



AWS 隐私参考架构 (AWS PRA)

AWS 规范性指导



AWS 规范性指导: AWS 隐私参考架构 (AWS PRA)

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

简介	1
版权声明	1
简介	1
责任 AWS 共担模式和隐私	1
了解 AWS PRA	3
使用 P AWS RA 和 SRA AWS	3
AWS Organizations 和专用账户结构	4
运营 AWS 隐私服务	5
AWS 隐私参考架构	7
组织管理账户	9
AWS Artifact	10
AWS Control Tower	11
AWS Organizations	11
安全 OU — 安全工具账户	13
AWS CloudTrail	14
AWS Config	15
Amazon GuardDuty	16
IAM Access Analyzer	16
Amazon Macie	17
安全 OU — 日志存档账户	17
集中式日志存储	18
基础设施 OU — 网络账户	19
Amazon CloudFront	21
AWS Resource Access Manager	21
AWS Transit Gateway	21
AWS WAF	22
个人数据 OU — PD 申请账户	23
Amazon Athena	25
Amazon CloudWatch 日志	26
Amazon CodeGuru Reviewer	26
Amazon Comprehend	26
Amazon Data Firehose	27
AWS Glue	27
AWS Key Management Service	29

AWS Local Zones	29
AWS Nitro 飞地	30
AWS PrivateLink	31
AWS Resource Access Manager	32
Amazon SageMaker	32
AWS 有助于管理数据生命周期的功能	33
有助于对数据进行细分的 AWS 服务和功能	34
隐私相关政策示例	35
需要从特定 IP 地址进行访问	35
需要组织成员才能访问 VPC 资源	36
限制跨数据传输 AWS 区域	37
授予对特定亚马逊 DynamoDB 属性的访问权限	39
限制对 VPC 配置的更改	40
需要认证才能使用密钥 AWS KMS	41
资源	43
AWS 规范性指导	43
AWS 文档	43
其他 AWS 资源	43
贡献者	44
文档历史记录	45
术语表	46
#	46
A	46
B	49
C	50
D	53
E	56
F	58
G	59
H	60
I	61
L	63
M	64
O	68
P	70
Q	72

R	73
S	75
T	78
U	79
V	80
W	80
Z	81
.....	lxxxii

AWS 隐私参考架构 (AWS PRA)

亚马逊 Web Services ([贡献者](#))

2024 年 3 月 ([文档历史记录](#))

我们很乐意听取你的意见。请通过[简短的调查](#)提供 AWS 有关 PRA 的反馈。

版权声明

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 (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，以支持隐私保护 AWS Cloud。

责任 AWS 共担模式和隐私

在中 AWS Cloud，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 Cloud。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，内容被定义为软件（包括机器图像）、数据、文本、音频、视频或图像，由 AWS 服务 您或任何最终用户传输给我们进行处理、存储或托管，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 您在数据中使用的
- 您收集、存储或处理数据 AWS 区域 的地方
- 数据的格式和结构，以及它是屏蔽的、匿名化的，还是加密的
- 如何定义、存储、轮换和操作加密密钥
- 谁有权访问您的数据、何时有权访问您的数据，以及如何授予、管理和撤销这些访问权限

了解 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，诸如亚马逊弹性计算云 (Amazon EC2) 之类的服务被归类为基础设施即服务 (IaaS)。因此，如果您使用 Amazon EC2，则必须为访客操作系统以及在 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。您的职责是管理和分类数据，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

我们很乐意听取你的意见。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 and 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

我们很乐意听取你的意见。请通过[简短的调查](#)提供 AWS 有关 PRA 的反馈。

AWS PRA提供的模式已被客户发现，这些模式有助于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。AWS [AWS 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 详细说明了許多相同的密钥。AWS 服务本指南仅包括对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中详述的許多安全准则可以与PRA中详述的隐私控制措施一起遵守。AWS 与安全性类似，一些基本的隐私注意事项可能有助于您在 AWS Cloud 旅程的早期阶段就做出这些考虑，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？
- 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来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分开？
- 我的组织有哪些跨境数据传输要求？

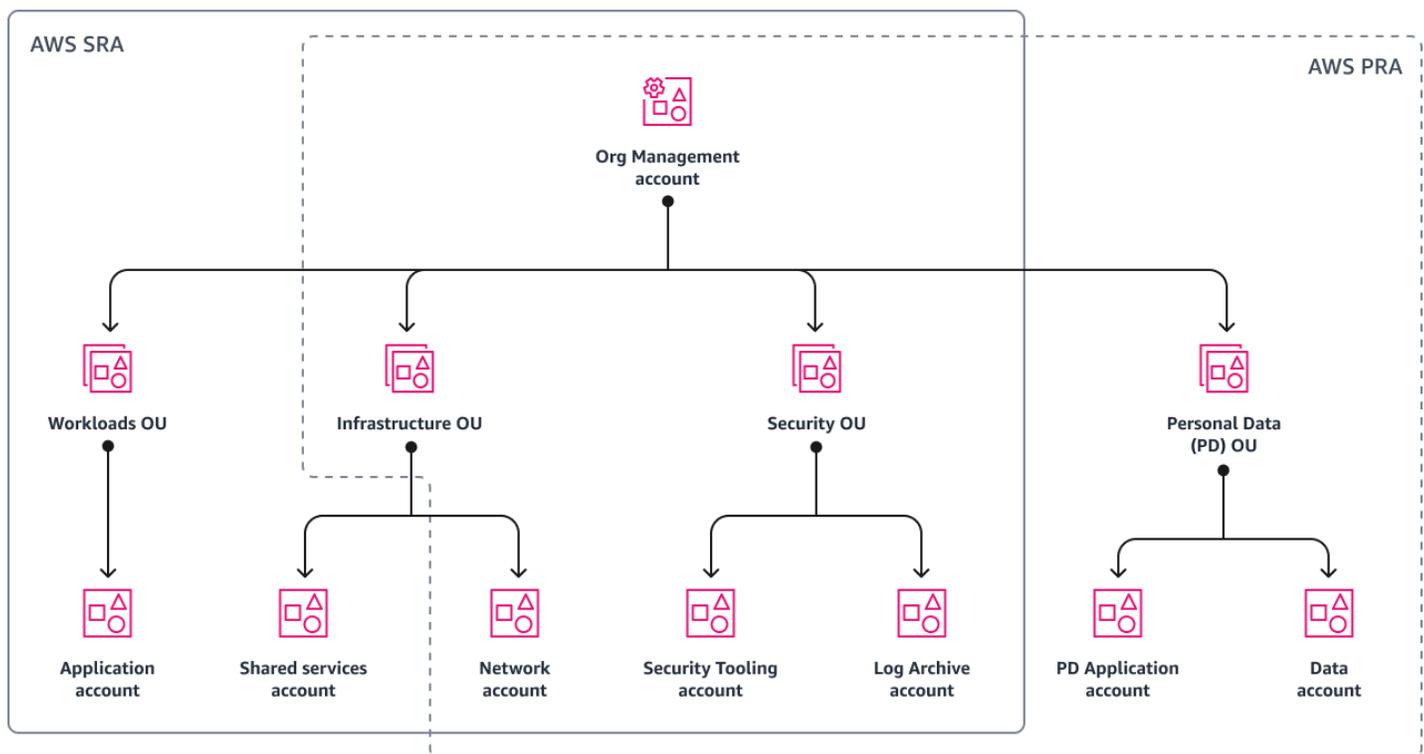
其中许多问题的答案可能会对您的云环境设计产生影响，例如您的 AWS 账户结构、服务控制策略和 AWS Identity and Access Management (IAM) 角色。

AWS Organizations 和专用账户结构

我们很乐意听取你的意见。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管理多个账户 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[建立最佳实践 AWS 环境](#)。

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 S 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](#)的其他指导。收集或处理个人数据的应用程序位于 PD OU 的专用账户中。

您可以使用在整个组织中[AWS Control Tower](#)进行整体基础治理和自动部署安全和隐私控制。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，考虑处理个人数据会很有帮助。您可能需要考虑正在处理的数据类型，以了解其独特的用例和适用的法律和法规。例如，持卡人数据受支付卡行业数据安全标准 (PCI DSS) 的保护，受保护的健康信息可能受《健康保险便携与责任法案》(HIPAA) 的约束。您可能需要查看哪些环境包含个人数据，并以此为基础制定细分策略。典型的客户细分策略可以包括与软件开发生命周期 (SDLC) 保持一致的专用账户，例如用于开发、试运行或质量保证 (QA) 和生产的专用账户。AWS 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，您的 OU 可能需要与您的特定监管要求保持一致。

运营 AWS 隐私服务

我们很乐意听取你的意见。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。许多不同的团队都可以发挥作用，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政策组成部分时，您可以根据隐私合规框架映射控制措施，以实现一致的运营。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来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共同努力才能实现实施目标。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，[阻止公众访问 Amazon](#)

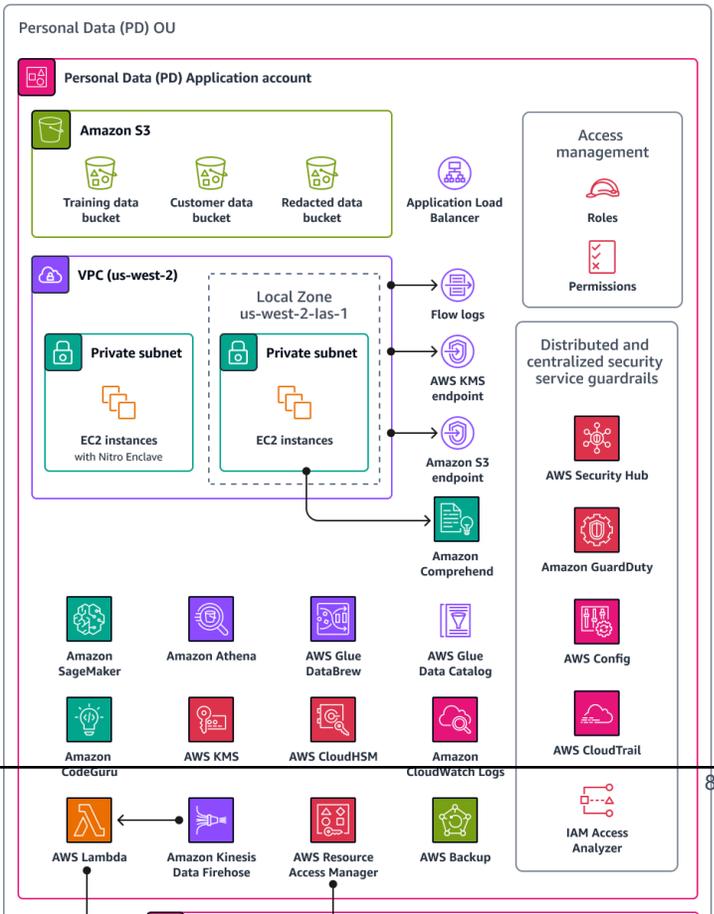
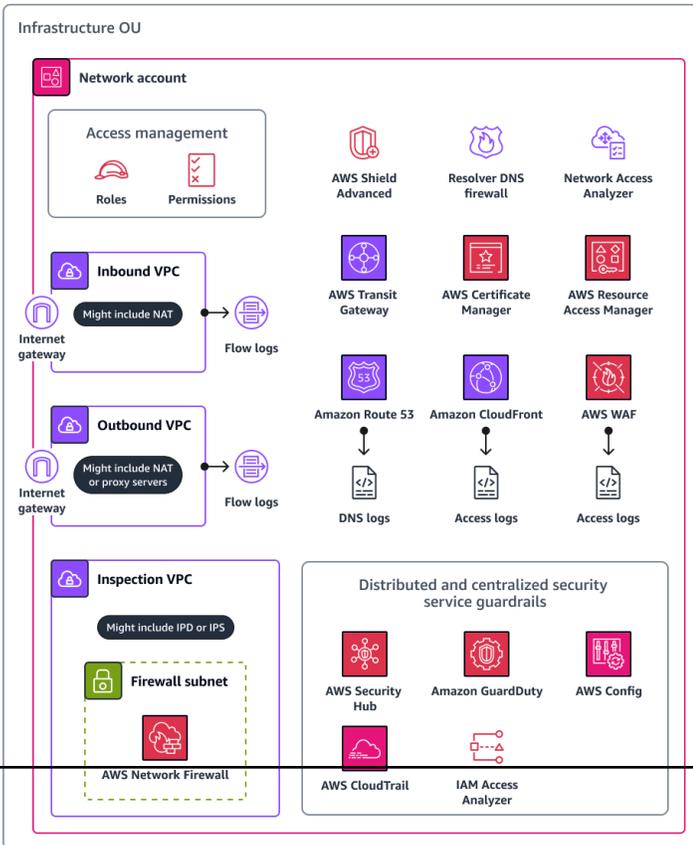
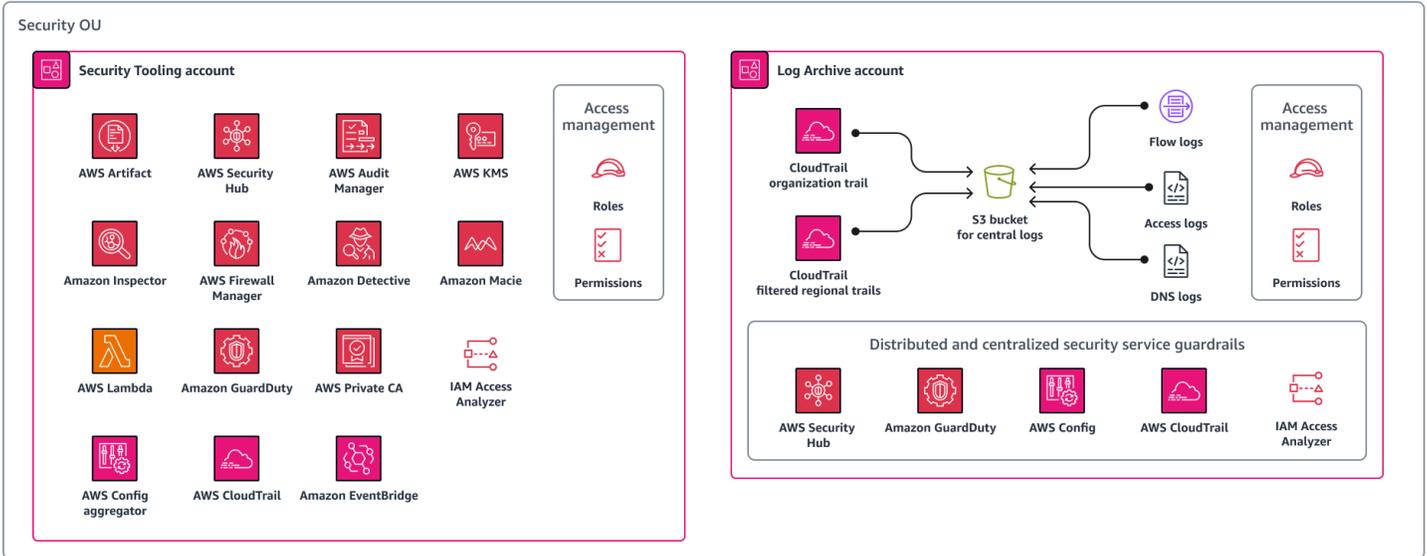
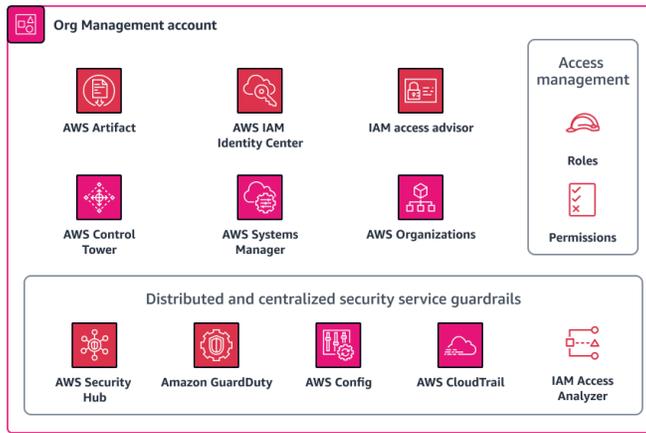
[S3 存储桶](#)是一种特定的控件，最好在组织根目录进行配置，而不是为每个账户单独配置。但是，您的保留策略可能因应用程序而异，这意味着您可以在资源级别应用控制权。

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

我们很乐意听取你的意见。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。该架构建立在受控制的着陆区 (landing zone) 之上 AWS Control Tower。



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。此账户中的架构是直接来自消费者那里收集个人数据的示例工作负载。在此工作负载中，用户通过 Web 层进行连接。Web 层与应用程序层交互。该层接收来自 Web 层的输入，处理和存储数据，允许授权的内部团队和第三方访问数据，并最终在不再需要时存档和删除数据。该架构有针对性地采用模块化和事件驱动，旨在演示许多基本的隐私工程技术，而无需深入研究数据湖、容器、计算或物联网 (IoT) 等特定用例。

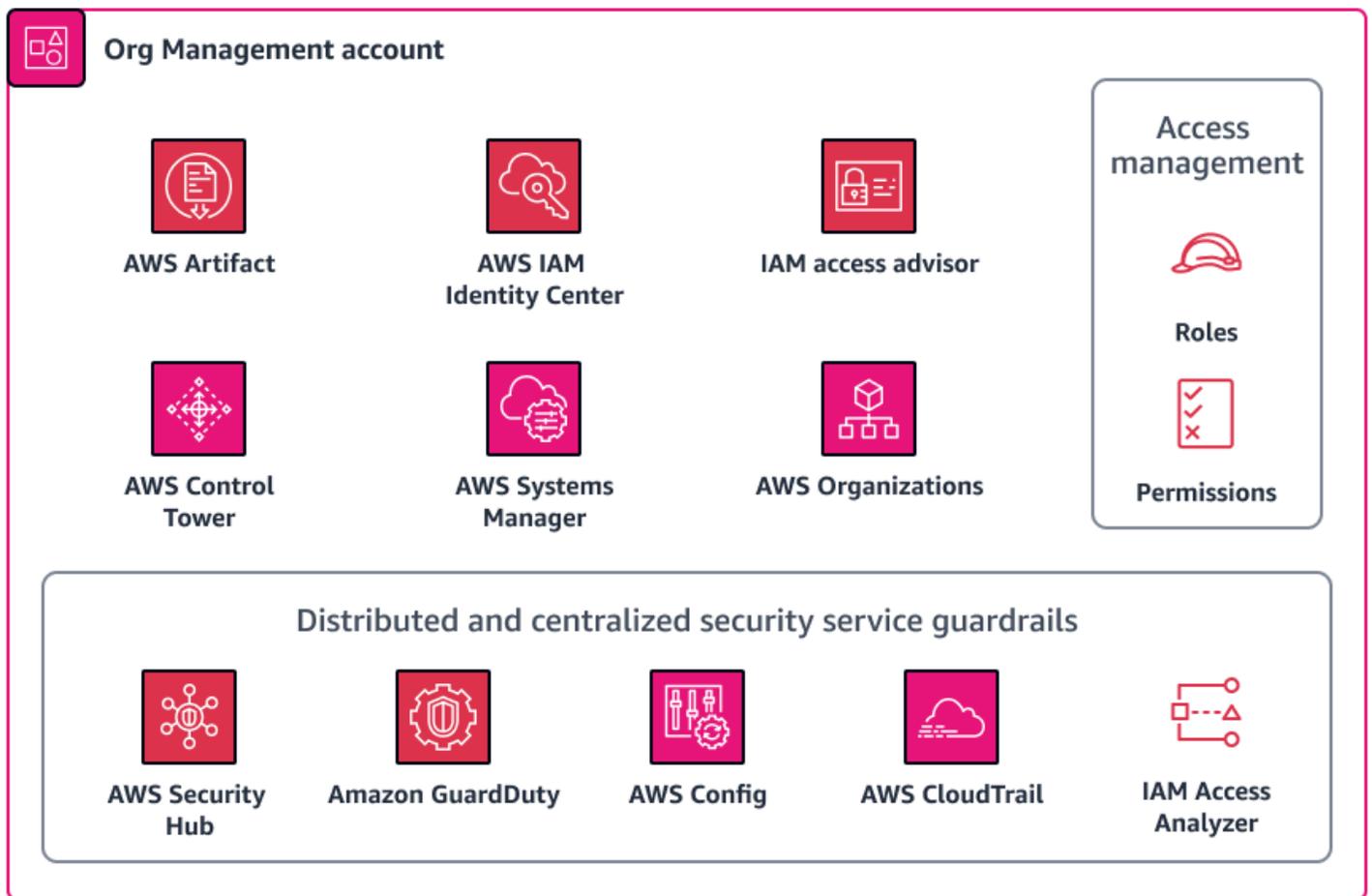
接下来，本指南详细描述了组织中的每个账户。它讨论了与隐私相关的服务和功能、注意事项和建议，以及以下每个账户的图表：

- [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 申请账户](#)

组织管理账户

我们很乐意听取你的意见。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组织中所有账户的基础隐私控制的资源配置偏差，这些账户由 AWS Organizations 管理。您还可以在此帐户中始终如一地部署新的成员帐户，并具有许多相同的安全和隐私控制措施。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。



本节提供有关此账户中 AWS 服务 使用的以下内容的更多详细信息：

- [AWS Artifact](#)
- [AWS Control Tower](#)
- [AWS Organizations](#)

AWS Artifact

[AWS Artifact](#) 可以通过按需下载 AWS 安全与合规性文档来帮助您进行审计。有关如何在安全环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 安全控制的证据。以下报告可能有助于证明 AWS 隐私控制的有效性：

- 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。有关更多信息，请参阅 [SOC 常见问题解答](#)。
- SOC 3 隐私报告 — [SOC 3 隐私报告](#) 对 SOC 隐私控制的描述不太详细，仅供广泛分发。
- 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) 的要求和指导方针。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最佳实践的 AWS 多账户环境。有关如何在安全环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、预防性和检测性控制措施（也称为护栏），这些控制措施与您的数据驻留和数据保护要求保持一致。例如，您可以指定护栏，将数据传输限制为仅获得批准。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 AWS Config 规则组成，可以在整个组织中统一部署。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](#)。

如果您需要在数据驻留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。在设置 landing zone 时，这些控件默认部署在每个 OU 中。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 以提供侦探控制。这些控件被称为 [服务管理标准: AWS Control Tower](#)。您可以使用这些控件来监控支持隐私的控件的配置偏差，例如亚马逊关系数据库服务 (Amazon RDS) 数据库实例的静态加密。

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 (SCP) [和管理策略](#) 来帮助保护个人数据和隐私。

服务控制策略 (SCP)

[服务控制策略 \(SCP\)](#) 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应用 SCP。

您可以使用 AWS Control Tower 在您的账户中统一部署 SCP。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 包括一整套预防性 SCPs。如果您的组织中当前 AWS Control Tower 未使用这些控件，您也可以手动部署这些控件。

使用 SCP 来满足数据驻留要求

通常通过在特定地理区域内存储和处理数据来管理个人数据驻留要求。为了验证司法管辖区的独特数据驻留要求是否得到满足，我们建议您与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 SCP 来限制 AWS 区域 可用于处理和存储数据的 SCP。有关策略示例，请参阅本指南[限制跨数据传输 AWS 区域](#)中的。

使用 SCP 限制高风险的 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，您应对可能针对您使用的 API 调 AWS 服务 用的结果负责。您还有责任了解其中哪些电话可能导致您的安全或隐私状况发生变化。如果您担心保持一定的安全和隐私状态，可以启用拒绝某些 API 调用的 SCP。这些 API 调用可能会产生影响，例如意外披露个人数据或违反特定的跨境数据传输。例如，您可能想要禁止以下 API 调用：

- 允许公众访问亚马逊简单存储服务 (Amazon S3) Service 存储桶
- 禁用 Amazon GuardDuty 或为数据泄露发现创建抑制规则，例如[特洛伊木马 DataExfiltration:ec2/DNS](#) 的发现
- 删除 AWS WAF 数据泄露规则
- 公开共享亚马逊 Elastic Block Store (Amazon EBS) Block Store 快照
- 从组织中移除成员账户
- 解除 Amazon CodeGuru Reviewer 与存储库的关联

管理政策

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 OU 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。应用标签来区分组织中处理个人数据的资源可能很有用。标签的使用支持本指南中的许多隐私解决方案。例如，您可能需要应用一个标

记，以指示资源中正在处理或存储的数据的一般数据分类。您可以编写基于属性的访问控制 (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，您的策略可能指定该SysAdmin角色无法访问带有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，如果您的组织习惯在多个账户的备份中广泛应用数据保留策略，则可以应用一个标签，将该资源置于该备份策略的范围内。[AWS Backup](#)

[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应用于资源的规则。例如，您可以要求使用特定的密钥（例如DataClassification或）标记资源DataSteward，并且可以为密钥指定有效的案例处理或值。您还可以使用[强制](#)措施来防止不合规的标记请求完成。

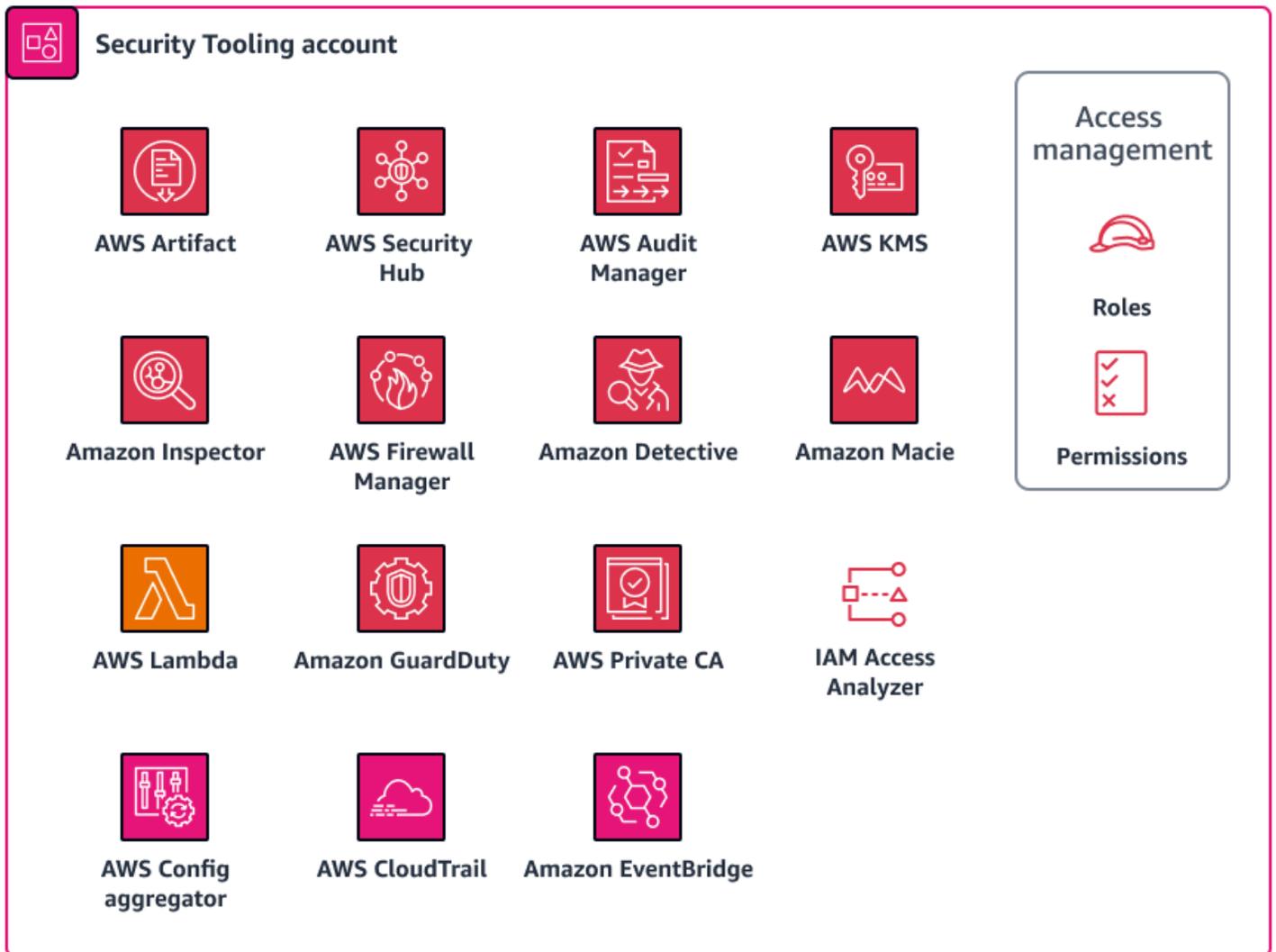
使用标签作为隐私控制策略的核心组成部分时，请考虑以下几点：

- 考虑将个人数据或其他类型的敏感数据放在标签键或值中的影响。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。在这种情况下，您可能需要取消标识标签值，然后使用客户控制的系统（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。
- 考虑一下，需要将某些标签值设为不可变（不可修改），以防止规避技术控制，例如依赖标签的 ABAC 条件。

安全 OU — 安全工具账户

我们很乐意听取你的意见。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。



本节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 Access Analyzer](#)
- [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 安全参考架构](#)建议

启用组织跟踪，这是记录组织中所有账户所有事件的单一跟踪。但是，启用此组织跟踪会将多区域日志数据聚合到日志存档账户中的单个 Amazon Simple Storage Service (Amazon S3) 存储桶中。对于处理个人数据的帐户，这可能会带来一些额外的设计注意事项。日志记录可能包含一些对个人数据的引用。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应将哪些区域工作负载包括在组织跟踪中或排除在外。对于您决定从组织跟踪中排除的工作负载，您可以考虑配置一个特定于区域的跟踪来掩盖个人数据。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，您的组织可能会将组织跟踪和区域跟踪组合到集中的日志存档帐户中。

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。

有关总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。此设计可帮助您为需要管理日志的人员和需要使用日志数据的用户创建最低权限访问策略。

AWS Config

[AWS Config](#) 提供了您的资源 AWS 账户 及其配置方式的详细视图。它可以帮助您确定资源之间的关系以及它们的配置如何随着时间的推移而发生变化。有关如何在安全环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。一致性包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 隐私框架操作最佳实践 v1.0](#) 一致性包与 NIST 隐私框架中的许多与隐私相关的控件保持一致。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`— 此规则通过持续监控 VPC 路由表中是否存在通往 Internet `::/0` 网关的默认路由 `0.0.0.0/0` 或出口路由，帮助防止数据平面上的数据泄露。这可以帮助您限制互联网流量可以发送到何处，尤其是在已知存在恶意的 CIDR 范围的情况下。
- `encrypted-volumes`— 该规则检查附加到亚马逊弹性计算云 (Amazon EC2) 实例的亚马逊弹性区块存储 (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的密钥 ID，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 安全组是否允许不受限制的 TCP 流量流向指定端口。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 在您的资源上阻止来自常 `0.0.0.0/0` 用端口（例如 TCP 3389 和 TCP 21）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，您还可以将这些规则合并到侦测和主动评估模式中。这有助于在软件开发生命周期的早期实施隐私检查，因为应用程序开发人员可以开始采用部署前检查。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。有关如何在安全环境中使用此服务的更多信息，请参阅 [AWS 安全参考架构](#)。

借助 GuardDuty，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 账户中的所有人员启用，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过程中（从检测和分析到遏制和消除）中识别所有与隐私相关的利益相关者，并让他们参与任何可能涉及数据泄露的事件。

IAM Access Analyzer

许多客户希望持续确保与预先批准和预期的第三方处理者适当共享个人数据，而不是其他实体。[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环境中的可信资源。AWS 在为意外和故意披露个人数据定义控制措施时，您可以定义可信身份、可信资源和预期网络。

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 会分析 IAM 策略，

以帮助识别和解决对潜在敏感资源的意外公开或跨账户访问问题。IAM Access Analyzer 使用数学逻辑和推理来生成可以从外部 AWS 账户访问的资源的全面发现。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 最佳实践验证现有策略并提供建议。IAM Access Analyzer 可以根据 IAM 委托人先前的访问活动生成权限最低的 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。

有关如何在安全环境中使用 IAM Access Analyzer 的更多信息，请参阅[AWS 安全参考架构](#)。

Amazon Macie

[Amazon Macie](#) 是一项使用机器学习和模式匹配来发现敏感数据的服务，提供对数据安全风险的可见性，并帮助您自动防范这些风险。当 Macie 检测到潜在的违反政策或您的 Amazon S3 存储桶的安全或隐私问题时，它会生成调查结果。Macie 是组织可以用来实现自动化的另一种工具，以支持合规工作。有关如何在安全环境中使用此服务的更多信息，请参阅[AWS 安全参考架构](#)。

Macie 可以检测大量且不断增长的敏感数据类型，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](#)，以定义反映组织对个人数据的定义的检测标准。

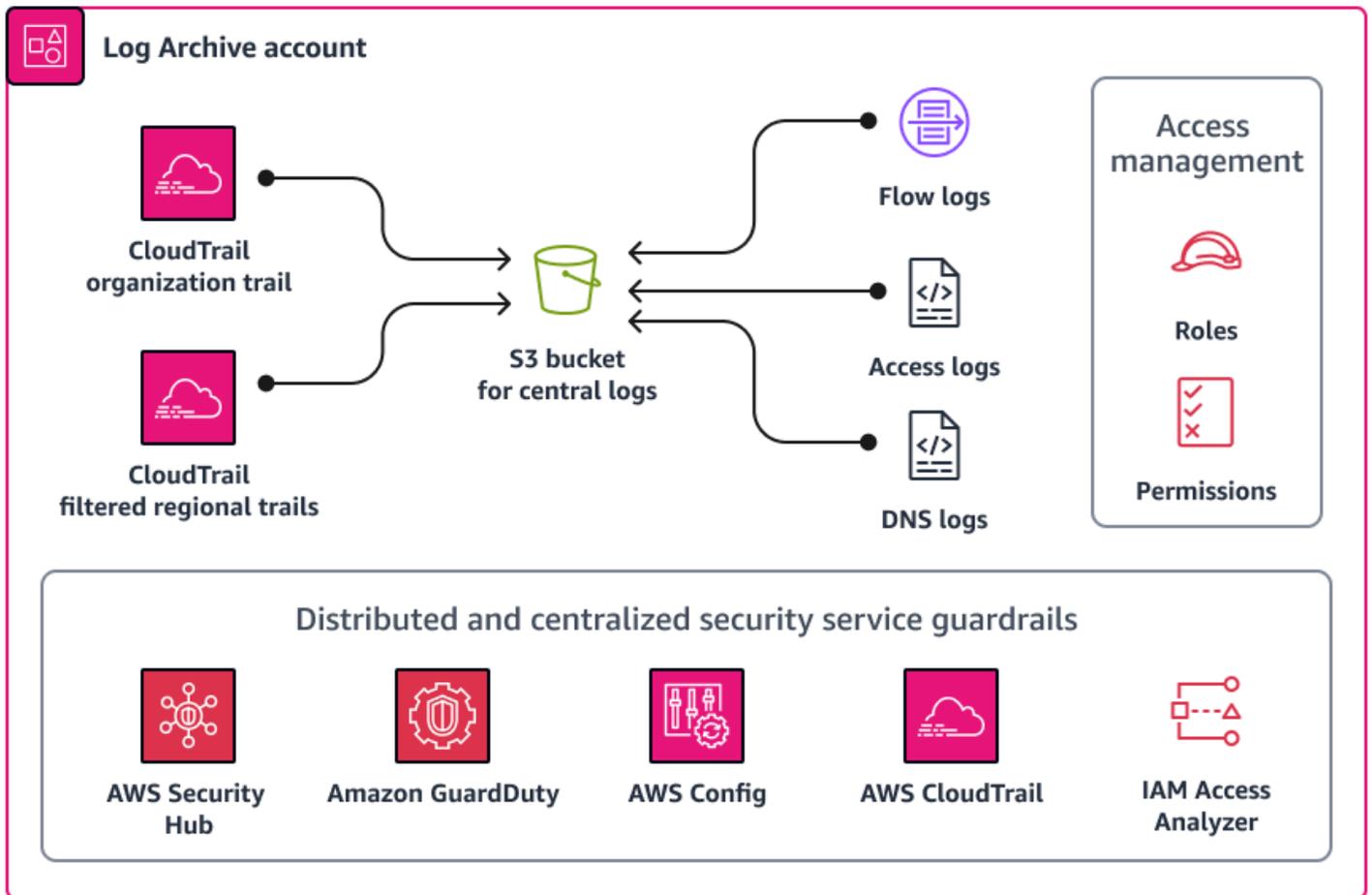
当您的组织为包含个人数据的 Amazon S3 存储桶定义预防性控制措施时，您可以使用 Macie 作为验证机制，持续保证您的个人数据存放在何处以及如何受到保护。首先，启用 Macie 并配置[自动发现敏感数据](#)。Macie 会持续分析您所有 S3 存储桶中的对象，跨账户和 AWS 区域 Macie 生成并维护交互式热图，描述个人数据所在的位置。自动敏感数据发现功能旨在降低成本并最大限度地减少手动配置发现任务的需求。您可以在自动敏感数据发现功能的基础上再接再厉，使用 Macie 自动检测新存储桶或现有存储桶中的新数据，然后根据分配的数据分类标签验证数据。配置此架构，以便及时将错误分类或未分类的存储桶通知相应的开发和隐私团队。

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 — 日志存档帐户

我们很乐意听取你的意见。请通过[简短的调查](#)提供 AWS 有关 PRA 的反馈。

在日志存档帐户中，您可以集中管理基础架构、服务和应用程序日志类型。有关此帐户的更多信息，请参阅[AWS 安全参考架构 \(AWS SRA\)](#)。使用日志专用帐户，您可以对所有日志类型应用一致的警报，并确认事件响应者可以从一个地方访问这些日志的汇总。您也可以从一个地方设置安全控制和数据保留策略，这可以简化隐私操作开销。下图说明了在日志存档帐户中配置 AWS 的安全和隐私服务。



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。

根据贵组织对个人数据的定义和适用的地区隐私法规，您可能需要考虑跨境数据传输。如果您的组织需要满足地区隐私法规对数据传输的要求，则以下选项可以提供支持：

1. 如果您的组织 AWS Cloud 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中的 S3 存储桶中，eu-central-1 AWS 区域 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。

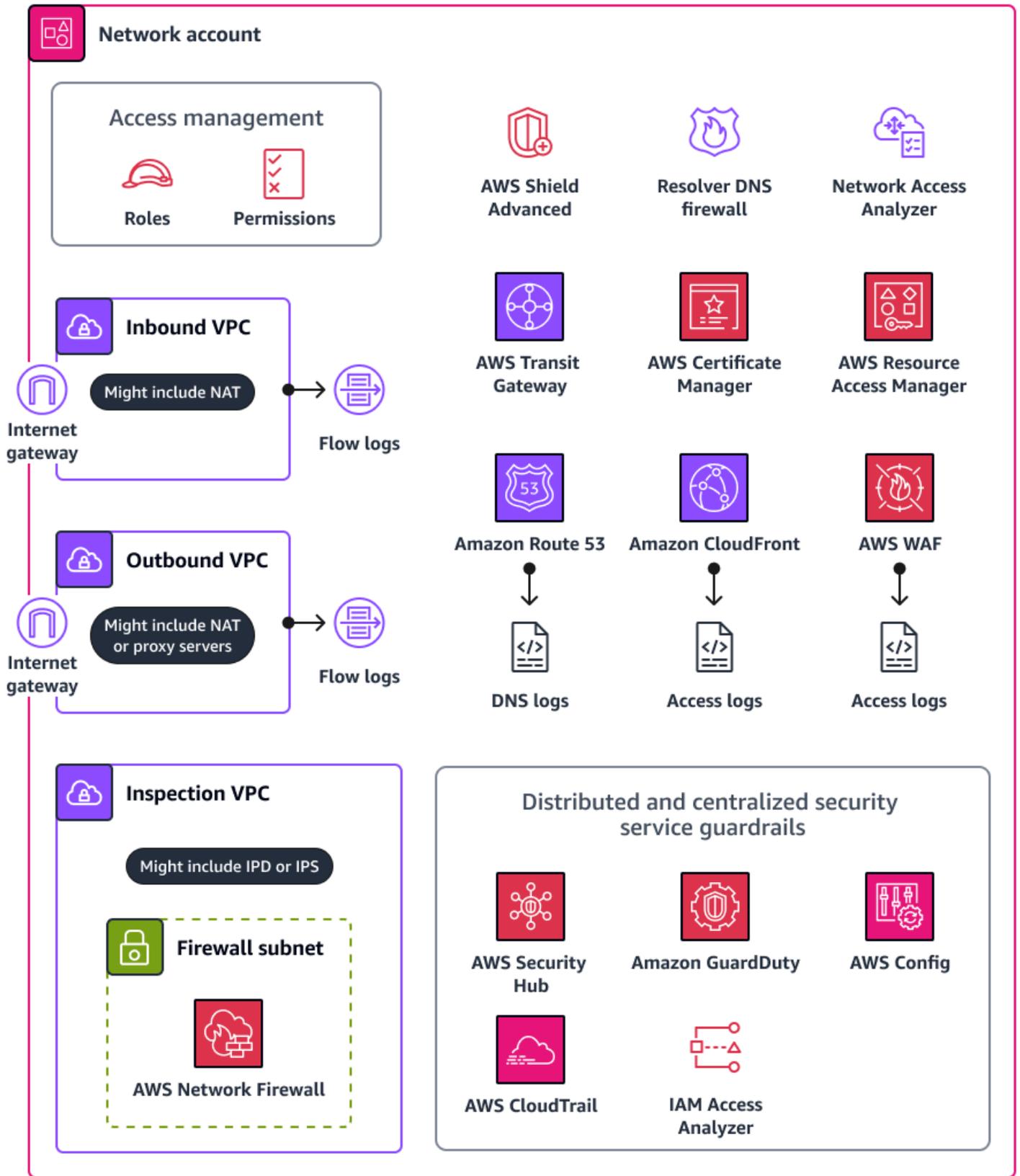
2. 在将数据复制并汇总到其他区域 AWS 区域 之前，请先编辑需要保留的个人数据。例如，在将日志传输到其他区域之前，您可以屏蔽应用程序宿主区域中的个人数据。有关屏蔽个人数据的更多信息，请参阅本指南的[Amazon Data Firehose](#)部分。

与您的法律顾问合作，确定哪些个人数据在范围内，以及允许哪些 AWS 区域间传输。

基础设施 OU – 网络账户

我们很乐意听取你的意见。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 (VPC) 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。



本节提供有关此账户中 AWS 服务 使用的以下内容的更多详细信息：

- [Amazon CloudFront](#)
- [AWS Resource Access Manager](#)
- [AWS Transit Gateway](#)
- [AWS WAF](#)

Amazon CloudFront

[Amazon CloudFront](#) 支持对前端应用程序和文件托管进行地理限制。CloudFront 可以通过全球数据中心网络 (称为边缘站点) 交付内容。当用户请求与您一起提供的内容时 CloudFront, 该请求会被路由到延迟最低的边缘站点。有关如何在安全环境中使用此服务的更多信息, 请参阅[AWS 安全参考架构](#)。

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。如果您使用与其他 AWS RAM 人共享数据平面连接 AWS 账户, 请考虑建立流程以检查连接是否已获得预先批准 AWS 区域。

除了共享 VPC 和公交网关连接外, 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[AWS Resource Access Manager 个人数据 OU — PD 申请账户部分](#)。

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。在控制层面, 您可以使用 IAM 和服务控制策略限制区域使用量, 从而限制跨区域数据流。

有多种选项可用于控制数据平面上的跨区域数据流。例如, 您可以使用路由表、VPC 对等互连和 AWS Transit Gateway 附件。[AWS Transit Gateway](#) 是连接虚拟私有云 (VPC) 和本地网络的中心枢纽。作为

更大的 AWS landing 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、直接 VPC 到 VPC 对等以及通过区域间对等。AWS Transit Gateway 例如，您可以在中执行以下操作 AWS Transit Gateway：

- 确认您的 VPC 和本地环境之间的东西向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。有关服务控制策略的示例，请参阅本指南[限制对 VPC 配置的更改](#)中的。

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。有关如何在安全环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。以下活动可能与意外披露个人数据有关：

- 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，包括与泄露相关的攻击](#)，例如 SQL 注入
- 请求率高
- 一般机器人流量
- 内容抓取器

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 数据库利用相关的请求模式（例如 SQL 注入攻击）的规则。如果您的应用程序与 SQL 数据库接口，请考虑使用此规则组。
- [已知的错误输入](#)-此规则组包含旨在阻止已知无效且与漏洞利用或发现相关的请求模式的规则。
- [Bot Control](#) — 此规则组包含旨在管理来自机器人的请求的规则，这些请求可能会消耗多余资源、歪曲业务指标、导致停机时间和执行恶意活动。
- [防止账户盗用 \(ATP\)](#)-此规则组包含旨在防止恶意账户盗用企图的规则。此规则组检查发送到应用程序登录端点的登录尝试。

个人数据 OU — PD 申请账户

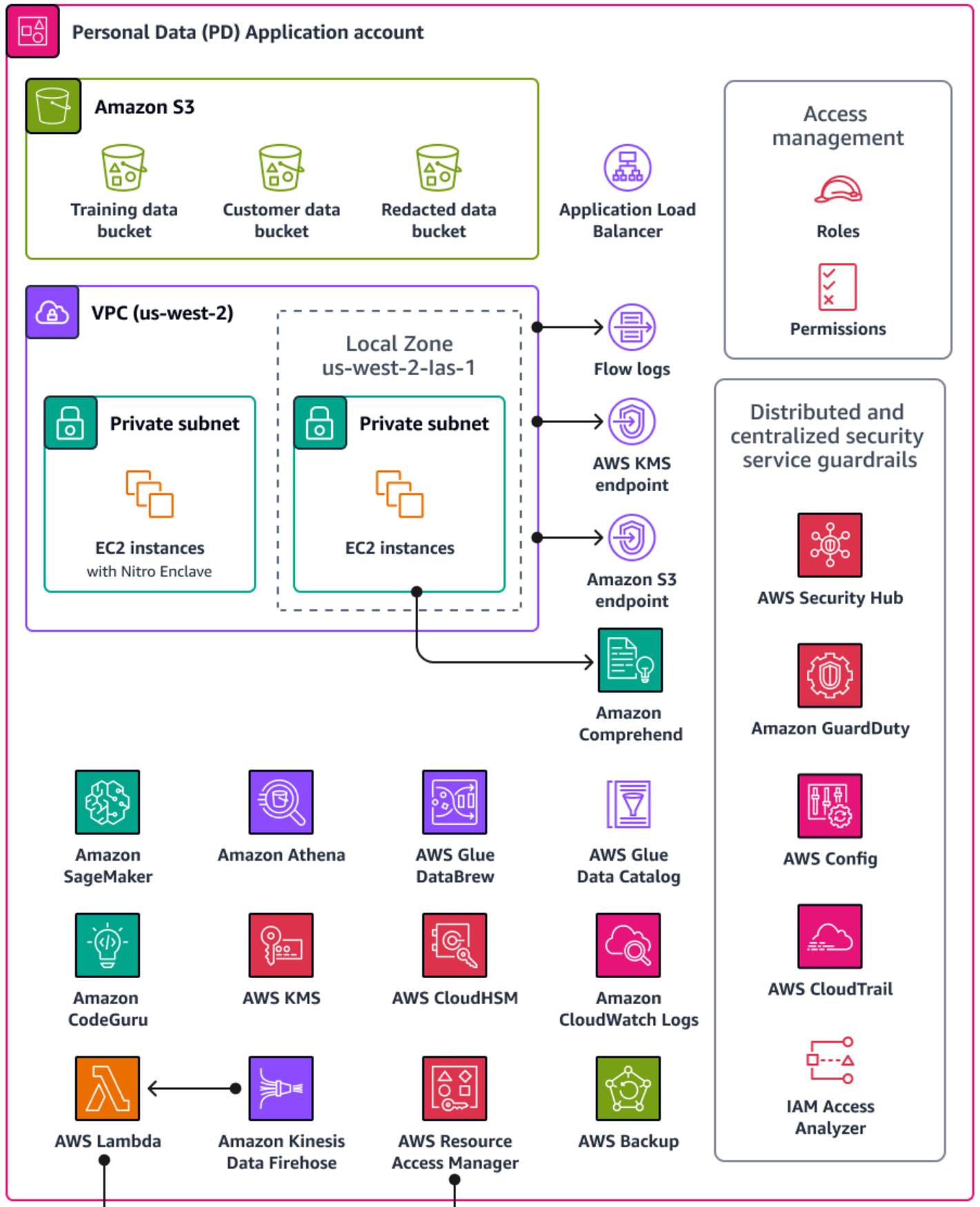
我们很乐意听取你的意见。请通过[简短的调查](#)提供 AWS 有关 PRA 的反馈。

个人数据 (PD) 应用程序账户是贵组织托管收集和处理个人数据的服务的地点。具体而言，您可以在此账户中存储您定义的个人数据。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，您的目标可能是了解基本概念，它们如何增强隐私，以及您的组织如何将解决方案应用于您的特定用例和架构。

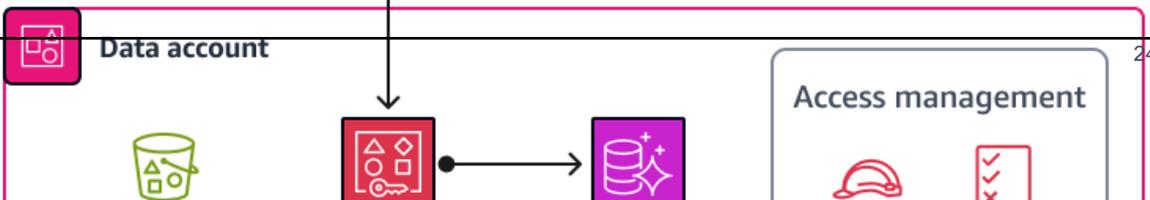
对于 AWS 账户 在收集、存储或处理个人数据的组织中，您可以使用 AWS Organizations 和 AWS Control Tower 部署基础且可重复的护栏。为这些客户设立专门的组织单位 (OU) 至关重要。例如，您可能只想将数据驻留保护措施应用于以数据驻留为核心设计考虑因素的一部分客户。对于许多组织来说，这些账户用于存储和处理个人数据。

您的组织可能支持专用的数据帐户，您可以在该帐户中存储个人数据集的权威来源。权威数据源是您存储数据主版本的位置，该版本可能被认为是最可靠、最准确的数据版本。例如，您可以将数据从权威数据源复制到其他位置，例如 PD 应用程序账户中的 Amazon Simple Storage Service (Amazon S3) 存储桶，用于存储培训数据、客户数据子集和经过编辑的数据。通过采用这种多账户方法将数据账户中完整且明确的个人数据集与 PD Application 账户中的下游消费者工作负载分开，可以缩小账户遭到未经授权访问时的影响范围。

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。



个人数据 OU — PD 申请账户



本节提供有关这些账户中 AWS 服务 使用的以下内容的更多详细信息：

- [Amazon Athena](#)
- [Amazon CloudWatch 日志](#)
- [Amazon CodeGuru Reviewer](#)
- [Amazon Comprehend](#)
- [Amazon Data Firehose](#)
- [AWS Glue](#)
- [AWS Key Management Service](#)
- [AWS Local Zones](#)
- [AWS Nitro 飞地](#)
- [AWS PrivateLink](#)
- [AWS Resource Access Manager](#)
- [Amazon SageMaker](#)
- [AWS 有助于管理数据生命周期的功能](#)
- [有助于对数据进行细分的 AWS 服务和功能](#)

Amazon Athena

您也可以考虑控制数据查询限制，以实现您的隐私目标。[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。您不必将数据加载到 Athena；它可以直接处理存储在 S3 存储桶中的数据。

Athena 的一个常见用例是为数据分析团队提供量身定制和经过清理的数据集。如果数据集包含个人数据，则可以通过屏蔽对数据分析团队几乎没有价值的整列个人数据来对数据集进行消毒。有关更多信息，请参阅使用 [Amazon 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在 [Athena 支持的函数](#) 之外获得额外的灵活性，则可以定义自定义函数，[称为用户定义函数 \(UDF\)](#)。您可以在提交给 Athena 的 SQL 查询中调用 UDF，它们就会继续运行。AWS Lambda 可以在 SELECT 和 FILTER SQL 查询中使用 UDF，也可以在同一个查询中调用多个 UDF。为了保护隐私，您可以创建执行特定类型数据屏蔽的 UDF，例如仅显示列中每个值的最后四个字符。

Amazon CloudWatch 日志

[Amazon CloudWatch Logs](#) 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。当用户通过访问日志时，数据保护策略可以屏蔽这些数据 AWS Management Console。当用户需要直接访问个人数据时，根据工作负载的总体目的规范，您可以为这些用户分配 `logs:Unmask` 权限。您还可以创建全账户的数据保护政策，并将该政策一致地应用于组织中的所有账户。默认情况下，这将为 Logs 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并将其发送到另一个日志组、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结果的详细记录。

Amazon CodeGuru Reviewer

对于隐私和安全而言，许多组织在部署和部署后阶段都必须支持持续的合规性，这一点至关重要。AWS PRA 在部署管道中包括针对处理个人数据的应用程序的主动控制。[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 Reviewer 可以识别各种安全、隐私和一般最佳实践中的缺陷。有关更多信息，请参阅 [Amazon CodeGuru 探测器库](#)。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
- 不安全的饼干
- 缺少授权
- 客户端重新 AWS KMS 加密

Amazon Comprehend

[Amazon Comprehend](#) 是一项自然语言处理 (NLP) 服务，它使用机器学习来发现英文文本文档中的宝贵见解和联系。Amazon Comprehend 可以检测和编辑结构化、半结构化或非结构化文本文档中的个人数据。有关更多信息，请参阅亚马逊 Comprehend 文档中的[个人信息 \(PII\)](#)。

您可以使用 AWS 软件开发工具包和亚马逊 Comprehend API 将 Amazon Comprehend 与许多应用程序集成。例如，使用 Amazon Comprehend 使用亚马逊 S3 Object Lambda 检测和编辑个人数据。组织可以使用 S3 Object Lambda 向 Amazon S3 GET 请求添加自定义代码，以便在数据返回到应用程序时对其进行修改和处理。S3 Object Lambda 可以筛选行、动态调整图像大小、编辑个人数据等。代码由 AWS Lambda 函数提供支持，在完全由管理的基础架构上运行 AWS，因此无需创建和存储数

据的衍生副本或运行代理。您无需更改应用程序即可使用 S3 Object Lambda 转换对象。您可以使用中的 `ComprehendPiiRedactionS3Object` Lambda 函数 AWS Serverless Application Repository 来编辑个人数据。此功能使用 Amazon Comprehend 来检测个人数据实体，并通过用星号替换这些实体来对其进行编辑。有关更多信息，请参阅 [Amazon S3 文档中的使用 S3 对象 Lambda 和 Amazon Comprehend 检测和编辑 PII 数据](#)。

由于 Amazon Comprehend 有许多通过 AWS 软件开发工具包进行应用程序集成的选项，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。亚马逊 Comprehend 提供两种编辑模式：

- `REPLACE_WITH_PII_ENTITY_TYPE` 用其类型替换每个 PII 实体。例如，Jane Doe 将被替换为 NAME。
- `MASK` 用您选择的角色替换 PII 实体中的字符 (!、#、\$、%、&、或 @)。例如，Jane Doe 可以替换为 **** *。

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，例如适用于 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，而不必从头开始构建处理管道。

在将数据发送到下游之前，您可以使用 Lambda 函数执行自定义或内置处理。为了保护隐私，此功能支持数据最小化和跨境数据传输要求。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 函数转换日志并将其发送到日志存档账户中的中央 S3 存储桶。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境传输 AWS 区域。通过使用这种方法，个人数据在传输和集中化之前被屏蔽，而不是在传输和集中之后。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 [AWS CloudTrail](#) 本指南的“安全 OU-安全工具帐户”部分。

AWS Glue

维护包含个人数据的数据集是“[设计隐私](#)”的关键组成部分。组织的数据可能以结构化、半结构化或非结构化形式存在。没有结构的个人数据集可能会使执行许多增强隐私的操作变得困难，包括数据最小化、追踪作为数据主体请求的一部分归因于单个数据主体的数据、确保一致的数据质量以及对数据集

进行整体细分。[AWS Glue](#)是一项完全托管的提取、转换和加载 (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 and 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](#)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。数据目录中的信息存储为元数据表，每个表指定一个数据存储。您可以运行 AWS Glue 爬虫程序来清点各种数据存储类型的数据。您将[内置和自定义分类器](#)添加到爬虫中，这些分类器会推断出个人数据的数据格式和架构。然后，爬虫程序将元数据写入数据目录。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，如果您的组织使用管理和[AWS Lake Formation](#)提供跨数据库、表、行和单元格的精细访问权限，则数据目录是一个关键组件。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)。

AWS Glue DataBrew

[AWS Glue DataBrew](#)帮助您清理和规范化数据，还可以对数据进行转换，例如删除或屏蔽个人身份信息以及加密数据管道中的敏感数据字段。您还可以直观地映射数据的谱系，以了解数据所经历的各种数据源和转换步骤。随着您的组织努力更好地了解 and 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。作为数据分析工作的一部分，您可以检测个人数据并收集统计信息，例如可能包含个人数据的列数和潜在类别。然后，您可以使用内置的可逆或不可逆数据转换技术，包括替换、哈希、加密和解密，所有这些都无需编写任何代码。然后，您可以使用下游经过清理和屏蔽的数据集来执行分析、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。
- 替换-用其他外观真实的值替换个人数据。
- 清空或删除-将特定字段替换为空值，或删除该列。
- 屏蔽-使用字符乱码，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。确定性加密总是为值生成相同的密文。
- 概率加密-对列值应用概率加密算法。概率加密每次应用时都会生成不同的密文。

有关提供的个人数据转换方法的完整列表 DataBrew，请参阅[个人信息 \(PII\) 配方步骤](#)。

AWS Glue 数据质量

[AWS Glue Data Quality](#) 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交付的自动化和操作。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 \(AWS KMS\)](#) 可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。有关如何在安全环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[客户托管的密钥](#)可以更好地控制强度、轮换、到期时间和其他选项。
- 使用专用的客户托管密钥来保护允许访问个人数据的个人数据和机密。
- 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托管密钥。例如，您可能有一个用于加密操作数据的密钥和另一个用于加密个人数据的密钥。
- 防止跨账户意外访问 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 密钥的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)。
- 通过预防性和反应性护栏强制自动轮换密钥。

默认情况下，KMS 密钥是存储的，并且只能在创建密钥的区域中使用。如果您的组织对数据驻留和主权有特定要求，请考虑[多区域 KMS 密钥](#)是否适合您的用例。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，因此这种缺乏区域隔离可能与您组织的合规目标不符。解决这个问题的一种方法是使用不同类型的 KMS 密钥，例如特定于区域的客户托管密钥。

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

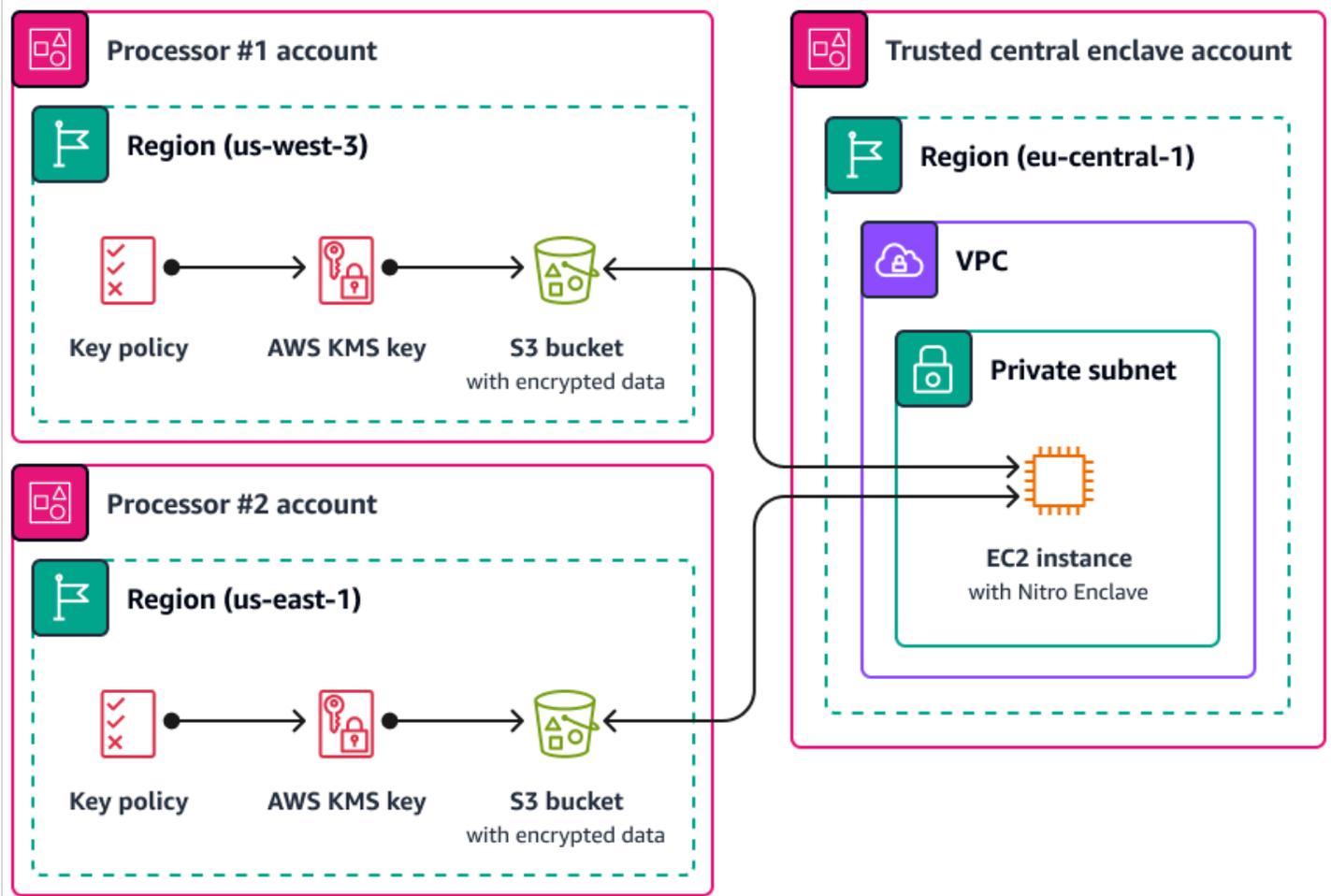
在靠近人口众多和工业中心的地方。局部区域是地理上靠近大型都市区的延伸。AWS 区域 您可以将特定类型的资源放置在本地区域内，靠近本地区域对应的区域。当某个区域在同一法律管辖区内不可用时，Local Zones 可以帮助您满足数据驻留要求。使用 Local Zones 时，请考虑在组织内部署的数据驻留控制。例如，您可能需要一个控件来防止数据从特定的本地区域传输到另一个区域。有关如何使用 SCP 维护跨境数据传输护栏的更多信息，请参阅使用[着陆区控制管理 AWS 本地区域数据驻留的最佳实践](#) (AWS 博客文章)。

AWS Nitro 飞地

从处理的角度考虑您的数据分段策略，例如使用诸如亚马逊弹性计算云 (Amazon EC2) 之类的计算服务处理个人数据。作为更大架构策略一部分的机密计算可以帮助您将个人数据处理隔离在隔离、受保护和可信的 CPU 飞地中。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，可以帮助您创建这些隔离的计算环境。有关更多信息，请参阅[AWS Nitro 系统的安全设计](#) (AWS 白皮书)。

Nitro Enclaves 部署的内核与父实例的内核分开。父实例的内核无权访问安全区。用户无法通过 SSH 或远程访问安全区中的数据 and 应用程序。处理个人数据的应用程序可以嵌入到安全区中，并配置为使用安全区的 [Vsock](#)，该套接字可以促进安全区与父实例之间的通信。

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。下图显示了如何使用安全区进行中央处理、使用 KMS 密钥在将个人数据发送到安全区之前对其进行加密，以及用于验证请求解密的飞地在其认证文档中是否具有唯一测量值的 AWS KMS key 策略。有关更多信息和说明，请参阅[使用加密认证](#)。AWS KMS 有关密钥策略的示例，请参阅本指南[需要认证才能使用密钥 AWS KMS](#)中的。



通过这种实现，只有相应的数据处理者和底层飞地才能访问纯文本个人数据。在相应数据处理器的环境之外，唯一暴露数据的位置是安全区本身，该安全区旨在防止访问和篡改。

AWS PrivateLink

许多组织都希望限制向不可信的网络泄露个人数据。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[有助于对数据进行细分的 AWS 服务和功能](#)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 (VPC) 到 VPC 外部服务的单向私有连接。使用 AWS PrivateLink，您可以与在您的环境中存储或处理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受信任的公共网络传输这些数据。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[需要组织成员才能访问 VPC 资源](#)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该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 ID 列表
- 如果消费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 委托人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 [PromoteResourceShareCreatedFromPolicy](#) API 操作。

Amazon SageMaker

[Amazon SageMaker](#) 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 旨在更轻松地准备训练数据和创建模型特征。

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。数据漂移是生产数据和用于训练机器学习模型的数据之间的有意义的差异，或者是输入数据随时间的推移而发生的有意义的变化。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。如果机器学习模型在生产中接收的数据的统计性质偏离了其训练所依据的基线数据的性质，则预测的准确性可能会下降。[Amazon SageMaker Model Monitor](#) 可以持续监控生产中的亚马逊 SageMaker 机器学习模型的质量并监控数据质量。尽早主动检测数据漂移可以帮助您实施纠正措施，例如再训练模型、审计上游系统或修复数据质量问题。Model Monitor 可以减少手动监控模型或构建其他工具的需求。

亚马逊 SageMaker 澄清

[Amazon 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，CI 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 可以标记失衡，这样您就可以避免使用不利于该年龄组的模型。您可以通过查看已训练模型的预测以及持续监控这些机器学习模型的偏差，来检查其是否存在偏差。最后，CI SageMaker arify 与 [Amazon SageMaker Experiments](#) 集成，提供了一个图表，解释了哪些特征对模型的整体预测过程贡献最大。这些信息对于实现可解释性结果可能很有用，它可以帮助您确定特定模型输入对模型整体行为的影响是否超过应有的影响力。

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。这些详细信息可能包括模型所有者、一般用途、预期用例、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)。

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。配置数据保留策略时，请考虑以下可能包含个人数据的位置：

- 数据库，例如亚马逊 DynamoDB 和亚马逊关系数据库服务 (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 应用于一组对象的操作。在 Amazon S3 生命周期配置中，您可以创建过期操作，这些操作定义了 Amazon S3 何时代表您删除过期对象。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 支持的亚马逊系统映像 (AMI) 的策略。
- [DynamoDB 存活时间 \(TTL\)](#) - 定义每个项目的时间戳，该时间戳决定何时不再需要某个项目。在指定时间戳的日期和时间过后不久，DynamoDB 就会从您的表中删除该项目。

- [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。通过集中式控制台审核和报告备份活动，以帮助满足备份合规性要求。

有助于对数据进行细分的 AWS 服务和功能

数据分段是将数据存储在不同的容器中的过程。这可以帮助您为每个数据集提供不同的安全性和身份验证措施，并缩小暴露对整个数据集的影响范围。例如，您可以将这些数据分成更小、更易于管理的组，而不是将所有客户数据存储在一个大型数据库中。

您可以使用物理和逻辑分离来分割个人数据：

- **物理分离** — 将数据存储在不同的数据存储中或将数据分发到单独的 AWS 资源中的行为。尽管数据在物理上是分开的，但相同的主体可能可以访问这两种资源。这就是为什么我们建议将物理分离与逻辑分离相结合。
- **逻辑分离**-使用访问控制来隔离数据的行为。不同的工作职能要求对个人数据子集访问权限各不相同。有关实现逻辑分离的示例策略，请参阅本指南[授予对特定亚马逊 DynamoDB 属性的访问权限](#)中的。

在编写基于身份和基于资源的策略以支持跨工作职能的差异访问权限时，逻辑和物理分离相结合，提供了灵活性、简单性和精细度。例如，在单个 S3 存储桶中创建在逻辑上分隔不同数据分类的策略在操作上可能很复杂。为每种数据分类使用专用 S3 存储桶可简化策略配置和管理。

隐私相关政策示例

我们很乐意听取你的意见。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前瞻性方法，自始至终都实施了多层侦查和被动控制。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 这些政策可以采用预防性方法，帮助您的组织实现各种使用、披露限制和跨境数据传输隐私目标。本指南的前几节中提到了其中许多政策。

本节包含以下示例策略：

- [需要从特定 IP 地址进行访问](#)
- [需要组织成员才能访问 VPC 资源](#)
- [限制跨数据传输 AWS 区域](#)
- [授予对特定亚马逊 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](#)

需要从特定 IP 地址进行访问

我们很乐意听取你的意见。请通过[简短的调查](#)提供 AWS 有关 PRA 的反馈。

只有当呼叫来自 192.0.2.0/24 或范围内的 IP 地址时，此策略才允许 john_styles 用户担任 IAM 角色 203.0.113.0/24。该政策可以帮助防止意外泄露个人数据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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_styles"
      }
    }
  ]
}
```

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

需要组织成员才能访问 VPC 资源

我们很乐意听取你的意见。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。有关本政策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 [AWS PrivateLink](#) 中的。

```
{
  "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

我们很乐意听取你的意见。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，是因为它考虑了 [全球 AWS 服务](#)（例如 IAM）和与全球服务集成的服务，例如 AWS Key Management Service (AWS KMS) 和 Amazon CloudFront。在参数值中，您可以将这些全球服务和其他不适用的服务指定为例外。有关本政策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 [AWS Organizations](#) 中的。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutsideEU",
      "Effect": "Deny",
      "NotAction": [
        "a4b:*",
        "acm:*",
        "aws-marketplace-management:*",
        "aws-marketplace:*",
        "aws-portal:*",
        "budgets:*",
        "ce:*",
        "chime:*",
        "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"
      ]
    }
  }
}

```

```
    ]
  }
}
]
```

授予对特定亚马逊 DynamoDB 属性的访问权限

我们很乐意听取你的意见。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的 Amazon DynamoDB 表中检索 UserIDSignUpTime、和 LastLoggedIn 属性。Users 例如，您可以将此政策附加到客户支持角色，而不是授予该角色访问完整个人数据集的权限。有关本政策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[有助于对数据进行细分的 AWS 服务和功能](#)中的。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:GetItem",
        "dynamodb:BatchGetItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:TransactGetItems"
      ],
      "Resource": [
        "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
      ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "dynamodb:Attributes": [
            "UserID",
            "SignUpTime",
            "LastLoggedIn"
          ]
        }
      }
    }
  ]
}
```

```
    },
    "StringEquals": {
      "dynamamodb:Select": [
        "SPECIFIC_ATTRIBUTES"
      ]
    }
  }
}
]
```

限制对 VPC 配置的更改

我们很乐意听取你的意见。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 配置偏差或意外修改。它拒绝新的互联网网关附件、VPC 对等连接、传输网关连接和新的 VPN 连接。有关本政策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[AWS Transit Gateway](#)中的。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:AttachEgressOnlyInternetGateway",
        "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

我们很乐意听取你的意见。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。此策略仅允许受信任的飞地解密数据。有关本政策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[AWS Nitro 飞地](#)中的。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":
"EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef0abcdef1abcdEXAMPLE",
        "kms:RecipientAttestation:PCR0":
"EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfd36c08b2c79552928702EXAM",
        "kms:RecipientAttestation:PCR1":
"EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbec2e2ec1bf0b4ae749d311c663f464cde9f718aEXAM",
        "kms:RecipientAttestation:PCR2":
"EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM",
        "kms:RecipientAttestation:PCR3":
"EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM",
        "kms:RecipientAttestation:PCR4":
"EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM",
        "kms:RecipientAttestation:PCR8":
"EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM"
      }
    }
  ]
}
```

资源

我们很乐意听取你的意见。请通过[简短的调查](#)提供 AWS 有关 PRA 的反馈。

AWS 规范性指导

- [AWS 安全参考架构 \(AWS SRA\)](#)

AWS 文档

- [数据保护](#) (Well-Architect AWS ed Framework)
- [数据分类](#) (AWS 白皮书)
- [Amazon Web Services : 风险与合规](#) (AWS 白皮书)
- [满足@@ 个人数据处理要求的混合架构](#) (AWS 白皮书)
- [浏览 GDPR 合规性 AWS](#) (AWS 白皮书)
- [在 AWS \(AWS 白皮书 \) 上构建数据边界](#)
- [AWS 安全文档](#)

其他 AWS 资源

- [AWS 合规计划](#)
- [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 数字主权承诺 : 毫不妥协的控制](#) (AWS 博客文章)
- [AWS 安全学习](#)

贡献者

我们很乐意听取你的意见。请通过[简短的调查](#)提供 AWS 有关 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

- 丹尼尔·尼特斯，AWS 首席隐私顾问
- Amber Welch，AWS 高级隐私顾问
- 罗伯特·卡特，AWS 技术项目经理

贡献者

- Avik Mukherjee，高级安全顾问 AWS
- David Bounds，AWS 高级解决方案架构师
- 杰夫·隆巴多，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
- 凡妮莎·雅各布斯，高级安全顾问 AWS

文档历史记录

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

变更	说明	日期
重要更新	我们自始至终都进行了重大更新。	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：将您的本地 Oracle 数据库迁移到 SQL 兼容 Amazon Aurora Postgre 的版本。
- **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：将您的本地 Oracle 数据库迁移到适用于 Oracle 的 Amazon Relational Database Service (AmazonRDS) AWS Cloud。
- **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：将您的客户关系管理 (CRM) 系统迁移到 Salesforce.com。
- **更换主机 (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：在中的 EC2 实例上将您的本地 Oracle 数据库迁移到 Oracle AWS Cloud。
- **重新定位 (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。您可以将服务器从本地平台迁移到同一平台的云服务。示例：迁移 Microsoft Hyper-V 应用到 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

参见[托管服务](#)。

ACID

参见[原子性、一致性、隔离性、耐久性](#)。

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。与[主动-被动迁移](#)相比，它更灵活，但需要更多的工作。

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

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

AI

参见[人工智能](#)。

AIOps

参见[人工智能操作](#)。

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、耐久性 () 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，[ABAC](#) 请参阅 AWS Identity and Access Management (IAM) 文档 AWS 中的。

权威数据源

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

坏机器人

旨在破坏个人或组织或对其造成伤害的[机器人](#)。

BCP

参见[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。您可以在 Amazon Detective 中使用行为图来检查登录尝试失败、可疑API呼叫和类似操作。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。另请参见[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的应用程序版本（蓝色），在另一个环境中运行新的应用程序版本（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互动的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的网络爬虫。其他一些被称为恶意机器人的机器人旨在破坏个人或组织或对其造成伤害。

僵尸网络

被[恶意软件](#)感染并受单方（称为[机器人](#)牧民或机器人操作员）控制的机器人网络。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）。

破碎的玻璃通道

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 [Well -Architected 指南](#) 中的“[实施破碎玻璃程序](#)”指示 AWS 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

参见[AWS 云采用框架](#)。

金丝雀部署

向最终用户缓慢而渐进地发布版本。当你有信心时，你可以部署新版本并全部替换当前版本。

CCoE

参见[云卓越中心](#)。

CDC

参见[变更数据捕获](#)。

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CDC用于各种用途，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弹性。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

查看[持续集成和持续交付](#)。

分类

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

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心 (CCoE)

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

云计算

通常用于远程数据存储和 IoT 设备管理的云技术。云计算通常与[边缘计算](#)技术相关。

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

组织迁移到以下阶段时通常会经历四个阶段 AWS Cloud：

- 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CCoE、建立运营模型）

- 迁移 - 迁移单个应用程序
- 重塑 - 优化产品和服务，在云中创新

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

CMDB

参见[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 或者 Bitbucket Cloud。每个版本的代码都称为分支。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 管道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)

[人工智能](#)领域，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，AWS Panorama 提供将 CV 添加到本地摄像机网络的设备，而 Amazon 则为 CV SageMaker 提供图像处理算法。

配置偏差

对于工作负载，配置会从预期状态发生变化。这可能会导致工作负载变得不合规，而且通常是渐进的，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。您通常使用来自投资组合CMDB中的迁移发现和分析阶段的数据。

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模板将合规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 is commonly described as a pipeline. 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

参见[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-Architected AWS d Framework 中安全支柱的一个组成部分。有关详细信息，请参阅[数据分类](#)。

数据漂移

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

传输中数据

在网络中主动移动的数据，例如在网络资源之间移动的数据。

数据网格

一种架构框架，可提供分布式、去中心化的数据所有权以及集中式管理和治理。

数据最少化

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

数据边界

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

数据预处理

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

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

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

数据库定义语言 (DDL)

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言 (DML)

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

参见[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。

委托管理员

在中 AWS Organizations，兼容的服务可以注册 AWS 成员帐户来管理组织的帐户并管理该服务的权限。此帐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

参见[环境](#)。

侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出警报。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

在[星型架构](#)中，一种较小的表，其中包含事实表中有关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)

您用来最大限度地减少[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 Framework AWS work 中的[“工作负载灾难恢复：云端 AWS 恢复”](#)。

DML

参见[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。[有关如何使用带有 strangler fig 模式的域驱动设计的信息，请参阅对旧版 Microsoft 进行现代化改造。ASP NET\(ASMX\) 通过使用容器和 Amazon API Gateway 逐步提供网络服务。](#)

DR

参见[灾难恢复](#)。

漂移检测

跟踪与基线配置的偏差。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

参见[开发价值流映射](#)。

E

EDA

参见[探索性数据分析](#)。

EDI

参见[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](#)相比，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)

组织之间自动交换业务文档。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密文的计算过程。

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

参见[服务端点](#)。

端点服务

您可以托管在虚拟私有云 (VPC) 中与其他用户共享的服务。您可以使用其他 AWS 账户 或 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。这些账户或委托人可以通过创建接口终端节点私密连接到您的终VPC端节点服务。有关更多信息，请参阅 Amazon Virtual Private Cloud (AmazonVPC) 文档中的[创建终端节点服务](#)。

企业资源规划 (ERP)

一种自动化和管理企业关键业务流程（例如会计和项目管理）的系统。[MES](#)

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](#)。

environment

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

参见[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 是通过计算汇总统计数据和创建数据可视化来执行的。

F

事实表

[星形架构](#)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。

失败得很快

一种使用频繁和增量测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

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

功能分支

参见[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。这通常表示为数字分数，可以通过各种技术进行计算，例如 Shapley Additive Explanations (SHAP) 和积分梯度。有关更多信息，请参阅[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。

few-shot 提示

在要求 LLM 其执行类似任务之前，提供少量示例，演示该任务和所需的输出。这种技术是情境学习的应用，模型可以从提示中嵌入的示例（镜头）中学习。对于需要特定格式、推理或领域知识的任务，Few-shot 提示可能非常有效。另请参见[零镜头提示](#)。

FGAC

请参阅[精细的访问控制](#)。

精细的访问控制 () 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，它使用连续的数据复制，通过[更改数据捕获](#)在尽可能短的时间内迁移数据，而不是使用分阶段的方法。目标是将停机时间降至最低。

FM

参见[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

[人工智能](#)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工件，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 AI](#)。

地理封锁

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 , 而[基于主干的工作流程](#)是现代的首选方法。

金色影像

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配置软件 , 并有助于提高设备制造运营的速度、可扩展性和生产力。

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

一项高级规则 , 可帮助管理各组织单位的资源、策略和合规性 (OUs)。预防性防护机制会执行策略以确保符合合规性标准。它们通过使用服务控制策略和IAM权限边界来实现。侦测性防护机制会检测策略违规和合规性问题 , 并生成警报以进行修复。它们通过使用 AWS Config、Amazon、AWS Security Hub GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

H

HA

参见[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。

抵制数据

从用于训练[机器学习](#)模型的数据集中扣留的一部分带有标签的历史数据。通过将模型预测与抵制数据进行比较，您可以使用抵制数据来评估模型性能。

同构数据库迁移

将您的源数据库迁移到共享相同数据库引擎的目标数据库（例如，将 Microsoft SQL Server 迁移到 Amazon RDS 或 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。

hypercure 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 hypercure 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。

I

IaC

参见[基础架构即代码](#)。

基于身份的策略

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

空闲应用程序

一种在 90 天内平均使用率 CPU 和内存使用率介于 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。

IloT

参见 [工业物联网](#)。

不可变的基础架构

一种为生产工作负载部署新基础架构，而不是更新、修补或修改现有基础架构的模型。[不可变基础架构本质上比可变基础架构更一致、更可靠、更可预测](#)。有关更多信息，请参阅 Well-Architected Framework 中的 [使用不可变基础架构 AWS 部署最佳实践](#)。

入站 (入口) VPC

在 AWS 多账户架构中 VPC，接受、检查和路由来自应用程序外部的网络连接。[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 [克劳斯·施瓦布 \(Klaus Schwab \)](#) 于 2016 年推出，指的是通过连接、实时数据、自动化、分析和人工智能/机器学习的进步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置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 (IloT)

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 [构建工业物联网 \(IloT\) 数字化转型战略](#)。

检查 VPC

在 AWS 多账户架构中，VPC 一种集中式管理 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](#)。

IoT

参见 [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 为... 提供了基础 ITSM。

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。有关将云操作与 ITSM 工具集成的信息，请参阅[操作集成指南](#)。

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) 的实现，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](#)。

大型语言模型 (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，请参阅文档中的[应用最低权限权限](#)。IAM

直接迁移

见 [7 R](#)。

小端序系统

一个先存储最低有效字节的系统。另请参见[字节顺序](#)。

LLM

参见[大型语言模型](#)。

下层环境

参见[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

参见[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。恶意软件的示例包括病毒、蠕虫、勒索软件、特洛伊木马、间谍软件和键盘记录器。

托管服务

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。亚马逊简单存储服务 (Amazon S3) Service 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、记录和控制将原材料转化为成品的生产过程。

MAP

参见[迁移加速计划](#)。

机制

一个完整的过程，在此过程中，您可以创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运行过程中自我增强和改进的循环。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

参见[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

Migration 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 包括一种以有条不紊的方式执行遗留迁移的迁移方法，以及一组用于自动化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 DevOps 人员和冲刺专业人员。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：EC2 使用 AWS 应用程序迁移服务重新托管向 Amazon 的迁移。

迁移组合评估 (MPA)

一种在线工具，可提供信息，用于验证迁移到的业务案例。AWS Cloud MPA 提供详细的产品组合评估（服务器规模调整、定价、TCO 比较、迁移成本分析）以及迁移规划（应用程序数据分析和数据收集、应用程序分组、迁移优先级划分和波浪规划）。所有 AWS 顾问和 APN 合作伙伴顾问均可免费使用该[MPA 工具](#)（需要登录）。

迁移准备情况评估 (MRA)

使用以下方法获取有关组织云就绪状态的见解、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 AWS CAF。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

用于将工作负载迁移到的方法 AWS Cloud。有关更多信息，请参阅此词汇表中的 [7 R](#) 条目和[动员组织以加快大规模迁移](#)。

ML

参见[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[中的应用程序现代化策略](#)。AWS Cloud

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[中的评估应用程序的现代化准备情况](#) AWS Cloud。

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

参见[迁移组合评估](#)。

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？”

可变基础架构

一种用于更新和修改现有生产工作负载基础架构的模型。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[源站访问控制](#)。

OAI

参见[源访问身份](#)。

OCM

参见[组织变更管理](#)。

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

参见[运营集成](#)。

OLA

参见[运营层协议](#)。

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

参见[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 提供数据加密、身份验证和授权方案的互操作性标准。

运营层协议 () OLA

一项协议，阐明 IT 职能部门承诺相互提供哪些服务，以支持服务级别协议 () SLA。

操作准备情况审查 (ORR)

一份问题清单和相关的最佳实践，可帮助您理解、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 Well-Architecte AWS d Frame [ORRwork 中的运营准备情况评估 \(\)](#)。

操作技术 (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并过渡到新系统和战略。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](#)。

源站访问控制 (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) 的服务器端加密以及对 S3 存储桶的动态PUT和DELETE请求。

源站访问身份 (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。使用时OAI，CloudFront 会创建 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](#)，它提供了更精细和更增强的访问控制。

ORR

参见[运营准备情况审查](#)。

OT

参见[运营技术](#)。

出站 (出口) VPC

在 AWS 多账户架构中 VPC，用于处理从应用程序内部启动的网络连接。[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 委托人的 IAM 管理策略，用于设置用户或角色可以拥有的最大权限。有关更多信息，请参阅 IAM 文档中的[权限边界](#)。

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。的示例 PII 包括姓名、地址和联系信息。

PII

查看[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

参见[可编程逻辑控制器](#)。

PLM

参见[产品生命周期管理](#)。

策略

一个对象，可以在中定义权限（参见[基于身份的策略](#)）、指定访问条件（参见[基于资源的策略](#)）或定义组织中所有账户的最大权限 AWS Organizations（参见[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。有关更多信息，请参阅[在微服务中实现数据持久性](#)。

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或的查询条件false，通常位于子WHERE句中。

谓词下推

一种数据库查询优化技术，可在传输前筛选查询中的数据。这减少了必须从关系数据库检索和处理的数据量，并提高了查询性能。

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。该实体通常是 AWS 账户、IAM 角色或用户的 root 用户。有关更多信息，请参见 IAM 文档中的[角色承担者术语和概念](#)。

通过设计保护隐私

一种在整个开发过程中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](#)措施，旨在防止部署不合规的资源。这些控件会在资源配置之前对其进行扫描。如果资源与控件不兼容，则不会对其进行配置。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)

在产品的整个生命周期中，从设计、开发和上市，到成长和成熟，再到衰落和移除，对产品进行数据和流程的管理。

生产环境

参见[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。

提示链接

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，以提高可扩展性和响应能力。例如，在基于微服务的微服务中[MES](#)，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

一系列步骤，例如指令，用于访问SQL关系数据库系统中的数据。

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

参见[负责任、负责、咨询、知情 \(RACI \)](#)。

RAG

请参见[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

参见[负责任、负责、咨询、知情 \(RACI \)](#)。

RCAC

请参阅[行和列访问控制](#)。

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。

重新架构师

见 [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

见 [7 R](#)。

区域

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

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

见 [7 R](#)。

版本

在部署过程中，推动生产环境变更的行为。

搬迁

见 [7 R](#)。

更换平台

见 [7 R](#)。

回购

见 [7 R](#)。

故障恢复能力

应用程序抵御中断或从中断中恢复的能力。在中规划弹性时，[高可用性](#)和[灾难恢复](#)是常见的考虑因素。AWS Cloud有关更多信息，请参阅[AWS Cloud 弹性](#)。

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。

负责、负责、咨询、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

见 [7 R](#)。

退休

见 [7 R](#)。

检索增强生成 (RAG)

一种 [生成式 AI](#) 技术，其中在生成响应之前 [LLM](#) 引用其训练数据源之外的权威数据源。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据的过程。

行和列访问控制 (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

参见 [恢复点目标](#)。

RTO

参见 [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

SAML2.0

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)，因此用户无需为组织中的IAM所有人创建用户即可登录 AWS Management Console 或调用 AWS API操作。有关SAML基于 2.0 的联合身份验证的更多信息，请参阅文档中的 [关于SAML基于 2.0 的联合](#)。IAM

SCADA

参见 [监督控制和数据采集](#)。

SCP

参见 [服务控制政策](#)。

secret

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 密钥中有什么？](#) 在 Secrets Manager 文档中。

安全性源于设计

一种在整个开发过程中考虑安全性的系统工程方法。

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。安全控制主要有四种类型：[预防性](#)、[侦测](#)、[响应式](#)和[主动式](#)。

安全加固

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

一种预定义和编程的操作，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 实例或轮换证书。

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 AWS Organizations的组织中所有账户的权限。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

URL的入口点的 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](#)。

服务级别协议 () 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。

服务级别指示器 () SLI

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 () SLO

代表服务运行状况的目标指标，由服务[级别指标](#)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

参见[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

参见[服务级别协议](#)。

SLI

参见[服务级别指标](#)。

SLO

参见[服务级别目标](#)。

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[中的分阶段实现应用程序现代化的方法。AWS Cloud](#)

SPOF

参见[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交易数据或测量数据，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 [对旧版 Microsoft ASP 进行现代化改造。NET\(ASM\) 通过使用容器和 Amazon API Gateway 逐步提供网络服务。](#)

子网

您的 IP 地址范围 VPC。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有形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。您可以使用 [Amazon S CloudWatch ynthetic](#) 来创建这些测试。

系统提示符

一种向提供上下文、说明或指导方针 [LLM](#) 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 标签可帮助您管理、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

参见[环境](#)。

训练

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

中转网关

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

基于中继的工作流程

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

可信访问权限

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

优化

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

双披萨团队

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

U

不确定性

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

无差别任务

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

上层环境

参见[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凝视

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对等互连](#)。

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

一种对一组以某种方式与当前记录相关的行进行计算的SQL函数。窗口函数对于处理任务很有用，例如计算移动平均线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

参见[一次写入，多读](#)。

WQF

参见[AWS工作负载资格框架](#)。

写一次，读多次 (WORM)

一种存储模型，它可以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，但他们无法对其进行更改。这种数据存储基础架构被认为是[不可变的](#)。

Z

零日漏洞利用

一种利用未修补[漏洞](#)的攻击，通常是恶意软件。

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。

零镜头提示

提供执行任务[LLM](#)的说明，但没有可以帮助指导任务的示例（镜头）。LLM必须使用其预先训练的知识来处理任务。零镜头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[few-shot 提示](#)。

僵尸应用程序

平均值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。