazon 和 AWS Security Hub CSPM EventBridge，您可以创建一个灵活、自动化的管道，用于路由安全数据、发出警报和管理解决问题的操作。

设计注意事项

- EventBridge 能够将事件路由到多个不同的目标。自动执行安全操作的一种有价值的模式是将特定事件与个人 AWS Lambda 响应者联系起来，后者会采取适当的行动。例如，在某些情况下，您可能需要使用将公有 S3 存储桶查找结果路由 EventBridge 到更正存储桶策略并

删除公共权限的 Lambda 响应器。可以将这些响应者整合到您的调查手册和操作手册中，以协调响应活动。

- 成功的安全运营团队的最佳做法是将安全事件和发现的流程集成到通知和工作流系统中，例如票务系统、 bug/issue 系统或其他安全信息和事件管理 (SIEM) 系统。这样可以省去电子邮件和静态报告的工作流程，并帮助您路由、上报和管理事件或发现。中的灵活路由功能 EventBridge 是实现这种集成的强大推动力。

Amazon Detective

Amazon Detective 让您的安全分析师可以直接分析、调查和快速识别安全发现或可疑活动的根本原因，从而支持您的响应式安全控制策略。Detective 会自动从 AWS CloudTrail 日志和 Amazon VPC 流日志中提取基于时间的事件，例如登录尝试、API 调用和网络流量。Detective 通过使用独立的日志流和 Amazon VPC 流 CloudTrail 日志来使用这些事件。您可以使用 Detective 访问长达一年的历史事件数据。Detective 使用机器学习和可视化来创建统一的交互式视图，以了解您的资源行为以及资源之间随时间推移的交互情况，这称为行为图。您可以浏览行为图来检查不同的操作，例如登录尝试失败或可疑 API 调用。

Detective 与 Amazon Security Lake 集成，使安全分析师能够查询和检索存储在 Security Lake 中的日志。在 Detective 中进行安全调查时，您可以使用此集成从存储在 Security Lake 中的 CloudTrail 日志和 Amazon VPC 流日志中获取更多信息。

Detective 还会提取亚马逊检测到的结果 GuardDuty，包括GuardDuty 运行时监控检测到的威胁。当某个帐户启用 Detective 时，它将成为行为图的管理员帐户。在尝试启用 Detective 之前，请确保您的账户已注册至少 48 小时。 GuardDuty 如果您不满足此要求，则无法启用 DetectiveDetective。

Detective 的其他可选数据源包括 Amazon EKS 审核日志和 AWS Security Hub CSPM。Amazon EKS 审核日志数据源增强了所提供的有关以下实体类型的信息：Amazon EKS 集群、Kubernetes 容器、容器镜像和 Kubernetes 主体。Security Hub 数据源是AWS 安全发现的一部分，它将跨产品的发现关联到 Security Hub，然后将其摄取到 Detective 中。

Detective 会自动将与单个安全漏洞事件相关的多个发现分组到查找组中。威胁行为者通常会执行一系列操作，这些操作会导致多个跨时间和资源的安全发现。因此，调查小组应是涉及多个实体和调查结果的调查的起点。Detective 还使用生成式 AI 来提供查找小组摘要，该人工智能会自动分析查找群组，并以自然语言提供见解，以帮助您加快安全调查。

Detective 与... 集成 AWS Organizations。组织管理账户委托一个成员账户作为 Detective 管理员账户。在 AWS SRA 中，这是安全工具帐户。Detective 管理员帐户能够自动启用组织中所有当前成员帐户作为 Detective 成员帐户，还可以在将新成员帐户添加到 AWS 组织时添加这些帐户。Detective 管

理员账户还可以邀请当前不居住在 AWS 组织中但位于同一地区的成员账户将其数据贡献到主账户的行为图中。当成员账户接受邀请并启用时，Detective 开始提取该成员账户的数据并将其提取到该行为图中。

> **设计注意事项**
>
> 您可以导航到 Detective，从 GuardDuty 和 AWS Security Hub CSPM 控制台中查找个人资料。这些链接可以帮助简化调查流程。你的账户必须是 Detective 和你要转出的服务（GuardDuty或 Security Hub CSPM）的管理账户。如果服务的主账户相同，则集成链接可以无缝运行。

AWS Audit Manager

AWS Audit Manager帮助您持续审核 AWS 使用情况，从而简化管理审计和遵守法规和行业标准的方式。它使您能够从手动收集、审查和管理证据转变为自动收集证据的解决方案，提供一种跟踪审计证据来源的简单方法，支持团队协作，并有助于管理证据的安全性和完整性。当需要进行审计时，Audit Manager 可帮助您管理利益相关者对控件的审核。

使用 Audit Manager，您可以根据预先构建的框架进行审计，例如互联网安全中心 (CIS) 基准、CIS AWS 基金会基准、系统和组织控制 2 (SOC 2) 和支付卡行业数据安全标准 (PCI DSS)。它还使您能够根据内部审计的具体要求使用标准或自定义控件创建自己的框架。

Audit Manager 收集了四种类型的证据。自动生成三种类型的证据：来自和的合规性检查证据 AWS Security Hub CSPM、来自 AWS Config 和的管理事件证据 AWS CloudTrail，以及来自 AWS service-to-service API 调用的配置证据。对于无法自动处理的证据，Audit Manager 允许您上传手动证据。

默认情况下，您在 Audit Manager 中的数据使用 AWS 托管密钥进行加密。 AWS SRA 使用客户管理的密钥进行加密，以更好地控制逻辑访问。您还应该在 Audit Manager 发布评估报告 AWS 区域 的地方配置 S3 存储桶。这些存储桶应使用客户托管密钥进行加密，并具有配置为仅允许 Audit Manager 发布报告的存储桶策略。

> **Note**
>
> Audit Manager 协助收集与验证是否符合特定合规标准和法规相关的证据。但是，它不会评估您的合规性。因此，通过 Audit Manager 收集的证据可能不包括审计所需的操作流程细节。Audit Manager 不能替代法律顾问或合规专家。我们建议您聘请第三方评估员的服务，该评估机构已根据您接受评估的合规框架获得认证。

Audit Manager 评估可以跨 AWS 组织中的多个账户进行。Audit Manager 收集证据并将其合并到中的委托管理员帐户中。 AWS Organizations此审计功能主要由合规和内部审计团队使用，只需要您的读取权限 AWS 账户。

设计注意事项

- Audit Manager 补充了其他 AWS 安全服务，例如 AWS Security Hub CSPM AWS Security Hub、和， AWS Config 以帮助实施风险管理框架。Audit Manager 提供独立的风险保障功能，而 Security Hub CSPM 可帮助您监督风险， AWS Config 合规包有助于管理风险。熟悉内部审计师协会（IIA）开发的三条线模型的审计专业人员应注意，这种组合 AWS 服务 可以帮助您涵盖三道防线。有关更多信息，请参阅 “ AWS Cloud 操作与迁移” 博客上由两部分组成的博客系列。
- 为了让 Audit Manager 收集 Security Hub CSPM 证据，两个服务的委派管理员帐户必须相同。 AWS 账户因此，在 AWS SRA 中，安全工具帐户是 Audit Manager 的授权管理员。

AWS Artifact

AWS Artifact托管在 Security Tools 账户中，用于将合规性项目管理功能与 AWS 组织管理账户分开。这种职责分工很重要，因为除非绝对必要，否则我们建议您避免使用 AWS 组织管理帐户进行部署。相反，将部署传递给成员账户。由于审计对象管理可以通过成员帐户完成，并且该职能与安全与合规团队密切一致，因此 Security Tools 帐户被指定为 AWS Artifact管理员帐户。您可以使用 AWS Artifact 报告下载 AWS 安全和合规性文档，例如 AWS ISO 认证、支付卡行业 (PCI) 以及系统和组织控制 (SOC) 报告。

AWS Artifact 不支持委派管理功能。相反，您可以将此功能限制为 Security Tools 账户中与您的审计和合规团队相关的 IAM 角色，这样他们就可以根据需要下载、查看这些报告并将其提供给外部审计员。此外，您还可以通过 IAM 策略限制特定的 IAM 角色只能访问特定的 AWS Artifact 报告。有关 IAM 策略的示例，请参阅AWS Artifact 文档。

设计注意事项

如果您选择 AWS 账户 为审计和合规团队设立一个专门的账户，则可以托管 AWS Artifact 一个安全审计账户，该账户与安全工具账户是分开的。 AWS Artifact 报告提供的证据表明一个组织正在遵循记录在案的流程或满足特定要求。审计工件在整个系统开发生命周期中收集和存档，可用作内部或外部审计和评估的证据。

AWS KMS

AWS Key Management Service(AWS KMS) 可帮助您创建和管理加密密钥，并控制其在各种 AWS 服务 应用程序中的使用。 AWS KMS 是一项安全且有弹性的服务，它使用硬件安全模块来保护加密密钥。它遵循行业标准的密钥材料生命周期流程，例如密钥的存储、轮换和访问控制。 AWS KMS 可以使用加密和签名密钥来帮助保护您的数据，并且可以通过加密 SDK 用于服务器端加密和客户端加AWS密。为了保护和灵活性， AWS KMS 支持三种类型的密钥：客户托管密钥、 AWS 托管密钥和 AWS 自有密钥。客户管理的密 AWS KMS 钥 AWS 账户 是您创建、拥有和管理的密钥。 AWS 托管 AWS KMS 密钥是您账户中的密钥，由与集成的用户代表您创建、管理和使用 AWS KMS。 AWS 服务 AWS 拥有的密钥是 AWS 服务 拥有并管理的 AWS KMS 密钥的集合，用于多个密钥 AWS 账户。有关使用 AWS KMS 密钥的更多信息，请参阅AWS KMS 文档和AWS KMS 加密详细信息。

一种部署选项是将 AWS KMS 密钥管理的责任集中到单个账户，同时使用密钥和 IAM 策略的组合，委托应用程序资源使用应用程序账户中密钥的权限。这种方法既安全又易于管理，但是由于限制限制、账户服务 AWS KMS 限制以及安全团队被大量操作密钥管理任务所淹没，您可能会遇到障碍。另一种部署选项是采用去中心化模式，在这种模式中，您可以 AWS KMS 允许驻留在多个账户中，并允许负责特定账户中基础设施和工作负载的人员管理自己的密钥。此模型使您的工作负载团队能够更好地控制加密密钥的使用，提高灵活性和敏捷性。它还有助于避免 API 限制，将影响范围限制为 AWS 账户 仅一个，并简化报告、审计和其他与合规相关的任务。在去中心化模式中，重要的是要部署和强制执行护栏，以便以相同的方式管理分散式密钥，并根据既定的最佳实践和政策对 AWS KMS 密钥的使用进行审计。有关更多信息，请参阅白皮书AWS Key Management Service 最佳实践。 AWS SRA 建议采用分布式密钥管理模式，在这种模式中， AWS KMS 密钥存储在本地使用密钥的账户中。我们建议您避免在一个账户中使用单一密钥来实现所有加密功能。可以根据功能和数据保护要求创建密钥，并强制执行最小权限原则。在某些情况下，加密权限将与解密权限分开，管理员将管理生命周期功能，但无法使用他们管理的密钥加密或解密数据。

在 Security AWS KMS Tools 帐户中，用于管理集中式安全服务的加密，例如由 AWS CloudTrail 组织管理的 AWS 组织跟踪。

AWS 私有 CA

AWS 私有证书颁发机构(AWS 私有 CA) 是一项托管私有 CA 服务，可帮助您安全地管理 EC2 实例、容器、物联网设备和本地资源的私有终端实体 TLS 证书的生命周期。它允许与正在运行的应用程序进行加密 TLS 通信。使用 AWS 私有 CA，您可以创建自己的 CA 层次结构（从属于终端实体证书的根 CA）CAs，并使用它颁发证书，以对内部用户、计算机、应用程序、服务、服务器和其他设备进行身份验证，并对计算机代码进行签名。私有 CA 颁发的证书仅在您的 AWS 组织内部受信任，在互联网上不受信任。

公钥基础架构 (PKI) 或安全团队可以负责管理所有 PKI 基础架构。这包括私有 CA 的管理和创建。但是，必须有一项规定，允许工作量团队自行满足其证书要求。 AWS SRA 描绘了一个集中的 CA 层次结构，其中根 CA 托管在安全工具账户中。这使安全团队能够实施严格的安全控制，因为根 CA 是整个 PKI 的基础。但是，通过使用 AWS Resource Access Manager (AWS RAM) 将私有 CA 共享给应用程序账户，将私有 CA 的私有证书创建委托给应用程序开发团队。 AWS RAM 管理跨账户共享所需的权限。这样就无需在每个账户中都使用私有 CA，并提供了一种更具成本效益的部署方式。有关工作流程和实现的更多信息，请参阅博客文章 “AWS RAM 如何使用共享您的 AWS 私有 CA 跨账户”。

> **Note**
>
> AWS Certificate Manager (ACM) 还可以帮助您配置、管理和部署公有 TLS 证书以供使用 AWS 服务。为了支持此功能，ACM 必须驻留在 AWS 账户 将使用公共证书的。本指南后面的应用程序账户部分将对此进行讨论。

> **设计注意事项**
>
> - 使用 AWS 私有 CA，您可以创建最多五个级别的证书颁发机构层次结构。您还可以创建多个层次结构，每个层次结构都有自己的根。 AWS 私有 CA 层次结构应符合贵组织的 PKI 设计。但是，请记住，增加 CA 层次结构会增加认证路径中的证书数量，这反过来又会增加最终实体证书的验证时间。定义明确的 CA 层次结构提供的好处包括适用于每个 CA 的精细安全控制、将从属 CA 委派给不同的应用程序（这会导致管理任务的分工）、使用具有有限的可撤销信任的 CA、能够定义不同的有效期以及强制执行路径限制的能力。理想情况下，你的根和下级 CAs 是分开的 AWS 账户。有关使用规划 CA 层次结构的更多信息 AWS 私有 CA，请参阅AWS 私有 CA 文档和博客文章《如何保护汽车和制造业的企业规模 AWS 私有 CA 层次结构》。
> - AWS 私有 CA 可以与现有的 CA 层次结构集成，这样您就可以将 ACM 的自动化和原生 AWS 集成功能与您当前使用的现有信任根结合使用。您可以在本地创建由父 CA AWS 私有 CA 支持的从属 CA。有关实现的更多信息，请参阅 AWS 私有 CA 文档中的安装由外部父 CA 签名的从属 CA 证书。

Amazon Inspector

Amazon Inspector 是一项自动漏洞管理服务，可自动发现和扫描 Amazon EC2 实例、Amazon Elastic Container Registry (Amazon ECR) 中的容器映像、 AWS Lambda 函数和源代码管理器中的代码存储库，以查找已知的软件漏洞和意外网络泄露。

每当你对资源进行更改时，Amazon Inspector 都会自动扫描资源，从而在资源的整个生命周期中持续评估您的环境。启动资源重新扫描的事件包括在 EC2 实例上安装新软件包、安装补丁以及发布影响资源的新常见漏洞和暴露 (CVE) 报告。Amazon Inspector 支持互联网安全中心 (CIS) 对 EC2 实例中的操作系统进行基准评估。

Amazon Inspector 与 Jenkins 等开发者工具集成， TeamCity 用于容器映像评估。您可以评估您的容器镜像是否存在持续集成和持续交付（CI/CD) tools, and push security to an earlier point in the software development lifecycle. Assessment findings are available in the CI/CD工具控制面板）中的软件漏洞，这样您就可以执行自动操作来应对关键的安全问题，例如构建受阻或映像推送到容器注册表。如果你有活跃的 AWS 账户，你可以从你的 CI/CD 工具市场安装 Amazon Inspector 插件，然后在你的构建管道中添加亚马逊 Inspector 扫描，而无需激活 Amazon Inspector 服务。此功能适用于托管在任何地方（本地 AWS、本地或混合云中）的 CI/CD 工具，因此您可以在所有开发管道中始终如一地使用单一解决方案。激活 Amazon Inspector 后，它会自动大规模发现您的所有 EC2 实例、Amazon ECR 和 CI/CD 工具中的容器镜像以及 Lambda 函数，并持续监控它们是否存在已知漏洞。

Amazon Inspector 的网络可访问性调查结果评估您的 EC2 实例通过虚拟网关进出 VPC 边缘（例如互联网网关、VPC 对等连接或虚拟专用网络 (VPNs)）的可访问性。这些规则有助于自动监控您的 AWS 网络，并识别安全组、访问控制列表 (ACLs)、Internet 网关等管理不善可能导致对 EC2 实例的网络访问配置不当的地方。有关更多信息，请参阅 Amazon Inspector 文档。

当 Amazon Inspector 发现漏洞或开放的网络路径时，它会生成一个可供您调查的结果。该发现包括有关该漏洞的全面细节，包括风险评分、受影响的资源和补救建议。风险评分是专门针对您的环境量身定制的，其计算方法是将 up-to-date CVE 信息与时间和环境因素（例如网络可访问性和可利用性信息）关联起来，从而提供上下文调查结果。

Amazon Inspector Code Secur ity 会扫描第一方应用程序源代码、第三方应用程序依赖项和基础设施即代码 (IaC) 以查找漏洞。 激活 Code Security 后，您可以创建扫描配置并将其应用于代码存储库，以确定扫描频率、扫描类型和要扫描的存储库。 代码安全支持静态应用程序安全测试 (SAST)、软件组成分析 (SCA) 和 IaC 扫描。要配置频率，您可以按需、更改代码时或定期定义扫描。代码扫描可捕获代码片段以突出显示检测到的漏洞。代码片段使用 KMS 密钥加密存储。组织的委派管理员无法查看属于成员账户的代码片段。将源代码管理器 (SCMs) 与代码安全集成后，所有代码存储库都会在 Amazon Inspector 控制台中作为项目列出。代码安全仅监控每个存储库的默认分支。Amazon Inspector 通过直接在开发人员工作的地方提供特定的代码修复建议来简化安全补救措施。与您的 SCM 的双向集成会自动在拉取请求 (PRs) 和合并请求 (MRs) 中以评论形式建议修复关键和重要发现，并提醒开发人员注意需要解决的最重要的漏洞，而不会中断他们的工作流程。

要扫描漏洞，必须使用 AWS Systems Manager 代理 (SSMAgent) 管理 EC2 实例。 AWS Systems Manager 无需代理即可实现 EC2 实例的网络可访问性或对 Amazon ECR 或 Lambda 函数中的容器映像进行漏洞扫描。

Amazon Inspector 与委托管理集成 AWS Organizations 并支持委托管理。在 AWS SRA 中，安全工具账户被设为 Amazon Inspector 的委托管理员账户。Amazon Inspector 委托管理员账户可以管理 AWS 组织成员的调查结果数据和某些设置。这包括查看所有成员账户的汇总结果的详细信息、启用或禁用对成员账户的扫描，以及查看 AWS 组织内扫描的资源。

设计注意事项

- 启用这两项服务后，Amazon Inspector 会自动与 AWS Security Hub CSPM Security Hub 集成。您可以使用此集成将来自 Amazon Inspector 的所有调查结果发送到 Security Hub CSPM，然后 Security Hub CSPM 会将这些发现纳入对您的安全态势的分析中。
- Amazon Inspector 会自动将调查结果、资源覆盖范围变化和单个资源的初始扫描的事件导出到亚马逊 EventBridge，也可以导出到亚马逊简单存储服务 (Amazon S3) 存储桶。要将活动调查结果导出到 S3 存储桶，您需要一个 Amazon Inspector 可用于加密调查结果的 AWS KMS 密钥，以及一个具有允许 Amazon Inspector 上传对象的权限的 S3 存储桶。EventBridge集成使您能够近乎实时地监控和处理调查结果，这是现有安全与合规工作流程的一部分。 EventBridge 除了事件来源的成员账户外，还会将事件发布到 Amazon Inspector 委托的管理员账户。
- Amazon Inspector Code Security 与 GitHub SaaS、 GitHub 企业云和 GitHub 企业服务器的集成需要公共互联网接入。

实现示例

AWS SRA 代码库提供了 Amazon Inspec tor 的示例实现。它演示了委托管理（安全工具），并为 AWS 组织中所有现有和未来的账户配置 Amazon Inspector。

AWS 安全事件响应

AWS 安全事件响应是一项服务，可帮助您为 AWS 环境中的安全事件做好准备并做出响应。它会对发现的结果进行分类，升级安全事件，并管理需要您立即关注的案例。 此外，它还允许您访问 AWS 客户事件响应小组 (CIRT)，该小组负责调查受影响的资源。 AWS 安全事件响应 还通过 AWS Systems Manager 文档（SSM 文档）提供自动响应和补救功能，帮助安全团队更有效地响应安全事件并从中恢复。 AWS 安全事件响应 与 Amazon GuardDuty 集成 AWS Security Hub CSPM，可接收安全调查结果并编排自动响应。

在 AWS SRA 中 AWS 安全事件响应 ，作为委托管理员帐户部署在安全工具帐户中。之所以选择 Security Tools 帐户，是因为它符合该账户的目的，即运营安全服务以及自动发送安全警报和响应。安全工具帐户还充当 Security Hub CSPM 的委托管理员帐户，除此之外 GuardDuty，它还有助于简化工作流程管理。 AWS 安全事件响应 AWS 安全事件响应 配置为使用 AWS Organizations，因此您可以通过 Security Tooling 帐户管理组织账户中的事件响应。

AWS 安全事件响应 帮助您实施事件响应生命周期的以下阶段：

- 准备：为遏制行动制定和维护应对计划和 SSM 文档。
- 检测和分析：自动分析安全发现并确定事件的严重性。
- 检测和分析：提交服务支持的案例，并与 AWS CIRT 联系以获得更多帮助。CIRT 是一群在活跃的安全事件中提供支持的个人。
- 遏制和根除：通过 SSM 文档运行自动遏制操作。
- 事后活动：记录事件详细信息并进行事后分析。

您也可以使用创建自我管理 AWS 安全事件响应 的案例。 AWS 安全事件响应 当您需要了解可能影响您的账户或资源的事情或采取行动时，可以创建出站通知或案例。只有当您在订阅中启用主动响应和警报分类工作流程时，此功能才可用。

设计注意事项

- 在实施自动响应操作时 AWS 安全事件响应，请仔细检查和测试自动响应操作，然后再将其投入生产。自动化可以加快事件响应速度，但配置不当的自动操作可能会影响合法的工作负载。
- 考虑使用中的 SSM 文档 AWS 安全事件响应 来实施组织特定的控制程序，同时维护该服务针对常见事件类型的内置最佳实践。
- 如果您计划在 VPC AWS 安全事件响应 中使用，请确保为 Systems Manager 和其他集成服务配置了相应的 VPC 终端节点，以便在私有子网中启用遏制操作。

在所有内部署通用安全服务 AWS 账户

本参考文献前面的 “在 AWS 组织中应用安全服务” 部分重点介绍了保护组织的安全服务 AWS 账户，并指出其中许多服务也可以在内部配置和管理 AWS Organizations。其中一些服务应部署在所有账户中，您将在 AWS SRA中看到它们。这可以实现一组一致的护栏，并在整个组织中提供集中式监控、管理和治理。 AWS

Security Hub CSPM、、 GuardDuty、 AWS Config、IAM Access Analyzer 和 CloudTrail 组织跟踪出现在所有账户中。前三个支持前面在 “管理帐户”、“可信访问权限和委派管理员” 一节中讨论的委派管理员功能。 CloudTrail 目前使用不同的聚合机制。

AWS SRA GitHub 代码存储库提供了在所有账户（包括组织管理账户）上启用 Security Hub CSPM GuardDuty AWS Config AWS Firewall Manager、、、和 CloudTrail 组织跟踪的 AWS 实现示例。

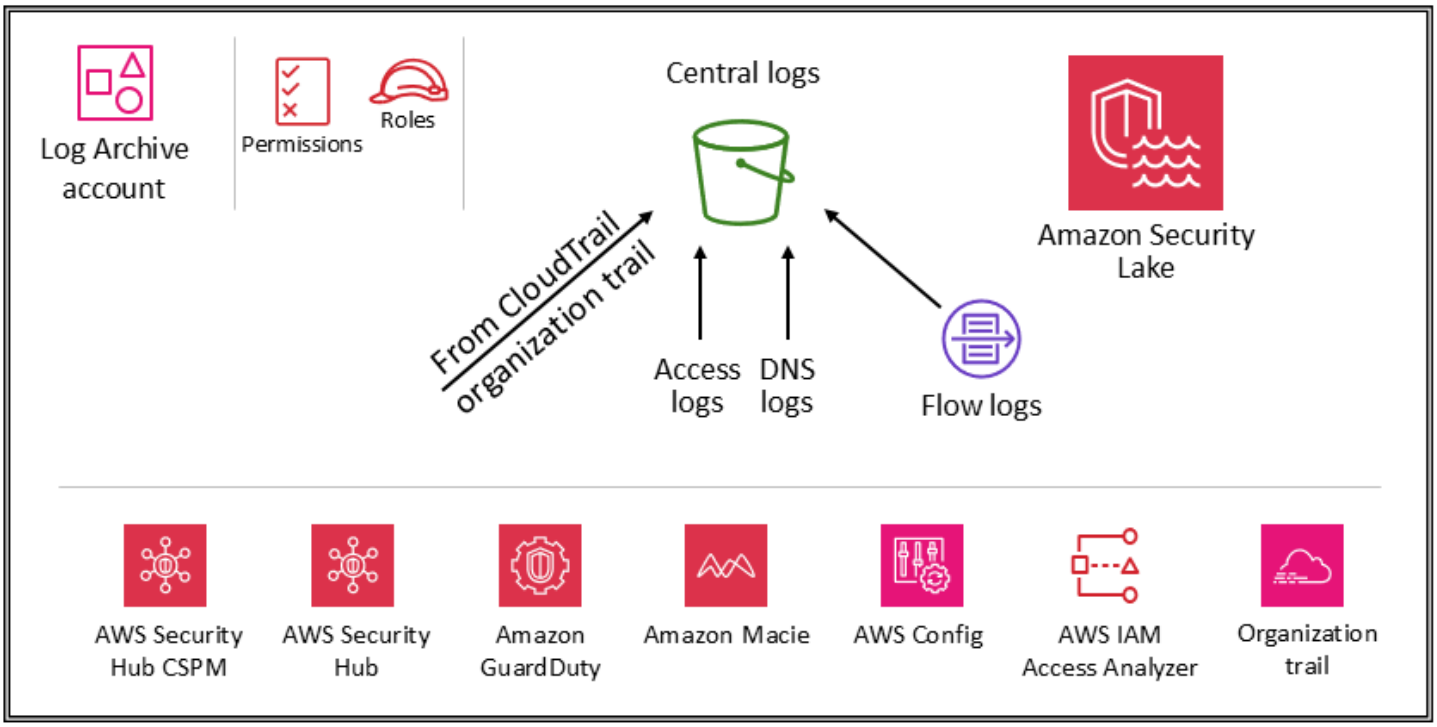
设计注意事项

- 特定的账户配置可能需要额外的安全服务。例如，管理 S3 存储桶（应用程序和日志存档账户）的账户还应包括 Amazon Macie，并考虑在这些常见安全服务中启 CloudTrail 用 S3 数据事件记录。（Macie 支持通过集中配置和监控进行委托管理。）另一个例子是 Amazon Inspector，它仅适用于托管 EC2 实例或亚马逊 ECR 映像的账户。
- 除了本节前面介绍的服务外， AWS SRA 还包括两项以安全为重点的服务，即 Amazon Detective 和 AWS Audit Manager，它们支持 AWS Organizations 集成和委托管理员功能。但是，这些服务并未包含在账户基准的推荐服务中，因为我们已经看到，这些服务最适合在以下场景中使用：
  - 您有一个专门的团队或一组资源来执行这些职能。安全分析团队最能利用 Detective，而 Audit Manager 对您的内部审计或合规团队很有帮助。
  - 您希望在项目开始时专注于一组核心工具，例如 GuardDuty 和 Security Hub CSPM，然后使用提供额外功能的服务在这些工具的基础上再接再厉。

安全 OU – 日志存档账户

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

下图说明了在日志存档帐户中配置 AWS 的安全服务。



日志存档账户专门用于摄取和存档所有与安全相关的日志和备份。有了集中日志，您可以监控、审计 Amazon S3 对象访问、身份未经授权的活动、IAM 策略变更以及对敏感资源执行的其他关键活动并发出警报。安全目标很简单：这应该是不可变的存储，只能通过受控、自动化和受监控的机制进行访问，并且专为持久性而构建（例如，通过使用适当的复制和存档流程）。可以深入实施控制措施，以保护日志和日志管理过程的完整性和可用性。除了预防性控制（例如分配用于访问的最低权限角色和使用受控 AWS KMS 密钥加密日志）外，还可以使用侦探控件，例如监控（并提醒和修复）这组权限 AWS Config 以防意外更改。

> **设计注意事项**
>
> 基础架构、运营和工作负载团队使用的操作日志数据通常与安全、审计和合规团队使用的日志数据重叠。我们建议您将操作日志数据整合到日志存档帐户中。根据您的特定安全和监管要求，您可能需要筛选保存到此账户的操作日志数据。您可能还需要指定谁有权访问日志存档帐户中的操作日志数据。

日志的类型

AWS SRA 中显示的主要日志包括 AWS CloudTrail （组织跟踪）、Amazon VPC 流日志、来自亚马逊和的访问日志 AWS WAF， CloudFront 以及来自 Amazon Route 53 的 DNS 日志。这些日志提供对用户、角色或网络实体（例如，通过 IP 地址识别）所采取（或尝试）操作的审计。 AWS 服务也可以捕

获和存档其他日志类型（例如应用程序日志或数据库日志）。有关日志源和日志记录最佳实践的更多信息，请参阅每项服务的安全文档。

亚马逊 S3 作为中央日志存储

Amazon S3 中有许多 AWS 服务 日志信息，无论是默认还是独有的。 AWS CloudTrail、Amazon VPC 流日志、Elastic Load Balancing GuardDuty AWS Config、Amazon 以及 AWS WAF 在 Amazon S3 中记录信息的服务的一些示例。这意味着日志完整性是通过 S3 对象完整性实现的；日志机密性是通过 S3 对象访问控制实现的；日志可用性是通过 S3 对象锁定、S3 对象版本和 S3 生命周期规则实现的。通过将信息记录在位于专用账户中的集中式 S3 存储桶中，您只需在几个存储桶中即可管理这些日志，并实施严格的安全控制、访问和职责分离。

在 AWS SRA 中，存储在 Amazon S3 中的主日志来自 CloudTrail，因此本节介绍如何保护这些对象。本指南也适用于由您自己的应用程序或其他应用程序创建的任何其他 S3 对象 AWS 服务。每当 Amazon S3 中有需要高度完整性、强有力的访问控制以及自动保留或销毁的数据时，都要应用这些模式。

默认情况下，上传到 S3 存储桶的所有新对象（包括 CloudTrail 日志）都使用亚马逊服务器端加密和 Amazon S3 托管的加密密钥 (SSE-S3) 进行加密。这有助于保护静态数据，但访问控制完全由 IAM 策略控制。要提供额外的托管安全层，您可以在所有安全 S3 存储桶上对您管理的 AWS KMS 密钥使用服务器端加密 (SSE-KMS)。这增加了第二级访问控制。要读取日志文件，用户必须同时拥有 Amazon S3 对 S3 对象的读取权限以及允许他们通过关联的密钥策略进行解密的 IAM 策略或角色。

有两个选项可帮助您保护或验证存储在 Amazon S3 中的 CloudTrail 日志对象的完整性。 CloudTrail 提供日志文件完整性验证，以确定日志文件在 CloudTrail 传送后是被修改还是被删除。另一个选项是 S3 对象锁定。

除了保护 S3 存储桶本身外，您还可以遵守日志服务（例如 CloudTrail）和日志存档账户的最低权限原则。例如，拥有 AWS 托管 IAM 策略授予权限的用户`AWSCloudTrail_FullAccess`可以禁用或重新配置其 AWS 账户中最敏感和最重要的审计功能。将此 IAM 策略的应用限制在尽可能少的个人身上。

使用侦探控件（例如由 AWS Config IAM Access Analyzer 提供的控制措施）来监控（并提醒和补救）这一更广泛的预防性控制集合，以防意外变化。

有关 S3 存储桶安全最佳实践的更深入讨论，请参阅 Amazon S3 文档、在线技术讲座和博客文章《保护 Amazon S3 中数据的十大安全最佳实践》。

实现示例

AWS SRA 代码库提供了 Amazon S3 封禁账户公开访问的实现示例。此模块阻止 Amazon S3 对 AWS 组织中所有现有和未来账户的公开访问。

Amazon Security Lake

AWS SRA 建议您使用日志存档账户作为 Amazon Security Lake 的委托管理员账户。当您执行此操作时，Security Lake 会使用与其他 SRA 推荐的安全日志相同的账户在专用 S3 存储桶中收集支持的日志。

为了保护日志和日志管理过程的可用性，Security Lake 的 S3 存储桶只能由 Security Lake 服务或由 Security Lake 为源或订阅者管理的 IAM 角色进行访问。除了使用预防性控制（例如分配访问权限最低的角色以及使用受控密 AWS KMS 钥加密日志）之外，还可以使用侦探控件，例如监控（并提醒和修复）这组权限 AWS Config 以防意外更改。

Security Lake 管理员可以在整个 AWS 组织中启用日志收集。这些日志存储在日志存档账户的区域 S3 存储桶中。此外，为了集中管理日志并便于存储和分析，Security Lake 管理员可以选择一个或多个汇总区域，整合和存储来自所有区域 S3 存储桶的日志。支持的 AWS 服务 日志会自动转换为名为开放网络安全架构框架 (OCSF) 的标准化开源架构，并以 Apache Parquet 格式保存在 Security Lake S3 存储桶中。在 OCSF 的支持下，Security Lake 可以高效地标准化和整合来自 AWS 和其他企业安全来源的安全数据，从而创建统一而可靠的安全相关信息存储库。

Security Lake 可以收集与 Amazon S3 和的 AWS CloudTrail 管理事件和 CloudTrail数据事件相关的日志 AWS Lambda。 要在 Security Lake 中收集 CloudTrail 管理事件，您必须至少有一个用于收集读取和写入 CloudTrail 管理事件的 CloudTrail 多区域组织跟踪。您必须为该跟踪启用日志记录。多区域跟踪将来自多个区域的日志文件传输到单个区域的单个 S3 存储桶。 AWS 账户如果区域位于不同的国家，请考虑数据导出要求以确定是否可以启用多区域跟踪。

AWS Security Hub CSPM 是 Security Lake 中受支持的原生数据源，你应该将 Security Hub CSPM 发现结果添加到安全湖。Security Hub CSPM 从许多不同的 AWS 服务 第三方集成中生成调查结果。这些发现可帮助您大致了解自己的合规态势，以及您是否遵循了安全建议 AWS 和 AWS Partner 解决方案。

要从日志和事件中获得可见性和可操作的见解，您可以使用 Amazon Athena 、Amazon Service OpenSearch 、 Amazon Quick 和第三方解决方案等工具查询数据。需要访问 Security Lake 日志数据的用户不应直接访问日志存档帐户。他们只能从安全工具帐户访问数据。或者，他们可以使用其他

AWS 账户 提供分析工具（例如 OpenSearch 服务、Quick）或第三方工具（例如安全信息和事件管理 (SIEM) 工具）的本地位置。要提供对数据的访问权限，管理员应在日志存档帐户中配置 Sec urity Lake 订阅者，并将需要访问数据的帐户配置为查询访问订阅者。有关更多信息，请参阅本指南安全 OU — 安全工具账户部分中的 Amazon Security Lak e。

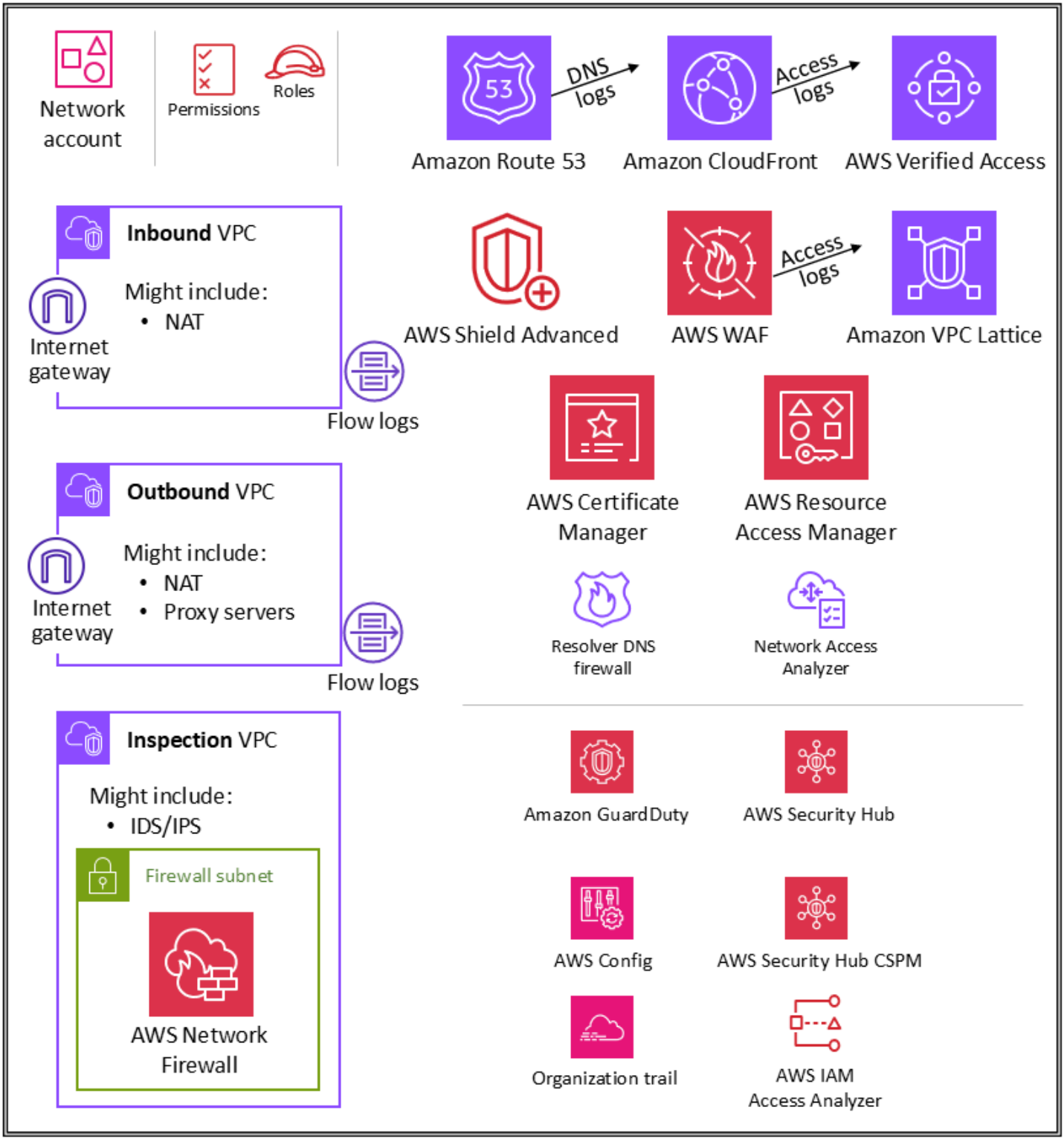
Security Lake 提供了 AWS 托管策略，可帮助您管理管理员对服务的访问权限。有关更多信息，请参阅 Sec urity Lake 用户指南。作为最佳实践，我们建议您通过开发管道限制 Security Lake 的配置，并防止通过 AWS 控制台或 AWS Command Line Interface (AWS CLI) 更改配置。此外，您应设置严格的 IAM 策略和服务控制策略 (SCPs)，以便仅提供管理 Security Lake 所需的权限。您可以配置通知以检测对这些 S3 存储桶的任何直接访问。

> **设计注意事项**
>
> 当你在 Security Lake 中启用 CloudTrail 管理事件时，它们会产生安全湖费用。在 Security Lake 中收集 CloudTrail 管理事件需要 CloudTrail 多区域组织跟踪，以收集读取和写入 CloudTrail 管理事件。您可以免费使用这条第一条路线。 CloudTrail 管理事件通常只占 CloudTrail 事件总数的一小部分（大约 5%）。这适用于在日志存档账户中使用 AWS Control Tower 或拥有集中 CloudTrail 日志的客户。

基础设施 OU – 网络账户

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

下图说明了在网络帐户中配置 AWS 的安全服务。



网络账户可管理应用程序与广泛的互联网之间的网关。保护这一双向接口十分重要。网络账户可将网络服务、配置和操作与各个应用程序工作负载、安全性及其他基础设施隔离开来。此方案不仅可限制连接、权限和数据流，而且还能为需要在这些账户中进行操作的团队分离职责和提供最低权限。通过将网

络流分成单独的入站和出站虚拟私有云 (VPCs)，您可以保护敏感基础设施和流量免受意外访问。一般认为入站网络风险较高，因而需要适当的路由、监控和潜在问题缓解措施。这些基础设施账户将继承组织管理账户和基础设施 OU 中的权限防护机制。网络（和安全）团队将管理此账户中的大部分基础设施。

网络架构

尽管网络设计和细节超出了本文档的范围，但我们建议使用以下三个选项来实现不同账户之间的网络连接：VPC 对等互连 AWS PrivateLink、和。 AWS Transit Gateway在这三个选项中进行选择时的重要考虑因素包括操作规范、预算以及具体带宽需求。

- VPC 对等互连-连接两者的最简单方法 VPCs 是使用 VPC 对等连接。连接可实现两者之间的完全双向连接。 VPCs VPCs 它们位于不同的账户中， AWS 区域 也可以互相监视。从规模上看，当你有数十到数百个对等连接时 VPCs，将它们与对等互连互连会形成一个由数百到数千个对等连接组成的网格，这可能很难管理和扩展。当一个 VPC 中的资源必须与另一个 VPC 中的资源通信，两 VPCs 者的环境都受到控制和保护，并且 VPCs 要连接的数量少于 10（以便对每个连接进行单独管理）时，最好使用 VPC 对等连接。
- AWS PrivateLink– 在服务和应用程序之间 PrivateLink VPCs提供私有连接。您可以在 VPC 中创建自己的应用程序，并将其配置为 PrivateLink由支持的服务（称为终端节点服务）。其他 AWS 委托人可以使用接口 VPC 终端节点或 Gateway Load Balancer 终端节点创建从其 VPC 到您的终端节点服务的连接，具体取决于服务类型。使用时 PrivateLink，服务流量不会通过可公开路由的网络。PrivateLink 在您的客户端-服务器设置中，要向一个或多个使用者提供对服务提供商 VPC 中特定服务或一组实例的 VPCs 单向访问权限时使用。当两 VPCs 者中的客户端和服务器的 IP 地址重叠时，这也是一个不错的选择，因为在客户端 VPC 中 PrivateLink 使用弹性网络接口，因此不会与服务提供商发生 IP 冲突。
- AWS Transit Gateway¿Transit Gateway 提供了一种连接 VPCs 和本地网络的 hub-and-spoke设计，作为一项完全托管的服务，无需您配置虚拟设备。 AWS 管理高可用性和可扩展性。公交网关是一种区域资源，可以连接同一个区域 VPCs 内的数千个 AWS 区域。您可以将混合连接（VPN 和 AWS Direct Connect 连接）连接到单个传输网关，从而将 AWS 组织的整个路由配置整合到一个地方，并对其进行控制。中转网关解决了大规模创建和管理多个 VPC 对等连接所带来的复杂性。它是大多数网络架构的默认设置，但如果在成本、带宽和延迟方面有特定的需求，则 VPC 对等可能更适合您。

入站（入口）VPC

入站 VPC 旨在接受、检查和路由从应用程序外部启动的网络连接。根据应用程序的具体情况，您可能会在此 VPC 中看到一些网络地址转换（NAT）。来自此 VPC 的流日志将被捕获并存储在日志存档账户中。

出站（出口）VPC

出站 VPC 旨在处理应用程序内部发起的网络连接。根据应用程序的具体情况，您可以期望在此 VPC 中看到 NAT 流量、 AWS 服务特定的 VPC 终端节点以及外部 API 终端节点的托管。来自此 VPC 的流日志将被捕获并存储在日志存档账户中。

检查 VPC

专用的检查 VPC 为管理 VPCs（相同或不同 AWS 区域）、互联网和本地网络之间的检查提供了一种简化的集中方法。对于 AWS SRA，请确保两者之间的所有流量都 VPCs 通过检查 VPC，并避免将检查 VPC 用于任何其他工作负载。

AWS Network Firewall

AWS Network Firewall是一项适用于您的 VPC 的高可用性托管网络防火墙服务。它使您能够毫不费力地部署和管理状态检查、入侵防御和检测以及 Web 过滤，以帮助保护您的虚拟网络。 AWS您可以使用 Network Firewall 来解密 TLS 会话并检查入站和出站流量。有关配置 Network Firewall 的更多信息，请参阅《AWS Network Firewall VPC 中的新增防火墙托管服务》博客文章。

您可以在 VPC 中按可用区使用防火墙。对于每个可用区，您可以选择一个子网来托管筛选流量的防火墙端点。一个可用区中的防火墙端点可以保护该区内除其所在子网外的所有其他子网。根据应用场景和部署模型，防火墙子网可能是公有子网，也可能是私有子网。防火墙对流量完全透明，并且不执行网络地址转换（NAT）。它会保留源地址和目标地址。在此参考架构中，防火墙端点托管在检查 VPC 中。从入站 VPC 流向出站 VPC 的所有流量都将经由此防火墙子网进行路由，以便进行检查。

Network Firewall 通过亚马逊 CloudWatch 指标实时显示防火墙活动，并通过向亚马逊简单存储服务 (Amazon S3) 和 Amazon D CloudWatch ata Firehose 发送日志来提高网络流量的可见性。Network Firewall 可与您的现有安全方法（包括合作伙伴提供的AWS 技术）互操作。您还可以导入现有的 Suricata 规则集，这些规则集可以是内部编写的，也可以是从第三方供应商或开源平台外部获取而来。

在 AWS SRA 中，网络帐户中使用 Network Firewall，因为该服务以网络控制为重点的功能与账户的意图一致。

设计注意事项

- AWS Firewall Manager 支持 Network Firewall，因此您可以在整个组织中集中配置和部署网络防火墙规则。（有关详细信息，请参阅 AWS 文档中的在 Firewall Manager 中使用 AWS Network Firewall 策略。）配置 Firewall Manager 时，它会自动创建一个防火墙，其中 VPCs 包含您指定的帐户中的规则集。它还会在包含公有子网的每个可用区的专用子网中部署端点。同时，对集中配置的规则集所做的任何更改都会自动在已部署的 Network Firewall 防火墙的下游更新。
- Network Firewall 有多种部署模型可供选择。模型是否合适取决于您的应用场景和要求。示例包括：
  - 一种分布式部署模型，其中将 Network Firewall 部署到个人中 VPCs。
  - 集中式部署模型，其中将 Network Firewall 部署到集中式 VPC 中，用于东-西（VPC 到 VPC）流量或南-北（互联网出口和入口、本地）流量。
  - 组合式部署模型，其中将 Network Firewall 部署到集中式 VPC 中，用于东-西流量和部分南-北流量。
- 作为最佳实践，请勿使用 Network Firewall 子网部署任何其他服务。这是因为 Network Firewall 无法检查来自防火墙子网内源或目标的流量。

网络访问分析器

网络访问分析器是 Amazon VPC 的一项功能，可识别对资源的意外网络访问。您可以使用网络访问分析器来验证网络分段、识别可从互联网访问或只能从可信 IP 地址范围访问的资源，并验证是否所有网络路径上都存在适当的网络控制。

Network Access Analyzer 使用自动推理算法来分析数据包在网络中的资源之间可以走的 AWS 网络路径，并生成与您定义的网络访问范围相匹配的路径的结果。网络访问分析器对网络配置执行静态分析，这意味着在此分析过程中，不会在网络中传输任何数据包。

Amazon Inspector 网络可到达性规则提供了相关功能。这些规则生成的调查发现将在应用程序账户中使用。Network Access Analyzer 和 Network Reachability 都使用AWS 可证明安全计划中的最新技术，他们将这项技术应用于不同的关注领域。Network Reachability 软件包特别关注 EC2 实例及其互联网可访问性。

网络帐户定义了控制进出您 AWS 环境的流量的关键网络基础架构。这些流量需要加以严格监控。在 AWS SRA 中，Network Access Analyzer 用于帮助识别意外的网络访问，识别通过互联网网关访问互

联网的资源，并验证资源和互联网网关之间的所有网络路径上是否存在适当的网络控制，例如网络防火墙和 NAT 网关。

> 设计注意事项
>
> 网络访问分析器是 Amazon VPC 的一项功能，它可以在任何 AWS 账户 拥有 VPC 的企业中使用。网络管理员可以获得范围严格的跨账户 IAM 角色，以验证每个角色中是否强制使用经批准的网络路径。 AWS 账户

AWS RAM

AWS Resource Access Manager(AWS RAM) 可帮助您安全地将您在一个 AWS 资源中创建的资源 AWS 账户 与其他资源共享 AWS 账户。AWS RAM 为管理资源共享和标准化跨账户的这种体验提供了一个中心位置。这样可以在利用管理和计费隔离的同时更轻松地管理资源，并缩小多账户策略造成的影响控制优势的范围。如果您的账户由管理 AWS Organizations，则 AWS RAM 允许您与组织中的所有账户共享资源，或者仅与一个或多个指定组织单位内的账户共享资源（OUs）。无论该账户是否属于某个组织，您都可以 AWS 账户 按账户 ID 与其共享。您还可以与指定的 IAM 角色和用户共享某些支持的资源类型。

AWS RAM 允许您共享不支持基于 IAM 资源的策略的资源，例如 VPC 子网和 Route 53 规则。此外，通过使用 AWS RAM，资源的所有者可以看到哪些委托人有权访问他们共享的单个资源。IAM 委托人可以直接检索与他们共享的资源列表，但他们无法使用由 IAM 资源策略共享的资源执行此操作。 如果 AWS RAM 用于在 AWS 组织外部共享资源，则会启动邀请流程。在授予对资源的访问权限之前，收件人必须接受邀请。 这提供了额外的制衡措施。

AWS RAM 由资源所有者在部署共享资源的账户中调用和管理。 AWS SRA 中 AWS RAM 说明的一个常见用例是网络管理员与整个 AWS 组织共享 VPC 子网和传输网关。这提供了分离功能 AWS 账户 和网络管理功能，并有助于实现职责分离。有关 VPC 共享的更多信息，请参阅 AWS 博客文章 VPC 共享：多账户和 VPC 管理的新方法以及AWS 网络基础设施白皮书。

> 设计注意事项
>
> 尽管 AWS RAM 作为一项服务仅部署在 AWS SRA 的网络帐户中，但它通常会部署在多个账户中。例如，您可以将数据湖管理集中到单个数据湖账户，然后与 AWS 组织中的其他账户共享 AWS Lake Formation 数据目录资源（数据库和表）。有关更多信息，请参阅AWS Lake Formation 文档和 AWS 博客文章跨 AWS 账户 使用安全地共享您的数据 AWS Lake Formation。 此外，安全管理员在构建 AWS 私有证书颁发机构 层次结构时可以 AWS RAM 用

来遵循最佳实践。 CAs 可以与外部第三方共享，这些第三方无需访问 CA 层次结构即可颁发证书。这将允许发起组织限制和撤销第三方访问。

AWS Verified Access

AWS Verified Access无需使用 VPN 即可安全访问企业应用程序和资源。它可以根据预定义的要求实时评估每个访问请求，从而改善安全状况并帮助应用零信任访问权限。您可以根据身份数据和设备状态，为每个应用程序定义唯一的访问策略。Verified Access 为 Git 存储库、数据库和实例组等应用程序提供通过 TCP、SSH 和 RDP 协议安全访问 HTTP (S) 应用程序（例如基于浏览器的应用程序）和非 HTTP (S) 应用程序。 EC2 可以使用命令行终端或桌面应用程序访问它们。Verified Access 还可以帮助管理员高效地设置和监控访问策略，从而简化安全操作。这有助于腾出时间来更新政策、响应安全和连接事件以及审核合规性标准。Verified Access 还支持与集成， AWS WAF 以帮助您过滤掉常见的威胁，例如 SQL 注入和跨站脚本 (XSS)。Verified Access 与无缝集成 AWS IAM Identity Center，允许用户使用基于 SAML 的第三方身份提供商进行身份验证（ ）IdPs。如果您已拥有与 OpenID Connect（OIDC）兼容的自定义 IdP 解决方案，则 Verified Access 还可通过直接与 IdP 连接来对用户进行身份验证。Verified Access 会记录每次访问尝试，以便您可以快速响应安全事件及审核请求。Verified Access 支持将这些日志传送到亚马逊简单存储服务 (Amazon S3)、亚马逊日志和 CloudWatch 亚马逊数据 Firehose。

Verified Access 支持两种常见的企业应用程序模式：内部应用程序模式和面向互联网的应用程序模式。Verified Access 使用应用程序负载均衡器或弹性网络接口与应用程序集成。如果您使用的是 Application Load Balancer，则验证访问需要内部负载均衡器。由于 Verified AWS WAF Access 支持实例级别，因此与 Application Load Balancer AWS WAF 集成的现有应用程序可以将策略从负载均衡器移至已验证访问实例。企业应用程序表示为 Verified Access 端点。每个端点都与一个 Verified Access 组相关联，并继承该组的访问策略。Verified Access 组是 Verified Access 端点和组级别 Verified Access 策略的集合。组简化了策略管理，让 IT 管理员可以设置基准标准。应用程序所有者可以根据应用程序的敏感度进一步定义精细的策略。

在 AWS SRA 中，已验证访问权限托管在网络账户中。中心 IT 团队设置集中管理的配置。例如，他们可能会连接身份提供者（例如 Okta）和设备信任提供商（例如 Jamf）等信任提供商，创建组并确定组级别策略。然后，可以使用与数十、数百或数千个工作负载帐户共享这些配置 AWS RAM。这使应用程序团队能够管理管理其应用程序的底层端点，而无需其他团队的开销。 AWS RAM 为托管在不同工作负载帐户中的公司应用程序提供了一种可扩展的方式，可以利用已验证的访问权限。

设计注意事项

您可以对具有类似安全要求的应用程序的端点进行分组，以简化策略管理，然后与应用程序账户共享该组。该组中的所有应用程序均共享组策略。如果组中某个应用程序因边缘情况需要特定策略，您可以为该应用程序应用应用程序级别的策略。

Amazon VPC Lattice

Amazon VPC Lattice 是一项用于连接、监控和保护 service-to-service通信的应用程序联网服务。 服务通常称为微服务，是一种可独立部署的软件单元，用于交付特定任务。VPC Lattice 可自动管理跨 VPCs 服务之间的网络连接和应用层路由， AWS 账户 无需您管理底层网络连接、前端负载均衡器或 sidecar 代理。它提供了完全托管的应用程序层代理，可根据路径和标头等请求特征提供应用程序级别的路由。VPC Lattice 内置于 VPC 基础设施中，因此它为各种计算类型提供了一种一致的方法，例如亚马逊弹性计算云 (Amazon EC2)、Amazon Elastic Kubernetes Service (Amazon EKS) 和。 AWS Lambda VPC Lattice 还支持加权路由 blue/green 和金丝雀式部署。您可以使用 VPC Lattice 创建具有逻辑边界的服务网络，该网络可自动实现服务发现和连接。VPC Lattice 与 IAM 集成，可使用 service-to-service身份验证策略进行身份验证和授权。

VPC Lattice 与 AWS RAM VPC 集成，可实现服务和服务网络的共享。 AWS SRA描绘了一种分布式架构，开发人员或服务所有者在其应用程序账户中创建VPC Lattice服务。服务所有者可定义侦听器、路由规则和目标组以及身份验证策略。然后，他们可与其他账户共享服务，并将这些服务与 VPC Lattice 服务网络关联。这些网络由网络管理员在网络账户中创建，并与应用程序账户共享。网络管理员配置服务网络级别的身份验证策略和监控。管理员将 VPCs VPC 莱迪思服务与一个或多个服务网络相关联。有关此分布式架构的详细演练，请参阅 AWS 博客文章使用 Amazon VPC Lattice 为您的应用程序构建安全的多账户多 VPC 连接

设计注意事项

- 根据贵组织的服务运营模式或服务网络可见性，网络管理员可以共享他们的服务网络，并可以让服务所有者控制其服务以及 VPCs与这些服务网络的关联。或者，服务所有者可以共享其服务，并且网络管理员可以将服务与服务网络关联。
- 仅当客户端位于与同一服务网络关联的 VPC 中时，客户端才可以向与该服务网络关联的服务发送请求。遍历 VPC 对等连接或中转网关的客户端流量会被拒绝。

边缘安全

边缘安全通常需要三种类型的保护：安全内容交付、网络和应用层保护以及分布式拒绝服务DDo缓解。数据、视频、应用程序等内容 APIs 必须快速、安全地交付，使用推荐版本的 TLS 来加密端点之间的通信。内容还应通过签名 URLs、签名 Cookie 和令牌身份验证进行访问限制。应用程序级别安全性应设计为控制机器人流量，阻止 SQL 注入或跨站脚本攻击（XSS）等常见攻击模式，并提供 Web 流量可见性。在边缘， DDoS 缓解提供了重要的防御层，可确保关键任务业务运营和服务的持续可用性。APIs 应保护应用程序和免受 SYN 洪水、UDP 洪水或其他反射攻击，并具有内联缓解措施以阻止基本的网络层攻击。

AWS 提供多种服务，帮助提供从核心云到 AWS 网络边缘的安全环境。亚马逊 CloudFront、 AWS Certificate Manager (ACM)、 AWS Shield AWS WAF、和 Amazon Route 53 携手合作，帮助创建灵活的分层安全边界。使用 CloudFront、 APIs、内容或应用程序可以通过 HTTPS 传送，方法是使用 TLSv1 .3 来加密和保护查看者客户端与之间的通信 CloudFront。您可以使用 ACM 创建自定义 SSL 证书并将其免费部署到 CloudFront 发行版中。ACM 会自动处理证书续订。Shield 是一项托管 DDo S 保护服务，可帮助保护在其上运行的应用程序 AWS。它提供动态检测和自动内联缓解措施，可最大限度地减少应用程序停机时间和延迟。 AWS WAF 允许您创建规则，根据特定条件（IP 地址、HTTP 标头和正文或自定义 URIs）、常见 Web 攻击和普遍存在的机器人来过滤 Web 流量。Route 53 是一种可用性高、可扩展性强的 DNS Web 服务。Route 53 将用户请求连接到本地 AWS 或本地运行的互联网应用程序。 AWS SRA 采用集中式网络入口架构 AWS Transit Gateway，使用托管在网络账户中，因此边缘安全基础设施也集中在该账户中。

Amazon CloudFront

Amazon CloudFront 是一个安全的内容分发网络 (CDN)，可针对公共网络层和传输 DDo S 尝试提供固有的保护。您可以使用 TLS 证书交付内容或应用程序，并且会自动启用高级 TLS 功能。 APIs您可以使用 AWS Certificate Manager (ACM) 创建自定义 TLS 证书，并在查看者和之间强制执行 HTTPS 通信 CloudFront，如后面的 ACM 部分所述。此外，您还可以要求与您的自定义源 CloudFront 之间的通信在传输过程中实现 end-to-end加密。对于这种情况，您必须在原始服务器上安装 TLS 证书。如果源是弹性负载均衡器，则可使用由 ACM 生成的证书或由第三方证书颁发机构（CA）验证并导入到 ACM 中的证书。如果 S3 存储桶网站终端节点用作来源 CloudFront，则无法配置 CloudFront 为在源端节点中使用 HTTPS，因为 Amazon S3 不支持网站终端节点的 HTTPS。（但是，您仍然可以要求在查看者和之间使用 HTTPS CloudFront。）对于支持安装 HTTPS 证书的所有其他源，您必须使用由可信第三方 CA 签名的证书。

CloudFront 提供了多种选项来保护和限制对您的内容的访问。例如，它可以通过使用签名 URLs 和签名的 Cookie 来限制对您的 Amazon S3 来源的访问。有关更多信息，请参阅 CloudFront文档中的配置安全访问和限制对内容的访问。

AWS SRA 说明了网络账户中的集中式 CloudFront 分布，因为它们与使用 AWS Transit Gateway实现的集中式网络模式一致。通过在网络账户中部署和管理 CloudFront 分配，您可以从集中控制中受益。您可以在一个地方管理所有 CloudFront 分配，这样可以更轻松地控制访问权限、配置设置和监控所有账户的使用情况。此外，您还可以从一个集中式账户管理 ACM 证书、DNS 记录和 CloudFront 日志记录。

CloudFront 安全控制面板可直接在您的 CloudFront 分发中提供 AWS WAF 可见性和控制。您可以了解应用程序的主要安全趋势、允许和阻止的流量以及机器人活动。您可以使用调查工具（例如可视化日志分析器和内置屏蔽控件）来隔离流量模式并屏蔽流量，无需查询日志或编写安全规则。

设计注意事项

- 或者，您可以在应用程序帐户中 CloudFront 作为应用程序的一部分进行部署。在这种情况下，应用程序团队会做出决策，例如如何部署 CloudFront 发行版，确定适当的缓存策略，并负责 CloudFront 分发的治理、审计和监控。通过在多个账户之间 CloudFront 分配分配，您可以从额外的服务配额中受益。另一个好处是，您可以使用 CloudFront固有的自动源访问身份 (OAI) 和源站访问控制 (OAC) 配置来限制对 Amazon S3 来源的访问。
- 当您通过诸如的 CDN 交付网页内容时 CloudFront，必须防止观看者绕过 CDN 直接访问您的原始内容。要实现此源访问限制，在将请求转发 AWS WAF 到自定义源之前，您可以使用和添加自定义标头并验证标头。 CloudFront 有关此解决方案的详细说明，请参阅 AWS 安全博客文章如何使用 AWS WAF 和增强 Amazon O CloudFront rigin 安全 AWS Secrets Manager。另一种方法是仅限制与 Application Load Balancer 关联的安全组中的 CloudFront 前缀列表。这将有助于确保只有 CloudFront 分配才能访问负载均衡器。

AWS WAF

AWS WAF是一种 Web 应用程序防火墙，可帮助保护您的 Web 应用程序免受 Web 漏洞的侵害，例如可能影响应用程序可用性、危及安全性或消耗过多资源的常见漏洞和机器人。 它可以与亚马逊 CloudFront 发行版、亚马逊 API Gateway REST API、应用程序负载均衡器、 AWS AppSync GraphQL API、Amazon Cognito 用户池和服务集成。 AWS App Runner

AWS WAF 使用 Web 访问控制列表 (ACLs) 来保护一组 AWS 资源。Web ACL 是一组规则，用于定义检查标准，以及在 Web 请求满足标准时要采取的相关操作（阻止、允许、计数或运行机器人控制）。AWS WAF 提供了一组托管规则，可针对常见的应用程序漏洞提供保护。这些规则由和 AWS 合作伙伴策划 AWS 和管理。 AWS WAF 还为创作自定义规则提供了强大的规则语言。您可以使用自定义规则

来编写符合特定需求的检查标准。示例包括 IP 限制、地理限制，以及更适合特定应用程序行为的托管规则的自定义版本。

AWS WAF 为常见和有针对性的机器人程序和账户接管保护 (ATP) 提供了一套智能分层管理规则。如果使用机器人控制功能和 ATP 规则组，需要支付订阅费和流量检查费。因此，我们建议您首先监控流量，然后再决定要使用的对象。您可以使用 AWS WAF 控制台上免费提供的机器人管理和账户接管仪表板来监控这些活动，然后决定是否需要智能等级 AWS WAF 规则组。

在 AWS SRA CloudFront 中 AWS WAF ，与网络账户集成。在此配置中， AWS WAF 规则处理发生在边缘位置，而不是 VPC 内。这可以筛选更靠近请求内容的最终用户的恶意流量，并有助于限制恶意流量进入您的核心网络。

通过配置对 S3 存储桶的跨账户访问权限，您可以将完整 AWS WAF 日志发送到日志存档账户中的 S3 存储桶。有关更多信息，请参阅有关此主题的 AWS re: Post 文章。

设计注意事项

- 作为在网络帐户中 AWS WAF 集中部署的替代方案，在应用程序帐户 AWS WAF 中进行部署可以更好地满足某些用例。例如，当您在应用程序账户中部署 CloudFront分配或拥有面向公众的应用程序负载均衡器时，或者如果您在 Web 应用程序前面使用 API Gateway，则可以选择此选项。如果您决定 AWS WAF 在每个应用程序账户中进行部署，请使用 AWS Firewall Manager 集中式 Security Tools 账户管理这些账户中的 AWS WAF 规则。
- 您还可以在 CloudFront 层中添加一般 AWS WAF 规则，并在区域资源（例如 Application Load Balancer 或 API 网关）上添加其他特定于应用程序的 AWS WAF 规则。

AWS Shield

AWS Shield是一项托管 DDo S 保护服务，用于保护在其上运行的应用程序 AWS。盾牌有两个等级：Shield Standard和Shield Advanced。Shield Standard 为所有 AWS 客户提供针对最常见基础设施（第 3 层和第 4 层）事件的保护，无需额外付费。Shield Advanced 为针对受保护的亚马逊 EC2、Elastic Load Balancing（Elastic Load Balancing）和 Route 53 托管区域上的应用程序的未经授权的事件提供了更复杂的自动缓解措施。 CloudFront AWS Global Accelerator如果您拥有高知名度的网站或容易受到频繁的 DDo S 攻击，则可以考虑 Shield Advanced 提供的其他功能。

您可以使用 Shield Advanced 自动应用层 DDo S 缓解功能将 Shield Advanced 配置为自动响应，以缓解针对受保护 CloudFront 分配、弹性负载平衡（弹性负载平衡）负载均衡器（应用程序、网络和经典）、Amazon Route 53 托管区域、亚马逊 EC2 弹性 IP 地址和 AWS Global Accelerator 标准加速器

的应用程序层（第 7 层）攻击。启用此功能后，Shield Advanced 会自动生成自定义 AWS WAF 规则来缓解 DDo S 攻击。Shield Advanced 还允许你访问AWS Shield 响应小组 (SRT)。您可以随时联系 SRT，为您的应用程序创建和管理自定义缓解措施，也可以在主 DDo动 S 攻击期间创建和管理自定义缓解措施。如果您希望 SRT 主动监控您受保护的资源并在尝试 DDo S 时与您联系，请考虑启用主动参与功能。

设计注意事项

- 如果应用程序账户中有面向互联网的资源（例如应用程序负载均衡器或网络负载均衡器）前置的工作负载 CloudFront，请在应用程序账户中配置 Shield Advanced，然后将这些资源添加到 Shield 保护中。您可以使用 AWS Firewall Manager 大规模配置这些选项。
- 如果您的数据流中有多个资源，例如在 Application Load Balancer 前面的 CloudFront分配，请仅使用入口点资源作为受保护的资源。这样可以确保您不会为两个资源支付两次 Shield 数据传出（DTO）费用。
- Shield Advanced 记录了您可以在亚马逊中监控的指标 CloudWatch。（有关更多信息，请参阅 AWS 文档 CloudWatch中的使用 Amazon 进行监控。）设置 CloudWatch 警报，以便在检测到 S 事件时向您的安全中心接收 SN DDo S 通知。在可疑的 DDo S 事件中，请通过提交支持AWS 请求并将其分配为最高优先级来联系 Enterpris e Support 团队。处理该事件时，Enterprise Support 团队会涉及 Shield Response Team（SRT）。此外，您可以预先配置 AWS Shield 互动 Lambda 函数，以创建支持请求并向 SRT 团队发送电子邮件。

AWS Certificate Manager (ACM)

AWS Certificate Manager(ACM) 允许您预置、管理和部署公有和私有 TLS 证书，以便 AWS 服务 与内部连接的资源一起使用。使用 ACM，您可以快速申请证书，将其部署在 ACM 集成的 AWS 资源上，例如 Elastic Load Balancing 负载均衡器、 CloudFront 分配和 Amazon API APIs Gateway 上，然后让 ACM 处理证书续订。 申请 ACM 公共证书时，无需生成密钥对或证书签名请求 (CSR)，无需向证书颁发机构 (CA) 提交 CSR，也无需在收到证书后上传并安装证书。ACM 还提供了导入第三方 CAs 颁发的 TLS 证书并将其与 ACM 集成服务一起部署的选项。当您使用 ACM 管理证书时，使用强大的加密和密钥管理最佳实践，可以安全地保护和存储证书私钥。借助 ACM，预置公有证书无需额外付费，并且 ACM 负责管理续订流程。

ACM 在网络账户中用于生成公共 TLS 证书，而 CloudFront 分发又使用该证书在查看者和 CloudFront 之间建立 HTTPS 连接。有关详情，请参阅 CloudFront 文档。

设计注意事项

对于面向外部的证书，ACM 必须与为其预置证书的资源位于同一个账户中。证书无法在账户之间共享。

Amazon Route 53

Amazon Route 53 是一种可用性高、可扩展性强的 DNS Web 服务。您可以使用 Route 53 执行三个主要功能：域注册、DNS 路由和运行状况检查。

您可以使用 Route 53 作为 DNS 服务，将域名映射到您的 EC2 实例、S3 存储桶、 CloudFront 分配和其他 AWS 资源。 AWS DNS 服务器的分布式特性有助于确保您的最终用户始终如一地路由到您的应用程序。 Route 53 流量和路由控制等功能可帮助您提高可靠性。如果主应用程序端点不可用，则可将失效转移配置为将用户重新路由到其他位置。Route 53 解析器通过 AWS Direct Connect 或 AWS 托管 VPN 为您的 VPC 和本地网络提供递归 DNS。

通过将 IAM 服务与 Route 53 配合使用，您可以精细地控制谁可以更新您的 DNS 数据。您可以启用 DNS 安全扩展（DNSSEC）签名，让 DNS 解析器验证 DNS 响应是否来自 Route 53 且未被篡改。

R@@ oute 53 解析器 DNS 防火墙为来自您的 VPCs出站 DNS 请求提供保护。这些请求通过 Route 53 Resolver 进行域名解析。DNS Firewall 保护的主要用途是帮助防止数据的 DNS 泄露。使用 DNS Firewall，您可以监控和控制应用程序可以查询的域。您可以拒绝对已知不良域的访问，并允许所有其他查询通过。或者，您可以拒绝对除明确信任的域之外的所有域的访问。您还可以使用 DNS Firewall 阻止在私有托管区（共享或本地）中对 VPC 端点名称等资源的解析请求。它还可以阻止对公共或私有 EC2 实例名称的请求。

默认情况下，Route 53 解析器作为每个 VPC 的一部分创建。在 AWS SRA 中，在网络帐户中使用 Route 53 主要用于 DNS 防火墙功能。

设计注意事项

DNS 防火墙和 AWS Network Firewall 两者都提供域名过滤，但针对的流量类型不同。您可以同时使用 DNS Firewall 和 Network Firewall，为通过两个不同网络路径的应用层流量配置基于域的过滤：

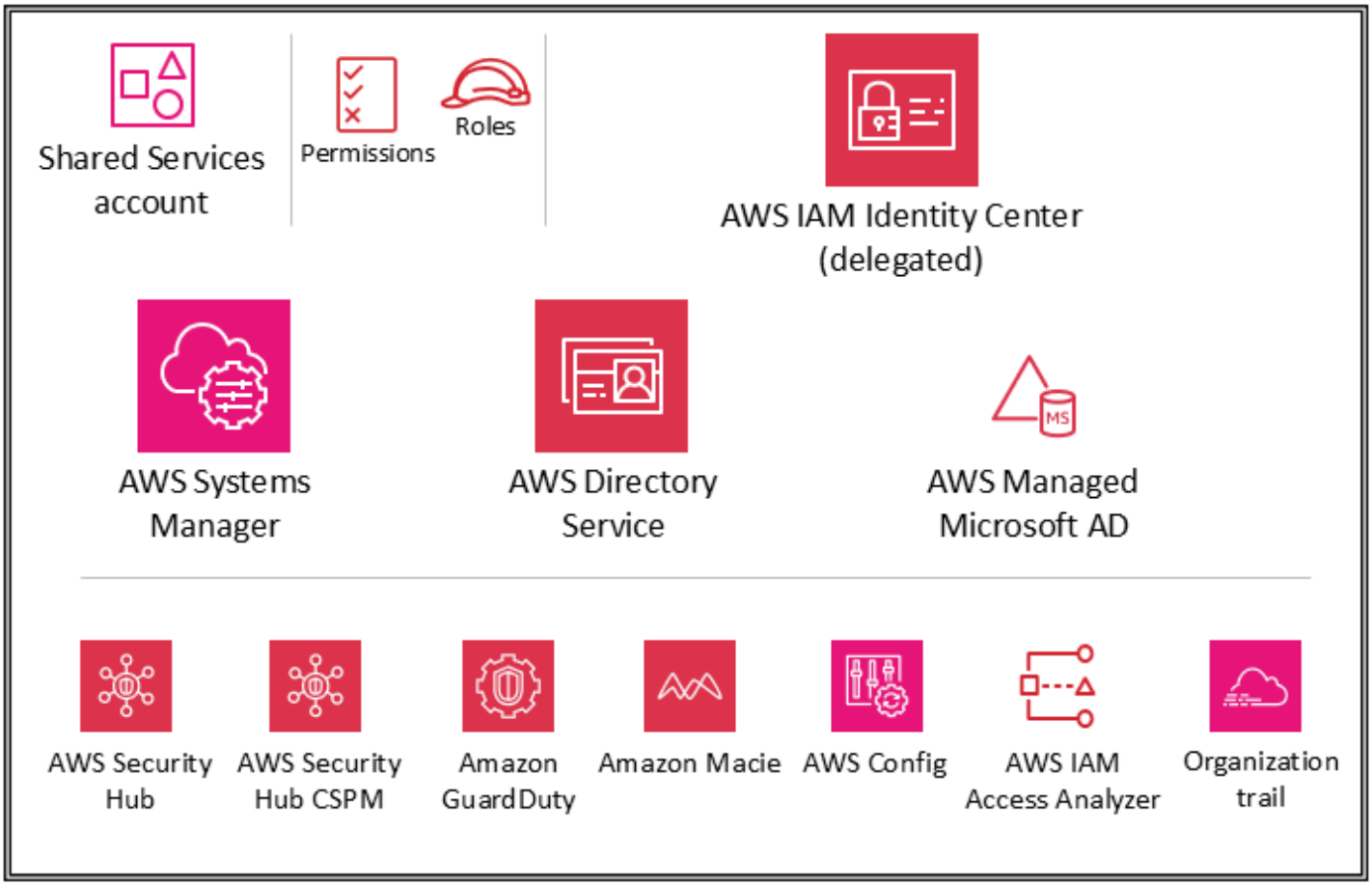
- DNS Firewall 可过滤来自您 VPCs内部应用程序通过 Route 53 解析器的出站 DNS 查询。您还可以将 DNS Firewall 配置为向阻止的域名发送查询的自定义响应。

- Network Firewall 为网络层和应用程序层流量提供筛选，但无法查看 Route 53 Resolver 所做的查询。

基础架构 OU — 共享服务账户

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

下图说明了在共享服务帐户中配置 AWS 的安全服务。



共享服务账户是基础设施 OU 的一部分，其目的是支持多个应用程序和团队用来交付成果的服务。例如，目录服务（Active Directory）、邮件服务和元数据服务属于此类别。 AWS SRA 重点介绍了支持安全控制的共享服务。尽管网络帐户也是基础架构 OU 的一部分，但为了支持职责分离，它们已从共享服务帐户中删除。管理这些服务的团队不需要网络账户的权限或访问权限。

AWS Systems Manager

AWS Systems Manager（也包含在组织管理账户和应用程序账户中）提供了一系列功能，可让您查看和控制您的 AWS 资源。其中一项功能是 Systems Manager Explorer，它是一个可自定义的操作控制面板，用于报告有关您的 AWS 资源的信息。您可以使用 AWS Organizations 和 Systems Manager Explorer 同步 AWS 组织中所有账户的操作数据。Systems Manager 通过中的委托管理员功能部署到共享服务帐户中 AWS Organizations。

Systems Manager 通过扫描您的托管实例并报告（或采取纠正措施）它检测到的任何违反策略的情况来帮助您努力维护安全与合规性。通过将 Systems Manager 与单个成员 AWS 账户（例如应用程序帐户）中的相应部署配对，您可以协调实例清单数据收集并集中自动化，例如修补和安全更新。

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory，也称为 AWS Managed Microsoft AD，使您的目录感知工作负载和 AWS 资源能够在上使用托管 Active Directory。 AWS您可以使用 AWS Managed Microsoft AD 将 EC2 适用于 Windows Server 的亚马逊、适用 EC2 于 Linux 的亚马逊和 Amazon RDS for SQL Server 实例加入您的域，并与 Active Directory 用户和群组一起使用AWS 最终用户计算 (EUC) 服务 WorkSpaces，例如亚马逊。

AWS Managed Microsoft AD 可帮助您将现有 Active Directory 扩展到云资源， AWS 并使用现有的本地用户凭据访问云资源。您还可以管理本地用户、群组、应用程序和系统，而无需复杂地运行和维护本地、高度可用的 Active Directory。您可以将现有的计算机、笔记本电脑和打印机加入 AWS Managed Microsoft AD 域中。

AWS Managed Microsoft AD 基于 Microsoft Active Directory 构建，不需要你将现有 Active Directory 中的数据同步或复制到云端。您可以使用熟悉的 Active Directory 管理工具和功能，例如组策略对象 (GPOs)、域信任、精细密码策略、组托管服务帐户 (gMSAs)、架构扩展和基于 Kerberos 的单点登录。您还可以使用 Active Directory 安全组委派管理任务和授权访问权限。

多区域复制使您能够跨多个 AWS 区域区域部署和使用单个 AWS Managed Microsoft AD 目录。这使你能够更轻松、更具成本效益地在全球部署和管理微软 Windows 和 Linux 工作负载。当您使用自动多区域复制功能时，您可以获得更高的弹性，而您的应用程序则使用本地目录来实现最佳性能。

AWS Managed Microsoft AD 在客户端和服务器角色中都支持通过 SSL/TLS（也称为 LDAPS）的轻型目录访问协议 (LDAP)。充当服务器时， AWS Managed Microsoft AD 支持通过端口 636 (SSL) 和 389 (TLS) 进行的 LDAPS。您可以通过在 AWS Managed Microsoft AD 域控制器上安装来自 AWS基于 Active Directory 证书服务 (AD CS) 的证书颁发机构 (CA) 的证书来启用服务器端 LDAPS 通信。充当客户端时， AWS Managed Microsoft AD 支持通过端口 636 (SSL) 进行的 LDAPS。您可以通过

将服务器证书颁发者的 CA 证书注册到中来启用客户端 LDAPS 通信 AWS，然后在您的目录中启用 LDAPS。

在 AWS SRA 中，在共享服务账户中用于 Directory Service 为多个成员账户中支持 Microsoft 的工作负载提供域服务。 AWS

> 设计注意事项
>
> 您可以使用 IAM 身份中心 AWS 管理控制台 并选择 AWS Managed Microsoft AD 作为身份源，向本地 Active Directory 用户授予使用其现有的 Active Directory 证书登录和 AWS Command Line Interface (AWS CLI) 的访问权限。这样，您的用户就可以在登录时扮演分配给他们的角色之一，并根据为该角色定义的权限访问资源并对其执行操作。另一种选择是使用让您的用户 AWS Managed Microsoft AD 能够担任 IAM 角色。

IAM Identity Center

AWS SRA 使用支持的 AWS IAM Identity Center 委托管理员功能将 IAM 身份中心的大部分管理委托给共享服务账户。这有助于限制需要访问组织管理账户的用户数量。仍需要在组织管理账户中启用 IAM Identity Center 才能执行某些任务，包括管理在组织管理账户中配置的权限集。

使用共享服务账户作为 IAM 身份中心的委派管理员的主要原因是 Active Directory 位置。如果您计划使用 Active Directory 作为 IAM Identity Center 身份中心身份源，则需要在已指定为 IAM Identity Center 委托管理员账户的成员账户中找到该目录。在 AWS SRA 中，共享服务账户托管 AWS Managed Microsoft AD，因此该账户成为 IAM Identity Center 的委托管理员。

IAM Identity Center 支持将单个成员账户同时注册为委托管理员。只有使用管理账户的凭据登录后，才能注册成员账户。要启用委托，您必须考虑 IAM 身份中心文档中列出的先决条件。委派的管理员账户可以执行大多数 IAM Identity Center 管理任务，但有一些限制，这些限制在 IAM Identity Center 文档中列出。应严格控制对 IAM Identity Center 委派管理员账户的访问权限。

> 设计注意事项
>
> - 如果您决定将 IAM Identity Center 身份源从任何其他来源更改为 Active Directory，或者将其从 Active Directory 更改为任何其他来源，则该目录必须位于 IAM Identity Center 委托的管理员成员账户（如果存在）中（归其所有）；否则，它必须位于管理账户中。
> - 您可以将您的子网托管在专用 VPC AWS Managed Microsoft AD 内的其他账户中，然后使用 AWS Resource Access Manager (AWS RAM) 将该其他账户的子网共享给委派的管理员

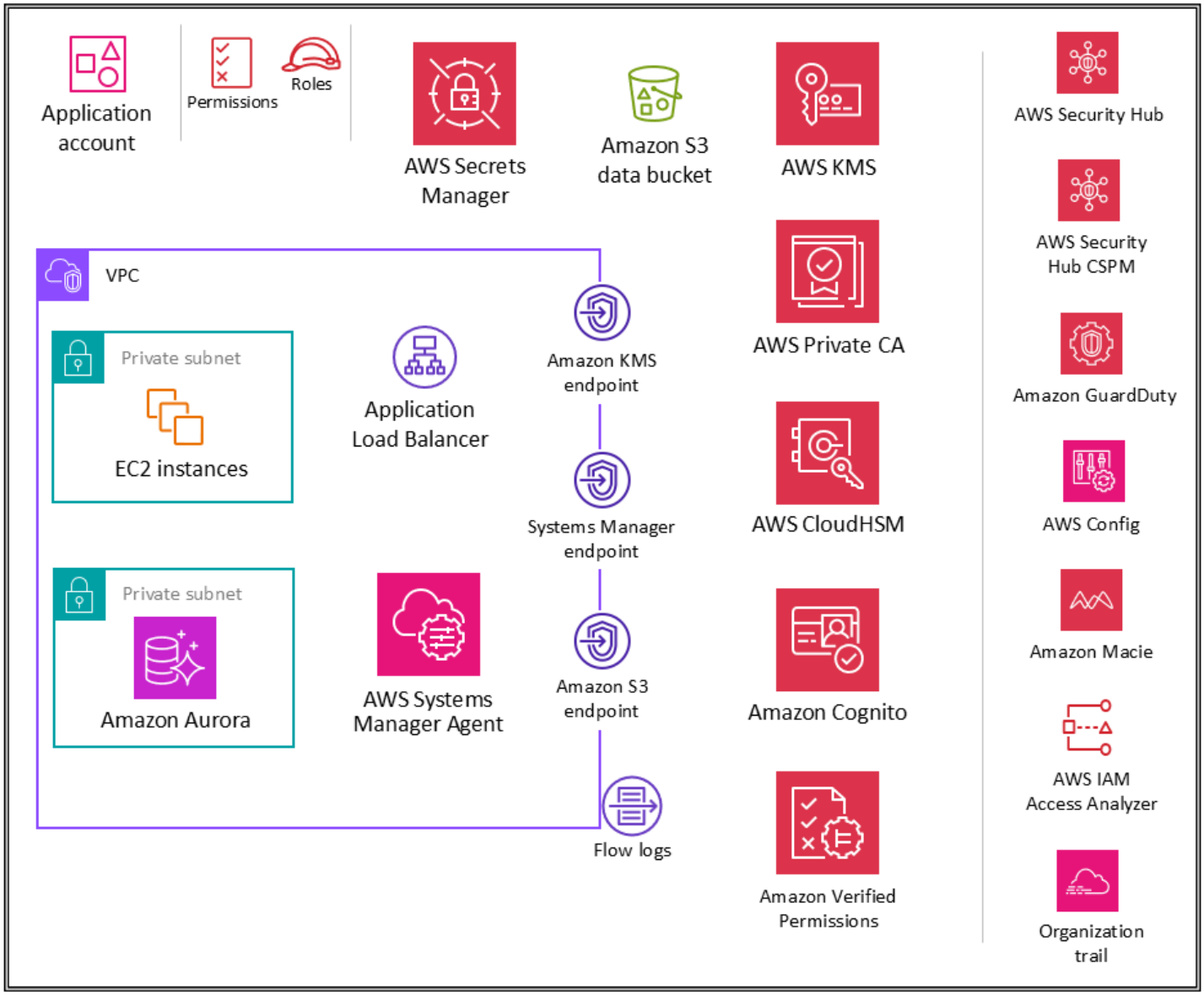
账户。这样， AWS Managed Microsoft AD 实例就可以在委托的管理员账户中进行控制，但从网络的角度来看，它的行为就像部署在另一个账户的 VPC 中一样。如果您有多个 AWS Managed Microsoft AD 实例，并且想要将它们部署到工作负载运行的本地位置，但要通过一个账户集中管理它们，这会很有用。

- 如果您有专门的身份团队负责定期执行身份和访问管理活动，或者有严格的安全要求将身份管理功能与其他共享服务功能区分开来，则可以托管一个专门 AWS 账户 用于身份管理的团队。在这种情况下，您将此账户指定为 IAM Identity Center 的委托管理员，它还托管您的 AWS Managed Microsoft AD 目录。通过在单个共享服务账户中使用精细的 IAM 权限，您可以在身份管理工作负载和其他共享服务工作负载之间实现相同级别的逻辑隔离。
- IAM 身份中心目前不提供多区域支持。（要在其他区域启用 IAM 身份中心，必须先删除当前的 IAM 身份中心配置。）此外，它不支持对不同的账户集使用不同的身份源，也不允许您将权限管理委托给组织的不同部分（即多个委派的管理员）或不同的管理员组。如果您需要这些功能中的任何一项，则可以使用 IAM 联合来管理您在外部身份提供商 (IdP) 中的用户身份， AWS 并授予这些外部用户身份使用您账户中的 AWS 资源的权限。与 OpenID Connect (OIDC) 或 SAML 2.0 兼容的 IAM 支持 IdPs 。最佳实践是，使用与第三方身份提供商（例如活动目录联合身份验证服务 (AD FS)、Okta、Azure Active Directory (Azure AD) 或 Ping 身份）的 SAML 2.0 联合，为用户提供登录 AWS 管理控制台 或调用 AWS API 操作的单点登录功能。有关 IAM 联合身份验证和身份提供商的更多信息，请参阅 IAM 文档中的关于基于 SAML 2.0 的联合。

工作负载 OU — 应用程序帐户

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

下图说明了在应用程序帐户中配置 AWS 的安全服务（以及应用程序本身）。



应用程序帐户托管用于运行和维护企业应用程序的主要基础设施和服务。应用程序帐户和工作负载 OU 有几个主要的安全目标。首先，您可以为每个应用程序创建一个单独的帐户，以便在工作负载之间提供界限和控制，从而避免角色、权限、数据和加密密钥混合的问题。你想提供一个单独的账户容器，应用团队可以在不影响其他人的情况下获得管理自己的基础架构的广泛权限。接下来，您可以通过为安全运营团队提供监控和收集安全数据的机制来增加一层保护。采用组织跟踪和本地部署账户安全服务（Amazon、、、Amazon GuardDuty AWS Config AWS Security Hub CSPM EventBridge、IAM Access Analyzer），这些服务由安全团队配置和监控。最后，您可以让您的企业集中设置控制。您可以使应用程序帐户与更广泛的安全结构保持一致，方法是使其成为 Workdloads OU 的成员，通过该组织单元继承相应的服务权限、约束和护栏。

设计注意事项

在您的组织中，您可能有多个业务应用程序。工作负载 OU 旨在容纳大多数特定于业务的工作负载，包括生产和非生产环境。这些工作负载可以是商用 off-the-shelf (COTS) 应用程序和您自己内部开发的自定义应用程序和数据服务的混合体。组织不同的业务应用程序及其开发环境的模式很少。一种模式是 OUs 根据您的开发环境（例如生产、暂存、测试和开发）创建多个子级，并在与不同应用程序相关的子 AWS 账户 项下使用单独 OUs 的子级。另一种常见的模式是为 OUs 每个应用程序设置单独的子级，然后 AWS 账户 为单独的开发环境使用单独的子级。确切的 OU 和账户结构取决于您的应用程序设计以及管理这些应用程序的团队。考虑一下您要实施的安全控制措施，无论它们是特定于环境还是特定于应用程序，因为像以前一样实施这些控制措施会更容易。 SCPs OUs有关组织面向工作负载的更多注意事项 OUs，请参阅 AWS 白皮书《使用 OUs多个帐户组织 AWS 环境》的 “应用程序” 部分。

应用程序 VPC

应用程序账户中的虚拟私有云 (VPC) 既需要入站访问权限（用于您正在建模的简单 Web 服务），也需要出站访问权限（用于应用程序需求或 AWS 服务 需求）。默认情况下，VPC 内的资源可以相互路由。有两个私有子网：一个用于托管 EC2 实例（应用程序层），另一个用于 Amazon Aurora（数据库层）。不同层（例如应用层和数据库层）之间的网络分段是通过 VPC 安全组完成的，VPC 安全组限制了实例级别的流量。为了提高弹性，工作负载跨越两个或多个可用区，每个区域使用两个子网。

设计注意事项

您可以使用流量镜像从 EC2 实例的 elastic network interface 复制网络流量。然后，您可以将流量发送到 out-of-band安全和监控设备进行内容检查、威胁监控或故障排除。例如，您可能想要监控离开您的 VPC 的流量或来源在您的 VPC 之外的流量。在这种情况下，您将镜像除在您的 VPC 内经过的流量之外的所有流量，并将其发送到单个监控设备。Amazon VPC 流日志不捕获镜像流量；它们通常仅从数据包标头中捕获信息。流量镜像允许您分析包括有效载荷在内的实际流量内容，从而更深入地了解网络流量。仅为可能作为敏感工作负载一部分运行或在出现问题时需要详细诊断的 EC2实例的 elastic network interface 启用流量镜像。

VPC 端点

VPC 端点提供了另一层安全控制以及可扩展性和可靠性。使用它们将您的应用程序 VPC 连接到其他 VPC AWS 服务。（在应用程序账户中， AWS SRA 使用、和 Amazon S3 的 AWS KMS VPC 终端节

点。 ）AWS Systems Manager终端节点是虚拟设备。它们是水平扩展、冗余和高度可用的 VPC 组件。通过它们，可以在 VPC 中的实例与服务之间进行通信，而不会对网络通信带来可用性风险或带宽约束。 AWS PrivateLink 无需互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接，即可使用 VPC 终端节点将您的 VPC 私密连接到支持的 AWS 服务 和由其提供支持的 VPC 终端节点服务。您的 VPC 中的实例不需要公有 IP 地址即可与其他实例通信 AWS 服务。您的 VPC 与另一个 VPC 之间的流量 AWS 服务 不会离开 Amazon 网络。

使用 VPC 终端节点的另一个好处是可以配置终端节点策略。VPC 端点策略是一种 IAM 资源策略，您在创建或修改端点时可将它附加到端点。如果您在创建终端节点时未附加 IAM 策略，则会为您 AWS 附加允许完全访问服务的默认 IAM 策略。端点策略不会覆盖或取代 IAM 用户策略或特定于服务的策略（如 S3 存储桶策略）。它是一个单独的 IAM 策略，用于控制从终端节点到指定服务的访问权限。通过这种方式，它增加了另一层控制层，控制哪些 AWS 委托人可以与资源或服务进行通信。

Amazon EC2

构成我们应用程序的 Amazon EC2 实例使用实例元数据服务 (IMDSv2) 的版本 2。 IMDSv2 增加了对可用于尝试访问 IMDS 的四种漏洞的保护：网站应用程序防火墙、开放反向代理、服务器端请求伪造 (SSRF) 漏洞、开放第 3 层防火墙和。 NATs有关更多信息，请参阅博客文章 “通过增强实例元数据服务，为开放的防火墙、反向代理和 SSRF 漏洞添加深度防御。 EC2

使用单独的 VPCs （作为账户边界的子集）按工作负载分段隔离基础架构。可以使用子网隔离单个 VPC 中的应用程序层（例如，Web、应用程序和数据库）。如果不应直接从 Internet 访问实例，请使用私有子网访问。要在不使用互联网网关的情况下从您的私有子网调用 Amazon EC2 API，请使用 AWS PrivateLink。使用安全组限制对您的实例的访问。 使用 VPC 流日志监控到达您的实例的流量。使用会话管理器（一项功能）远程访问您的实例 AWS Systems Manager，而不必打开入站 SSH 端口和管理 SSH 密钥。使用单独的亚马逊 Elastic Block Store (Amazon EBS) 卷来存放操作系统和您的数据。 您可以 AWS 账户将您的配置为强制对您创建的新 EBS 卷和快照副本进行加密。

> 实现示例
>
> AWS SRA 代码库提供了在亚马逊中实现默认 Amazon EBS 加密的示例。 EC2它演示了如何在每个账户 AWS 账户和 AWS 区域组织中启用账户级别的默认 Amazon EBS 加密。 AWS

AWS Nitro 飞地

AWS Nitro Enclaves 是 Amazon EC2 的一项功能，允许您从实例创建隔离的执行环境（称为安全区）。 EC2 Enclave 是独立的、强化的和高度受限的虚拟机。单个父 EC2 实例的 CPU 和内存被分成隔离的飞地。每个安全区都运行一个独立的内核。Enclaves 仅提供与其父实例的安全本地套接字连

接。它们没有持久性存储、交互式访问或外部联网。用户不能 SSH 进入安全区，父实例的进程、应用程序或用户（root 或管理员）也无法访问安全区内的数据和应用程序。您可以在 EC2 实例中保护最敏感的数据，例如个人身份信息 (PII)、医疗保健、财务和知识产权数据。Nitro Enclaves 使您能够专注于应用程序，而不必担心与外部服务的集成。Nitro Enclaves 包括对您的软件的加密认证，这样您就可以确保只有经过授权的代码在运行，并与其集成， AWS KMS 以便只有您的飞地才能访问敏感材料。这有助于减少最敏感的数据处理应用程序的攻击面积。使用 Nitro Enclaves 不会产生额外费用。

加密认证是用于证明飞地身份的过程。认证过程是通过 Nitro Hypervisor 完成的，它为飞地生成一份签名的认证文件，用于向其他第三方或服务证明其身份。认证文档包含飞地的关键细节，例如飞地的公钥、飞地图像和应用程序的哈希值等。

使用 Nitro Enclaves 的 AWS Certificate Manager (ACM)，您可以使用公有和私有证书。SSL/TLS certificates with your web applications and web servers running on EC2 instances with Nitro Enclaves. SSL/TLS certificates are used to secure network communications and to establish the identity of websites over the internet and resources on private networks. ACM for Nitro Enclaves removes the time-consuming and error-prone manual process of purchasing, uploading, and renewing SSL/TLSACM for Nitro Enclaves 可创建安全的私钥，将证书及其私钥分发到您的安全区，并管理证书续订。使用 ACM for Nitro Enclaves，证书的私钥在安全区中保持隔离，这会阻止实例及其用户对其进行访问。有关更多信息，请参阅AWS Certificate Manager Nitro Enclaves 文档中的 Nitro Enclaves。

应用程序负载均衡器

应用程序负载均衡器将传入的应用程序流量分发到多个可用区域中的多个目标（例如 EC2 实例）。在 AWS SRA 中，负载均衡器的目标组是应用程序 EC2 实例。 AWS SRA 使用 HTTPS 侦听器来确保通信信道已加密。Application Load Balancer 使用服务器证书终止前端连接，然后解密来自客户端的请求，然后再将其发送到目标。

AWS Certificate Manager (ACM) 以原生方式与应用程序负载均衡器集成， AWS SRA 使用 ACM 生成和管理必要的 X.509（TLS 服务器）公共证书。您可以通过 Application Load Balancer 安全策略为前端连接强制执行 TLS 1.2 和强密码。有关更多信息，请参阅弹性负载均衡文档。

设计注意事项

- 对于常见场景，例如需要在 Application Load Balancer 上使用私有 TLS 证书的严格内部应用程序，您可以使用此账户中的 ACM 从 AWS 私有 CA生成私有证书。在 AWS SRA 中，ACM 根私有 CA 托管在 Security Tools 帐户中，可以与整个 AWS 组织共享，也可以与特定组织共享， AWS 账户 以颁发最终实体证书，如前面的 “安全工具帐户” 部分所述。

- 对于公共证书，您可以使用 ACM 生成并管理这些证书，包括自动轮换。或者，您可以使用 SSL/TLS 工具生成自己的证书，方法是创建证书签名请求 (CSR)，获取由证书颁发机构 (CA) 签署的 CSR 以生成证书，然后将证书导入 ACM 或将证书上传到 IAM 以用于 Application Load Balancer。如果将证书导入 ACM，则必须监控证书的到期日期，并在证书到期之前对其进行续订。
- 要获得更多防御层，您可以部署 AWS WAF 策略来保护 Application Load Balancer。拥有边缘策略、应用程序策略，甚至是私有或内部策略实施层，可以提高通信请求的可见性，并提供统一的策略实施。有关更多信息，请参阅博客文章使用 f AWS 托管式规则 or 深入部署防御 AWS WAF。

AWS 私有 CA

AWS 私有证书颁发机构(AWS 私有 CA) 在应用程序账户中用于生成要与 Application Load Balancer 配合使用的私有证书。应用程序负载均衡器通常会通过 TLS 提供安全内容。这需要在 Application Load Balancer 上安装 TLS 证书。对于严格属于内部的应用程序，私有 TLS 证书可以提供安全通道。

在 AWS SRA 中，托管 AWS 私有 CA 在 Security Tools 帐户中，并通过使用 AWS RAM共享到应用程序帐户。这允许应用程序账户中的开发者向共享的私有 CA 申请证书。 CAs 跨组织共享或跨组织共享 AWS 账户 有助于降低在所有组织 CAs 中创建和管理重复项的成本和复杂性 AWS 账户。当您使用 ACM 从共享 CA 颁发私有证书时，证书将在请求的账户中本地生成，并且 ACM 提供完整的生命周期管理和续订。

Amazon Inspector

AWS SRA 使用 Amazon Inspector 自动发现和扫描驻留在亚马逊弹性容器注册表 (Amazon ECR) Container Registry 中的 EC2 实例和容器映像，以查找软件漏洞和意外网络泄露。

Amazon Inspector 被置于应用程序账户中，因为它为该账户中的 EC2 实例提供漏洞管理服务。此外，Amazon Inspector 还会报告进出 EC2 实例的不想要的网络路径。

成员账户中的 Amazon Inspector 由委派的管理员账户集中管理。在 AWS SRA 中，安全工具帐户是委派的管理员帐户。委派的管理员帐户可以管理组织成员的调查结果数据和某些设置。这包括查看所有成员账户的汇总结果详细信息、启用或禁用对成员账户的扫描，以及查看 AWS 组织内扫描的资源。

设计注意事项

您可以使用 Patch Manager（一项功能）触发按需修补 AWS Systems Manager，以修复 Amazon Inspector 未修补漏洞或其他关键安全漏洞。Patch Manager 可以帮助您修补这些漏

洞，而无需等待正常的修补计划。补救措施是使用 Systems Manager 自动化运行手册进行的。有关更多信息，请参阅由两部分组成的博客系列《AWS 使用 Amazon Inspector 实现漏洞管理和补救》和 AWS Systems Manager。

AWS Systems Manager

AWS Systems Manager可以 AWS 服务 用来查看来自多个资源的操作数据， AWS 服务 并自动执行跨 AWS 资源的操作任务。借助自动审批工作流程和运行手册，您可以努力减少人为错误，简化 AWS 资源的维护和部署任务。

除了这些常规的自动化功能外，Systems Manager 还支持许多预防、检测和响应式安全功能。AWS Systems Manager 代理（SSM 代理）是 Amazon 软件，可以在 EC2 实例、本地服务器或虚拟机 (VM) 上安装和配置。SSM Agent 让 Systems Manager 可以更新、管理和配置这些资源。Systems Manager 通过扫描这些托管实例并报告（或采取纠正措施）它在补丁、配置和自定义策略中检测到的任何违规行为，帮助您维护安全与合规性。

AWS SRA 使用会话管理器（Systems Manager 的一项功能）来提供基于浏览器的交互式外壳和 CLI 体验。这提供了安全且可审计的实例管理，无需打开入站端口、维护堡垒主机或管理 SSH 密钥。AWS SRA 使用补丁管理器（Systems Manager 的一项功能）将补丁应用于操作系统和应用程序的 EC2 实例。

AWS SRA 还使用自动化（Systems Manager 的一项功能）来简化亚马逊 EC2 实例和其他 AWS 资源的常见维护和部署任务。自动化可以根据计划简化常见的 IT 任务，如更改一个或多个节点的状态（使用批准自动化流程）和管理节点状态。Systems Manager 包含可通过使用标签帮助您确定大型目标实例组的功能，以及可根据您定义的限制帮助实施更改的速度控制功能。Automation 提供一键式自动化，用于简化复杂任务，例如创建金色 Amazon 系统映像 (AMIs) 和恢复无法 EC2 访问的实例。此外，您可以通过授予 IAM 角色访问特定 runbook 的权限来执行某些功能，而无需直接向这些角色授予权限，从而增强运营安全性。例如，如果您希望 IAM 角色有权在补丁更新后重启特定 EC2 实例，但又不想直接向该角色授予权限，则可以创建自动化运行手册并授予该角色仅运行运行手册的权限。

设计注意事项

- Systems Manager 依靠 EC2 实例元数据来正常运行。Systems Manager 可以使用实例元数据服务（IMDSv1 和 IMDSv2）的版本 1 或版本 2 访问实例元数据。
- SSM 代理必须与不同的 AWS 服务 资源进行通信，例如亚马逊 EC2 消息、Systems Manager 和 Amazon S3。要进行这种通信，子网需要出站 Internet 连接或配置相应的 VPC

终端节点。 AWS SRA 使用 VPC 端点作为 SSM 代理建立通往各种服务器的专用网络路径。AWS 服务

- 通过使用自动化，您可以与组织中的其余人员分享最佳实践。您可以在 Runbook 中创建资源管理的最佳实践， AWS 区域 并跨组共享运行手册。您还可以限制 runbook 参数的允许值。对于这些用例，您可能需要在中央帐户（例如安全工具或共享服务）中创建自动化运行手册，并与 AWS 组织的其他成员共享。常见用例包括集中实施修补和安全更新、修复 VPC 配置或 S3 存储桶策略的偏差以及大规模管理 EC2 实例的能力。有关实现的详细信息，请参阅 S ystems Manager 文档。

Amazon Aurora

在 AWS SRA 中，Amazon Aurora 和 Amazon S3 构成了逻辑数据层。Aurora 是一个与 MySQL 和 PostgreSQL 兼容的完全托管式的关系数据库引擎。在 EC2 实例上运行的应用程序会根据需要与 Aurora 和 Amazon S3 通信。Aurora 在数据库子网组中配置了一个数据库集群。

设计注意事项

与许多数据库服务一样，Aurora 的安全管理分为三个级别。要控制谁可以对 Aurora 数据库集群和数据库实例执行亚马逊关系数据库服务 (Amazon RDS) 管理操作，您可以使用 IAM。要控制哪些设备和 EC2 实例可以为 VPC 中的 Aurora 数据库集群打开与集群终端节点和数据库实例端口的连接，您可以使用 VPC 安全组。要对 Aurora 数据库集群的登录名和权限进行身份验证，您可以采用与 MySQL 或 PostgreSQL 独立数据库实例相同的方法，也可以对兼容 Aurora MySQL 的版本使用 IAM 数据库身份验证。使用后一种方法，您可以使用 IAM 角色和身份验证令牌对与 Aurora MySQL 兼容的数据库集群进行身份验证。

Amazon S3

Amazon S3 是一项对象存储服务，提供行业领先的可扩展性、数据可用性、安全性和性能。它是许多基于其构建的应用程序的数据支柱 AWS，适当的权限和安全控制对于保护敏感数据至关重要。有关推荐的 Amazon S3 安全最佳实践，请参阅文档、在线技术讲座和博客文章中的深入探讨。最重要的最佳做法是阻止对 S3 存储桶的过于宽松的访问（尤其是公共访问）。

AWS KMS

AWS SRA 说明了推荐的密钥管理分发模式，其中密钥与要加密的资源 AWS KMS key 位于同一个 AWS 账户 分发模式中。因此，除了包含在 AWS KMS Security Tools 帐户中外，还用于应用程序帐

户。在应用程序帐户中，AWS KMS 用于管理特定于应用程序资源的密钥。您可以使用密钥策略向本地应用程序角色授予密钥使用权限，并将管理和监控权限限制给密钥保管人，从而实现职责分离。

> 设计注意事项
>
> 在分布式模型中，AWS KMS 密钥管理责任由应用团队承担。但是，您的中央安全团队可以负责管理和监控重要的加密事件，例如：
>
> - KMS 密钥中导入的密钥材料临近到期日期。
> - KMS 密钥中的密钥材料已自动轮换。
> - AKMS 密钥已删除。
> - 解密失败率很高。

AWS CloudHSM

AWS CloudHSM在中提供了托管硬件安全模块 (HSMs) AWS Cloud。它允许您使用经过验证的 FIPS 140-2 3 级加密密钥来生成和使用自己的加密密钥 HSMs ，该密钥 AWS 由您控制访问权限。您可以使用 AWS CloudHSM 卸载 Web 服务器的 SSL/TLS 处理负载。这减轻了 Web 服务器的负担，并通过将 Web 服务器的私钥存储在中来提供额外的安全性 AWS CloudHSM。同样，如果您需要充当证书颁发机构，则可以在网络账户的入站 VPC 中部署 HSM 来存储您的私钥并签署证书请求。 AWS CloudHSM

> 设计注意事项
>
> 如果您对 FIPS 140-2 第 3 级有硬性要求，也可以选择将 AWS CloudHSM 集群配置 AWS KMS 为使用自定义密钥存储，而不是使用原生 KMS 密钥存储。通过这样做，您可以受益于加密数据的 AWS KMS 和 AWS 服务 之间的集成，同时负责保护您的 HSMs KMS 密钥。它将单租户 HSMs 控制与易用性和集成性相结合。 AWS KMS要管理您的 AWS CloudHSM 基础架构，您必须使用公钥基础架构 (PKI)，并拥有一支具有管理 HSMs经验的团队。

AWS Secrets Manager

AWS Secrets Manager帮助您保护访问应用程序、服务和 IT 资源所需的凭证（机密）。该服务使您能够在数据库凭证、API 密钥和其他密钥的整个生命周期中高效地轮换、管理和检索它们。您可以将代码中的硬编码凭据替换为对 Secrets Manager 的 API 调用，以编程方式检索密钥。这有助于确保密码不会被正在检查您的代码的人泄露，因为密码中已不存在该机密。此外，Secrets Manager 可以帮助您在不同环境（开发、预生产、生产）之间移动应用程序。您可以确保环境中存在适当命名和引用的密钥，

而不必更改代码。这提高了应用程序代码在不同环境中的一致性和可重用性，同时在测试代码后需要更少的更改和人为交互。

借助 Secrets Manager，您可以使用精细的 IAM 策略和基于资源的策略来管理对机密的访问权限。您可以使用自己管理的加密密钥对机密进行加密，从而帮助保护机密。 AWS KMS Secrets Manager 还集成了 AWS 日志和监控服务，用于集中审计。

Secrets Manager 使用信封加密 AWS KMS keys 和数据密钥来保护每个密钥值。创建密钥时，您可以选择 AWS 账户 和区域中的任何对称客户托管密钥，也可以将托管密钥用于 Secret AWS s Manager。

作为最佳实践，您可以监控您的密钥以记录对它们的任何更改。这可以帮助您确保可以调查任何意外的使用或更改。可以回退不需要的更改。Secrets Manager 目前支持两种 AWS 服务 允许你监控自己的组织和活动的功能： AWS CloudTrail 和 AWS Config。 CloudTrail 将 Secrets Manager 的所有 API 调用捕获为事件，包括来自 Secrets Manager 控制台的调用和对 Secrets Manager 的代码调用 APIs。此外，还会 CloudTrail 捕获其他可能对您的安全或合规性产生影响 AWS 账户 或可能帮助您解决操作问题的相关（非 API）事件。其中包括某些密钥轮换事件和秘密版本的删除。 AWS Config 可以通过跟踪和监视 Secrets Manager 中密钥的更改来提供侦探控制。这些更改包括密钥的描述、轮换配置、标签以及与其他 AWS 来源（例如 KMS 加密密钥或用于轮换密钥的 AWS Lambda 函数）的关系。您还可以将接收配置和合规性更改通知的 Amazon EventBridge 配置为路由特定的机密事件以进行通知或补救操作。 AWS Config

在 AWS SRA 中，Secrets Manager 位于应用程序帐户中，用于支持本地应用程序用例并管理接近其使用情况的密钥。在这里，将实例配置文件附加到应用程序账户中的 EC2 实例。然后可以在 Secrets Manager 中配置单独的密钥，以允许该实例配置文件检索密钥，例如，加入相应的 Active Directory 或 LDAP 域并访问 Aurora 数据库。Secret s Manager 与 Amazon RDS 集成，可在您创建、修改或还原 Amazon RDS 数据库实例或多可用区数据库集群时管理用户证书。这可以帮助您管理密钥的创建和轮换，并将代码中的硬编码凭据替换为对 Secrets Manager 的编程 API 调用。

> **设计注意事项**
>
> 通常，请在最接近密钥使用位置的账户中配置和管理 Secrets Manager。这种方法利用了当地对用例的了解，为应用程序开发团队提供了速度和灵活性。对于可能需要额外控制层的严格控制信息，可以由安全工具帐户中的 Secrets Manager 集中管理机密。

Amazon Cognito

Amazon Cognito 允许您快速高效地将用户注册、登录和访问控制添加到您的网络和移动应用程序中。Amazon Cognito 可扩展到数百万用户，并支持通过社交身份提供商（例如苹果、Facebook、谷

歌和亚马逊）以及通过 SAML 2.0 和 OpenID Connect 登录企业身份提供商。Amazon Cognito 的两个主要组成部分是用户池和身份池。用户池是为应用程序用户提供注册和登录选项的用户目录。身份池使您能够向您的用户授予对其他人的访问权限 AWS 服务。您可以单独或配合使用身份池和用户池。有关常见使用场景，请参阅 Amazon Cognito 文档。

Amazon Cognito 为用户注册和登录提供了一个可自定义的内置用户界面。你可以使用安卓、iOS 和适用 JavaScript SDKs 于 Amazon Cognito 的 Amazon Cognito 向你的应用程序添加用户注册和登录页面。Amazon Cognito Sync 是一个 AWS 服务 和客户端库，它支持跨设备同步与应用程序相关的用户数据。

Amazon Cognito 支持对静态数据和传输中的数据进行多因素身份验证和加密。 Amazon Cognito 用户池提供高级安全功能，有助于保护对应用程序中用户账户的访问。这些高级安全功能提供基于风险的自适应身份验证，并保护其免受泄露凭据的使用。

设计注意事项

- 您可以创建一个 AWS Lambda 函数，然后使用 Lambda 触发器在用户池操作期间触发该函数，例如用户注册、确认和登录（身份验证）。您可以添加身份验证质询、迁移用户和自定义验证消息。有关常见操作和用户流程，请参阅 Amazon Cognito 文档。Amazon Cognito 同步调用 Lambda 函数。
- 您可以使用 Amazon Cognito 用户池来保护小型的多租户应用程序。多租户设计的一个常见用例是运行工作负载以支持测试应用程序的多个版本。多租户设计对于使用不同数据集测试单个应用程序也很有用，这样可以充分利用您的集群资源。但是，请确保租户数量和预期容量与相关的 Amazon Cognito 服务配额保持一致。这些配额在应用程序中的所有租户之间共享。

Amazon Verified Permissions

Amazon V erified Permissions 是一项可扩展的权限管理和精细授权服务，适用于您构建的应用程序。开发人员和管理员可以使用 Cedar（一种专门构建且以安全为先的开源策略语言），通过角色和属性来定义更精细、更具情境感知能力、基于策略的访问控制。通过外部化授权和集中策略管理和管理，开发人员可以更快地构建更安全的应用程序。Verified Permissions 包括架构定义、策略声明语法和可扩展到数百万个权限的自动推理，因此您可以强制执行默认拒绝和最小权限原则。该服务还包括评估模拟器工具，可帮助您测试授权决策和作者政策。这些功能有助于部署深入、细粒度的授权模型，以支持您的零信任目标。Verified Permissions 将权限集中在策略存储中，并帮助开发人员使用这些权限来授权用户在其应用程序中执行的操作。

您可以通过 API 将您的应用程序连接到服务，以授权用户访问请求。对于每个授权请求，该服务都会检索相关策略并评估这些策略，以根据用户、角色、群组成员资格和属性等上下文输入来确定是否允许用户对资源采取操作。您可以配置并连接已验证的权限，以便将策略管理和授权日志发送到 AWS CloudTrail。如果您使用 Amazon Cognito 作为身份存储，则可以与已验证权限集成，并使用 Amazon Cognito 在应用程序的授权决策中返回的 ID 和访问令牌。您向已验证权限提供 Amazon Cognito 令牌，该权限使用令牌包含的属性来代表委托人并标识委托人的权利。有关此集成的更多信息，请参阅 AWS 博客文章 “使用亚马逊验证权限和 Amazon Cognito 简化细粒度授权”。

已验证权限可帮助您定义基于策略的访问控制 (PBAC)。PBAC 是一种访问控制模型，它使用以策略形式表示的权限来确定谁可以访问应用程序中的哪些资源。PBAC 将基于角色的访问控制 (RBAC) 和基于属性的访问控制 (ABAC) 结合在一起，从而形成了更强大、更灵活的访问控制模型。要详细了解 PBAC 以及如何使用已验证权限设计授权模型，请参阅 AWS 博客文章使用 Amazon Verified Permissions 开发应用程序时基于策略的访问控制。

在 AWS SRA 中，已验证权限位于应用程序账户中，通过与 Amazon Cognito 集成，支持应用程序的权限管理。

分层防御

应用程序帐户提供了一个机会来说明 AWS 启用的分层防御主体。考虑构成 AWS SRA 中表示的简单示例应用程序核心的 EC2 实例的安全性，您可以看到在分层防御中协同 AWS 服务 工作的方式。这种方法符合 AWS 安全服务的结构视图，如本指南前面的 “在AWS 组织中应用安全服务” 一节中所述。

- 最里面的层是实例。 EC2 如前所述， EC2 实例包括许多原生安全功能，无论是默认还是作为选项。示例包括 IMDSv2Nitro 系统和 Amazon EBS 存储加密。
- 第二层保护侧重于 EC2 实例上运行的操作系统和软件。诸如 Amazon Inspec tor 之类的服务AWS Systems Manager使您能够监控、报告这些配置并采取纠正措施。Amazon Inspector 会监控您的软件是否存在漏洞，Systems Manager 会扫描托管实例的补丁和配置状态，然后报告并采取您指定的任何纠正措施，从而帮助您努力维护安全与合规性。
- 这些实例和在这些实例上运行的软件与您的 AWS 网络基础设施同在。除了使用 Amazon VPC 的安全功能外， AWS SRA 还利用 VPC 终端节点在 VPC 和受支持的 VPC 之间提供私有连接 AWS 服务，并提供一种将访问策略置于网络边界的机制。
- EC2 实例、软件、网络以及 IAM 角色和资源的活动和配置由 AWS 账户专注于服务的进一步监控，例如、、、Amazon AWS Security Hub CSPM、、 AWS Security Hub GuardDuty AWS CloudTrail AWS Config、IAM Access Analyzer 和 Amazon Macie。
- 最后，除了应用程序账户之外， AWS RAM 还有助于控制与其他账户共享哪些资源，而 IAM 服务控制策略可帮助您在整个 AWS 组织中强制执行一致的权限。

用于安全的 AI/ML

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

人工智能和机器学习（ 20 多年来AI/ML) is transforming businesses. AI/ML一直是 Amazon 关注的焦点，客户使用的许多功能（包括安全服务）都是由 AI/ML 驱动的。 AWS这创造了一种内在的差异化价值，因为您可以安全地进行构建， AWS 而无需您的安全团队或应用程序开发团队具有 AI/ML 方面的专业知识。

人工智能是一种先进的技术，它使机器和系统能够获得智能和预测能力。人工智能系统通过其消耗或训练的数据从过去的经验中吸取教训。机器学习是 AI 最重要的方面之一。机器学习是计算机在不经过明确编程的情况下从数据中学习的能力。在传统编程中，程序员编写规则来定义程序应如何在计算机或机器上运行。在机器学习中，模型从数据中学习规则。机器学习模型可以发现数据中的隐藏模式，或者对训练期间未使用的新数据做出准确的预测。多种 AWS 服务 用途 AI/ML ，可以从庞大的数据集中学习并做出安全推断。

- Amazon Macie 是一项数据安全服务，它使用机器学习和模式匹配来发现和帮助保护您的敏感数据。Macie 会自动检测大量且不断增长的敏感数据类型，包括姓名、地址等个人身份信息 (PII) 和信用卡号等财务信息。它还使您可以持续查看存储在亚马逊简单存储服务 (Amazon S3) 中的数据。Macie 使用在不同类型数据集上训练的自然语言处理 (NLP) 和机器学习模型，以了解您的现有数据，并分配业务价值以确定关键业务数据的优先级。然后，Macie 会生成敏感数据发现。
- Amazon GuardDuty 是一项威胁检测服务，它使用机器学习、异常检测和集成威胁情报来持续监控恶意活动和未经授权的行为，以帮助保护您的实例 AWS 账户、无服务器和容器工作负载、用户、数据库和存储。 GuardDuty 整合了机器学习技术，这些技术可以非常有效地将潜在的恶意用户活动与内部的异常但良性的操作行为区分开来。 AWS 账户此功能可以持续对账户内的 API 调用进行建模，并结合概率预测，以便更准确地隔离高度可疑的用户行为并发出警报。这种方法有助于识别与已知威胁策略相关的恶意活动，包括发现、初始访问、持久性、权限升级、防御规避、凭据访问、影响和数据泄露。要了解有关如何 GuardDuty 使用机器学习的更多信息，请参阅 re AWS : inForce 2023 分组讨论会在 Ama GuardDuty zon 中使用机器学习开发新发现 (0)。TDR31

可证明的安全性

AWS 开发自动推理工具，这些工具使用数学逻辑来回答有关基础架构的关键问题，并检测可能暴露数据的错误配置。这种功能之所以称为可证明安全，是因为它为云端和云端的安全性提供了更高的保障。Provable Security 使用自动推理，这是人工智能的一门特定学科，用于将逻辑推导应用于计算机

系统。例如，自动推理工具可以分析策略和网络架构配置，并证明不存在可能暴露易受攻击数据的意外配置。这种方法为云的关键安全特性提供了可能的最高级别的保障。有关更多信息，请参阅 AWS 网站上的可证明安全资源。以下内容 AWS 服务 和功能目前使用自动推理来帮助您实现可证明的应用程序安全性：

- Amazon V erified Permissions 是一项可扩展的权限管理和精细授权服务，适用于您构建的应用程序。Verified Permissions 使用 Ced ar，这是一种用于访问控制的开源语言，使用自动推理和差异测试构建。Cedar 是一种将权限定义为描述谁应该有权访问哪些资源的策略的语言。它也是评估这些政策的规范。使用 Cedar 策略来控制应用程序的每个用户可以执行的操作以及他们可以访问哪些资源。Cedar 策略是允许或禁止的声明，用于确定用户是否可以对资源进行操作。策略与资源关联，您可以将多个策略附加到一个资源。 禁止政策优先于许可政策。当您的应用程序的用户尝试对资源执行操作时，您的应用程序会向 Cedar 策略引擎发出授权请求。Cedar 会评估适用的政策并返回`ALLOW`或`DENY`决定。Cedar 支持任何类型的委托人和资源的授权规则，允许基于角色和基于属性的访问控制，并支持通过自动推理工具进行分析，这些工具可以帮助优化您的策略并验证您的安全模型。
- AWS Identity and Access Management Access Analyzer帮助您简化权限管理。您可以使用此功能来设置精细权限、验证预期权限以及通过删除未使用的访问权限来优化权限。IAM Access Analyzer 会根据您的日志中捕获的访问活动生成精细的策略。它还提供 100 多份政策检查，以帮助您撰写和验证您的政策。IAM Access Analyzer 使用可证明的安全性来分析访问路径，并为公共和跨账户访问您的资源提供全面的调查结果。该工具基于 Zelkova 构建，它将 IAM 策略转换为等效的逻辑语句，并针对问题运行一套通用和专门的逻辑求解器（可满足性模数理论）。IAM Access Analyzer 反复将 Zelkova 应用于具有越来越具体查询的策略，以根据策略的内容表征策略允许的行为类别。分析器不会检查访问日志来确定外部实体是否访问了您的信任区域内的资源。当基于资源的策略允许访问资源时，即使外部实体没有访问该资源，它也会生成调查结果。要了解有关可满足性模数理论的更多信息，请参阅《可满足性手册》中的可满足性模数理论。 *
- Amazon S3 阻止公共访问是 Amazon S3 的一项功能，它允许您阻止可能导致对您的存储桶和对象进行公开访问的可能的错误配置。您可以为接入点、存储桶、账户和 AWS 组织启用 Amazon S3 阻止公共访问权限（这会影响账户中的现有存储桶和新存储桶）。通过访问控制列表 (ACLs)、存储桶策略或两者兼而有之，向存储桶和对象授予公共访问权限。通过使用Zelkova自动推理系统来确定给定的策略或ACL是否被视为公开。Amazon S3 使用 Zelkova 来检查每项存储桶策略，并在未经授权的用户能够读取或写入您的存储桶时向您发出警告。如果存储桶被标记为公有，则允许某些公共请求访问该存储桶。如果存储桶被标记为非公开，则所有公共请求都将被拒绝。Zelkova 之所以能够做出这样的决定，是因为它对 IAM 策略进行了精确的数学表示。它为每种策略创建了一个公式，并证明了关于该公式的定理。
- Amazon VPC 网络访问分析器是 Amazon VPC 的一项功能，可帮助您了解通往资源的潜在网络路径，并识别潜在的意外网络访问。Network Access Analyzer 可帮助您验证网络分段、识别互联网可

访问性以及验证可信的网络路径和网络访问权限。此功能使用自动推理算法来分析数据包在网络中的资源之间可以走的 AWS 网络路径。然后，它会生成与您的网络访问范围相匹配的路径的调查结果，这些路径定义了出站和入站流量模式。网络访问分析器对网络配置执行静态分析，这意味着在此分析过程中，不会在网络中传输任何数据包。

- Amazon VPC Reachability Analyzer 是 Amazon VPC 的一项功能，可让您调试、了解和可视化网络中的连接。 AWS Reachability Analyzer 是一种配置分析工具，使您能够在虚拟私有云中的源资源和目标资源之间执行连接测试（ ）。VPCs当目标可以到达时，Reachability Analyzer 会生成源和目标之间虚拟网络路径的 hop-by-hop详细信息。当无法到达目的地时，Reachability Analyzer 会识别阻塞组件。Reachability Analyzer 使用自动推理，通过构建源和目标之间的网络配置模型来识别可行路径。然后，它会根据配置检查可达性。它不发送数据包或分析数据平面。

* Biere、A.M. Heule、H. van Maaren 和 T. Walsh。2009。《满意度手册》。IOS 出版社，NLD。

构建您的安全架构 — 分阶段的方法

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

AWS SRA 推荐的多账户安全架构是一种基准架构，可帮助您在设计过程中尽早注入安全性。每个组织的云之旅都是独一无二的。要成功发展您的云安全架构，您需要设想所需的目标状态，了解您当前的云就绪情况，并采用敏捷的方法来缩小任何差距。 AWS SRA 为您的安全架构提供了参考目标状态。渐进式转型使您能够快速展示价值，同时最大限度地减少做出深远预测的需求。

AWS 云采用框架 (AWS CAF) 推荐了四个迭代和增量云转型阶段：构想、调整、启动和扩展。当你进入启动阶段并专注于在生产环境中交付试点计划时，你应该专注于构建一个强大的安全架构，作为扩展阶段的基础，这样你就有技术能力满怀信心地迁移和操作最关键业务的工作负载。如果您是一家初创公司、想要扩展业务的中小型公司，或者正在收购新业务部门或正在进行合并和收购的企业，则这种分阶段的方法适用。 AWS SRA 可帮助您实现该安全基准架构，以便您可以在不断扩大的组织中统一应用安全控制。 AWS Organizations基准架构由多个 AWS 账户 和服务组成。规划和实施应该是一个多阶段的过程，这样您就可以对较小的里程碑进行迭代，以实现设置基准安全架构的更大目标。本节基于结构化方法描述云之旅的典型阶段。这些阶段符合 Well-Architect AWS ed Framework 的安全设计原则。

第 1 阶段：构建 OU 和账户结构

精心设计的 AWS 组织和账户结构是建立牢固安全基础的先决条件。如本指南前面的 SRA 构造块部分所述，拥有多个构 AWS 账户 件可以帮助您通过设计隔离不同的业务和安全功能。一开始这似乎是不必要的工作，但这是一项可以帮助您快速安全地扩展规模的投资。该部分还说明了 AWS Organizations 如何使用管理多个账户 AWS 账户，以及如何使用可信访问权限和委派管理员功能对这 AWS 服务 多个账户进行集中管理。

你可以AWS Control Tower按照本指南前面概述的方法来编排你的着陆区。如果您目前正在使用单个账户 AWS 账户，请参阅《过渡到多个账户 AWS 账户》指南，尽早迁移到多个账户。例如，如果您的初创公司目前正在单一构思和原型设计您的产品 AWS 账户，那么在将产品投放市场之前，您应该考虑采用多账户策略。同样，中小型和企业组织应在规划初始生产工作负载后立即开始制定其多账户战略。从基础开始 AWS 账户， OUs然后添加与工作负载相关的账户 OUs 和账户。

有关 AWS 账户 AWS SRA 中提供的内容之外的 OU 结构建议，请参阅中小型企业多账户策略博客文章。在最终确定 OU 和账户结构时，请考虑要使用服务控制策略 (SCPs)、资源控制策略 () 和声明性策略在组织范围内实施的高级安全控制。RCPs

设计注意事项

在设计组织单位和账户结构时，请勿复制公司的报告结构。您 OUs 应该基于工作负载功能和一组适用于工作负载的常用安全控制措施。不要试图从一开始就设计完整的账户结构。专注于基础知识 OUs，然后根据需要添加工作负载 OUs 。在设计的早期阶段，您可以在账户之间移动 OUs以尝试其他方法。但是，这可能会导致在管理逻辑权限方面产生一些开销，具体取决于 SCPs、 RCPs、声明性策略以及基于 OU 和账户路径的 IAM 条件。

实现示例

AWS SRA 代码库提供了 “账户备用联系人” 的实现示例。此解决方案为组织内的所有账户设置账单、运营和安全备用联系人。

第 2 阶段：建立坚实的身份基础

一旦你创建了多个账户 AWS 账户，你就应该允许你的团队访问这些账户中的 AWS 资源。身份管理一般分为两类：员工身份和访问管理以及客户身份和访问管理 (CIAM)。Workforce IAM 适用于员工和自动化工作负载需要登录 AWS 才能完成工作的组织。当组织需要一种方法来对用户进行身份验证以提供对组织应用程序的访问权限时，使用 CIAM。您首先需要制定员工 IAM 策略，这样您的团队才能构建和迁移应用程序。您应始终使用 IAM 角色而不是 IAM 用户来向人类或机器用户提供访问权限。按照 AWS SRA 指南，了解如何在组织管理和共享服务账户 AWS IAM Identity Center 中使用来集中管理对您的单点登录 (SSO) 访问权限。 AWS 账户该指南还提供了在您无法使用 IAM 身份中心时使用 IAM 联合身份验证的设计注意事项。

在使用 IAM 角色为用户提供 AWS 资源访问权限时，您应按照本指南的安全工具和组织管理部分所述使用 IAM Access Analyzer 和 IAM 访问顾问。这些服务可帮助您实现最低权限，这是一项重要的预防性控制措施，可帮助您建立良好的安全态势。

设计注意事项

要实现最低权限，请设计流程以定期审查和了解您的身份与其正常运行所需的权限之间的关系。在学习过程中，请微调这些权限，并逐渐将其缩小到尽可能少的权限。为了实现可扩展性，这应该由您的中央安全团队和应用程序团队共同负责。使用基于资源的策略、权限边界、基于属性的访问控制和会话策略等功能，帮助应用程序所有者定义精细的访问控制。

实施示例

AWS SRA 代码库提供了两个适用于此阶段的示例实现：

- IAM 密码策略为用户设置账户密码策略，使其符合常见的合规性标准。
- Access Analyz er 在委派的管理员账户中配置组织级分析器，在每个账户中配置账户级分析器。

第 3 阶段：保持可追溯性

当您的用户可以访问 AWS 并开始构建时，您将想知道谁在做什么、何时以及从何处开始做什么。您还需要了解潜在的安全配置错误、威胁或意外行为。更好地了解安全威胁可以使您确定适当的安全控制的优先顺序。要监控 AWS 活动，请按照 AWS SRA 的建议设置组织跟踪，方法是使用日志存档AWS CloudTrail帐户并将日志集中在日志存档帐户中。要监控安全事件 AWS Security Hub CSPM，请使用 Amazon 和 Ama GuardDuty zon Security Lake，如安全工具账户部分所述。 AWS Config

设计注意事项

开始使用新版本时 AWS 服务，请确保为该服务启用特定于服务的日志，并将其存储为中央日志存储库的一部分。

实施示例

AWS SRA 代码库提供了以下适用于此阶段的示例实现：

- 组织 CloudTrail创建组织跟踪并设置默认值来配置数据事件（例如，在 Amazon S3 和中 AWS Lambda） CloudTrail ，以减少重复配置的 AWS Control Tower内容。此解决方案提供了配置管理事件的选项。
- AWS Config Cont@@ rol Tower 管理账户允许 AWS Config 在管理账户中监控资源合规性。
- Conformance Pack 组织规则将合规包部署到组织内的账户和指定区域。
- AWS Config A@@ ggregato r 通过将管理委托给除审计账户以外的成员账户来部署聚合器。
- S@@ ecurity Hub CSPM Organization 在委托的管理员账户中为组织内的账户和受管区域配置 Security Hub CSPM。

- GuardDuty 组织 GuardDuty 在委派的管理员账户中为组织内的账户进行配置。

第 4 阶段：在所有层面应用安全措施

此时，你应该：

- 适合您的安全控制措施 AWS 账户。
- 定义明确的账户和 OU 结构，其预防控制措施通过 SCPs、 RCPs、声明性策略以及最低权限 IAM 角色和策略进行定义。
- 能够使用记录 AWS 活动 AWS CloudTrail；使用 AWS Security Hub CSPM、Amazon 和检测安全事件 AWS Config；使用 Amazon GuardDuty Security Lake 对专门构建的数据湖进行高级分析，以确保安全。

在此阶段，计划在组织的其他层面上应用安全保护，如在整个 AWS 组织中应用安全服务一节中所述。 AWS 您可以使用、、、、 AWS Certificate Manager (ACM)、Amazon、Amazon AWS WAF AWS Shield AWS Firewall Manager AWS Network Firewall、Amazon Route 53 和 Ama CloudFront zon VPC 等服务为您的网络层构建安全控制，如网络账户部分所述。当您向下移动技术堆栈时，请应用特定于您的工作负载或应用程序堆栈的安全控制。使用 VPC 终端节点、Amazon Inspector AWS Systems Manager AWS Secrets Manager、、和 Amazon Cognito，如应用程序账户部分所述。

设计注意事项

在设计深度防御 (DiD) 安全控制时，请考虑缩放系数。您的中央安全团队不会有足够的带宽或完全了解每个应用程序在您的环境中的行为。让您的应用程序团队负责为其应用程序识别和设计正确的安全控制措施，并承担责任。中央安全团队应专注于提供正确的工具和咨询，以支持应用团队。要了解过去采用更加左移的安全方法的扩展机制， AWS 请参阅博客文章《Security Guardians 计划是如何 AWS 构建的，这是一种分配安全所有权的机制》。

实施示例

AWS SRA 代码库提供了以下适用于此阶段的示例实现：

- EC2 默认 EBS 加密将 Amazon EC2 中的默认 Amazon EBS 加密配置为使用所提供的默认 AWS KMS key 加密。 AWS 区域

- S3 封禁账户公共访问在 Amazon S3 中为组织内的账户配置账户级别的阻止公开访问 (BPA) 设置。
- Fi@@ rewall Manager 演示了如何为组织内的账户配置安全组 AWS WAF 策略和策略。
- Inspect or Organization 在委托的管理员账户中为组织内的账户和受管区域配置 Amazon Inspector。

第 5 阶段：保护传输中的数据和静态数据

您的业务和客户数据是您需要保护的宝贵资产。 AWS 提供各种安全服务和功能，以保护动态和静态数据。如网络账户部分所述 AWS Certificate Manager，使用Amaz CloudFront on来保护通过互联网收集的动态数据。对于内部网络中的动态数据，请使用带的 Application Load Balancer AWS 私有证书颁发机构，如应用程序帐户部分所述。 AWS KMS 并 AWS CloudHSM 帮助您提供加密密钥管理以保护静态数据。

第 6 阶段：为安全事件做好准备

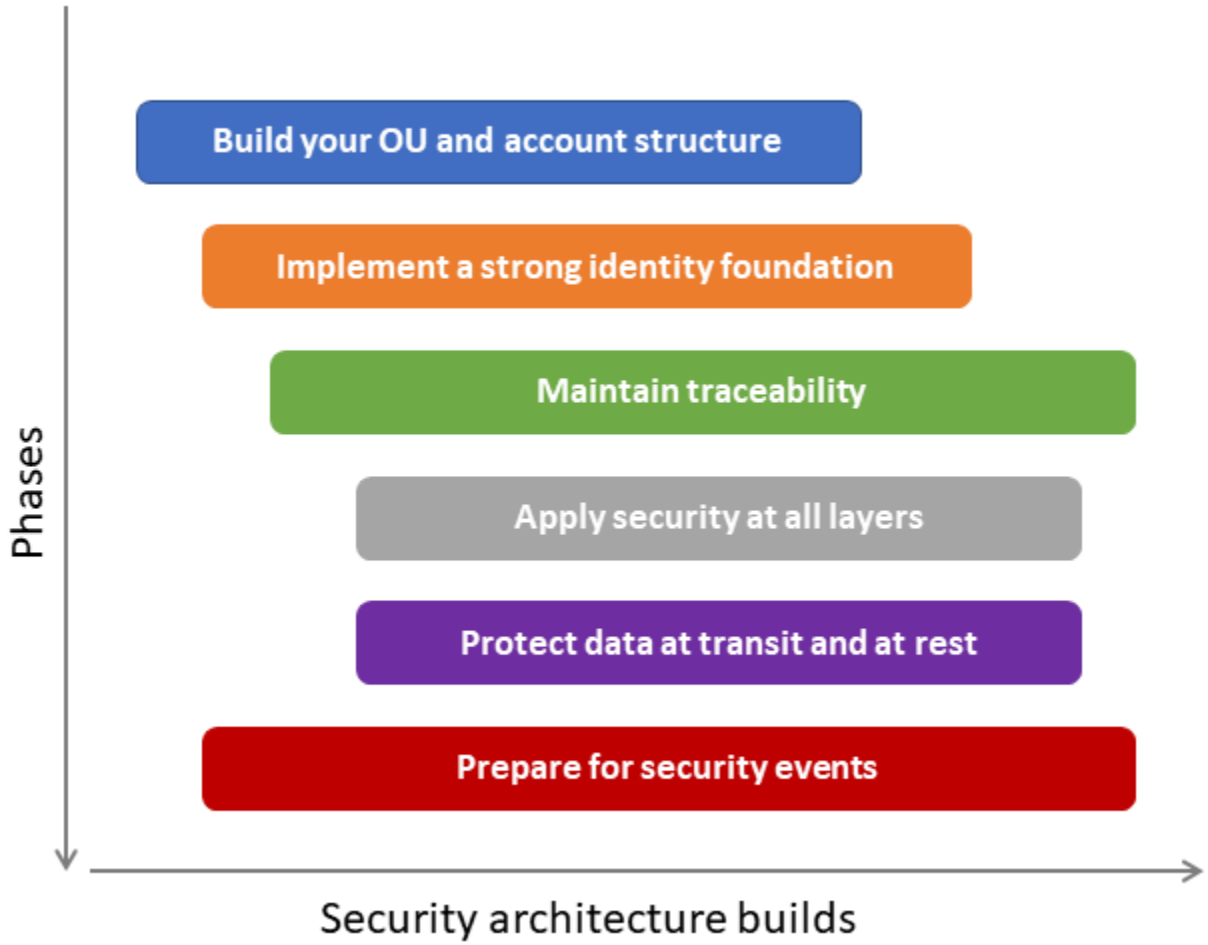
在运行 IT 环境时，您会遇到安全事件，这些事件是 IT 环境日常操作的变化，表明可能存在违反安全策略或安全控制失败的情况。适当的可追溯性至关重要，这样您才能尽快意识到安全事件。同样重要的是要做好对此类安全事件进行分类和响应的准备，以便在安全事件升级之前采取适当的措施。准备工作可帮助您快速对安全事件进行分类，以了解其潜在影响。

AWS SRA 通过设计安全工具账户并在所有账户中部署常用安全服务 AWS 账户，使您能够检测整个 AWS 组织中的安全事件。 安全工具@@ 账户中的 Amazon Detective 可帮助您对安全事件进行分类并确定根本原因。在安全调查期间，您必须能够查看相关日志，以记录和了解事件的全部范围和时间表。当发生感兴趣的特定操作时，还需要日志来生成警报。 AWS SRA 建议使用中央日志存档帐户，用于所有安全和操作日志的不可变存储。您可以使用 CloudWatch Logs Insights 查询存储在 CloudWatch 日志组中的数据，使用 Amazon Athena 和 OpenSearch 亚马逊服务查询存储在 Amazon S3 中的数据。使用 Amazon Security Lake 自动集中来自 AWS 环境、软件即服务 (SaaS) 提供商、本地和其他云提供商的安全数据。按照 AWS SRA 的规定，在 Security Tools 帐户或任何专用帐户中@@ 设置订阅者，以查询这些日志以进行调查。

AWS 安全事件响应帮助您自动执行安全事件响应、调查和修复。它提供了预先构建的行动手册和工作流程，可帮助您快速、一致地响应安全事件。启用主动响应功能后，安全事件响应将与 Security Hub CSPM 集成，并在 GuardDuty检测到安全发现时自动触发响应工作流程。该服务可帮助您在整个 AWS 组织中实现事件响应流程的标准化和自动化。如果您需要其他帮助，可以提出服务支持的案例，与 AWS 客户事件响应小组 (CIRT) 接触。

设计注意事项

- 您应该从云之旅的一开始就开始做好检测和响应安全事件的准备。为了更好地利用有限的资源，请为您的 AWS 资源分配数据和业务重要性，以便在检测到安全事件时，可以根据所涉及资源的重要性确定分类和响应的优先级。
- 如本节所述，构建云安全架构的各个阶段本质上是按顺序排列的。但是，您不必等到一个阶段完全完成后再开始下一阶段。我们建议您采用迭代方法，即开始并行处理多个阶段，并随着云安全态势的发展而逐渐发展每个阶段。当你经历不同的阶段时，你的设计将不断演变。考虑根据您的特定需求量身定制下图所示的建议顺序。



实现示例

AWS SRA 代码库提供了侦探组织的示例实现，该组织通过将管理委托给账户（例如审计或安全工具）来自动启用 Amazon Detective，并为现有和未来的 AWS Organizations 账户配置 Detective。

AWS SRA 最佳实践清单

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

本节将本指南中详细介绍的 AWS SRA 最佳实践提炼成一份清单，您可以在构建安全架构版本时遵循该清单。 AWS使用此列表作为参考点，而不是作为阅读指南的替代品。清单按以下顺序分组 AWS 服务。如果您想根据 AWS SRA 最佳实践清单以编程方式验证现有 AWS 环境，则可以使用 S RA Verify。

SRA Verify 是一款安全评估工具，可帮助您评估组织在多个地区与 AWS SRA 的一致 AWS 账户 性。它通过提供自动检查，根据 AWS SRA指南验证您的实施情况，从而直接映射到 AWS SRA建议。该工具可帮助您验证您的安全服务是否根据参考架构进行了正确配置。 它提供了详细的调查结果和可行的补救步骤，以帮助确保您的 AWS 环境遵循安全最佳实践。SRA Verify 旨在 AWS CodeBuild 在组织审计（安全工具）账户中运行。您也可以在本地运行它或使用 SRA Verify 库对其进行扩展。

> **Note**
>
> SRA Verify 包含多项服务的支票，但可能不包含针对 AWS SRA 所有考虑因素的支票。有关更多信息，请查看 AWS SRA 库中的指南。

AWS Organizations

- AWS Organizations 已启用所有功能。
- 服务控制策略 (SCPs) 用于定义 IAM 委托人的访问控制指南。
- 资源控制策略 (RCPs) 用于定义 AWS 资源的访问控制准则。
- 声明性策略用于在整个组织中大规模地集中声明和强制执行您所需的配置。 AWS 服务
- 为提供基础 OUs 服务的群组成员账户创建了三个基础账户（安全、基础设施和工作负载）。
- 安全工具帐户是在安全 OU 下创建的。此账户提供对 AWS 安全服务和其他第三方安全工具的集中管理。
- 日志存档帐户是在安全 OU 下创建的。此帐户提供了一个严格控制的中央日志存储库 AWS 服务 和应用程序日志。
- 网络账户是在基础设施 OU 下创建的。此帐户管理您的应用程序和更广泛的互联网之间的网关。它将网络服务、配置和操作与单个应用程序工作负载、安全和其他基础设施隔离开来。

- 共享服务帐户在基础架构 OU 下创建。此账户支持多个应用程序和团队用来交付成果的服务。
- 应用程序帐户是在工作负载 OU 下创建的。此账户托管运行和维护企业应用程序的主要基础设施和服务。本指南提供了一种表示方式，但在现实世界中，会有多个账户 OUs 和成员账户，按应用程序、开发环境和其他安全考虑因素进行隔离。
- 为所有成员账户配置账单、运营和安全的备用联系信息。

AWS CloudTrail

- 配置了组织跟踪，允许在 CloudTrail 管理账户和 AWS 组织中的所有成员账户中交付管理事件。
- 组织跟踪配置为多区域跟踪。
- 组织跟踪配置为从全球资源中捕获事件。
- 根据需要配置用于捕获特定数据事件的其他跟踪，以监控敏感 AWS 资源活动。
- 安全工具账户被设置为组织跟踪的委托管理员。
- 组织跟踪配置为自动为所有新成员账户启用。
- 组织跟踪配置为将日志发布到托管在日志存档账户中的集中式 S3 存储桶。
- 组织跟踪启用了日志文件验证，以验证日志文件的完整性。
- 组织跟踪与 CloudWatch 日志集成以保留日志。
- 使用客户托管密钥对组织跟踪进行加密。
- 用于日志存档账户中日志存储库的中央 S3 存储桶使用客户托管密钥进行加密。
- 日志存档账户中用于日志存储库的中央 S3 存储桶配置了 S3 对象锁以实现不可变性。
- 已为用于日志存档账户中日志存储库的中央 S3 存储桶启用版本控制。
- 用于日志存档账户中日志存储库的中央 S3 存储桶定义了资源策略，该策略仅通过资源 Amazon 资源名称 (ARN) 的组织跟踪限制对象上传。

AWS Security Hub CSPM

- Security Hub CSPM 已为所有成员账户和管理账户启用。
- AWS Config 作为 Security Hub CSPM 的先决条件，已为所有成员账户启用。
- 安全工具账户设置为 Security Hub CSPM 的委托管理员。
- Amazon GuardDuty 和 Amazon Detective 拥有与 Security Hub CSPM 相同的委托管理员账户，可实现顺畅的服务集成。

- 中央配置用于跨多个 AWS 账户 和设置和管理 Security Hub CSPM。 AWS 区域
- 所有 OU 和成员账户均由 Security Hub CSPM 的授权管理员指定为集中管理。
- 系统会自动为所有新成员账户启用 Security Hub CSPM。
- Security Hub CSPM 会自动启用，用于配置新标准。
- 来自所有区域的 Security Hub CSPM 调查结果汇总到一个主区域。
- 来自所有成员账户的 Security Hub CSPM 调查结果汇总到安全工具账户中。
- Security Hub CSPM 中的AWS 基础最佳实践 (FSBP) 标准已适用于所有成员账户。
- Security Hub CSPM 中的 CI S AWS 基金会基准测试标准已适用于所有成员账户。
- 如果适用，其他 Security Hub CSPM 标准也已启用。
- Security Hub CSPM 自动化规则用于通过资源上下文丰富调查结果。
- Security Hub CSPM 自动响应和补救功能用于创建自定义 EventBridge 规则，以便针对特定发现自动采取措施。

AWS Config

- 所有成员账户和管理账户都启用了 AWS Config 录制器。
- 所有区域都启用了 AWS Config 录制器。
- 传 AWS Config 送通道 S3 存储桶集中在日志存档账户中。
- AWS Config 委托管理员帐户设置为安全工具帐户。
- AWS Config 已设置组织聚合器。聚合器包括所有区域。
- AWS Config 一致性包将统一部署到委派管理员账户中的所有成员账户。
- AWS Config 规则发现结果会自动发送到 Security Hub CSPM。

Amazon GuardDuty

- GuardDuty 检测器已为所有成员账户和管理账户启用。
- GuardDuty 所有区域都启用了探测器。
- GuardDuty 检测器会自动为所有新成员帐户启用。
- GuardDuty 委托管理设置为安全工具帐户。
- GuardDuty CloudTrail 管理事件、VPC 流日志和 Route 53 Resolver DNS 查询日志等基础数据源已启用。

- GuardDuty S3 保护已启用。
- GuardDuty 已启用 EBS 卷的恶意软件防护。
- GuardDuty S3 的恶意软件防护已启用。
- GuardDuty RDS 保护已启用。
- GuardDuty Lambda 保护已启用。
- GuardDuty EKS 保护已启用。
- GuardDuty EKS 运行时监控已启用。
- GuardDuty 已启用扩展威胁检测。
- GuardDuty 结果将导出到日志存档帐户中的中央 S3 存储桶中进行保留。

IAM

- 不使用 IAM 用户。
- 强制对成员账户的 root 访问权限进行集中管理。
- 管理账户的集中特权 root 用户任务由授权管理员强制执行。
- 集中式根访问权限管理委托给安全工具账户。
- 所有成员账户根凭证均已删除。
- 所有成员和管理 AWS 账户 密码策略均根据组织的安全标准进行设置。
- IAM 访问顾问用于查看 IAM 群组、用户、角色和策略上次使用的信息。
- 权限边界用于限制 IAM 角色的最大可能权限。

IAM 访问分析器

- IAM Access Analyzer 已为所有成员账户和管理账户启用。
- IAM Access Analyzer 委派的管理员设置为安全工具账户。
- IAM Access Analyzer 外部访问分析器在每个区域都配置了组织信任区域。
- IAM Access Analyzer 外部访问分析器配置了每个区域的账户信任区域。
- IAM Access Analyzer 内部访问分析器配置了每个区域的组织信任区域。
- IAM Access Analyzer 内部访问分析器配置了每个区域的账户信任区域。
- 已为当前账户创建了 IAM 访问分析器未使用的访问分析器。

- 创建了当前组织的 IAM Access Analyzer 未使用的访问分析器。

Amazon Detective

- Detective 已为所有成员账户启用。
- Detective 会自动为所有新成员账户启用。
- 所有区域都启用了 Detective。
- Detective 委派的管理员设置为安全工具帐户。
- Detective GuardDuty、和 Security Hub CSPM 授权管理员设置为相同的安全工具帐户。
- Detective 与 Security Lake 集成，用于存储和分析原始日志。
- Detective 集成 GuardDuty 在一起以获取发现。
- Detective 正在摄取 Amazon EKS 审计日志进行分析。
- Detective 正在摄取 Security Hub CSPM 日志进行分析。

AWS Firewall Manager

- Firewall Manager 安全策略已设置。
- Firewall Manager 授权的管理员设置为安全工具帐户。
- AWS Config 已作为先决条件启用。
- 为每个 OU、账户和区域设置了多个 Firewall Manager 管理员，其范围受限。
- Firewall Manager AWS WAF 安全策略已定义。
- 定义了 Firew AWS WAF all Manager 集中记录策略。
- Firewall Manager Shield 高级安全策略已定义。
- 已定义 Firewall Manager 安全组安全策略。

Amazon Inspector

- 所有成员账户均已启用 Amazon Inspector。
- 任何新成员账户都会自动启用 Amazon Inspector。
- Amazon Inspector 委派的管理员设置为安全工具账户。
- Amazon Inspector EC2 漏洞扫描已启用。

- Amazon Inspector ECR 图像漏洞扫描已启用。
- Amazon Inspector Lambda 功能和层漏洞扫描已启用。
- Amazon Inspector Lambda 代码扫描已启用。
- Amazon Inspector 代码安全扫描已启用。

Amazon Macie

- 适用的成员账户已启用 Macie。
- 适用的新成员账户会自动启用 Macie。
- Macie 委派的管理员设置为安全工具帐户。
- Macie 的调查结果将导出到日志存档账户中的中央 S3 存储桶中。
- 存储 Macie 调查结果的 S3 存储桶使用客户托管密钥进行加密。
- Macie 策略和分类策略已发布到 Security Hub CSPM。

Amazon Security Lake

- Security Lake 组织配置已启用。
- Security Lake 委派的管理员设置为安全工具帐户。
- 已为新成员账户启用 Security Lake 组织配置。
- Security Tooling 账户设置为数据访问订阅者，用于对日志进行分析。
- Security Tooling 帐户设置为数据查询订阅者，用于对日志进行分析。
- 在所有或指定的活跃成员账户中，已为 Security Lake 启用 CloudTrail 管理日志源。
- 在所有或指定的活跃成员账户中，已为安全湖启用了 VPC 流日志源。
- 已在所有或指定活跃成员账户中为 Security Lake 启用了 Route 53 日志源。
- CloudTrail S3 日志源的数据事件已在所有或指定的活跃成员账户中启用 Security Lake。
- 已在所有或指定的活跃成员账户中为安全湖启用了 Lambda 执行日志源。
- 在所有或指定的活跃成员账户中，已为安全湖启用了 Amazon EKS 审核日志源。
- 在所有或指定的活跃成员账户中，Security Lake 已启用 Security Hub 发现日志源。
- 在所有或指定的活跃成员账户中，Security Lake 已启用 AWS WAF 日志源。
- 委派管理员账户中的 Security Lake SQS 队列使用客户托管密钥进行加密。
- 委派管理员账户中的 Security Lake SQS 死信队列使用客户托管密钥进行加密。

- Security Lake S3 存储桶使用客户托管密钥进行加密。
- Security Lake S3 存储桶的资源策略仅限制 Security Lake 的直接访问。

AWS WAF

- 所有 CloudFront 分布都与相关联 AWS WAF。
- 所有 Amazon API Gateway REST APIs 都与之关联 AWS WAF。
- 所有应用程序负载均衡器都与关联。 AWS WAF
- 所有 AWS AppSync GraphQL APIs 都与之关联。 AWS WAF
- 所有 Amazon Cognito 用户池都与之关联。 AWS WAF
- 所有 AWS App Runner 服务都与相关联 AWS WAF。
- 所有 AWS Verified Access 实例都与关联 AWS WAF。
- 所有 AWS Amplify 应用程序都与关联 AWS WAF。
- AWS WAF 日志记录已启用。
- AWS WAF 日志集中在日志存档账户的 S3 存储桶中。

AWS Shield Advanced

- 对于拥有面向公众的资源的所有应用程序帐户，Shield Advanced 订阅已启用，并设置为自动续订。
- Shield Advanced 已针对所有 CloudFront 发行版进行了配置。
- 为所有应用程序负载均衡器配置了 Shield Advanced。
- 为所有网络负载均衡器配置了 Shield Advanced。
- 为所有 Route 53 托管区域配置了 Shield Advanced。
- 为所有弹性 IP 地址配置了 Shield Advanced。
- 所有全球加速器都配置了 Shield Advanced。
- CloudWatch 警报是为 CloudFront 受 Shield Advanced 保护的 Route 53 资源配置的。
- Shield 响应小组 (SRT) 访问权限已配置。
- Shield 高级主动交战已启用。
- Shield 高级主动交互联系人已配置。
- Shield 高级受保护资源已配置自定义 AWS WAF 规则。
- Shield Advanced 受保护的资源已启用自动应用层 DDo S 缓解措施。

AWS 安全事件响应

- AWS 已为整个 AWS 组织启用安全事件响应。
- AWS 安全事件响应授权管理员设置为安全工具帐户。
- 主动响应和警报分类工作流程已启用。
- AWS 客户事件响应小组 (CIRT) 的遏制行动已获得授权。

AWS Audit Manager

- 所有成员账户都启用了 Audit Manager。
- Audit Manager 会自动为新成员账户启用。
- Audit Manager 委派的管理员设置为安全工具帐户。
- AWS Config 已作为 Audit Manager 的先决条件启用。
- 客户管理的密钥用于存储在 Audit Manager 中的数据。
- 已配置默认评估报告目标。

IAM 资源

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

尽管 AWS Identity and Access Management (IAM) 不是传统架构图中包含的服务，但它涉及 AWS 组织的方方面面 AWS 账户、和 AWS 服务。如果不先创建 IAM 实体并授予权限，则无法部署任何 AWS 服务 实体。对 IAM 的完整解释超出了本文档的范围，但本节提供了最佳实践建议的重要摘要以及其他资源指南。

- 有关 IAM 最佳实践，请参阅 AWS 文档中的 IAM 安全最佳实践、 AWS 安全博客中的 IAM 文章以及 re AWS : Invent 演示文稿。
- W AWS ell-Architected 安全支柱概述了权限管理流程中的关键步骤：定义权限护栏、授予最低权限访问权限、分析公共和跨账户访问权限、安全共享资源、持续减少权限以及建立紧急访问流程。
- 下表及其附注简要概述了有关可用的 IAM 权限策略类型以及如何在安全架构中使用这些策略的推荐指南。要了解更多信息，请参阅 re AWS : Invent 2020 视频，了解如何正确选择 IAM 策略组合。

用例或政策	效果	由... 管理	目的	与以下内容有关	影响	部署于
服务控制策略 (SCPs)	Restrict	中心团队，例如平台或安全团队 [1]	护栏、治理	组织、组织单位、账户	组织、OU 和账户中的所有负责人	组织管理账户 [2]
资源控制策略 (RCPs)	Restrict	中心团队，例如平台或安全团队 [1]	护栏、治理	组织、组织单位、账户	成员账号中的资源 [12]	组织管理账户 [2]
基准账户自动化策略（平台用于操作账户的 IAM 角色）	授予和限制	中央团队，例如平台、安全团队或 IAM 团队 [1]	（基准）非工作负载自动化角色的权限 [3]	单一账户 [4]	成员账户中自动化使用的委托人	成员账户

基准人工策略（授予用户执行其工作的权限的 IAM 角色）	授予和限制	中央团队，例如平台、安全团队或 IAM 团队 [1]	人类角色的权限 [5]	单一账户 [4]	联邦委托人 [5] 和 IAM 用户 [6]	成员账户
权限边界（获得授权的开发者可以分配给其他委托人的最大权限）	Restrict	中央团队，例如平台、安全团队或 IAM 团队 [1]	应用程序角色的护栏（必须使用）	单一账户 [4]	此账户中应用程序或工作负载的个人角色 [7]	成员账户
应用程序的计算机角色策略（角色附加到开发人员部署的基础架构）	授予和限制	委托给开发者 [8]	应用程序或工作负载的权限 [9]	单一账户	此账户中的本金	成员账户
资源策略	授予和限制	委托给开发者 [8,10]	资源权限	单一账户	账户中的本金 [11]	成员账户
中央根用户管理	授予和限制	中央团队，例如平台、安全团队或 IAM 团队 [1]	大规模集中管理成员账户 root 用户	Organization（组织）	成员账户中的所有 root 用户	组织管理账号、委派管理员账号

表中的注释：

1. 企业有许多集中式团队（例如云平台、安全运营或身份和访问管理团队），他们分担这些独立控制的责任，并对彼此的政策进行同行审查。表中的示例是占位符。你需要为你的企业确定最有效的职责分工。
2. 要使用 SCPs，必须启用其中的所有功能 AWS Organizations。

3. 通常需要常用的基准角色和策略来实现自动化，例如管道权限、部署工具、监控工具（例如 AWS Lambda 和 AWS Config 规则）以及其他权限。此配置通常在配置账户时交付。
4. 尽管它们与单个账户中的资源（例如角色或策略）有关，但可以通过使用AWS CloudFormation StackSets将其复制或部署到多个账户。
5. 定义一组核心的基准人类角色和策略，这些角色和策略由中央团队部署到所有成员账户（通常是在账户配置期间）。示例包括平台团队中的开发人员、IAM 团队和安全审计团队。
6. 尽可能使用联合身份验证（而不是本地 IAM 用户）。
7. 权限边界由授权的管理员使用。此 IAM 策略定义了最大权限并覆盖了其他策略（包括允许对资源进行所有操作的"*:*"策略）。在基准人工策略中应规定权限边界，以此作为创建角色（例如工作负载性能角色）和附加策略的条件。其他配置，例如 SCPs 强制附加权限边界。
8. 这假设已经部署了足够的护栏（例如， SCPs 和权限边界）。
9. 这些可选策略可以在账户配置期间交付，也可以作为应用程序开发过程的一部分交付。创建和附加这些策略的权限将由应用程序开发者自己的权限控制。
10. 除了本地账户权限外，集中式团队（例如云平台团队或安全运营团队）通常还会管理一些基于资源的策略，以启用跨账户访问权限来操作账户（例如，提供对 S3 存储桶的访问权限以进行日志记录）。
11. 基于资源的 IAM 策略可以引用任何账户中的任何委托人来允许或拒绝对其资源的访问。它甚至可以引用匿名委托人来启用公共访问权限。
12. RCPs 适用于其子集的资源 AWS 服务。有关更多信息，请参阅 AWS Organizations 文档 RCPs中的支持列表。 AWS 服务

确保 IAM 身份仅拥有一组精心划分的任务所必需的权限，对于降低恶意或无意滥用权限的风险至关重要。建立和维护最低权限模型需要制定周密的计划，以持续更新、评估和缓解超额特权。以下是该计划的一些其他建议：

- 使用贵组织的治理模式和既定的风险偏好来建立特定的防护和权限边界。
- 通过不断迭代的过程实现最低权限。这不是一次性的练习。
- 用于降低 SCPs 可操作的风险。这些措施旨在成为宽阔的护栏，而不是针对性狭窄的控制措施。
- 使用权限边界以更安全的方式委派 IAM 管理。
  - 确保委派的管理员将相应的 IAM 边界策略附加到他们创建的角色和用户。
- 作为一种 defense-in-depth方法（与基于身份的策略结合使用），使用基于资源的 IAM 策略来拒绝对资源的广泛访问。

- 使用 IAM 访问顾问 AWS CloudTrail、IAM Access Analyzer 和相关工具定期分析历史使用情况和授予的权限。立即纠正明显的过度权限。
- 在适用的情况下，将广泛的操作范围限定为特定资源，而不是使用星号作为通配符来表示所有资源。
- 实施一种机制，根据请求快速识别、审查和批准 IAM 策略异常。

AWS SRA 示例的代码存储库

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

为了帮助您开始构建和实施 AWS SRA 中的指南，本指南附带了 https://github.com/aws-samples/aws-security-reference-architecture- examples 中的基础设施即代码 (IaC) 存储库。此存储库包含的代码可帮助开发人员和工程师部署本文档中介绍的一些指导和架构模式。此代码来自 AWS 专业服务顾问与客户的第一手经验。这些模板本质上是通用的，它们的目标是说明实现模式，而不是提供完整的解决方案。 AWS 服务 配置和资源部署故意设置了非常严格的限制。您可能需要修改和定制这些解决方案以适应您的环境和安全需求。

AWS SRA 代码存储库提供了包含两者 AWS CloudFormation 和 Terraform 部署选项的代码示例。解决方案模式支持两种环境：一种需要环境 AWS Control Tower ，另一种 AWS Organizations 不支持环境 AWS Control Tower。此存储库中需要的解决方案 AWS Control Tower 已通过使用和定制 AWS Control Tower (cfCT) 在AWS Control Tower环境中进行部署 AWS CloudFormation和测试。不需要的解决方案 AWS Control Tower 已通过使用在 AWS Organizations环境中进行了测试 AWS CloudFormation。cfcT 解决方案可帮助客户根据 AWS 最佳实践快速设置安全的多账户 AWS 环境。它通过自动设置环境来运行安全和可扩展的工作负载，同时通过创建帐户和资源来实现初始安全基准，从而帮助节省时间。 AWS Control Tower 还为开始使用多账户架构、身份和访问管理、治理、数据安全、网络设计和日志记录提供了一个基准环境。 AWS SRA 存储库中的解决方案提供了额外的安全配置来实现本文档中描述的模式。

以下是 AWS SRA 存储库中解决方案的摘要。每个解决方案都包含一个包含详细信息的`README.md`文件。

- CloudTrail 组织解决方案在组织管理账户中创建组织跟踪，并将管理委托给成员账户，例如审计或安全工具账户。此跟踪使用在 Security Tools 账户中创建的客户托管密钥进行加密，并将日志传送到日志存档账户中的 S3 存储桶。或者，可以为 Amazon S3 和 AWS Lambda 函数启用数据事件。组织跟踪记录 AWS 组织 AWS 账户 中所有人的事件，同时防止成员账户修改配置。
- GuardDuty 组织解决方案 GuardDuty 通过将管理委托给安全工具账户来支持 Amazon。它在安全工具帐户 GuardDuty 中为所有现有和未来的 AWS 组织帐户进行配置。还会使用 KMS 密钥对 GuardDuty 发现结果进行加密，并发送到日志存档账户中的 S3 存储桶。
- Sec urity Hub CSPM 组织解决方案通过将管理委托给安全工具帐户来配置 Security Hub CSPM。它在安全工具帐户中为所有现有和未来的 AWS 组织帐户配置 Security Hub CSPM。该解决方案还提供了用于在所有账户和区域之间同步已启用的安全标准以及在安全工具账户中配置区域聚合器的参数。

将 Security Hub CSPM 集中在 Security Tooling 账户中，可以跨账户查看安全标准合规性以及两者 AWS 服务 与第三方集成的调查结果。 AWS Partner

- Inspector 解决方案在委托管理员（安全工具）账户中为 AWS 组织下的所有账户和受管区域配置 Amazon Inspector。
- Fi re wall Manager 解决方案通过将 AWS Firewall Manager 管理委托给安全工具帐户并使用安全组策略和多个 AWS WAF 策略配置 Firewall Manager 来配置安全策略。安全组策略要求在解决方案部署的 VPC（现有或由解决方案创建）中允许的最大安全组。
- Macie 组织解决方案通过将管理委托给安全工具账户来支持 Amazon Macie。它在安全工具帐户中为所有现有和未来的 AWS 组织帐户配置 Macie。Macie 进一步配置为将其发现结果发送到使用 KMS 密钥加密的中央 S3 存储桶。
- AWS Config:
  - Config Aggregato AWS Config r 解决方案通过将管理委托给安全工具帐户来配置聚合器。然后，该解决方案在安全工具帐户中为组织中所有现有和未来的帐户配置 AWS Config 聚合器。 AWS
  - Conformance Pack 组织规则解决方案 AWS Config 规则 通过将管理委托给安全工具帐户来部署。然后，它在委派的管理员账户中为组织中所有现有和将来的账户创建 AWS 组织合规包。该解决方案配置为部署加密和密钥管理最佳操作实践一致性包示例模板。
  - Cont AWS Config rol Tower 管理账户解决方案启用 AWS Config AWS Control Tower 管理账户，并相应地更新安全工具账户中的 AWS Config 聚合器。该解决方案使用启用 AWS Control Tower CloudFormation 模板 AWS Config 作为参考，以确保与 AWS 组织中的其他账户保持一致。
- IAM：
  - A ccess Analyzer 解决方案通过将管理委托给安全工具账户来启用 IAM Access Analyzer。然后，它在安全工具账户中为组织中所有现有和未来的账户配置组织级的 IAM Access Analyzer。 AWS 该解决方案还将 IAM Access Analyzer 部署到所有成员账户和区域，以支持分析账户级权限。
  - I AM 密码策略解决方案更新 AWS 组织中所有账户的 AWS 账户 密码策略。该解决方案提供了用于配置密码策略设置的参数，以帮助您与行业合规性标准保持一致。
- EC2 默认 EBS 加密解决方案支持在每个账户 AWS 账户 和 AWS 区域 组织内进行账户级默认 Amazon EBS 加密。 AWS 它会强制对您创建的新 EBS 卷和快照进行加密。例如，Amazon EBS 会加密您启动实例时创建的 EBS 卷以及您从未加密的快照中复制的快照。
- S3 封禁账户公共访问解决方案在组织 AWS 账户 中的每个账户内启用 Amazon S3 账户级别设置。AWS Amazon S3 屏蔽公共访问权限特征提供接入点、存储桶和账户设置，帮助您管理对 Amazon S3 资源的公有访问。默认情况下，新存储桶、接入点和对象不允许公有访问。但是，用户可以修改存储桶策略、接入点策略或对象权限以允许公有访问。Amazon S3 阻止公共访问设置会覆盖这些策略和权限，因此您可以限制对这些资源的公开访问。

- Det ec tive Organization 解决方案通过将管理委托给账户（例如审计或安全工具账户），并为所有现有和未来的 AWS Organizations 账户配置 Detective，从而自动启用 Amazon Detective。
- Shield Advanc ed 解决方案可自动部 AWS Shield Advanced 署，为您的应用程序提供增强的 DDo S 保护。 AWS
- AMI Bakery Organization 解决方案有助于自动生成和管理标准的、经过强化的 Amazon 系统映像 (AMI) 映像。这可以确保您的 AWS 实例之间的一致性和安全性，并简化部署和维护任务。
- 补丁管理器解决方案有助于简化多个补丁管理 AWS 账户。您可以使用此解决方案更新所有托管实例上的 AWS Systems Manager 代理（SSM 代理），并在带有 Windows 和 Linux 标签的实例上扫描和安装关键和重要的安全补丁和错误修复。该解决方案还配置了默认主机管理配置设置以检测新帐户的创建情况， AWS 账户 并自动将解决方案部署到这些帐户。

贡献者

主要作者：

- Avik Mukherjee，SA 高级安全 AWS

贡献者：

- AWS CIRT 高级安全调查员杰森·赫斯特
- Abhishek Panday， AWS 首席产品经理 — 科技
- Itay Meller，SA AWS 高级专家
- 乔纳森 VanKim， AWS 首席安全 SA
- Josh Du Lac， AWS 企业安全策略师
- 詹姆斯·汤普森， AWS 高级解决方案架构师
- Jeremy Girven，S AWS A 专家
- Rodney Underkoffler，SA 高级专家 AWS
- Farhan Farooq，高级解决方案架构师 AWS
- Prashob Krishnan，技术客户经理 AWS
- Meg Peddada，高级安全顾问 AWS
- Ashwin Phadke，高级解决方案架构师 AWS
- Sowjanya Rajavaram，SA 高级安全 AWS
- Tomek Jakubowski，高级顾问 AWS
- Arun Thomas， AWS 高级解决方案架构师
- 罗斯·沃伦， AWS 产品解决方案架构师
- 斯科特·康克林，高级顾问 AWS
- Ilya Epshteyn，身份解决方案 AWS 高级经理
- 迈克尔·哈肯， AWS 首席技术专家
- Mehial Mendrin，高级顾问 AWS
- 克里斯托弗·埃文森， AWS 高级技术客户经理

正在审阅：

- Eric Rose， AWS 首席安全 SA
- Manoj Kumar， AWS 交付顾问

技术写作：

- Handan Selamoglu，资深技术撰稿人 AWS

附录： AWS 安全、身份和合规服务

通过进行简短的调查来影响 AWS 安全参考架构 (AWS SRA) 的未来。

有关简介或复习内容，请参阅 AWS 网站AWS上的安全、身份和合规性，以获取可帮助您在云中保护工作负载和应用程序的列表。 AWS 服务 这些服务分为五类：数据保护、身份和访问管理、网络和应用程序保护、威胁检测和持续监控，以及合规和数据隐私。

数据保护- AWS 提供可帮助您保护数据、帐户和工作负载免遭未经授权访问的服务。

- Amazon Macie — 利用基于机器学习的安全功能发现、分类和保护敏感数据。
- AWS KMS— 创建和控制用于加密数据的密钥。
- AWS CloudHSM— 在中管理您的硬件安全模块 (HSMs) AWS Cloud。
- AWS Certificate Manager— 配置、管理和部署用于的 SSL/TLS 证书 AWS 服务。
- AWS Secrets Manager— 在数据库凭证、API 密钥和其他密钥的生命周期中轮换、管理和检索它们。

身份和访问管理 — AWS 身份服务使您能够安全地大规模管理身份、资源和权限。

- IAM — 安全地控制对 AWS 服务 资源的访问权限。
- IAM 身份中心 — 集中管理对多个应用程序 AWS 账户 和业务应用程序的 SSO 访问权限。
- Amazon Cognito — 为您的网络和移动应用程序添加用户注册、登录和访问控制。
- AWS Directory Service— 在中使用托管的 Microsoft 活动目录 AWS Cloud。
- AWS RAM— 简单安全地共享 AWS 资源。
- AWS Organizations— 对多 AWS 账户人实施基于策略的管理。
- Amazon 已验证权限 — 在您的自定义应用程序中管理可扩展、精细的权限和授权。

网络和应用程序保护 — 这些类别的服务使您能够在整个组织的网络控制点实施精细的安全策略。AWS 服务 帮助您检查和过滤流量，以帮助防止在主机级、网络级别和应用程序级边界上进行未经授权的资源访问。

- AWS Shield— 使用托管 DDo S 保护来保护运行 AWS 的 Web 应用程序。
- AWS WAF— 保护您的 Web 应用程序免受常见的 Web 漏洞攻击，并确保可用性和安全性。

- AWS Firewall Manager— 从一个中心位置配置 AWS 账户 和管理跨应用程序的 AWS WAF 规则。
- AWS Systems Manager— 配置和管理 Amazon EC2 和本地系统，以应用操作系统补丁、创建安全的系统映像和配置安全的操作系统。
- Amazon VPC — 预置一个逻辑上隔离的部分，您可以在 AWS 其中启动您定义的虚拟网络中的 AWS 资源。
- AWS Network Firewall— 为您部署基本的网络保护 VPCs。
- Amazon Route 53 DNS 防火墙 — 保护您的出站 DNS 请求免受您的攻 VPCs击。
- AWS Verified Access— 无需虚拟专用网络即可提供对应用程序的安全访问 (VPNs)。
- Amazon VPC Lattice — 简化 service-to-service连接、安全和监控。

威胁检测和持续监控 — AWS 监控和检测服务提供指导，帮助识别 AWS 环境中潜在的安全事件。

- AWS Security Hub CSPM— 从中心位置查看和管理安全警报并自动执行合规性检查。
- AWS Security Hub— 关联并丰富安全调查结果，对账户中的关键安全问题进行优先级排序，以及 AWS 区域.
- Amazon GuardDuty — 通过智能威胁检测 AWS 账户 和持续监控保护您的和工作负载。
- Amazon Inspector — 自动进行安全评估，以帮助提高部署在其上的应用程序的安全性和合规性 AWS。
- AWS Config— 记录和评估您的 AWS 资源配置，以实现合规性审计、资源变更跟踪和安全分析。
- AWS Config 规则— 创建可根据环境变化自动采取措施的规则，例如隔离资源、使用其他数据丰富事件或将配置恢复到已知的良好状态。
- AWS 安全事件响应— 利用预先构建的行动手册和工作流程，自动执行安全事件响应、调查和修复。
- AWS CloudTrail— 跟踪用户活动和 API 使用情况，以便对您的用户进行治理、运营和风险审计 AWS 账户。
- Amazon Detective — 分析和可视化安全数据，以快速找出潜在安全问题的根本原因。
- AWS Lambda— 无需预置或管理服务器即可运行代码，因此您可以扩展对事件的编程自动响应。

合规性和数据隐私 — 根据您的业务遵循 AWS 的最佳实践和行业标准，使用自动合规性检查， AWS 让您全面了解自己的合规状态，并持续监控您的环境。

- AWS Artifact— 使用免费的自助服务门户，按需访问 AWS 安全与合规报告并选择在线协议。
- AWS Audit Manager— 持续审计您的 AWS 使用情况，以简化评估风险以及对法规和行业标准的合规性的方式。

文档历史记录

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

变更	说明	日期
内容重组和更新	• 添加了 Sec urity Hub 和 AWS Nitro Enc laves 的指南。 • 重组了 AWS SRA，将重点放在核心架构上，并将深入研究部分移至身份管理、周边安全、网络取证、生成人工智能和物联网的单独指南。 • 更新了现有指南，加入了、、Amazon Detective AWS CloudTrail、 AWS Config、Amazon AWS Firewall Manager、I AM Acces GuardDuty s Analyzer、Amazon Security Lake 和的更多详细信息 AWS Audit Manager。 AWS Shield Advanced	2025年12月22日
主要更新	• 添加了有关新的 IAM 集中式根用户访问管理、资源控制策略 (RCPs) 和声明性策略的信息。 • 更新了 Security Hub CSPM 对新 Security Hub CSPM 的引用。	2025 年 8 月 29 日

	• 包括亚马逊 GuardDuty和 Sec urity Hub CSP M 的新服务功能。 • 增加了AWS 安全事件响应服务指南。 • 更新了 IAM 深入研究指南，将用于 machine-to-machine 身份管理的 VPC Lattice 包括在内。 • 添加了新的深度潜水指南：适用于物联网的 SRA。	
补充和澄清	• 在 “安全工具帐户” 部分中，更新了 AWS KMS 指南。 • 在客户身份管理部分中，扩展了有关授权 API Gateway 的信息。 • 更新了 G eneration AI 部分，添加了 OU 和账户设计的设计注意事项。 • 在 AWS SRA 代码存储库部分，添加了有关新增补程序管理解决方案的信息。	2024 年 9 月 12 日

主要更新	• 为深入研究架构指南添加了两个部分：使用 Amazon Bedrock 的生成式 AI 和身份管理。 • 使用新的服务功能更新了 AWS Identity and Access Management Access AnalyzerAmazon Detective AWS Artifact、AWS ConfigAmaz on Inspector、、、AWS Security Hub CSPM、Amazon Security Lak e 和 Amazon CloudFront 部分。 • 更新了 AWS SRA 代码存储库部分，加入了新的 Terraform 部署选项以及新增的 AWS Shield Advanced AMI Bakery 解决方案。	2024 年 6 月 7 日
主要更新	• 更新了网络账户和应用程序账户部分，添加了亚马逊验证权限和 Amazon VPC Lattice 的架构指南。 AWS Verified Access • 添加了基于安全功能的深入架构指南。 • 添加了有关如何 AWS 服务使用 AI/ML 以提供更好的安全结果的新指南。 • 添加了有关如何分阶段规划安全架构的指南。	2023年11月4日

增加安全湖	更新了安全工具账户和日志存档账户部分，添加了与 Amazon Security Lake 相关的设计指南。	2023 年 9 月 22 日
次要更新	• 更新了现有指南，以反映新的 AWS 服务 功能和最佳实践。 • 更新了 AWS CloudTrail AWS IAM Identity Center、和边缘安全的架构指南。	2023 年 5 月 10 日
调查	添加了一个简短的调查，以更好地了解您在组织中如何使用 AWS SRA。	2022 年 12 月 14 日
参考架构图的源文件	在 “AWS 安全参考架构” 部分，添加了一个下载文件，该文件以可编辑的 PowerPoint 格式提供了本指南的架构图。	2022 年 11 月 17 日
安全基础部分的更新	在安全基础部分中，更新了有关 Well-Architected Framework 支柱和安全设计原则的信息。	2022 年 9 月 27 日

主要新增内容和更新	• 添加了有关如何使用 AWS SRA 和关键实施指南的信息。 • 为其他内容（ AWS 服务 例如 Amazon Inspector AWS Artifact、Amazon Route 53、、、 AWS Control Tower AWS Audit Manager Directory Service、Amazon Cognito 和网络访问分析器）添加了架构指南。 AWS RAM • 更新了现有指南，以反映新的 AWS 服务 功能和最佳实践。	2022 年 7 月 25 日
一	初次发布	2021 年 6 月 23 日

AWS 规范性指导词汇表

以下是 AWS 规范性指导提供的策略、指南和模式中的常用术语。若要推荐词条，请使用术语表末尾的提供反馈链接。

数字

7 R

将应用程序迁移到云中的 7 种常见迁移策略。这些策略以 Gartner 于 2011 年确定的 5 R 为基础，包括以下内容：

- 重构/重新架构：充分利用云原生功能来提高敏捷性、性能和可扩展性，以迁移应用程序并修改其架构。这通常涉及到移植操作系统和数据库。示例：将本地 Oracle 数据库迁移到 Amazon Aurora PostgreSQL 兼容版。
- 更换平台：将应用程序迁移到云中，并进行一定程度的优化，以利用云功能。示例：将本地 Oracle 数据库迁移到 AWS Cloud中的 Amazon Relational Database Service（Amazon RDS）for Oracle。
- 重新购买：转换到其他产品，通常是从传统许可转向 SaaS 模式。示例：将客户关系管理（CRM）系统迁移到 Salesforce.com。
- 重新托管（直接迁移）：将应用程序迁移到云中，无需进行任何更改即可利用云功能。示例：将本地 Oracle 数据库迁移到 AWS Cloud中 EC2 实例上的 Oracle。
- 重新放置（虚拟机监控器级直接迁移）：将基础设施迁移到云中，无需购买新硬件、重写应用程序或修改现有操作。您将服务器从本地平台迁移到同一平台的云服务中。示例：将Microsoft Hyper-V应用程序迁移到 AWS。
- 保留（重访）：将应用程序保留在源环境中。其中可能包括需要进行重大重构的应用程序，并且您希望将工作推迟到以后，以及您希望保留的遗留应用程序，因为迁移它们没有商业上的理由。
- 停用：停用或删除源环境中不再需要的应用程序。

A

ABAC

请参阅基于属性的访问控制。

抽象服务

请参阅托管服务。

ACID

请参阅原子性、一致性、隔离性、持久性。

主动-主动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步（通过使用双向复制工具或双写操作），两个数据库都在迁移期间处理来自连接应用程序的事务。这种方法支持小批量、可控的迁移，而不需要一次性割接。它比主动-被动迁移更灵活，但工作量更大。

主动-被动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步，但在将数据复制到目标数据库时，只有源数据库处理来自连接应用程序的事务。目标数据库在迁移期间不接受任何事务。

聚合函数

一种 SQL 函数，它对一组行进行操作并计算该组的单个返回值。聚合函数的示例包括 SUM 和 MAX。

AI

请参阅人工智能。

AIOps

请参阅人工智能运营。

匿名化

永久删除数据集中个人信息的过程。匿名化可以帮助保护个人隐私。匿名化数据不再被视为个人数据。

反模式

一种用于解决反复出现的问题的常用解决方案，而在这类问题中，此解决方案适得其反、无效或不如替代方案有效。

应用程序控制

一种安全方法，仅允许使用经批准的应用程序，以帮助保护系统免受恶意软件的侵害。

应用程序组合

有关组织使用的每个应用程序的详细信息的集合，包括构建和维护该应用程序的成本及其业务价值。这些信息是产品组合发现和分析过程的关键，有助于识别需要进行迁移、现代化和优化的应用程序并确定其优先级。

人工智能（AI）

计算机科学领域致力于使用计算技术执行通常与人类相关的认知功能，例如学习、解决问题和识别模式。有关更多信息，请参阅什么是人工智能？

人工智能操作 (AIOps)

使用机器学习技术解决运营问题、减少运营事故和人为干预以及提高服务质量的过程。有关如何在 AIOps AWS 迁移策略中使用的更多信息，请参阅操作集成指南。

非对称加密

一种加密算法，使用一对密钥，一个公钥用于加密，一个私钥用于解密。您可以共享公钥，因为它不用于解密，但对私钥的访问应受到严格限制。

原子性、一致性、隔离性、持久性（ACID）

一组软件属性，即使在出现错误、电源故障或其他问题的情况下，也能保证数据库的数据有效性和操作可靠性。

基于属性的访问权限控制（ABAC）

根据用户属性（如部门、工作角色和团队名称）创建精细访问权限的做法。有关更多信息，请参阅 AWS Identity and Access Management (I AM) 文档 AWS中的 AB AC。

权威数据来源

存储主要数据版本的位置，被认为是最可靠的信息源。您可以将数据从权威数据来源复制到其他位置，以便处理或修改数据，例如对数据进行匿名化、编辑或假名化。

可用区

中的一个不同位置 AWS 区域 ，不受其他可用区域故障的影响，并向同一区域中的其他可用区提供低成本、低延迟的网络连接。

AWS 云采用框架 (AWS CAF)

该框架包含指导方针和最佳实践 AWS ，可帮助组织制定高效且有效的计划，以成功迁移到云端。AWS CAF将指导分为六个重点领域，称为视角：业务、人员、治理、平台、安全和运营。业务、人员和治理角度侧重于业务技能和流程；平台、安全和运营角度侧重于技术技能和流程。例如，人

员角度针对的是负责人力资源（HR）、人员配置职能和人员管理的利益相关者。从这个角度来看，AWS CAF 为人员发展、培训和沟通提供了指导，以帮助组织为成功采用云做好准备。有关更多信息，请参阅 AWS CAF 网站和 AWS CAF 白皮书。

AWS 工作负载资格框架 (AWS WQF)

一种评估数据库迁移工作负载、推荐迁移策略和提供工作估算的工具。 AWS WQF 包含在 AWS Schema Conversion Tool (AWS SCT) 中。它用来分析数据库架构和代码对象、应用程序代码、依赖关系和性能特征，并提供评测报告。

B

恶意机器人

一种旨在扰乱或伤害个人或组织的机器人。

BCP

请参阅业务连续性计划。

行为图

一段时间内资源行为和交互的统一交互式视图。您可以使用 Amazon Detective 的行为图来检查失败的登录尝试、可疑的 API 调用和类似的操作。有关更多信息，请参阅 Detective 文档中的行为图中的数据。

大端序系统

一个先存储最高有效字节的系统。另请参阅字节顺序。

二进制分类

一种预测二进制结果（两个可能的类别之一）的过程。例如，您的 ML 模型可能需要预测诸如“该电子邮件是否为垃圾邮件？”或“这个产品是书还是汽车？”之类的问题

bloom 筛选条件

一种概率性、内存高效的数据结构，用于测试元素是否为集合的成员。

蓝/绿部署

一种部署策略，您可以创建两个独立但完全相同的环境。在一个环境中运行当前应用程序版本（蓝色），在另一个环境中运行新应用程序版本（绿色）。此策略可帮助您在影响最小的情况下快速回滚。

自动程序

一种通过互联网运行自动任务并模拟人类活动或交互的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的 Web 爬网程序。还有一些被称为恶意机器人的机器人，其目的是扰乱或伤害个人或组织。

僵尸网络

被恶意软件感染并受单方（称为僵尸网络控制者或僵尸网络操作者）控制的僵尸网络。僵尸网络是最著名的扩展机器人及其影响力的机制。

分支

代码存储库的一个包含区域。在存储库中创建的第一个分支是主分支。您可以从现有分支创建新分支，然后在新分支中开发功能或修复错误。为构建功能而创建的分支通常称为功能分支。当功能可以发布时，将功能分支合并回主分支。有关更多信息，请参阅关于分支（GitHub 文档）。

紧急（break-glass）访问

在特殊情况下，通过批准的流程，用户 AWS 账户 可以快速访问他们通常没有访问权限的内容。有关更多信息，请参阅 AWS Well-Architected Guidance 中的 Implement break-glass procedures 指示器。

棕地策略

您环境中的现有基础设施。在为系统架构采用棕地策略时，您需要围绕当前系统和基础设施的限制来设计架构。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

缓冲区缓存

存储最常访问的数据的内存区域。

业务能力

企业如何创造价值（例如，销售、客户服务或营销）。微服务架构和开发决策可以由业务能力驱动。有关更多信息，请参阅在 AWS上运行容器化微服务白皮书中的围绕业务能力进行组织部分。

业务连续性计划（BCP）

一项计划，旨在应对大规模迁移等破坏性事件对运营的潜在影响，并使企业能够快速恢复运营。

C

CAF

请参阅 AWS 云采用框架。

金丝雀部署

缓慢而渐进地向最终用户发布版本。当您确信无误后，即可部署新版本，并完全替换当前版本。

CCoE

请参阅云卓越中心。

CDC

请参阅更改数据捕获。

更改数据捕获（CDC）

跟踪数据来源（如数据库表）的更改并记录有关更改的元数据的过程。您可以将 CDC 用于各种目的，例如审计或复制目标系统中的更改以保持同步。

混沌工程

故意引入故障或破坏性事件来测试系统的韧性。您可以使用 AWS Fault Injection Service (AWS FIS) 来执行实验，对您的 AWS 工作负载施加压力并评估其响应。

CI/CD

请参阅持续集成和持续交付。

分类

一种有助于生成预测的分类流程。分类问题的 ML 模型预测离散值。离散值始终彼此不同。例如，一个模型可能需要评估图像中是否有汽车。

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心 (CCoE)

一个多学科团队，负责推动整个组织的云采用工作，包括开发云最佳实践、调动资源、制定迁移时间表、领导组织完成大规模转型。有关更多信息，请参阅 AWS Cloud 企业战略博客上的 CCoE 帖子。

云计算

通常用于远程数据存储和 IoT 设备管理的云技术。云计算通常连接到边缘计算技术。

云运营模型

在 IT 组织中，一种用于构建、完善和优化一个或多个云环境的运营模型。有关更多信息，请参阅构建您的云运营模型。

云采用阶段

组织迁移到 AWS Cloud中时通常会经历四个阶段：

- 项目 - 出于概念验证和学习目的，开展一些与云相关的项目
- 基础 — 进行基础投资以扩大云采用率（例如，创建着陆区、定义 CCo E、建立运营模型）
- 迁移 - 迁移单个应用程序
- 重塑 - 优化产品和服务，在云中创新

Stephen Orban在 AWS Cloud 企业战略博客的博客文章《云优先之旅和采用阶段》中定义了这些阶段。有关它们与 AWS 迁移策略的关系的信息，请参阅迁移准备指南。

CMDB

请参阅配置管理数据库。

代码存储库

通过版本控制过程存储和更新源代码和其他资产（如文档、示例和脚本）的位置。常见的云存储库包括 GitHub 或 Bitbucket Cloud。每个版本的代码都称为一个分支。在微服务结构中，每个存储库都专门用于一个功能。单个 CI/CD 管线可以使用多个存储库。

冷缓存

一种空的、填充不足或包含过时或不相关数据的缓冲区缓存。这会影响性能，因为数据库实例必须从主内存或磁盘读取，这比从缓冲区缓存读取要慢。

冷数据

很少访问的数据，且通常是历史数据。查询此类数据时，通常可以接受慢速查询。将这些数据转移到性能较低且成本更低的存储层或类别可以降低成本。

计算机视觉（CV）

一种 AI 领域，它使用机器学习来分析和提取数字图像和视频等视觉格式中的信息。例如，Amazon SageMaker AI 为 CV 提供了图像处理算法。

配置偏移

对于工作负载而言，一种偏离预期状态的配置更改。这可能会导致工作负载变得不合规，且通常是渐进的，不是故意的。

配置管理数据库（CMDB）

一种存储库，用于存储和管理有关数据库及其 IT 环境的信息，包括硬件和软件组件及其配置。您通常在迁移的产品组合发现和分析阶段使用来自 CMDB 的数据。

合规性包

一系列 AWS Config 规则和补救措施，您可以汇编这些规则和补救措施，以自定义您的合规性和安全性检查。您可以使用 YAML 模板将一致性包作为单个实体部署在 AWS 账户 和区域或整个组织中。有关更多信息，请参阅 AWS Config 文档中的一致性包。

持续集成和持续交付（CI/CD）

自动执行软件发布过程的源代码、构建、测试、暂存和生产阶段的过程。 CI/CD 通常被描述为管道。 CI/CD 可以帮助您实现流程自动化、提高生产力、提高代码质量和更快地交付。有关更多信息，请参阅持续交付的优势。CD 也可以表示持续部署。有关更多信息，请参阅持续交付与持续部署。

CV

请参阅计算机视觉。

D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

根据网络中数据的关键性和敏感性对其进行识别和分类的过程。它是任何网络安全风险管理策略的关键组成部分，因为它可以帮助您确定对数据的适当保护和保留控制。数据分类是 Well-Architecte AWS d Framework 中安全支柱的一个组成部分。有关详细信息，请参阅数据分类。

数据漂移

生产数据与用来训练机器学习模型的数据之间的有意义差异，或者输入数据随时间推移的有意义变化。数据漂移可能降低机器学习模型预测的整体质量、准确性和公平性。

传输中数据

在网络中主动移动的数据，例如在网络资源之间移动的数据。

数据网格

一种架构框架，可提供分布式、去中心化的数据所有权以及集中式管理和治理。

数据最少化

仅收集并处理绝对必要数据的原则。在中进行数据最小化 AWS Cloud 可以降低隐私风险、成本和分析碳足迹。

数据边界

AWS 环境中的一组预防性防护措施，可帮助确保只有可信身份才能访问来自预期网络的可信资源。有关更多信息，请参阅在上构建数据边界。 AWS

数据预处理

将原始数据转换为 ML 模型易于解析的格式。预处理数据可能意味着删除某些列或行，并处理缺失、不一致或重复的值。

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

一种支持商业智能（例如分析）的数据管理系统。数据仓库通常包含大量历史数据，通常用于查询和分析。

数据库定义语言（DDL）

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言（DML）

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

请参阅数据库定义语言。

深度融合

组合多个深度学习模型进行预测。您可以使用深度融合来获得更准确的预测或估算预测中的不确定性。

深度学习

一个 ML 子字段使用多层人工神经网络来识别输入数据和感兴趣的目标变量之间的映射。

defense-in-depth

一种信息安全方法，经过深思熟虑，在整个计算机网络中分层实施一系列安全机制和控制措施，以保护网络及其中数据的机密性、完整性和可用性。当你采用这种策略时 AWS，你会在 AWS

Organizations 结构的不同层面添加多个控件来帮助保护资源。例如，一种 defense-in-depth方法可以结合多因素身份验证、网络分段和加密。

委派管理员

在中 AWS Organizations，兼容的服务可以注册 AWS 成员帐户来管理组织的帐户并管理该服务的权限。此账户被称为该服务的委托管理员。有关更多信息和兼容服务列表，请参阅 AWS Organizations 文档中使用 AWS Organizations的服务。

部署

使应用程序、新功能或代码修复在目标环境中可用的过程。部署涉及在代码库中实现更改，然后在应用程序的环境中构建和运行该代码库。

开发环境

请参阅环境。

侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出提醒。这些控制是第二道防线，提醒您注意绕过现有预防性控制的安全事件。有关更多信息，请参阅在 AWS上实施安全控制中的侦测性控制。

开发价值流映射（DVSM）

用于识别对软件开发生命周期中的速度和质量产生不利影响的限制因素并确定其优先级的流程。DVSM 扩展了最初为精益生产实践设计的价值流映射流程。其重点关注在软件开发过程中创造和转移价值所需的步骤和团队。

数字孪生

真实世界系统的虚拟再现，如建筑物、工厂、工业设备或生产线。数字孪生支持预测性维护、远程监控和生产优化。

维度表

星型架构中的一种较小的表，其中包含事实表中定量数据的数据属性。维度表属性通常是文本字段或行为类似于文本的离散数字。这些属性通常用于查询约束、筛选和结果集标注。

灾难

阻止工作负载或系统在其主要部署位置实现其业务目标的事件。这些事件可能是自然灾害、技术故障或人为操作的结果，例如无意的配置错误或恶意软件攻击。

灾难恢复（DR）

您用来最大程度地减少由灾难造成的停机时间和数据丢失的策略和流程。有关更多信息，请参阅 Well-Architected Fr ame AWS work 中的 “工作负载灾难恢复：云端 AWS 恢复”。

DML

请参阅数据库操作语言。

领域驱动设计

一种开发复杂软件系统的方法，通过将其组件连接到每个组件所服务的不断发展的领域或核心业务目标。Eric Evans 在其著作领域驱动设计：软件核心复杂性应对之道（Boston: Addison-Wesley Professional, 2003）中介绍了这一概念。有关如何将领域驱动设计与 strangler fig 模式结合使用的信息，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

DR

请参阅灾难恢复。

偏差检测

跟踪与基准配置的偏差。例如，您可以使用 AWS CloudFormation 来检测系统资源中的偏差，也可以使用 AWS Control Tower 来检测着陆区中可能影响监管要求合规性的变化。

DVSM

请参阅开发价值流映射。

E

EDA

请参阅探索性数据分析。

EDI

请参阅电子数据交换。

边缘计算

该技术可提高位于 IoT 网络边缘的智能设备的计算能力。与云计算比较时，边缘计算可以减少通信延迟并缩短响应时间。

电子数据交换（EDI）

组织之间业务文件的自动交换。有关更多信息，请参阅什么是电子数据交换。

加密

一种将人类可读的纯文本数据转换为加密文字的计算流程。

加密密钥

由加密算法生成的随机位的加密字符串。密钥的长度可能有所不同，而且每个密钥都设计为不可预测且唯一。

字节顺序

字节在计算机内存中的存储顺序。大端序系统先存储最高有效字节。小端序系统先存储最低有效字节。

端点

请参阅服务端点。

端点服务

一种可以在虚拟私有云（VPC）中托管，与其他用户共享的服务。您可以使用其他 AWS 账户 或 AWS Identity and Access Management (IAM) 委托人创建终端节点服务， AWS PrivateLink 并向其授予权限。这些账户或主体可通过创建接口 VPC 端点来私密地连接到您的端点服务。有关更多信息，请参阅 Amazon Virtual Private Cloud（Amazon VPC）文档中的创建端点服务。

企业资源规划（ERP）

一种自动化和管理企业关键业务流程（例如会计、MES 和项目管理）的系统。

信封加密

用另一个加密密钥对加密密钥进行加密的过程。有关更多信息，请参阅 AWS Key Management Service (AWS KMS) 文档中的信封加密。

环境

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

- 开发环境 — 正在运行的应用程序的实例，只有负责维护应用程序的核心团队才能使用。开发环境用于测试更改，然后再将其提升到上层环境。这类环境有时称为测试环境。
- 下层环境 — 应用程序的所有开发环境，比如用于初始构建和测试的环境。

- 生产环境 — 最终用户可以访问的正在运行的应用程序的实例。在 CI/CD 管道中，生产环境是最后一个部署环境。
- 上层环境 — 除核心开发团队以外的用户可以访问的所有环境。这可能包括生产环境、预生产环境和用户验收测试环境。

epic

在敏捷方法学中，有助于组织工作和确定优先级的功能类别。epics 提供了对需求和实施任务的总体描述。例如， AWS CAF 安全史诗包括身份和访问管理、侦探控制、基础设施安全、数据保护和事件响应。有关 AWS 迁移策略中 epics 的更多信息，请参阅计划实施指南。

ERP

请参阅企业资源规划。

探索性数据分析（EDA）

分析数据集以了解其主要特征的过程。您收集或汇总数据，并进行初步调查，以发现模式、检测异常并检查假定情况。EDA 通过计算汇总统计数据和创建数据可视化得以执行。

F

事实表

星型架构中的中心表。它存储有关业务运营的定量数据。通常，事实表包含两种类型的列：包含度量的列和包含维度表外键的列。

快速失效机制

一种使用频繁且增量式的测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

在中 AWS Cloud，诸如可用区 AWS 区域、控制平面或数据平面之类的边界，它限制了故障的影响并有助于提高工作负载的弹性。有关更多信息，请参阅 AWS 故障隔离边界。

功能分支

请参阅分支。

特征

您用来进行预测的输入数据。例如，在制造环境中，特征可能是定期从生产线捕获的图像。

特征重要性

特征对于模型预测的重要性。这通常表示为数值分数，可以通过各种技术进行计算，例如 Shapley 加法解释（SHAP）和积分梯度。有关更多信息，请参阅使用机器学习模型的可解释性 AWS。

功能转换

为 ML 流程优化数据，包括使用其他来源丰富数据、扩展值或从单个数据字段中提取多组信息。这使得 ML 模型能从数据中获益。例如，如果您将“2021-05-27 00:15:37”日期分解为“2021”、“五月”、“星期四”和“15”，则可以帮助学习与不同数据成分相关的算法学习精细模式。

少样本提示

在要求 LLM 执行类似任务之前，先向其提供少量示例，以演示任务和预期输出。此技术是上下文内学习的一种应用，其中模型可以从提示中嵌入的示例（样本）中学习。对于需要特定格式、推理或领域知识的任务，少样本提示可能非常有效。另请参阅零样本提示。

FGAC

请参阅精细访问控制。

精细访问控制（FGAC）

使用多个条件允许或拒绝访问请求。

快闪迁移

一种数据库迁移方法，通过更改数据捕获使用连续数据复制，在极短的时间内迁移数据，而非使用分阶段方法。目标是将停机时间降至最低。

FM

请参阅基础模型。

基础模型（FM）

一个大型深度学习神经网络，一直在广义和未标记数据的大量数据集上进行训练。 FMs 能够执行各种各样的一般任务，例如理解语言、生成文本和图像以及用自然语言进行对话。有关更多信息，请参阅什么是基础模型。

G

生成式人工智能

AI 模型的一个子集，这些模型已经过大量数据训练，可以使用简单的文本提示来创建新的内容和构件，例如图像、视频、文本和音频。有关更多信息，请参阅什么是生成式人工智能。

地理阻止

请参阅地理限制。

地理限制（地理阻止）

在 Amazon 中 CloudFront，一种阻止特定国家/地区的用户访问内容分发的选项。您可以使用允许列表或阻止列表来指定已批准和已禁止的国家/地区。有关更多信息，请参阅 CloudFront 文档中的限制内容的地理分布。

GitFlow 工作流程

一种方法，在这种方法中，下层和上层环境在源代码存储库中使用不同的分支。Gitflow 工作流程被认为是传统的工作流程，而基于中继的工作流程则是现代的、首选的方法。

黄金映像

系统或软件的快照，用作部署该系统或软件的新实例的模板。例如，在制造业中，黄金映像可用于在多个设备上预调配软件，并有助于提高设备制造操作的速度、可扩展性和生产效率。

全新策略

在新环境中缺少现有基础设施。在对系统架构采用全新策略时，您可以选择所有新技术，而不受对现有基础设施（也称为棕地）兼容性的限制。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

防护机制

帮助管理各组织单位的资源、策略和合规性的高级规则 (OUs)。预防性防护机制会执行策略以确保符合合规性标准。它们是使用服务控制策略和 IAM 权限边界实现的。侦测性护栏会检测策略违规和合规性问题，并生成提醒以进行修复。它们通过使用 AWS Config、、Amazon、 AWS Security Hub CSPM GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

H

HA

请参阅高可用性。

异构数据库迁移

将源数据库迁移到使用不同数据库引擎的目标数据库（例如，从 Oracle 迁移到 Amazon Aurora）。异构迁移通常是重新架构工作的一部分，而转换架构可能是一项复杂的任务。AWS 提供了 AWS SCT 来帮助实现架构转换。

高可用性（HA）

在遇到挑战或灾难时，工作负载无需干预即可连续运行的能力。HA 系统旨在自动进行故障转移、持续提供良好性能，并以最小的性能影响处理不同负载和故障。

历史数据库现代化

一种用于实现运营技术（OT）系统现代化和升级以更好满足制造业需求的方法。历史数据库是一种用于收集和存储工厂中各种来源数据的数据库。

保留数据

从用于训练机器学习模型的数据集中保留的一部分标注的历史数据。通过将模型预测与保留数据进行比较，您可以使用保留数据来评估模型性能。

同构数据库迁移

将源数据库迁移到共享同一数据库引擎的目标数据库（例如，从 Microsoft SQL Server 迁移到 Amazon RDS for SQL Server）。同构迁移通常是更换主机或更换平台工作的一部分。您可以使用本机数据库实用程序来迁移架构。

热数据

经常访问的数据，例如实时数据或近期的转化数据。这些数据通常需要高性能存储层或存储类别才能提供快速的查询响应。

修补程序

针对生产环境中关键问题的紧急修复。由于其紧迫性，修补程序通常是在典型的 DevOps 发布工作流程之外进行的。

hypercare 周期

割接之后，迁移团队立即管理和监控云中迁移的应用程序以解决任何问题的时间段。通常，这个周期持续 1-4 天。在 hypercare 周期结束时，迁移团队通常会将应用程序的责任移交给云运营团队。

我

IaC

请参阅基础设施即代码。

基于身份的策略

附加到一个或多个 IAM 委托人的策略，用于定义他们在 AWS Cloud 环境中的权限。

空闲应用程序

90 天内平均 CPU 和内存使用率在 5% 到 20% 之间的应用程序。在迁移项目中，通常会停用这些应用程序或将其保留在本地。

IIoT

请参阅工业物联网。

不可变基础设施

一种模型，可为生产工作负载部署新的基础设施，而不是更新、修补或修改现有基础设施。不可变基础设施本质上比可变基础设施更一致、更可靠、更可预测。有关更多信息，请参阅 AWS Well-Architected Framework 中的使用不可变基础设施进行部署最佳实践。

入站（入口）VPC

在 AWS 多账户架构中，一种接受、检查和路由来自应用程序外部的网络连接的 VPC。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查， VPCs 以保护您的应用程序与更广泛的互联网之间的双向接口。

增量迁移

一种割接策略，在这种策略中，您可以将应用程序分成小部分进行迁移，而不是一次性完整割接。例如，您最初可能只将几个微服务或用户迁移到新系统。在确认一切正常后，您可以逐步迁移其他微服务或用户，直到停用遗留系统。这种策略降低了大规模迁移带来的风险。

工业 4.0

该术语由 Klaus Schwab 在 2016 年提出，指的是通过连接、实时数据、自动化、分析和 AI/ML 的进步来实现制造流程的现代化。

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码（IaC）

通过一组配置文件预调配和管理应用程序基础设施的过程。IaC 旨在帮助您集中管理基础设施、实现资源标准化和快速扩展，使新环境具有可重复性、可靠性和一致性。

工业物联网 (IIoT)

在工业领域使用联网的传感器和设备，例如制造业、能源、汽车、医疗保健、生命科学和农业。有关更多信息，请参阅制定工业物联网 (IIoT) 数字化转型战略。

检查 VPC

在 AWS 多账户架构中，一种集中式 VPC，用于管理对 VPCs（相同或不同 AWS 区域）、互联网和本地网络之间的网络流量的检查。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查， VPCs 以保护您的应用程序与更广泛的互联网之间的双向接口。

物联网（IoT）

由带有嵌入式传感器或处理器的连接物理对象组成的网络，这些传感器或处理器通过互联网或本地通信网络与其他设备和系统进行通信。有关更多信息，请参阅什么是 IoT？

可解释性

它是机器学习模型的一种特征，描述了人类可以理解模型的预测如何取决于其输入的程度。有关更多信息，请参阅使用机器学习模型的可解释性 AWS。

物联网

请参阅物联网。

IT 信息库（ITIL）

提供 IT 服务并使这些服务符合业务要求的一套最佳实践。ITIL 是 ITSM 的基础。

IT 服务管理（ITSM）

为组织设计、实施、管理和支持 IT 服务的相关活动。有关将云运营与 ITSM 工具集成的信息，请参阅运营集成指南。

ITIL

请参阅 IT 信息库。

ITSM

请参阅 IT 服务管理。

L

基于标签的访问控制（LBAC）

强制访问控制（MAC）的一种实施方式，其中明确为用户和数据本身分配了安全标签值。用户安全标签和数据安全标签之间的交集决定了用户可以看到哪些行和列。

登录区

landing zone 是一个架构精良的多账户 AWS 环境，具有可扩展性和安全性。这是一个起点，您的组织可以从这里放心地在安全和基础设施环境中快速启动和部署工作负载和应用程序。有关登录区的更多信息，请参阅设置安全且可扩展的多账户 AWS 环境。

大语言模型（LLM）

一种基于大量数据进行预训练的深度学习 AI 模型。LLM 可以执行多项任务，例如回答问题、总结文档、将文本翻译成其他语言以及完成句子。有关更多信息，请参阅什么是 LLMs。

大规模迁移

迁移 300 台或更多服务器。

LBAC

请参阅基于标签的访问控制。

最低权限

授予执行任务所需的最低权限的最佳安全实践。有关更多信息，请参阅 IAM 文档中的应用最低权限许可。

直接迁移

请参阅 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参阅字节顺序。

LLM

请参阅大型语言模型。

下层环境

请参阅环境。

M

机器学习（ML）

一种使用算法和技术进行模式识别和学习的人工智能。ML 对记录的数据（例如物联网（IoT）数据）进行分析和学习，以生成基于模式的统计模型。有关更多信息，请参阅机器学习。

主分支

请参阅分支。

恶意软件

旨在危害计算机安全或隐私的软件。恶意软件可能会破坏计算机系统、泄露敏感信息或获得未经授权的访问权限。恶意软件的示例包括病毒、蠕虫、勒索软件、木马、间谍软件和键盘记录器。

托管式服务

AWS 服务 它 AWS 运行基础设施层、操作系统和平台，您可以访问端点来存储和检索数据。Amazon Simple Storage Service（Amazon S3）和 Amazon DynamoDB 就是托管服务的示例。这些服务也称为抽象服务。

制造执行系统（MES）

一种软件系统，用于跟踪、监控、记录和控制在车间将原材料转化为成品的生产过程。

MAP

请参阅迁移加速计划。

机制

一个完整的过程，您可以在其中创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运作过程中自我强化和改善的循环。有关更多信息，请参阅在 Well-Architect AWS ed 框架中构建机制。

成员账户

AWS 账户 除属于组织中的管理账户之外的所有账户 AWS Organizations。一个账户一次只能是一个组织的成员。

MES

请参阅制造执行系统。

消息队列遥测传输（MQTT）

一种基于发布/订阅模式的轻量级 machine-to-machine (M2M) 通信协议，适用于资源受限的物联网设备。

微服务

一种小型的独立服务，通过明确的定义进行通信 APIs ，通常由小型的独立团队拥有。例如，保险系统可能包括映射到业务能力（如销售或营销）或子域（如购买、理赔或分析）的微服务。微服务

的好处包括敏捷、灵活扩展、易于部署、可重复使用的代码和恢复能力。有关更多信息，请参阅使用 AWS 无服务器服务集成微服务。

微服务架构

一种使用独立组件构建应用程序的方法，这些组件将每个应用程序进程作为微服务运行。这些微服务使用轻量级通过定义明确的接口进行通信。 APIs该架构中的每个微服务都可以更新、部署和扩展，以满足对应用程序特定功能的需求。有关更多信息，请参阅在上实现微服务。 AWS

迁移加速计划（MAP）

AWS 该计划提供咨询支持、培训和服务，以帮助组织为迁移到云奠定坚实的运营基础，并帮助抵消迁移的初始成本。MAP 提供了一种以系统的方式执行遗留迁移的迁移方法，以及一套用于自动执行和加速常见迁移场景的工具。

大规模迁移

将大部分应用程序组合分波迁移到云中的过程，在每一波中以更快的速度迁移更多应用程序。本阶段使用从早期阶段获得的最佳实践和经验教训，实施由团队、工具和流程组成的迁移工厂，通过自动化和敏捷交付简化工作负载的迁移。这是 AWS 迁移策略的第三阶段。

迁移工厂

跨职能团队，通过自动化、敏捷的方法简化工作负载迁移。迁移工厂团队通常包括运营、业务分析师和所有者、迁移工程师、开发人员和从事冲刺工作的 DevOps 专业人员。20% 到 50% 的企业应用程序组合由可通过工厂方法优化的重复模式组成。有关更多信息，请参阅本内容集中有关迁移工厂的讨论和云迁移工厂指南。

迁移元数据

有关完成迁移所需的应用程序和服务器的信息。每种迁移模式都需要一套不同的迁移元数据。迁移元数据的示例包括目标子网、安全组和 AWS 账户。

迁移模式

一种可重复的迁移任务，详细列出了迁移策略、迁移目标以及所使用的迁移应用程序或服务。示例：使用 AWS 应用程序迁移服务重新托管向 Amazon EC2 的迁移。

迁移组合评测（MPA）

一种在线工具，提供了用于验证迁移到 AWS Cloud的业务案例的信息。MPA 提供了详细的组合评测（服务器规模调整、定价、TCO 比较、迁移成本分析）以及迁移计划（应用程序数据分析和数据收集、应用程序分组、迁移优先级排序和波次规划）。所有 AWS 顾问和 APN 合作伙伴顾问均可免费使用 MPA 工具（需要登录）。

迁移准备情况评测（MRA）

使用 AWS CAF 深入了解组织的云就绪状态、确定优势和劣势以及制定行动计划以缩小已发现差距的过程。有关更多信息，请参阅迁移准备指南。MRA 是 AWS 迁移策略的第一阶段。

迁移策略

将工作负载迁移到 AWS Cloud的方法。有关更多信息，请参见术语表中的 7 R 词条，以及动员您的组织以加快大规模迁移。

ML

请参阅机器学习。

现代化

将过时的（原有的或单体）应用程序及其基础设施转变为云中敏捷、弹性和高度可用的系统，以降低成本、提高效率和利用创新。有关更多信息，请参阅在 AWS Cloud中实现应用程序现代化的策略。

现代化准备情况评估

一种评估方式，有助于确定组织应用程序的现代化准备情况；确定收益、风险和依赖关系；确定组织能够在多大程度上支持这些应用程序的未来状态。评估结果是目标架构的蓝图、详细说明现代化进程发展阶段和里程碑的路线图以及解决已发现差距的行动计划。有关更多信息，请参阅在 AWS Cloud中评估应用程序的现代化准备情况。

单体应用程序（单体式）

作为具有紧密耦合进程的单个服务运行的应用程序。单体应用程序有几个缺点。如果某个应用程序功能的需求激增，则必须扩展整个架构。随着代码库的增长，添加或改进单体应用程序的功能也会变得更加复杂。若要解决这些问题，可以使用微服务架构。有关更多信息，请参阅将单体分解为微服务。

MPA

请参阅迁移组合评测。

MQTT

请参阅消息队列遥测传输。

多分类器

一种帮助为多个类别生成预测（预测两个以上结果之一）的过程。例如，ML 模型可能会询问“这个产品是书、汽车还是手机？”或“此客户最感兴趣什么类别的产品？”

可变基础设施

一种用于更新和修改生产工作负载的现有基础设施的模型。为了提高一致性、可靠性和可预测性，Well-Architect AWS ed Framework 建议使用不可变基础设施作为最佳实践。

O

OAC

请参阅来源访问控制。

OAI

请参阅来源访问身份。

OCM

请参阅组织变革管理。

离线迁移

一种迁移方法，在这种方法中，源工作负载会在迁移过程中停止运行。这种方法会延长停机时间，通常用于小型非关键工作负载。

OI

请参阅运营集成。

OLA

请参阅运营级别协议。

在线迁移

一种迁移方法，在这种方法中，源工作负载无需离线即可复制到目标系统。在迁移过程中，连接工作负载的应用程序可以继续运行。这种方法的停机时间为零或最短，通常用于关键生产工作负载。

OPC-UA

请参阅开放流程通信 – 统一架构。

开放流程通信 – 统一架构（OPC-UA）

一种用于工业自动化的 machine-to-machine（M2M）通信协议。OPC-UA 提供了一个包含数据加密、身份验证和授权方案的互操作性标准。

运营级别协议（OLA）

一项协议，阐明了 IT 职能部门承诺相互交付的内容，以支持服务水平协议（SLA）。

运营准备情况审查（ORR）

一份问题核对清单和关联的最佳实践，可帮助您了解、评估、预防或缩小事件和可能的故障的范围。有关更多信息，请参阅 AWS Well-Architected Framework 中的运营准备情况审查（ORR）。

运营技术（OT）

与物理环境配合使用以控制工业运营、设备和基础设施的硬件和软件系统。在制造业中，OT 和信息技术（IT）系统的集成是工业 4.0 转型的关键重点。

运营整合（OI）

在云中实现运营现代化的过程，包括就绪计划、自动化和集成。有关更多信息，请参阅运营整合指南。

组织跟踪

由 AWS CloudTrail 此创建的跟踪记录组织 AWS 账户 中所有人的所有事件 AWS Organizations。该跟踪是在每个 AWS 账户 中创建的，属于组织的一部分，并跟踪每个账户的活动。有关更多信息，请参阅 CloudTrail文档中的为组织创建跟踪。

组织变革管理（OCM）

一个从人员、文化和领导力角度管理重大、颠覆性业务转型的框架。OCM 通过加快变革采用、解决过渡问题以及推动文化和组织变革，帮助组织为新系统和战略做好准备和过渡。在 AWS 迁移策略中，该框架被称为人员加速，因为云采用项目需要变更的速度。有关更多信息，请参阅 OCM 指南。

来源访问控制（OAC）

在中 CloudFront，一个增强的选项，用于限制访问以保护您的亚马逊简单存储服务 (Amazon S3) 内容。OAC 全部支持所有 S3 存储桶 AWS 区域、使用 AWS KMS (SSE-KMS) 进行服务器端加密，以及对 S3 存储桶的动态PUT和DELETE请求。

来源访问身份（OAI）

在中 CloudFront，一个用于限制访问权限以保护您的 Amazon S3 内容的选项。当您使用 OAI 时，CloudFront 会创建一个 Amazon S3 可以对其进行身份验证的委托人。经过身份验证的委托人只能通过特定 CloudFront 分配访问 S3 存储桶中的内容。另请参阅 OAC，其中提供了更精细和增强的访问控制。

ORR

请参阅运营准备情况审查。

OT

请参阅运营技术。

出站（出口）VPC

在 AWS 多账户架构中，一种处理从应用程序内部启动的网络连接的 VPC。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查， VPCs 以保护您的应用程序与更广泛的互联网之间的双向接口。

P

权限边界

附加到 IAM 主体的 IAM 管理策略，用于设置用户或角色可以拥有的最大权限。有关更多信息，请参阅 IAM 文档中的权限边界。

个人身份信息（PII）

直接查看其他相关数据或与之配对时可用于合理推断个人身份的信息。PII 的示例包括姓名、地址和联系信息。

PII

请参阅个人身份信息。

playbook

一套预定义的步骤，用于捕获与迁移相关的工作，例如在云中交付核心运营功能。playbook 可以采用脚本、自动化运行手册的形式，也可以是操作现代化环境所需的流程或步骤的摘要。

PLC

请参阅可编程逻辑控制器。

PLM

请参阅产品生命周期管理。

policy

一个对象，可以定义权限（请参阅基于身份的策略）、指定访问条件（请参阅基于资源的策略）或定义 AWS Organizations 的组织中所有账户的最大权限（请参阅服务控制策略）。

多语言持久性

根据数据访问模式和其他要求，独立选择微服务的数据存储技术。如果您的微服务采用相同的数据存储技术，它们可能会遇到实现难题或性能不佳。如果微服务使用最适合其需求的数据存储，则可以更轻松地实现微服务，并获得更好的性能和可扩展性。

组合评测

一个发现、分析和确定应用程序组合优先级以规划迁移的过程。有关更多信息，请参阅评估迁移准备情况。

谓词

返回 `true` 或 `false` 的查询条件，通常位于 `WHERE` 子句中。

谓词下推

一种数据库查询优化技术，可在传输之前筛选查询中的数据。这将减少从关系数据库检索和处理的数据量，并提高查询性能。

预防性控制

一种安全控制，旨在防止事件发生。这些控制是第一道防线，帮助防止未经授权的访问或对网络的意外更改。有关更多信息，请参阅在 AWS上实施安全控制中的预防性控制。

主体

中 AWS 可以执行操作和访问资源的实体。此实体通常是 IAM 角色的根用户或用户。 AWS 账户有关更多信息，请参阅 IAM 文档中角色术语和概念中的主体。

隐私设计

一种在整个开发过程中都考虑隐私的系统工程方法。

私有托管区

一个容器，其中包含有关您希望 Amazon Route 53 如何响应针对一个或多个 VPCs域名及其子域名的 DNS 查询的信息。有关更多信息，请参阅 Route 53 文档中的私有托管区的使用。

主动控制

一种安全控制，旨在防止部署不合规资源。这些控制会在资源预置之前对其进行扫描。如果资源与控制不兼容，则不会预置它。有关更多信息，请参阅 AWS Control Tower 文档中的控制参考指南，并参见在上实施安全控制中的主动控制 AWS。

产品生命周期管理（PLM）

对产品在其整个生命周期内的数据和流程的管理，从设计、开发和发布，到增长和成熟，再到衰退和淘汰。

生产环境

请参阅环境。

可编程逻辑控制器（PLC）

在制造业中，一种高度可靠、适应性强的计算机，用于监控机器并实现制造过程自动化。

提示串接

使用一个 LLM 提示的输出作为下一个提示的输入，以生成更好的响应。该技术用于将复杂的任务分解为子任务，或者迭代地完善或扩展初步响应。它有助于提高模型响应的准确性和相关性，并允许获得更精细的个性化结果。

假名化

用占位符值替换数据集中个人标识符的过程。假名化可以帮助保护个人隐私。假名化数据仍被视为个人数据。

publish/subscribe (pub/sub)

一种支持微服务间异步通信的模式，可提高可扩展性和响应能力。例如，在基于微服务的 MES 中，微服务可以将事件消息发布到其他微服务可以订阅的频道。系统可以在不更改发布服务的情况下添加新的微服务。

Q

查询计划

一系列用于访问 SQL 关系数据库系统中的数据的步骤，类似于指令。

查询计划回归

当数据库服务优化程序选择的最佳计划不如数据库环境发生特定变化之前时。这可能是由统计数据、约束、环境设置、查询参数绑定更改和数据库引擎更新造成的。

R

RACI 矩阵

请参阅责任、问责、咨询和知情（RACI）。

RAG

请参阅检索增强生成。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI 矩阵

请参阅责任、问责、咨询和知情（RACI）。

RCAC

请参阅行列访问控制。

只读副本

用于只读目的的数据库副本。您可以将查询路由到只读副本，以减轻主数据库的负载。

重新架构

请参阅 7 R。

恢复点目标（RPO）

自上一个数据恢复点以来可接受的最长时间。这决定了从上一个恢复点到服务中断之间可接受的数据丢失情况。

恢复时间目标（RTO）

服务中断和服务恢复之间可接受的最大延迟。

重构

请参阅 7 R。

Region

地理区域内的 AWS 资源集合。每一个 AWS 区域 都相互隔离，彼此独立，以提供容错、稳定性和弹性。有关更多信息，请参阅指定您的账户可以使用的 AWS 区域。

回归

一种预测数值的 ML 技术。例如，要解决“这套房子的售价是多少？”的问题 ML 模型可以使用线性回归模型，根据房屋的已知事实（如建筑面积）来预测房屋的销售价格。

重新托管

请参阅 7 R。

版本

在部署过程中，推动生产环境变更的行为。

重新放置

请参阅 7 R。

更换平台

请参阅 7 R。

重新购买

请参阅 7 R。

韧性

应用程序抵御中断或从中断中恢复的能力。在 AWS Cloud中规划韧性时，高可用性和灾难恢复是常见的考虑因素。有关更多信息，请参阅 AWS Cloud 韧性。

基于资源的策略

一种附加到资源的策略，例如 AmazonS3 存储桶、端点或加密密钥。此类策略指定了允许哪些主体访问、支持的操作以及必须满足的任何其他条件。

责任、问责、咨询和知情（RACI）矩阵

定义参与迁移活动和云运营的所有各方的角色和责任的矩阵。矩阵名称源自矩阵中定义的责任类型：负责（R）、问责（A）、咨询（C）和知情（I）。支持（S）类型是可选的。如果包括支持，则该矩阵称为 RASCI 矩阵，如果将其排除在外，则称为 RACI 矩阵。

响应性控制

一种安全控制，旨在推动对不良事件或偏离安全基线的情况进行修复。有关更多信息，请参阅在AWS上实施安全控制中的响应性控制。

保留

请参阅 7 R。

停用

请参阅 7 R。

检索增强生成（RAG）

一种生成式人工智能技术，其中 LLM 在生成响应之前引用其训练数据来源之外的权威数据来源。例如，RAG 模型可以对组织的知识库或自定义数据执行语义搜索。有关更多信息，请参阅什么是 RAG。

轮换

定期更新密钥以使攻击者更难访问凭证的过程。

行列访问控制（RCAC）

使用已定义访问规则的基本、灵活的 SQL 表达式。RCAC 由行权限和列掩码组成。

RPO

请参阅恢复点目标。

RTO

请参阅恢复时间目标。

运行手册

执行特定任务所需的一套手动或自动程序。它们通常是为了简化重复性操作或高错误率的程序而设计的。

S

SAML 2.0

许多身份提供商 (IdPs) 使用的开放标准。此功能支持联合单点登录 (SSO)，因此用户无需在 IAM 中为组织中的所有人创建用户即可登录 AWS 管理控制台 或调用 AWS API 操作。有关基于 SAML 2.0 的联合身份验证的更多信息，请参阅 IAM 文档中的关于基于 SAML 2.0 的联合身份验证。

SCADA

请参阅监督控制和数据采集。

SCP

请参阅服务控制策略。

机密密钥

在中 AWS Secrets Manager，您以加密形式存储的机密或受限信息，例如密码或用户凭证。它由密钥值及其元数据组成。密钥值可以是二进制、单个字符串或多个字符串。有关更多信息，请参阅 Secrets Manager 文档中的什么是 Amazon Secrets Manager 密钥？。

安全设计

一种在整个开发过程中都考虑安全的系统工程方法。

安全控制

一种技术或管理防护机制，可防止、检测或降低威胁行为体利用安全漏洞的能力。安全控制有以下四种类型：预防性、检测性、响应性和主动性。

安全固化

缩小攻击面，使其更能抵御攻击的过程。这可能包括删除不再需要的资源、实施授予最低权限的最佳安全实践或停用配置文件中不必要的功能等操作。

安全信息和事件管理（SIEM）系统

结合了安全信息管理（SIM）和安全事件管理（SEM）系统的工具和服务。SIEM 系统会收集、监控和分析来自服务器、网络、设备和其他来源的数据，以检测威胁和安全漏洞，并生成警报。

安全响应自动化

一种预定义的程序化操作，旨在自动响应或修复安全事件。这些自动化可作为侦探或响应式安全控制措施，帮助您实施 AWS 安全最佳实践。自动响应操作的示例包括修改 VPC 安全组、修补 Amazon EC2 实例或轮换凭证。

服务器端加密

由接收数据的人在目的地对数据 AWS 服务 进行加密。

服务控制策略（SCP）

一种策略，用于集中控制组织中所有账户的权限 AWS Organizations。 SCPs 定义防护措施或限制管理员可以委托给用户或角色的操作。您可以使用 SCPs 允许列表或拒绝列表来指定允许或禁止哪些服务或操作。有关更多信息，请参阅 AWS Organizations 文档中的服务控制策略。

服务端点

的入口点的 URL AWS 服务。您可以使用端点，通过编程方式连接到目标服务。有关更多信息，请参阅 AWS 一般参考 中的 AWS 服务 端点。

服务水平协议（SLA）

一份协议，阐明了 IT 团队承诺向客户交付的内容，比如服务正常运行时间和性能。

服务水平指示器（SLI）

对服务性能方面的衡量，例如错误率、可用性或吞吐量。

服务水平目标（SLO）

代表服务运行状况的目标指标，由服务水平指示器衡量。

责任共担模式

描述您在云安全与合规方面共同承担 AWS 的责任的模型。 AWS 负责云的安全，而您则负责云中的安全。有关更多信息，请参阅责任共担模式。

SIEM

请参阅安全信息和事件管理系统。

单点故障（SPOF）

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

请参阅服务水平协议。

SLI

请参阅服务水平指示器。

SLO

请参阅服务水平目标。

split-and-seed 模型

一种扩展和加速现代化项目的模式。随着新功能和产品发布的定义，核心团队会拆分以创建新的产品团队。这有助于扩展组织的能力和服务，提高开发人员的工作效率，支持快速创新。有关更多信息，请参阅在 AWS Cloud中实现应用程序现代化的分阶段方法。

SPOF

请参阅单点故障。

星型架构

一种数据库组织结构，它使用一个大型事实表来存储事务数据或测量数据，并使用一个或多个较小的维度表来存储数据属性。此结构专为在数据仓库中使用或用于商业智能目的而设计。

strangler fig 模式

一种通过逐步重写和替换系统功能直至可以停用原有的系统来实现单体系统现代化的方法。这种模式用无花果藤作为类比，这种藤蔓成长为一棵树，最终战胜并取代了宿主。该模式是由 Martin Fowler 提出的，作为重写单体系统时管理风险的一种方法。有关如何应用此模式的示例，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

监督控制和数据采集（SCADA）

在制造业中，一种使用硬件和软件来监控实物资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

以模拟用户交互的方式测试系统，以检测潜在问题或监控性能。你可以使用 Amazon S CloudWatch ynthetics 来创建这些测试。

系统提示

一种为 LLM 提供上下文、说明或准则以指导其行为的技术。系统提示有助于设置上下文并制定与用户交互的规则。

T

标签

键值对，用作组织资源的元数据。 AWS 标签有助于您管理、识别、组织、搜索和筛选 资源。有关更多信息，请参阅标记您的 AWS 资源。

目标变量

您在监督式 ML 中尝试预测的值。这也被称为结果变量。例如，在制造环境中，目标变量可能是产品缺陷。

任务列表

一种通过运行手册用于跟踪进度的工具。任务列表包含运行手册的概述和要完成的常规任务列表。对于每项常规任务，它包括预计所需时间、所有者和进度。

测试环境

请参阅环境。

训练

为您的 ML 模型提供学习数据。训练数据必须包含正确答案。学习算法在训练数据中查找将输入数据属性映射到目标（您希望预测的答案）的模式。然后输出捕获这些模式的 ML 模型。然后，您可以使用 ML 模型对不知道目标的新数据进行预测。

中转网关

一个网络传输中心，可用于将您的网络 VPCs 和本地网络互连。有关更多信息，请参阅 AWS Transit Gateway 文档中的什么是公交网关。

基于中继的工作流程

一种方法，开发人员在功能分支中本地构建和测试功能，然后将这些更改合并到主分支中。然后，按顺序将主分支构建到开发、预生产和生产环境。

可信访问权限

向您指定的服务授予权限，该服务可以代表您在其账户中执行任务。 AWS Organizations 当需要服务相关的角色时，受信任的服务会在每个账户中创建一个角色，为您执行管理任务。有关更多信息，请参阅 AWS Organizations 文档中的AWS Organizations 与其他 AWS 服务一起使用。

优化

更改训练过程的各个方面，以提高 ML 模型的准确性。例如，您可以通过生成标签集、添加标签，并在不同的设置下多次重复这些步骤来优化模型，从而训练 ML 模型。

双披萨团队

一个小 DevOps 团队，你可以用两个披萨来喂食。双披萨团队的规模可确保在软件开发过程中充分协作。

U

不确定性

这一概念指的是不精确、不完整或未知的信息，这些信息可能会破坏预测式 ML 模型的可靠性。不确定性有两种类型：认知不确定性是由有限的、不完整的数据造成的，而偶然不确定性是由数据中固有的噪声和随机性导致的。有关更多信息，请参阅量化深度学习系统中的不确定性指南。

无差别任务

也称为繁重工作，即创建和运行应用程序所必需的工作，但不能为最终用户提供直接价值或竞争优势。无差别任务的示例包括采购、维护和容量规划。

上层环境

请参阅环境。

V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC 对等连接

两者之间的连接 VPCs ，允许您使用私有 IP 地址路由流量。有关更多信息，请参阅 Amazon VPC 文档中的什么是 VPC 对等连接。

漏洞

损害系统安全的软件缺陷或硬件缺陷。

W

热缓存

一种包含经常访问的当前相关数据的缓冲区缓存。数据库实例可以从缓冲区缓存读取，这比从主内存或磁盘读取要快。

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

一种对与当前记录有某种关联的一组行执行计算的 SQL 函数。窗口函数对于处理任务很有用，例如计算移动平均值或根据当前行的相对位置访问行的值。

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

迁移项目中负责一组特定任务的职能小组。每个工作流都是独立的，但支持项目中的其他工作流。例如，组合工作流负责确定应用程序的优先级、波次规划和收集迁移元数据。组合工作流将这些资产交付给迁移工作流，然后迁移服务器和应用程序。

WORM

请参阅一次写入多次读取。

WQF

请参阅 AWS 工作负载资格鉴定框架。

一次写入多次读取（WORM）

一种存储模型，可一次写入数据并防止数据被删除或修改。授权用户可以根据需要多次读取数据，但无法对其进行更改。此数据存储基础设施被认为不可变。

Z

零日漏洞利用

一种利用零日漏洞的攻击，通常为恶意软件。

零日漏洞

生产系统中不可避免的缺陷或漏洞。威胁主体可能利用这种类型的漏洞攻击系统。开发人员经常因攻击而意识到该漏洞。

零样本提示

为 LLM 提供执行任务的说明，但没有可以帮助指导的示例（样本）。LLM 必须使用预先训练的知识来处理任务。零样本提示的有效性取决于任务的复杂性和提示的质量。另请参阅少样本提示。

僵尸应用程序

平均 CPU 和内存使用率低于 5% 的应用程序。在迁移项目中，通常会停用这些应用程序。

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。