AWS规范性指导

AWS安全参考架构



AWS规范性指导: AWS安全参考架构

Copyright © 2023 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 拥有的其它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

介绍 1
AWS SRA 的价值 2
如何使用 2
AWS SRA 的关键实施指南 3
安全基础 5
安全功能 5
安全设计原则 6
SRA 构建模块 — AWS Organizations、账户和护栏 7
使用 AWS Organizations 实现安全 7
管理账户、可信访问权限和委派管理员 8
专用账户结构 9
AWS SRA 的 AWS 组织和账户结构 10
在您的 AWS 组织中应用安全服务 12
全组织或多个账户 13
AWS 账户 14
虚拟网络、计算和内容交付 15
校长和资源 16
AWS 安全参考架构 19
组织管理账户 21
服务控制策略 22
IAM Identity Center 22
IM 访问顾问 23
AWS Systems Manager 23
AWS Control Tower 24
AWS Artifact 24
分布式和集中式安全服务护栏 25
安全 OU — 安全工具帐户 25
安全服务的委托管理员 27
AWS CloudTrail 27
AWS Security Hub 27
AWS GuardDuty 28
AWS Config 29
Amazon Macie 30
AWS IAM Access Analyzer 31
AWS Firewall Manager 31
Amazon EventBridge 32
Amazon Detective 32
Amazon Audit Manager 33
AWS Artifact 33
AWS KMS 34
AWS 私有 CA 34
Amazon Inspector 35
在所有 AWS 账户中部署通用安全服务 35
安全 OU — 日志存档账户 36
日志的类型 37
Amazon S3 作为中央日志存储 37
基础架构 OU — 网络账户 38
网络架构 39
入站（入口）VPC 39
出站（出口）VPC 39
检查 VPC 39
AWS 网络防火墙 39
Network Access Analyzer 40
AWS 内存 40

边缘安全 41
Amazon CloudFront 41
AWS WAF 42
AWS Shield 43
AWS Certificate Manager 43
Amazon Route 53 43
基础架构 OU — 共享服务账户 44
AWS Systems Manager 45
AWS MSMSMS 45
IAM Identity Center 46
工作负载 OU — 应用程序帐户 47
应用程序 VPC 48
VPC 端点 48
Amazon EC2 48
Application Load Balancer 49
AWS 私有 CA 49
Amazon Inspector 49
亚马逊系统经理 50
Amazon Aurora 50
Amazon S3 51
AWSKS 51
AWS CloudHS 51
AWS 机密管理器 51
Amazon Cognito 52
分层防御 53
IAM 资源 54
AWS SRA 示例的代码存储库 56
致谢 58
身份与身份与身份AWS 身份与身份与身份与身份与身份与身份与合规性 59
文档历史记录 61
术语表 62
安全条款 62
..... lxvi

AWS安全参考架构 (AWSSRA)

Amazon Web Services (AWS)

2023 年 5 月（文件历史记录 (p. 61)）

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

Amazon Web Services (AWS) 安全参考架构 (AWS SRA) 是一套全面的指导方针，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 推荐的做法。这些建议是围绕包含 AWS 安全服务的单页架构构建的，这些服务如何帮助实现安全目标，在您的 AWS 账户中可以最好地部署和管理这些服务，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、针对特定服务的建议，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。本文档是参考——一套关于使用 AWS 服务保护特定环境的全面指南，而 AW S SRA 代码存储库 (p. 56)中的解决方案模式是为本参考文献中说明的特定架构设计的。每个客户都有不同的要求。因此，您的 AWS 环境的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。 在整个文档中，我们会酌情为经常出现的替代场景提出备选方案。

AWS SRA 是一套活的指南，会根据新服务和功能发布、客户反馈以及不断变化的威胁格局定期更新。每次更新都将包括修订日期和相关的更改日志 (p. 61)。

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，必须建立在结构良好的基础和安全原则基础上。您可以通过两种方式使用本文档：作为叙述或作为参考。这些主题以故事的形式组织，因此您可以从开头（基础安全指南）到结尾（讨论可以实现的代码示例）阅读它们。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。

本文档分为六个部分和一个附录：

- AWS SRA 的价值 (p. 2)讨论了构建 AWS SRA 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。
- 安全基金会审查 (p. 5)了 AWS 云采用框架 (AWS CAF)、AWS Well-Architected Framework 和 AWS 共同责任模型，并重点介绍了与 AWS SRA 特别相关的元素。
- AWS Organizations、账户和 IAM Guardrails (p. 7) 介绍了 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 (p. 19)是一个单页架构图，显示了正常运行的 AWS 账户以及通常可用的安全服务和功能。
- IAM 资源 (p. 54)提供了对您的安全架构很重要的 AWS Identity and Access Management (IAM) 指南的摘要和一组指导。
- AWS SRA 示例代码存储库 (p. 56)概述了关联GitHub存储库，该存储库包含示例 AWSCloudFormation 模板和用于部署 AWS SRA 中讨论的一些模式的代码。

附录 (p. 59)包含各个 AWS 安全、身份和合规服务的列表，并提供了指向每项服务的更多信息的链接。文档历史记录 (p. 61)部分提供了更改日志，用于跟踪此文档的版本。您也可以订阅 RSS 提要以获取变更通知。

Note

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）

AWS SRA 的价值

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

AWS 拥有大量（且不断增长）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赞赏。他们还告诉我们，他们想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信息？ 客户应该注意哪些权衡取舍（设计注意事项）？
- 客户有兴趣从不同的角度对许多 AWS 安全服务进行逻辑组织。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。本指南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，以最有效的方式整合安全服务。例如，他们应该如何最好地将AWS Config 与其他服务协调和连接，以完成自动审计和监控管道中的繁重工作？ 客户要求获得有关每个 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 中解决了所有这些问题。列表中的第一个优先级（事情的发展方向）是主架构图和本文档中随附讨论的重点。我们提供了推荐的 AWS Organizationaccount-by-account s 架构，并描述了哪些服务的去向。 要从列表中的第二个优先级（如何考虑全套安全服务）开始，请阅读 “在您的 AWS 组织中应用安全服务 (p. 12)” 部分。本节介绍一种根据您的 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应用程序账户的讨论中，该讨论强调了如何运营安全服务，将重点放在账户 (p. 47)的某些层面：Amazon Elastic Compute Cloud (Amazon EC2) 实例、Amazon Virtual Private Cloud (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，尤其是在本文档的账户深度分析部分中对个别服务的讨论以及 AWS SRA 代码存储库中的代码中。

如何使用

AWS SRA 有不同的使用方式，具体取决于您在云采用之旅中所处的位置。以下是从 AWS SRA 资产（架构图、书面指南和代码示例）中获得最大见解的方法列表。

- 为自己的安全架构@@ 定义目标状态。

无论您是刚刚开始 AWS 云之旅（设置第一组账户），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 并将其用作组织安全参考架构的基础。

- 查看（并修订）您已经实现的设计和功能。

如果您已经有了安全设计和实现，那么值得花点时间将您拥有的与 AWS SRA 进行比较。AWS SRA 的设计非常全面，可为检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，则您可以更有信心在使用 AWS 服务时遵循了最佳实践。如果您的安全设计与AWS SRA中的指导存在分歧甚至不同意，这并不一定表示您做错了什么。相反，这种观察结果为您提供了审查决策过程的机会。您可能会偏离 AWS SRA 最佳实践，这有正当的商业和技术原因。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，而是偏爱来自 AWS 合作伙伴网络的产品或您构建和管理的自定义应用程序的功能。有时，在这次审查中，您可能会发现之前的决策是基于旧技术、AWS 功能或不再适用的业务限制做

出的。这是一个很好的机会，可以审查任何更新，确定任何更新的优先级，并将它们添加到工程待办事项的适当位置。无论您在根据 AWS SRA 评估安全架构时发现了什么，您都会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为future 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) 模块为开始构建和实施安全架构提供了一种快速、可靠的方法。代码存储库部分和公共GitHub存储库 (p. 56)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 指南中模式的高质量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 AWS Identity and Access Management (IAM) 密码策略、亚马逊简单存储服务 (Amazon S3) 封禁账户公共访问、Amazon EC2 默认 Amazon Elastic Block Store (Amazon EBS) 加密以及与 AWS Control Tower 的集成，以便在新的 AWS 账户加入或停用时应用或删除控制措施。

- 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各个 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，它简要介绍了 AWS 安全服务的广度以及它们如何在多账户环境中协同工作。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。其中一个例子是讨论 (p. 27) AWS Security Hub 如何从各种 AWS 服务、AWS 合作伙伴产品甚至您自己的应用程序中提取安全发现。

- 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要素是了解组织中谁负有哪些与安全相关的职责。例如，在哪里汇总和监控安全发现的问题与哪个小组将负责该活动的问题息息相关。整个组织的所有发现是否都由需要访问专用 Security Tooling 账户的中央团队监控？ 还是个别应用程序团队（或业务单位）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，如果您的组织有一个集中管理所有加密密钥的群组，这将影响谁有权创建 AWS Key Management Service (AWS KMS) 密钥以及这些密钥将在哪些账户中管理。了解您组织的特征（不同的团队和职责）将帮助您量身定制 AWS SRA，使其最适合您的需求。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 建议采用分散的决策流程，工作负载团队负责根据其工作负载功能和要求定义安全控制。集中式安全和治理团队的目标是建立一个系统，使工作负载所有者能够做出明智的决策，并让所有各方都能了解配置、发现和事件。AWS SRA 可以作为识别和为这些讨论提供信息的工具。

AWS SRA 的关键实施指南

以下是 AWS SRA 的八个关键要点，在设计和实施安全性时要记住。

- AWS Organizations 适当的多账户策略是您的安全架构的必要元素。正确分离工作量、团队和职能为职责和defense-in-depth战略分离提供了基础。该指南将在后面的章节 (p. 10)中进一步介绍这一点。
- Defense-in-depth 是为您的组织选择安全控制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：如果某一层出现问题，则会采取控制措施隔离其他宝贵的 IT 资源。AWS SRA 演示了不同的 AWS 服务如何在 AWS 技术堆栈的不同层面上运行，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 (p. 12)将进一步讨论 AWS 上的这一defense-in-depth概念，并在应用程序账户 (p. 47)下显示了设计示例。
- 使用跨多个 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设施。在根据您的特定需求定制 AWS SRA 时，不仅要考虑 AWS 服务和功能（例如，身份验证、加密、监控、权限策略）的主要功能，还要考虑它们如何适应您的架构结构。指南的后面部分 (p. 13)描述了某些服务在整个 AWS 组织中的运行方式。其他服务在单一账户中运行效果最佳，有些服务旨在授予或拒绝个人委托人许可。考虑这两种视角有助于你构建更灵活的分层安全方法。
- 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 AWS 服务，并建立一组一致的共享防护栏，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 SRA 使用 AWS Security Hub（集中查找监控和合规性检查）、AmazonGuardDuty（威胁检测和异常检测）、AWS Config（资源监控和变更检测）、IAM Access AnalyzerCloudTrail（资源访问监

控、AWS（记录整个环境中的服务 API 活动）和 Amazon Macie（数据分类）作为一组基础的 AWS 服务，可在每个 AWS 账户中部署。

- 使用支持的 AWS Organizations 委托管理功能，如本指南稍后的 “委托管理 (p. 27)” 部分所述。这使您能够将 AWS 成员账户注册为支持服务的管理员。委托管理为企业内的不同团队提供了灵活性，使他们能够根据各自的职责使用不同的账户来管理整个环境中的 AWS 服务。此外，使用委托管理员可以帮助您限制对 AWS Organizations 管理账户的访问权限并管理 AWS 组织管理账户的权限开销。
- 在您的 AWS 组织中实施集中监控、管理和监管。通过使用支持多账户（有时是多区域）聚合以及委托管理功能的 AWS 服务，您可以让您的中央安全、网络和云工程团队对适当的安全配置和数据收集具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 AWS Control Tower 设置和管理您的多账户 AWS 环境，实施预先构建的安全控制以引导您的安全参考架构构构构建。AWS Control Tower 提供了一个蓝图，用于提供身份管理、账户的联合访问权限、集中日志记录和预置额外账户的定义工作流程。然后，您可以使用 Control T ower 自定义 (cFcT) 解决方案为由 AWS Control Tower 管理的账户提供额外的安全控制、服务配置和监管，如 AWS SRA 代码存储库所示。账户工厂功能可根据经批准的账户配置自动使用可配置模板预置新账户，以标准化您的 AWS Organizations 内的账户。您还可以通过将现有个人账户注册到已经由 AWS Control Tower 管理的组织单位 (OU)，将监管范围扩展到个人现有 AWS 账户。
- AWS SRA 代码示例演示了如何使用基础设施即代码 (iaC) 自动实现 AWS SRA 指南中的模式。编纂这些模式可以将 iaC 视为组织中的其他应用程序，在这些应用程序中，可以在部署完成之前自动进行测试。iaC 还通过在多个（例如 SDLC 或特定区域）环境中部署护栏来帮助确保一致性和可重复性。SRA 代码示例使用带有 AWS Control Tower (cFcT) 自定义功能的 AWS Control Tower，以加快 iaC 整合 AWS 环境的速度。

安全基础

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

AWS 安全参考架构符合三个 AWS 安全基础：AWS 云采用框架 (AWS CAF)、AWS Well-Architected 和 AWS 共担责任模型。

AWS Professional Services 创建了 AWS CAF，以帮助公司设计和走上成功采用云的加速之路。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，即视角。每种视角都涵盖职能相关利益攸关方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、安全和运营视角则侧重于技术能力。

- AWS CAF 的安全视角可帮助您在整个业务中组织控制措施的选择和实施。遵循 AWS 在安全支柱中的最新建议可以帮助您满足业务和监管要求。

AWS Well-Ar chitected ework itected ework ework ework ework ework ework ted 该框架work ework ework ework ework e work ework e work e work e AWS ork e work 和实施可随时间推移扩展的设计的一致方法。我们相信，精心设计的工作负载会大大增加业务成功的可能性。

- WW ell-Architected ted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。这将通过遵循当前的 AWS 建议来帮助您满足您的业务和监管要求。还有其他Well-Architected 的框架重点领域，可为治理、无服务器、AI/ML 和游戏等特定领域提供更多背景信息。这些镜头被称为 AWS Well-Architected 镜头。

安全与合规是 A WS 和客户的共同责任。在 AWS 运行、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时，这种共享模型可以帮助您减轻运营负担。例如，您负责和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 Simple Storage Service (Amazon S3) 和 Amazon DynamoDB。AWS mazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB。您负责管理您的数据（包括加密选项），对资产进行分类，并使用 AWS Identity and Access Management (IAM) 工具来应用相应的权限。这种共享模式通常被描述为 AWS 负责云的安全（即保护运行 AWS 云中提供的所有服务的基础设施），而您对云中的安全负责（由您选择的 AWS 云服务决定）。

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：安全能力和安全设计原则。

安全功能

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，用于在组织的 AWS 环境中制定和传达安全角色、责任、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。
- 威胁检测可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及其在组织中的访问和使用方式的可见性和控制力。

- 应用程序安全，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危害。

安全设计原则

Well-Architected Framework 的安全支柱涵盖了一组七项设计原则，这些原则将特定的安全领域转化为可帮助您增强工作负载安全性的实用指南。在安全功能构成整体安全策略的地方，这些Well-Architected 的原则描述了您可以开始做什么。它们非常刻意地反映在这个 AWS SRA 中，包括以下内容：

- 奠@@ 定坚实的身份基础 — 实施最小权限原则，通过对每次与 AWS 资源的交互进行适当授权，强制实行职责分离。集中化身份管理，旨在消除对长期静态证书的依赖。
- 实现可追溯性-实时监控、生成警报和审核操作和环境更改。将日志和指标收集与系统集成，以自动调查和采取行动。
- 在所有层面应用安全性-应用具有多种安全控制措施defense-in-depth的方法。将多种类型的控制（例如预防和侦测控制）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。创建安全架构，并在版本控制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，并在适当时使用加密、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。这降低了处理敏感数据时出现不当处理或修改以及人为错误的风险。
- 为安全事件做好准备 — 通过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。运行事件响应模拟，并使用具有自动化的工具来提高检测、调查和恢复的速度。

SRA 构建模块 — AWS Organizations、账户和护栏

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

AWS 安全服务、其控制和交互最好在 A WS 多账户战略以及身份和访问管理防护栏的基础上使用。这些防护栏为您设置了实现最低权限、职责分离和隐私的能力，并为决定需要哪些类型的控制、在哪里管理每项安全服务以及它们如何在 AWS SRA 中共享数据和权限提供支持。

AWS 账户为您的 AWS 资源提供安全、访问和计费边界，使您能够实现资源独立和隔离。使用多个 AWS 账户在如何满足安全要求方面起着重要作用，如使用多个账户组织 AWS 环境白皮书的 “使用多个 AWS 账户的好处” 部分所述。例如，您可以根据职能、合规性要求或一组常见的控制措施将工作负载组织在组织单位 (OU) 内的单独账户和群组帐户中，而不是镜像企业的报告结构。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通用护栏。这种方法在工作负载之间提供了强大的边界和控制。账户级分离与 AWS Organizations 相结合，用于将生产环境与开发和测试环境隔离开来，或者在处理支付卡行业数据安全标准 (PCI DSS) 或《Health 保险便携性和责任法案》(HIPAA) 等不同分类数据的工作负载之间提供强大的逻辑边界。尽管您可以从单个账户开始 AWS 之旅，但随着工作负载规模和复杂性的增加，AWS 建议您设置多个账户。

权限允许您指定对 AWS 资源的访问权限。向称为委托人的 IAM 实体（用户、组和角色）授予权限。默认情况下，校长一开始没有权限。在您授予权限之前，IAM 实体无法在 AWS 中执行任何操作，您可以设置与整个 AWS 组织一样广泛适用的防护栏，也可以根据委托人、操作、资源和条件的个人组合进行细粒度设置。

使用 AWS Organizations 实现安全

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

在您增长和扩展 AWS 资源时，AWS O rganizations 帮助您集中管理和治理您的环境。通过使用 AWS Organizations，您可以以编程方式创建新的 AWS 账户、分配资源、对账户进行分组以组织您的工作负载，并将策略应用于账户或账户组进行治理。AWS 组织整合您的 AWS 账户，以便您可以将它们作为一个整体进行管理。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位于成员账户中，但一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特定 AWS 服务的委托管理员的账户中。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。您可以将账户分组为 AWS 组织单元 (OU)，这些组织单位可以根据工作负载的要求和目的代表不同的环境。

通过 AWS Organization s，您可以使用服务控制策略 (SCP) 在 AWS 组织、OU 或账户级别应用权限保护措施。这些保护措施适用于组织账户内的委托人，但管理账户除外（这是不在该账户中运行工作负载的原因之一）。将 SCP 连接到 OU 时，它会由该 OU 下的子 OU 和账户继承。SCP 不授予任何权限。相反，SCP 指定了 AWS 组织、OU 或账户的最大权限。您仍然需要将基于身份或基于资源的策略附加到 AWS 账户中的委托人或资源，以实际向他们授予权限。例如，如果 SCP 拒绝访问所有 Amazon S3，则即使通过 IAM 策略明确授予了受该 SCP 影响的委托人访问权限，他们也将无法访问 Amazon S3。有关如何评估 IAM 策略、SCP 的作用以及最终如何授予或拒绝访问的详细信息，请参阅 IAM 文档中的策略评估逻辑。

AWS Control Tower 提供了一种设置和管理多个账户的简便方法。它可以自动在您的 AWS 组织中设置账户、自动配置、应用护栏（包括预防和侦测控制），并为您提供可见性的控制面板。附加的 IAM 管理策略，即权限边界，用于设置基于身份的策略可以为 IAM 实体授予的最大权限。

AWS Organizations 可帮助您配置适用于您的所有账户的 AWS 服务。例如，您可以使用 AWS 配置在 AWS 组织中执行的所有操作的集中日志记录CloudTrail，并防止成员账户禁用日志记录。您还可以集中聚合使用 AWS Config 定义的规则的数据，这样您就可以审核工作负载的合规性并对变化做出快速反应。您可以使用 AWSCloudFormationStackSets 集中管理 AWS 组织中跨账户和 OU 的 AWSCloudFormation 堆栈，这样您就可以自动预置新账户以满足您的安全要求。

AWS Organizations 默认配置支持使用 SCP 作为拒绝列表。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，直到您创建并连接拒绝特定服务或一组操作的 SCP 为止。与允许列表相比，拒绝语句所需的维护更少，因为在 AWS 添加新服务时，您不必对其进行更新。Deny 语句的字符长度通常较短，因此更容易保持在 SCP 的最大大小范围内。在 `Effect` 元素具有值 `Deny` 的语句中，您还可以限制对特定资源的访问，或者定义 SCP 何时生效的条件。相比之下，SCP 中的 Allow 语句适用于所有资源 (`"*"`)，并且不受条件限制。有关更多信息和示例，请参阅 AWS Or ganizations 文档中的 SCP 使用策略。

设计注意事项

- 或者，要使用 SCFullAWSAccess P 作为允许列表，您必须将 AWS 托管的 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（从根目录到该账户的直接路径中的每个 OU，甚至附加到该账户本身）都必须允许该权限。此模型本质上更具限制性，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 AWS 账户到 OU 的路径中的每个 IAM 服务或操作。
- 理想情况下，您可以组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 服务列表，并将此 SCP 附加到您的 AWS 组织的根目录中。如果您的开发环境允许使用不同的服务集，则应在每个 OU 上连接相应的 SCP。然后，您可以使用拒绝列表通过明确拒绝特定的 IAM 操作来定义企业防护栏。

管理账户、可信访问权限和委派管理员

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

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，与 AWS Organizations 中的所有其他账户不同。它是创建 AWS 组织的账户。通过该账户，您可以在 AWS 组织中创建 AWS 账户、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 组织中删除账户，以及将 IAM 策略应用于 AWS 组织内的根、OU 或账户。

管理账户通过 SCP 和服务部署（例如 AWSCloudTrail）部署通用安全防护栏，这将影响 AWS 组织中的所有成员账户。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 组织的管理账户。一个 AWS 账户一次只能成为一个 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。可以帮助您实现此目的的两个功能是可信访问和委派管理员。您可以使用信任访问，使您指定的 AWS 服务（称为信任服务），以在您的 AWS 组织及其账户中执行任务。这涉及向信任服务授予权限，但不会以其他方式影响 IAM 实体的权限。您可以使用可信访问来指定您希望可信服务代表您在 AWS 组织的账户中维护的设置和配置详细信息。例如，AWS SRA 的组织管理账户 (p. 21)部分说明了如何授予 AWSCloudTrail 服务可信访问权限，以便在您的 AWSCloudTrail 组织的所有账户中创建组织跟踪。

某些 AWS 服务支持 AWS Organizations 中的委托管理员功能。 使用此功能，兼容的服务可以将 AWS 成员账户注册为 AWS 组织在该服务中的 AWS 成员账户。此功能为企业内的不同团队提供了灵活性，使他们

能够根据各自的职责使用不同的账户来管理整个环境中的 AWS 服务。AWS SRA 中目前支持委托管理员的 AWS 安全服务包括 AWS IAM 身份中心（AWS 单点登录的继任者）、AWS Config、AWS FGuardDuty irewall Manager、AWS IAM Access Analyzer、AWS Security Hub、Amazon Detective、AWS Audit Manager、AWS Amazon Inspector tor 和 AWS Systems Manager。AWS SRA 强调使用委托管理员功能是一种最佳实践，我们将安全相关服务的管理委托给 Security Tooling 账户。

专用账户结构

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

AWS 账户为您的 AWS 资源提供安全、访问和计费边界，使您能够实现资源独立和隔离。默认情况下，账户之间不允许访问。

在设计 OU 和账户结构时，首先要考虑安全性和基础架构。我们建议为这些特定功能创建一组基础 OU，分为基础架构和安全 OU。这些 OU 和账户建议涵盖了我们针AWS Organizations 多账户结构设计的更广泛、更全面的指南的一部分。有关全套建议，请参阅 AWS 文档中的使用多个账户组织您的 AWS 环境和博客文章 AWS Organizations 组织单位最佳实践。

AWS SRA 利用以下账户在 AWS 上实现有效的安全操作。这些专用账户有助于确保职责分离，为应用程序和数据的不同敏感部分支持不同的治理和访问策略，并帮助减轻安全事件的影响。在随后的讨论中，我们将重点放在生产 (prod) 账户及其相关工作负载上。软件开发生命周期 (SDLC) 帐户（通常称为开发和测试帐户）旨在暂存交付成果，可以在与生产帐户不同的安全策略下运行。

账户	OU	安全角色
管理	—	所有 AWS 区域和账户的集中管理和管理。托管 AWS 组织根目录的 AWS 账户。
安全工具	安全性	专用 AWS 账户，用于运营广泛适用的安全服务（例如亚马逊GuardDuty、AWS Security Hub、AWS Audit Manager、Amazon Detective、Amazon Inspector 和 AWS Config）、监控 AWS 账户以及自动发出安全警报和响应。（在 AWS Control Tower 中，安全 OU 下账户的默认名称是审计账户。）
日志存档	安全性	专用 AWS 账户，用于接收和存档所有 AWS 区域和 AWS 账户的所有日志记录和备份。这应该被设计为不可变的存储。
Network	基础设施	您的应用程序与更广泛的互联网之间的网关。网络账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	基础设施	该账户支持多个应用程序和团队用来交付结果的服务。示例包括身份中心目录服务（Active Directory）、消息服务和元数据服务。
应用程序	工作负载	托管 AWS 组织应用程序和执行工作负载的 AWS 账户。（这些帐户有时称为工作负载帐户。）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。这使部署的应用程序更能适应组织变化。

AWS SRA 的 AWS 组织和账户结构

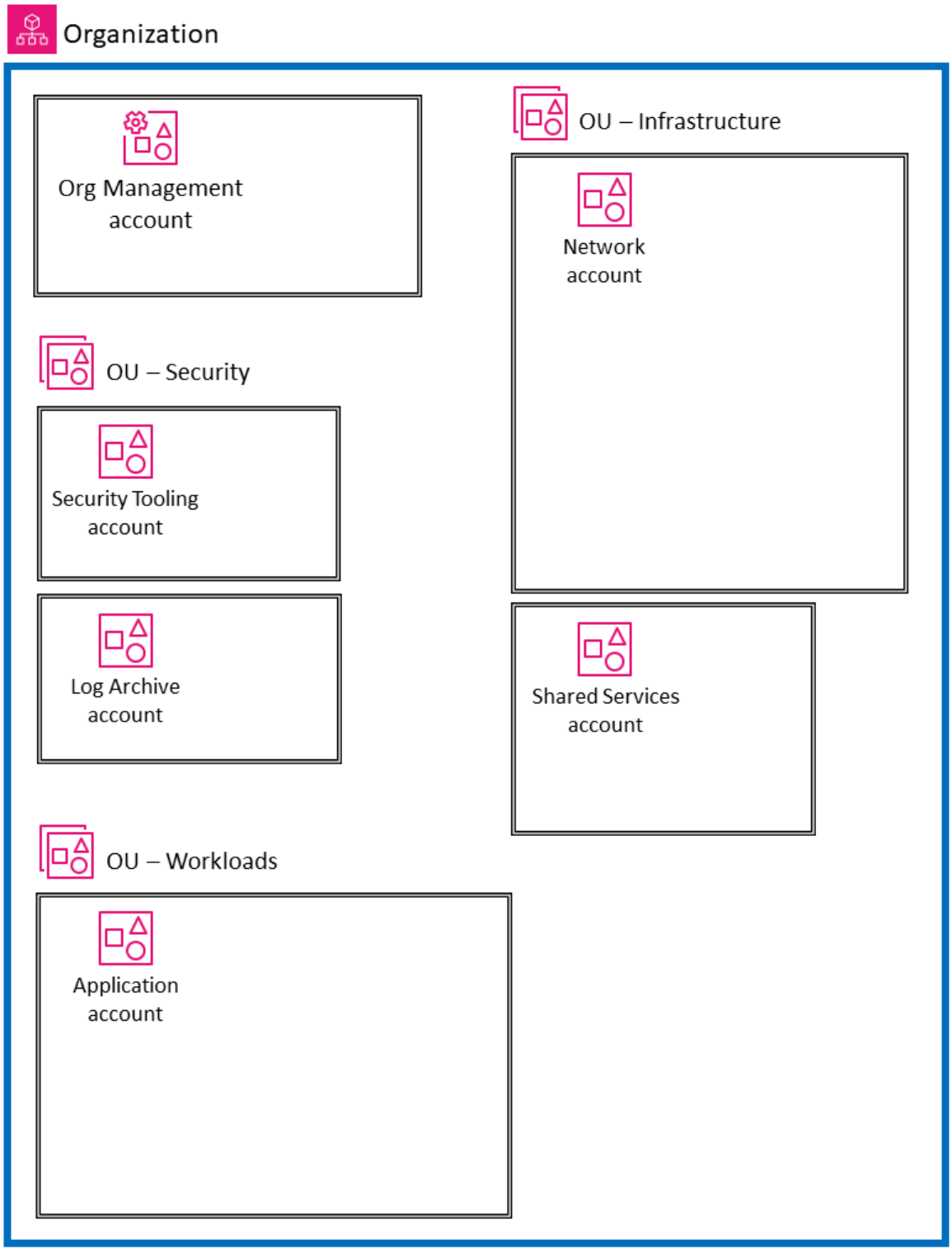
通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

下图捕捉了 AWS SRA 的高级结构，但未显示特定服务。它反映了上一节中讨论的专用账户结构，我们在此附上了示意图，以围绕架构的主要组件展开讨论：

- 图中显示的所有账户都是单个 AWS 组织的一部分。
- 图表的左上角是组织管理账户，用于创建 AWS 组织。
- 组织管理帐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 Workloads OU，它与容纳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 区域运营的生产 (产品) 账户。大多数 AWS 服务（全球服务除外）都具有区域范围，这意味着该服务的控制和数据平面独立存在于每个 AWS 区域。因此，您必须在计划使用的所有 AWS 区域复制此架构，以确保覆盖您的整个 AWS 环境。如果您在特定 AWS 区域中没有任何工作负载，则应使用 SCP 或使用日志记录和监控机制禁用该区域。您可以使用 AWS Security Hub 将来自多个 AWS 区域的调查结果和安全分数汇总到单个聚合区域，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编排层是有益的。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 AWS Control Tower (cFcT) 的自定义解决方案来部署 AWS SRA 推荐的结构。

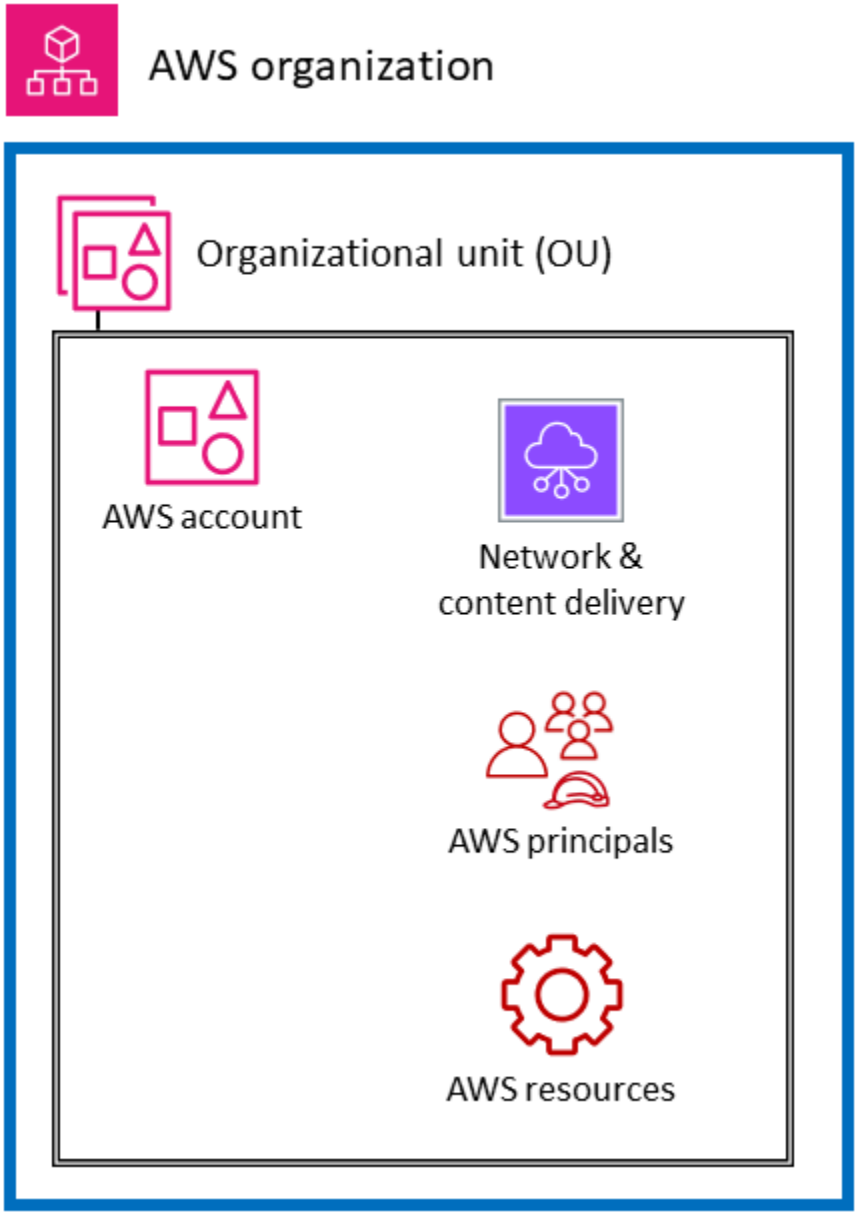

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

在您的 AWS 组织中应用安全服务

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

如前一节 (p. 2)所述，客户正在寻找另一种思考和战略性组织全套 AWS 安全服务的方式。当今最常见的组织方法是按主要功能（根据每项服务的功能）对安全服务进行分组。AWS CAF 的安全视角列出了九种功能功能，包括身份和访问管理、基础设施保护、数据保护和威胁检测。将 AWS 服务与这些功能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 身份中心是值得考虑的服务。在设计威胁检测方法时，亚马逊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查看您的安全性。也就是说，除了问 “我应该使用哪些 AWS 服务来控制和保护我的身份、逻辑访问或威胁检测机制？”，您还可以问：“我应该在整个 AWS 组织中应用哪些 AWS 服务？ 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 AWS 服务和功能映射到 AWS 环境中的图层。某些服务和功能非常适合在整个 AWS 组织中实施控制。例如，阻止对 Amazon S3 存储桶的公有访问。最好在根组织完成，而不是作为个人账户设置的一部分。其他服务和功能最适合用于帮助保护 AWS 账户内的单个资源。在需要私有 TLS 证书的账户中实现下级证书颁发机构 (CA) 就是此类别的示例。另一个同样重要的分组包括对您的 AWS 基础设施的虚拟网络层有影响的服务。下图显示了典型 AWS 环境中的六个层：AWS 组织、组织单位 (OU)、账户、网络基础设施、主体和资源。



了解这种结构背景下的服务，包括每层的控制和保护，有助于您在整个 AWS 环境中规划和实施defense-in-depth策略。从这个角度来看，您可以自上而下地回答问题（例如，“我在整个 AWS 组织中使用哪些服务来实施安全控制？”）以及自下而上（例如，“哪些服务管理此 EC2 实例的控制？”）。在本节中，我们将介绍 AWS 环境的元素并确定相关的安全服务和功能。当然，一些 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的 AWS 环境的多个元素。

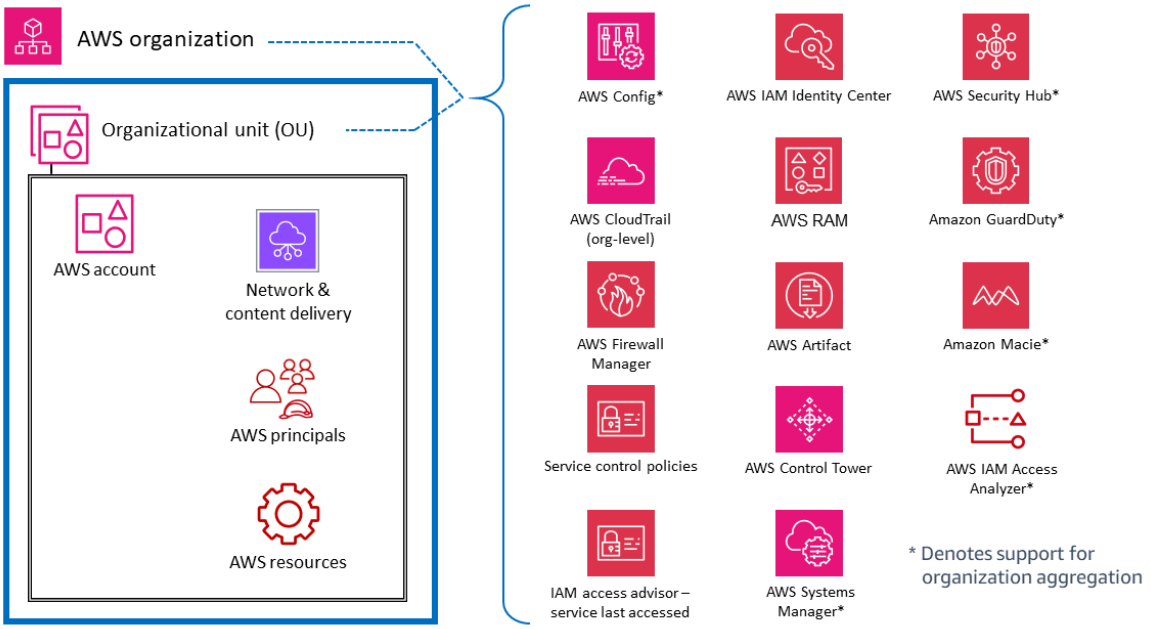
为清楚起见，我们简要描述了某些服务如何实现既定目标。下一节 (p. 19)将进一步讨论每个 AWS 账户内的各项服务。

全组织或多个账户

在最高级别上，有一些 AWS 服务和功能旨在在 AWS 组织中的多个账户（包括整个组织或特定 OU）中应用治理和控制能力或防护措施。服务控制策略 (SCP) 是 IAM 功能的一个很好的示例，该功能可在全组织范围

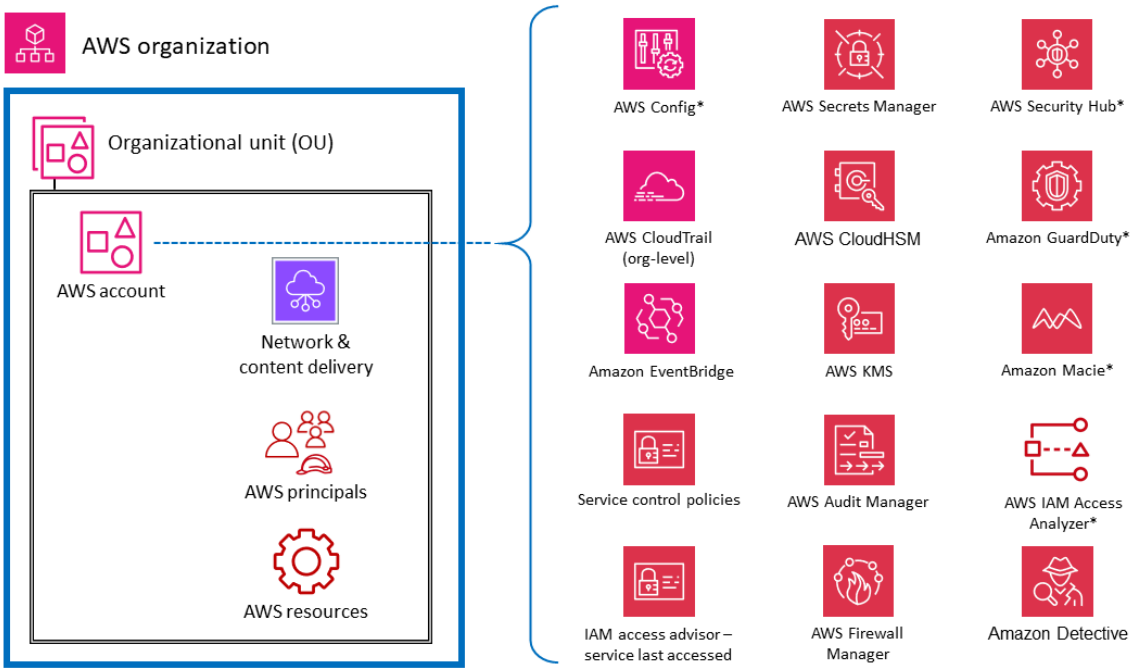
内提供预防性保护。另一个示例是 AWSCloudTrail，它通过组织跟踪提供监控，该跟踪记录了该 AWS 组织中所有 AWS 账户的所有事件。这条综合路径不同于可能在每个账户中创建的单个路径。第三个示例是 AWS Firewall Manager，您可以使用它来配置、应用和管理您的 AWS 组织中所有账户的多个资源：AWS WAF 规则、AWS WAF 经典规则、AWS Shield 高级保护、Amazon Virtual Private Cloud (Amazon VPC) 安全组、AWS Network Firewall 策略和 Amazon Route 53 Resolver DNS 防火墙策略。

下图中标有星号*的服务具有双重范围：全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内的安全。但是，它们还支持将来自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，请考虑适用于整个 OU、AWS 账户或 AWS 组织的 SCP。相比之下，您可以在账户级别（生成个人调查结果）和 AWS 组织级别（通过使用委托管理员功能）配置和管理 AmazonGuardDuty，在那里可以汇总查看和管理调查结果。



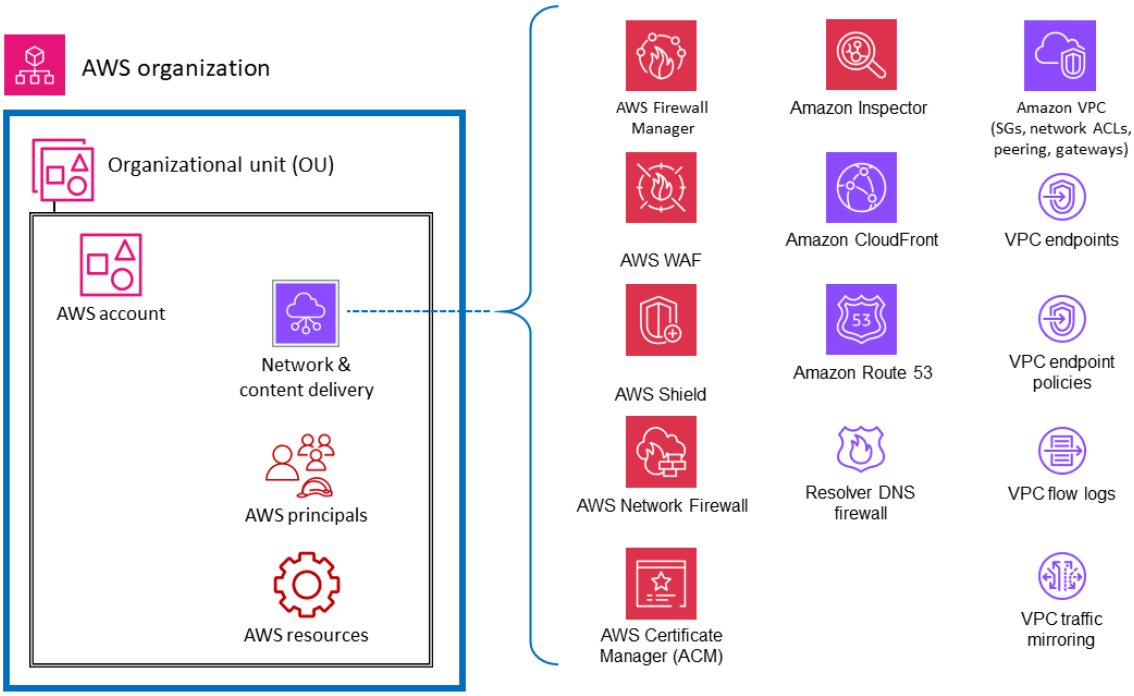
AWS 账户

在 OU 中，有一些服务可帮助保护 AWS 账户中的多种类型的元素。例如，AWS Secrets Manager 通常由特定账户进行管理，并保护该账户中的资源（例如数据库凭证或身份验证信息）、应用程序和 AWS 服务。可以将 AWS IAM Access Analyzer 配置为在 AWS 账户之外的委托人可以访问指定资源时生成调查结果。如上一节所述，其中许多服务也可以在 AWS Organizations 中配置和管理，因此可以跨多个账户进行管理。这些服务在图中以星号 (*) 表示。它们还使汇总来自多个账户的结果并将其发送到单个账户变得更加容易。这为各个应用程序团队提供了灵活性和可见性，使他们能够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。亚马逊GuardDuty就是此类服务的一个例子。GuardDuty监控与单个账户相关的资源和活动，可以从委托管理员账户收集、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，可持续扫描您的 AWS 工作负载以查找漏洞。这些扫描包括网络可达性检查，这些检查表明您的环境中允许通往 Amazon EC2 实例。通过 Amazon Virtual Private Cloud on Valtuam VPC，您可以定义一个虚拟网络，您可以在该网络中启动 AWS 资源。此虚拟网络与传统网络极为相似，包含各种功能和优点。VPC 终端节点使您能够将 VPC 私密地连接到支持的 AWS 服务和 AWS 提供支持的 AWS 服务，PrivateLink而无需通往互联网的路径。下图说明了侧重于网络、计算和内容交付基础架构的安全服务。



校长和资源

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

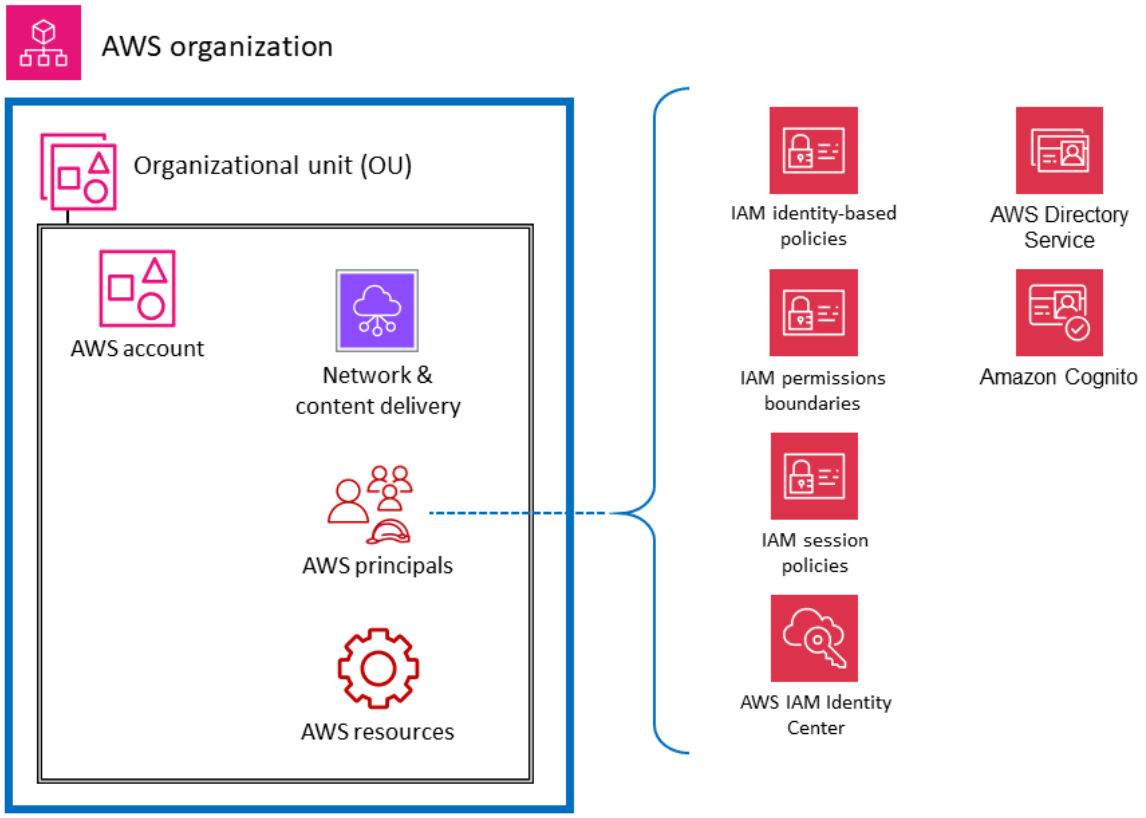
Note

不要创建与 AWS 根用户关联的永久性 API 密钥。根用户的访问权限应仅限于需要根用户的任务，然后只能通过严格的例外和批准流程。有关保护账户根用户的最佳实践，请参阅 AWS 文档。

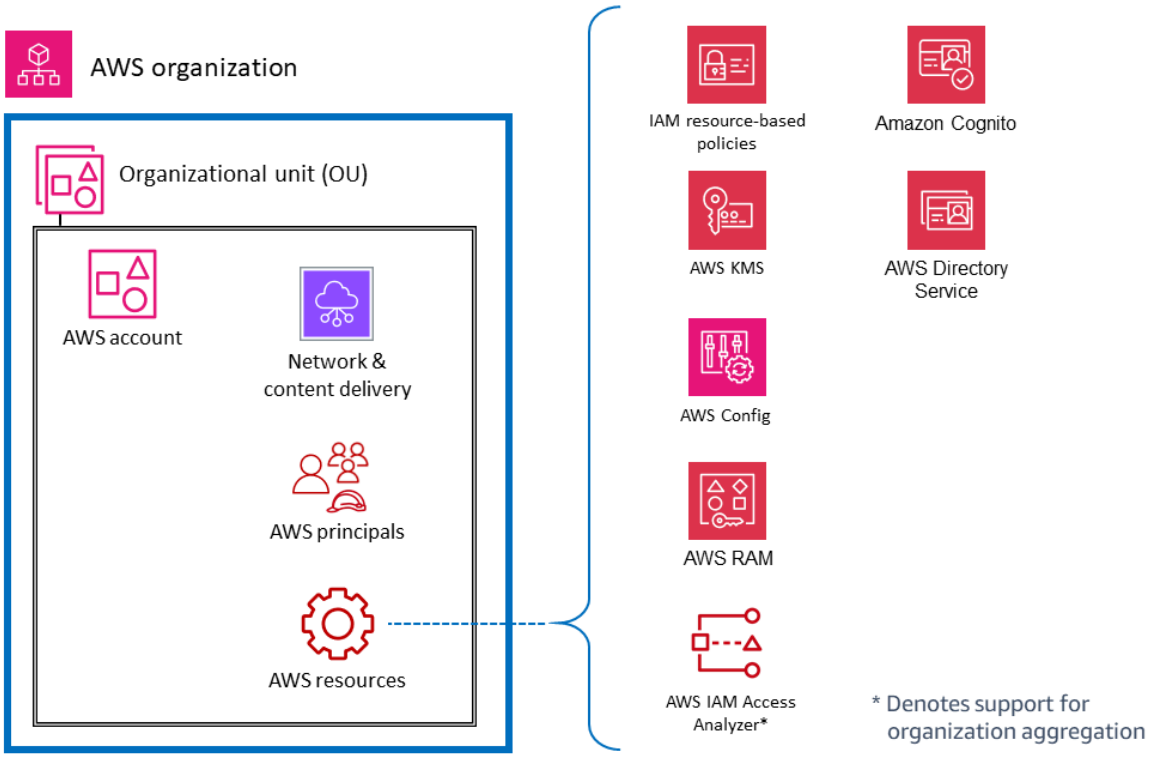
AWS 资源是位于AWS 服务中的对象，您可以使用。示例包括 EC2 实例、AWSCloudFormation 堆栈、Amazon ServSimple Notification Service (Amazon SNS) 主题和 S3 存储桶。IAM 策略是定义权限的对象，当它们与 IAM 身份（用户、组或角色）或 AWS 资源关联时，IAM 策略是定义权限的对象。基于身份的策略文档，附加到委托人（角色、用户和用户组），用于控制委托人可在什么样的条件下对哪些资源执行哪些操作。基于资源的策略是附加到资源（如 S3 存储桶）的策略文档。这些策略授予指定的主体对该资源执行特定操作的权限，并定义该权限的条件。基于资源的策略是内联策略。I AM 资源 (p. 54)部分深入探讨了 IAM 策略的类型及其使用方式。

为简单起见，在本讨论中，我们列出了主要用于在账户委托人上运营或应用于账户委托人的 IAM 实体的 AWS 安全服务和功能。我们在保持这种简单性的同时，承认 IAM 权限策略的灵活性和影响范围。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，尽管基于身份的 IAM 策略与 IAM 实体关联并定义了该实体的权限（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元素。

下图说明了适用于 AWS 委托人的 AWS 安全服务和功能。基于身份的策略附加到 IAM 资源对象，例如用户、组和角色。这些策略可让您指定该身份可执行哪些操作（其权限）。IAM 会话策略是一种内联权限策略，用户在担任角色时在会话中传递该策略。您可以自己传递策略，也可以将您的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他们必须创建的角色数量，因为多个用户可以担任相同的角色但具有唯一的会话权限。IAM Identity Center 服务与 AWS Organizations 和 AWS API 操作集成在一起，可帮助您管理 AWS AWS Organizations 中 AWS 账户的 SSO 访问和用户权限。



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、Amazon Simple Queue Service (Amazon SQS) 队列、VPC 终端节点和 AWS KMS 加密密钥。您可以使用基于资源的策略来指定哪些用户有权访问资源，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类型。AWS IAM Acess 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。这可以帮助您识别对资源和数据的意外访问，此类访问会带来安全风险。AWS Config 使您能够评估、审计和评估您的 AWS 账户中支持的 AWS 资源配置。AWS Config 持续监控和记录 AWS 资源配置，并根据所需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

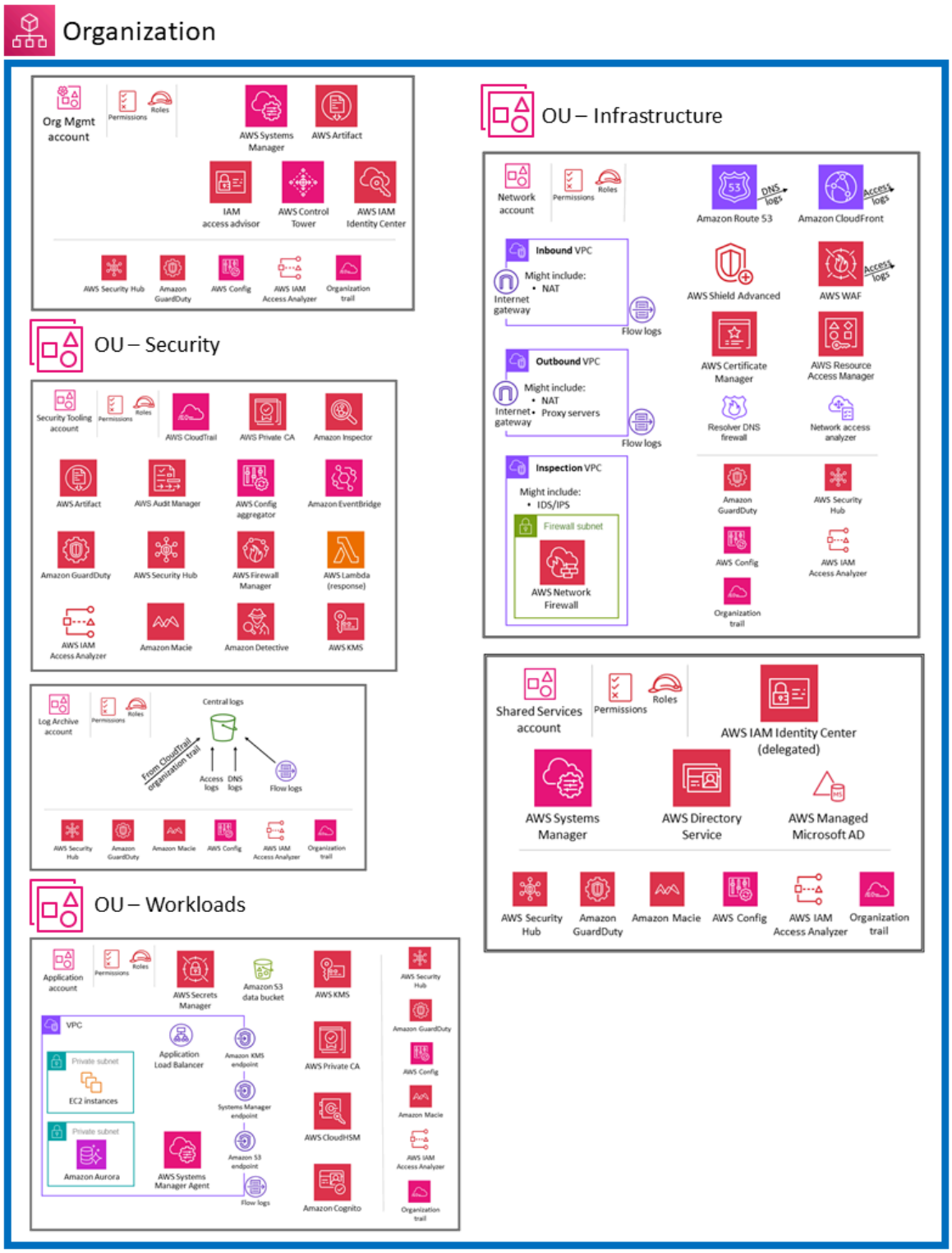
AWS 安全参考架构

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

下图说明了AWS 过程。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 架构构构构建，可以容纳在单个页面上。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，该层处理应用程序的实际业务逻辑：从用户那里获取输入、进行一些计算并生成输出。应用程序层存储和检索数据层中的信息。该架构特意采用模块化结构，为许多现代 Web 应用程序提供高级抽象。

注意

为简单起见，下图故意以较高的层次显示了架构，并掩盖了每个账户的详细信息。要更详细地查看单个帐户的图表，请参阅 OU 和帐户的单独部分。
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）



对于此参考架构，特意通过亚马逊Elastic Compute Cloud (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于并深入研究 Web、应用程序和数据层。为了便于阅读，他们经常省略安全控件。此图突显了重点，尽可能地显示了安全性，并尽可能简化了应用程序和数据层，从而有意义地展示了安全功能。

AWS SRA 包含发布时可用的所有 AWS 安全相关服务。（请参阅文档历史记录 (p. 61)。）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，这样您的企业就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。

以下部分将介绍每个 OU 和账户，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：

- 简要概述 AWS SRA 中的元素及其安全目的。有关各项服务的更多详细描述和技术信息，请参阅附录 (p. 59)。
- 推荐放置位置，以最有效地启用和管理服务。这是在每个账户和 OU 的单独架构图中记录的。
- 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，该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所致），则文档描述了这些选项。

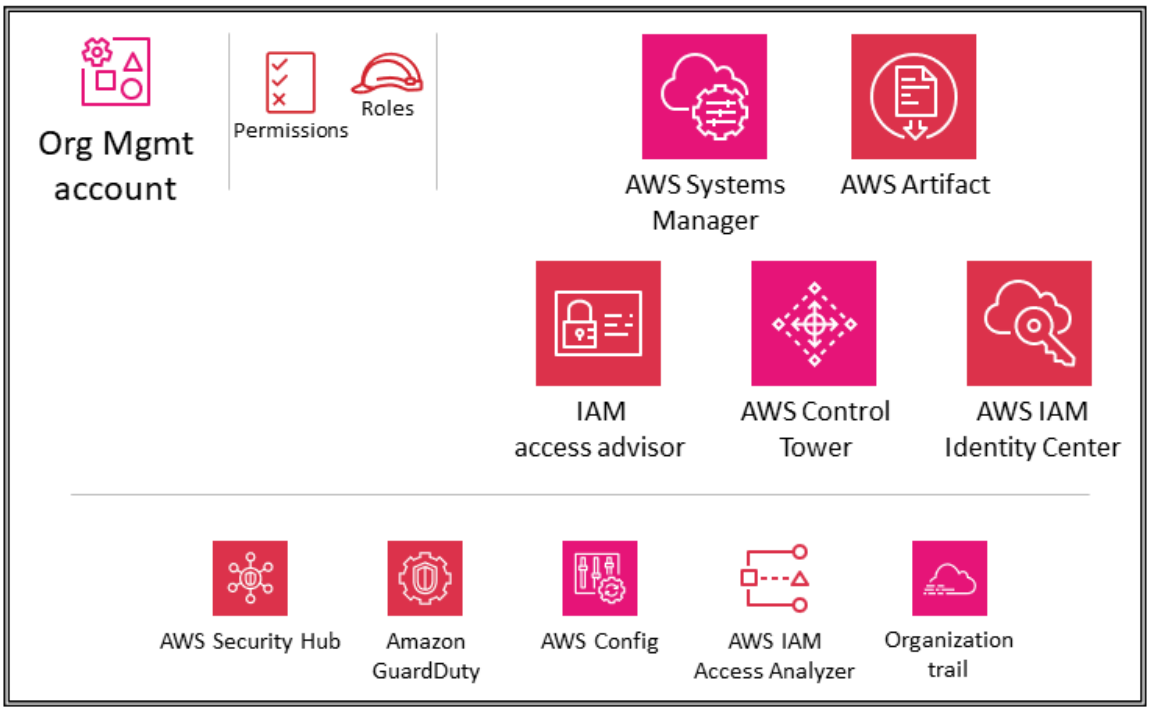
OU 和账户

- 组织管理账户 (p. 21)
- 安全 OU — 安全工具帐户 (p. 25)
- 安全 OU — 日志存档账户 (p. 36)
- 基础架构 OU — 网络账户 (p. 38)
- 基础架构 OU — 共享服务账户 (p. 44)
- 工作负载 OU — 应用程序帐户 (p. 47)

组织管理账户

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

下图说明了在组织管理账户中配置的 AWS 安全服务。



本指南前面的 “使用 AWS Organizations 实现安全 (p. 7)” 和 “管理账户、可信访问和委托管理员 (p. 8)” 部分深入讨论了组织管理账户的用途和安全目标。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在账户上附加电话号码），为所有用户启用多重身份验证 (MFA)，以及定期检查谁有权访问组织管理账户。应使用适当的角色、信任策略和其他权限配置在组织管理账户中部署的服务，这样这些服务的管理员（必须通过组织管理帐户访问这些服务）也不会不恰当地访问其他服务。

服务控制策略

借助 AWS O rganizations，您可以集中管理多个 AWS 账户的策略。例如，您可以将服务控制策略 (SCP) 应用于作为组织成员的多个 AWS 账户。SCP 允许您定义哪些 AWS 服务 API 可以和不能由您组织的成员 AWS 账户中的 AWS Identity and Access Manag ement (IAM) 实体（例如 IAM 用户和角色）运行。SCP 是从组织管理账户创建和应用的，该账户是您在创建组织时使用的 AWS 账户。在本参考资料前面的 “使用 AWS Organizations 实现安全 (p. 7)” 部分中阅读有关 SCP 的更多信息。

如果您使用 AWS Control Tower 管理您的 AWS 组织，它将部署一组 SCP 作为预防性护栏（归类为强制性、强烈推荐或选修性）。这些护栏通过实施组织范围的安全控制来帮助您管理资源。这些 SCP 会自动使用值为的aws-control-tower标签managed-by-control-tower。

设计注意事项

- SCP 仅影响 AWS 组织中的成员账户。尽管它们是从组织管理账户中应用的，但它们对该账户中的用户或角色没有任何影响。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 AWS 博客文章如何在 AWS Organizations 中使用服务控制策略。

IAM Identity Center

AWS IAM Identity Center（AWS Single Sign-On 的继任者）是一项身份联合服务，可帮助您集中管理对所有 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。批量和just-

in-time配置可以通过使用跨域身份管理系统 (SCIM) 来完成。IAM Identity Center 还可以通过使用 AWS 目录服务，以身份提供商的身份与本地或 AWS 管理的 Microsoft Active Directory (AD) 域集成。IAM Identity Center 包括一个用户门户，您的最终用户可以在其中找到并访问分配的 AWS 账户、角色、云应用程序和自定义应用程序。

IAM Identity Center 原生与 AWS Organizations 集成，默认情况下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 管理权委托给特定的成员账户。在 AWS SRA 中，共享服务账户是 IAM 身份中心的委托管理员账户。在为 IAM 身份中心启用委托管理之前，请查看这些注意事项。您可以在 Shared Services 帐户 (p. 44)部分找到有关委派的更多信息。即使在您启用委派之后，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预置的权限集。

在 IAM Identity Center 控制台中，账户由其封装的 OU 显示。这使您能够快速发现您的 AWS 账户、应用常用权限集并从中心位置管理访问权限。

IAM Identity Center 包括一个身份存储，其中必须存储特定的用户信息。但是，IAM 身份中心不一定是劳动力信息的权威来源。如果您的企业已经拥有权威来源，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。创建用户、进行群组分配，并在身份存储中分配权限。即使您的权威来源不在 IAM Identity Center 之外，主体属性的副本也将存储在身份存储中。
- Microsoft Active Directory (AD) — 如果您想继续管理适用于 Microsoft Active DireAWS Directory Service Directory 中的目录或 Active Directory 中自
- 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。

您可以依靠企业中已经存在的现有 IdP。这样可以更轻松地管理多个应用程序和服务的访问权限，因为您要从一个位置创建、管理和撤消访问权限。例如，如果有人离开您的团队，您可以从一个位置撤消他们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) 流程整合的机会。

设计注意事项

- 如果您的企业可以使用外部 IdP，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，对于新员工、即将调到另一个团队的员工和即将离开公司的员工，AWS 的访问权限可以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。

IM 访问顾问

IAM 访问顾问以您的 AWS 账户和 OU 的上次访问服务信息的形式提供可追溯性数据。使用此侦探控件为最低权限策略做出贡献。对于 IM 实体，您可以查看两种类型的上次访问信息：允许AWS M 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 组织中组织管理账户、OU、成员账户或 IAM 策略的上次访问服务数据。这些信息可在管理账户的 IAM 控制台中获得，也可以通过 AWS Command Line Interface (AWS CLI) 中的 IAM 访问顾问 API 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。上次访问的信息可让您深入了解实际服务使用情况（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

作为 AWS Systems Manag er 的功能，Quick Setup 和 Explorer 均支持 AWS Organizations，并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。它使组织管理账户能够轻松定义配置，让 Systems Manager 代表您在 AWS 组织中的各个账户中进行互动。您可以在整个 AWS 组织中启用快速设置，也可以选择特定的 OU。Quick Setup 可以安排 AWS Systems Manager 代理 (SSM Agent) 每两周对您的 EC2 实例运行一次更新，并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控制面板，用于报告有关 AWS 资源的信息。Explorer 显示您的 AWS 账户和 AWS 区域的运营数据的汇总视图。这包括有关您的 EC2 实例的数据和补丁合规性详细信息。在 AWS Organizations 内完成集成设置（还包括Systems ManagerOpsCenter）后，您可以在 Explorer 中按 OU 或整个 AWS 组织聚合数据。Systems Manager 将数据聚合到 AWS xplorer 中，然后在 Explorer 中显示这些数据。

本指南后面的 Workloads OU (p. 47) 部分讨论了在应用程序账户的 EC2 实例上使用Systems Manager 代理 (SSM 代理) 的情况。

AWS Control Tower

AWS Control Tower 提供了一种可设置和管理安全的多账户环境的简单方法，该环境称为landing zone。AWS Control Tower 使用 AWS Organizations 创建您的landing zone，并提供持续的账户管理和监管以及实施最佳实践。您可以使用 AWS Control Tower 通过几个步骤预置新账户，同时确保这些账户符合您的组织政策。您甚至可以将现有账户添加到新的 AWS Control Tower 环境中。

AWS Control Tower 具有广泛而灵活的功能。一项关键功能是它能够协调其他几个 AWS 服务（包括 AWS Organizations、AWS Service Catalog 和 IAM 身份中心）的功能，以构建landing zone。例如，默认情况下，AWS Control Tower 使用 AWSCloudFormation 建立基准，使用 AWS Organizations 服务控制策略 (SCP) 来防止配置更改，使用 AWS Config 规则来持续检测不合规情况。AWS Control Tower 采用蓝图来帮助您快速调整您的多账户 AW S 环境与 AWS 架构完善的安全基础设计原则。在监管功能中，AWS Control Tower 提供的防护栏可防止部署不符合选定策略的资源。

您可以开始使用 AWS 控制塔实施 AWS SRA 指南。例如，AWS Control Tower 使用推荐的多账户架构建立一个 AWS 组织。它提供蓝图以提供身份管理、提供账户的联合访问权限、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现账户基准。

在 AWS SRA 中，AWS Control Tower 位于组织管理账户内，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。此账户用于整个 AWS 组织的账单。它还用于Account Factory 配置账户、管理 OU 和管理护栏。如果您在现有 AWS 组织中启动 AWS Control Tower，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

- 如果您想对各个账户的控制和配置进行额外的基准设置，可以使用 AWS Control Tower (cFcT) 的自定义。借助 CfCT，您可以使用 AWSCloudFormation 模板和服务控制策略 (SCP) 自定义 AWS Control Tower landing zone。您可以将自定义模板和策略部署到组织内的单个账户和 OU。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 Arti fact 提供对 AWS 安全与合规性报告以及精选在线协议的按需访问。AWS Artifact 中提供的报告包括系统和组织控制 (SOC) 报告、支付卡行业 (PCI) 报告，以及来自不同地域和合规垂直领域的认证机构的认证，用于验证 AWS 安全控制的实施和运营有效性。AWS Artifact 可帮助您执行 AWS 的尽职调查，提高我们安全控制环境的透明度。它还允许您通过即时访问新报告来持续监控 AWS 的安全性和合规性。

AWS Artifact 协议使您能够查看、接受和跟踪 AWS 协议的状态，例如针对个人账户和 AWS Organizations 中属于您组织的账户的商业伙伴附录 (BAA)。

您可以将 AWS 审计文件提供给您的审计师或监管机构，作为 AWS 安全控制的证据。您还可以使用某些 AWS 审计项目提供的责任指导来设计您的云架构。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 Artifacts 托管在组织管理账户中，为您提供一个中心位置，您可以在此查看、接受和管理与 AWS 的协议。这是因为管理账户接受的协议会流向下流向成员账户。

设计注意事项

- 应限制组织管理账户内的用户只能使用 AWS Artifact 的协议功能，不得使用其他任何功能。为了实现职责分离，AWS Artifact 还托管在 Security Tooling 账户中，您可以在该账户中向合规利益相关者和外部审计员授予访问审计对象的权限。您可以通过定义细粒度的 IAM 权限策略来实现这种分离。有关示例，请参阅 AWS 文档中的 IA M 策略示例。

分布式和集中式安全服务护栏

在 AWS SRA 中，AWS Security HubGuardDuty、亚马逊、AWS Config、IAM 访问分析器、AWSCloudTrail 组织跟踪以及 Amazon Macie 通常是在向安全工具账户进行适当的委托管理或聚合的情况下部署的。这可以实现跨账户的一系列一致的防护措施，还可以在整个 AWS 组织中提供集中监控、管理和监管。您可以在 AWS SRA 中代表的每种账户中找到这组服务。这些应该是 AWS 服务的一部分，必须作为账户入门和基准设定流程的一部分进行配置。GitHub代码存储库提供了在您的账户（包括 AWS 组织管理账户）上实现以安全为重点的 AWS 服务的示例。

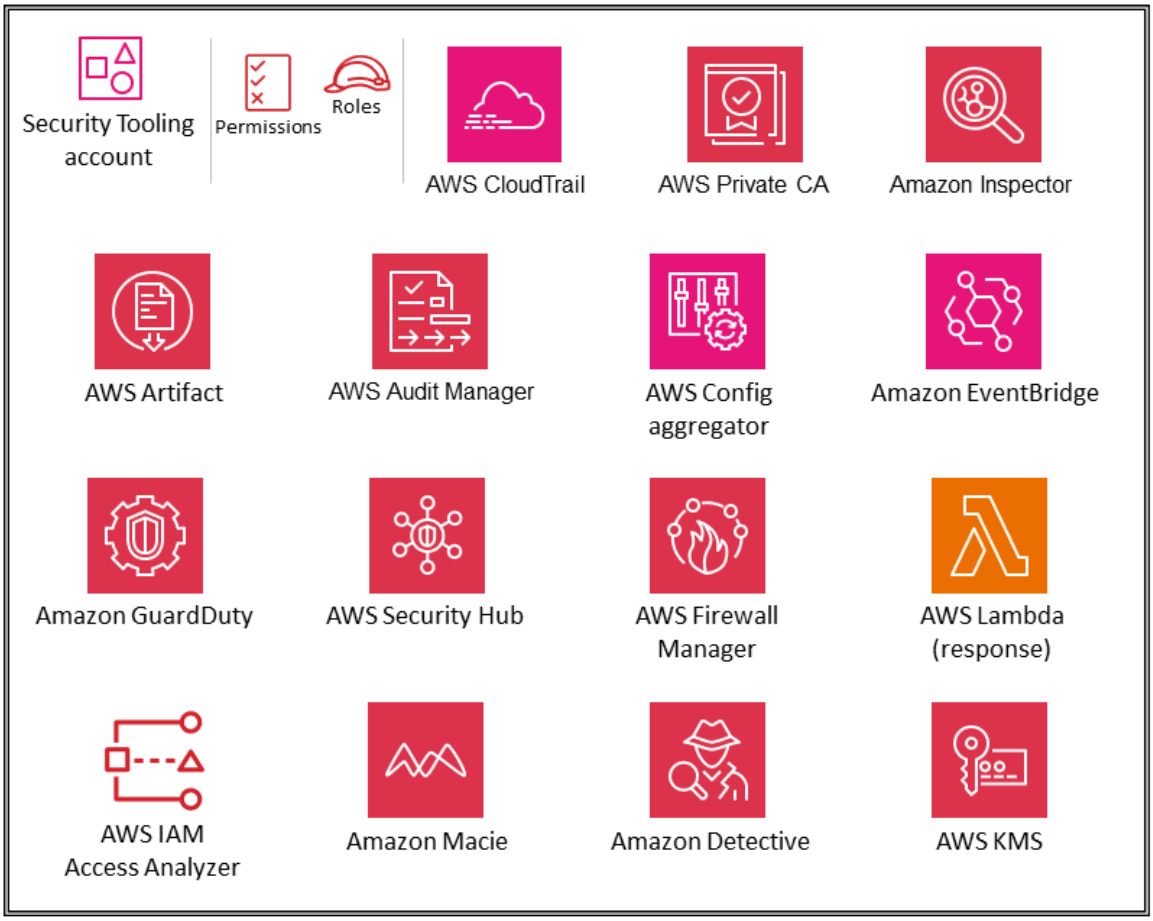
除这些服务外，AWS SRA 还包括两项以安全为重点的服务，即 Amazon Detective 和 AWS Audit Manager，它们支持 AWS Organizations 中的集成和委派管理员功能。但是，这些并未作为账户基准确定推荐服务的一部分包括在内。我们已经看到，这些服务最适合在以下场景中使用：

- 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。Amazon Detective 最适合安全分析团队使用，而 AWS 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，然后使用提供额外功能的服务在这些工具的基础上进行构建。

安全 OU — 安全工具帐户

通过简短的调查影响AWS安全参考架构 (AWSSRA) 的future。

下图说明了在安全工具账户中配置的 AWS 安全服务。



安全工具账户专门用于运营安全服务、监控 AWS 账户以及自动发送安全警报和响应。安全目标包括以下几个：

- 提供具有受控访问权限的专用账户，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。
- 通过维护对适当的安全配置和操作（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，而写入/修改角色的数量有限，受到严格控制、监控和记录。

设计注意事项

- 默认情况下，AWS Control Tower 将安全 OU 下的账户命名为审计账户。您可以在 AWS Control Tower 设置期间重命名账户。
- 拥有多个安全工具帐户可能是合适的。例如，监控和响应安全事件通常分配给专门的团队。网络安全可能需要与云基础架构或网络团队合作，拥有自己的帐户和角色。这种分割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、最低权限和团队任务的潜在简单性。如果您使用的是 AWS Control Tower，它会限制在安全 OU 下创建其他 AWS 账户。

安全服务的委托管理员

Security Tooling 账户充当安全服务的管理员账户，这些服务在整个 AWS 账户中以管理员/成员结构进行管理。如前所述，这是通过 AWS Organizations 委托管理员功能处理的。AWS SRA 中目前支持委托管理员的服务包括 AWS Config、AWS Firewall Manager、AWS IAM Access Analyz GuardDuty er、Amazon Macie、AWS Security Hub、Amazon Detective、AWS Audit Manager 器、AWS 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。

IAM 身份中心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，如稍后共享服务账户的 IAM 身份中心 (p. 46)部分所述。

AWS CloudTrail

AWS CloudTrail 是一项支持管理、合规和审计您的 AWS 账户中活动的服务。借助CloudTrail，您可以记录、持续监控和保留与您的 AWS 基础设施中的操作相关的账户活动。CloudTrail与 AWS Organizations 集成，该集成可用于创建单个跟踪。这称为组织跟踪。您只能从组织的管理帐户或委托的管理员帐户中创建和管理组织跟踪。当您创建组织跟踪时，将在属于您的 AWS 组织的每个 AWS 账户中创建具有您指定名称的跟踪。此跟踪会记录 AWS 组织中包括管理账户在内的所有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 (p. 37)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线索。但是，成员 AWS 账户拥有此跟踪的仅限查看权限。默认情况下，在CloudTrail控制台中创建组织跟踪时，此跟踪为多区域跟踪。有关其他安全最佳实践，请参阅 A WS CloudTrail 文档。

在 AWS SRA 中，安全工具账户是用于管理CloudTrail的委托管理员账户。用于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。这是为了将CloudTrail日志权限的管理和使用分开。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 AWS CloudTrail 文档。

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

设计注意事项

- 如果成员账户需要访问自己账户CloudTrail的日志文件，则可以选择性地从中央 S3 存储桶共享组织的CloudTrail日志文件。但是，如果成员帐户需要本地CloudWatch日志组来存储其帐户CloudTrail的日志，或者想要以不同于组织跟踪的方式配置日志管理和数据事件（只读、只写、管理事件、数据事件），则他们可以使用相应的控件创建本地跟踪。本地账户特定的跟踪会产生额外费用。

AWS Security Hub

AWS Security Hub 提供了 AWS 中安全状况的全面视图，可帮助您检查环境是否符合安全行业标准和最佳实践。Security Hub 从跨 AWS 集成服务、受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。除了采集的来源外，Security Hub 还会生成自己的调查结果，这些发现由与一个或多个安全标准对应的安全控制措施表示。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 修订版 5、支付卡行业数据安全标准 (PCI DSS) 和服务管理标准。有关当前安全标准的列表和特定安全控制的详细信息，请参阅 Security Hub 文档中的 Security Hub 标准参考资料。

Security Hub 与 AWS Organizations 集成，可简化 AWS 组织中所有现有和future 账户的安全状况管理。Security Hub 委托管理员账户（在本例中为安全工具）已自动启用 Security Hub，可以选择要启用的 AWS 账户作为成员账户。Security Hub 委托管理员帐户还可以查看所有成员帐户的调查结果、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收集您的调查结果。您的发现将在聚合器区域和所有其他区域之间持续双向同步。

Security Hub 支持与多个 AWS 服务集成。亚马逊GuardDuty、AWS Config、Amazon Macie、AWS IAM Access Analyzer、AWS Firewall Manager 器、Amazon Inspector tor 和 AWS Systems Manager 此外，你可以从 Security Hub 转向 Amazon Detective 来调查亚马逊的调查GuardDuty结果。Security Hub 建议调整这些服务的委托管理员帐户（如果有），以便更顺畅地集成。例如，如果您没有在 Detective 和 Security Hub 之间调整管理员帐户，则从调查结果切换到 Detective 将不起作用。有关完整列表，请参阅 Security Hub 文档中的 AWS 服务与 Security Hub 集成概述。

您可以将 Security Hub 与 Amazon VPC 的网络访问分析器功能结合使用，以帮助持续监控 AWS 网络配置的合规性。这将帮助您阻止不必要的网络访问，并有助于防止您的关键资源被外部访问。有关架构和实施的更多详细信息，请参阅 AWS 博客文章使用 Amazon VPC 网络访问分析器和 AWS Security Hub 持续验证网络合规性。

除监控外，Security Hub 还支持与亚马逊集成EventBridge，以自动修复特定发现。您可以定义收到查找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。以下两篇 AWS 博客文章中提供了进一步的讨论和示例：使用 AWS S ecurity Hub 进行自动响应和修复，以及如何部署 AWS Security Hub 解决方案自动响应和修复。

Security Hub 使用与服务相关的 AWS Config 规则来执行其大部分安全控制检查。要支持这些控制，必须在每个启用 Security Hub 的 AWS 区域中的所有账户（包括管理员（或委托管理员）账户和成员账户）上启用 AWS Config。

设计注意事项

- 如果Security Hub 中已经存在诸如 PCI-DSS 之类的合规标准，则完全托管的 Security Hub 服务是将其付诸实施的最简单方法。但是，如果您想制定自己的合规性或安全标准，其中可能包括安全性、运营或成本优化检查，AWS Config 一致性包提供了一种简化的自定义方法。（有关 AWS Confg 和一致性包的更多信息，请参阅 AWS Config (p. 29) 部分。
- Security Hub 的常见使用场景包括：
  - 作为控制面板，让应用程序所有者可以查看其 AWS 资源的安全性和合规性状况
  - 作为安全发现的中心视图，安全运营部门、事件响应人员和威胁猎人使用这些视图对各个 AWS 账户和区域的 AWS 安全和合规性发现进行分类并采取行动
  - 汇总来自各个 AWS 账户和区域的安全和合规性调查结果，并将其传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（包括如何设置每个用例）的更多指导，请参阅博客文章 S ecurity Hub 的三种重复使用模式以及如何部署它们。

执行示例

A WS SRA 代码库提供了 S ecurity Hub 的示例实现。它包括自动启用服务、向成员账户（安全工具）进行委托管理，以及为 AWS 组织中的所有现有和future 账户启用 Security Hub 的配置。

AWS GuardDuty

亚马逊GuardDuty是一种威胁检测服务，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用于监控和审计，但亚马逊会直接从 AWS、Amazon VPC 流日志和 AWS CloudTrail 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GuardDuty来撤消这些角色。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。其中包括 EKS 保护、RDS 保护、S3 保护、恶意软件保护和 Lambda 防护。对于新探测器，这些可选功能默认处于启用状态，但 EKS 保护除外，后者必须手动启用。

- 借助 GuardDutyS3 保护，除了GuardDuty监控默认CloudTrail管理事件外，还可以监控 Amazon S3 数据事件。CloudTrail监控数据事件可以监控对象级 API 操作，GuardDuty以防您的 S3 存储桶中数据的潜在安全风险。
- GuardDuty恶意软件保护通过对连接Amazon EC2 Elastic Block Store (Amazon EBS) 卷上启动无代理扫描。
- GuardDutyRDS 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。
- GuardDutyEKS 保护包括 EKS 审核日志监控和 EKS 运行时系统监控。使用 EKS 审核日志监控，GuardDuty监控来自 Amazon E KS 集群的 Kubernetes 审核日志，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 Amazon EKS 的附加组件）来提供对单个 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。它还可以检测到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通过 AWS Organizations 在所有账户中启用，所有发现均可由GuardDuty委托管理员账户（在本例中为 Security Tooling 账户）中的相应安全团队查看和采取行动。

启用 AWS Security Hub 后，GuardDuty调查结果会自动流向Security Hub。启用 Amazon Detective 后，GuardDuty调查结果将包含在Detective 日志采集过程中。GuardDuty而且 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，可将你从选定的发现重定向到Detective 页面，该页面包含一组用于调查该发现的精选可视化效果。例如，您还可以GuardDuty与亚马逊集成EventBridge，自动执行最佳实践GuardDuty，例如自动对新GuardDuty发现做出响应。

执行示例

A WS SRA 代码库提供了亚马逊GuardDuty的示例实现。它包括加密 S3 存储桶配置、委托管理以及 AWS 组织中所有现有和future 账户的GuardDuty支持。

AWS Config

AWS Config 是一项服务，可让您评估、审计和评估您的 AWS 账户中受支持的 AWS 资源配置。AWS Config 持续监控和记录 AWS 资源配置，并根据所需配置自动评估记录的配置。您还可以将 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 可以在 AWS Secrets Manager 中监视个人密钥的变化。

您可以使用 AWS Config 规则评估您的 AWS 资源的配置设置。AWS Config 提供了一个可自定义的预定义规则库，称为托管规则，或者您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）或侦测模式（部署资源之后）运行 AWS Config 规则。可以在配置发生更改时评估资源，也可以定期评估资源，或者同时评估两者。

一致性包是 AAWS Config 规则和补救操作的集AWS Organizations。一致性包是通过创建 YAML 模板创建的，该模板包含 AWS Config 托管或自定义规则和补救操作列表。要开始评估您的 AWS 环境，请使用一致性包模板示例。

AWS Config 与 AWS Security Hub 集成，将 AWS Config 托管规则和自定义规则评估的结果作为调查结果发送到Security Hub。

AWS Config 规则可以与 AWS Systems Manager 结合使用，以有效修复不合规的资源。您可以使用 AWS Systems Manager Explorer 在您的 AWS 账户中收集 AWS Config 规则的合规性状态，然后使用 S ystems Manager 自动化文档（运行手册）来解决不合规的 AWS Config 规则。有关实施细节，请参阅博客文章使用 AWS S ystems Manager 自动化运行手册修复不合规的 AWS Config 规则。

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（分为强制性、强烈推荐或选择性）。这些防护栏可帮助您管理资源并监控 AWS 组织中各个账户的合规性。这些 AWS Config 规则将自动使用值为的`aws-control-tower`标签`managed-by-control-tower`。

必须为 AWS 组织和 AWS 区域中包含您要保护的资源的每个成员账户启用 AWS Config。您可以集中管理（例如，创建、更新和删除）您的 AWS 组织内所有账户的 AWS Config 规则。通过 AWS Config 委托管理

员账户，您可以在所有账户中部署一组通用 AWS Config 规则，并指定不应在其中创建 AWS Config 规则的账户。AWS Config 委托管理员账户还可以聚合所有成员账户中的资源配置和合规性数据。使用委托管理员账户的 API 通过确保 AWS 组织中的成员账户无法修改底层 AWS Config 规则来实施治理。

设计注意事项

- AWS Config 将配置和合规性更改通知流式传输到亚马逊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，以便将特定类型的通知路由到特定目标。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路由到外部 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 命令行接口 (CLI) 为您提供一种声明性域特定语言 (DSL)，您可以使用该语言将策略表示为代码。此外，您可以使用 CLI 命令验证 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。

执行示例

AWS SRA 代码库提供了将 AWS Config 合规包部署到 AWS 组织内的所有 AWS 账户和区域的示例实现。AWS Config 聚合器模块可帮助您配置 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），然后在委托管理员账户中为 AWS 组织中的所有现有和future 账户配置 AWS Config 聚合器。您可以使用 AWS Config Control Tower 管理账户模块在组织管理账户中启用 AWS Config，AWS Control Tower 未启用它。

Amazon Macie

Amazon Macie 是一个完全托管式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并帮助保护 AWS 中的敏感数据。您需要确定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。您可以通过两种方式使用 Macie 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作业。通过自动发现敏感数据，Macie 每天评估您的 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方面的潜在问题。默认情况下，所有新 Macie 客户均启用自动数据发现，现有 Macie 客户只需点击一下即可启用自动数据发现。

通过 AWS Organizations 在所有账户中启用 Macie。在委托管理员帐户（在本例中为 Security Tooling 帐户）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。敏感数据发现只能由创建敏感发现任务的帐户查看。有关更多信息，请参阅 Macie 文档中的在 Amazon Macie 中管理多个账户。

Macie 的调查结果将流向 AWS Security Hub 进行审查和分析。Macie 还与 Amazon EventBridge 集成，便于自动响应警报、向安全信息和事件管理 (SIEM) 系统反馈以及自动补救等调查结果。

设计注意事项

- 如果使用您管理的 AWS Key Management Service (AWS KMS) 密钥加密 S3 对象，则可以将 Macie 服务相关角色作为密钥用户添加到该 KMS 密钥，以使 Macie 能够扫描数据。
- Macie 针对扫描 Amazon S3 中的对象进行了优化。因此，可以扫描任何可放置在 Amazon S3 中（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，Amazon Relational Database Serv ice (Amazon RDS) 或 Amazon Aurora 数据库的定期快照导出、导出的 Amazon DynamoDB 表或从本机或第三方应用程序提取的文本文件）可以移至 Amazon S3 并由 Macie 进行评估。

执行示例

A WS SRA 代码库提供了 A mazon 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 AWS 组织中的所有现有和future 账户配置 Macie。Macie 还配置为将调查结果发送到使用 AWS KMS 中的客户托管密钥加密的中央 S3 存储桶。

AWS IAM Access Analyzer

AWS IAM Acess Analyzer 帮助您识别 AWS 组织和账户中与外部实体共享的资源，例如 Amazon S3 存储桶或 IAM 角色。此检测控件可帮助您识别对数据和资源的意外访问，此类访问会带来安全风险。IAM Acess Analyzer 还可以帮助您根据策略语法和最佳实践验证 IAM policy，并根据 AWS CloudTrail 日志中的访问活动生成 IAM policy。

Access Analyzer 通过 AWS Organizations 中的委托管理员功能部署在安全工具账户中。委托管理员有权创建和管理将 AWS 组织作为信任区域的分析器。Access Analyzer 的调查结果会自动流向Security Hub。Acess Analyzer 还EventBridge针对每个生成的结果、现有结果状态更改以及删除结果的时间向。EventBridge可以进一步将这些事件定向到通知或补救流。

设计注意事项

- 要获得账户范围内的调查结果（其中账户充当可信边界），你需要在每个成员账户中创建一个账户范围内的分析器。这可以作为账户管道的一部分来完成。账户范围内的调查结果在成员账户级别流入 Security Hub。它们从那里流向 Security Hub 委托管理员帐户（安全工具）。

执行示例

A WS SRA 代码库提供了 IAM 访问分析器的示例实现。它演示了如何在委托管理员帐户中配置组织级分析器，并在每个帐户中配置帐户级分析器。

AWS Firewall Manager

AWS Firewall Manager 通过简化跨多个账户和资源的 AWS WAF、AWS Shield Advanced、亚马逊 VPC 安全组、AWS Network Firewall 和 Route 53 Resolver DNS 防火墙的管理和维护任务，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 Advanced 保护、Amazon VPC 安全组、AWS Network Firewall 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。

如果要保护整个 AWS 组织而不是少量特定账户和资源，或者经常添加要保护的新资源，Firewall Manager 尤其有用。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账户和 VPC。即使创建了新帐户和资源，这些策略也会自动持续执行您配置的规则。通过 AWS Organizations 在所有账户中启用Firewall Manager，配置和管理由Firewall Manager 委托管理员账户（在本例中为安全工具账户）中的相应安全团队执行。

您必须为包含要保护的资源的每个 AWS 区域启用 AWS Config。如果您不想为所有资源启用 AWS Config，则必须为与您使用的Firewall Manager 策略类型相关的资源启用它。当您同时使用 AWS Security Hub 和 Firewall Manager 时，Firewall Manager 会自动将您的发现发送到 Security Hub。Firewall Manager 会针对不合规的资源和检测到的攻击创建调查结果，并将发现结果发送到 Security Hub。当您为 AWS WAF 设置 Firewall Manager 策略时，您可以为所有范围内的账户集中启用 Web 访问控制列表 (Web ACL) 的日志登录，并将日志集中到单个账户下。

设计注意事项

- AWS 组织中单个成员账户的账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制措施（例如 AWS WAF 规则和 Amazon VPC 安全组）。

执行示例

AWS SRA 代码库提供了 AW S Firewall Manager 器的示例实现。它演示了委托管理（安全工具）、部署允许的最大安全组、配置安全组策略以及配置多个 WAF 策略。

Amazon EventBridge

Amazon EventBridge 是一种无服务器事件总线服务，可以轻松地将应用程序与来自各种来源的数据相连接。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，以构建可对所有数据源做出实时反应的应用程序架构。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。您可以在安全工具账户中创建事件总线，该总线可以接收来自 AWS 组织中其他账户的特定安全事件。例如，通过将 AWS Config 规则和 Security Hub 与EventBridge，您可以创建灵活的自动化管道，用于路由安全数据、发出警报和管理解决问题的操作。GuardDuty

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各个 AWS Lambda 响应者联系起来，后者会采取适当的操作。例如，在某些情况下，您可能需要使用公共 S3 存储桶查找结果路由EventBridge到更正存储桶策略并移除公共权限的 Lambda 响应器。这些响应者可以集成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、错误/问题系统或其他安全信息和事件管理 (SIEM) 系统。这样可以减少电子邮件和静态报告的工作流程，并帮助您传送、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 让安全分析师可以轻松地分析、调查和快速识别安全结果或可疑活动的根本原因。Detective 会自动从 AWS CloudTrail 日志和 Amazon VPC 流日志中自动提取基于时间的事件，例如登录尝试、API 调用和网络流量。您可以使用 Detective 访问长达一年的历史事件数据。Detective 通过使用独立CloudTrail的日志流和 Amazon VPC 流日志来处理这些事件。Detective 使用机器学习和可视化来创建一个统一的交互视图，显示您的资源行为以及它们之间随时间推移的交互情况，这称为行为图。您可以浏览行为图以检查不同的操作，例如登录尝试失败或可疑的 API 调用。

Detective 还采集了亚马逊GuardDuty发现的调查结果。当账户启用 Detective 时，它将成为行为图的管理员账户。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 Detective。

Detective 会自动将与单个安全漏洞事件相关的多个发现分组为查找组。威胁行为者通常执行一系列操作，这些操作会导致跨时间和资源分布的多个安全发现。因此，寻找小组应是涉及多个实体和调查结果的调查的起点。这有助于缩短分类时间并支持更全面的安全调查。

DDetective ve 与 AWS Organizations gan 组织管理账户将成员账户委托为Detective 管理员账户。在 AWS SRA 中，这是安全工具账户。Detective 管理员账户能够自动将组织中的所有当前成员账户启用为侦探成员账户，还可以在将新成员账户添加到 AWS 组织时添加这些账户。Detective 管理员账户还可以邀请目前不在 AWS 组织内但位于同一地区的成员账户向主账户的行为图提供数据。当成员账户接受邀请并启用时，Detective 开始提取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 控制台查找配置文件。这些链接可以帮助简化调查流程。您的帐户必须是Detective 和您从中转出的服务（GuardDuty或 Security Hub）的管理帐户。如果服务的主账户相同，则集成链接可以无缝运行。

Amazon Audit Manager

AWS Audit Manager 帮助您持续审计您的 AWS 使用情况，以简化管理审计以及与相关法规和相关法规和标准的合规性的方式。它使您能够从手动收集、审查和管理证据转变为可自动收集证据、提供跟踪审计证据来源的简单方法、支持团队协作以及帮助管理证据安全性和完整性的解决方案。当需要进行审计时，Audit Manager 可帮助您管理利益攸关方对控件的审核。

使用 Audit Manager，您可以根据互联网安全中心 (CIS) 基准、CIS AWS 基础基准、系统和组织控制 2 (SOC 2) 和支付卡行业数据安全标准 (PCI DSS) 等预建框架进行审计。它还使您能够根据内部审计的具体要求创建带有标准或自定义控制的框架。

Audit Manager 收集四种类型的证据。三种类型的证据是自动生成的：来自 AWS Config 和 AWS Security Hub 的合规性检查证据、来自 AWS CloudTrail 的管理事件证据以及来自 AWS service-to-service API 调用的配置证据。对于无法自动执行的证据，Audit Manager 允许您手动上传证据。

> Note
>
> Audit Manager 协助收集与验证遵守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运营流程的详细信息。Audit Manager 不能替代法律顾问或合规专家。我们建议您聘请经过评估所依据的合规框架认证的第三方评估师的服务。

Audit Manager 评估可以在您的 AWS 组织中的多个账户上运行。Audit Manager 收集证据并将其整合到 AWS Organizations 中的委托管理员账户中。此审计功能主要由合规和内部审计团队使用，只需要您的 AWS 账户的读取权限。

设计注意事项

- Audit Manager 补充了其他 AWS 安全服务，例如 Security Hub 和 AWS Config，以帮助实施风险管理框架。Audit Manager 提供独立的风险保证功能，而 Security Hub 可帮助您监督风险，AWS Config 合规包可帮助您管理风险。熟悉内部审计师协会 (IIA) 开发的三线模型的审计专业人员应注意，这种 AWS 服务组合可以帮助您覆盖三道防线。有关更多信息，请参阅 AWS 云运营与迁移博客上的由两部分组成的博客系列。
- 为了让Audit Manager 收集 Security Hub 证据，这两项服务的委托管理员账户必须是相同的 AWS 账户。因此，在 AWS SRA 中，安全工具账户是Audit Manager 的委托管理员。

AWS Artifact

AWS Arti fact 托管在安全工具账户中，用于从 AWS Org 管理账户委托合规性项目管理功能。这种委托很重要，因为我们建议您避免使用 AWS Org 管理账户进行部署，除非绝对必要。而是将部署委托给成员账户。由于审计项目管理可以通过成员账户完成，并且该职能与安全和合规团队密切相关，因此 Security Tooling 账户被指定为 AWS Artifact 的委托管理员账户。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。您可以将此功能限制为仅限于与您的审计和合规团队相关的 AWS Identity and Access Management (IAM) 角色，以便他们可以根据需要下载、审查这些报告并将其提供给外部审计员。此外，您还可以通过 IAM 策略将特定的 IAM 角色限制为只能访问特定的 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

- 如果您选择为审计和合规团队设立专用 AWS 账户，则可以将 AWS Artifact 托管在与安全工具账户分开的安全审计账户中。AWS Artifact 报告提供的证据表明组织正在遵循记录在案的流程或满足特定要求。在整个系统开发生命周期中收集和归档审计文件，可用作内部或外部审计和评估的证据。

AWS KMS

AWS Key Management Servic e (AWS KMS) 可帮助您创建和管理加密密钥，并控制其在各种 AWS 服务和应用程序中的使用。AWS KMS 是一种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。它遵循密钥材料的行业标准生命周期流程，例如密钥的存储、轮换和访问控制。AWS KMS 可以通过加密和签名密钥帮助保护您的数据，并且可以通过 A WS Encryption SDK 用于服务器端加密和客户端加密。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。客户托管密钥是在您的 AWS 账户中创建、拥有和管理的 AWS KMS 密钥。AWS 托管密钥是由与 AWS KMS 集成的 AWS 服务代表您在您的账户中创建、管理和使用的 AWS KMS 密钥。AWS 自有密钥是 AWS 服务拥有并管理以用于多个 AWS 账户的 AWS KMS 密钥的集合。有关使用 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 KMS 密钥管理的责任集中到单个账户，同时通过使用密钥和 IAM 策略的组合，将应用程序账户中密钥的使用权委托给应用程序资源。这种方法既安全又易于管理，但由于AWS KMS限制限制、账户服务限制以及安全团队被大量处理操作密钥管理任务，您可能会遇到障碍。另一种部署选项是采用去中心化模式，在该模式中，您允许 AWS KMS 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，将影响范围仅限于一个 AWS 账户，并简化报告、审计和其他合规相关任务。在去中心化模式中，部署和强制执行防护非常重要，以便以相同的方式管理去中心化密钥，并根据既定的最佳实践和政策审计 KMS 密钥的使用情况。有关更多信息，请参阅白皮书 AWS Key Management Service (AWS Key AWS SRA 建议采用分布式密钥管理模型，其中 KMS 密钥存储在本地使用它们的账户中。我们建议您避免在一个账户中为所有加密功能使用单个密钥。密钥可以根据功能和数据保护要求创建，以执行最小权限原则。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。

在安全工具账户中，AWS KMS 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 Private Certificate Authority(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、IoT 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（根 CA，通过下属 CA）层次结构，并使用该层次结构创建根 CA 层次结构，并使用该层次结构颁发证书，以便对内部用户、计算机、应用程序、服务、服务器和其他设备进行身份验证。由私有 CA 颁发的证书仅在您的 AWS 组织内部可信，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，必须有允许工作负载团队自助满足其证书要求的规定。AWS SRA 描述了一个集中式 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 CA 共享到应用程序账户，将私有 CA 的私有证书的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使用私有 CA，提供了一种更具成本效益的部署方式。有关工作流程和实施的更多信息，请参阅博客文章如何使用 AWS RAM 共享您的AWS 私有 CA跨账户。

> **Note**
>
> ACM 还可以帮助您预置、管理和部署用于 AWS 服务的公有 TLS 证书。要支持此功能，ACM 必须驻留在将使用公共证书的 AWS 账户中。本指南稍后的 “应用程序帐户 (p. 47)” 部分将对此进行讨论。

设计注意事项

- 使用 AWS 私有 CA，您可以创建最多五级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层次结构应符合您组织的 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 层次结构带来的好处包括适用于每个 CA 的精细安全控制、将下属 CA 委托给不同的应用程序（这会导致管理任务的分工）、使用具有有限可撤消信任的 CA、能够定义不同的有效期以及强制执行路径限制。理想情况下，您的根 CA 和下属 CA 位于不同的 AWS 账

户中。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可以与您现有的 CA 层次结构集成，这允许您将 ACM 的自动化和原生 AWS 集成功能与您目前使用的现有信任根相结合。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 Inspec tor 是一个自动漏洞管理服务，它可以自动发现并扫描 Amazon EC2 实例、Amazon Container Registor（Amazon ECR）中的AWS Lambda mazon Inspector（Amazon ECR）中的自动漏洞管理服务。

每当您对资源进行更改时，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。启动重新扫描资源的事件包括在 EC2 实例上安装新软件包、安装补丁以及何时发布影响该资源的新常见漏洞和暴露 (CVE) 报告。

Amazon Inspector 的网络可访问性调查结果评估了您的 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 (VPN)）的可访问性。这些规则有助于自动监控您的 AWS 网络，并通过管理不当的安全组、访问控制列表 (ACL)、互联网网关等，确定对您的 EC2 实例的网络访问可能存在错误配置的地方。有关更多信息，请参阅 Amazon Inspector 文档。

当 Amazon Inspector 发现漏洞或打开网络路径时，它会得出调查结果。调查结果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，通过将 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）相关联来计算，以提供背景调查结果。

为了扫描漏洞，必须使用 AWS Systems Manager 代理（SSM 代理）在 AWS Systems Manager 中管理 EC2 实例。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。

亚马逊 Inspector 与 AWS Organizations 集成并支持委托管理。在 AWS SRA 中，安全工具账户被设置为 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 组织内的扫描资源。

设计注意事项

- 启用这两项服务后，Amazon Inspector 会自动与 AWS Security Hub 集成。您可以使用此集成将 Amazon Inspector 中的所有结果发送到 Security Hub，Security Hub 将这些结果包含在对您的安保状况分析中。
- Amazon Inspector 会自动将有关结果、资源覆盖范围更改和单个资源的初始扫描的事件导出到 Amazon EventBridge Inspector Service（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 可以用来加密调查结果的 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，将其作为现有安全与合规工作流程的一部分。EventBridge事件除了发布到其来源的成员账户外，还会发布到 Amazon Inspector 委托管理员账户。

执行示例

AWS SRA 代码库提供了 A mazon Inspec tor 的示例实现。它演示了委托管理（安全工具），并为 AWS 组织中的所有现有和future 账户配置 Amazon Inspector。

在所有 AWS 账户中部署通用安全服务

本参考文献前面的 “在您的 AWS 组织中应用安全服务 (p. 12)” 部分重点介绍了保护 AWS 账户的安全服务，并指出其中许多服务也可以在 AWS Organizations 内进行配置和管理。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防护措施，并在整个 AWS 组织内提供集中监控、管理和治理。

Security Hub GuardDuty、AWS Config、Access Analyzer 和 AWS CloudTrail 组织跟踪信息出现在所有账户中。前三个支持前面在 “管理帐户、可信访问和委派管理员” 部分中讨论的委派管理员 (p. 8)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 AWS Org 管理账户）上启用 Security Hub、AWS Config、防火墙管理器和CloudTrail组织跟踪的实施示例。GuardDuty

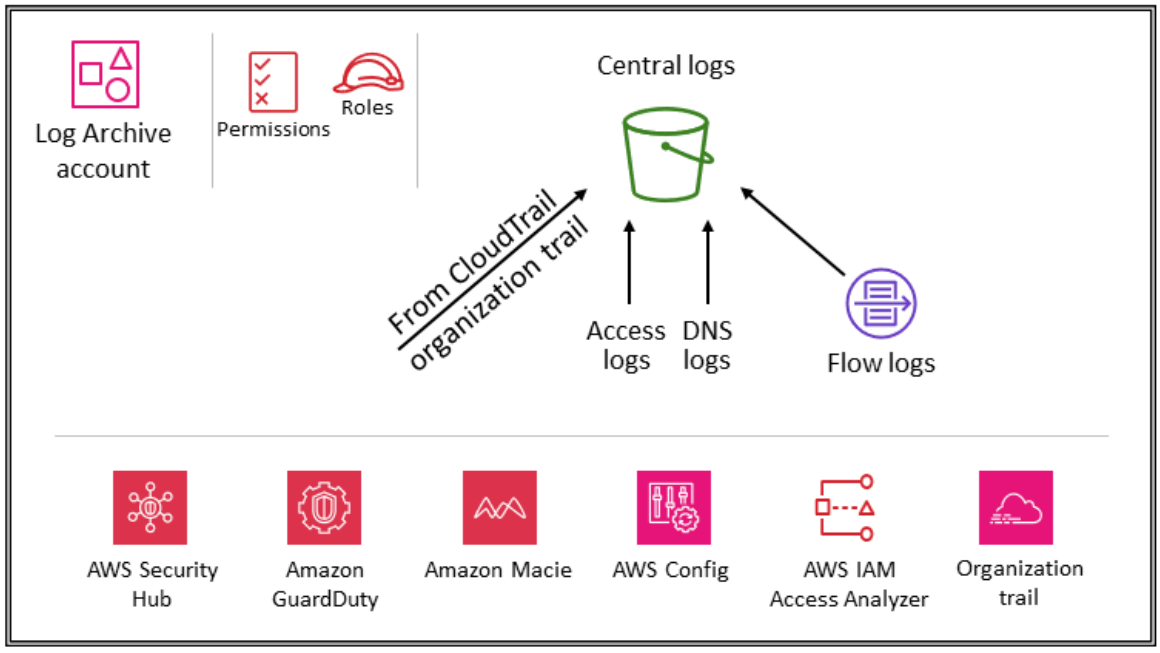
设计注意事项

- 特定的账户配置可能需要额外的安全服务。例如，管理 S3 存储桶的账户（应用程序和日志存档账户）还应包括 Amazon Macie，并考虑在这些常见安全服务中启用 CloudTrail S3 数据事件记录。（Macie 通过集中配置和监控支持委托管理。）另一个例子是 Amazon Inspector，它仅适用于托管 EC2 实例或 Amazon ECR 映像的账户。
- 除了本节前面描述的服务外，AWS SRA 还包括两项以安全为中心的服务，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，因为我们已经发现这些服务最适合用于以下场景：
  - 您有一个专门的团队或一组资源来执行这些职能。Detective 最适合安全分析团队使用，Audit Manager 可以为您的内部审计或合规团队提供帮助。
  - 您希望在项目开始时专注于一组核心工具，例如GuardDuty和 Security Hub，然后使用提供额外功能的服务在这些工具的基础上进行构建。

安全 OU — 日志存档账户

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

下图说明了在日志存档账户中配置的 AWS 安全服务。



Log Archive 帐户专用于接收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、未经授权的身份活动、IAM 策略变更以及在敏感资源上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，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（例如分配最低权限角色以使用受控的 AWS KMS 密钥访问和加密日志）外，还可以使用 AWS Config 等侦测控件来监控（并提醒和修复）此权限集合，以防出现意外变化。

设计注意事项

- 您的基础架构、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合并到日志存档帐户中。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CloudTrail（组织跟踪）、亚马逊 VPC 流日志、来自亚马逊CloudFront和 AWS WAF 的访问日志以及来自 Amazon Route 53 的 DNS 日志。这些日志可对用户、角色、AWS 服务或网络实体（例如，通过 IP 地址识别）采取（或尝试）的操作进行审计。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。

Amazon S3 作为中央日志存储

许多 AWS 服务在 Amazon S3 中记录信息，要么默认，要么只记录信息。AWSCloudTrail、亚马逊 VPC 流日志、AWS Config 和Elastic Load Balancing 是在 Amazon S3 中记录信息的服务的一些示例。这意味着日志完整性通过 S3 对象完整性实现；日志机密性通过 S3 对象访问控制实现；日志可用性通过 S3 对象锁定、S3 对象版本和 S3 生命周期规则实现。通过将信息记录在位于专用账户中的专用和集中化的 Simple Storage（A3）存储桶中，您可以将这些日志，您可以强制实施严格的安全控制、访问和责任划分。

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

上传到 Service Service（Amazon S3）存储桶的所有新对象（包括CloudTrail日志）都默认使用具有 Amazon S3 托管加密密钥（SSE-S3）来加密。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 Service Service Service Service（SSE-KMS）使用使用具有 AWS KMS) 来使用具有 AWS KMS) 来使用具有 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，还必须应用允许他们通过关联密钥策略进行解密的 IAM 策略或角色。

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。CloudTrailCloudTrail 另一个选项是 S3 对象锁定。

除了保护 S3 存储桶本身，您还可以遵守日志服务（例如CloudTrail）和日志存档账户的最小权限原则。例如，拥有 AWS Management IAM 策略授予的用户 AWSCloudTrail_FullAccess能够禁用或重新配置他们的 AWS 账户中最敏感且最重要的审计功能。将此 IAM 策略的应用范围限制为尽可能少的人员。

使用 AWS Config 和 AWS IAM Access Analyzer 提供的侦测控件，监控（并提醒和修复）这一更广泛的预防性控制集合，以防出现意外变化。

要更深入地讨论 S3 存储桶的安全最佳实践，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。

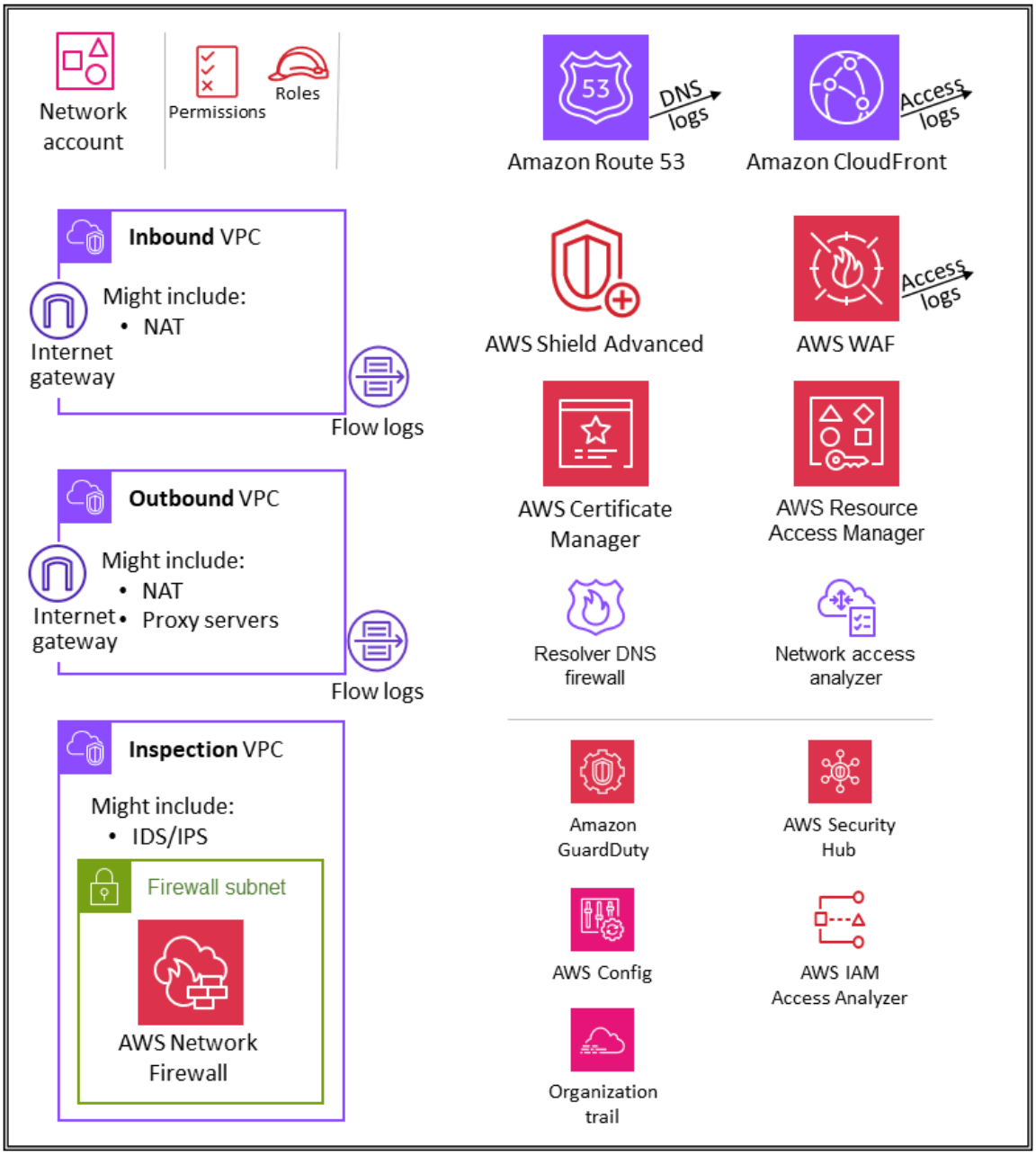
平安的

A WS SRA 代码库提供了 A mazon S3 区块账户公共访问的示例实现。此模块阻止 AWS 组织中所有现有和future 账户的 Amazon S3 公共访问权限。

基础架构 OU — 网络账户

通过简短的调查影响AWS安全参考架构 (AWSSRA) 的future。

下图说明了在网络账户中配置的 AWS 安全服务。



网络帐户管理您的应用程序和更广泛的互联网之间的网关。保护那个双向接口很重要。网络帐户将网络服务、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。这种安排不仅限制了连接、权限和数据流，还支持对需要使用这些账户进行操作的团队进行职责分离和最低权限。通过将网络流量拆分为单独的入站和出站虚拟私有云 (VPC)，您可以保护敏感基础设施和流量免受不必要的访问。入站网络通常被认

为风险较高，值得进行适当的路由、监控和潜在问题缓解。这些基础设施账户将继承组织管理账户和基础架构 OU 的权限护栏。网络（和安全）团队管理该账户中的大部分基础架构。

网络架构

尽管网络设计和具体细节超出了本文档的范围，但我们建议在不同账户之间使用以下三种网络连接选项：VPC 对等、AWS 和 AWS PrivateLink Transit Gateway。在其中进行选择时需要考虑的重要因素是操作规范、预算和特定的带宽需求。

- VPC 对等-连接两个 VPC 的最简单方法是使用 VPC 对等。连接可在 VPC 之间实现完全的双向连接。位于不同账户和 AWS 区域中的 VPC 也可以对等连接在一起。大规模而言，当您拥有数十到数百个 VPC 时，将它们与对等连接互连会形成由数百到数千个对等连接组成的网格，这可能难以管理和扩展。当一个 VPC 中的资源必须与另一个 VPC 中的资源通信，两个 VPC 的环境都受到控制和保护，并且要连接的 VPC 数量少于 10 个（允许对每个连接进行单独管理）时，最好使用 VPC 对等关系。
- AW PrivateLink S-在 VPC、服务和应用程序之间PrivateLink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支持的服务（也称作终端节点服务）。其他 AWS 委托人可以通过接口 VPC 终端节点或 Gateway Load Balancer 终端节点创建从他们的 VPC 到您的终端节点服务的连接，具体取决于服务类型。当您使用时PrivateLink，服务流量不会通过可公开路由的网络。PrivateLink当您要在客户端-服务器设置中为一个或多个消费者 VPC 提供对服务提供商 VPC 中的特定服务或一组实例的单向访问权限时使用。当两个 VPC 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，这样就不会与服务提供商发生 IP 冲突。
- AWS Tran sit Gateway — Transit Gateway 提供了一种无需您预置虚拟设备即可将 VPC 和本地网络作为完全托管的服务进行连接的hub-and-spoke设计。AWS 管理高可用性和可扩展性。传输网关是一种区域资源，可以连接同一 AWS 区域内的数千个 VPC。您可以将混合连接（VPN 和 AWS Direct Connect 连接）连接到单个传输网关，从而将您的 AWS 组织的整个路由配置整合到一个地方。传输网关解决了大规模创建和管理多个 VPC 对等连接所涉及的复杂性。它是大多数网络架构的默认设置，但是围绕成本、带宽和延迟的特定需求可能会使 VPC 对等更适合您的需求。

入站（入口）VPC

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

出站（出口）VPC

出站 VPC 旨在处理从应用程序内部启动的网络连接。根据应用程序的具体情况，您可以期望在此 VPC 中看到流量 NAT、特定于 AWS 服务的 VPC 终端节点以及外部 API 终端节点的托管。来自此 VPC 的流日志被捕获并存储在日志存档账户中。

检查 VPC

专用检查 VPC 为管理 VPC（位于相同或不同的 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，确保 VPC 之间的所有流量都通过检查 VPC，并避免将检查 VPC 用于任何其他工作负载。

AWS 网络防火墙

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。它使您能够轻松部署和管理状态检查、入侵防御和检测以及 Web 过滤，以帮助保护您在 AWS 上的虚拟网络。有关配置Network Firewall 的更多信息，请参阅 AWS Network Firewall — VPC 中的新托管防火墙服务博客文章。

您在 VPC 中以每个可用区为单位使用防火墙。对于每个可用区，您可以选择一个子网来托管过滤流量的防火墙端点。可用区中的防火墙端点可以保护该区域内的所有子网，但它所在的子网除外。根据用例和部署模型，防火墙子网可以是公共子网也可以是私有子网。Firewall 对流量完全透明，不执行网络地址转换

(NAT)。它保留了源地址和目标地址。在此参考架构中，防火墙端点托管在检查 VPC 中。来自入站 VPC 和出站 VPC 的所有流量都通过此防火墙子网进行检查。

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Simple Storage Service (Amazon S3) 和亚马逊 Kinesis Data Firehose 发送日志CloudWatch，提高网络流量的可见性。Network Firewall 可与您现有的安全方法（包括 AWS 合作伙伴的技术）互操作。您还可以导入现有的 Suricata 规则集，这些规则集可能是内部编写的，也可能是外部来源于第三方供应商或开源平台。

在 AWS SRA 中，在网络账户内使用Network Firewall，因为该服务以网络控制为中心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Network Firewall 规则。（有关详细信息，请参阅 AWS 文档中的 AWS Network Firewall 策略。）当您配置 Firewall Manager 时，它会使用您指定的帐户和 VPC 中的规则集自动创建防火墙。它还在包含公有子网的每个可用区域的专用子网中部署终端节点。同时，对集中配置的规则集所做的任何更改都会在部署的Network Firewall 的下游自动更新。
- Network Firewall 有多种部署模式可用。正确的模型取决于您的使用案例和要求。示例包括：
  - 一种分布式部署模型，其中Network Firewall 部署到单个 VPC 中。
  - 一种集中式部署模式，将Network Firewall 部署到集中式 VPC 中，用于东西向（vpc 到 vPC）或南北（互联网出口和入口，本地）流量。
  - 一种组合部署模型，其中Network Firewall 部署到集中式 VPC 中，用于东西向流量和南北流量子集。
- 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来源或目的地的流量。

Network Access Analyzer

网络访问分析器是 Amazon VPC 的一项功能，用于识别对您资源的意外网络访问。您可以使用 Network Access Analyzer 验证网络分段，识别可从 Internet 访问的资源或只能从可信 IP 地址范围访问的资源，并验证您在所有网络路径上是否有适当的网络控制。

Network Access Analyzer 使用自动推理算法来分析数据包在 AWS 网络中的资源之间可能采用的网络路径，并得出与您定义的网络访问范围相匹配的路径的结果。Network Access Analyzer 对网络配置进行静态分析，这意味着分析过程中不会在网络中传输任何数据包。

亚马逊 Inspector 网络可访问性规则提供了相关功能。这些规则生成的发现将在应用程序帐户中使用。网络访问分析器和网络可访问性都使用 AWS Provable Security 计划的最新技术，并将这项技术应用于不同的重点领域。网络可访问性套餐专门针对 EC2 实例及其互联网可访问性。

网络账户定义了控制进出您的 AWS 环境的流量的关键网络基础设施。需要严格监控这些流量。在 AWS SRA 中，网络账户内使用网络访问分析器来帮助识别非预期的网络访问，识别可通过互联网网关访问互联网的资源，并验证资源与 Internet 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，可以在任何拥有 VPC 的 AWS 账户中使用。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 AWS 账户内是否已强制执行经批准的网络路径。

AWS 内存

AWS Resource Access Manager (AWS RAM) 可帮助您安全地与其他 AWS 账户共享您在一个 AWS 账户中创建的 AWS 资源。AWS RAM 提供了一个管理资源共享和标准化跨账户体验的中心场所。这样可以更轻

松地管理资源，同时利用管理和账单隔离，并缩小多账户策略提供的影响控制优势的范围。如果您的账户由 AWS Organizations 管理，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 (OU) 内的账户共享资源。您还可以通过账户 ID 与特定 AWS 账户共享，无论该账户是否属于组织。您还可以与指定的 IAM 角色和用户共享一些支持的资源类型。

AWS RAM 使您能够共享不支持基于资源的 IAM 策略的资源，例如 VPC 子网和 Route 53 规则。此外，使用 AWS RAM，资源的所有者可以查看哪些委托人有权访问他们共享的各个资源。IAM 实体可以直接检索与其共享的资源列表，而使用 IAM 资源策略共享的资源则无法进行此操作。如果使用 AWS RAM 在您的 AWS 组织外部共享资源，则会启动邀请流程。在授予资源访问权限之前，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 中说明的 AWS RAM 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 AWS 账户和网络管理功能的能力，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 AWS 网络基础设施白皮书。

设计注意事项

- 尽管 AWS RAM 即服务仅部署在 AWS SRA 的网络账户内，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，然后与您的 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）。欲了解更多信息，请参阅 AWS Lake Formation 文档和 AWS 博客文章使用 AWS AWS Lake Formation 账户之间安全共享您的数据... 此外，安全管理员在构建AWS 私有 CA层次结构时可以使用 AWS RAM 遵循最佳实践。CA 可以与外部第三方共享，后者可以在不访问 CA 层次结构的情况下颁发证书。这允许发起组织限制和撤消第三方访问权限。

边缘安全

边缘安全通常包括三种类型的保护：安全内容传输、网络和应用层保护以及分布式拒绝服务 (DDoS) 缓解。数据、视频、应用程序和 API 等内容必须快速、安全地交付，使用推荐版本的 TLS 来加密端点之间的通信。还应通过签名 URL、签名 Cookie 和令牌身份验证对内容进行访问限制。应用程序级安全应设计为控制机器人流量，阻止 SQL 注入或跨站脚本 (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，可确保关键业务运营和服务的持续可用性。应保护应用程序和 API 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。

从核心云到 AWS 网络边缘，AWS 提供多种服务来帮助提供安全的环境。亚马逊CloudFront、AWS Certificate Manager (ACM)、AWS Shield、AWS WAF 和Amazon Route 53 共同努力，帮助创建灵活的分层安全边界。在亚马逊CloudFront，内容、API 或应用程序可以通过 HTTPS 传输，方法是使用 TLSv1.3 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。ACM 自动处理证书续订。AWS Shield 是一项托管 DDoS 保护服务，可帮助保护在 AWS 上运行的应用程序。它提供动态检测和自动内联缓解措施，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 URI）、常见的 Web 攻击和普遍存在的机器人过滤 Web 流量。Route 53 是一种可用性高、可扩展性强的 DNS Web 服务。Route 53 将用户请求连接到在 AWS 或本地运行的互联网应用程序。AWS SRA 使用托管在网络账户内的 AWS Transit Gateway 采用集中式网络入口架构，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)，可针对常见的网络层和传输 DDoS 尝试提供固有的保护。您可以使用 TLS 证书交付内容、API 或应用程序，高级 TLS 功能会自动启用。您可以使用 ACM 创建自定义 TLS 证书并强制查看者与之间进行 HTTPS 通信CloudFront，如后面的 ACM (p. 43) 部分所述。此外，您还可以要求与您的自定义来源CloudFront之间的通信在传输过程中实现端到端加密。在这种情况下，您必须在原始服务器上安装 TLS 证书。如果您的来源是弹性负载均衡器，则可以使用由 ACM 生成的证书或经第三方证书颁发机构 (CA) 验证并导入 ACM 的证书。如果 S3 存储桶网站终端节点作为源，则无法CloudFront将配置为CloudFront将 HTTPS 与源结合使用，因为 Amazon S3 不支持对网站终端节点使用 HTTPS。（但您仍可以要求在观看者和之间使用 HTTPS CloudFront。）对于支持安装 HTTPS 证书的所有其他源，您必须使用信任的第三方 CA 签署的证书。

CloudFront提供多种选项来保护和限制对内容的访问。例如，它可以通过使用签名 URL 和签名 Cookie 限制对 Amazon S3 源访问。有关更多信息，请参阅配置安全访问和限制对CloudFront文档内容的访问。

AWS SRA 说明了网络账户中的集中式CloudFront分布，因为它们与使用 Transit Gateway 实现的集中式网络模式一致。通过在网络账户CloudFront中部署和管理分发，您可以获得集中控制的好处。您可以在一个地方管理所有CloudFront发行版，这样可以更轻松地控制所有账户的访问权限、配置设置和监控使用情况。此外，您可以从一个集中账户管理 ACM 证书、DNS CloudFront 记录和登录。

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诸如如何部署CloudFront发行版之类的决策，确定适当的缓存策略，并负责管理、审计和监控CloudFront发行版。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固有的自动原始访问身份 (OAI) 和原始访问控制 (OAC) 配置来限制对 Amazon S3 来源的访问。
- 当您通过CDN提供网络内容时CloudFront，必须防止观众绕过CDN直接访问您的原始内容。要实现此源访问限制，您可以使用CloudFront和 AWS WAF 添加自定义标头并在将请求转发到自定义来源之前验证标头。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 AWS Secrets Manager 增强亚马逊CloudFront原始安全。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 漏洞攻击，例如常见漏洞和机器人，这些漏洞可能会影响应用程序可用性、危害安全性或消耗过多资源。它可以与Amazon CloudFront API Gateway REST API、Application Load Balancer、Amazon AppSync GraphQL API、AWS mazon Cognito 用户群和 Amazon Application Apps Application Apps App

AWS WAF 使用网络访问控制列表 (ACL) 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 请求符合条件时应采取的相关操作（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，可针对常见应用程序漏洞提供保护。这些规则由 AWS 和 AWS 合作伙伴策划和管理。AWS WAF 还提供了一种用于编写自定义规则的强大规则语言。您可以使用自定义规则来编写适合您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您的特定应用程序行为的托管规则的自定义版本。

AWS WAF 为常见和目标机器人和账户接管保护 (ATP) 提供了一组智能层管理规则。当您使用机器人控制和 ATP 规则组时，您需要支付订阅费和交通检查费。因此，我们建议您先监控您的流量，然后决定使用什么。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控制面板来监控这些活动，然后决定是否需要智能层 AWS WAF 规则组。

在 AWS SRA 中，AWS WAF 已集成到网络账户CloudFront中。在此配置中，WAF 规则处理发生在边缘站点，而不是 VPC 内。这样可以过滤离请求内容的最终用户更近的恶意流量，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，您可以将完整的 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 Ams re: Post 有关此主题的文章。

设计注意事项

- 作为在网络账户中集中部署 AWS WAF 的替代方案，在应用程序账户中部署 AWS WAF 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发行版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 应用程序前使用 Amazon API Gateway，则可以选择此选项。如果您决定在每个应用程序账户中部署 AWS WAF，请使用 AWS Firewall Manager 从集中式安全工具账户管理这些账户中的 AWS WAF 规则。
- 您还可以在CloudFront层添加常规 AWS WAF 规则，在区域资源（例如Application Load Balancer 或 API 网关）中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 DDoS 保护服务，用于保护 AWS 上运行的应用程序。Shield 有两个等级：Shield 标准和Shield 高级。Shield Standard 为所有 AWS 客户提供保护，使其免受最常见的基础设施（第 3 层和第 4 层）事件的影响，无需额外付费。Shield Advanced 为针对受保护的亚马逊弹性计算云 (Amazon EC2)、Elastic Load Balancing (ELB)、亚马逊、AWS Global Accelerator 和 Route 53 托管区域上的应用程序的未授权事件提供更复杂的自动缓解措施。CloudFront如果您拥有知名度高的网站或容易受到频繁的DDoS攻击，则可以考虑Shield Advanced提供的其他功能。

您可以使用 Shield Advanced 自动应用程序层 DDoS 缓解功能将 Shield Advanced 配置为自动响应，以缓解针对受保护CloudFront分布式和应用程序负载均衡器的应用程序层（第 7 层）攻击。当您启用此功能时，Shield Advanced 会自动生成自定义 AWS WAF 规则以缓解 DDoS 攻击。Shield Advanced 还允许您访问 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，或者在活跃 DDoS 攻击期间创建和管理自定义缓解措施。如果您希望 SRT 主动监控您的受保护资源并在尝试 DDoS 期间与您联系，请考虑启用主动参与功能。

设计注意事项

- 如果您的任何工作负载由应用程序账户中的面向互联网的资源（例如亚马逊 CloudFront、Application Load Balancer 或Network Load Balancer）提供，请在应用程序账户中配置 Shield Advanced 并将这些资源添加到 Shield protection 中。您可以使用 AWS Firewall Manager 器大规模配置这些选项。
- 如果您在数据流中有多个资源，例如Application Load Balancer 前面的CloudFront分配，则仅使用入口点资源作为受保护资源。这将确保您不会为两种资源两次支付 Shield Data Transfort Out (DTO) 费用。
- Shield Advanced 会记录您可以在亚马逊监控的指标CloudWatch。（有关更多信息，请参阅 AWS 文档中的 AWS Shield 高级指标和警报。）设置CloudWatch警报，以便在检测到 DDoS 事件时向您的安全中心接收 SNS 通知。如果出现疑似的 DDoS 事件，请联系 AWS 企业Support 团队，提交支持请求并将其指定为最高优先级。在处理事件时，企业Support 团队将包括Shield 响应小组（SRT）。此外，您可以预先配置 AWS Shield 参与 Lambda 函数，以创建支持票证并向 SRT 团队发送电子邮件。

AWS Certificate Manager

AWS Certificate Manager (ACM) 允许您预置、管理和部署公有和私有 TLS 证书，用于 AWS 服务和内部连接资源。使用 ACM，您可以快速申请证书，将其部署到集成 ACM 的 AWS 资源上，例如Elastic Load Balancing 均衡器、亚马逊CloudFront分发和 Amazon API Gateway 上的 API，然后让 ACM 处理证书续订。请求 ACM 公共证书时，无需生成key pair 或证书签名请求 (CSR)，无需向证书颁发机构 (CA) 提交 CSR，也无需在收到证书时上传和安装证书。ACM 还提供导入第三方 CA 颁发的 TLS 证书并使用 ACM 集成服务部署这些证书的选项。使用 ACM 管理证书时，使用强加密和密钥管理最佳实践安全地保护和存储证书私钥。使用 ACM，预置公共证书不收取额外费用，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，CloudFront发行版又使用该证书在查看者和CloudFront之间建立 HTTPS 连接。有关更多信息，请参阅 CloudFront 文档。

设计注意事项

- 对于面向外部的证书，ACM 必须与为其提供证书的资源位于同一个账户中。不能在账户之间共享证书。

Amazon Route 53

Amazon Route 53 是一种可用性高、可扩展性强的网络服务。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分发和其他 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。如果您的主应用程序终端节点不可用，则可以将故障转移配置为将用户重新路由到其他位置。Route 53 Resolver 通过 Ams Direct 或 AWS 托管 VPN 为您的 VPC 和本地网络提供递归 DNS。

通过将 AWS Identity and Access Management (IAM) 服务与 Route 53 配合使用，您可以精确控制谁可以更新您的 DNS 数据。您可以启用 DNS 安全扩展 (DNSSEC) 签名以允许 DNS 解析程序验证来自 Route 53 且未被篡改的 DNS 响应。

R@@ oute 53 Resolver DNS Firewall 为来自您 VPC 的出站 DNS 请求提供保护 这些请求通过 Route 53 解析程序进行域名解析。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，并允许所有其它查询通过。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 阻止在私有托管区域（共享或本地）中对资源（包括 VPC 终端节点名称）的解析请求。它还可以阻止对公有或私有 EC2 实例名称的请求。

默认情况下，Route 53 解析器是作为每个 VPC 的一部分创建的。在 AWS SRA 中，Route 53 在网络账户中主要用于 DNS 防火墙功能。

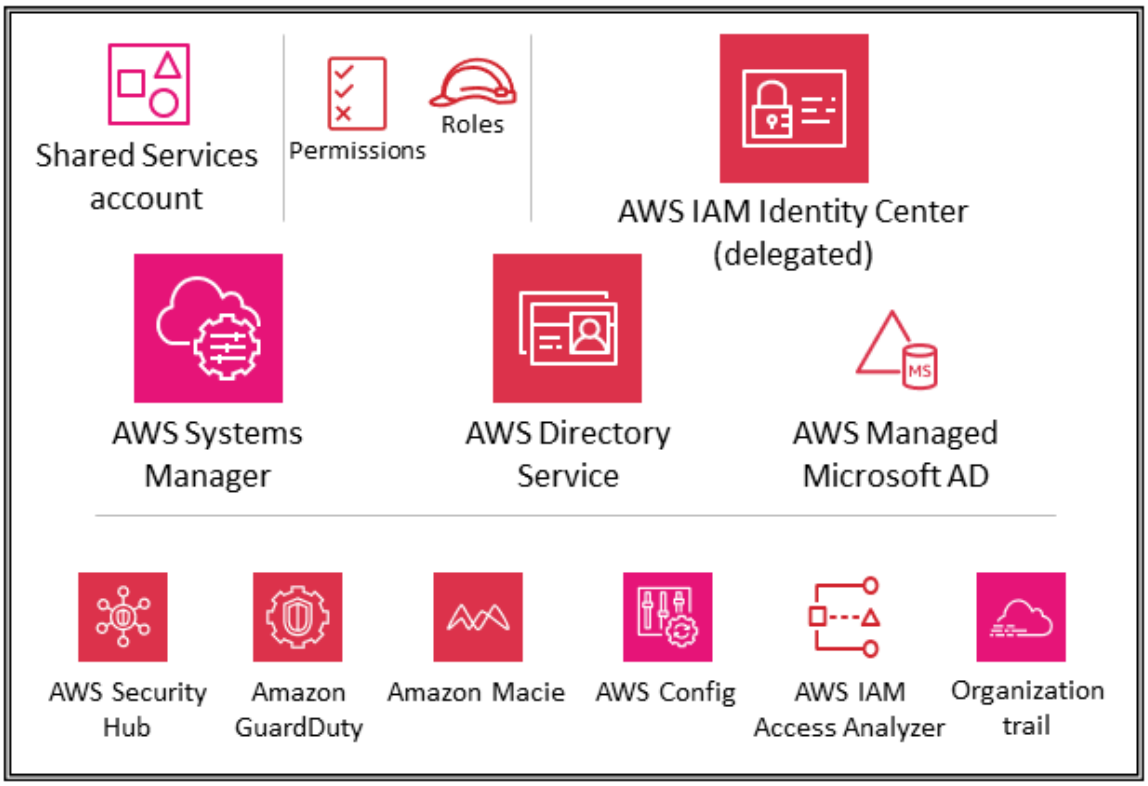
设计注意事项

- DNS Firewall 和 AWS Network Firewall 都提供域名筛选，但适用于不同类型的流量。您可以将 DNS Firewall 和 Network Firewall 相结合，为两个不同的网络路径上的应用程序层流量配置基于域的筛选。
  - DNS Firewall 为通过 Route 53 Resolver 从 VPC 内的应用程序传递的出站 DNS 查询提供筛选。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

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

下图说明了在共享服务账户中配置的 AWS 安全服务。



Shared Services 账户是基础架构 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）、消息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 Shared Services 帐户中删除。管理这些服务的团队不需要网络帐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，可实现对您的 AWS 资源的可见性和控制。Systems Manager Manager Managems Managems Managems Managems ManAWS ems M 您可以使用 AWS 组织中的所有账户和Systems Manager Manager Managems Manager Managems Manager Systems Manager 通过 AWS Organizations 中的委托管理员功能部署在 Shared Services 账户中。

Systems Manager Systems Manager 通过扫描托管实例并报告其检测到的任何策略违规行为（或采取纠正措施）来帮助您维护安全性和合规性。通过将 Systems Manager 与单个成员 AWS 账户（例如应用程序账户）中的相应部署配对，您可以协调实例库存数据收集并集中实现自动化，例如补丁和安全更新。

AWS MSMSMS

适用于微软 Active Di rectory 的 AWS Directory Service，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 AWS 上使用托管的 A 您可以使用 AWS Managed Microsoft AD 将适用于 Windows Server 的A mazon EC2、适用于 Linux 的Amazon EC2 和适用于 SQL Server 的亚马逊 RD S 实例加入您的域名，也可以使用 AWS 最终用户计算 (EUC) 服务，例如亚马逊WorkSpaces，与 Active Directory 用户和群组。

AWS Managed Microsoft AD 可帮助您将现有 Active Directory 扩展到 AWS，并使用现有的本地用户证书访问云资源。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到 AWS 管理的 Microsoft AD 域中。

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

多区域复制使您能够跨多个 AWS 区域部署和使用单个 AWS 管理的 Microsoft AD 目录。这使您可以更轻松、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 支持客户端和服务器角色中基于 SSL/TLS 的轻量级目录访问协议 (LDAP)，也称为 LDAPS。充当服务器时，AWS Managed Microsoft AD 支持端口 636 (SSL) 和 389 (TLS) 上的 LDAPS。通过在 AWS 管理的 Microsoft AD 域控制器上安装来自基于 AWS 的 Active Directory 证书服务 (AD CS) 证书颁发机构 (CA) 的证书，即可启用服务器端 LDAPS 通信。作为客户时，AWS Managed Microsoft AD 支持端口 636 上的 LDAPS (SSL)。您可以通过将服务器证书颁发机构的 CA 证书注册到 AWS 来启用客户端 LDAPS 通信，然后在您的目录上启用 LDAPS。

在 AWS SRA 中，AWS Directory Service 在共享服务账户中使用，为多个 AWS 成员账户中的 Microsoft 感知工作负载提供域服务。

设计注意事项

- 您可以使用 IAM 身份中心并选择 AWS Managed Microsoft AD 作为身份来源，授予您的本地 Active Directory 用户使用其现有 Active Directory 证书登录 AWS 管理控制台和 AWS Command Line Interface (AWS CLI) 的访问权限。这使您的用户能够在登录时担任其分配的角色之一，并根据为该角色定义的权限访问资源并对其进行操作。另一种选择是使用 AWS Managed Microsoft AD 让您的用户担任 AWS Identity and Access Manag ement (IAM) 角色。

IAM Identity Center

AWS SRA 使用 IAM 身份中心支持的委托管理员功能，将 IAM 身份中心的大部分管理权委托给共享服务账户。这有助于限制需要访问组织管理帐户的用户数量。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 Shared Services 账户作为 IAM 身份中心的委托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 身份来源，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 身份中心的委托管理员。

IAM Identity Center 支持一次性将单个成员账户注册为委托管理员。只有使用管理账户的证书登录时，才能注册成员账户。要启用委派，您必须考虑 IAM 身份中心文档中列出的先决条件。委托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 委托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 委托管理员账户中（归其所有）；否则，它必须位于管理账户中。
- 您可以在其他账户的专用 VPC 内托管您的 AWS Managed Microsoft AD，然后使用 AWS Resource Access Manager (AWS RAM) 将该其他账户的子网共享给委托管理员账户。这样，AWS Managed Microsoft AD 实例在委托管理员账户中进行控制，但从网络角度来看，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进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分开，则可以托管一个专用 AWS 账户进行身份管理。在这种情况下，

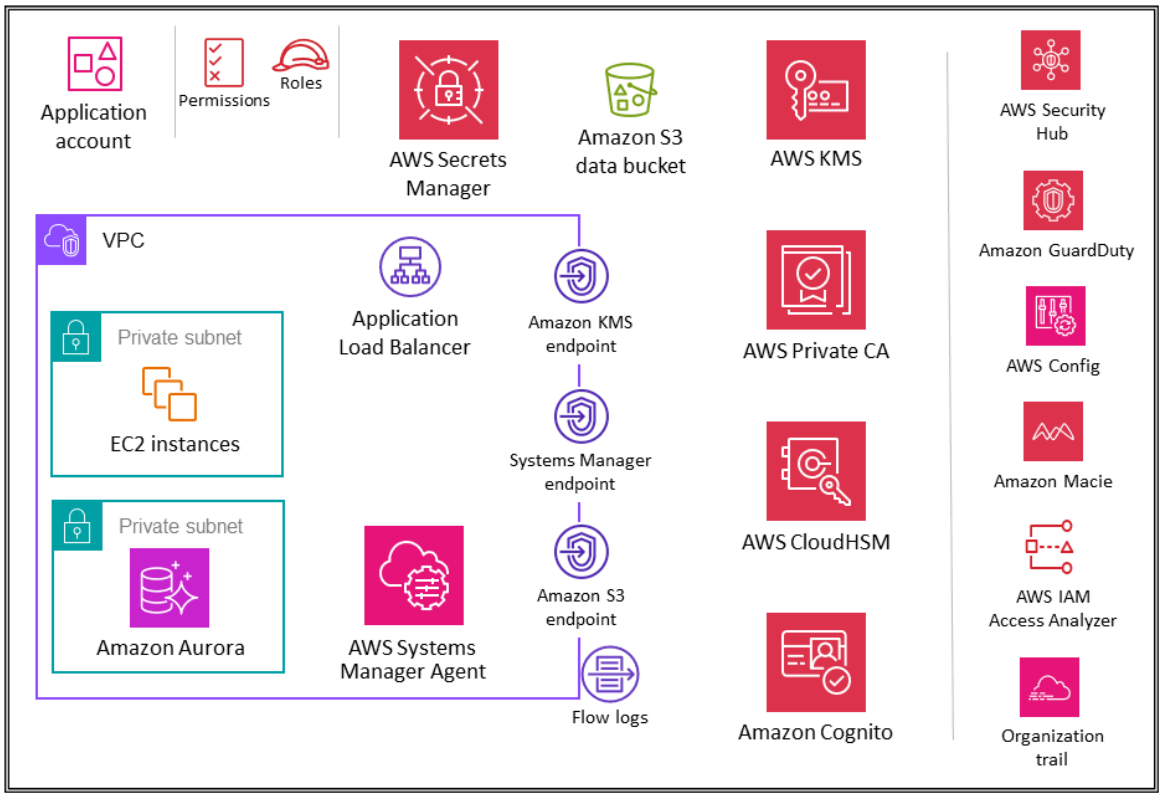
您将此账户指定为 IAM Identity Center 的委托管理员，它还托管您的 AWS Managed Microsoft AD 目录。通过在单个共享服务账户中使用精细的 IAM 权限，您可以在身份管理工作负载和其他共享服务工作负载之间实现相同级别的逻辑隔离。

- 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，您必须先删除当前 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来源，也不支持将权限管理委托给组织的不同部分（即多个委派管理员）或不同的管理员组。如果您需要这些功能中的任何功能，您可以使用 IAM 联合身份提供程序 (IdP) 中的用户身份，并向这些外部用户身份授予使用您账户中的 AWS 资源的权限。与 OpenID Connect (OIDC) 或 SAML 2.0 兼容的 IAM 支持IdPs。作为最佳实践，使用 SAML 2.0 联合第三方身份提供商，如活动目录联合服务 (AD FS)、Okta、Azure Active Directory (Azure AD) 或 Ping Identity，为用户提供登录到 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程序的更多信息，请参阅 IAM 文档中的关于基于 SAML 2.0 的联合 AWS Identity。

工作负载 OU — 应用程序帐户

通过简短的调查影响AWS安全参考架构 (AWSSRA) 的未来。

下图说明了在应用程序账户中配置的 AWS 安全服务（以及应用程序本身）。



应用程序帐户托管运行和维护企业应用程序的主要基础架构和服务。应用程序账户和工作负载 OU 有一些主要的安全目标。首先，您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边界和控制，这样您就可以避免角色、权限、数据和加密密钥混杂的问题。您希望提供一个单独的账户容器，在其中可以授予应用程序团队在不影响其他人的情况下管理自己的基础架构的广泛权限。接下来，您可以为安全运营团队提供监控和收集安全数据的机制，从而增加一层保护。使用组织跟踪和本地部署账户安全服务（亚马逊GuardDuty、AWS Config、AWS Security Hub、亚马逊EventBridge、AWS 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措施。通过使应用程序帐户成为

Workloads OU 的成员，它可以通过该成员继承相应的服务权限、限制和护栏，使之与更广泛的安全结构保持一致。

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 旨在容纳您的大多数特定业务工作负载，包括生产和非生产环境。这些工作负载可以混合商业 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。组织不同的业务应用程序及其开发环境的模式很少。一种模式是基于您的开发环境（例如生产、试运行、测试和开发）设置多个子 OU，并在与不同应用程序相关的 OU 下使用单独的子 AWS 账户。另一种常见模式是为每个应用程序设置单独的子 OU，然后为各个开发环境使用单独的子 AWS 账户。确切的 OU 和账户结构取决于您的应用程序设计和管理这些应用程序的团队。考虑您要强制实施的安全控制，无论它们是特定环境的还是特定于应用程序的，因为在 OU 上以 SCP 的形式实施这些控制更容易。有关组织面向工作负载的 OU 的更多注意事项，请参阅 AWS 白皮书使用多个账户组织您的 AWS 环境的组织面向工作负载的 OU 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（用于您正在建模的简单 Web 服务），也需要出站访问（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（例如应用程序层和数据库层）之间的网络分段通过 VPC 安全组完成，这些安全组在实例级别限制流量。为了实现弹性，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 实例的弹性网络接口复制网络流量。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，您可能需要监控离开您的 VPC 的流量或源在您的 VPC 之外的流量。在这种情况下，您将镜像除您的 VPC 内传递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捕获信息。流量镜像允许您分析包括负载在内的实际流量内容，从而更深入地了解网络流量。仅为 EC2 实例的弹性网络接口启用流量镜像，这些接口可能作为敏感工作负载的一部分运行，或者您预计在出现问题时需要对其进行详细诊断。

VPC 端点

VPC 终端节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 AWS 服务。（在应用程序账户中，AWS SRA 为 AWS KMS、AWS Systems Manager 和 Amazon S3 使用 VPC 终端节点。）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。您可以使用 VPC 终端节点将您的 VPC 私下连接到由 AWS 提供支持的 AWS 服务和 VPC 终端节点服务，PrivateLink无需互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。您的 VPC 中的实例不需要公有 IP 地址即可与其他 AWS 服务通信。您的 VPC 与其他 AWS 服务之间的流量不会离开亚马逊网络。

使用 VPC 终端节点的另一个好处是启用终端节点策略的配置。VPC 终端节点策略是一种 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没有附加 IAM 策略，AWS 会为您附加一个默认 IAM 策略，允许您完全访问该服务。终端节点策略不会替代或取代 IAM 策略或服务特定策略（例如 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。通过这种方式，它为哪些 AWS 委托人可以与资源或服务进行通信增加了另一层控制。

Amazon EC2

构成我们应用程序的 Amazon EC 2 实例使用了实例元数据服务 (imdsv2) 的版本 2。imdsv2 增加了对四种可用于尝试访问 IMDS 的漏洞的保护：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 NAT。有关更多信息，请参阅博客文章通过增强 EC2 实例元数据服务，深入防御开放式防火墙、反向代理和 SSRF 漏洞。

使用单独的 VPC（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权限。使用 VPC Flow Logs 监控到达实例的流量。使用会话管理器（AWS Systems Manager 的一项功能）远程访问您的实例，而不是打开入站 SSH 端口和管理 SSH 密钥。为操作系统和数据使用单独的亚马逊弹性区块存储 (Amazon EBS) 卷。您可以配置您的 AWS 账户以强制加密您创建的新 EBS 卷和快照副本。

实现示例

AWS SRA 代码库提供了亚马逊 EC2 中默认 Amazon EBS 加密的示例实现。它演示了如何在 AWS 组织中的每个 AWS 账户和 AWS 区域内启用账户级默认 Amazon EBS 加密。

Application Load Balancer

应用程序负载均衡器在多个可用区中的多个目标（例如 EC2 实例）之间分配传入的应用程序流量。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 侦听器来确保通信通道已加密。应用程序负载均衡器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，然后将其发送到目标。

AWS 证书管理器 (ACM) 在本地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。您可以通过应用程序负载均衡器安全策略对前端连接强制执行 TLS 1.2 和强密码。有关更多信息，请参阅 Elastic Load Balancing 文档。

设计注意事项

- 对于诸如要求应用程序负载均衡器上的私有 TLS 证书的严格内部应用程序之类的常见场景，您可以在此账户中使用 ACM 从AWS 私有 CA生成私有证书。在 AWS SRA 中，ACM 根私有 CA 托管在安全工具账户中，可以与整个 AWS 组织共享，也可以与特定 AWS 账户共享以颁发最终实体证书，如前面的 “安全工具 (p. 34)账户” 部分所述。
- 对于公共证书，您可以使用 ACM 生成这些证书并对其进行管理，包括自动轮换。或者，您可以使用 SSL/TLS 工具生成自己的证书，创建证书签名请求 (CSR)，让证书颁发机构 (CA) 签名的 CSR 生成证书，然后将证书导入 ACM 或将证书上传到 IAM 以用于应用程序负载均衡器。如果将证书导入 ACM，则必须监控证书的到期日期并在到期之前续订。
- 要获得更多防御层，您可以部署 AWS WAF 策略来保护应用程序负载均衡器。拥有边缘策略、应用程序策略甚至私有或内部策略实施层可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适用于 AWS WAF 的 AWS 托管规则深入部署防御。

AWS 私有 CA

AWS Private Certificate Authority(AWS 私有 CA) 在应用程序账户中用于生成用于应用程序负载均衡器的私有证书。应用程序负载均衡器通过 TLS 提供安全内容是常见的情况。这需要在应用程序负载均衡器上安装 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AWS 私有 CA，托管在安全工具账户中，使用 AWS RAM 共享到应用程序账户。这允许应用程序账户中的开发人员向共享私有 CA 申请证书。在您的组织内或在 AWS 账户之间共享 CA 有助于降低在所有 AWS 账户中创建和管理重复 CA 的成本和复杂性。当您使用 ACM 从共享 CA 颁发私有证书时，证书是在请求账户中本地生成的，ACM 提供完整的生命周期管理和续订。

Amazon Inspector

AWS SRA 使用 A mazon Inspec tor 自动发现和扫描位于亚马逊弹性容器注册表 (Amazon ECR) 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 位于应用程序账户中，因为它为该账户中的 EC2 实例提供漏洞管理服务。此外，Amazon Inspector 还会报告往返于 EC2 实例的有害网络路径。

成员账户中的 Amazon Inspector 由委托管理员账户集中管理。在 AWS SRA 中，安全工具账户是委托管理员账户。委托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发现详情、启用或禁用对成员账户的扫描，以及查看 AWS 组织内的扫描资源。

设计注意事项

- 您可以使用补丁管理器（AWS Systems Manager 的一项功能）触发按需补丁，以修复 Amazon Inspector 零日漏洞或其他关键安全漏洞。Patch Manager 可帮助您修补这些漏洞，无需等待正常的补丁计划。补救措施是使用系统管理器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使用 Amazon Inspector 和 AWS Systems Manager 在 AWS 中自动进行漏洞管理和修复。

亚马逊系统经理

AWS Systems Manager 是一项 AWS 服务，您可以使用它来查看来自多个 AWS 服务的运营数据，并在 AWS 资源上自动执行操作任务。借助自动批准工作流程和运行手册，您可以努力减少人为错误并简化 AWS 资源的维护和部署任务。

除了这些常规自动化功能外，Systems Manager 还支持许多预防、侦测和响应式安全功能。AWS Systems Manager 代理（SSM 代理）是可以在 EC2 实例、本地服务器或虚拟机 (VM) 上安装和配置的亚马逊软件。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，来帮助您维护安全性和合规性。

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 shell 和 CLI 体验。这提供了安全和可审计的实例管理，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（系统管理器的一项功能）为操作系统和应用程序的 EC2 实例应用补丁。

AWS SRA 还使用自动化（系统管理器的一项功能）来简化 Amazon 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。自动化提供一键式自动化，可简化复杂任务，例如创建黄金亚马逊系统映像 (AMI) 和恢复无法访问的 EC2 实例。此外，您可以通过授予 IAM 角色访问特定运行手册以执行某些功能来增强操作安全性，而无需直接向这些角色授予权限。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，则可以改为创建 Automation 运行手册并向该角色授予仅运行运行手册的权限。

设计注意事项

- Systems Manager 需要依靠 EC2 实例元数据才能正常运行。系统管理员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 服务和资源通信，例如亚马逊 EC2 消息、系统管理器和亚马逊 S3。要进行这种通信，子网需要出站互联网连接或配置适当的 VPC 终端节点。AWS SRA 使用 VPC 终端节点作为 SSM 代理建立通往各种 AWS 服务的私有网络路径。
- 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。您可以在运行手册中创建资源管理最佳实践，并在 AWS 区域和群组之间共享运行手册。您也可以限制运行手册参数的允许值。对于这些用例，您可能需要在安全工具或共享服务等中央账户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补丁和安全更新、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，请参阅系统管理器文档。

Amazon Aurora

在 AWS SRA 中，亚马逊 Aurora 和亚马逊 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 进行通信。Aurora 在数据库子网组内配置了数据库集群。

设计注意事项

- 与许多数据库服务一样，Aurora 的安全性在三个级别上进行管理。要控制谁可以在 Aurora 数据库集群和数据库实例上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 Aurora 数据库集群的集群终端节点和端口的连接，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 的独立数据库实例相同的方法，也可以对 Aurora MySQL 兼容版本使用 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 是一种对象存储服务，可提供业界领先的可扩展性、数据可用性、安全性和性能。它是许多在 AWS 上构建的应用程序的数据支柱，适当的权限和安全控制对于保护敏感数据至关重要。有关 Amazon S3 的推荐安全最佳实践，请参阅文档、在线技术讲座和博客文章中的更深入探讨。最重要的最佳做法是阻止对 S3 存储桶的过度宽松访问（尤其是公共访问）。

AWSKS

AWS SRA 说明了密钥管理的推荐分发模式，其中 KMS 密钥与要加密的资源位于同一 AWS 账户中。因此，AWS KMS 除了包含在安全工具账户中外，还用于应用程序账户。在应用程序账户中，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，并限制密钥保管人的管理和监控权限，从而实现职责分离。

设计注意事项

- 在分布式模型中，AWS KMS 密钥管理由应用程序团队负责。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。
  - KMS 密钥已删除。
  - 解密失败率很高。

AWS CloudHS

AWS CloudHSM 在 AWS 云中提供托管硬件安全模块 (HSM)。它使您能够使用可控制访问权限的 FIPS 140-2 3 级验证 HSM 在 AWS 上生成和使用自己的加密密钥。您可以使用 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 CloudHSM 中来提供额外的安全性。如果您需要充当证书颁发机构，您同样可以在网络账户的入站 VPC 中部署 CloudHSM 来存储您的私钥并签署证书请求。

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 KMS 配置为使用 CloudHSM 集群作为自定义密钥存储，而不是使用本地 KMS 密钥存储。通过这样做，您可以受益于 AWS KMS 与加密数据的 AWS 服务之间的集成，同时负责保护您的 KMS 密钥。这使您可以控制的单租户 HSM 与 AWS KMS 的易用性和集成性相结合。要管理您的 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 HSM 经验的团队。

AWS 机密管理器

AWS Secrets Manager 可帮助您保护访问应用程序、服务和 IT 资源所需的证书（机密）。该服务使您能够在数据库凭证、API 密钥和其他机密的整个生命周期中高效轮换、管理和检索这些凭证、API 密钥和其他机

密。您可以将代码中的硬编码凭证替换为 Secrets Manager 的 API 调用，以编程方式检索密钥。这有助于确保秘密不会被正在检查您的代码的人泄露，因为该机密已不存在于代码中。此外，Secrets Manager 可帮助您在环境（开发、预生产、生产）之间移动应用程序。无需更改代码，而是可以确保环境中存在适当命名和引用的密钥。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，同时减少了代码测试后的更改和人为交互。

使用 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。您可以使用使用 AWS KMS 管理的加密密钥对机密进行加密，从而帮助保护机密。Secrets Manager 还集成了 AWS 日志和监控服务，用于集中审计。

Secrets Manager 使用信封加密和 AWS KMS 密钥和数据密钥来保护每个机密值。创建密钥时，您可以在 AWS 账户和区域中选择任何对称的客户托管密钥，也可以使用 Secrets Manager 的 AWS 托管密钥。

最佳做法是，您可以监控您的机密信息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情况或更改。可以回退不需要的更改。Secrets Manager 目前支持两项使您能够监控您的组织和活动的 AWS 服务：AWS CloudTrail 和 AWS Config。CloudTrail将 Secrets Manager 的所有 API 调用作为事件捕获，包括来自 Secrets Manager 控制台的调用和对密钥管理器 API 的代码调用。此外，CloudTrail捕获其他可能对您的 AWS 账户产生安全或合规性影响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密钥版本的删除。AWS Config 可以通过跟踪和监控 Secrets Manager 中机密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 来源的关系，例如 KMS 加密密钥或用于密钥轮换的 AWS Lambda 函数。您还可以将接收来自 AWS Config 的配置和合规性变更通知的亚马逊EventBridge配置为路由特定的机密事件以进行通知或补救操作。

在 AWS SRA 中，Secrets Manager 位于应用程序账户中，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，实例配置文件附加到应用程序账户中的 EC2 实例。然后可以在密钥管理器中配置单独的密钥，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、修改或恢复 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证替换为 Secrets Manager 的编程 API 调用。

设计注意事项

- 通常，在最接近密钥使用位置的帐户中配置和管理 Secrets Manager。这种方法利用了用例的本地知识，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的信息，可以由 Secrets Manager 在 Security Tooling 帐户中集中管理机密。

Amazon Cognito

Amazon Cognito 允许您快速高效地向您的网络和移动应用程序添加用户注册、登录和访问控制。亚马逊 Cognito 可扩展到数百万用户，并支持通过苹果、Facebook、谷歌和亚马逊等社交身份提供商登录，以及通过 SAML 2.0 和 OpenID Connect 登录企业身份提供商。Amazon Cognito 的两个主要组件是用户池和身份池。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。身份池使您能够向用户授予其他 AWS 服务的访问权限。您可以单独或配合使用身份池和用户池。有关常见的使用场景，请参阅亚马逊 Cognito 文档。

Amazon Cognito 为用户注册和登录提供内置且可自定义的用户界面。您可以使用适用于 Amazon Cognito 的安卓、iOS 和JavaScript软件开发工具包向您的应用程序添加用户注册和登录页面。A@@ mazon Cognito Sync 是一个 AWS 服务和客户端库，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，帮助保护对应用程序中账户的访问。这些高级安全功能提供基于风险的自适应身份验证，并防止使用泄露的凭证。

设计注意事项

- 您可以创建 AWS Lambda 函数，然后使用 AWS Lambda 触发器在用户池操作（例如用户注册、确认和登录（身份验证）期间触发该函数。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。亚马逊 Cognito 会同步调用 Lambda 函数。

- 您可以使用 Amazon Cognito 用户池来保护小型多租户应用程序。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 服务配额一致。这些配额在应用程序中的所有租户之间共享。

分层防御

应用程序账户为说明 AWS 支持的分层防御原则提供了机会。考虑构成 AWS SRA 中简单示例应用程序核心的 EC2 实例的安全性，您可以看到 AWS 服务在分层防御中协同工作的方式。此方法与 AWS 安全服务的结构视图一致，如本指南前面的 “在 AWS 组织中应用安全服务 (p. 12)” 部分所述。

- 最内层是 EC2 实例。如前所述，EC2 实例默认或作为选项包含许多原生安全功能。示例包括 imdsv2、Nitro 系统和亚马逊 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。A mazon Inspector 和 AWS Systems Manager 等服务使您能够监控、报告这些配置并采取纠正措施。Inspector 会监控您的软件是否存在漏洞，Systems Manager 通过扫描托管实例的补丁和配置状态，然后报告和采取您指定的任何纠正措施，来帮助您维护安全性和合规性。
- 实例和在这些实例上运行的软件位于您的 AWS 网络基础设施中。除了使用 A mazon VPC 的安全功能外，AWS SRA 还利用 VPC 终端节点在 VPC 和支持的 AWS 服务之间提供私有连接，并提供在网络边界放置访问策略的机制。
- EC2 实例、软件、网络和 IAM 角色和资源的活动和配置由 AWS 账户为中心的服务进行进一步监控，例如 AWS Security Hub、亚马逊、AWS、AWS Config GuardDuty CloudTrail、AWS IAM 访问分析器和 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 组织内强制执行一致的权限。

IAM 资源

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

尽管 AWS Identity and Access Management (IAM) 不是一项包含在传统架构图中的服务，但它涉及 AWS 组织、AWS 账户和 AWS 服务的方方面面。如果不创建 IAM 实体并先授予权限，则无法部署任何 AWS 服务。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的指导。

- 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 IA M 文章和 A WS re: Invent 演示。
- AWS Well-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。
- 下表及其随附说明概述了有关可用 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 AWS re: 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... 有关	影响	部署于
服务控制策略 (SCP)	Restrict	中央团队，例如平台或安全团队 [1]	护栏、治理	组织、OU、账户	组织、OU 和账户中的所有负责人	组织管理账户 [2]
基准账户自动化策略（平台用于运营账户的 IAM 角色）	许可和限制	中央团队，例如平台、安全或 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]	成员账户内自动化使用的委托人	成员账户
基准人工政策（授予用户执行工作权限的 IAM 角色）	许可和限制	中央团队，例如平台、安全或 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另一位委托人的最大权限）	Restrict	中央团队，例如平台、安全或 IAM 团队 [1]	应用程序角色的护栏（必须应用）	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（附加到开发人员部署的基础架构的角色）	许可和限制	委托给开发人员 [8]	应用程序或工作负载的权限 [9]	单一账户	此账户的委托人	成员账户

资源策略	许可和限制	委托给开发者 [8,10]	资源权限	单一账户	账户中的委托人 [11]	成员账户

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），负责划分这些独立控制的职责，并对彼此的政策进行同行审查。表中的示例是占位符。您需要确定企业最有效的职责分离。
2. 要使用 SCP，您必须启用 AWS Organizations 内的所有功能。
3. 实现自动化通常需要通用的基准角色和策略，例如管道权限、部署工具、监控工具（例如 AWS Lambda 和 AWS Config 规则）和其他权限。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，但可以使用 AWS 将其复制或部署到多个账户 CloudFormationStackSets。
5. 定义一组核心的基准人员角色和政策，由中央团队部署到所有成员账户（通常在账户配置期间）。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（而不是本地 IAM 用户）。
7. 权限边界由委派管理员使用。此 IAM 策略定义了最大权限并替代了其他策略（包括允许对资源进行所有操作的“*:*”策略）。基准人类策略中应要求权限边界，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。诸如 SCP 之类的其他配置会强制附加权限边界。
8. 这假设已经部署了足够的护栏（例如 SCP 和权限边界）。
9. 这些可选策略可以在账户配置期间交付，也可以在应用程序开发过程中交付。创建和附加这些策略的权限将由应用程序开发人员自己的权限管理。
10. 除本地账户权限外，集中式团队（例如云平台团队或安全运营团队）通常管理一些基于资源的策略，以实现跨账户访问来操作账户（例如，提供对 S3 存储桶的访问权限以进行登录）。
11. 基于资源的 IAM 策略可以引用任何账户中的任何委托人，以允许或拒绝访问其资源。它甚至可以引用匿名校长来启用公共访问权限。

确保 IAM 身份仅拥有一组明确定义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、评估和缓解超额权限。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护栏和权限边界。
- 通过持续迭代的过程实现最低权限。这不是一次性练习。
- 使用 SCP 降低可操作的风险。它们旨在成为宽阔的护栏，而不是狭隘的有针对性的控制。
- 使用许可边界以更安全的方式委派权限管理。
  - 确保委托管理员将适当的 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CloudTrail、AWS、AWS IAM 访问分析器和相关工具定期分析历史使用情况和授予的权限。立即修复明显的过度权限。
- 在适用的情况下，将广泛的操作范围限定到特定资源，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 政策异常。

AWS SRA 示例的代码存储库

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

为了帮助您开始构建和实施 AWS SRA 中的指南，本指南附带了位于 https://github.com/aws-samples/aws-security-reference-architecture- examples 的基础设施即代码 (iaC) 存储库。该存储库包含可帮助开发人员和工程师部署本文档中介绍的一些指南和架构模式的代码。此代码摘自 AWS Professional Services 顾问与客户打交道的第一手经验。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非常严格。您可能需要修改和定制这些解决方案以满足您的环境和安全需求。

该存储库中的示例已使用 AWS 和 AWS Control Tower (cFcT) 定制解决方案在 AWS Control Tower 环境中部署CloudFormation和测试。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，以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内创建组织跟踪。此跟踪使用在 Security Tooling 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。启用 Amazon S3 和 AWS Co用 AWS Co用 Amazon Amazon EBDS Co 组织跟踪记录 AWS 组织中所有 AWS 账户的事件，同时防止成员账户修改配置。
- GuardDuty组织解决方案GuardDuty通过将管理权委托给安全工具账户来支持亚马逊。它GuardDuty在 Security Tooling 账户中为所有现有和future 的 AWS 组织账户进行配置。GuardDuty发现结果还使用 KMS 密钥加密，并发送到日志存档账户中的 S3 存储桶。
- Sec urity Hub 组织解决方案通过将管理权委托给安全工具账户来配置 AWS Security Hub。它在安全工具账户中为所有现有和future 的 AWS 组织账户配置 Security Hub。该解决方案还提供了用于同步所有账户和区域中启用的安全标准以及在 Security Tooling 账户中配置区域聚合器的参数。将 Security Hub 集中在 Security Tooling 账户中，可以跨账户查看 AWS 服务和第三方 AWS 合作伙伴集成的安全标准合规性以及调查结果。
- Inspector 解决方案在 AWS 组织下的所有账户和受管辖区域的委托管理员（安全工具）账户中配置 Amazon Inspector。
- Fi rew all Manager 解决方案通过将管理委托给安全工具账户并使用安全组策略和多个 AWS WAF 策略配置Firewall Manager 来配置 AWS Firewall Manager 安全策略。安全组策略要求在 VPC（现有或由解决方案创建）中允许的最大安全组，该安全组由解决方案部署。
- Macie 组织解决方案通过将管理权委托给安全工具账户来支持 Amazon Macie。它在安全工具账户中为所有现有和future 的 AWS 组织账户配置 Macie。Macie 被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 Agregator 解决方案通过将管理权委托给安全工具账户来配置 AWS Config 聚合器。然后，该解决方案在 Security Tooling 账户中为 AWS 组织中的所有现有和future 账户配置 AWS Config 聚合器。
  - Conformance Pack 组织规则解决方案通过将管理权委托给安全工具账户来部署 AWS Config 规则。然后，它在委托管理员账户中为 AWS 组织中的所有现有和future 账户创建组织合规包。该解决方案配置为部署加密和密钥管理操作最佳实践合规包示例模板。
  - AWS Config Control Tower 管理账户解决方案在 AWS Control Tower 管理账户中启用 AWS Config，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 AWS ConCloudFormation trol Tower 模板启用 AWS Config 作为参考，以确保与 AWS 组织中的其他账户保持一致。

- IAM
  - 访问分析器解决方案通过将管理委托给安全工具账户来启用 AWS IAM 访问分析器。然后，它在 Security Tooling 账户中为 AWS 组织中的所有现有和future 账户配置组织级访问分析器。该解决方案还将 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。该解决方案提供了配置密码策略设置的参数，以帮助您符合行业合规性标准。
- EC2 默认 EBS 加密解决方案在 AWS 组织的每个 AWS 账户和 AWS 区域内启用账户级默认 Amazon EBS 加密。它对您创建的新 EBS 卷和快照强制加密。例如，Amazon EBS 加密当您启动实例时创建的 EBS 卷以及您从未加密的快照复制的快照。
- S 3 区块账户公共访问解决方案在 AWS 组织的每个 AWS 账户中启用 Amazon S3 账户级别的设置。Amazon S3 阻止公有访问功能提供接入点、桶和账户设置，帮助您管理对 Amazon S3 资源的公有访问。新存储存储桶，新存储存储桶，新存储桶。但是，用户可以修改桶策略、接入点策略或对象权限以允许公有访问。Amazon Emazon Emazon S3 阻止公有访问。

致谢

通过简短的调查来影响AWS安全参考架构 (AWSSRA) 的future。

主要作者

- Avik Mukherjee，AWS 高级顾问
- Neal Rothleder，AWS 首席顾问
- 达明德拉·班达拉，AWS 高级顾问

贡献者

- 斯科特·康克林，AWS 高级顾问
- Ilya Epshteyn，AWS 身份解决方案高级经理
- Josh Du Lac，AWS 首席解决方案架构师
- 迈克尔·哈肯，AWS 首席技术专家
- Jorg Huser，AWS 首席顾问
- Mehial Mendrin，AWS 高级顾问
- 埃里克·罗斯，AWS 首席顾问
- Handan Selamoglu，AWS 高级技术作家
- Andy Wickersham，AWS 高级安全工程师

身份与身份与身份AWS 身份与身份与身份与身份与身份与合规性

通过简短的调查影响AWS安全参考架构 (AWSSRA) 的future。

有关简介或复习信息，请参阅 AWS 网站上的 AWS 安全、身份和合规性，以获取可帮助您保护云中工作负载和应用程序的 AWS 服务列表。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 提供的服务可帮助您保护数据、账户和工作负载免遭未经授权的访问。

- Amazon Macie — 利用机器学习支持的安全性对敏感数据进行发现、分类和分类和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 AWS 云中管理您的硬件安全模块 (HSM)。
- AWS Certificate Manager — 预置 SSL/TL/TL/TL/TL/TL/TL/TL/TLAWS 证书，管理和管理和管理和
- AWS Secrets Manager — 在数据库凭证，API 密钥和其他密钥的生命周期内对其进行轮换、管理和管理和管理和检索数据库凭证，API 密钥

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 — 安全地控制对亚马逊云AWS 服务和资源的访问权限。
- IAM 身份中心 — 集中管理对多个 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 S ervice erv——在亚马逊云中使用托管的Microsoft
- AWS Resource Access Manager — 简单安全地共享 AWS 资源。
- AWS Or ganizations — 对多个 AWS 账户实施基于策略的管理。

网络和应用程序保护 — 这些类别的服务使您能够在组织中的网络控制点强制执行精细的安全策略。AWS 服务可帮助您检查和筛选流量，以防止在主机级、网络级和应用程序级边界上进行未经授权的资源访问。

- AWS Shield — 利用托管 DDoS 保护保护在 AWS 上运行的 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 器 — 从中心位置配置和管理 AWS 账户和应用程序的 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 — 预置逻辑隔离部分，在自己定义的虚拟网络中预置逻辑隔离部分，在自己定义的虚拟网络中启动亚马逊云科技资源。
- AWS Network Firewall — 为您的 VPC 部署基本的网络保护。
- Amazon Route 53 DNS Firewall — 保护来自您 VPC 的出站 DNS 请求

威胁检测和持续监控 — AWS 监控和检测服务提供指导，帮助识别您的 AWS 环境中的潜在安全事件。

- AWS Security Hub — 从中心位置查看和管理安全警报并自动进行合规性检查。
- A@@ mazonGuardDuty — 通过智能威胁检测和持续监控保护您的 AWS 账户和工作负载。

- Amazon Inspector — 自动进行安全评估，以帮助提高在 AWS 上部署的应用程序的安全性和合规性。
- AWS Config — 记录和评估 AWS 资源的配置，以实现合规性审计、资源变更跟踪和安全分析。
- AWS Config Rules — 创建规则以响应环境的变化，例如隔离资源、使用额外数据丰富事件或将配置恢复到已知的良好状态。
- AWSCloudTrail — 跟踪用户活动和 API 使用情况，以实现对您的 AWS 账户的管理、运营和风险审计。
- Amazon Detecti ve — 分析和可视化安全数据，以快速找到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，这样您就可以扩展对事件的编程自动响应。

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

- AWS Arti fact — 使用免费的自助服务门户按需访问 AWS 安全与合规性报告以及精选在线协议。
- AWS Audit Manager — 持续审计您的 AWS 使用情况，以简化评估风险以及与相关法规与相关法规和行业标准合规性的方式。

文档历史记录

下表描述了本指南的重大更改。如果您想收到有关future 更新的通知，可以订阅 RSS 提要。

变更	说明	日期
次要更新 (p. 61)	• 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 AWSCloudTrail、AWS IAM 身份中心和边缘安全的架构指南。	2023 年 5 月 10 日
调查 (p. 61)	添加了一项简短的调查，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 (p. 61)	在 “AWS安全参考架构” 部分中，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 (p. 61)	在安全基础部分中，更新了有关 Well-Architected 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 (p. 61)	• 添加了有关如何使用 AWS SRA 和关键实施指南的信息。 • 为其他 AWS 服务（例如 AWS Artifact、Amazon Inspector、AWS RAM、AWS RAM、AWS Control Tower、AWS Audit Manager、AWS Directory Service、Amazon Cognito 和网络访问分析器）增加了架构指南。 • 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
— (p. 61)	首次发布产品 此版本不包含多项AWS服务（例如AWS Directory Service Amazon Cognito 和 AWS Audit Manager），我们计划在future 版本中添加这些服务。AWS Resource Access Manager	2021 年 6 月 23 日

AWS规范性指导词汇表

以下是AWS规范性指南提供的策略、指南和模式中的常用术语。要建议条目，请使用词汇表末尾的提供反馈链接。

安全条款

基于属性的访问控制 (ABAC)

根据用户属性（例如部门、工作角色和团队名称）创建细粒度权限的做法。有关更多信息，请参阅 AWS Identity and Access Management (I A M) 文档AWS中的 ABAC。

非对称加密

一种使用一对密钥、用于加密的公钥和用于解密的私钥的加密算法。您可以共享公钥，因为它不用于解密，但是对私钥的访问应受到严格限制。

行为图

一段时间内资源行为和交互情况的统一交互视图。您可以在 Amazon Detective 中使用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。

客户端加密

在目标AWS 服务收到数据之前，在本地对数据进行加密。

合规包

一组AWS Config规则和补救措施，您可以汇编这些规则和补救措施来自定义合规性和安全检查。您可以使用 YAML 模板将合规包作为单个实体部署在AWS 账户和区域内或整个组织中。有关更多信息，请参阅AWS Config文档中的一致性包。

静止数据

网络中固定的数据，例如存储中的数据。

数据分类

一种根据网络中的重要性和敏感性对数据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适当的数据保护和保留控制。数据分类是AWS架构完善的框架中安全支柱的组成部分。有关更多信息，请参阅数据分类。

传输中的数据

在您的网络中积极传输的数据，例如在网络资源之间。

defense-in-depth

一种信息安全方法，将一系列安全机制和控制措施巧妙地分层到整个计算机网络中，以保护网络和内部数据的机密性、完整性和可用性。当您采用此策略时AWS，可以在AWS Organizations结构的不同层添加多个控件以帮助保护资源。

委托管理员

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AWS Organizations中使用的服务。

侦探控制

一种安全控件，旨在在事件发生后进行检测、记录和发出警报。这些控制措施是第二道防线，可提醒您注意绕过现有预防性控制措施的安全事件。有关更多信息，请参阅启用安全控制中的侦探控件AWS。

加密密钥

由加密算法生成的由随机位组成的加密字符串。密钥的长度可能不同，每个密钥的设计都不可预测且独一无二。

端点服务

您可以托管在虚拟私有云 (VPC) 中与其他用户共享的服务。您可以使用其他AWS 账户或 IAM 委托人创建终端节点服务AWS PrivateLink并向其授予权限。这些账户或委托人可以通过创建接口 VPC 终端节点来私下连接到您的终端节点服务。有关更多信息，请参阅 Amazon VPC 文档中的创建终端节点服务。

信封加密

使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。

地理限制（地理封锁）

在亚马逊中CloudFront，一种防止特定国家/地区的用户访问内容分发版的选项。您可以使用允许列表或阻止列表来指定已批准和禁止的国家。有关更多信息，请参阅CloudFront文档中的限制内容的地理分布。

护栏

帮助管理组织单位 (OU) 的资源、策略和合规性的高级规则。预防性护栏强制执行政策，确保与合规标准保持一致。它们是通过使用服务控制策略和 IAM 权限边界来实现的。侦探护栏会检测违反政策和合规性问题，并生成警报以进行补救。它们是通过使用AWS Config、、亚马逊AWS Security HubGuardDutyAWS Trusted Advisor、亚马逊 Inspector 和自定义AWS Lambda检查来实现的。

基于身份的政策

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

入站（入口）VPC

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

检查 VPC

在AWS多账户架构中，一种集中式 VPC，用于管理 VPC（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安全参考架构建议使用入站、出站和检查 VPC 设置您的网络帐户，以保护您的应用程序与更广泛的互联网之间的双向接口。

最低权限

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

成员账户

AWS 账户除作为组织一部分的管理账户以外的所有账户AWS Organizations。一个账户一次只能是一个组织的成员。

组织线索

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。此跟踪是在组织中的每个成员中创建AWS 账户的，用于跟踪每个账户中的活动。有关更多信息，请参阅CloudTrail文档中的为组织创建路径。

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安全参考架构建议使用入站、出站和检查 VPC 设置您的网络帐户，以保护您的应用程序与更广泛的互联网之间的双向接口。

原始访问控制 (OAC)

中CloudFront，这是一个增强的选项，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。

原始访问身份 (OAI)

中CloudFront，这是一个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会创建一个可供 Amazon S3 进行身份验证的主体。经过身份验证的委托人只能通过特定的CloudFront分发访问 S3 存储桶中的内容。另请参阅 OAC (p. 64)，它提供了更精细和更增强的访问控制。

权限边界

附加到 IAM 委托人的 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。

policy

可以定义权限（参见基于身份的政策 (p. 63)）、指定访问条件（参见基于资源的策略 (p. 64)）或定义组织中所有账户的最大权限的对象AWS Organizations（参见服务控制策略 (p. 65)）。

预防性控制

一种旨在防止事件发生的安全控制。这些控制措施是第一道防线，有助于防止未经授权的访问或对您的网络进行不必要的更改。有关更多信息，请参阅上实施安全控制中的预防性控制。AWS

委托人

AWS 中可执行操作并访问资源的实体。此实体通常是根用户AWS 账户、IAM 角色或用户。有关更多信息，请参阅 IAM 文档中的角色术语和概念 “负责人”。

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。

基于资源的策略

附加到资源的策略，例如 Amazon S3 存储桶、终端节点或加密密钥。此类策略指定允许哪些委托人访问、支持的操作以及必须满足的任何其他条件。

响应式控制

一种安全控制措施，旨在推动对不良事件或偏离安全基准的行为进行补救。有关更多信息，请参阅上实现安全控制中的响应式控件AWS。

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)，因此用户可以登录AWS Management Console或调用 AWS API 操作，而无需您在 IAM 中为组织中的每个人创建用户。有关基于 SAML 2.0 的联合身份验证的更多信息，请参阅 IAM 文档中关于基于 SAML 2.0 的联合身份验证。

安全控制

一种技术或管理防护栏，用于防止、检测或降低威胁参与者利用安全漏洞的能力。安全控制主要有三种类型：预防性 (p. 64)的、侦 (p. 63)测的和响应式 (p. 64)的。

安全强化

缩小攻击面以使其更能抵抗攻击的过程。这可能包括诸如删除不再需要的资源、实施授予最低权限的安全最佳做法或停用配置文件中不必要的功能之类的操作。

安全信息和事件管理 (SIEM) 系统

结合安全信息管理 (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。

服务器端加密

由接收方在目的地对数据AWS 服务进行加密。

服务控制策略 (SCP)

一种提供对组织中所有账户权限的集中控制的策略AWS Organizations。SCP 为管理员可以委托给用户或角色的操作定义防护栏或设置限制。您可以将 SCP 用作允许列表或拒绝列表，以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。

责任共担模型

描述您在云安全与合规方面的共同责任AWS的模型。 AWS负责云的安全，而您负责云中的安全。有关更多信息，请参阅责任共担模式。

对称加密

一种使用相同密钥对数据进行加密和解密的加密算法。

可信访问

向您指定的服务授予权限，该服务可在您的组织内AWS Organizations及其账户中代表您执行任务。当需要服务相关角色时，可信服务会在每个账户中创建该角色以为您执行管理任务。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。

工作量

提供业务价值的资源和代码集合，例如面向客户的应用程序或后端流程。

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。