AWS 决策指南

选择 AWS 安全、身份和治理服务

选择 AWS 安全、身份和治理服务: AWS 决策指南

Table of Contents

选择 AWS 安全、身份和治理服务

迈出第一步

该读书了	27 分钟	
目的	帮助您确定哪些 AWS 安全、身份和治理服务最适合您的组织。	
上次更新	2024 年 12 月 30 日	
涵盖的服务	• AWS Artifact • AWS Audit Manager • AWS Certificate Manager • AWS CloudHSM • AWS CloudTrail • Amazon Cognito • AWS Config • AWS Control Tower • Amazon Detective • AWS Firewall Manager • Amazon GuardDuty • AWS IAM • AWS IAM Identity Center • Amazon Inspector	• AWS KMS • Amazon Macie • AWS Network Firewall • AWS Organizations • AWS Payment Cryptography • AWS 私有 CA • AWS RAM • AWS Secrets Manager • AWS Security Hub CSPM • Amazon Security Lake • AWS 安全事件响应 • AWS Shield • AWS WAF

简介

云端的安全、身份和治理是实现和维护数据和服务的完整性和安全性的重要组成部分。随着越来越多的企业迁移到云提供商，例如Amazon Web Services (AWS)，这一点尤其重要。

本指南可帮助您选择最适合您的需求和组织的 AWS 安全、身份和治理服务和工具。

首先，让我们探讨一下我们所说的安全、身份和治理是什么意思：

- 云安全是指使用措施和实践来保护数字资产免受威胁。这包括数据中心的物理安全和防范在线威胁的网络安全措施。 AWS 通过加密数据存储、网络安全和持续监控潜在威胁来优先考虑安全性。
- 身份服务可帮助您以可扩展的方式安全地管理身份、资源和权限。 AWS 提供专为员工和面向客户的应用程序以及管理工作负载和应用程序访问权限而设计的身份服务。
- 云治理是一组规则、流程和报告，可指导您的组织遵循最佳实践。您可以跨 AWS 资源建立云治理，使用内置的最佳实践和标准，并自动执行合规和审计流程。云端@@ 合规性是指遵守有关数据保护和隐私的法律法规。AWS 合规计划提供有关 AWS 符合的认证、法规和框架的信息。

这段 one-and-a-half简短的视频总结了如何 AWS 以我们的核心构建强大的安全性。

了解 AWS 安全、身份和治理服务

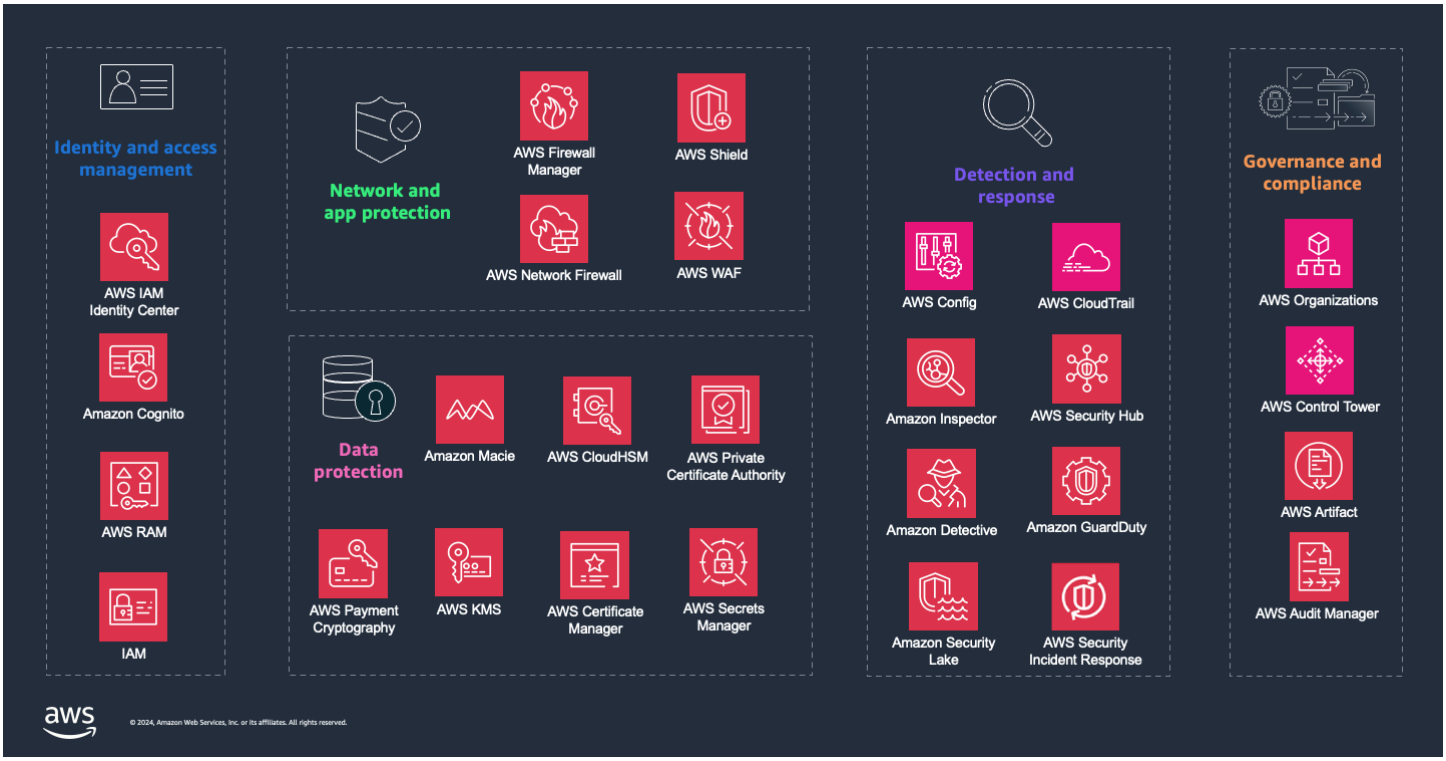
安全和合规是共同的责任

在选择 AWS 安全、身份和治理服务之前，请务必明白，安全和合规性是您和之间的共同责任 AWS。

这种分担责任的性质有助于减轻您的运营负担，并为您提供了灵活性和对部署的控制权。这种责任差异通常被称为云端的 “安全” 和 “云端的” 安全。

通过了解此模型，您可以了解可用的选项范围，以及 AWS 服务 适用的选项是如何组合在一起的。

您可以将 AWS 工具和服务结合起来，以帮助保护您的工作负载



如上图所示， AWS 它提供了跨五个域的工具和服务，以帮助您在云中实现和维护强大的安全、身份管理和治理。你可以 AWS 服务 跨这五个域名来帮助你完成以下任务：

- 形成多层次的方法来保护您的数据和环境
- 强化您的云基础架构，抵御不断变化的威胁
- 遵守严格的监管标准

要了解有关 AWS 安全性的更多信息，包括安全文档 AWS 服务，请参阅AWS 安全文档。

在以下各节中，我们将进一步研究每个域。

了解 AWS 身份和访问管理服务

AWS 安全的核心是最低权限原则：个人和服务只有他们需要的访问权限。 AWS IAM Identity Center推荐 AWS 服务 用于管理用户对 AWS 资源的访问权限。您可以使用此服务来管理对您的账户的访问权限和这些账户内的权限，包括来自外部身份提供商的身份。

下表汇总了本指南中讨论的身份和访问管理产品：

AWS IAM Identity Center

AWS IAM Identity Center帮助您连接身份来源或创建用户。您可以集中管理员工对多个应用程序 AWS 账户 的访问权限。

Amazon Cognito

Amazon Cognito 为网络和移动应用程序提供了一种身份工具，用于对来自内置用户目录、企业目录和消费者身份提供商的用户进行身份验证和授权。

AWS RAM

AWS RAM帮助您安全地在组织之间 AWS 账户、组织内部以及与 IAM 角色和用户共享资源。

IAM

IAM 支持对 AWS 工作负载资源的访问进行安全、精细的控制。

了解 AWS 数据保护服务

数据保护在云中至关重要， AWS 它提供的服务可帮助您保护数据、帐户和工作负载。例如，对传输中的数据和静态数据进行加密有助于保护其免遭泄露。使用 AWS Key Management Service(AWS KMS)，AWS CloudHSM您可以创建和控制用于保护数据的加密密钥。

下表汇总了本指南中讨论的数据保护产品：

Amazon Macie

Amazon Macie 使用机器学习和模式匹配来发现敏感数据，并启用针对相关风险的自动防护。

AWS KMS

AWS KMS创建和控制用于保护数据的加密密钥。

AWS CloudHSM

AWS CloudHSM提供高度可用、基于云的硬件安全模块 (HSMs)。

AWS Certificate Manager

AWS Certificate Manager处理创建、存储和续订公共和私有 SSL/TLS X.509 证书和密钥的复杂性。

AWS 私有 CA

AWS 私有 CA帮助您创建私有证书颁发机构层次结构，包括根证书颁发机构和从属证书颁发机构 (CAs)。

AWS Secrets Manager

AWS Secrets Manager帮助您管理、检索和轮换数据库凭证、应用程序凭证、 OAuth 令牌、API 密钥和其他密钥。

AWS Payment Cryptography

AWS Payment Cryptography根据支付卡行业 (PCI) 标准，提供对支付处理中使用的加密功能和密钥管理的访问权限。

了解 AWS 网络和应用程序保护服务

AWS 提供多种服务来保护您的网络和应用程序。 AWS Shield为您提供针对分布式拒绝服务 (DDoS) 攻击的保护，并AWS WAF帮助您保护 Web 应用程序免受常见的 Web 漏洞攻击。

下表汇总了本指南中讨论的网络和应用程序保护产品：

AWS Firewall Manager

AWS Firewall Manager简化了跨多个帐户和资源的管理和维护任务，以实现保护。

AWS Network Firewall

AWS Network Firewall为您的 VPC 提供有状态的托管网络防火墙以及入侵检测和防御服务。

AWS Shield

AWS Shield为网络、传输层和应用程序层的 AWS 资源提供保护，使其免受 DDo S 攻击。

AWS WAF

AWS WAF提供 Web 应用程序防火墙，因此您可以监控转发到受保护的 Web 应用程序资源的 HTTP (S) 请求。

了解 AWS 检测和响应服务

AWS 提供的工具可帮助您简化整个环境（包括多账户 AWS 环境）的安全操作。例如，您可以使用 Amazon GuardDuty 进行智能威胁检测，也可以使用 Amazon Detec tive 通过收集日志数据来识别和分析安全发现。 AWS Security Hub CSPM支持多种安全标准，并提供安全警报和合规状态的概述 AWS 账户。 AWS CloudTrail跟踪用户活动和应用程序编程接口 (API) 使用情况，这对于理解和响应安全事件至关重要。

下表汇总了本指南中讨论的检测和响应产品：

AWS Config

AWS Config提供了中 AWS 资源配置的详细视图 AWS 账户。

AWS CloudTrail

AWS CloudTrail记录用户、角色或采取的操作 AWS 服务。

AWS Security Hub CSPM

AWS Security Hub CSPM提供了您的安全状态的全面视图 AWS。

Amazon GuardDuty

Amazon 会 GuardDuty持续监控您的工作负载 AWS 账户、运行时活动和数据中是否存在恶意活动。

Amazon Inspector

Amazon Inspector 会扫描您的 AWS 工作负载中是否存在软件漏洞和意外网络泄露。

Amazon Security Lake

Amazon Security L ake 会自动将来自 AWS 环境、SaaS 提供商、本地环境、云源和第三方来源的安全数据集中到数据湖中。

Amazon Detective

Amazon Detective 可帮助您分析、调查和快速识别安全结果或可疑活动的根本原因。

AWS Security Incident Response

AWS 安全事件响应

帮助您快速做好准备、响应和接受指导，以帮助从安全事件中恢复过来。

了解 AWS 治理和合规服务

AWS 提供的工具可帮助您遵守安全、运营、合规和成本标准。例如，您可以使用使用规范性控制AWS Control Tower来设置和管理多账户环境。使用 AWS Organizations，您可以为组织内的多个账户设置基于策略的管理。

AWS 还可以根据您的组织所遵循 AWS 的最佳实践和行业标准，使用自动合规性检查，让您全面了解您的合规状态，并持续监控您的环境。例如，AWS Artifact提供对合规报告的按需访问权限，并AWS Audit Manager自动收集证据，以便您可以更轻松地评估控制措施是否有效运行。

下表汇总了本指南中讨论的治理和合规性产品：

AWS Organizations

AWS Organizations帮助您将多个组织整合 AWS 账户 到一个由您创建和集中管理的组织中。

AWS Control Tower

AWS Control Tower帮助您设置和管理基于最佳实践的 AWS 多账户环境。

AWS Artifact

AWS Artifact提供按需下载 AWS 安全与合规性文档。

AWS Audit Manager

AWS Audit Manager

帮助您持续审计 AWS 使用情况，以简化风险和合规性的评估方式。

考虑 AWS 安全、身份和治理标准

选择合适的安全、身份和治理服务 AWS 取决于您的具体要求和用例。决定采用 AWS 安全服务可以提供一个决策树，帮助您决定采用 AWS 服务 安全性、身份和治理性服务是否适合您的组织。此外，在决定使用哪些服务时，需要考虑以下标准。

Security requirements and threat landscape

对贵组织的特定漏洞和威胁进行全面评估。这包括识别您处理的数据类型，例如个人客户信息、财务记录或专有业务数据。了解与每种风险相关的潜在风险。

评估您的应用程序和基础架构架构。确定您的应用程序是否面向公众以及它们处理的网络流量类型。这会影响您对诸如防范网络利用 AWS WAF 之类的服务的需求。对于内部应用程序，请考虑内部威胁检测和使用 Amazon 进行持续监控的重要性 GuardDuty，这样可以识别异常访问模式或未经授权的部署。

最后，考虑一下您现有安全态势的复杂性以及安全团队的专业知识。如果您的团队资源有限，那么选择提供更多自动化和集成的服务可以为您提供有效的安全增强功能，而不会让您的团队不堪重负。示例服务包括针 AWS Shield 对 DDo S 保护和集中安全监控 AWS Security Hub CSPM 的服务。

Compliance and regulatory requirements

确定您所在行业或地理区域的相关法律和标准，例如《通用数据保护条例》(GDPR)、1996 年的《美国健康保险便携性和责任法案》(HIPAA) 或支付卡行业数据安全标准 (PCI DSS)。

AWS 提供诸如 AWS Config 和 A AWS rtifact 之类的服务，以帮助您管理对各种标准的合规性。借 AWS Config助，您可以评估、审计和评估您的 AWS 资源配置，从而更轻松地确保遵守内部策略和监管要求。 AWS Artifact 提供对 AWS 合规文档的按需访问权限，帮助您进行审计和合规报告。

选择符合您的特定合规需求的服务可以帮助您的组织满足法律要求并为您的数据构建一个安全可信的环境。浏览AWS 合规计划以了解更多信息。

Scalability and flexibility

考虑一下您的组织将如何发展以及增长速度。选择 AWS 服务 这样可以帮助您的安全措施与基础架构无缝发展并适应不断变化的威胁。

为了帮助您快速扩展， AWS Control Tower 我们整合了包括 AWS Organizations 和 AWS IAM Identity Center AWS 服务在内的其他几项功能，以便在不到一小时的时间内构建一个着陆区。Control Tower 代表您设置和管理资源。

AWS 还设计了许多服务以根据应用程序的流量和使用模式自动扩展，例如 GuardDuty 用于威胁检测和 AWS WAF 保护 Web 应用程序的 Amazon。随着业务的扩展，这些服务会随之扩展，无需手动调整或造成瓶颈。

此外，至关重要的是，您可以自定义安全控制措施，以满足您的业务需求和威胁形势。考虑使用管理您的账户 AWS Organizations，这样您就可以跨多个账户管理 40 多个服务资源。这为各个应用程序团队提供了灵活性和可见性，以管理特定于其工作负载的安全需求，同时还为他们提供了集中式安全团队的管理和可见性。

考虑可扩展性和灵活性有助于确保您的安全态势稳健、响应迅速，并且能够支持动态业务环境。

Integration with existing systems

考虑采取安全措施来增强而不是破坏您当前的运营。例如，请考虑以下内容：

- 通过汇总来自 AWS 服务 现有安全信息和事件管理 (SIEM) 系统的安全数据和警报，并将其与现有的安全信息和事件管理 (SIEM) 系统一起进行分析，从而简化工作流程。
- 创建跨本地和本地环境的安全威胁和漏洞的统一视图。 AWS
- AWS CloudTrail 与现有的日志管理解决方案集成，全面监控 AWS 基础架构和现有应用程序中的用户活动和 API 使用情况。
- 研究如何优化资源利用率并在各个环境中始终如一地应用安全策略。这可以帮助您降低安全覆盖范围出现漏洞的风险。

Cost and budget considerations

查看您正在考虑的每项服务的定价模式。 AWS 通常根据使用情况收费，例如 API 调用次数、处理的数据量或存储的数据量。例如，Amazon 根据为检测威胁而分析的日志数据量 GuardDuty收费，而 AWS WAF 账单则根据部署的规则数量和收到的 Web 请求数量收费。

估算您的预期使用量以准确预测成本。同时考虑当前需求和潜在的增长或需求激增。例如，可扩展性是的关键特性 AWS 服务，但如果管理不当，也会导致成本增加。使用AWS 定价计算器对不同的情景进行建模并评估其财务影响。

评估总拥有成本 (TCO)，包括直接成本和间接成本，例如管理和维护所需的时间和资源。选择托管服务可以减少运营开销，但价格可能会更高。

最后，根据风险评估确定安全投资的优先顺序。并非所有安全服务对您的基础架构都同样重要，因此请将预算集中在对降低风险和确保合规性影响最大的领域。在成本效益与所需安全级别之间取得平衡是成功实施 AWS 安全策略的关键。

Organizational structure and access needs

评估您的组织的结构和运作方式，以及您的访问需求可能因团队、项目或地点而异。这会影响您如何管理和验证用户身份、分配角色以及在整个 AWS 环境中实施访问控制。实施最佳实践，例如应用最低权限和要求多因素身份验证 (MFA)。

大多数组织都需要多账户环境。查看此类环境的最佳实践，并考虑使用 AWS Organizations 和 AWS Control Tower 来帮助您实现它。

您应该考虑的另一个方面是凭证和访问密钥的管理。考虑使用 IAM Identity Center 集中管理多个应用程序 AWS 账户 和业务应用程序的访问权限，从而增强安全性和用户便利性。为了帮助您顺利管理组织账户的访问权限，IAM Identity Center 集成 AWS Organizations了。

此外，请评估这些身份和访问管理服务如何与您现有的目录服务集成。如果您已有身份提供商，则可以使用 SAML 2.0 或 Open ID Connect (OIDC) 将其与 IAM 身份中心集成。IAM Identity Center 还支持跨域身份管理系统 (SCIM) 配置，以帮助保持目录同步。这可以帮助您在访问 AWS 资源时确保无缝安全的用户体验。

选择 AWS 安全、身份和治理服务

既然您已经知道了评估安全选项的标准，就可以选择哪种 AWS 安全服务最适合您的组织需求了。

下表突出显示了哪些服务针对哪些情况进行了优化。使用下表来帮助确定最适合您的组织和用例的服务。

Note

[1] 与 AWS Security Hub CSPM （完整列表）集成
[2] 与亚马逊集成 GuardDuty （完整列表）
[3] 与 Amazon Security Lake 集成（完整列表）

选择 AWS 身份和访问管理服务

向相应的个人授予对系统、应用程序和数据的适当访问权限。

你应该什么时候使用它？	它针对什么进行了优化？	安全、身份和治理服务
使用这些服务来帮助您安全地管理和控制客户、员工和工作负载的访问权限。	帮助您连接身份来源或创建用户。您可以集中管理员工对多个 AWS 账户和应用程序的访问权限。	AWS IAM Identity Center
	针对对 Web 和移动应用程序的用户进行身份验证和授权进行了优化。	Amazon Cognito
	针对安全共享内部资源进行了优化 AWS。	AWS RAM
	支持对 AWS 工作负载资源的访问进行安全、精细的控制。	IAM [1]

选择 AWS 数据保护服务

自动化和简化从密钥管理和敏感数据发现到凭据管理等数据保护和安全任务。

你应该什么时候使用它？	它针对什么进行了优化？	数据保护服务
使用这些服务可以帮助您实现和维护在 AWS 环境中存储和	针对发现敏感数据进行了优化。	亚马逊 Macie [1]

你应该什么时候使用它？	它针对什么进行了优化？	数据保护服务
处理的敏感数据的机密性、完整性和可用性。	针对加密密钥进行了优化。	AWS KMS
	针对... 进行了优化 HSMs。	AWS CloudHSM
	针对 SSL/TLS X.509 私有证书和密钥进行了优化。	AWS Certificate Manager
	针对创建私有证书颁发机构层次结构进行了优化。	AWS 私有 CA
	针对数据库凭证、应用程序凭证、 OAuth 令牌、API 密钥和其他机密进行了优化。	AWS Secrets Manager
	根据PCI标准，针对提供对支付处理中使用的加密功能和密钥管理的访问权限进行了优化。	AWS Payment Cryptography

选择 AWS 网络和应用程序保护服务

集中保护您的互联网资源免受常见 DDo的 S 和应用程序攻击。

你应该什么时候使用它？	它针对什么进行了优化？	网络和应用程序保护服务
使用这些服务来帮助您在每个网络控制点强制执行详细的安全策略。	针对集中配置和管理防火墙规则进行了优化。	AWS Firewall Manager[1]
	针对提供有状态的托管网络防火墙以及入侵检测和防御服务进行了优化。	AWS Network Firewall
	经过优化，可抵御网络、传输层和应用层 AWS 资源的 DDo S 攻击。	AWS Shield

你应该什么时候使用它？	它针对什么进行了优化？	网络和应用程序保护服务
	针对提供 Web 应用程序防火墙进行了优化。	AWS WAF

选择 AWS 检测和响应服务

持续识别安全风险并确定其优先级，同时尽早整合安全最佳实践。

你应该什么时候使用它？	它针对什么进行了优化？	检测和响应服务
使用这些服务可以帮助您检测和应对账户中的安全风险，从而大规模保护您的工作负载。	经过优化，可自动执行安全检查，并通过第三方集成集中安全警报。 AWS	AWS Security Hub CSPM[2、3]
	针对评估、审计和评估您的资源配置进行了优化。	AWS Config[1]
	针对将来自他人的事件记录 AWS 服务 为审计跟踪进行了优化。	AWS CloudTrail
	针对智能威胁检测和详细报告进行了优化。	亚马逊 GuardDuty [1]
	针对漏洞管理进行了优化。	亚马逊 Inspector [1]
	针对集中安全数据进行了优化。	亚马逊安全湖 [1]
	针对聚合和总结潜在安全问题进行了优化。	Amazon Detective [1、2、3]
	经过优化，可帮助您对发现结果进行分类、升级安全事件并管理需要您立即关注的案例。	AWS 安全事件响应

选择 AWS 治理和合规服务

对您的资源进行云监管，并自动执行合规和审计流程。

你应该什么时候使用它？	它针对什么进行了优化？	治理和合规服务
使用这些服务可以帮助您在使用时实施最佳实践并满足行业标准 AWS。	针对集中管理多个账户和整合账单进行了优化。	AWS Organizations
	经过优化，可按需下载 AWS 安全与合规性文档。	AWS Artifact
	针对审计 AWS 使用情况进行了优化。	AWS Audit Manager[1]
	针对设置和管理 AWS 多账户环境进行了优化。	AWS Control Tower

使用 AWS 安全、身份和治理服务

现在，您应该清楚地了解每项 AWS 安全、身份和治理服务（以及支持 AWS 工具和服务）的用途，以及哪些可能适合您。

为了探索如何使用每种可用的 AWS 安全、身份和治理服务并进一步了解这些服务，我们提供了探索每种服务的工作原理的途径。以下各节提供了指向深入文档、动手教程和资源的链接，以帮助您入门。

使用 AWS 身份和访问管理服务

下表显示了一些有用的身份和访问管理资源（按服务组织），可帮助您入门。

AWS IAM Identity Center

- 启用 AWS IAM 身份中心

  启用 IAM 身份中心并开始将其用于您的 AWS Organizations。

  浏览指南

- 使用默认 IAM 身份中心目录配置用户访问权限

  使用默认目录作为身份源，并设置和测试用户访问权限。

  开始阅读本教程
- 使用活动目录作为身份源

  完成使用 Active Directory 作为 IAM 身份中心身份源的基本设置。

  开始阅读本教程
- 使用 Okta 和 IAM 身份中心配置 SAML 和 SCIM

  与 Okta 和 IAM 身份中心建立 SAML 连接。

  开始阅读本教程

Amazon Cognito

- 亚马逊 Cognito 入门

  了解最常见的 Amazon Cognito 任务。

  浏览指南
- 教程：创建用户池

  创建用户池，允许您的用户登录您的网络或移动应用程序。

  开始阅读本教程
- 教程：创建身份池

  创建身份池，允许您的用户获取临时 AWS 凭证进行访问 AWS 服务。

  开始阅读本教程
- 亚马逊 Cognito 研讨会

  练习使用 Amazon Cognito 为假设的宠物店构建身份验证解决方案。

  开始阅读本教程

AWS RAM

- 入门 AWS RAM

  了解 AWS RAM 术语和概念。

  浏览指南

- 使用共享 AWS 资源

  共享您拥有的 AWS 资源，并访问与您共享的 AWS 资源。

  浏览指南

- 在 AWS RAM 中管理权限

  了解两种类型的托管权限：托 AWS 管权限和客户托管权限。

  浏览指南

- 配置对使用 AWS RAM 共享的资源的详细访问权限

  使用客户托管权限自定义您的资源访问权限并实现最低权限的最佳实践。

  阅读博客

IAM

- IAM 入门

  使用创建 IAM 角色、用户和策略 AWS 管理控制台。

  开始阅读本教程

- AWS 账户 使用角色委派访问权限

  使用角色委派对您拥有的不同 AWS 账户 资源（称为 “生产和开发”）的访问权限。

  开始阅读本教程

- 创建客户托管策略

  使用创建客户托管策略，然后将该策略附加到您的中的 IAM 用户 AWS 账户。 AWS 管理控制台

  开始阅读本教程

- 根据标签定义访问 AWS 资源的权限

  创建并测试允许具有委托人标签的 IAM 角色访问带有匹配标签的资源的策略。

  开始阅读本教程

- IAM 安全最佳实操

  使用 IAM 最佳实践帮助保护您的 AWS 资源。

  浏览指南

使用 AWS 数据保护服务

以下部分为您提供描述 AWS 数据保护的详细资源的链接。

Macie

- 亚马逊 Macie 入门

  为您启用 Macie AWS 账户，评估您的 Amazon S3 安全状况，并配置用于发现和报告 S3 存储桶中的敏感数据的关键设置和资源。

  浏览指南

- 使用 Amazon Macie 监控数据安全和隐私

  使用 Amazon Macie 监控亚马逊 S3 的数据安全并评估您的安全状况。

  浏览指南

- 分析 Amazon Macie 的调查结果

  查看、分析和管理 Amazon Macie 的调查结果。

  浏览指南

- 使用 Amazon Macie 的调查结果检索敏感数据样本

  使用 Amazon Macie 检索和显示个别调查结果报告的敏感数据样本。

  浏览指南

- 使用 Amazon Macie 发现敏感数据

自动发现、记录和报告 Amazon S3 数据资产中的敏感数据。

浏览指南

AWS KMS

- 入门 AWS KMS

  从创建到删除，管理对称加密 KMS 密钥。

  浏览指南
- 特殊用途钥匙

  了解除对称加密 KMS 密钥之外还 AWS KMS 支持的不同类型的密钥。

  浏览指南
- 通过以下方式扩展您的静态加密功能 AWS KMS

  了解其中提供的静态加密选项 AWS。

  探索工作坊

AWS CloudHSM

- 入门 AWS CloudHSM

  创建、初始化和激活集 AWS CloudHSM 群。

  浏览指南
- 管理 AWS CloudHSM 集群

  Connect 连接到您的 AWS CloudHSM 集群以及管理集群时执行各种管理任务。

  浏览指南
- 管理 HSM 用户和密钥 AWS CloudHSM

  在集群 HSMs 中创建用户和密钥。

  浏览指南

- 在 CloudHSM 中使用带有 TLS 卸载功能的 Amazon ECS 自动部署 NGINX 网络服务

  AWS CloudHSM 用于存储托管在云端的网站的私钥。

  阅读博客

AWS Certificate Manager

- 申请公共证书

  使用 AWS Certificate Manager (ACM) 控制台或 AWS CLI 申请公有 ACM 证书。

  浏览指南
- 的最佳实践 AWS Certificate Manager

  根据当前 ACM 客户的实际经验，学习最佳实践。

  浏览指南
- 如何使用 AWS Certificate Manager 来强制执行证书颁发控制

  使用 IAM 条件密钥确保您的用户根据贵组织的指南颁发或请求 TLS 证书。

  阅读博客

AWS 私有 CA

- 规划您的 AWS 私有 CA 部署

  在创建私有证书颁发机构之前做好使用准备 AWS 私有 CA 。

  浏览指南
- AWS 私有 CA 管理

  创建由根证书颁发机构和从属证书颁发机构组成的完全 AWS 托管的层次结构，供组织内部使用。

  浏览指南
- 证书管理

  使用执行基本的证书管理任务 AWS 私有 CA，例如颁发、检索和列出私有证书。

浏览指南

- AWS 私有 CA 工作坊

  积累有关私有证书颁发机构的各种用例的实践经验。

  探索工作坊

- 如何使用简化 Active Directory 中的证书配置 AWS 私有 CA

  用于更轻松地 AWS 私有 CA 为 Microsoft Active Directory 环境中的用户和计算机配置证书。

  阅读博客

- 如何在中强制执行 DNS 名称限制 AWS 私有 CA

  使用该 AWS 私有 CA 服务将 DNS 名称限制应用于从属 CA。

  阅读博客

AWS Secrets Manager

- AWS Secrets Manager 概念

  使用执行基本的证书管理任务 AWS 私有 CA，例如颁发、检索和列出私有证书。

  浏览指南

- 为用户设置交替轮换 AWS Secrets Manager

  为包含数据库凭据的密钥设置交替用户轮换。

  浏览指南

- 在 Kubern AWS Secrets Manager etes 中使用秘密

  使用密钥和配置提供程序 (ASCP) 将 Secrets Manager 中的 AWS 密钥显示为挂载在 Amazon EKS 容器中的文件。

  浏览指南

AWS Payment Cryptography

- 入门 AWS Payment Cryptography

创建密钥并将其用于各种加密操作。

浏览指南

- AWS Payment Cryptography FAQs

  了解以下基础知识 AWS Payment Cryptography。

  探索 FAQs

使用 AWS 网络和应用程序保护服务

下表提供了指向描述 AWS 网络和应用程序保护的详细资源的链接。

AWS Firewall Manager

- AWS Firewall Manager 策略入门

  AWS Firewall Manager 用于激活不同类型的安全策略。

  浏览指南

- 如何通过以下方式持续审计和限制安全组 AWS Firewall Manager

  AWS Firewall Manager 用于限制安全组，确保仅打开所需的端口。

  阅读博客

- AWS Firewall Manager 用于大规模部署保护 AWS Organizations

  AWS Firewall Manager 用于在您的范围内部署和管理安全策略 AWS Organizations。

  阅读博客

AWS Network Firewall

- 入门 AWS Network Firewall

  为具有基本互联网网关架构的 VPC 配置和实施 AWS Network Firewall 防火墙。

  浏览指南

- AWS Network Firewall 工作坊

使用基础架构 AWS Network Firewall 即代码进行部署。

探索工作坊

- AWS Network Firewall 灵活规则引擎的动手演练 — 第 1 部分

  AWS Network Firewall 在您的内部部署演示 AWS 账户 ，以便与其规则引擎进行交互。

  阅读博客

- AWS Network Firewall 灵活规则引擎的动手演练 — 第 2 部分

  创建具有严格规则顺序的防火墙策略并设置一个或多个默认操作。

  阅读博客

- 的部署模型 AWS Network Firewall

  学习常见用例的部署模型，您可以在其中 AWS Network Firewall 添加流量路径。

  阅读博客

- AWS Network Firewall 带有 VPC 路由增强功能的部署模型

  使用增强型 VPC 路由原语在同一 VPC 的不同子网中的工作负载 AWS Network Firewall 之间进行插入。

  阅读博客

AWS Shield

- 如何 AWS Shield 运作

  了解如何 AWS Shield Advanced 为网络 AWS Shield Standard 和传输层（第 3 层和第 4 层）以及应用层（第 7 层）的 AWS 资源提供防御 DDo S 攻击的方法。

  浏览指南

- 入门 AWS Shield Advanced

  使用 Shield Advan AWS Shield Advanced ced 控制台开始使用。

  浏览指南

- AWS Shield Advanced 工作坊

保护暴露在互联网上的资源免 DDo受 S 攻击，监控针对您的基础设施的 DDo S 攻击，并通知相应的团队。

探索工作坊

AWS WAF

- 入门 AWS WAF

  设置 AWS WAF、创建 Web ACL，并 CloudFront 通过添加规则和规则组来筛选网络请求来保护 Amazon。

  开始阅读本教程

- 分析 Amazon AWS WAF 日志中的 CloudWatch 日志

  设置对 Amazon AWS WAF 日志的原生 CloudWatch 日志记录，并可视化和分析日志中的数据。

  阅读博客

- 使用 Amazon CloudWatch 控制面板可视化 AWS WAF 日志

  使用 Amazon CloudWatch 通过 CloudWatch指标、贡献者见解和日志见解来监控和分析 AWS WAF 活动。

  阅读博客

使用 AWS 检测和响应服务

下表提供了描述 AWS 检测和响应服务的详细资源的链接。

AWS Config

- 入门 AWS Config

  设置 AWS Config 并使用 AWS SDKs。

  浏览指南

- 风险与合规研讨会

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

探索工作坊

- AWS Config 规则开发套件库：大规模构建和操作规则

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

  阅读博客

AWS CloudTrail

- 查看事件历史记录

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

  开始阅读本教程
- 创建记录管理事件的跟踪

  创建跟踪以记录所有区域的管理事件。

  开始阅读本教程

AWS Security Hub CSPM

- 正在启用 AWS Security Hub CSPM

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

  浏览指南
- 跨区域聚合

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

  浏览指南
- AWS Security Hub CSPM 工作坊

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

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

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

阅读博客

Amazon GuardDuty

- 开始使用亚马逊 GuardDuty

  启用 Amazon GuardDuty，生成样本调查结果并设置提醒。

  浏览教程

- Amazon 中的 EKS 保护 GuardDuty

  使用亚马逊监控您的亚马逊 GuardDuty Elastic Kubernetes Service（亚马逊 EKS）审核日志。

  浏览指南

- 亚马逊的 Lambda 保护 GuardDuty

  在调用 AWS Lambda 函数时识别潜在的安全威胁。

  浏览指南

- GuardDuty 亚马逊 RDS 保护

  使用亚马逊 GuardDuty 分析和分析亚马逊关系数据库服务 (Amazon RDS) 的登录活动，以了解您的亚马逊 Aurora 数据库是否存在潜在的访问威胁。

  浏览指南

- 亚马逊中的亚马逊 S3 保护 GuardDuty

  GuardDuty 用于监控 CloudTrail 数据事件并识别 S3 存储桶中的潜在安全风险。

  浏览指南

- 使用 Amazon 和 Amazon Detective 进行威胁检测 GuardDuty 和响应

  学习 Amazon GuardDuty 和 Amazon Detective 的基础知识。

  探索工作坊

Amazon Inspector

- 开始使用 Amazon Inspector

  激活 Amazon Inspector 扫描以了解控制台中的结果。

  开始阅读本教程

- 使用 Amazon Inspector 管理漏洞

  使用 Amazon Inspector 扫描亚马逊弹性容器注册表 (Amazon ECR) Container Registry 中的亚马逊 EC2 实例和容器映像，以查找软件漏洞。

  探索工作坊

- 如何使用 Amazon In EC2 AMIs spector 进行扫描

  使用多个漏洞扫描您的已知漏洞 AMIs ， AWS 服务 从而构建解决方案。

  阅读博客

Amazon Security Lake

- 亚马逊安全湖入门

  启用并开始使用 Amazon Security Lake。

  浏览指南

- 使用管理多个账户 AWS Organizations

  从多个中收集安全日志和事件 AWS 账户。

  浏览指南

- 收录、转换由 Amazon Security Lake 发布的事件并将其发送到亚马逊 OpenSearch 服务

  提取、转换亚马逊安全湖数据，并将其传送到亚马逊 OpenSearch 服务，供您的 SecOps 团队使用。

  阅读博客

- How to visualize Amazon Security Lake findings with Quick Suite

  使用亚马逊 Athena 和 Quick Suite 查询和可视化来自亚马逊安全湖的数据。

阅读博客

Amazon Detective

- Amazon Detective 术语和概念

  了解对于理解 Amazon Detective 及其工作原理非常重要的关键术语和概念。

  浏览指南
- 设置 Amazon Detective

  通过 Amazon Detective 控制台、Amazon Detective API 或启用 Amazon Detective AWS CLI。

  浏览指南
- 使用 Amazon 和 Amazon Detective 进行威胁检测 GuardDuty 和响应

  学习 Amazon GuardDuty 和 Amazon Detective 的基础知识。

  探索工作坊

使用 AWS 治理和合规服务

下表提供了描述治理和合规性的详细资源的链接。

AWS Organizations

- 创建和配置组织

  创建您的组织并使用两个 AWS 成员帐户对其进行配置。

  开始阅读本教程
- 与之配合使用的服务 AWS Organizations

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

  浏览指南
- 使用多个账户组织您的 AWS 环境

实施组织整体 AWS 环境的最佳实践和最新建议。

阅读白皮书

AWS Artifact

- 入门 AWS Artifact

  下载安全与合规报告、管理法律协议和管理通知。

  浏览指南
- 在中管理协议 AWS Artifact

  使用 AWS 管理控制台 来查看、接受和管理您的账户或组织的协议。

  浏览指南
- 为 AWS 第 1 部分中的审计做准备 — AWS Audit Manager 和 A AWS rtifact AWS Config

  AWS 服务 用于帮助您自动收集用于审计的证据。

  阅读博客

AWS Audit Manager

- 启用 Audi AWS t Manager

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

  浏览指南
- 审计所有者教程：创建评估

  使用 Audit Manager 示例框架创建评估。

  浏览指南
- 代表教程：审阅控件集

  在 Audit Manager 中查看审计责任人与您共享的控制集。

  浏览指南

AWS Control Tower

- 入门 AWS Control Tower

  按照规范性最佳做法设置并启动名为 landing zone 的多账户环境。

  浏览指南

- 使用 Amazon Bedrock 实现账户管理的现代化改造 AWS Control Tower

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

  阅读博客

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

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

  阅读博客

探索 AWS 安全、身份和治理服务

Editable architecture diagrams

参考架构图

浏览参考架构图，帮助您制定安全、身份和治理策略。

探索安全、身份和监管参考架构

Ready-to-use code

精选解决方案

上的安全见解 AWS

部署 AWS构建的代码来帮助您可视化 Amazon Security Lake 中的数据，从而更快地调查和响应安全事件。

探索此解决方案

AWS 解决方案

探索由构建的预配置、可部署的解决方案及其实施指南。 AWS

探索所有 AWS 安全、身份和治理解决方案

Documentation

安全、身份和治理白皮书

浏览白皮书，了解有关选择、实施和使用最适合您组织的安全、身份和治理服务的更多见解和最佳实践。

浏览安全、身份和治理白皮书

AWS 安全博客

浏览针对特定安全用例的博客文章。

浏览 AWS 安全博客

文档历史记录

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

变更	说明	日期
re: Invent 更新	添加了有关 AWS 安全事件响应和 AWS Payment Cryptography. 更新了 AWS Identity and Access Management 和的服务信息 AWS IAM Identity Center。	2024 年 12 月 30 日
视频更新	更新了介绍性视频，其中包含最近来自 re: InForce 2024 的闪电演讲。	2024 年 6 月 25 日
添加了治理服务	将文档的范围扩大到包括治理，包括添加 AWS CloudTrail AWS Control Tower、和。AWS Organizations更新了图形以反映新的范围。阐明了身份的最佳实践。对全文进行了编辑性修改。	2024 年 6 月 7 日
初次发布	指南首次出版。	2024 年 3 月 21 日

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