AWS 隐私参考架构

AWS 规范性指导

AWS 规范性指导: AWS 隐私参考架构

Table of Contents

AWS 隐私参考架构

Amazon Web Services（贡献者）

2025 年 9 月（文档历史记录）

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

通知

本指南仅供参考。它不是法律建议，也不应被用作法律建议。 AWS 鼓励其客户就其隐私和数据保护环境的实施以及更笼统地说，与其业务相关的适用法律获得适当的建议。

客户有责任对本文档中的信息进行单独评测。本文件：(a) 仅供参考，(b) 代表当前 AWS 的产品供应和实践，如有更改，恕不另行通知，以及 (c) 不产生其关联公司、供应商或许可方的任何承诺或保证。 AWS AWS 产品或服务“按原样”提供，不附带任何形式的担保、陈述或条件，无论是明示还是暗示。

对客户的责任和责任由 AWS 协议控制，本文档不属于其客户之间的任何协议，也不会对其 AWS 进行修改。 AWS

简介

AWS 隐私参考架构 (AWS PRA) 提供了一套专门针对中支持隐私的控件的设计和配置的指导方针。 AWS 服务本指南可以帮助您做出有关人员、流程和技术的决策，从而支持 AWS 云中的隐私保护。

责任 AWS 共担模式和隐私

在中 AWS 云，您共同承担安全与合规责任 AWS。 AWS 负责云的安全，这意味着 AWS 它负责保护运行云中提供的所有服务的基础架构 AWS 云。您对云中的安全负责，这意味着您负责根据安全和隐私要求进行配置和管理 AWS 服务 。有关更多信息，请参阅责任AWS 共担模型。

AWS 服务 提供允许您在云端实施自己的隐私控制的功能，以支持您的隐私要求。您的隐私责任因许多因素而异，包括 AWS 区域 您选择的内容、将这些服务集成到您的 IT 环境以及适用于您的组织和工作负载的法律和法规。 AWS 服务

使用时 AWS 服务，您可以控制自己的内容。具体而言，客户内容被定义为您或任何最终用户传输给我们进行处理、存储或托管的软件（包括机器图像）、数据、文本、音频、视频或图像，这些 AWS 服务内容与您的账户有关。它还包括您或最终用户通过使用 AWS 服务得出的任何计算结果。您将负责管理由您控制的以下决策：

- 您选择收集、存储或处理的数据 AWS
- AWS 服务 你在数据中使用的
- 您收集、存储或处理数据 AWS 区域 的地方
- 数据的格式和结构，以及数据是否经过屏蔽、匿名化或加密
- 如何定义、存储、轮换和操作用于加密的密钥
- 有权访问数据的人员、其有权访问数据的时间，以及如何授予、管理和撤销这些访问权限

了解了 AWS 分担责任模型及其通常如何适用于云端运营后，您必须确定它如何适用于您的用例。您选择使用的配置决定了您作为组织隐私责任的一部分必须执行的配置量。 AWS 服务 例如，Amazon Elastic Compute Cloud（Amazon EC2）等服务被归类为基础设施即服务（IaaS）。因此，如果您使用 Amazon EC2，则必须为来宾操作系统以及在 EC2 实例上安装的应用程序软件或实用程序执行所有必要的隐私配置。当您使用抽象服务（例如亚马逊简单存储服务 (Amazon S3) Simple Storage Service 和 Amazon DynamoDB）时，将负责基础设施层 AWS 、操作系统和平台。您的责任是管理和分类数据（客户内容），并配置用于访问端点的策略，以便存储和检索数据。有关如何 AWS 帮助您保护数据和隐私的更多信息，请参阅数据保护和隐私，网址为 AWS。

了解 AWS PRA

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

本节描述了 AWS 隐私参考架构 (AWS PRA) 与其他 AWS 指南之间的关系。本节还回顾了 AWS PRA 中示例 AWS 多账户环境的总体布局和结构。

本节包含以下主题：

- 使用 P AWS RA 和 SRA AWS
- AWS Organizations 和专用账户结构
- 运营 AWS 隐私服务

使用 P AWS RA 和 SRA AWS

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

AWS PRA 提供的模式有助于客户为其基础架构和工作负载规划基础和应用程序级隐私控制。AWSAWS 安全参考架构 (AWS SRA) 为构建架构提供了一套指南，该架构可在您的 AWS 着陆区和应用程序中实施和支持一组正确的安全控制。为了建立本指南中详述的隐私控制， AWS PRA假设许多与SRA中描述的基本准则和账户结构相同。 AWS P AWS RA 和 AWS SRA 详细说明了许多相同的密钥。 AWS 服务本指南仅包含这些服务的简要描述。您可以在 AWS SRA 中详细了解这些服务以及如何在安全环境中使用它们。

AWS SRA 可以帮助您设计、实施和管理 AWS 安全服务，使其符合 AWS 建议的做法。您可以将 AWS SRA 用作独立指南，也可以使用 AWS SRA 和 AWS PRA 作为配套指南。 AWS SRA中详述的许多安全准则可以与PRA中详述的隐私控制措施一起遵守。 AWS 与安全性类似，在您 AWS 云 旅程的早期阶段就进行基本隐私考量可能非常有用，因为这些决策可能会影响组织账户结构的设计。例如，您可能会考虑的一些问题包括：

- 我的组织如何定义个人数据？

- 我的组织是否支持处理个人数据的应用程序？
- 那处理其他类型受监管数据的应用程序呢？
- 我可以实施哪些组织级别的控制措施，使我的开发人员和云工程师尽可能远离个人数据？
- 如何将个人数据与其他类型的数据隔离？
- 我的组织有哪些跨境数据传输要求？

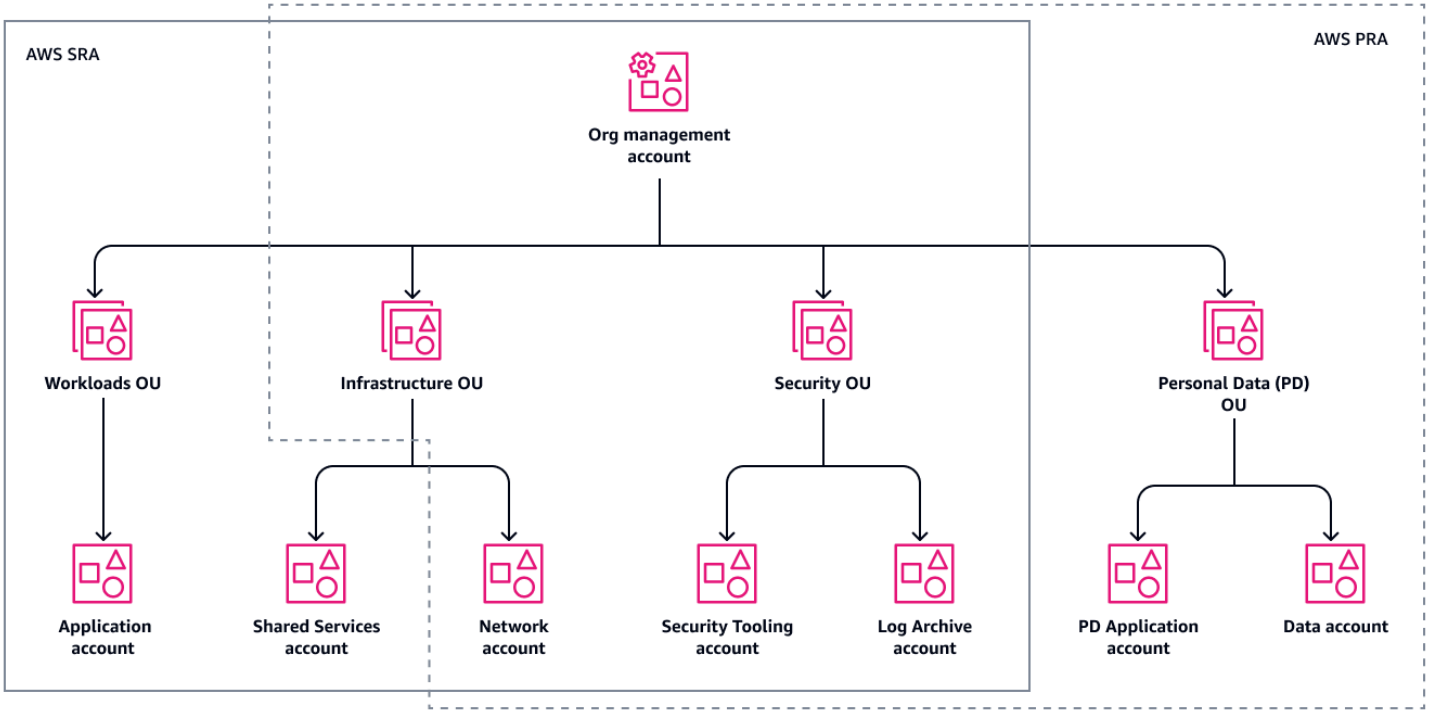
其中许多问题的答案可能会对您的云环境设计产生影响，例如您的 AWS 账户 结构、服务控制策略和 AWS Identity and Access Management (IAM) 角色。

AWS Organizations 和专用账户结构

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

AWS Organizations 是一项账户管理服务，可帮助您集中管理和治理多个 AWS 账户。的使用 AWS Organizations 是架构良好的多 AWS 账户环境的基础。有关更多信息，请参阅 Establishing your best practice AWS environment。

下图显示了 AWS PRA 的高级账户和组织单位 (OU) 结构。在大多数情况下，PRA的组织结构与 AWS AWS RA的组织结构相匹配。



与 AWS SRA 组织的偏差包括：

- AWS PRA 增加了个人数据 (PD) OU，专门用于收集、存储和处理个人数据。这种结构分离提供了灵活性，因此您可以定义具体、细粒度的控制措施，以帮助保护个人数据免遭意外泄露。
- 在基础设施 OU 中， AWS PRA 目前不包含 AWS SRA 中描述的共享服务账户的其他指导。
- P AWS RA 目前不包含 AWS SRA 中描述的工作负载 OU 的其他指南。收集或处理个人数据的应用程序位于 PD OU 的专用账户中。

您可以使用 AWS Control Tower 在整个组织中进行整体基础治理，并自动部署安全和隐私控制措施。如果您的组织目前 AWS Control Tower 没有使用，您仍然可以在其各自的服务中部署许多安全和隐私控件 AWS Control Tower，例如服务控制策略和 AWS Config 规则。

您可能会发现，在规划账户和 OU 结构（包括账户细分策略）时，考虑处理个人数据很有帮助。您可能需要根据所处理的数据类型，考虑其独特的使用案例和适用的法律法规。例如，持卡人数据受支付卡行业数据安全标准（PCI DSS）保护，而受保护的健康信息可能受《健康保险流通与责任法案》（HIPAA）约束。您可能需要查看哪些环境包含个人数据，并以此为重点制定细分策略。典型的客户细分策略可以包括与软件开发生命周期（SDLC）保持一致的专用 AWS 账户 ，例如用于开发、暂存或质量保证（QA）和生产的专用账户。诸如此类的细分策略可能是整个设计讨论中的关键组成部分，您 OUs 可能需要与特定的监管要求保持一致。

有些多账户 AWS 环境需要每个账户专用的应用程序账户 AWS 区域，或者可能需要多账户登录区域。在这种情况下，您需要进行额外的细分，以满足客户和监管机构的独特数据主权要求。有关更多信息，请参阅本指南中的制定全球扩展战略。

运营 AWS 隐私服务

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

对于许多人来说，隐私是跨领域的。许多不同的团队都在其中发挥作用，包括监管、合规和工程团队。当您的组织开始定义隐私计划的关键人员和策略组成部分时，您可以根据隐私合规框架映射控制措施，以实施一致的运营。框架可以作为在您的环境中对个人数据实施基础和特定于应用程序的隐私控制的标准。 AWS

无论客户使用哪种框架对其隐私要求进行分类，隐私合规、隐私工程和应用程序团队通常都需要协同工作才能实现实施目标。例如，监管和合规团队可能会提供高级要求，而工程和应用团队可以根据这些要求进行配置 AWS 服务 和功能。从控制框架入手可以帮助您定义更具规范性的组织和技术控制措施。

在定义技术控制 AWS 服务 和功能时，另一个关键决定是控制应适用于整个组织、组织单位、账户还是特定资源。有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 存储桶的公开访问是一项特定的控制措施，最好在组织根目录进行配置，而不是为每个账户单独配置。但是，您的保留策略可能因应用程序而异，这意味着可能需要在资源级别应用控制措施。

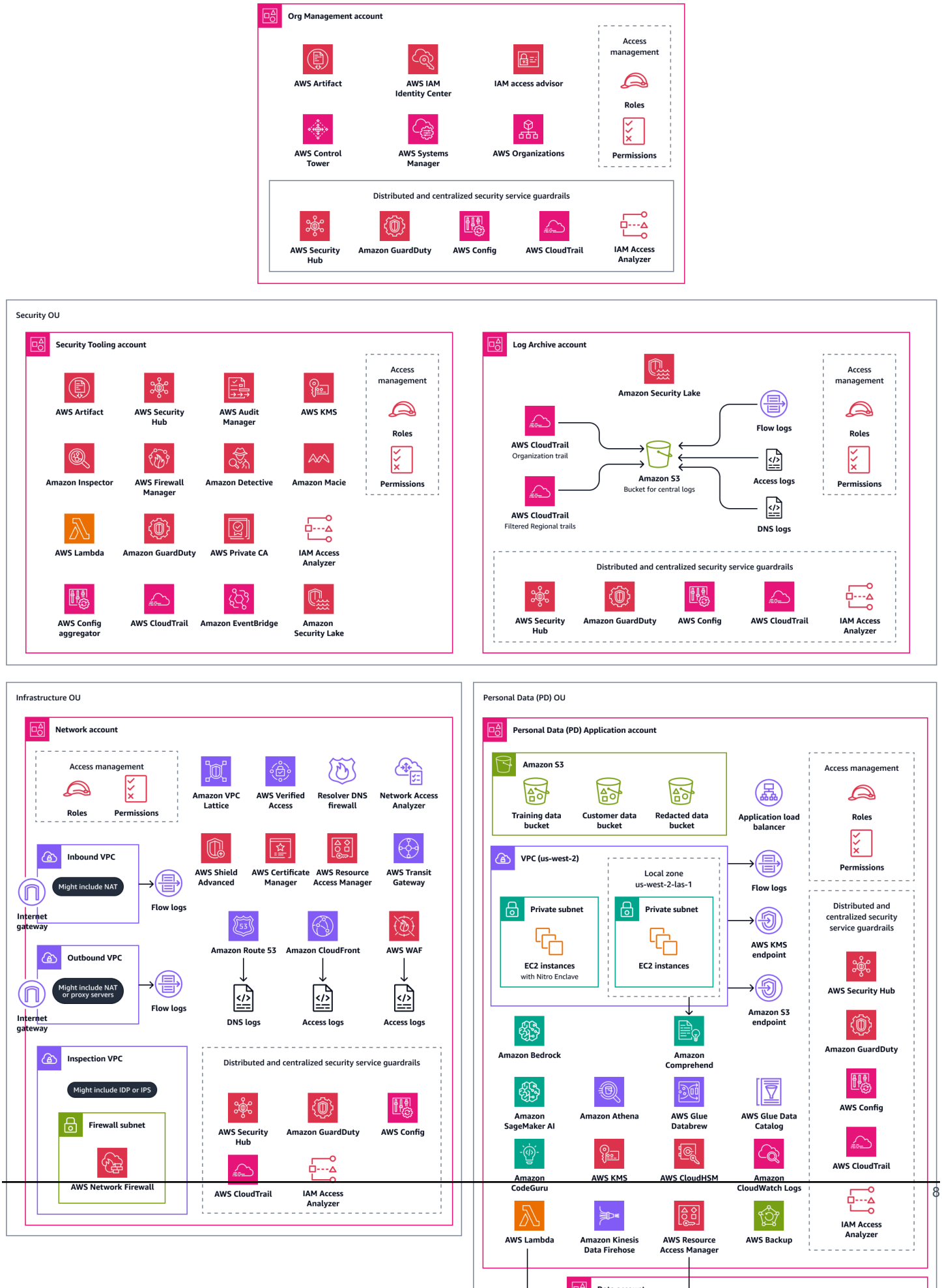
为帮助您加快组织中隐私的实施，为您的 AWS 工作负载 AWS 提供审计和合规咨询服务。欲了解更多信息，请联系 AWS SAS。

AWS 隐私参考架构

调查

我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

下图说明了 AWS 隐私参考架构 (AWS PRA)。这是连接许多与隐私相关的 AWS 服务 功能的架构示例。该架构基于受 AWS Control Tower管辖的登录区构建。


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Access management
Roles
Permissions
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Amazon Security Lake
Log Archive account
Amazon Security Lake
AWS CloudTrail
Organization trail
Flow logs
Amazon S3
Bucket for central logs
Access logs
AWS CloudTrail
Filtered Regional trails
DNS logs
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IDP or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup

AWS PRA 包括托管在个人数据 (PD) 应用程序账户中的无服务器 Web 架构。此账户中的架构是一个示例工作负载，它直接从用户那里收集个人数据。在此工作负载中，用户通过 Web 层进行连接。Web 层与应用程序层进行交互。该层接收来自 Web 层的输入，对其进行处理并存储数据，允许授权的内部团队和第三方访问这些数据，并且在不再需要这些数据时对其进行存档和删除。该架构具有明确的模块化和事件驱动的特点，旨在展示许多基础的隐私工程技术，而不深入探讨诸如数据湖、容器、计算或物联网（IoT）等具体使用案例。

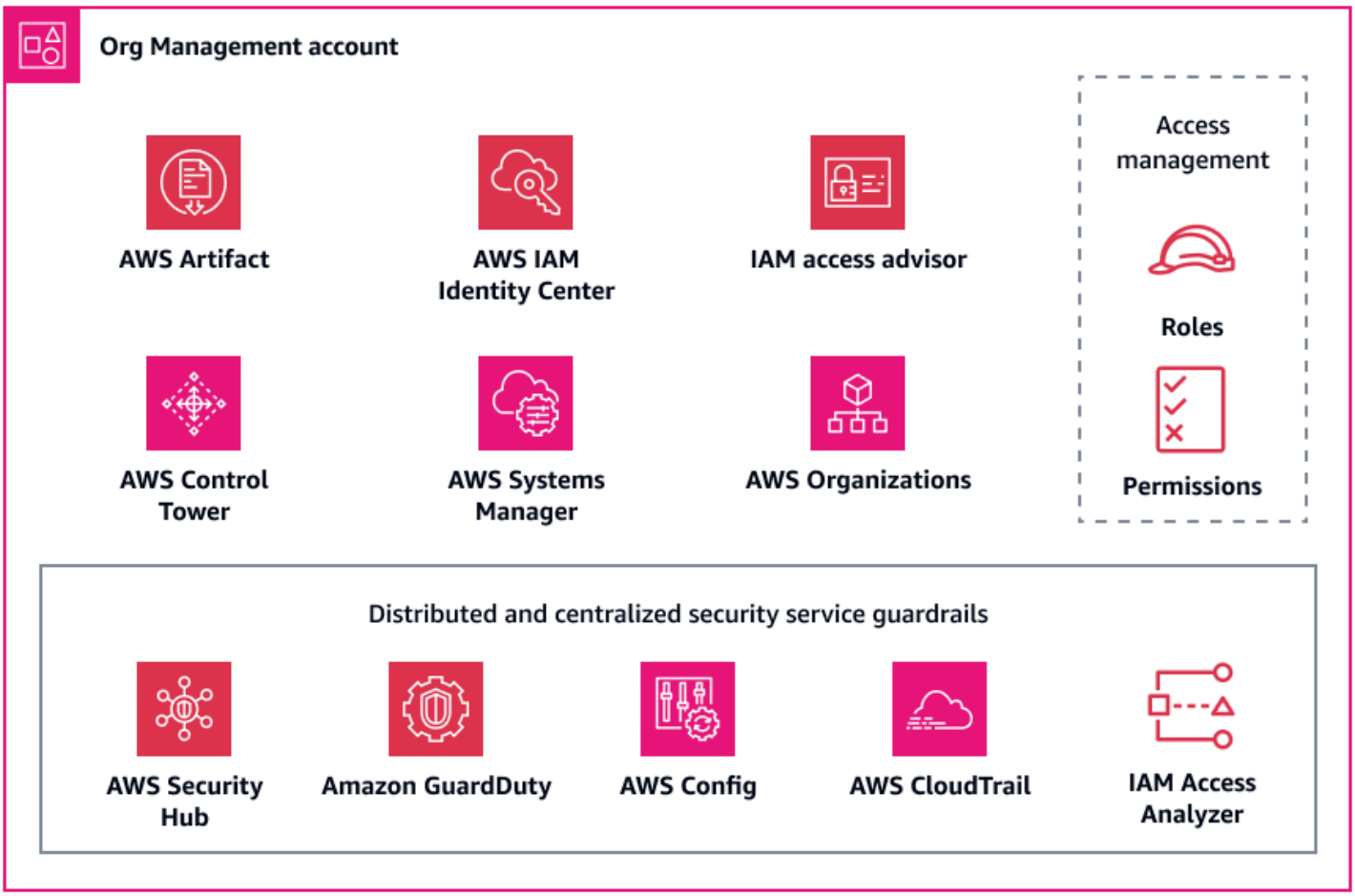
接下来，本指南将详细描述组织内的每个账户。它将讨论与隐私相关的服务和功能、注意事项和建议，以及以下每个账户的示意图：

- 组织管理账户
- 安全 OU – 安全工具账户
- 安全 OU – 日志存档账户
- 基础设施 OU – 网络账户
- 个人数据 OU – PD 应用程序账户

组织管理账户

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

组织管理账户主要用于管理您组织内所有账户中基础隐私控件的资源配置漂移，该功能由 AWS Organizations负责管理。您还可以在此账户中始终如一地部署新的成员账户，而且还能享受到与现有账户相同的安全和隐私保护措施。有关此账户的更多信息，请参阅AWS 安全参考架构 (AWS SRA)。下图说明了在组织管理账户中配置 AWS 的安全和隐私服务。



本部分提供有关此账户中使用的以下 AWS 服务 的更多详细信息：

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifact 可以通过提供 AWS 安全与合规性文档的按需下载来帮助您进行审计。有关如何在安全情境中使用此服务的更多信息，请参阅 AWS 安全参考架构。

这 AWS 服务 可以帮助您了解继承自哪些控件， AWS 并确定在您的环境中可能还有哪些控件可供您实施。 AWS Artifact 提供对 AWS 安全与合规报告的访问权限，例如系统和组织控制 (SOC) 报告和支付卡行业 (PCI) 报告。它还提供获得来自不同地区和合规垂直行业的认证机构的认证的机会，这些认证可以验证控制措施的实施和运营有效性。 AWS 使用 AWS Artifact，您可以向 AWS 审计师或监管机构提

供审计工件，作为 AWS 安全和隐私控制的证据。以下报告可能有助于证明 AWS 隐私控制措施的有效性：

- SOC 2 第 2 类隐私报告 — 该报告展示了对个人数据收集、使用、保留、披露和处置方式的 AWS 控制措施的有效性。还有一份 SOC 3 隐私报告，该报告对 SOC 2 隐私控制措施的描述不太详细。有关更多信息，请参阅 SOC 常见问题。
- 云计算合规性控制目录（C5）：此报告由德国国家网络安全管理机构联邦信息安全局（BSI）编写。它详细介绍了 AWS 为满足 C5 要求而实施的安全控制措施。它还包括与数据位置、服务预调配、管辖区域以及信息披露义务相关的额外隐私控制要求。
- ISO/IEC 27701:2019 认证报告：ISO/IEC 27701:2019 描述了建立和持续改进隐私信息管理系统（PIMS）的要求和指南。该报告详细说明了该认证的范围，可以作为 AWS 认证证明。有关该标准的更多信息，请参阅 ISO/IEC 27701:2019（ISO 网站）。

AWS Control Tower

AWS Control Tower帮助您设置和管理遵循规范性安全建议做法的 AWS 多账户环境。有关如何在安全情境中使用此服务的更多信息，请参阅 AWS 安全参考架构。

在中 AWS Control Tower，您还可以自动部署许多主动式、预防性和侦查性控制措施（也称为护栏），这些控制措施符合您的数据隐私要求，特别是针对数据驻留和主权的要求。例如，您可以指定护栏，将数据传输仅限于获得批准的 AWS 区域。要进行更精细的控制，您可以从超过 17 个旨在控制数据驻留的护栏中进行选择，例如禁止亚马逊虚拟专用网络 (VPN) 连接、不允许 Amazon VPC 实例访问互联网以及根据请求拒绝 AWS 访问。 AWS 区域这些护栏由许多 AWS CloudFormation 挂钩、服务控制策略和规则组成，这些策略和 AWS Config 规则可以在您的组织中统一部署。有关更多信息，请参阅 AWS Control Tower 文档中的增强数据驻留保护的控件。

在数据主权方面， AWS Control Tower 目前提供了预防性控制措施，例如要求将附加的 Amazon EBS 卷配置为对静态数据进行加密，以及要求 AWS KMS 密钥策略具有将 AWS KMS 授权创建限制为的声明。 AWS 服务主权控制的范畴远不止数据驻留控制这一项。它们有助于防止可能出现违反数据驻留、精细访问限制、加密以及恢复能力要求的操作。有关更多信息，请参阅 AWS Control Tower 文档中有助于实现数字主权的预防性控制措施。

如果您需要在数据驻留和主权控制之外部署隐私护栏，请 AWS Control Tower 包括一些强制性控制措施。设置登录区时，这些控制措施会默认部署于每个 OU。其中许多是旨在保护日志的预防性控制措施，例如 “不允许删除日志存档” 和 “启用日志文件完整性 CloudTrail 验证”。

AWS Control Tower 还集成在一起 AWS Security Hub CSPM 以提供侦探控制。这些控件被称为服务管理标准: AWS Control Tower. 您可以使用这些控制措施来监控与隐私保护相关的控制措施（例如

Amazon Relational Database Service（Amazon RDS）数据库实例中的静态加密）的配置是否出现漂移。

AWS Organizations

P AWS RA AWS Organizations 用于集中管理架构中的所有账户。有关更多信息，请参阅本指南中的AWS Organizations 和专用账户结构。在中 AWS Organizations，您可以使用服务控制策略 (SCPs) 和管理策略来帮助保护个人数据和隐私。

服务控制策略 (SCPs)

服务控制策略 (SCPs) 是一种组织策略，可用于管理组织中的权限。它们可以集中控制目标账户、组织单位 AWS Identity and Access Management (OU) 或整个组织中 (IAM) 角色和用户的最大可用权限。您可以通过组织管理账户创建和申请 SCPs 。

您可以使用 AWS Control Tower 在您的账户中 SCPs 统一部署。有关您可以申请的数据驻留控制的更多信息 AWS Control Tower，请参阅本指南AWS Control Tower中的。 AWS Control Tower 包括全套的预防措施 SCPs。如果您的组织当前未使用 AWS Control Tower ，您也可以手动部署这些控制措施。

SCPs 用于满足数据驻留要求

通过在特定的地理区域内存储和处理数据来满足个人数据驻留要求是常见的做法。为了验证某个司法管辖区所规定的独特数据驻留要求是否得到满足，我们建议您与您的监管团队密切合作，以确认您的要求。确定这些要求后，有许多 AWS 基本的隐私控制措施可以提供支持。例如，您可以使用 SCPs 来限制哪些数据 AWS 区域 可用于处理和存储数据。有关策略示例，请参阅本指南中的 限制跨数据传输 AWS 区域。

SCPs 用于限制高风险 API 调用

重要的是要了解哪些安全和隐私控制措施 AWS 负责，哪些由您负责。例如，您需要对针对您所使用的 AWS 服务 所进行的 API 调用所产生的结果负责。您还需负责弄清楚其中哪些调用可能会对您的安全或隐私状况产生影响。如果您担心保持一定的安全和隐私状态，则可以启用 SCPs 拒绝某些 API 调用的功能。这些 API 调用可能会产生影响，例如可能导致个人数据意外泄露或违反特定跨境数据传输的规定。例如，您可能希望禁止以下的 API 调用：

- 允许公众访问 Amazon Simple Storage Service（Amazon S3）存储桶
- 禁用 Amazon GuardDuty 或为数据泄露发现创建禁止规则，例如特洛伊木马:ec2/ Extiltrati DNSData on 发现

- 删除 AWS WAF 数据泄露规则
- 公开共享 Amazon Elastic Block Store（Amazon EBS）快照
- 从组织中移除成员账户
- 解除 Amazon CodeGuru Reviewer 与存储库的关联

管理策略

中的@@ 管理策略 AWS Organizations 可以帮助您集中配置 AWS 服务 和管理其功能。您选择的管理策略类型决定了策略如何影响 OUs 和继承这些策略的账户。标签策略是与隐私直接相关的管理策略 AWS Organizations 的一个示例。

使用标签策略

标签是键值对，可帮助您管理、识别、组织、搜索和筛选 AWS 资源。应用标签来区分您所在组织中处理个人数据的相关资源，这一做法可能会很有用。标签的使用支持本指南中提及的许多隐私解决方案。例如，您可能需要为该资源内正在处理或存储的数据应用一个标签，以表明这些数据的大致数据分类。您可以编写基于属性的访问权限控制（ABAC）策略，以限制对具有特定标签或一组标签的资源的访问。例如，您的策略可能会规定，SysAdmin 角色不能访问带有 dataclassification:4 标签的资源。有关更多信息和教程，请参阅 IAM 文档中的基于标签定义 AWS 资源访问权限。此外，如果您的组织使用 AWS Backup 来在多个账户中的备份中广泛应用数据留存策略，您可以应用一个标签，以将该资源纳入该备份策略的适用范围内。

标签策略可帮助您在整个组织中保持标签的一致性。在标签策略中，您可以指定在标记资源时适用于资源的规则。例如，您可以要求将资源标记上特定的键（例如 DataClassification 或 DataSteward），并且可以为键指定有效的大小写处理或值。您还可以使用强制措施来防止不合规的标记请求完成。

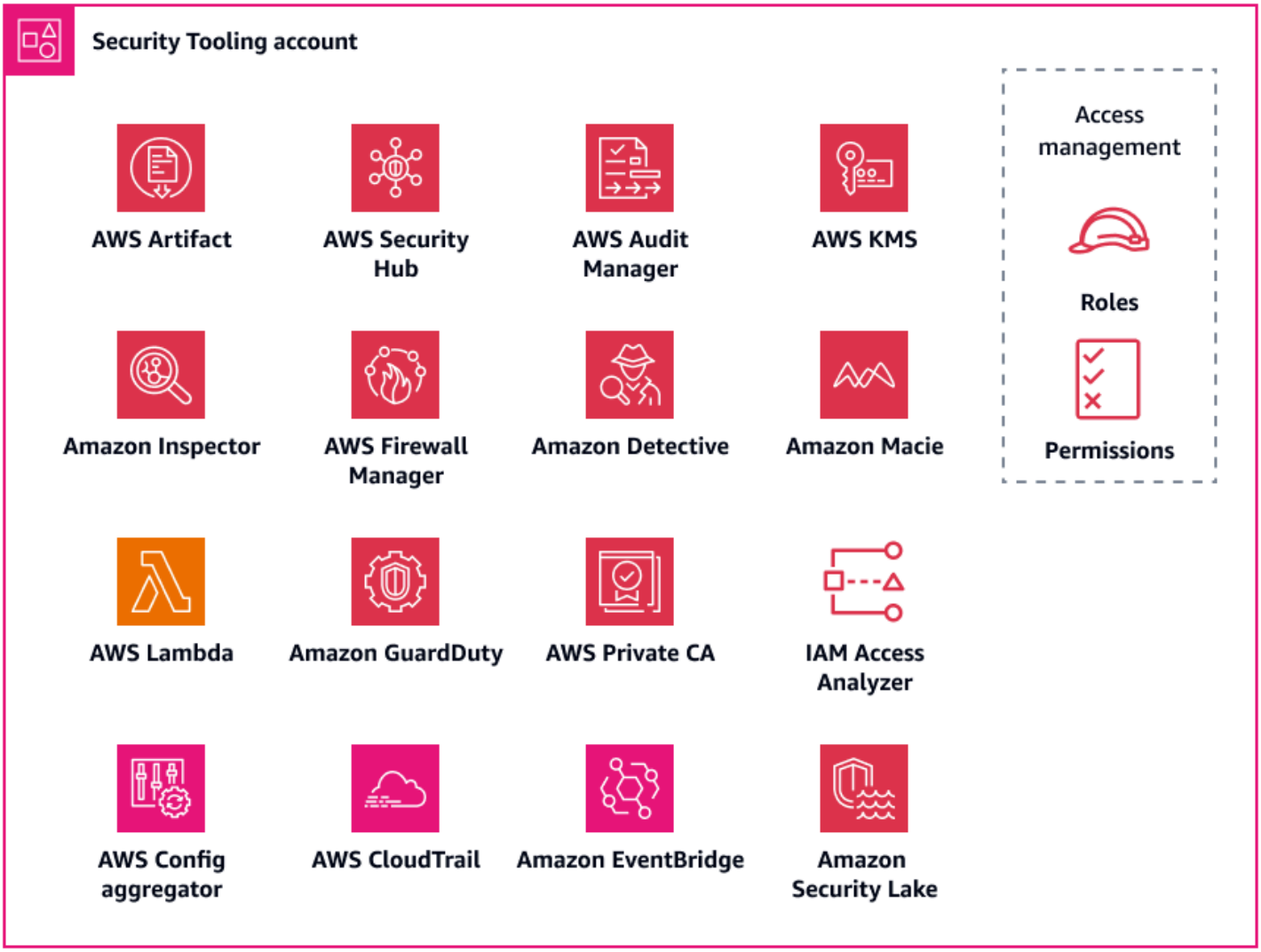
在将标签用作隐私控制策略的核心组成部分时，请考虑以下几点：

- 请考虑将个人数据或其他类型的敏感数据置于标签键或标签值中的影响。当您联系 AWS 寻求技术帮助时， AWS 可能会分析标签和其他资源标识符以帮助解决问题。标签数据未加密 AWS 服务，例如 AWS 账单与成本管理，可以读取它们。因此，您可能需要取消标识标签值，然后使用您控制的系统（例如 IT 服务管理 (ITSM) 系统）对其进行重新标识。 AWS 建议不要在标签中包含个人身份信息。
- 需要考虑的是，某些标签值需要设置为不可变（不可修改），以防止技术控制措施被规避，例如那些依赖于标签的 ABAC 条件。

安全 OU – 安全工具账户

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

Security Tooling 账户专门用于运营安全和隐私基础服务 AWS 账户、监控以及自动发送安全和隐私警报和响应。有关此账户的更多信息，请参阅AWS 安全参考架构 (AWS SRA)。下图说明了在 AWS 安全工具账户中配置的安全和隐私服务。



本部分提供有关此账户中以下内容的更多详细信息：

- AWS CloudTrail

- AWS Config
- Amazon GuardDuty
- IAM 访问分析器
- Amazon Macie

AWS CloudTrail

AWS CloudTrail可帮助您审核您的整体 API 活动 AWS 账户。启用 CloudTrail 所有 AWS 账户 存储、处理或传输个人数据可以帮助您跟踪这些数据的使用和披露情况。 AWS 区域 AWS Security Reference Architecture 建议启用组织跟踪，这是记录组织中所有账户的所有事件的单个跟踪。但是，启用此组织跟踪功能会将多个区域的日志数据聚合到“日志存档”账户中的一个 Amazon Simple Storage Service（Amazon S3）存储桶中。对于处理个人数据的账户，这可能会带来一些额外的设计注意事项。日志记录可能包含对个人数据的一些引用。为了满足您的数据驻留和数据传输要求，您可能需要重新考虑将跨区域日志数据聚合到 S3 存储桶所在的单个区域中。您的组织可能会考虑确定哪些区域的工作负载应被纳入或排除在组织跟踪之外。对于您决定排除在组织跟踪范围之外的工作负载，您可以考虑配置一个特定于区域的跟踪方案，以对个人数据进行屏蔽处理。有关屏蔽个人数据的更多信息，请参阅本指南的 Amazon Data Firehose 部分。最终，您的组织可能会同时拥有组织跟踪和区域跟踪，这些跟踪会汇总到集中的日志存档账户中。

有关配置单区域跟踪的更多信息，请参阅 AWS Command Line Interface （ AWS CLI ）或控制台的使用说明。创建组织跟踪时，可以在中使用选择加入设置 AWS Control Tower，也可以直接在CloudTrail 控制台中创建跟踪。

有关整体方法以及如何管理日志集中化和数据传输要求的更多信息，请参阅本指南中的 集中式日志存储 部分。根据 AWS SRA的说法，无论您选择哪种配置，您都可能希望将安全工具帐户中的跟踪管理与日志存档帐户中的日志存储分开。此设计有助于您为需要管理日志的人员以及需要使用日志数据的人员制定最低权限访问策略。

AWS Config

AWS Config 提供 AWS 账户 中资源及其配置方式的详细视图。它能帮助您确定各种资源之间的相互关系，以及它们的配置情况是如何随时间发生变化的。有关如何在安全情境中使用此服务的更多信息，请参阅 AWS 安全参考架构。

在中 AWS Config，您可以部署一致性包，这是一组 AWS Config 规则和补救措施。Conformance Packs 提供了一个通用框架，旨在使用托管或自定义规则来实现隐私、安全、运营和成本优化治理检查。 AWS Config 您可以将此工具用作更大的自动化工具集的一部分，以跟踪您的 AWS 资源配置是否符合您自己的控制框架要求。

NIST 隐私框架 v1.0 操作最佳实践一致性包与 NIST 隐私框架中的许多隐私相关控件保持一致。每 AWS Config 条规则都适用于特定的 AWS 资源类型，并且与一个或多个 NIST 隐私框架控件有关。您可以使用此一致性包来跟踪账户中各个资源的隐私相关持续合规性。以下是此一致性包中包含的一些规则：

- `no-unrestricted-route-to-igw`：此规则有助于防止数据在数据面板上的泄露，它会持续监控 VPC 路由表，查找默认的 `0.0.0.0/0` 或 `::/0` 出口路由至互联网网关的情况。这有助于您限制互联网流量的发送方向，特别是当存在已知为恶意的 CIDR 范围时。
- `encrypted-volumes`：此规则检查附加到 Amazon Elastic Compute Cloud（Amazon EC2）实例上的 Amazon Elastic Block Store（Amazon EBS）卷是否已加密。如果您的组织对使用 AWS Key Management Service (AWS KMS) 密钥保护个人数据有特定的控制要求，则可以在规则中指定特定密钥 IDs ，以检查卷是否使用特定 AWS KMS 密钥加密。
- `restricted-common-ports`：此规则检查 Amazon EC2 安全组是否允许对指定端口的无限制 TCP 流量访问。安全组可以对资源的入口和出口网络流量进行状态过滤，从而帮助您管理网络访问。 AWS 在您的资源上阻止从 `0.0.0.0/0` 到 TCP 3389 和 TCP 21 等常见端口的入口流量有助于限制远程访问。

AWS Config 可用于对您的 AWS 资源进行主动和被动合规性检查。除了考虑一致性包中的规则外，您还可以在检测和主动评估模式中将这些规则纳入考量范围。这有助于在软件开发周期的早期就实现隐私检查，因为应用程序开发者可以开始将预部署检查纳入其中。例如，他们可以在 AWS CloudFormation 模板中加入钩子，根据启用主动模式的所有隐私相关 AWS Config 规则检查模板中声明的资源。有关更多信息，请参阅AWS Config Rules No w Support 支持主动合规（AWS 博客文章）。

Amazon GuardDuty

AWS 提供多种可用于存储或处理个人数据的服务，例如亚马逊 S3、亚马逊关系数据库服务 (Amazon RDS) 或带有 Kubernetes 的 Amazon EC2。Amazon GuardDuty 将智能可视性与持续监控相结合，以检测可能与意外泄露个人数据相关的指标。有关如何在安全情境中使用此服务的更多信息，请参阅 AWS 安全参考架构。

借 GuardDuty助，您可以识别整个攻击生命周期中与隐私相关的潜在恶意活动。例如， GuardDuty 可以提醒您注意黑名单网站的连接、异常的网络端口流量或流量、DNS 泄露、EC2 实例意外启动以及异常的 ISP 呼叫者。您还可以配置 GuardDuty 为停止来自您自己的可信 IP 列表的可信 IP 地址的警报，并对自己的威胁列表中的已知恶意 IP 地址发出警报。

按照 AWS SRA 中的建议，您可以 GuardDuty 为组织 AWS 账户 中的所有人启用，并将安全工具帐户配置为 GuardDuty 授权管理员。 GuardDuty将整个组织的调查结果汇总到这个单一账户中。有关更多

信息，请参阅使用管理 GuardDuty 账户 AWS Organizations。您还可以考虑在事件响应流程中识别所有与隐私相关的利益相关者，涵盖从检测和分析到控制和根除的整个过程，并让这些人员参与到任何可能涉及数据泄露的事件中来。

IAM 访问分析器

许多客户都希望始终能得到这样的保证：个人数据仅会按照适当的方式与事先批准且预定的第三方处理程序共享，不会与其他任何实体共享。数据边界是一组预防性护栏，旨在仅允许来自预期网络的可信身份访问您的 AWS 环境中的可信资源。在为个人数据的意外泄露和预期泄露制定控制措施时，您可以定义可信身份、可信资源以及预期网络。

借助 AWS Identity and Access Management Access Analyzer （ IAM Access Analyzer ），组织可以定义信任 AWS 账户 区域并配置针对该信任区域的违规警报。IAM Access Analyzer 可分析 IAM 策略，以帮助识别和解决对潜在敏感资源的意外公开访问或跨账户访问。IAM Access Analyzer 使用数学逻辑和推理，为可以从 AWS 账户外部访问的资源生成详尽的调查发现。最后，为了响应和修复过于宽松的 IAM 策略，您可以使用 IAM Access Analyzer 根据 IAM 建议的做法验证现有策略并提供建议。IAM Access Analyzer 能够根据 IAM 主体之前的访问活动生成最低权限的 IAM 策略。它会分析 CloudTrail 日志并生成一个策略，该策略仅授予继续执行这些任务所需的权限。

有关如何在安全情境中使用 IAM Access Analyzer 的更多信息，请参阅 AWS 安全参考架构。

Amazon Macie

Amazon Macie 是一项服务，该服务使用机器学习和模式匹配来发现敏感数据，提供对数据安全风险的可见性，并帮助实现针对这些风险的自动防护。Macie 在检测到 Amazon S3 存储桶安全性或隐私性方面的潜在策略违规行为或问题时生成调查发现。Macie 是一款可供各组织使用的工具，它能够帮助实现自动化操作，从而助力合规工作。有关如何在安全情境中使用此服务的更多信息，请参阅 AWS 安全参考架构。

Macie 可以检测不断增长的大量敏感数据类型列表，包括个人身份信息（ PII ），例如姓名、地址和其他可识别属性。您甚至可以创建自定义数据标识符，以便设定符合您所在组织对个人数据定义的检测标准。

在您为包含个人数据的 Amazon S3 存储桶制定预防性控制措施时，您可以将 Macie 用作验证机制，以持续确保您的个人数据的存放位置以及其受到的保护程度。首先，启用 Macie 并配置自动化的敏感数据发现功能。Macie 会持续分析所有 S3 存储桶中的对象、账户和。 AWS 区域 Macie 生成并维护交互式热图，该图能够展示个人数据所在位置。自动化的敏感数据发现功能旨在降低成本，并最大限度降低手动配置发现作业的需求。您可以在此基础上利用自动化的敏感数据发现功能，并使用 Macie 来自动

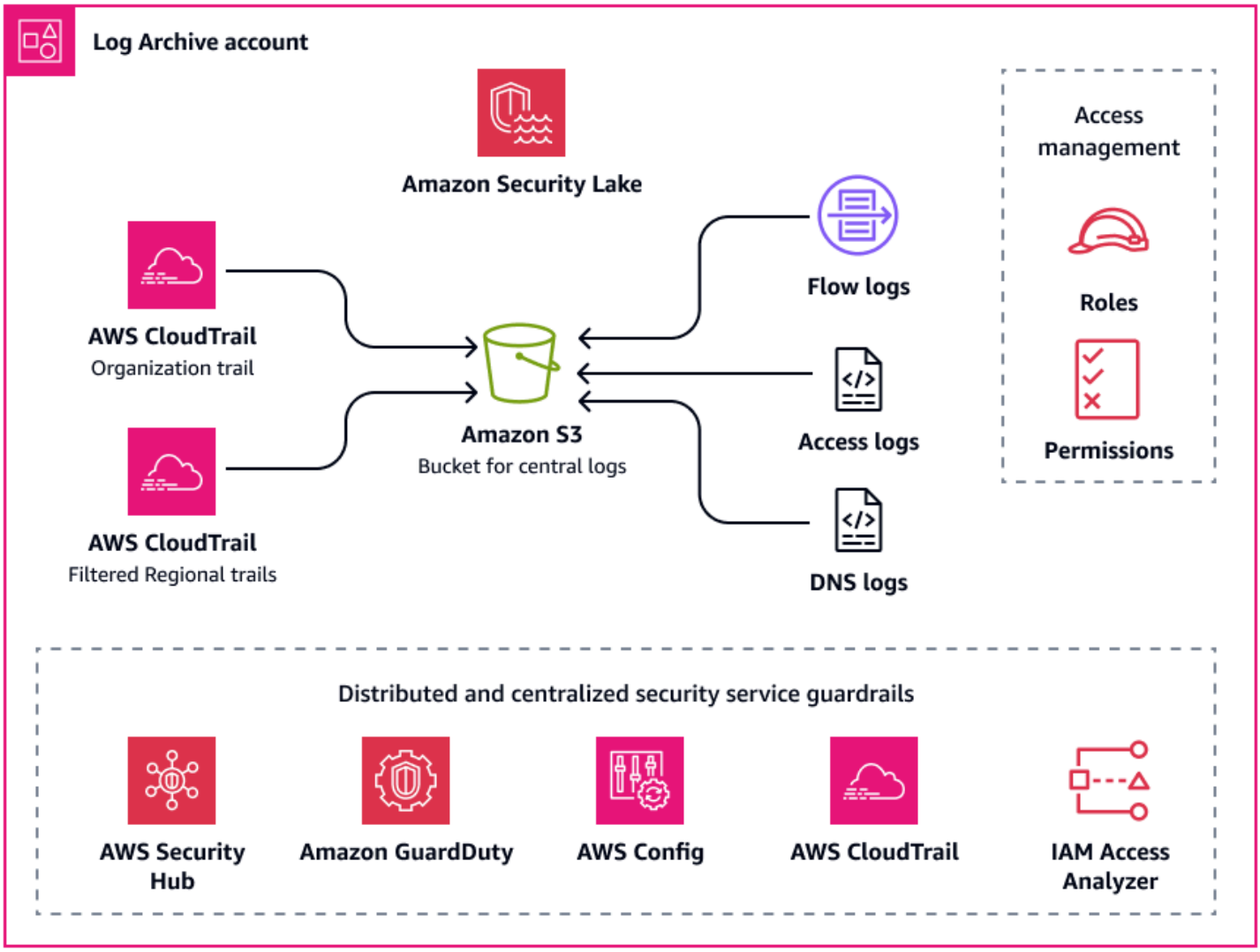
检测新的存储桶或现有存储桶中的新数据，然后根据指定的数据分类标签对这些数据进行验证。配置此架构，以便能够及时向相应的开发团队和隐私团队通报分类错误或未分类的存储桶。

您可以使用为组织中的每个帐户启用 Macie。 AWS Organizations有关更多信息，请参阅在 Amazon Macie 中集成和配置组织。

安全 OU – 日志存档账户

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

日志存档账户是您集中管理基础设施、服务和应用程序日志类型的地方。有关此账户的更多信息，请参阅AWS 安全参考架构 (AWS SRA)。通过专门的日志账户，您可以对所有日志类型实施一致的提醒设置，并确保事件响应人员能够从一个地方访问这些日志的汇总信息。您还可以在一个地方设置安全控制措施和数据保留策略，这能够简化隐私操作方面的繁琐流程。下图说明了在日志存档账户中配置的 AWS 安全和隐私服务。



集中式日志存储

日志文件（例如 AWS CloudTrail 日志）可能包含可视为个人数据的信息。一些组织选择使用组织跟踪将跨账户 AWS 区域 和跨账户的 CloudTrail 日志汇总到一个中心位置，以实现可见性。有关更多信息，请参阅本指南中的AWS CloudTrail。在实施日志集中化时， CloudTrail 日志通常存储在单个区域的亚马逊简单存储服务 (Amazon S3) 存储桶中。

根据您所在组织对个人数据的定义、与客户的合同义务以及适用的区域性隐私法规，当涉及到日志聚合时，您可能需要考虑跨境数据传输的问题。确定各种日志类型中的个人数据是否符合这些限制规定。例如， CloudTrail 日志可能包含贵组织的员工数据，但可能不包含客户的个人数据。如果您的组织需要遵守严格的数据传输要求，以下这些选项能够提供相应的支持：

- 如果您的组织 AWS 云 向多个国家/地区的数据主体提供服务，则可以选择汇总数据驻留要求最严格的国家/地区的所有日志。例如，如果您在德国运营并且德国有最严格的要求，则可以将数据聚合到

的 S3 存储桶`eu-central-1` AWS 区域 中，这样在德国收集的数据就不会离开德国边境。对于此选项，您可以在中配置单个组织跟踪 CloudTrail ，将来自所有账户的日志聚合 AWS 区域 到目标区域。

- 在将数据复制并汇总到其他区域 AWS 区域 之前，请先编辑需要保留的个人数据。例如，在将日志传输至其他区域之前，您可以在应用程序的主机区域对个人数据进行隐藏处理。有关屏蔽个人数据的更多信息，请参阅本指南的 Amazon Data Firehose 部分。
- 如果您有严格的数据主权问题，可以在中维护一个单独的多账户 landing zone AWS 区域 来强制执行这些要求。这样一来，您就可以简化区域中的登录区配置，从而实现集中式日志记录。它还提供了额外的基础设施分割优势，并有助于将日志保留在各自所在的区域内。与您的法律顾问合作，确定哪些个人数据在范围内，哪些允许 Region-to-Region传输。有关更多信息，请参阅本指南中的制定全球扩展战略。

默认情况下，通过服务日志、应用程序日志和操作系统 (OS) 日志，您可以使用 Amazon CloudWatch 监控 AWS 服务 相应账户和区域中的资源。许多用户会选择将来自多个账户和区域的日志及指标集中整合到一个账户中。默认情况下，这些日志会保留在相应的账户及其来源区域中。为了实现集中管理，您可以使用订阅筛选条件和 Amazon S3 导出任务将数据共享到一个集中的位置。在聚合具有跨境数据传输需求的工作负载的日志时，包含适当的筛选条件和导出任务可能很重要。如果某个工作负载的访问日志中包含个人数据，您可能需要确保这些数据会被传输到特定的账户和区域或存储在其中。

Amazon Security Lake

按照 AWS SRA 中的建议，您可能需要使用日志存档账户作为 Amazon Security Lake 的委托管理员账户。当您执行此操作时，Security Lake 会将受支持的日志收集到与 SRA 建议的安全日志相同的账户中的专用 Amazon S3 存储桶中。

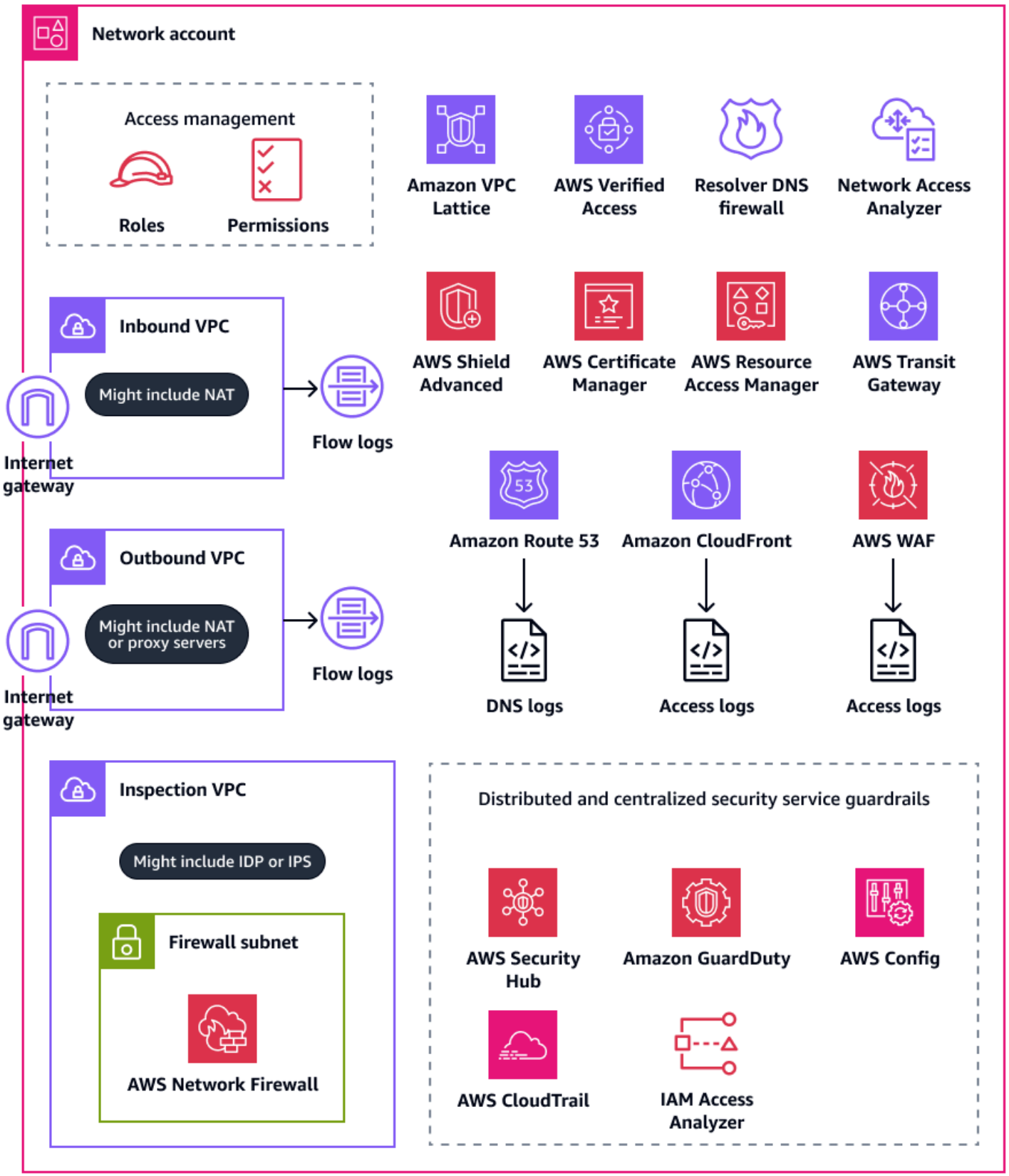
从隐私角度来看，您的事件响应者必须能够访问来自您的 AWS 环境、SaaS 提供商、本地、云源和第三方来源的日志。这有助于他们更迅速地阻止并修复对个人数据的未经授权访问问题。对于日志存储所涉及的那些注意因素，很可能同样适用于 Amazon Security Lake 内的日志驻留以及区域移动情况。这是因为 Security Lake 会从您启用该服务时收集安全日志和事件。 AWS 区域 要遵守数据驻留要求，请考虑您的汇总区域配置。汇总区域是 Security Lake 从您所选择的一个或多个贡献区域中整合数据所在的区域。在配置 Security Lake 和汇总区域之前，您的组织可能需要先统一关于数据驻留的区域合规要求。

基础设施 OU – 网络账户

调查

我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

在网络帐户中，您可以管理您的虚拟私有云 (VPCs) 和更广泛的互联网之间的网络。在此账户中，您可以通过使用来实施广泛的披露控制机制 AWS WAF，使用 AWS Resource Access Manager (AWS RAM) 共享 VPC 子网和 AWS Transit Gateway 附件，并使用 Amazon CloudFront 来支持有针对性的服务使用。有关此账户的更多信息，请参阅AWS 安全参考架构 (AWS SRA)。下图说明了在网络帐户中配置 AWS 的安全和隐私服务。



本部分提供有关此账户中使用的以下 AWS 服务 的更多详细信息：

- Amazon CloudFront
- AWS Resource Access Manager
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

Amazon CloudFront 支持前端应用程序和文件托管的地理限制。 CloudFront可以通过称为边缘位置的全球数据中心网络交付内容。当用户请求与你一起提供的内容时 CloudFront，该请求会被路由到延迟最低的边缘站点。有关如何在安全情境中使用此服务的更多信息，请参阅 AWS 安全参考架构。

您的隐私计划目前或许能够满足特定地区法律的要求。如果您的工作负载仅限于为仅位于这些区域的客户提供服务，那么您可以实施技术措施来阻止来自其他区域的使用请求。您可以使用 CloudFront 地理限制来阻止特定地理位置的用户访问您通过 CloudFront 发行版分发的内容。有关地理限制的更多信息和配置选项，请参阅 CloudFront文档中的限制内容的地理分布。

您还可以配置 CloudFront 为生成访问日志，其中包含有关 CloudFront 收到的每个用户请求的详细信息。有关更多信息，请参阅 CloudFront 文档中的配置和使用标准日志（访问日志）。最后，如果配置 CloudFront 为在一系列边缘位置缓存内容，则可以考虑缓存发生在哪里。对于某些组织而言，跨区域缓存可能会受到跨境数据传输要求的约束。

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) 可帮助您安全地共享资源， AWS 账户 从而减少运营开销并提供可见性和可审计性。使用 AWS RAM，组织可以限制哪些 AWS 资源可以与其组织 AWS 账户中的其他人或第三方账户共享。有关更多信息，请参阅可共享 AWS 资源。在网络账户中，您可以使用 AWS RAM 共享 VPC 子网和传输网关连接。如果您曾经与另一个人共享数据平面连接 AWS 账户，则可以考虑建立流程来检查连接是否经过预先批准 AWS 区域 并符合您的数据驻留要求。 AWS RAM

除了共享 VPCs 和传输网关连接外，还 AWS RAM 可用于共享不支持 IAM 基于资源的策略的资源。对于托管在个人数据 OU 中的工作负载，您可以使用 AWS RAM 访问位于单独的 OU 中的个人数据 AWS 账户。有关更多信息，请参阅个人数据 OU – PD 应用程序账户部分中的 AWS Resource Access Manager。

AWS Transit Gateway

如果您想部署符合组织数据驻留要求的收集、存储或处理个人数据的 AWS 资源 AWS 区域 ，并且您有适当的技术保障措施，请考虑实施防护措施，以防止控制平面和数据平面上未经批准的跨境数据流动。在控制面板，您可以利用 IAM 和服务控制策略来限制区域使用情况，并由此控制跨区域的数据流。

在数据面板上，有多个选项可以控制跨区域的数据流。例如，您可以使用路由表、VPC 对等和 AWS Transit Gateway 附件。 AWS Transit Gateway是连接虚拟私有云 (VPCs) 和本地网络的中央集线器。作为更大的 AWS 着陆区（Land VPC-to-VPC ing zone）的一部分，您可以考虑数据的各种传输方式 AWS 区域，包括通过互联网网关、通过直接对等以及通过区域间对等。 AWS Transit Gateway例如，您可以在 AWS Transit Gateway中执行以下操作：

- 确认您和本地环境之间的东西向 VPCs和南北连接符合您的隐私要求。
- 根据您的隐私要求配置 VPC 设置。
- 使用中的服务控制策略 AWS Organizations 和 IAM 策略来帮助防止修改您的配置 AWS Transit Gateway 和亚马逊虚拟私有云 (Amazon VPC) 配置。有关服务控制策略示例，请参阅本指南中的 限制对 VPC 配置的更改。

AWS WAF

为帮助防止个人数据意外泄露，您可以为 Web 应用程序部署一种 defense-in-depth方法。您可以在应用程序中内置输入验证和速率限制，但 AWS WAF 可以作为另一道防线。 AWS WAF是一种 Web 应用程序防火墙，可帮助您监控转发到受保护的 Web 应用程序资源的 HTTP 和 HTTPS 请求。有关如何在安全情境中使用此服务的更多信息，请参阅 AWS 安全参考架构。

使用 AWS WAF，您可以定义和部署检查特定标准的规则。以下这些活动可能会导致个人数据的非预期泄露：

- 来自未知或恶意 IP 地址或地理位置的流量
- 开放全球应用程序安全项目（OWASP）十大攻击类型，其中包括与泄露相关的攻击，例如 SQL 注入
- 请求速率高
- 一般机器人流量
- 内容抓取程序

您可以部署由管理的 AWS WAF 规则组 AWS。某些托管规则组 AWS WAF 可用于检测对隐私和个人数据的威胁，例如：

- SQL 数据库：此规则组包含旨在阻止与 SQL 数据库攻击（如 SQL 注入攻击）相关的请求模式的规则。如果应用程序与 SQL 数据库相连，请考虑此规则组。
- 已知错误输入：该规则组包含旨在用于阻止请求模式的规则，这些模式确认无效且与漏洞攻击或发现相关联。
- 机器人控制：此规则组包含一系列旨在管理来自机器人（这类机器人可能会消耗过多资源、影响业务指标、导致服务中断以及进行恶意活动）的请求的规则。
- 账户盗用防护（ATP）：此规则组包含旨在防止恶意账户盗用企图的规则。此规则组会检查发送至您是应用程序登录端点的登录尝试请求。

个人数据 OU – PD 应用程序账户

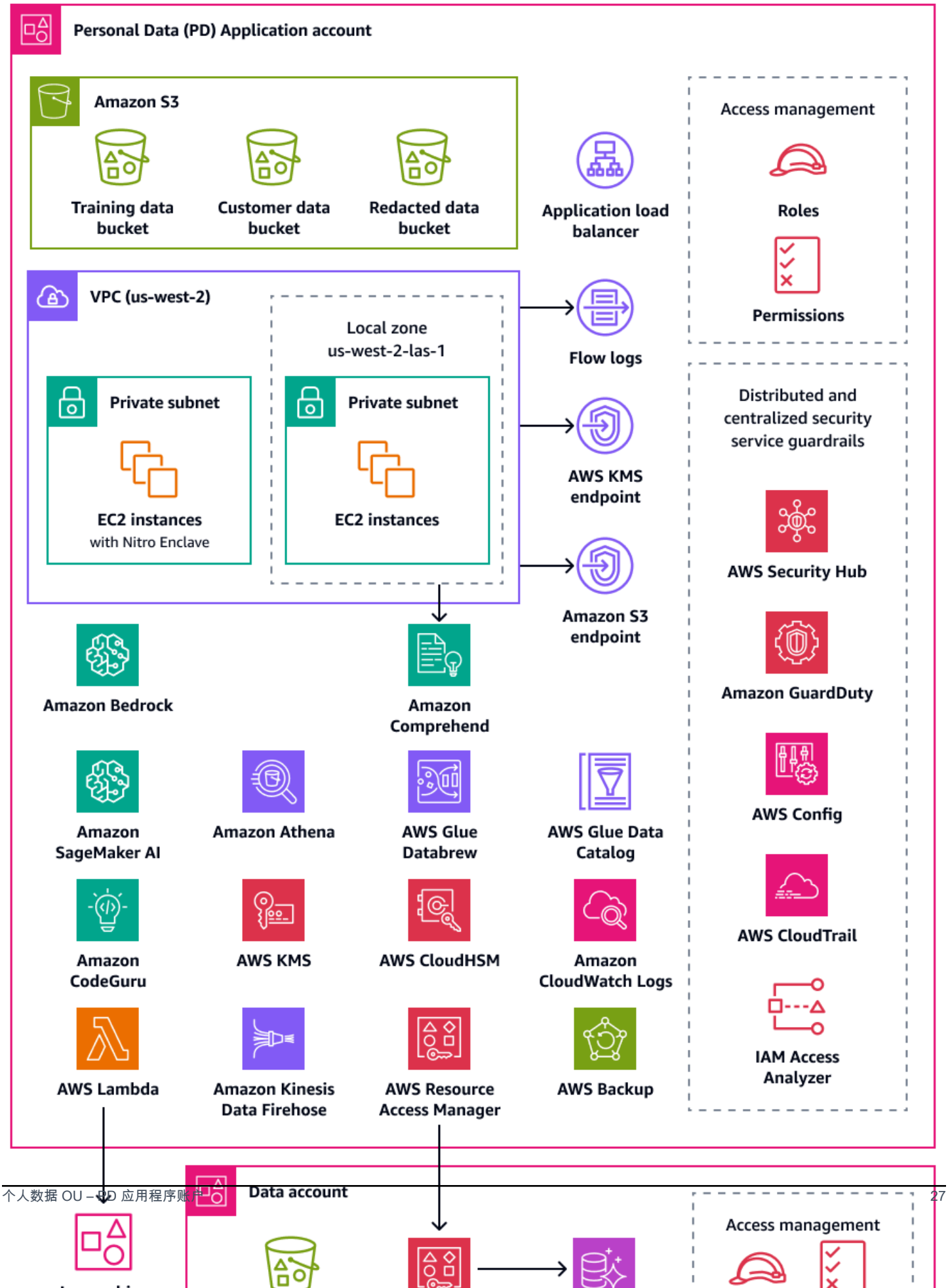
> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

个人数据（PD）应用程序账户是您的组织用于托管收集和处理个人数据的相关服务的平台。具体而言，您可以将您所定义的个人数据存储到此账户中。P AWS RA 通过多层无服务器 Web 架构演示了许多示例隐私配置。在跨 AWS 着陆区（Landing zone）操作工作负载时，不应将隐私配置视为 one-size-fits-all解决方案。例如，您的目标可能是要理解其背后的原理、这些原理如何增强隐私保护，以及您的组织如何针对特定的使用案例和架构应用解决方案。

对于 AWS 账户 在收集、存储或处理个人数据的组织中，您可以使用 AWS Organizations 和 AWS Control Tower 部署基础且可重复的护栏。为这些账户设立一个专门的组织单元（OU）至关重要。例如，您可能只想对部分账户应用数据驻留护栏，而这些账户的数据驻留正是其核心设计考虑因素。对于许多组织而言，这些账户负责存储和处理个人数据。

您的组织或许可以考虑设立一个专门的数据账户，这样您就可以在此存储个人数据集的权威来源信息了。权威数据来源是指您存储主要数据版本的地点，该版本通常被认为是数据中最可靠和最准确的版本。例如，您可以将数据从权威数据来源复制到其他位置，比如 PD 应用程序账户中用于存储训练数据、部分客户数据以及经过编辑的数据的 Amazon Simple Storage Service（Amazon S3）存储桶。通过采用这种多账户方式，将数据账户中完整且明确的个人数据与 PD 应用程序账户中下游使用者工作负载分离开来，这样在发生对您账户的未经授权访问时，就能减少受影响的范围。

下图说明了在 PD 应用程序和数据帐户中配置 AWS 的安全和隐私服务。


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Data account
Access management

本部分提供有关这些账户中使用的以下 AWS 服务 的更多详细信息：

- Amazon Athena
- Amazon Bedrock
- AWS Clean Rooms
- Amazon CloudWatch 日志
- Amazon CodeGuru Reviewer
- Amazon Comprehend
- Amazon Data Firehose
- Amazon DataZone
- AWS Glue
- AWS Key Management Service
- AWS Lake Formation
- AWS Local Zones
- AWS 硝基飞地
- AWS PrivateLink
- AWS Resource Access Manager
- 亚马逊 SageMaker AI
- AWS 有助于管理数据生命周期的功能
- AWS 服务 以及有助于细分数据的功能
- AWS 服务 以及有助于发现、分类或编目数据的功能

Amazon Athena

您可以考虑采用数据查询限制来实现您的隐私保护目标。Amazon Athena 是一种交互式查询服务，可帮助您使用标准 SQL 直接在 Amazon S3 中分析数据。您无需将数据加载到 Athena 中；它可以直接处理存储在 S3 存储桶中的数据。

Athena 的一个常见使用案例是为数据分析团队提供定制化且经过清洗的数据集。如果数据集包含个人数据，您可以对其中那些对数据分析团队价值不大的个人数据列进行遮蔽处理，从而对数据集进行清洗。有关更多信息，请参阅使用 A mazon AWS Lake Formation Athena AWS 对数据湖中的数据进行匿名化和管理（博客文章）。

如果您的数据转换方法需要超出 Athena 所支持函数之外的更多灵活性，您可以定义自定义函数，这些函数被称为用户定义函数（UDF）。你可以在提交给 Athena 的 SQL 查询 UDFs 中调用，然后它们就会继续运行。 AWS Lambda您可以 UDFs 在 in SELECT 和 quer FILTER SQL ies 中使用，也可以在同一个查询 UDFs 中调用多个查询。为了保护隐私，您可以创建 UDFs 执行特定类型的数据屏蔽的内容，例如仅显示列中每个值的最后四个字符。

Amazon Bedrock

Amazon Bedrock 是一项完全托管的服务，允许访问来自领先的人工智能公司（如 AI21 实验室、Anthropic、Meta、Mistral AI 和亚马逊）的基础模型。它可以帮助组织构建和扩展生成式人工智能应用程序。无论采用什么平台，在使用生成式人工智能时，组织都可能面临隐私风险，包括个人数据可能被泄露、未经授权的数据访问以及其他违反合规规定的情况。

Amazon Bedrock 护栏旨在通过在 Amazon Bedrock 的生成式人工智能工作负载中实施安全和合规的最佳实践，来帮助降低这些风险。人工智能资源的部署和使用可能并不总是符合一个组织的隐私和合规要求。在使用生成式人工智能模型时，组织可能会面临维护数据隐私方面的困难，因为这些模型有可能会记住或重现敏感信息。Amazon Bedrock 护栏通过评估用户输入和模型响应来帮助保护隐私。总体而言，如果输入数据包含个人数据，则模型的输出中就可能存在这些信息被泄露的风险。

Amazon Bedrock 护栏提供了相关机制，用于实施数据保护策略并帮助防止未经授权的数据泄露。它提供内容筛选功能，用于检测并阻止输入中的个人数据，设置主题限制以防止访问不适当或危险的内容，并使用词过滤功能来屏蔽或编辑模型提示和回复中的敏感词汇。这些功能有助于防止可能导致侵犯隐私的事件，比如出现带有偏见的响应，或者客户信任丧失。这些功能能够帮助您确保您的人工智能模型不会无意中处理或泄露个人数据。Amazon Bedrock Guardrails 还支持对 Amazon Bedrock 之外的输入和响应进行评估。有关更多信息，请参阅使用 Amazon Bedrock 护栏实施与模型无关的安全措施（AWS 博客文章）。

借助 Amazon Bedrock 护栏，您可以使用上下文一致性检查来评估事实依据和响应的相关性，从而限制模型产生幻觉的风险。例如，部署一个面向客户的生成式人工智能应用程序，该应用程序在检索增强生成（RAG）应用程序中使用了第三方数据来源。上下文一致性检查可用于将模型的响应与这些数据来源进行比对，并筛选出不准确的响应。在 AWS PRA 的背景下，您可以在工作负载账户中实施 Amazon Bedrock Guardrails，它会强制实施针对每个工作负载要求量身定制的特定隐私防护栏。

AWS Clean Rooms

随着各组织寻求通过分析相互交叉或重叠的敏感数据集来实现彼此间的协作，如何维护这些共享数据的安全性和隐私性便成为了问题。AWS Clean Rooms 能帮助您部署数据洁净室，这是一种安全且中立的环境，在这里，各组织可以对合并后的数据集进行分析，而无需共享原始数据本身。它还可以通过向其

他组织提供访问权限来生成独特的见解， AWS 而无需将数据从自己的帐户中移出或复制出来，也不会泄露底层数据集。所有数据都保留在源位置。内置分析规则会对输出进行限制，并对 SQL 查询进行约束。所有查询都会被记录下来，协作成员可以查看他们的数据是如何被查询的。

您可以创建 AWS Clean Rooms 协作并邀请其他 AWS 客户成为该协作的成员。您可以授予其中一位成员查询成员数据集的权限，并且您可以选择其他成员来接收这些查询的结果。如果有多名成员需要查询这些数据集，您可以使用相同的数据来源创建更多协作，并创建不同的成员设置。每位成员都可以筛选与协作成员共享的数据，并且您可以使用自定义分析规则来设置对他们提供给协作方的数据进行分析的限制条件。

除了限制向协作提供的数据以及其他成员如何使用这些数据外， AWS Clean Rooms 还提供了以下功能来帮助您保护隐私：

- 差别隐私是一种数学技术，通过在数据中加入适量精心调整的噪声来增强用户隐私保护。这有助于降低在数据集中对单个用户进行重新识别的风险，同时又不会掩盖相关值。使用 AWS Clean Rooms 差别隐私不需要差别隐私专业知识。
- AWS Clean Rooms 机器学习使双方或多方识别其数据中的相似用户，而无需彼此共享数据。这降低了成员身份推断攻击的风险，在这种攻击中，协作方的某位成员能够识别出另一方成员数据集中的个体信息。通过创建相似模型并生成相似区段， AWS Clean Rooms 机器学习可以帮助您在不暴露原始数据的情况下比较数据集。这并不要求任何一个成员都具备机器学习专业知识或在之外执行任何工作 AWS Clean Rooms。您保留对经过训练的模型的完全控制权和所有权。
- 洁净室密态计算（C3R）可与分析规则一起使用，以从敏感数据中得出见解。它通过加密技术对协作的任何一方所能获取的信息进行了限制。使用 C3R 加密客户端，数据在提供给之前在客户端进行加密。 AWS Clean Rooms由于数据表在上传至 Amazon S3 之前会使用客户端加密工具进行加密处理，所以数据一直处于加密状态，并在处理过程中得以持续保留。

在 AWS PRA 中，我们建议您在数据账户中创建 AWS Clean Rooms 协作。您可以用它们来与第三方共享加密后的客户数据。仅在所提供的数据集存在重叠的情况下，才使用它们。有关如何确定重叠的更多信息，请参阅 AWS Clean Rooms 文档中的列表分析规则。

Amazon CloudWatch 日志

Amazon CloudWatch Lo gs 可帮助您集中所有系统和应用程序的日志， AWS 服务 这样您就可以监控它们并安全地将其存档。在 CloudWatch 日志中，您可以对新的或现有的日志组使用数据保护策略，以帮助最大限度地降低个人数据泄露的风险。数据保护策略可以检测日志中的敏感数据，例如个人数据。数据保护策略能够在用户通过 AWS 管理控制台访问日志时对这些数据进行掩蔽处理。当用户需要直接访问个人数据时，根据您工作负载的整体目的说明，您可以为这些用户分配 `logs:Unmask` 权限。您

还可以创建一个适用于整个账户的数据保护策略，并在您所在组织的所有账户中一致地应用此策略。默认情况下，这将为日志中 CloudWatch 所有当前和将来的日志组配置屏蔽。我们还建议您启用审计报告功能，并将其发送至其他日志组、Amazon S3 存储桶或 Amazon Data Firehose。这些报告包含每个日志组中数据保护调查发现的详细记录。

Amazon CodeGuru Reviewer

出于隐私和安全方面的考虑，对于众多组织而言，确保在部署期间及部署后阶段都能持续保持合规性至关重要。 AWS PRA 在处理个人数据的应用程序的部署流程中包含了主动控制措施。Amazon CodeGuru Reviewer 可以检测可能泄露 Java 和 Python 代码中个人数据的潜在缺陷。 JavaScript它为开发人员提供了改进代码的建议。 CodeGuru 审阅者可以识别各种安全、隐私和一般推荐做法中的缺陷。它旨在与多个来源提供商合作 AWS CodeCommit，包括Bitbucket和Amazon S3。 GitHub CodeGuru Reviewer 可以检测到的一些与隐私相关的缺陷包括：

- SQL 注入
- 不安全的 Cookie
- 缺少授权
- 客户端重新 AWS KMS 加密

有关 CodeGuru Reviewer 可以检测到的内容的完整列表，请参阅 Amazon CodeGuru 探测器库。

Amazon Comprehend

Amazon Comprehend 是一项自然语言处理 （NLP） 服务，可通过机器学习发现英语文本文档中的有价值见解和关系。Amazon Comprehend 能够检测并编辑结构化、半结构化或非结构化的文本文档中的个人数据。有关更多信息，请参阅 Amazon Comprehend 文档中的个人身份信息（PII）。

由于 Amazon Comprehend 有许多应用程序 AWS SDKs集成选项，因此您可以使用 Amazon Comprehend 在收集、存储和处理数据的许多不同位置识别个人数据。您可以使用 Amazon Comprehend 机器学习功能来检测和编辑应用程序AWS 日志（博客文章）、客户电子邮件、支持票证等中的个人数据。PD 应用程序账户的架构图显示了如何在 Amazon EC2 上对应用程序日志执行此功能。Amazon Comprehend 提供两种编辑模式：

- `REPLACE_WITH_PII_ENTITY_TYPE` 将每个 PII 实体替换为其类型。例如，Jane Doe 将被替换为 NAME。
- `MASK` 将 PII 实体中的字符替换为您选择的字符（!、#、$、%、& 或 @）。例如，Jane Doe 可被替换为 **** ***。

Amazon Data Firehose

Amazon Data Firehose 可用于捕获、转换流数据并将其加载到下游服务，如适用于 Apache Flink 的亚马逊托管服务或 Amazon S3。Firehose 通常用于传输大量流数据，例如应用程序日志等，而无需从头开始构建处理管道。

您可以使用 Lambda 函数在数据向下游传输之前对其进行自定义或内置的处理。出于隐私保护的考虑，此功能支持数据最小化处理以及跨境数据传输要求。例如，您可以使用 Lambda 和 Firehose 转换多区域日志数据，然后再将其集中到日志存档账户中。有关更多信息，请参阅 Biogen：多账户集中式日志解决方案（YouTube 视频）。在 PD 应用程序账户中，您可以配置 Amazon CloudWatch 并将日志推送 AWS CloudTrail 到 Firehose 传输流。Lambda 函数对日志进行转换处理，并将它们发送到日志存档账户中的一个中央 S3 存储桶中。您可以将 Lambda 函数配置为屏蔽包含个人数据的特定字段。这有助于防止个人数据跨 AWS 区域传输。通过采用这种方法，个人数据在传输和集中管理之前就已经被进行了掩码处理，而非在之后才进行。对于不受跨境转账要求约束的司法管辖区的申请，通过组织跟踪汇总日志通常更具运营效率和成本效益。 CloudTrail有关更多信息，请参阅本指南的安全 OU – 安全工具账户部分中的 AWS CloudTrail。

Amazon DataZone

当组织通过 AWS 服务 诸如扩展其共享数据的方法时 AWS Lake Formation，他们希望确保差异访问由最熟悉数据的人控制：数据所有者。然而，这些数据所有者可能已经了解相关的隐私要求，比如用户同意或跨境数据传输方面的规定。Amazon DataZone 帮助数据所有者和数据治理团队根据您的数据治理政策在整个组织中共享和使用数据。在 Amazon 中 DataZone，业务LOBs部门 () 管理自己的数据，目录会跟踪这种所有权。相关各方可以查找并请求访问数据，作为其业务任务的一部分。只要数据所有者遵守数据发布者的制定政策，就可以直接对底层表格授予访问权限，而无需管理员干预或移动数据。

在隐私方面，Amazon DataZone 可以在以下示例用例中提供帮助：

- 面向客户的应用程序会生成使用数据，这些数据可以与独立的营销 LOB 共享。您需要确保仅将那些已选择接收营销信息的客户的数据发布到目录中。
- 欧洲客户数据已发布，但只能由欧洲经济区 (EEA) 的 LOBs当地人订阅。有关更多信息，请参阅在 Amazon 中通过精细的访问控制增强数据安全。 DataZone

在 AWS PRA 中，您可以将共享的 Amazon S3 存储桶中的数据 DataZone作为数据创建者连接到亚马逊。

AWS Glue

维护包含个人数据的数据集是隐私设计的关键组成部分。一个组织的数据可能以结构化、半结构化或非结构化的形式存在。无结构的个人数据可能会使执行一系列保护隐私的操作变得困难，例如数据最小化处理、根据数据主体的请求追踪属于单个数据主体的数据、确保数据的一致性质量以及对数据集的整体分段等。AWS Glue 是一项完全托管的提取、转换、加载（ETL）服务。它可以帮助您在数据存储和数据流之间对数据进行分类、清理、丰富和移动。 AWS Glue 功能旨在帮助您发现、准备、构造和合并用于分析、机器学习和应用程序开发的数据集。您可以使用 AWS Glue 在现有数据集之上创建可预测的通用结构。 AWS Glue Data Catalog AWS Glue DataBrew、和 AWS Glue 数据质量这些 AWS Glue 功能可以帮助支持贵组织的隐私要求。

AWS Glue Data Catalog

AWS Glue Data Catalog 可帮助您建立可维护的数据集。数据目录包含对用作中提取、转换和加载 (ETL) 作业的源和目标的数据的 AWS Glue引用。数据目录中的信息将存储为元数据表，且每个表指定单一数据存储。您可以运行 AWS Glue 爬网程序来对各种数据存储类型中的数据进行统计盘点。您可以在爬网程序中添加内置和自定义分类器，这些分类器会推断出个人数据的数据格式和架构。然后，爬网程序向数据目录写入元数据。集中式元数据表可以更轻松地响应数据主体请求（例如删除权），因为它可以增加环境中不同个人数据源的结构和可预测性。 AWS 有关如何使用数据目录自动响应这些请求的完整示例，请参阅使用 Amazon S3 Find and Forget 处理数据湖中的数据擦除请求（AWS 博客文章）。最后，如果您的组织使用 AWS Lake Formation 管理并对数据库、表、行和单元格进行精细的访问管理，数据目录是一个关键组成部分。Data Catalog 提供跨账户数据共享，并帮助您使用基于标签的访问控制来大规模管理数据湖（AWS 博客文章）。有关更多信息，请参阅此部分中的 AWS Lake Formation。

AWS Glue DataBrew

AWS Glue DataBrew 帮助您清理和规范化数据，并且能够对数据进行各种转换处理，例如移除或隐藏个人身份信息，以及对数据管道中的敏感数据字段进行加密。您还可以通过可视化的方式绘制出数据的沿袭，从而了解数据所经过的各类数据来源以及处理步骤。随着您的组织努力更好地了解和跟踪个人数据的来源，此功能变得越来越重要。 DataBrew 帮助您在数据准备期间屏蔽个人数据。在数据剖析作业中，您可以检测出个人数据，并收集相关统计信息，例如可能包含个人数据的列的数量以及潜在的类别等。然后，您可以使用内置的可逆或不可逆的数据转换技术，包括替代、哈希、加密和解密等操作，一切都无需编写任何代码。然后，您可以将清理并处理过的数据集用于后续的分析、报告和机器学习任务。中可用的一些数据屏蔽技术 DataBrew包括：

- 哈希：对列值应用哈希函数。
- 替代：将个人数据替换为其他看起来真实的值。

- 清空或删除：将特定字段替换为空值，或删除该列。
- 屏蔽：将字符置乱或屏蔽列中的某些部分。

以下是可用的加密技术：

- 确定性加密：对列值应用确定性加密算法。确定性加密始终为值生成相同的加密文字。
- 概率加密：对列值应用概率加密算法。每次应用概率加密时都会生成不同的加密文字。

有关中提供的个人数据转换方法的完整列表 DataBrew，请参阅个人身份信息 (PII) 配方步骤。

AWS Glue 数据质量

AWS Glue Data Q uality 可帮助您在将高质量数据交付给数据使用者之前，主动实现跨数据管道的交付并实现其可操作化。 AWS Glue Data Quality 可对您的数据管道中的数据质量问题进行统计分析，可以在 Amazon 中触发警报 EventBridge，并可以提出质量规则建议以进行补救。 AWS Glue Data Quality 还支持使用特定于域的语言创建规则，因此您可以创建自定义的数据质量规则。

AWS Key Management Service

AWS Key Management Service (AWS KMS) 帮助您创建和控制加密密钥以帮助保护您的数据。 AWS KMS 使用硬件安全模块在 FIPS 140-2 加密模块验证计划 AWS KMS keys 下进行保护和验证。有关如何在安全情境中使用此服务的更多信息，请参阅 AWS 安全参考架构。

AWS KMS 与大多数提供加密功能 AWS 服务 的软件集成，您可以在处理和存储个人数据的应用程序中使用 KMS 密钥。您可以使用 AWS KMS 来帮助支持您的各种隐私要求并保护个人数据，包括：

- 使用客户自主管理型密钥更好地控制强度、轮换、到期时间和其他选项。
- 使用专用的客户自主管理型密钥来保护个人数据和允许访问个人数据的机密密钥。
- 定义数据分类级别，并为每个级别指定至少一个专用的客户自主管理型密钥。例如，您可能会使用一个密钥来加密操作数据，而使用另一个密钥来加密个人数据。
- 防止意外的跨账户访问 KMS 密钥。
- 将 KMS 密钥存储在 AWS 账户 与要加密的资源相同的位置。
- 对 KMS 密钥管理和使用实行职责分离。有关更多信息，请参阅如何使用 KMS 和 IAM 为 S3 中的加密数据启用独立的安全控制（AWS 博客文章）。
- 通过预防性和应对性护栏来强制实施密钥自动轮换。

默认情况下，KMS 密钥会进行存储，并且只能在创建该密钥的区域内使用。如果您的组织对数据驻留和主权有特定要求，则考虑一下多区域 KMS 密钥是否适用于您的使用案例。多区域密钥是不同用途的 KMS 密钥 AWS 区域 ，可以互换使用。创建多区域密钥的过程会将您的密钥材料跨越 AWS 区域 国界 AWS KMS，因此这种缺乏区域孤立可能与您组织的主权和居住目标不相容。解决此问题的一种方法是使用不同类型的 KMS 密钥，例如区域特定的客户自主管理型密钥。

外部密钥存储

对于许多组织来说，中的默认 AWS KMS 密钥存储 AWS 云 可以满足其数据主权和一般监管要求。但有一些情况可能要求加密密钥须在云环境之外生成和维护，并且您需要有独立的授权和审计路径。通过存储外部密钥 AWS KMS，您可以使用您的组织在外部拥有和控制的密钥材料对个人数据进行加密 AWS 云。您仍然像往常一样与 AWS KMS API 交互，但只能与您提供的外部密钥存储代理（XKS 代理）软件进行 AWS KMS 交互。然后，您的外部密钥存储代理会调解与您的外部密钥管理器 AWS KMS 之间的所有通信。

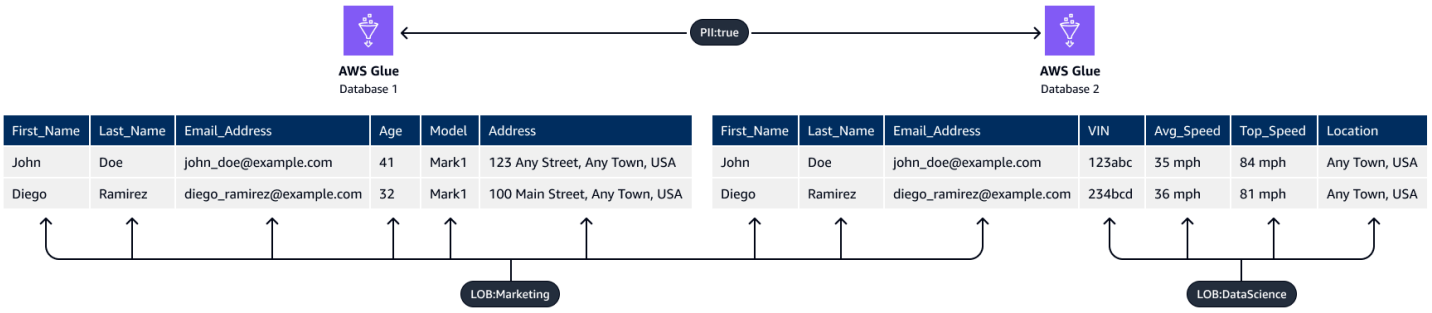
使用外部密钥存储进行数据加密时，重要的是，您需要考虑与在 AWS KMS中维护密钥相比，所增加的运营成本。对于外部密钥存储，您必须创建、配置和维护外部密钥存储。此外，如果新增的基础设施（如 XKS 代理）存在故障，并且网络连接中断，则用户可能会暂时无法解密并访问数据。与您的合规性及监管利益相关者密切合作，以了解有关个人数据加密的法律和合同义务，以及关于可用性和韧性的服务级别协议。

AWS Lake Formation

许多通过结构化元数据目录对其数据集进行编目和分类的组织，都希望在全组织范围内共享这些数据集。您可以使用 AWS Identity and Access Management (IAM) 权限策略来控制对整个数据集的访问权限，但是对于包含不同敏感度的个人数据的数据集，通常需要更精细的控制。例如，目的规范和使用限制（FPC 网站）可能会表明，营销团队需要获取客户地址信息，而数据科学团队则不需要。

此外，数据湖还存在隐私方面的挑战，因为它们会将大量敏感数据以原始格式集中起来供访问。一个组织的大部分数据都可以集中在一个地方进行访问，因此对数据集（尤其是包含个人数据的数据集）进行逻辑分隔就显得尤为重要。AWS Lake Formation 能够帮助您在共享数据（无论是来自单一来源还是数据湖中包含的多个来源）时设置治理和监控措施。在 AWS PRA 中，您可以使用 Lake Formation 对数据账户中共享数据存储桶中的数据进行精细的访问控制。

您可以在 Lake Formation 中使用基于标签的访问控制功能。基于标签的访问控制是一种授权策略，它根据属性来定义权限。在 Lake Formation 中，这些属性被称为 LF 标签。通过使用 LF 标签，您可以将这些标签附加到数据目录数据库、表和列上，并将相同的标签授予 IAM 主体。当主体已获授权，可以访问与资源标签值匹配的标签值时，Lake Formation 允许对这些资源执行操作。下图展示了如何为个人数据分配 LF 标签和权限，以实现差异化的访问控制。



此示例使用标签的层级结构特性。两个数据库都包含个人身份信息（`PII:true`），但是列级标签则将特定列限制给不同的团队。在此示例中，拥有 `PII:true` LF-Tag 的 IAM 委托人可以访问带有此标签的 AWS Glue 数据库资源。带有 `LOB:DataScience` LF 标签的主体可以访问带有此标签的特定列，而带有 `LOB:Marketing` LF 标签的主体只能访问带有此标签的列。市场营销部门只能访问与营销使用案例相关的 PII，而数据科学团队也只能访问与他们的使用案例相关的 PII。

AWS Local Zones

如果您需要遵守数据驻留要求，则可以部署专门存储和处理个人数据的资源 AWS 区域 来支持这些要求。您还可以使用 AWS Local Zones，它可以帮助您将计算、存储、数据库和其他精选 AWS 资源放在靠近人口众多和行业中心的地方。本地扩展区是指与大型都市区地理上相邻的一个 AWS 区域 的扩展部分。您可以将特定类型的资源放置在本地区域内，该区域靠近与之相对应的区域位置。当某个区域在同一法律管辖区内不可用时，本地区域可以帮助您满足数据驻留要求。使用本地区域时，请考虑在组织内部署的数据驻留控制措施。例如，您可能需要一项控制措施来防止数据从特定的本地区域传输到另一个区域。有关 SCPs 如何使用维护跨境数据传输护栏的更多信息，请参阅使用 AWS Local Zones landing zone 控制管理数据驻留的最佳实践（AWS 博客文章）。

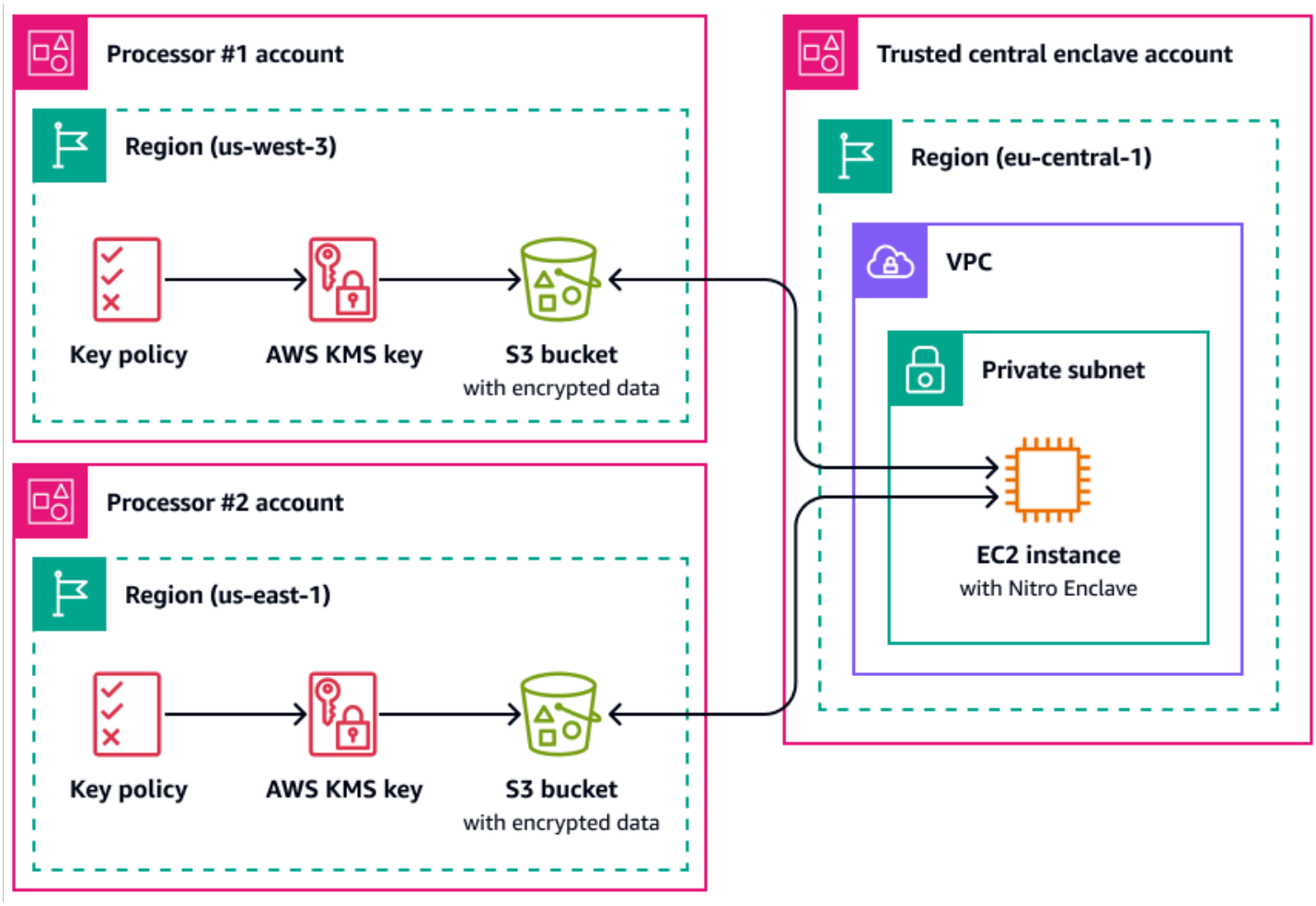
AWS 硝基飞地

从处理角度考虑您的数据分段策略，例如使用 Amazon Elastic Compute Cloud（Amazon EC2）等计算服务处理个人数据。作为更大架构策略的一部分，机密计算能够帮助您将个人数据处理工作置于一个独立、受保护且可信的 CPU enclave 中进行。Enclaves 是独立的、经过强化的、高度受限的虚拟机。AWS Nitro Enclaves 是 Amazon EC2 的一项功能，它能够帮助您创建这些独立的计算环境。有关更多信息，请参阅 AWS Nitro 系统的安全设计（AWS 白皮书）。

Nitro Enclaves 会部署一个与父实例内核相分离的内核。父实例的内核无权访问 enclave。用户无法通过 SSH 或远程方式访问 enclave 中的数据和应用程序。处理个人数据的应用程序可以嵌入到 enclave 中，并可配置为使用该 enclave 的 Vsock（即用于实现 enclave 与父实例之间通信的套接字）。

Nitro Enclaves 可以发挥作用的一个用例是两个数据处理器之间的联合处理，这两个数据处理器彼此分开 AWS 区域 ，可能彼此不信任。下图展示了如何利用 enclave 进行中央处理、如何使用 KMS 密钥对

发送至 enclave 之前的数据进行加密，以及如何使用 AWS KMS key 策略来验证请求解密的 enclave 在其证明文档中具有唯一的测量值。有关更多信息和说明，请参阅使用加密认证。 AWS KMS有关密钥策略示例，请参阅本指南中的 需要认证才能使用密钥 AWS KMS。



通过这种实施方式，只有相应的数据处理者以及底层的 enclave 才能访问明文个人数据。在相应数据处理者的环境之外，唯一暴露数据的位置是 enclave 本身，该 enclave 旨在防止访问和篡改。

AWS PrivateLink

许多组织都希望限制个人数据向不可信网络的泄露。例如，如果您想增强整体应用程序架构设计的隐私性，则可以根据数据敏感度对网络进行细分（类似于本AWS 服务 以及有助于细分数据的功能节中讨论的数据集的逻辑和物理分离）。 AWS PrivateLink帮助您创建从您的虚拟私有云 (VPCs) 到 VPC 外部服务的单向私有连接。使用 AWS PrivateLink，您可以为存储或处理您环境中个人数据的服务建立专用的私有连接；无需连接到公共端点，并通过不可信的公共网络传输此数据。当您为范围内的 AWS PrivateLink 服务启用服务终端节点时，无需互联网网关、NAT 设备、公有 IP 地址、 AWS Direct Connect 连接或 AWS Site-to-Site VPN 连接即可进行通信。当您使用 AWS PrivateLink 连接到提供个人数据访问权限的服务时，您可以根据组织的数据边界定义使用 VPC 终端节点策略和安全组来控制访

问权限。有关仅允许可信组织中的 IAM 原则和 AWS 资源访问服务终端节点的 VPC 终端节点策略示例，请参阅本指南访问 VPC 资源需要组织成员身份中的。

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) 可帮助您安全地共享资源， AWS 账户 从而减少运营开销并提供可见性和可审计性。在规划多账户细分策略时，可以考虑使用 AWS RAM 来共享存储在单独的隔离账户中的个人数据存储。您可以与其他受信任的账户共享这些个人数据以进行处理。在中 AWS RAM，您可以管理权限，这些权限定义可以对共享资源执行哪些操作。对的所有 API 调用 AWS RAM 均已登录 CloudTrail。此外，您还可以将 Amazon CloudWatch Events 配置为在中的 AWS RAM特定事件（例如资源共享发生更改时）自动通知您。

尽管您可以 AWS 账户 通过在 IAM 中使用基于 AWS 资源的策略或 Amazon S3 中的存储桶策略与其他人共享多种类型的资源，但这为隐私 AWS RAM 提供了一些额外的好处。 AWS 让数据所有者更清楚地了解在您之间共享数据的方式和与谁共享 AWS 账户，包括：

- 能够与整个 OU 共享资源，而不必手动更新账户列表 IDs
- 如果使用者账户不属于您的组织，则强制执行共享发起的邀请流程
- 了解哪些特定 IAM 主体有权访问每个单独的资源

如果您之前曾使用基于资源的策略来管理资源共享，但想 AWS RAM 改用，请使用 PromoteResourceShareCreatedFromPolicyAPI 操作。

亚马逊 SageMaker AI

Amazon SageMaker AI 是一项托管机器学习 (ML) 服务，可帮助您构建和训练机器学习模型，然后将其部署到生产就绪的托管环境中。 SageMaker AI 旨在让准备训练数据和创建模型特征变得更加容易。

Amazon SageMaker 模型监视器

许多组织在训练机器学习模型时会考虑数据漂移。数据漂移指的是生产数据与用来训练机器学习模型的数据之间的有意义差异，或者输入数据随时间推移的有意义变化。数据漂移可能降低机器学习模型预测的整体质量、准确性和公平性。如果 ML 模型在生产过程中接收到的数据的统计性质偏离了训练所依据的基准数据的性质，则预测的准确性可能会降低。Amazon SageMaker Model M onitor 可以持续监控生产中亚马逊 SageMaker AI 机器学习模型的质量并监控数据质量。尽早并主动地检测数据漂移，能够帮助您采取相应的纠正措施，比如重新训练模型、审计上游系统或者修复数据质量问题。Model Monitor 可以缓解手动监控模型或构建其他工具的需求。

亚马逊 SageMaker 澄清

Amaz SageMaker on Clarify 提供了对模型偏差和可解释性的见解。 SageMakerClarify 通常用于机器学习模型数据准备和整体开发阶段。开发人员可以指定感兴趣的属性，例如性别或年龄，Clarify 会运行一组算法来检测这些属性中是否存在偏差。 SageMaker 算法运行后，Cl SageMaker arify 会提供一份可视化报告，其中描述了可能的偏差的来源和测量结果，以便您可以确定纠正偏差的步骤。例如，在仅包含向一个年龄组与其他年龄组相比向一个年龄组提供商业贷款的几个示例的财务数据集中，SageMaker 可以标示失衡，这样您就可以避免使用不利于该年龄组的模型。您还可以通过查看已训练模型的预测，并持续监控这些 ML 模型是否存在偏差来检查其是否存在偏差。最后，Cl SageMaker arify 与 Amazon SageMaker AI Experiments 集成，提供了一个图表，解释了哪些功能对模型的整体预测过程贡献最大。此信息有助于实现可解释性结果，并且能够帮助您确定某个特定的模型输入是否对整体模型行为产生了超出其应有的影响。

亚马逊 SageMaker 模型卡

Amazon SageMaker 模型卡可以帮助您记录机器学习模型的关键细节，以用于管理和报告目的。这些详细信息可以包括模型所有者、一般用途、预期使用案例、所做的假设、模型的风险评级、训练详细信息和指标以及评估结果。有关更多信息，请参阅利用 AWS 人工智能和 Machine Learning 解决方案实现模型可解释性（AWS 白皮书）。

Amazon SageMaker Data Wrangler

Amazon SageMaker Data Wrangler 是一款机器学习工具，可帮助简化数据准备和功能工程流程。它提供了一个直观界面，有助于数据科学家和机器学习工程师快速、轻松地准备和转换数据，以便将其用于机器学习模型中。使用 Data Wrangler，您可以从各种来源导入数据，例如 Amazon S3、Amazon Redshift 和 Amazon Athena。然后，您可以使用 300 多种内置数据转换功能来对数据进行清理、标准化和组合处理，而无需编写任何代码。

Data Wrangler 可用作 PRA 中数据准备和特征工程过程的一部分。 AWS 它支持通过使用进行静态和传输中的数据加密 AWS KMS，并使用 IAM 角色和策略来控制对数据和资源的访问权限。它支持通过 AWS Glue 或 Amazon F SageMaker eature Stor e 进行数据屏蔽。如果您将 Data Wrangler 与集成 AWS Lake Formation，则可以强制执行精细的数据访问控制和权限。您甚至可以将 Data Wrangler 与 Amazon Comprehend 结合使用，通过其功能自动从表格数据中编辑个人数据，将其纳入您更广泛的机器学习运营工作流之中。有关更多信息，请参阅使用 Amazon D SageMaker ata Wrangler 自动编辑用于机器学习的 PII（AWS 博客文章）。

Data Wrangler 的多功能性使您能够为众多行业掩蔽敏感数据（如账户号码、信用卡号码、社会安全号码、患者姓名以及医疗和军事记录等）。您可以限制对任何敏感数据的访问权限或选择对其进行编辑。

AWS 有助于管理数据生命周期的功能

当不再需要个人数据时，您可以对许多不同数据存储中的数据使用生命周期和 time-to-live策略。配置数据留存策略时，请考虑以下可能包含个人数据的位置：

- 数据库，如 Amazon DynamoDB 和 Amazon Relational Database Service（Amazon RDS）
- Amazon S3 存储桶
- 来自 CloudWatch 和的日志 CloudTrail
- 缓存来自 AWS Database Migration Service (AWS DMS) 和 AWS Glue DataBrew 项目中迁移的数据
- 备份和快照

以下内容 AWS 服务 和功能可以帮助您在 AWS 环境中配置数据保留策略：

- Amazon S3 生命周期：一组规则，用于定义 Amazon S3 对一组对象应用的操作。在 Amazon S3 生命周期配置中，您可以创建过期操作，这些操作会定义 Amazon S3 代表您删除过期对象的时间。有关更多信息，请参阅管理存储生命周期。
- Amazon Data Lifecycle Manager — 在亚马逊 EC2 中，创建一个自动创建、保留和删除亚马逊弹性区块存储 (Amazon EBS) 快照和 EBS 支持的亚马逊机器映像 () 的策略 ()。AMIs
- 动态生存时间（TTL）：定义每个项目的时间戳，该时间戳用于确定某个项目不再被需要的时间点。在指定时间戳的日期和时间之后，DynamoDB 会立即从表中删除相应项目。
- 日志中的 CloudWatch 日志保留设置-您可以将每个日志组的保留策略调整为 1 天到 10 年之间的值。
- AWS Backup— 集中部署数据保护策略，以配置、管理和控制各种 AWS 资源的备份活动，包括 S3 存储桶、RDS 数据库实例、DynamoDB 表、EBS 卷等。通过指定资源类型将备份策略应用于您的 AWS 资源，或者根据现有资源标签进行应用，从而提供更高的精度。通过一个集中式控制台对备份活动进行审计并生成报告，以帮助满足备份合规要求。

AWS 服务 以及有助于细分数据的功能

数据分段是将数据存储在单独的容器中的过程。这能够帮助您为每个数据集制定差异化的安全和认证措施，并降低整个数据集因暴露而产生的影响范围。例如，不必将所有客户数据都存储在一个大型数据库中，而是可以将这些数据分段成更小、更易于管理的子组。

您可以使用物理和逻辑分离来对个人数据进行分段：

- 物理分离：将数据存储在单独的数据存储中或将数据分布到单独的 AWS 资源中的行为。尽管数据在物理上是分离的，但这两类资源仍可能被相同的主体所访问。这就是我们建议将物理分离与逻辑分离结合的原因。
- 逻辑分离：使用访问控制来隔离数据的行为。不同的工作职能需要不同程度的访问个人数据子集的权限。有关实施逻辑分离的示例策略，请参阅本指南中的 授予对特定 Amazon DynamoDB 属性的访问权限。

将逻辑分离与物理分离相结合，能够为编写基于身份和基于资源的策略提供灵活性、简便性和精细度，从而支持不同工作职能之间的差异化访问控制。例如，要在单个 S3 存储桶中创建能够逻辑上区分不同数据分类的策略，其操作过程可能会相当复杂。为每种数据分类使用专用的 S3 存储桶可简化策略配置和管理。

AWS 服务 以及有助于发现、分类或编目数据的功能

一些组织尚未开始在其环境中使用提取、加载、转换（ELT）工具来主动编目数据。这些客户可能正处于早期的数据发现阶段，他们希望更好地了解他们存储和处理的数据 AWS 以及数据的结构和分类方式。您可以使用 Amazon Macie 来更好地了解您在 Amazon S3 中的 PII 数据。但是，Amazon Macie 无法帮助您分析其他数据来源，例如 Amazon Relational Database Service（Amazon RDS）和 Amazon Redshift。在更大的数据映射练习开始时，您可以使用两种方法来加快初始发现：

- 手动方法：制作一个包含两列的表格，其行数根据需要而定。在第一列中，填写一些数据特征信息（例如用户名、地址或性别），这些信息可能出现在网络数据包的标头或主体部分，或者您所提供的任何服务中。请您的合规团队填写第二列。在第二列中，如果数据被视为个人数据，则输入“是”；如果不是，则输入“否”。请注明任何被认为特别敏感的个人数据，例如宗教信仰或健康状况方面的信息。
- 自动化方法：使用通过 AWS Marketplace提供的工具。Securiti 就是这样一个工具。这些解决方案提供了相应的集成功能，使其能够扫描并发现多种 AWS 资源类型中的数据，以及其他云服务平台中的资产。这些解决方案中有许多能够持续收集并维护数据资产及数据处理活动的清单，并将其存放在一个集中式的数据目录中。如果您依靠某种工具来进行自动化分类，那么可能需要对发现和分类规则进行调整，以使其符合您所在组织对个人数据的定义。

隐私相关策略示例

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

许多处理敏感数据的组织都采用预防性方法，在整个过程中实施多层检测和响应式控制。本节提供了 AWS Identity and Access Management (IAM)、 AWS Organizations和 AWS Key Management Service () 的隐私相关政策的示例。AWS KMS这些策略采用预防性方法，可帮助您的组织实现各种使用、披露限制和跨境数据传输的隐私目标。本指南的前几节中引用了其中许多策略。

本节包含以下示例策略：

- 要求从特定 IP 地址访问
- 访问 VPC 资源需要组织成员身份
- 限制跨数据传输 AWS 区域
- 授予对特定 Amazon DynamoDB 属性的访问权限
- 限制对 VPC 配置的更改
- 需要认证才能使用密钥 AWS KMS

要求从特定 IP 地址访问

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

仅当呼叫来自范围 `192.0.2.0/24` 或 `203.0.113.0/24` 内的 IP 地址时，此策略才允许 `john_stiles` 用户担任 IAM 角色。此策略可帮助防止个人数据意外披露和不必要的跨境数据传输。例如，如果您的组织中有需要访问个人数据的客户支持人员，则您可能希望该支持人员仅从位于特定子集的办公室访问这些数据 AWS 区域。此外，请核实组织对 PII 的定义，因为某些策略可能要求 `Condition` 或 `Principal` 部分限制对特定用户或 IP 地址的访问。

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

访问 VPC 资源需要组织成员身份

调查

我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

此 VPC 终端节点策略仅 AWS Identity and Access Management 允许o-1abcde123组织中的委托人和资源访问 Amazon Personalize (Amazon S3) 终端节点。这种预防性控制有助于建立信任区并定义个人数据边界。有关本策略如何帮助保护组织中的隐私和个人数据的更多信息，请参阅本指南中的 AWS PrivateLink。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

限制跨数据传输 AWS 区域

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

除两个 AWS Identity and Access Management (IAM) 角色外，此服务控制策略拒绝`eu-west-1`和以 AWS 区域 外的区域 AWS 服务的 API 调用`eu-central-1`。此 SCP 可以帮助防止在未经批准的地区创建 AWS 存储和处理服务。这可以帮助防止这些 AWS 服务 地区完全处理个人数据。此策略之所以使用`NotAction`参数 AWS 服务，是因为它考虑全球服务（例如 IAM）和与全球服务集成的服务 AWS Key Management Service （例如 (AWS KMS) 和 Amazon） CloudFront。您可以在参数值中将这些全球服务和其他不适用的服务指定为例外。有关本策略如何帮助保护组织中的隐私和个人数据的更多信息，请参阅本指南中的 AWS Organizations。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
```

```
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
```

```
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

授予对特定 Amazon DynamoDB 属性的访问权限

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

当您的组织讨论在物理和逻辑上分离个人数据的策略时，请考虑哪些 AWS 存储服务支持 AWS Identity and Access Management (IAM) 中的细粒度访问控制策略。以下基于身份的策略仅允许从名为 `Users` 的 Amazon DynamoDB 表中检索 `UserID`、`SignUpTime` 和 `LastLoggedIn` 属性。例如，您可以将此策略附加到客户支持角色，而不是授予该角色完整个人数据集的访问权限。有关本策略如何帮助保护组织中的隐私和个人数据的更多信息，请参阅本指南中的 AWS 服务 以及有助于细分数据的功能。

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
```

```
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
                  "SignUpTime",
                  "LastLoggedIn"
               ]
            },
            "StringEquals":{
               "dynamodb:Select":[
                  "SPECIFIC_ATTRIBUTES"
               ]
            }
         }
      }
   ]
}
```

限制对 VPC 配置的更改

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

在设计并部署了支持跨境数据传输要求（包括网络数据流）AWS 的基础架构之后，您可能需要防止修改。以下服务控制策略有助于防止 VPC 配置漂移或意外修改。该策略拒绝新的互联网网关连接、VPC 对等连接、中转网关连接以及新的 VPN 连接。有关本策略如何帮助保护组织中的隐私和个人数据的更多信息，请参阅本指南中的 AWS Transit Gateway。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
```

```
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

需要认证才能使用密钥 AWS KMS

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

以下 AWS Key Management Service (AWS KMS) 密钥策略允许 AWS Nitro Enclave 实例仅在请求中安全区的认证文档与条件语句中的测量值相匹配时使用 KMS 密钥。本策略仅允许受信任的 Enclave 解密数据。有关本策略如何帮助保护组织中的隐私和个人数据的更多信息，请参阅本指南中的 AWS 硝基飞地。有关可在密钥策略和 AWS Identity and Access Management (IAM) 策略中使用的 AWS KMS 条件密钥的完整列表，请参阅的条件密钥 AWS KMS。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
```

```
            "Sid": "Enable enclave data processing",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::123456789012:role/data-processing"
            },
            "Action": [
               "kms:Decrypt",
               "kms:GenerateDataKey",
               "kms:GenerateRandom"
            ],
            "Resource": "*",
            "Condition": {
               "StringEqualsIgnoreCase": {
                  "kms:RecipientAttestation:ImageSha384":
 "EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
                  "kms:RecipientAttestation:PCR0":
 "EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
                  "kms:RecipientAttestation:PCR1":
 "EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
                  "kms:RecipientAttestation:PCR2":
 "EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
                  "kms:RecipientAttestation:PCR3":
 "EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
                  "kms:RecipientAttestation:PCR4":
 "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
                  "kms:RecipientAttestation:PCR8":
 "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
               }
            }
         }
      ]
}
```

制定全球扩展战略

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供 AWS 有关 PRA 的反馈。

AWS 在全球扩张 AWS 时，安全保障服务经常会收到有关隐私架构的问题。这些问题通常围绕如何在符合特定隐私要求（例如数据主权义务或客户合同）的同时，避免增加额外成本和运营开销。设计考虑因素通常包括数据驻留、运营人员访问限制、恢复能力和生存能力以及整体独立性。有关更多信息，请参阅满足数字主权要求 AWS（re AWS：Invent 2022 演示文稿）。

以下是一些较为常见的问题，只有您才能根据自己的使用案例回答这些问题：

- 客户的个人数据需要存放在哪里？
- 我的客户数据存储在哪里？
- 个人数据如何以及在哪里进行跨境传输？
- 跨区域的人工或服务访问数据是否构成传输？
- 如何确保外国政府不会访问客户的个人数据？
- 我可以在哪里存储备份以及热站点或冷站点？
- 为了将数据保存在本地，我是否应该在我提供服务的每个区域都有一个 AWS 着陆区？或者我可以使用现有的 AWS Control Tower 着陆区？

对于数据驻留要求，不同的架构部署可能更适合不同的组织。有些组织可能要求将其客户的个人数据保留在特定区域内。如果是这种情况，您可能需要考虑如何在履行这些义务的同时，总体上遵守相关法规。无论情况如何，在选择多账户部署策略时都需要考虑多个因素。

要定义关键架构设计组件，请与您的合规与合同团队密切合作，以确认个人数据在何处、何时以及如何跨越 AWS 区域的要求。确定哪些行为属于数据传输，例如移动、复制或查看。此外，了解是否必须实施特定的韧性和数据保护控制措施。备份和灾难恢复策略是否需要跨区域失效转移？如果需要，请确定哪些区域可用于存储备份数据。确定是否对数据加密有任何要求，例如特定的加密算法或生成密钥的专用硬件安全模块。在与合规利益相关者就这些主题达成一致后，即可开始考虑多账户环境的设计方案。

以下是可用于规划 AWS 多账户策略的三种方法，按基础设施分割程度的升序排列：

- 带托管区域的中央登录区
- 区域登录区
- AWS 欧洲主权云

需要注意的是，隐私合规可能不仅仅局限于数据主权。查看本指南的其余部分，了解应对诸多其他挑战的可能解决方案，例如同意管理、数据主体的请求、数据治理和人工智能偏见。

带托管区域的中央登录区

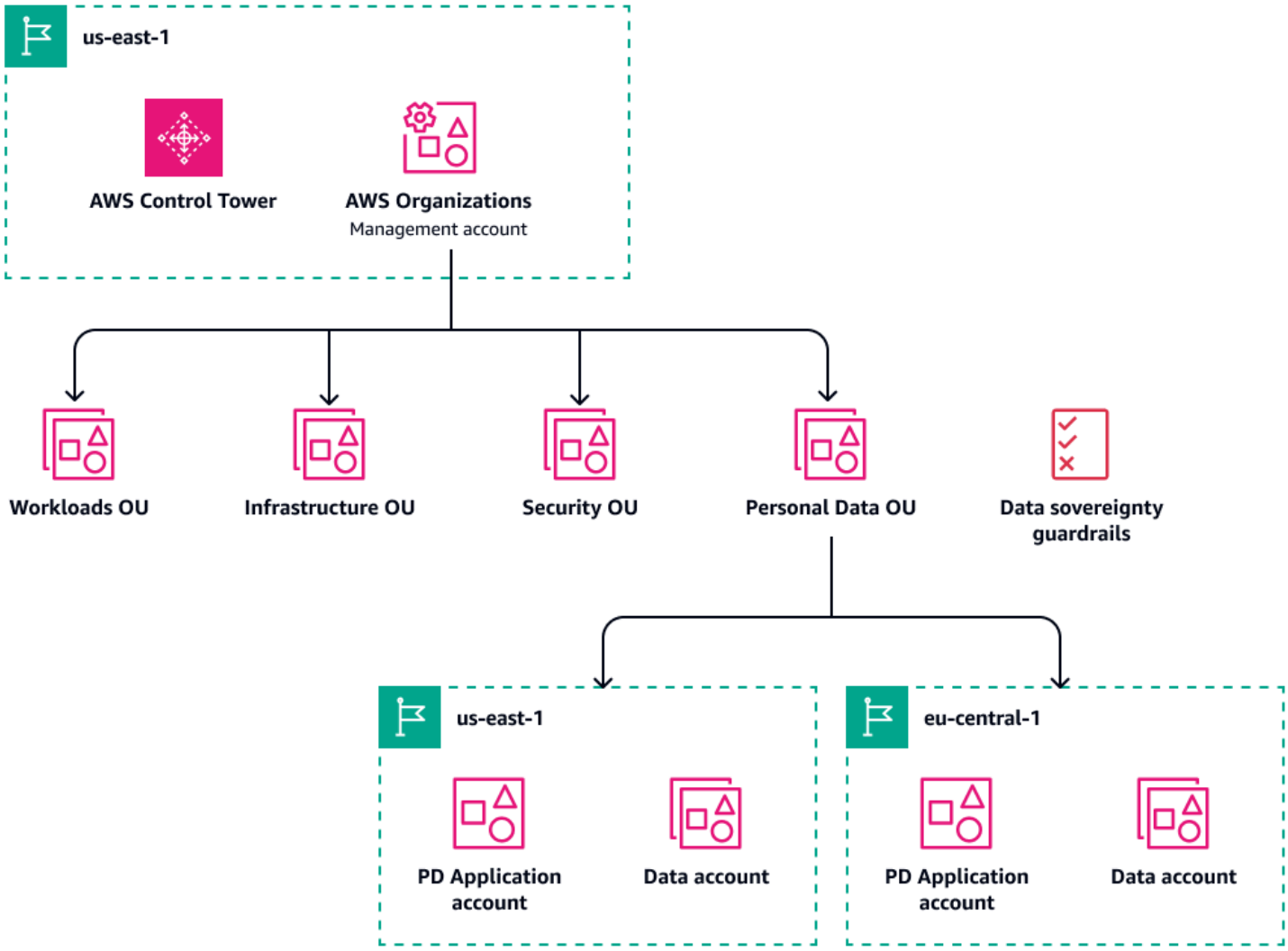
如果您想在全球范围内扩张，但已经在中建立了多账户架构 AWS，那么通常需要使用相同的多账户着陆区 (MALZ) 来管理其他账户。 AWS 区域在此配置中，您将继续从您创建登录区域的现有 AWS Control Tower 着陆区（Landing zone）运营基础设施服务，例如日志记录、账户工厂和一般管理。

对于生产工作负载，您可以通过将 AWS Control Tower 登录区扩展到新区域来运营区域部署。这样便可将 AWS Control Tower 治理范围扩展到新区域。这样，您就可以将个人数据存储在特定的托管区域内，数据仍存储在受益于基础设施服务和 AWS Control Tower 治理的账户中。在中 AWS Organizations，包含个人数据的帐户仍会汇总到专门的个人数据OU下，其中所有数据主权保护措施 AWS Control Tower 都在那里实施。此外，区域特定的工作负载放在专用账户中，而不是在多个区域中建立可能包含相同工作负载的生产账户。

这种部署可能是最具成本效益的，但要控制跨区域的个人数据流动 AWS 账户 ，还需要考虑其他因素。请考虑以下事项：

- 日志可能包含个人数据，因此可能需要进行一些额外的配置以包含或编辑敏感字段，从而防止在聚合期间进行跨区域传输。有关控制跨区域日志聚合的更多信息和推荐做法，请参阅本指南中的集中式日志存储。
- 在 AWS Transit Gateway 设计中考虑隔离 VPCs 和适当的双向网络流量。您可以限制允许和批准哪些中转网关连接，也可以限制哪些人员能够更改 VPC 路由表和可以更改哪些内容。
- 您可能需要阻止云运营团队成员访问个人数据。例如，系统可能认为包含客户事务数据的应用程序日志比其他日志源具有更高的敏感性。可能需要额外的批准和技术护栏，例如基于角色的访问控制和基于属性的访问控制。此外，访问数据时可能会受到驻留限制。例如，一个区域 A 中的数据只能从该区域内访问。

下图显示集中式登录区及区域部署。



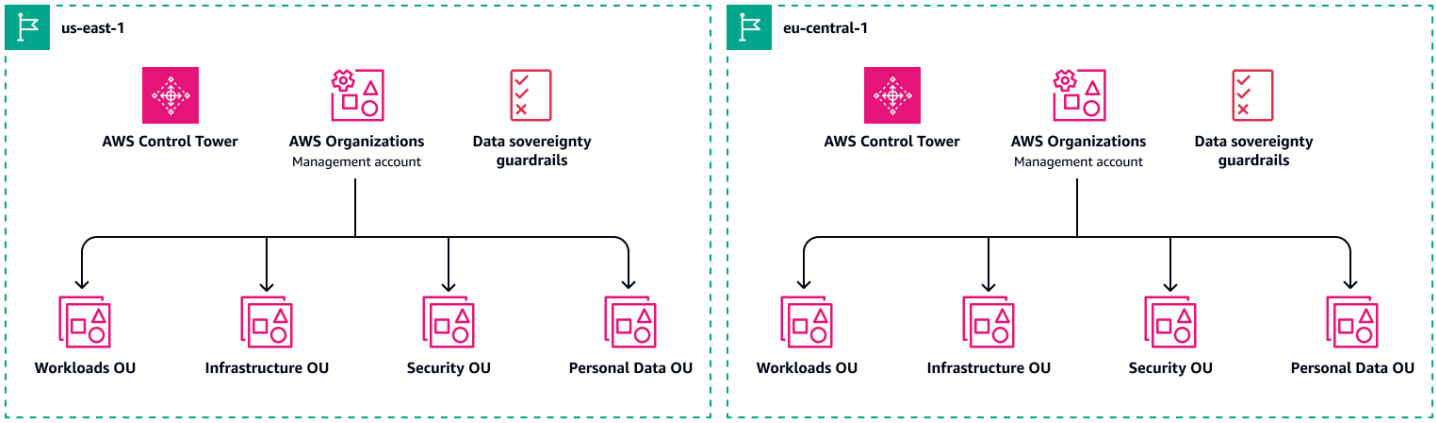
区域登录区

与非物质工作负载相比，拥有多个 MALZ 可以完全隔离处理个人数据的工作负载，从而帮助您实现更严格的合规要求。 AWS Control Tower 默认情况下可以配置集中式日志聚合，因此可以简化。使用此方法时，您无需为需要编辑的单独日志流维护日志记录例外。您甚至可以为每个 MALZ 设立本地专属云运营团队，从而将运营人员的访问权限限制为本地驻留。

许多组织在美国和欧盟都有单独的登录区部署。每个区域登录区都对该区域中的账户采用一刀切的安全策略和相关的治理。例如，在一个 MALZ 的工作负载中 HSMs 可能不需要使用专用加密个人数据，但在另一个 MALZ 中可能需要使用专用加密功能。

尽管此策略可以扩展以满足当前和未来的许多需求，但重要的是要了解与维护多个策略相关的额外成本和运营开销 MALZs。有关更多信息，请参阅AWS Control Tower 定价。

下图显示两个区域中单独的登录区。



AWS 欧洲主权云

一些组织要求将其在欧洲经济区（EEA）运营的工作量与在其他地区运营的工作量彻底分开。在这种情况下，可以考虑使用 AWS 欧盟主权云服务。 AWS 欧盟主权云服务是面向欧盟的新型独立云，旨在帮助客户满足该区域不断演进的主权需求，包括严格的数据驻留、运营自主权和韧性要求。

AWS 欧洲主权云在物理和逻辑上都与现有云分开 AWS 区域，同时提供相同的安全性、可用性和性能。只有位于欧盟的 AWS 员工才能控制 AWS 欧洲主权云的运营和支持。如果您有严格的数据驻留要求， AWS 欧洲主权云会将您创建的所有元数据（例如角色、权限、资源标签和他们用来运行的配置 AWS）保留在欧盟。 AWS 欧洲主权云还具有自己的计费和使用量计量系统。

对于此方法，您将使用与上一节区域登录区中类似的模式。但是，对于您向欧洲客户提供的服务，您可以在 AWS 欧洲主权云中部署专用的MALZ。

资源

> **调查**
>
> 我们很乐意听取您的意见。请通过简短的调查提供有关 AWS PRA 的反馈。

AWS Prescriptive Guidance

- AWS 安全参考架构（AWS SRA）

AWS 文档

- 数据保护（AWS Well-Architected Framework）
- 数据分类（AWS 白皮书）
- Amazon Web Services：风险与合规性（AWS 白皮书）
- Hybrid architectures to address personal data processing requirements（AWS 白皮书）
- 了解 AWS 上的 GDPR 合规性（AWS 白皮书）
- 在 AWS 上构建数据边界（AWS 白皮书）
- AWS 安全性文档

其他 AWS 资源

- AWS 合规性计划
- AWS 责任共担模型
- 数据隐私常见问题解答
- AWS 安全保障服务
- AWS Digital Sovereignty Pledge: Control without compromise（AWS 博客文章）
- AWS Security Learning

贡献者

调查

我们很乐意听取您的意见。请通过简短的调查提供有关 AWS PRA 的反馈。

本指南由 AWS 安全保障服务团队编写。如需支持实施本指南中的建议和操作您的工作负载，请联系 AWS 安全保障服务团队。

主要作者

- Amber Welch，AWS 高级隐私顾问
- Daniel Nieters，AWS 首席隐私顾问
- Robert Carter，AWS 技术项目经理

贡献者

- Avik Mukherjee，AWS 高级安全顾问
- David Bounds，AWS 高级解决方案架构师
- Jeff Lombardo，AWS 高级安全解决方案架构师
- Ram Ramani，AWS 首席安全解决方案架构师
- Vanessa Jacobs，AWS 高级安全顾问
- Thomas Nicholson，AWS 高级隐私顾问
- Jose DeJesus，AWS 高级保障顾问
- Doug Pardue，AWS 解决方案架构师经理

技术撰稿人

- Lilly AbouHarb，AWS 高级技术撰稿人

文档历史记录

调查

我们很乐意听取您的意见。请通过简短的调查提供有关 AWS PRA 的反馈。

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

变更	说明	日期
重大更新	我们在 AWS Artifact 部分增加了云计算合规性控制目录（C5）。我们在日志存档账户中增加了 Amazon Security Lake。我们增加了 Amazon Bedrock、AWS Clean Rooms、Amazon DataZone、AWS Lake Formation、Amazon SageMaker AI 以及可帮助发现数据、对数据进行分类和编目的 AWS 服务和功能到 PD 应用程序账户中。我们增加了制定全球扩展战略部分。	2025 年 9 月 16 日
重大更新	我们通篇进行了重大更新。	2024 年 3 月 26 日
初次发布	—	2023 年 10 月 2 日

AWS 规范性指导词汇表

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

数字

7 R

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

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

A

ABAC

请参阅基于属性的访问控制。

抽象服务

请参阅托管服务。

ACID

请参阅原子性、一致性、隔离性、持久性。

主动-主动迁移

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

主动-被动迁移

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

聚合函数

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

AI

请参阅人工智能。

AIOps

请参阅人工智能运营。

匿名化

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

反模式

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

应用程序控制

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

应用程序组合

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

人工智能（AI）

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

人工智能操作 (AIOps)

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

非对称加密

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

原子性、一致性、隔离性、持久性（ACID）

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

基于属性的访问权限控制（ABAC）

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

权威数据来源

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

可用区

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

AWS 云采用框架 (AWS CAF)

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

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

AWS 工作负载资格框架 (AWS WQF)

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

B

恶意机器人

一种旨在扰乱或伤害个人或组织的机器人。

BCP

请参阅业务连续性计划。

行为图

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

大端序系统

一个先存储最高有效字节的系统。另请参阅字节顺序。

二进制分类

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

bloom 筛选条件

一种概率性、内存高效的数据结构，用于测试元素是否为集合的成员。

蓝/绿部署

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

自动程序

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

僵尸网络

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

分支

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

紧急（break-glass）访问

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

棕地策略

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

缓冲区缓存

存储最常访问的数据的内存区域。

业务能力

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

业务连续性计划（BCP）

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

C

CAF

请参阅 AWS 云采用框架。

金丝雀部署

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

CCoE

请参阅云卓越中心。

CDC

请参阅更改数据捕获。

更改数据捕获（CDC）

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

混沌工程

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

CI/CD

请参阅持续集成和持续交付。

分类

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

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心 (CCoE)

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

云计算

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

云运营模型

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

云采用阶段

组织迁移到 AWS 云中时通常会经历四个阶段：

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

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

CMDB

请参阅配置管理数据库。

代码存储库

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

冷缓存

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

冷数据

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

计算机视觉（CV）

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

配置偏移

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

配置管理数据库（CMDB）

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

合规性包

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

持续集成和持续交付（CI/CD）

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

CV

请参阅计算机视觉。

D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

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

数据漂移

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

传输中数据

在网络中主动移动的数据，例如在网络资源之间移动的数据。

数据网格

一种架构框架，可提供分布式、去中心化的数据所有权以及集中式管理和治理。

数据最少化

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

数据边界

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

数据预处理

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

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

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

数据库定义语言（DDL）

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言（DML）

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

请参阅数据库定义语言。

深度融合

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

深度学习

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

defense-in-depth

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

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

委派管理员

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

部署

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

开发环境

请参阅环境。

侦测性控制

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

开发价值流映射（DVSM）

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

数字孪生

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

维度表

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

灾难

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

灾难恢复（DR）

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

DML

请参阅数据库操作语言。

领域驱动设计

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

DR

请参阅灾难恢复。

偏差检测

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

DVSM

请参阅开发价值流映射。

E

EDA

请参阅探索性数据分析。

EDI

请参阅电子数据交换。

边缘计算

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

电子数据交换（EDI）

组织之间业务文件的自动交换。有关更多信息，请参阅什么是电子数据交换。

加密

一种将人类可读的纯文本数据转换为加密文字的计算流程。

加密密钥

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

字节顺序

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

端点

请参阅服务端点。

端点服务

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

企业资源规划（ERP）

一种自动化和管理企业关键业务流程（例如会计、MES 和项目管理）的系统。

信封加密

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

环境

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

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

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

epic

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

ERP

请参阅企业资源规划。

探索性数据分析（EDA）

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

F

事实表

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

快速失效机制

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

故障隔离边界

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

功能分支

请参阅分支。

特征

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

特征重要性

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

功能转换

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

少样本提示

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

FGAC

请参阅精细访问控制。

精细访问控制（FGAC）

使用多个条件允许或拒绝访问请求。

快闪迁移

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

FM

请参阅基础模型。

基础模型（FM）

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

G

生成式人工智能

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

地理阻止

请参阅地理限制。

地理限制（地理阻止）

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

GitFlow 工作流程

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

黄金映像

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

全新策略

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

防护机制

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

H

HA

请参阅高可用性。

异构数据库迁移

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

高可用性（HA）

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

历史数据库现代化

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

保留数据

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

同构数据库迁移

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

热数据

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

修补程序

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

hypercare 周期

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

我

IaC

请参阅基础设施即代码。

基于身份的策略

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

空闲应用程序

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

IIoT

请参阅工业物联网。

不可变基础设施

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

入站（入口）VPC

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

增量迁移

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

工业 4.0

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

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码（IaC）

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

工业物联网 (IIoT)

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

检查 VPC

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

物联网（IoT）

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

可解释性

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

物联网

请参阅物联网。

IT 信息库（ITIL）

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

IT 服务管理（ITSM）

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

ITIL

请参阅 IT 信息库。

ITSM

请参阅 IT 服务管理。

L

基于标签的访问控制（LBAC）

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

登录区

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

大语言模型（LLM）

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

大规模迁移

迁移 300 台或更多服务器。

LBAC

请参阅基于标签的访问控制。

最低权限

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

直接迁移

请参阅 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参阅字节顺序。

LLM

请参阅大型语言模型。

下层环境

请参阅环境。

M

机器学习（ML）

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

主分支

请参阅分支。

恶意软件

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

托管式服务

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

制造执行系统（MES）

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

MAP

请参阅迁移加速计划。

机制

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

成员账户

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

MES

请参阅制造执行系统。

消息队列遥测传输（MQTT）

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

微服务

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

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

微服务架构

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

迁移加速计划（MAP）

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

大规模迁移

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

迁移工厂

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

迁移元数据

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

迁移模式

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

迁移组合评测（MPA）

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

迁移准备情况评测（MRA）

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

迁移策略

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

ML

请参阅机器学习。

现代化

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

现代化准备情况评估

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

单体应用程序（单体式）

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

MPA

请参阅迁移组合评测。

MQTT

请参阅消息队列遥测传输。

多分类器

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

可变基础设施

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

O

OAC

请参阅来源访问控制。

OAI

请参阅来源访问身份。

OCM

请参阅组织变革管理。

离线迁移

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

OI

请参阅运营集成。

OLA

请参阅运营级别协议。

在线迁移

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

OPC-UA

请参阅开放流程通信 – 统一架构。

开放流程通信 – 统一架构（OPC-UA）

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

运营级别协议（OLA）

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

运营准备情况审查（ORR）

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

运营技术（OT）

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

运营整合（OI）

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

组织跟踪

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

组织变革管理（OCM）

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

来源访问控制（OAC）

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

来源访问身份（OAI）

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

ORR

请参阅运营准备情况审查。

OT

请参阅运营技术。

出站（出口）VPC

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

P

权限边界

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

个人身份信息（PII）

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

PII

请参阅个人身份信息。

playbook

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

PLC

请参阅可编程逻辑控制器。

PLM

请参阅产品生命周期管理。

policy

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

多语言持久性

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

组合评测

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

谓词

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

谓词下推

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

预防性控制

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

主体

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

隐私设计

一种在整个开发过程中都考虑隐私的系统工程方法。

私有托管区

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

主动控制

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

产品生命周期管理（PLM）

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

生产环境

请参阅环境。

可编程逻辑控制器（PLC）

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

提示串接

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

假名化

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

publish/subscribe (pub/sub)

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

Q

查询计划

一系列用于访问 SQL 关系数据库系统中的数据的步骤，类似于指令。

查询计划回归

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

R

RACI 矩阵

请参阅责任、问责、咨询和知情（RACI）。

RAG

请参阅检索增强生成。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI 矩阵

请参阅责任、问责、咨询和知情（RACI）。

RCAC

请参阅行列访问控制。

只读副本

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

重新架构

请参阅 7 R。

恢复点目标（RPO）

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

恢复时间目标（RTO）

服务中断和服务恢复之间可接受的最大延迟。

重构

请参阅 7 R。

Region

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

回归

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

重新托管

请参阅 7 R。

版本

在部署过程中，推动生产环境变更的行为。

重新放置

请参阅 7 R。

更换平台

请参阅 7 R。

重新购买

请参阅 7 R。

韧性

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

基于资源的策略

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

责任、问责、咨询和知情（RACI）矩阵

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

响应性控制

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

保留

请参阅 7 R。

停用

请参阅 7 R。

检索增强生成（RAG）

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

轮换

定期更新密钥以使攻击者更难访问凭证的过程。

行列访问控制（RCAC）

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

RPO

请参阅恢复点目标。

RTO

请参阅恢复时间目标。

运行手册

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

S

SAML 2.0

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

SCADA

请参阅监督控制和数据采集。

SCP

请参阅服务控制策略。

机密密钥

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

安全设计

一种在整个开发过程中都考虑安全的系统工程方法。

安全控制

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

安全固化

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

安全信息和事件管理（SIEM）系统

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

安全响应自动化

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

服务器端加密

由接收数据的人在目的地对数据 AWS 服务 进行加密。

服务控制策略（SCP）

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

服务端点

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

服务水平协议（SLA）

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

服务水平指示器（SLI）

对服务性能方面的衡量，例如错误率、可用性或吞吐量。

服务水平目标（SLO）

代表服务运行状况的目标指标，由服务水平指示器衡量。

责任共担模式

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

SIEM

请参阅安全信息和事件管理系统。

单点故障（SPOF）

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

请参阅服务水平协议。

SLI

请参阅服务水平指示器。

SLO

请参阅服务水平目标。

split-and-seed 模型

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

SPOF

请参阅单点故障。

星型架构

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

strangler fig 模式

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

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

监督控制和数据采集（SCADA）

在制造业中，一种使用硬件和软件来监控实物资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

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

系统提示

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

T

标签

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

目标变量

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

任务列表

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

测试环境

请参阅环境。

训练

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

中转网关

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

基于中继的工作流程

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

可信访问权限

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

优化

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

双披萨团队

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

U

不确定性

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

无差别任务

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

上层环境

请参阅环境。

V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC 对等连接

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

漏洞

损害系统安全的软件缺陷或硬件缺陷。

W

热缓存

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

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

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

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

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

WORM

请参阅一次写入多次读取。

WQF

请参阅 AWS 工作负载资格鉴定框架。

一次写入多次读取（WORM）

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

Z

零日漏洞利用

一种利用零日漏洞的攻击，通常为恶意软件。

零日漏洞

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

零样本提示

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

僵尸应用程序

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

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