AWS 白皮书

了解 AWS 上的 GDPR 合规性

了解 AWS 上的 GDPR 合规性: AWS 白皮书

Table of Contents

了解 AWS 上的 GDPR 合规性

发布日期：2020 年 12 月（文档修订）

摘要

本文档介绍了有关 Amazon Web Services（AWS）为客户提供的服务和资源的信息，以帮助客户符合可能适用于其活动的欧盟《一般数据保护条例（GDPR）》的要求。此类要求包括遵守各项 IT 安全标准，获得 AWS 的云计算合规性控制目录（C5）认证，遵守欧洲云基础设施服务提供商（CISPE）行为准则，能够提供数据访问控制、监控和日志记录工具，加密和密钥管理功能。

《一般数据保护条例》概览

《一般数据保护条例（GDPR）》是一项欧洲隐私法（2016 年 4 月 27 日颁布的欧洲议会和理事会 2016/679 号条例），于 2018 年 5 月 25 日开始强制实施。GDPR 取代了欧盟数据保护指令（指令 95/46/EC），在每个欧盟成员国应用具有约束力的单一数据保护法，从而协调整个欧盟（EU）的数据保护法。

GDPR 适用于以下组织对个人数据进行的所有处理：在欧盟设有机构的组织，或者向欧盟个人提供商品、服务或监控欧盟居民行为时处理欧盟居民个人数据的组织。个人数据是指与已识别或可识别的自然人相关的所有信息。

GDPR 给在欧盟运营的组织带来的变化

GDPR 的一个主要方面是它能够在欧盟成员国之间就如何安全处理、使用和交换个人数据方面保持一致性。组织必须实施和定期审查技术和组织措施以及适用于个人数据处理的合规性政策，从而持续证明其处理的数据的安全性与 GDPR 合规性。若违反 GDPR 规定，欧盟监管机构有权处以最高 2000 万欧元或全球年营业额 4% 的罚款，以较高者为准。

AWS 针对 GDPR 所做的准备

AWS 合规性、数据保护和安全性专家将配合世界各地的客户，回答他们的问题，并帮助他们为依照 GDPR 在云中运行工作负载做准备。这些团队还会根据 GDPR 的要求审查 AWS 的准备情况。

> **Note**
>
> 我们可以确认所有 AWS 服务均按 GDPR 规定使用。

AWS 数据处理附录 (DPA)

AWS 提供了一项符合 GDPR 的数据处理附录 (GDPR DPA)，使客户能够符合 GDPR 合同义务。AWS GDPR DPA 包含在 AWS 服务条款中，自动适用于全球需要 AWS 遵守 GDPR 的所有客户。

2020 年 7 月 16 日，欧盟法院（CJEU）颁布了一项关于欧盟-美国隐私盾和标准合同条款（SCC）（也称为“示范条款”）的裁决。 CJEU 裁定，欧盟-美国隐私盾不再适用于从欧盟（EU）向美国（US）传输个人数据。但在该项裁决中，CJEU 确认公司可以继续使用 SCC 作为将数据传输到欧盟以外地区的机制。

根据这项裁决，AWS 客户和合作伙伴可以按照欧盟数据保护法律（包括《一般数据保护条例（GDPR）》），继续使用 AWS 将内容从欧洲传输到美国以及其他国家/地区。如果 AWS 客户选择按照 GDPR 将数据传输到欧盟以外地区，可以将 AWS 数据处理附录（DPA）中包含的 SCC 作为法律依据。随着监管和立法环境的发展，我们将努力确保我们的客户与合作伙伴在每一个运营地点都能继续享受 AWS 服务的益处。有关更多信息，请参阅欧盟-美国隐私护盾常见问题。

根据 GDPR 规定 AWS 的作用

根据 GDPR，AWS 同时承担数据处理者和数据控制者的角色。

第 32 条规定，控制者和处理者必须“…实施适当的技术和组织措施”，并考虑“现有技术和实施的成本与处理的性质、范围、背景和目的，以及处理给自然人的权利和自由带来的不同可能性和严重程度的风险”。GDPR 针对可能需要采取的安全措施提供了具体建议，包括：

- 对个人数据进行假名和加密处理。
- 能够确保处理系统和服务的持续机密性、完整性、可用性和恢复能力。
- 在发生物理或技术事故时，能够及时恢复个人数据的可用性和访问权限。
- 制定一个流程来定期测试、评估和评价技术和组织措施的有效性，以确保处理的安全性。

AWS 作为数据处理者

当客户和 AWS 合作伙伴网络（APN）合作伙伴使用 AWS 服务来处理其内容中的个人数据时，AWS 充当数据处理者。客户和 APN 合作伙伴可以使用 AWS 服务中提供的控制措施（包括安全配置控制措施）来处理个人数据。在这些情况下，客户或 APN 合作伙伴可能充当数据控制者或数据处理者，而 AWS 则充当数据处理者或子处理者。AWS 提供了一项符合 GDPR 的数据处理附录 (DPA)，其中包含 AWS 作为数据处理者的承诺。

AWS 作为数据控制者

当 AWS 收集个人数据并确定处理此类个人数据的目的和方式时，此时它充当数据控制者。例如，AWS 处理 AWS 账户的账户信息，用于账户注册、管理、服务访问或联系信息，以通过客户支持工作提供帮助时，其充当数据控制者。

共享安全责任模型

安全性和合规性是 AWS 与客户的共同责任。当客户将计算机系统和数据迁移到云中时，客户及云服务提供商将共同承担安全责任。当客户迁移到 AWS 云时，AWS 负责保护运行 AWS 云中提供的所有服

务的全球基础设施。对于 Amazon S3 和 Amazon DynamoDB 这样的抽象服务，AWS 还负责操作系统和平台的安全性。客户和 APN 合作伙伴充当数据控制者或数据处理者时，应对所放入云或连接到云的任何内容负责。责任的这种区分通常称为云的安全性与云中的安全性。该共享模型可以帮助客户减轻运营负担，并为他们提供必要的灵活性和控制权，以便在 AWS 云中部署其基础设施。有关更多信息，请参阅 AWS 责任共担模式。

GDPR 不会改变 AWS 的责任共担模式，该模式仍然与专注于使用云计算服务的客户和 APN 合作伙伴相关。责任共担模式是一种阐明 AWS（作为数据处理者或子处理者）以及客户或 APN 合作伙伴（作为数据控制者或数据处理者）在 GDPR 下的不同责任的有效途径。

强有力的合规框架和安全标准

根据 GDPR，适当的技术和组织措施可能需要包括“…确保处理系统和服务的持续机密性、完整性、可用性和弹性的能力”，以及可靠的恢复、测试和整体风险管理流程。

AWS 合规计划

AWS 不断维护我们所有全球业务之间的高标准安全性和合规性。安全性始终是我们最优先考虑的事项 – 安全是“1”，其他都是“0”。 AWS 会定期接受独立的第三方认证审计，以保证控制活动按预期运行。更具体地说，AWS 会根据各地区和行业的各种全球和区域性的安全框架接受审计。目前，AWS 参与了 50 多项不同的审计计划。

这些审计的结果将由评估机构记录并通过 AWS Artifact 提供给所有 AWS 客户。AWS Artifact 是一个免费的自助服务门户，用于按需访问 AWS 合规性报告。当新报告发布时，它们会在 AWS Artifact 中提供，让客户能够立即访问新报告，根据报告结果持续监督 AWS 的安全性与合规性。

客户可以享受到我们获得国际认可的认证和资格鉴定带来的好处，这可证实我们符合严格的国际标准，如适用于云安全性的 ISO 27017、适用于云隐私的 ISO 27018、SOC 1、SOC 2 和 SOC 3、PCI DSS 第 1 级以及其他标准。AWS 还会帮助客户符合当地安全标准，如 BSI 的通用云计算控制目录（C5），一项由德国政府提供支持的鉴证。

有关 AWS 认证计划、报告和第三方鉴证的更多详细信息，请参阅 AWS 合规计划。有关各个服务的特定信息，请参阅 AWS 范围内服务。

云计算合规性控制目录

云计算合规性控制目录（C5）是一项由德国政府支持的认证计划，由德国联邦信息安全办公室（BSI）引入。该计划旨在帮助组织在德国政府针对云提供商的安全建议的范围内展示防范常见网络攻击的运营安全性。

数据保护技术和组织措施以及信息安全措施以数据安全为目标来确保数据的机密性、完整性和可用性。C5 定义了与数据保护相关的安全要求。AWS 客户及其合规顾问在将工作负载迁移到云中时，可以使用 C5 认证来了解 AWS 为他们提供的 IT 安全保障服务的范围。C5 增加了与 IT-Grundschutz 相当的法规规定的 IT 安全级别，以及特定于云的控制力。

C5 增加了更多的控制力，可提供有关数据位置、服务预置、管辖地、现有认证、信息披露义务的信息以及一个全方位服务说明。使用此信息，您可以评估与使用云计算服务相关的法律法规（如数据隐私）、自己的策略或威胁环境。

数据访问控制

GDPR 第 25 条规定，控制者“应实施适当的技术和组织措施以确保在默认情形下，仅处理为实现特定目的而必需的个人数据。”以下 AWS 访问控制机制仅允许得到授权的管理员、用户和应用程序访问 AWS 资源和客户数据，从而能够帮助客户符合此要求。

AWS Identity and Access Management

在您创建 AWS 账户时，会为您的 AWS 账户自动创建一个根用户。此用户账户对您 AWS 账户中的所有 AWS 服务和资源具有完全访问权限。您应当仅将此账户用于初次创建额外角色和用户账户，以及需要它的管理活动，而不应用于日常任务。AWS 建议您从开始就应用最小特权原则：为不同的任务定义不同用户账户和角色，并且指定完成每项任务所需的最小权限集。这种方法是一种机制，用于调整 GDPR 中引入的一个关键概念：通过设计保护数据。AWS Identity and Access Management（IAM）是一项 Web 服务，可用于安全地控制对您的 AWS 资源的访问。

用户和角色使用特定权限定义 IAM 身份。授权用户可以代入一个 IAM 角色来执行特定任务。代入角色时将创建临时凭证。例如，您可以使用 IAM 角色安全地为在 Amazon Elastic Compute Cloud（Amazon EC2）中运行的应用程序提供访问其他 AWS 资源所需的临时凭证，如 Amazon S3 存储桶，Amazon Relational Database Service（Amazon RDS）或 Amazon DynamoDB 数据库。同样，执行角色为 AWS Lambda 函数提供访问其他 AWS 服务和资源所需的权限，如执行日志流式传输或从 Amazon Simple Queue Service（Amazon SQS）队列读取消息的 Amazon CloudWatch Logs。创建角色时，您需要向角色添加策略来定义授权。

为了帮助客户监控资源策略，并识别他们可能不想要的具有公有或跨账户访问权限的资源，可以启用 IAM 访问分析器来生成全面的发现结果，帮助识别可以从 AWS 账户外部访问的资源。IAM 访问分析器使用数学逻辑和推论对资源策略进行评估，进而确定策略允许的可能访问路径。IAM 访问分析器会持续监控新的或更新策略，分析使用针对 IAM 角色的策略授予的权限--同时也会分析针对 Amazon S3 存储桶、AWS Key Management Service（AWS KMS）密钥、Amazon SQS 队列和 Lambda 函数等服务资源的策略。

如果存在已配置为允许 Internet 上的任何人或其他 AWS 账户（包括组织外部的 AWS 账户）访问的存储桶，S3 访问分析器会向您发出提醒。在 Amazon S3 访问分析器中查看存在风险的存储桶时，只需单击一下即可阻止对存储桶的所有公有访问。AWS 建议您阻止所有对存储桶的访问，除非您需要公有访问才能支持特定使用案例。在阻止所有公有访问之前，请确保您的应用程序在没有公有访问权限的情况下可以继续正常工作。有关更多信息，请参阅使用 Amazon S3 阻止公有访问。

IAM 还提供上次访问的信息，帮助您识别未使用的权限，以便您可以将其从关联的主体中删除。使用上次访问的信息，可以细化您的策略，仅允许访问需要的服务和操作。这有助于更好地遵循和应用最低

权限的最佳实践。 您可以查看 IAM 中或整个 AWS Organizations 环境中存在的实体或策略的上次访问的信息。

通过 AWS STS 创建临时访问令牌

您可以使用 AWS Security Token Service（AWS STS）创建授予对您的 AWS 资源的访问权限的临时安全凭证，并将这些凭证提供给可信用户。临时安全凭证的工作方式几乎与您为 IAM 用户提供的长期访问密钥凭证相同，但有以下区别：

- 临时安全凭证供短期使用。您可以配置它们的有效时间长度，最短 15 分钟，最长 12 小时。临时凭证到期之后，AWS 将无法识别，也不允许通过它们发出的 API 请求进行任何类型的访问。
- 临时安全凭证不随用户账户存储在一起。相反，它们是动态生成的，并在请求时提供给用户。临时安全凭证到期时（或之前），用户可以请求新的凭证，如果该用户有此权限。

由于存在这些差异，使用临时凭证具有以下优势：

- 您无需在应用程序中分发或嵌入长期 AWS 安全凭证。
- 临时凭证是角色和身份联合的基础。通过为用户定义一个临时的 AWS 身份，您可以为他们提供对 AWS 资源的访问。
- 临时安全凭证的可自定义生命周期是有限的。因此，在不需要这些凭证时，您不必轮换或显式撤消它们。临时安全凭证到期后，不能重复使用。您可以指定凭证的最长有效时间。

多重身份验证

为了提高安全性，您可以向 AWS 账户和 IAM 用户添加双重身份验证。借助多重身份验证（MFA），当您登录 AWS 管理控制台时，系统会提示您输入用户名和密码（第一重），以及来自您的 AWS MFA 设备的身份验证响应（第二重）。您可以为您的 AWS 账户、在您账户中创建的各个 IAM 用户启用 MFA。您还可以使用 MFA 来控制对 AWS 服务 API 的访问。

例如，您可以定义一个策略，允许完全访问 Amazon EC2 中的所有 AWS API 操作，但明确拒绝访问特定 API 操作，如 `StopInstances` 和 `TerminateInstances` – 如果该用户未经过 MFA 身份验证。

```
{
 “Version”: “2012-10-17”,
```

```
        “Statement”: [
            {
               “Sid”: “AllowAllActionsForEC2”,
               “Effect”: “Allow”,
               “Action”: “ec2:*”,
               “Resource”: “*”
            },
           {
               “Sid”: “DenyStopAndTerminateWhenMFAIsNotPResent”,
               “Effect”: “Deny”,
               “Action”: [
                   “ec2:StopInstances”,
                   “ec2:TerminateInstances”
              ],
               “Resource”: “*”,
               “Conditions”: {
                  “BoolIfExists”: {“aws:MultiFactorAuthPresent”:false}
               }
           }
       }
}
```

要为您的 Amazon S3 存储桶添加额外的安全层，您可以配置 MFA 删除，此功能会对更改存储桶的版本控制状态和永久删除对象版本执行额外的身份验证。“MFA 删除”可在您的安全凭证遭到破坏时提供额外的安全性。

要使用“MFA 删除”，您可以使用硬件或虚拟 MFA 设备来生成身份验证代码。有关支持的硬件或虚拟 MFA 设备的列表，请参阅多重身份验证页面。

访问 AWS 资源

为了实现精细访问您的 AWS 资源，您可以向不同人员授予不同级别的权限来访问不同资源。例如，您可以只允许某些用户完全访问 Amazon EC2、Amazon S3、DynamoDB、Amazon Redshift 和其他 AWS 服务。

对于其他用户，您可以允许仅针对某些 Amazon S3 存储桶的只读访问权限，或是仅管理某些 Amazon EC2 实例的权限，或是仅访问您的账单信息。

以下策略是一种方法的示例，您可以通过它允许对特定 Amazon S3 存储桶执行所有操作，并明确拒绝访问 Amazon S3 之外的每个 AWS 服务。

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Effect”: “Allow”,
                “Action”: “s3:*”,
                “Resource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ],
              },
              {
                “Effect”: “Deny”,
                “NotAction”: “s3:*”,
                “NotResource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ]
               }
            ]
}
```

您可以将策略附加到用户账户或角色。有关 IAM 策略的其他示例，请参阅基于 IAM 身份的策略示例。

定义区域性服务访问的边界

作为客户，您对自己的内容拥有所有权，而且您可以选择使用哪项 AWS 服务处理、存储和托管您的内容。未经您的同意，AWS 不会出于任何目的而访问或使用您的内容。基于责任共担模型，您可以选择存储您的内容的 AWS 区域，这样您就可以根据自己对地理位置的具体要求，在自己选择的地点部署 AWS 服务。例如，如果您想要确保您的内容仅位于欧洲，可以选择仅在其中一个欧洲 AWS 区域部署 AWS 服务。

IAM 策略提供一种简单的机制来限制对位于特定区域的服务的访问。您可以将全局条件（`aws:RequestedRegion`）添加到您的 IAM 主体所附的 IAM 策略中，来对所有 AWS 服务强制执行此条件。例如，以下策略使用具有 `Deny` 效果的 `NotAction` 元素，如果请求的区域不是欧洲的区域，它会明确拒绝访问语句中未列出的所有操作。CloudFront、IAM、Amazon Route 53 和 AWS Support 服务中的操作应不会被拒绝，因为这些服务属于热门的 AWS 全球服务。

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Sid”: “DenyAllOutsideRequestedRegions”,
                “Effect”: “Deny”,
                “NotAction”: [
                     “cloudfront:*”,
                     “iam:*”,
                     ”route53:*”,
                     “support:*”
                 ],
                 “Resource”: “*”,
                 “Condition”: {
                    “StringNotLike”: {
                        “aws:RequestedRegion”: [
                              “eu-*”
                        ]
                    }
                 }
            }
          ]
}
```

此示例 IAM 策略还可以在 AWS Organizations 中作为服务控制策略（SCP）实施，它定义应用于组织内特定 AWS 账户或组织部门（OU）的权限边界。这让您可以在复杂的多账户环境中控制用户对区域性服务的访问权限。

新启动的区域具有地理限制功能。2019 年 3 月 20 日之后推出的区域默认处于禁用状态。您必须先启用这些地区，然后才能使用它们。如果默认禁用 AWS 地区，则您可以使用 AWS 管理控制台启用和禁用该地区。启用和禁用 AWS 地区可让您控制 AWS 账户中的用户是否可以访问该地区的资源。有关更多信息，请参阅管理 AWS 区域。

控制对 Web 应用程序和移动应用程序的访问

AWS 提供了用于在客户应用程序中管理数据访问控制的服务。如果您需要在 Web 应用程序和移动应用程序中添加用户登录和访问控制功能，则可以使用 Amazon Cognito。Amazon Cognito 用户池提供了一个可扩展到数亿用户的安全用户目录。为了保护用户的身份，您可以向用户池添加多重身份验证 (MFA)。您还可以使用自适应身份验证，该机制使用基于风险的模型来预测您何时可能需要其他身份验证因素。

使用 Amazon Cognito 身份池（联合身份），您可以查看您的资源访问者以及访问来源（移动应用程序或 Web 应用程序）。您可以使用此信息来创建 IAM 角色和策略，以基于访问源的类型（移动应用程序或 Web 应用程序）和身份提供商允许或拒绝访问资源。

监控和日志记录

GDPR 的第 30 条规定“...所有控制者及其代表（如适用）应保留其职责范围内的处理活动记录。”本文还包括有关在监控所有个人数据的处理时必须记录哪些信息的详细信息。还要求控制者和处理者及时发送违规通知，因此快速检测事件非常重要。为了帮助客户履行这些义务，AWS 提供了以下监控和日志记录服务。

使用 AWS Config 管理和配置资产

AWS Config 提供 AWS 账户中多种 AWS 资源的配置的详细视图。其中包括资源彼此之间的关系以及以前的配置方式，让您可以了解配置和关系随时间的变化。

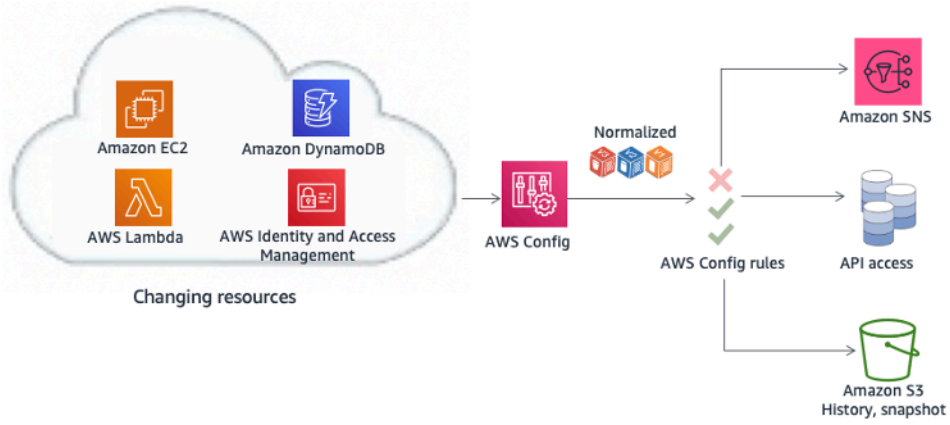

图 1 – 使用 AWS Config 监控随时间推移的配置变化

AWS 资源是指您可以在 AWS 中使用的实体，例如 EC2 实例、Amazon Elastic Block Store（Amazon EBS）卷、安全组或 Amazon Virtual Private Cloud（Amazon VPC）。有关 AWS Config 支持的完整 AWS 资源列表，请参阅支持的 AWS 资源类型。

利用 AWS Config，您可以：

- 评估您的 AWS 资源配置以验证设置是否正确。
- 获得与您的 AWS 账户关联的受支持资源的当前配置快照。
- 获取账户中一个或多个资源的配置。
- 获取一个或多个资源的历史配置。
- 在创建、修改或删除资源时获取通知。

- 查看资源之间的关系。例如，查找使用特定安全组的所有资源。

合规性审计和安全性分析

借助 AWS CloudTrail，您可以持续监控 AWS 账户活动。捕获账户的 AWS API 调用历史记录，包括通过 AWS 管理控制台、AWS 软件开发工具包、命令行工具和更高级别的 AWS 服务执行的 API 调用。您可以识别哪些用户和账户调用了支持 CloudTrail 的服务的 AWS API、执行调用的源 IP 地址以及调用发生的时间。您可以使用 API 将 CloudTrail 集成到应用程序中，为组织自动创建跟踪，检查跟踪状态，以及控制管理员启用和禁用 CloudTrail 日志记录的方式。

CloudTrail 日志可以从多个区域和多个 AWS 账户聚合到单个 Amazon S3 存储桶中。AWS 建议您将日志（尤其是 AWS CloudTrail 日志）写入指定用于日志记录（日志存档）的 AWS 账户中具有受限访问权限的 Amazon S3 存储桶。存储桶上的权限应防止日志被删除，还应使用服务器端加密和 Amazon S3 托管加密密钥（SSE-S3）或 AWS KMS 托管密钥（SSE-KMS）对日志进行静态加密。CloudTrail 日志文件完整性验证可用于确定在 CloudTrail 交付后日志文件是否被修改、删除或未进行更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这样，从计算的角度来说，要修改、删除或伪造 CloudTrail 日志文件而不被检测到会很困难。您可以使用 AWS Command Line Interface（AWS CLI）在 CloudTrail 交付文件的位置验证这些文件。

可以出于审计目的或为故障排除活动分析在 Amazon S3 存储桶中聚合的 CloudTrail 日志。日志集中化后，您可以与安全信息和事件管理（SIEM）解决方案集成，或者使用 Amazon Athena 或 CloudTrail Insights 等 AWS 服务分析日志，还可以使用 Amazon QuickSight 控制面板将其可视化。将 CloudTrail 日志集中化后，您还可以使用同一个日志存档账户集中管理来自其他来源（如 CloudWatch Logs 和 AWS 负载均衡器）的日志。

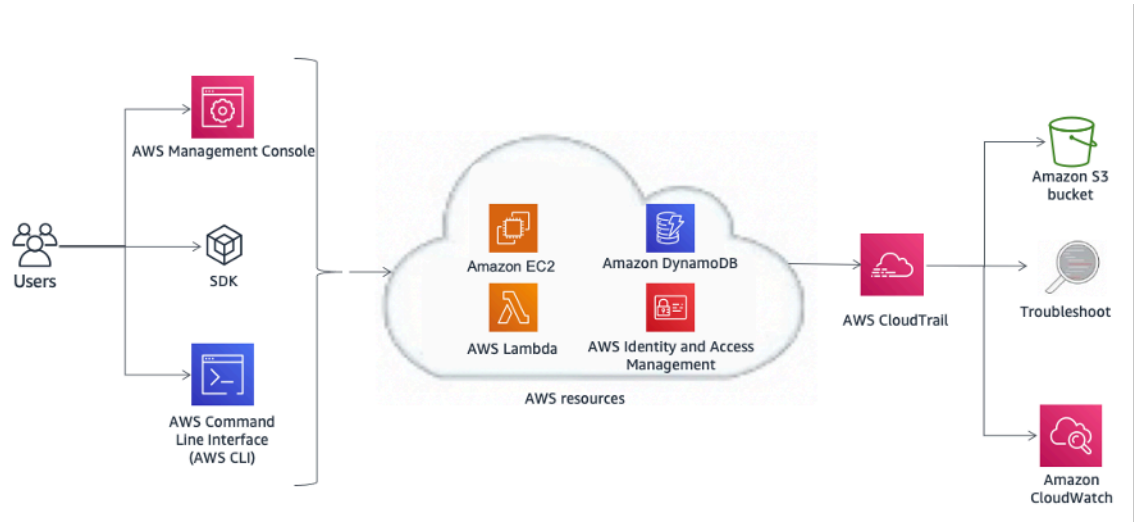

图 2 – 使用 AWS CloudTrail 进行合规性审计和安全分析的示例架构

AWS CloudTrail 日志还可以触发预配置的 Amazon CloudWatch 事件。您可以使用这些事件来通知用户或系统发生了某个事件或需要执行修复操作。例如，如果您要监控 Amazon EC2 实例中的活动，您可以创建 CloudWatch 事件规则。如果 Amazon EC2 实例中发生特定活动，并将事件捕获到日志中，该规则将触发 AWS Lambda 函数，该函数会向管理员发送一封关于该事件的通知电子邮件。（参阅图 3。）电子邮件中包含事件发生时间、执行操作的用户、Amazon EC2 详细信息等详细信息。下图显示了事件通知的架构。

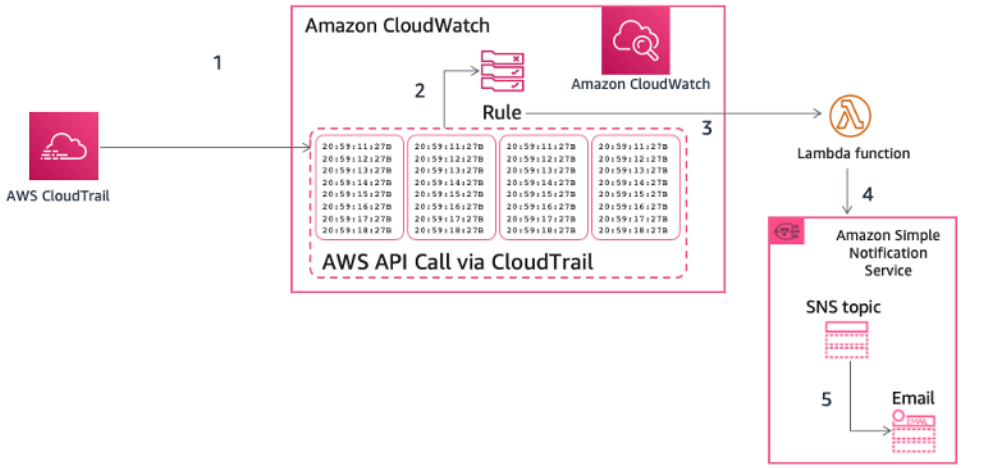

图 3 – AWS CloudTrail 事件通知示例

收集和处理日志

CloudWatch Logs 可用于监控、存储和访问来自 Amazon EC2 实例、AWS CloudTrail、Route 53 和其他来源的日志文件。请参阅将日志发布到 CloudWatch Logs 的 AWS 服务文档页面。

日志信息包括如：

- 对 Amazon S3 对象的访问进行细粒度日志记录
- 有关通过 VPC-Flow Logs 的网络流量的详细信息
- 使用 AWS Config 规则进行基于规则的配置验证和操作
- 在 CloudFront 中通过 Web 应用程序防火墙（WAF）功能对应用程序的 HTTP 访问进行筛选和监控

通过在 Amazon EC2 实例或本地服务器上安装 CloudWatch 代理，还可以将自定义应用程序指标和日志发布到 CloudWatch Logs。

可以使用 CloudWatch Logs Insights 以交互方式分析日志，进而执行查询来帮助您更高效、更有效地对运营问题作出响应。

CloudWatch Logs 可以通过配置订阅筛选器近乎实时地进行处理，并可以传送到其他服务进行自定义处理、分析或加载到其他系统，如 Amazon OpenSearch Service（OpenSearch Service）集群、Amazon Kinesis 流、Amazon Kinesis Data Firehose 流或 Lambda。

CloudWatch 指标筛选器可用于定义要在日志数据中查找的模式，将它们转换为数字 CloudWatch 指标，以及根据您的业务要求设置警报。例如，按照不使用根用户执行日常任务的 AWS 建议，可以在 CloudTrail 日志（传送到 CloudWatch Logs）上设置特定的 CloudWatch 指标筛选器来创建自定义指标，并可以配置警报，在根凭证被用来访问您的 AWS 账户时通知相关的利益攸关方。

Amazon S3 服务器访问日志、Elastic Load Balancing 访问日志、VPC 流日志和 AWS Global Accelerator 流日志等日志可以直接传送到 Amazon S3 存储桶。例如，当您启用 Amazon Simple Storage Service 服务器访问日志时，您可以获取有关向 Amazon S3; 存储桶发起的请求的详细信息。访问日志记录包含有关请求的详细信息，例如请求类型、请求中指定的资源，以及处理请求的时间和日期。有关日志消息内容的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南中的 Amazon Simple Storage Service 服务器访问日志格式。服务器访问日志记录对许多应用程序都十分有用，因为它们让存储桶拥有者可以深入了解不受其控制的客户端所发出的请求的性质。默认情况下，Amazon S3 不会收集服务访问日志，但是当您启用日志记录后，Amazon S3 通常会在几小时内将访问日志传送到您的存储桶。如果您需要更快的传送速度或需要将日志传送到多个目标位置，请考虑使用 CloudTrail 日志或将 CloudTrail 日志与 Amazon S3 结合使用。通过在目标存储桶中配置默认对象加密，可以对日志进行静态加密。这些对象使用具有 Amazon S3 托管密钥（SSE-S3）或 AWS Key Management Service（AWS KMS）中存储的客户主密钥（CMK）的服务器端加密进行加密。

可以使用 Amazon Athena 查询和分析存储在 Amazon S3 存储桶中的日志。Amazon Athena 是一种交互式查询服务，借助它，您能够使用标准 SQL 分析 S3 中的数据。使用 Athena，您可以通过 ANSI SQL 运行临时查询，而无需将数据聚合或加载到 Athena 中。Athena 可以处理非结构化、半结构化和结构化数据集，并可以与 Amazon QuickSight 集成，轻松实现可视化。

日志也是自动化威胁检测的有用信息源。Amazon GuardDuty 是一项持续运行的安全监控服务，可分析和处理来自多个来源的事件，如 VPC 流日志、CloudTrail 管理事件日志、CloudTrail Amazon S3 数据事件日志和 DNS 日志。它使用威胁情报源（例如，恶意 IP 地址和域的列表）和机器学习来标识您 AWS 环境中意外的和未经授权的恶意活动。当您在某个区域启用 GuardDuty 时，它会立即开始分析您的 CloudTrail 事件日志。它通过独立的重复事件流直接从 CloudTrail 中使用 CloudTrail 管理和 Amazon S3 数据事件。

使用 Amazon Macie 规模化地发现和保护数据

GDPR 第 32 条规定：“...控制者和处理者应采取适当的技术和组织性措施以确保达到与风险相称的安全级别，酌情包括：[...]

(b) 能够确保处理系统和服务的持续机密性、完整性、可用性和恢复能力；

[…]

(d) 制定一个流程来定期测试、评估和评价技术和组织措施的有效性，以确保处理的安全性。”

使用持续的数据分类流程对于根据数据的性质调整安全数据处理至关重要。如果您的组织需要管理敏感数据，应监控敏感数据所在的位置，对其进行适当保护，并根据需要提供证据证明您正在实施数据安全和隐私保护，以满足合规要求。为了帮助客户规模化地识别和保护他们的敏感数据，AWS 提供了 Amazon Macie，这是一项完全托管式数据安全和数据隐私服务，使用模式匹配和机器学习模型来检测个人身份信息（PII），以发现和保护存储在 S3 存储桶中的敏感数据。Amazon Macie 会扫描这些存储桶，并使用专门用于检测多种敏感数据类别的托管数据标识符对这些存储桶进行数据分类。Macie 可以检测 PII，如全名、电子邮件地址、出生日期、身份证号码、纳税人识别号或参考号等。客户可以定义反映其组织特定场景的自定义数据标识符（例如，客户账号或内部数据分类）。

Amazon Macie 会持续评估存储桶内的对象，并自动为发现的与定义的数据类别匹配的任何未加密或可公开访问的数据提供发现结果摘要（图 4）。此数据可以包括针对任何可公开访问的未加密对象，或与您在 AWS Organizations 中定义的 AWS 账户之外的账户共享的存储桶发出的警报。Amazon Macie 已与其他 AWS 服务（如 AWS Security Hub）集成，可以生成可操作的安全发现结果，并针对发现结果提供自动的反应性操作（图 5）。

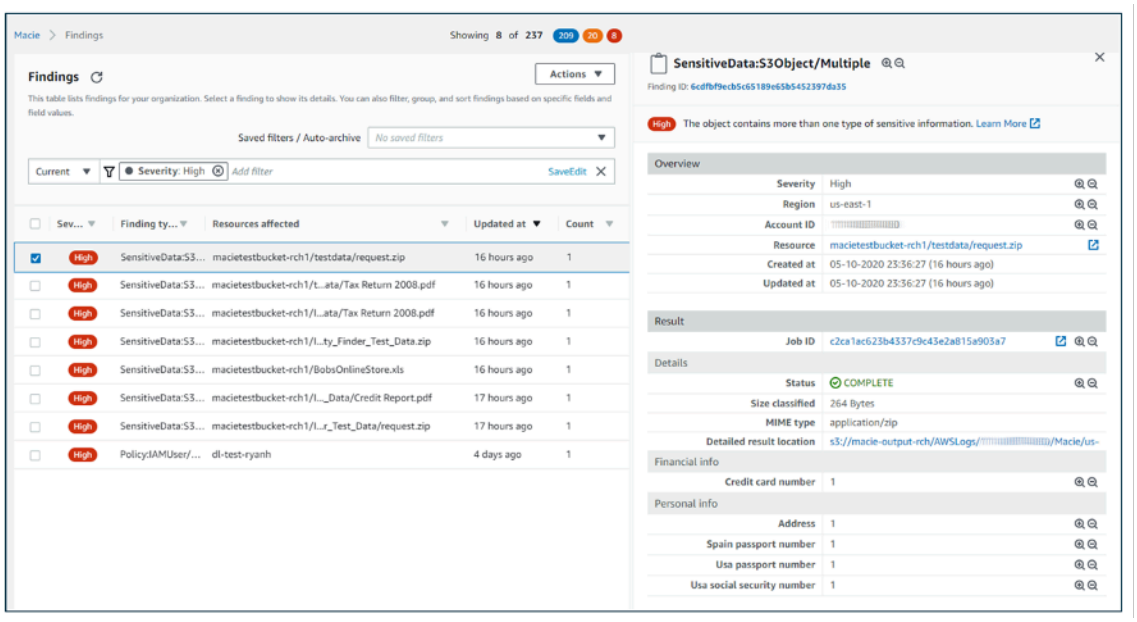

图 4 – 数据检查和查找示例

集中式安全管理

许多组织都面临与环境的可见性和集中管理相关的挑战。随着运营范围的扩大，除非仔细考虑安全设计，否则这些挑战可能会更加复杂。缺乏知识，加之监管和安全流程管理分散且不均衡，会导致您的环境易受攻击。

AWS 提供了一些工具帮助您解决 IT 管理和监管方面一些最具挑战性的要求，还提供了一些工具来支持按设计保护数据的方法。

AWS Control Tower 提供设置和管理新的安全的多账户 AWS 环境的最简单方法。它会自动设置一个登录区，这是一个基于最佳实践蓝图的多账户环境，并使用您可从预先打包的列表中选择的防护机制提供监管。防护机制实施监管规则以实现安全性、合规性和运营。AWS Control Tower 使用 AWS IAM Identity Center（IAM Identity Center）默认目录提供身份管理，并使用 IAM Identity Center 和 IAM 支持跨账户审计。它还集中了来自 CloudTrail 的日志和存储在 Amazon S3 中的 AWS Config 日志。

AWS Security Hub 是另一个支持集中化的服务，可以提高组织的可见性。Security Hub 会集中来自各个 AWS 账户和服务的安全性与合规性发现结果并确定其优先级，如 Amazon GuardDuty 和 Amazon Inspector，还可以与第三方合作伙伴的安全软件集成，帮助您分析安全趋势并确定最高优先级的安全问题。

Amazon GuardDuty 是一种智能威胁检测服务，可以帮助客户更准确、更轻松地监控和保护他们的 AWS 账户、工作负载以及 Amazon S3 中存储的数据。GuardDuty 分析来自多个来源跨您的各个 AWS 账户的数十亿个事件，包括 AWS CloudTrail 管理事件、CloudTrail Amazon S3 数据事件、Amazon Virtual Private Cloud 流日志和 DNS 日志。例如，它能够检测异常 API 调用、发往已知恶意 IP 地址的可疑出站通信或将 DNS 查询用作传输机制可能造成的数据被盗。GuardDuty 能够利用机器学习驱动的威胁情报以及第三方安全合作伙伴提供更准确的发现结果。

Amazon Inspector 是一项自动安全评估服务，有助于提高在 Amazon EC2 实例上部署的应用程序的安全性与合规性。Amazon Inspector 会自动评估应用程序的风险、漏洞或者相较于最佳实践的偏差。执行评估后，Amazon Inspector 会生成按严重程度确定优先级的安全检验详细列表。

借助 Amazon CloudWatch Events，您可以设置 AWS 账户以将事件发送到其他 AWS 账户，还可以接收其他账户或组织的事件。通过在发生安全事件时根据需要及时采取纠正措施（例如，通过调用 Lambda 函数或对 Amazon EC2 实例运行命令），该机制对于实现跨账户事件响应场景非常有用。

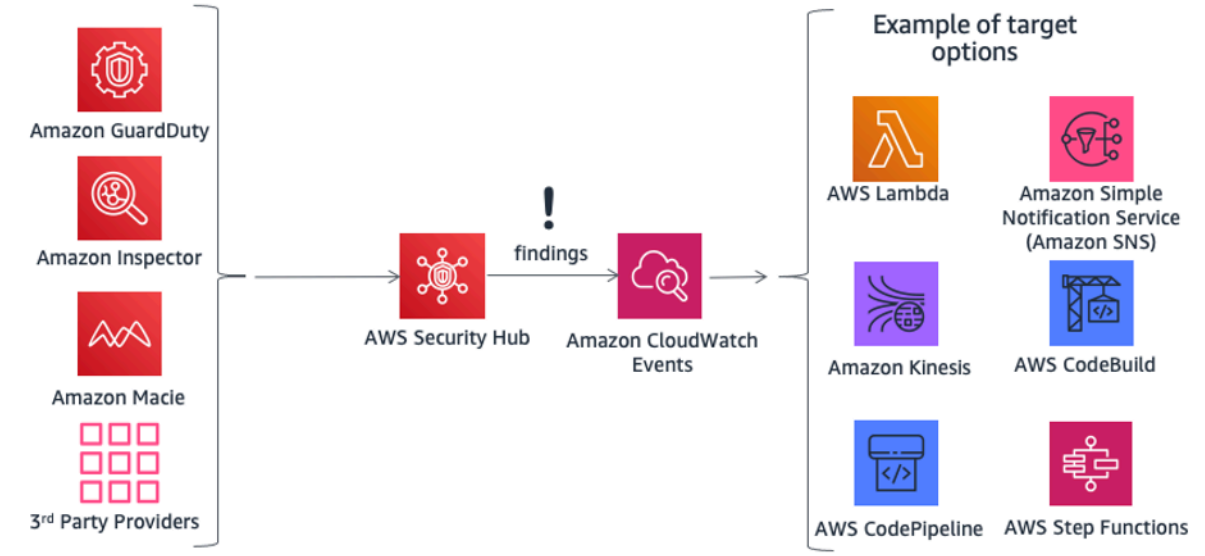

图 5 – 使用 AWS Security Hub 和 Amazon CloudWatch Events 采取措施

AWS Organizations 可帮助您集中管理和控制复杂的环境。它使您能够在多账户环境中控制访问、合规性和安全性。AWS Organizations 支持服务控制策略（SCP），这些策略定义可以用于组织内的特定账户或组织部门（OU）的 AWS 服务操作。

AWS Systems Manager 让您能够查看和控制 AWS 上的基础设施。您可以从一个统一控制台查看来自多个 AWS 服务的操作数据，并可以跨这些服务自动执行操作任务。您可以获取有关最近的 API 活动、资源配置更改、操作警报、软件清单和补丁合规性状态的信息。使用与其他 AWS 服务的集成，您还可以根据您的运营需求对资源采取行动，以帮助您的环境处于合规状态。

例如，通过将 Amazon Inspector 与 AWS Systems Manager 集成，可以简化和自动化安全评估，因为您可以在 Amazon EC2 实例启动时，使用 Amazon Elastic Compute Cloud Systems Manager 自动安装 Amazon Inspector 代理。您还可以使用 Amazon EC2 System Manager 和 Lambda 函数对 Amazon Inspector 发现结果执行自动修复。

在 AWS 上保护您的数据

GDPR 第 32 条要求组织必须“实施适当的技术和组织措施，以确保具有可避免风险的适当安全级别，包括…对个人数据进行假名和加密处理[...]”。此外，组织必须防止未经授权的个人数据披露或访问。”

加密减少了与个人数据存储相关的风险，因为如果没有正确的密钥，数据将无法读取。细致的加密策略可以帮助减轻各种安全事件（包括某些安全漏洞）的影响。

加密静态数据

加密静态数据对于法规遵从性和数据保护至关重要。它有助于确保任何没有有效密钥的用户或应用程序都无法读取保存在磁盘上的敏感数据。AWS 为静态加密和加密密钥管理提供了多个选项。例如，您可以将 AWS Encryption SDK 与在 AWS KMS 中创建和管理的 CMK 结合使用来加密任意数据。

加密的数据可以安全地以静态形式存储，并且只能由有权访问 CMK 的一方解密。因此，您可以获得机密的信封加密数据、用于授权和经过身份验证的加密的策略机制，以及通过 AWS CloudTrail 进行的审计日志记录。一些 AWS Foundation Services 具有内置的静态加密功能，提供了在将数据写入非易失性存储之前对其进行加密的选项。例如，您可以使用 AES-256 加密对 Amazon EBS 卷进行加密并配置 Amazon S3 存储桶以进行服务器端加密（SSE）。Amazon S3 还支持客户端加密，这允许您在将数据发送到 Amazon S3 之前对其进行加密。AWS SDK 支持客户端加密，以方便对象的加密和解密操作。Amazon RDS 还支持透明数据加密（TDE）。

可以使用内置的 Linux 库对 Linux Amazon EC2 实例存储上的数据进行加密。这种方法可以透明地加密文件，保护机密数据。因此，处理数据的应用程序不会发现磁盘级别的加密。

您可以使用两种方法来加密实例存储上的文件：

- 磁盘级加密 — 使用此方法，整个磁盘或磁盘中的一个数据块使用一个或多个加密密钥进行加密。磁盘加密在文件系统级别以下运行，与操作系统无关，并隐藏目录和文件信息，如名称和大小。例如，加密文件系统是 Windows NT 操作系统新技术文件系统（NTFS）的 Microsoft 扩展，该系统提供磁盘加密。
- 文件系统级加密 — 通过这种方法，会加密文件和目录，但不是整个磁盘或分区。文件系统级加密在文件系统之上运行，并且可跨操作系统移植。

对于非易失性存储标准（NVMe）SSD 实例存储卷，磁盘级加密是默认选项。NVMe 实例存储中的数据使用 XTS-AES-256 分组密码进行加密，这一密码在实例上的硬件模块中实现。加密密钥使用硬件模块生成，并且对于每个 NVMe 实例存储设备都是唯一的。所有加密密钥会在实例停止或终止时被销毁，并且无法恢复。您不能使用自己的加密密钥。

加密传输中的数据

AWS 强烈建议对从一个系统传输到另一个系统的数据进行加密，包括 AWS 内外的资源。

创建 AWS 账户时，会为其预配置 AWS 云的逻辑隔离部分，即 Amazon Virtual Private Cloud（Amazon VPC）。在那里，您可以在您定义的虚拟网络中启动 AWS 资源。您可以完全控制虚拟网络环境，包括选择自己的 IP 地址范围、创建子网，以及配置路由表和网络网关。您还可以在公司数据中心和您的 Amazon VPC 之间创建硬件虚拟专用网络 (VPN) 连接，以便您可以将 AWS 云用作公司数据中心的扩展。

为了保护您的 Amazon VPC 与公司数据中心之间的通信，您可以从多个 VPN 连接选项中进行选择，然后选择最符合您需求的一个选项。您可以使用 AWS Client VPN 通过基于客户端的 VPN 服务启用对 AWS 资源的安全访问。您也可以使用 AWS Marketplace 中提供的第三方软件 VPN 设备，您可以将其安装在 Amazon VPC 中的 Amazon EC2 实例上。或者，您可以建立 IPsec VPN 连接来保护 VPC 与您的远程网络之间的通信。要创建从远程网络到您的 Amazon VPC 的专用私有连接，您可以使用 AWS Direct Connect。您可以将此连接与 AWS 站点到站点 VPN 结合来创建经 IPSec 加密的私有连接。

AWS 提供使用 TLS 协议进行通信的 HTTPS 终端节点，当您使用 AWS API 时，该协议可在传输过程中提供加密。您可以使用 AWS Certificate Manager（ACM）服务来生成、管理和部署用于在工作负载的系统之间建立加密传输的私有和公有证书。Elastic Load Balancing 已经与 ACM 集成，用于支持 HTTPS 协议。如果您的内容是通过 Amazon CloudFront 分发的，则它支持加密的终端节点。

加密工具

AWS 提供各种高度可扩展的数据加密服务、工具和机制，以帮助保护您在 AWS 上存储和处理的数据。有关 AWS 服务功能和隐私的信息，请参阅 AWS 服务功能的隐私注意事项。

AWS 提供的加密服务使用了广泛的加密和存储技术，旨在维护静态或传输中数据的完整性。AWS 提供了四种用于加密操作的主要工具。

- AWS Key Management Service（AWS KMS）是一项 AWS 托管服务，可生成和管理主密钥和数据密钥。AWS KMS 已与很多 AWS 服务集成，可以使用来自客户账户的 AWS KMS 密钥提供服务器端数据加密。AWS KMS 硬件安全模块（HSM）通过了 FIPS 140-2 Level 2 认证。
- AWS CloudHSM 提供通过了 FIPS 140-2 Level 3 认证的 HSM。它们可以安全地存储您的各种自管理加密密钥，包括主密钥和数据密钥。
- AWS 加密服务和工具
  - AWS Encryption SDK 提供了一个客户端加密库，用于对各种类型的数据实施加密和解密操作。

- Amazon DynamoDB 加密客户端提供了一个客户端加密库，用于在将数据表发送到数据库服务（如 Amazon DynamoDB）之前对其进行加密。

AWS Key Management Service

AWS Key Management Service 是一项托管服务，可让您轻松创建和控制用于加密数据的加密密钥，它使用硬件安全模块（HSM）保护您的密钥安全。AWS KMS 已经与其他几项 AWS 服务集成，可帮助您保护通过这些服务存储的数据。AWS KMS 还与 AWS CloudTrail 集成，可为您提供记录所有密钥使用情况的日志，满足您的法规和合规性需求。

您可以通过 AWS Management Console 或者使用 AWS SDK 或 AWSAWS CLI 轻松创建、导入和轮换密钥，还可以定义使用策略并审计使用情况。

AWS KMS 中的 CMK，无论是由您导入还是由 KMS 代表您创建的，都以加密格式存储在高度持久的存储中，以帮助确保在需要时可以使用它们。您可以选择让 KMS 每年自动轮换一次在 KMS 中创建的 CMK，而无需重新加密已使用主密钥加密的数据。您不需要跟踪旧版本的 CMK，因为在需要自动解密以前加密的数据时，KMS 可以提供这些密钥。

对于 AWS KMS 中的任何 CMK，您可以通过许多访问控制（包括授予、密钥策略或 IAM 策略中的密钥策略条件）来控制谁有权访问这些密钥以及它们可用于哪些服务。您还可以从自己的密钥管理基础设施导入密钥，并在 KMS 中使用这些密钥。

例如，以下策略使用 `kms:ViaService` 条件，仅当请求来自代表特定用户（`ExampleUser`）的特定区域（us-west-2）中的 Amazon EC2 或 Amazon RDS 时，才允许将客户托管的 CMK 用于指定的操作。

```
{
 “Version”: “2012-10-17”,
 “Statement”: [
     {
        “Effect”: “Allow”,
        “Principal”: {
            “AWS”: “arn:aws:iam::111122223333:user/ExampleUser”
         }
        “Action”: [
             “kms:Encrypt*”,
             “kms:Decrypt”,
             ”kms:ReEncrypt*”,
             “kms:GenerateDataKey*”,
```

```
                    “kms:CreateGrant”,
                    “kms:ListGrants”,
                    “kms:DescribeKey”
                ],
                “Resource”: “*”,
                “Condition”: {
                   “ForAnyValue:StringEquals”: {
                       “kms:ViaService”: [
                             “ec2.us-west-2.amazonaws.com”,
                             “rds.us-west-2.amazonaws.com”
                       ]
                    }
            }
}
```

AWS 服务集成

AWS KMS 已与很多 AWS 服务集成 – 有关集成的服务的完整列表，请参见 KMS 网站。这些集成意味着您可以轻松使用 AWS KMS CMK 来加密使用这些服务存储的数据。除了使用客户托管的 CMK，许多集成服务还允许您使用自动为您创建和管理的 AWS 托管的 CMK，但仅在创建它的特定服务中可用。

审计功能

AWS CloudTrail 会在日志文件中记录您存储在 AWS KMS 中的密钥的每一次使用，日志文件会被传送到您在 CloudTrail 配置中指定的 Amazon S3 存储桶。记录的信息包括用户、时间、日期、执行的操作和使用的密钥等详细信息。

安全性

AWS KMS 的主要任务是确保任何人都无法访问您的主密钥。该服务的基础系统广泛采用了各种强化技术来保护主密钥，例如不将纯文本主密钥存储在磁盘上、不将其保留在内存中，并且限制哪些系统可以访问使用密钥的主机。服务中更新软件的所有访问都由多方访问控制来管理，该访问控制由 AWS 内的独立组审核和审查。

有关 AWS KMS 的更多信息，请参阅 AWS Key Management Service 白皮书：

AWS CloudHSM

AWS CloudHSM 是一个基于云的硬件安全模块（HSM），通过它，您可以在 FIPS 140-2 3 级验证硬件上生成和使用加密密钥，从而帮助您满足企业、合同与合规性方面的数据安全要求。

使用 AWS CloudHSM，您可以控制 HSM 执行的加密密钥和加密操作。

AWS 和 AWS Marketplace 合作伙伴提供了各种用于保护 AWS 平台内敏感数据的解决方案，但对于需要遵守严格的合同或法规要求来管理加密密钥的应用程序和数据，有时需要进行额外的保护。以前，您唯一的选择是将敏感数据（或保护敏感数据的加密密钥）存储在本地数据中心。这可能会阻止您将这些应用程序迁移到云或显著降低其性能。使用 AWS CloudHSM，您可以保护按照政府安全密钥管理标准设计和验证的 HSM 中的加密密钥。您可以安全地生成、存储和管理用于数据加密的加密密钥，以确保只有您才能访问数据。AWS CloudHSM 可帮助您在不牺牲应用程序性能的情况下满足严格的密钥管理要求。

AWS CloudHSM 服务与 Amazon VPC 配合使用。AWS CloudHSM 实例在您的 Amazon VPC 内配置了您指定的 IP 地址，为您提供与 Amazon EC2 实例的简单的专用网络连接。将 HSM 实例放在 Amazon EC2 实例附近可减少网络延迟，从而提高应用程序性能。AWS 提供对 HSM 实例的专用和独占（单一租户）访问，与其他 AWS 客户隔离。AWS CloudHSM 可在多个区域和可用区中使用，让您可以为应用程序添加安全持久的密钥存储。

与 AWS 服务和第三方应用程序集成

您可以将 CloudHSM 与 Amazon Redshift、Amazon RDS for Oracle 或用作可信根的第三方应用程序（如 SafeNet Virtual KeySecure）、Apache（SSL 终端）或者 Microsoft SQL Server（透明数据加密）等结合使用。您还可以在编写自己的应用程序时使用 AWS CloudHSM，并继续使用标准加密库，包括 PKCS#11、Java JCA/JCE 以及 Microsoft CAPI 和 CNG。

审计活动

如果您出于安全性和合规性目的需要跟踪资源更改或审核活动，您可以使用 AWS CloudTrail 查看从您的账户通过 AWS CloudHSM 进行的管理 API 调用。此外，您可以使用 syslog 审计 HSM 设备上的操作或向您的日志采集器发送 syslog 日志消息。

AWS 加密服务和工具

AWS 提供了符合各种加密安全标准的机制，您可以使用这些机制来实现加密最佳实践。AWS Encryption SDK 是一个客户端加密库，在 Java、Python、C、JavaScript 中，以及支持 Linux、macOS 和 Windows 的命令行界面中可用。它提供了高级数据保护功能，包括安全的、经过身份验证的对称密钥算法套件，例如，具有密钥派生和签名功能的 256 位 AES-GCM。由于该 SDK 是专为使用 Amazon DynamoDB 的应用程序设计的，所以 DynamoDB 加密客户端使用户能够保护他们的表格数据，然后再将数据发送到数据库。检索数据时，它还会验证和解密数据。该客户端可用于 Java 和 Python。

Linux DM-Crypt 基础设施

Dm-crypt 是一种 Linux 内核级加密机制，允许用户挂载加密的文件系统。挂载文件系统是将文件系统附加到目录（挂载点）的过程，这使其可供操作系统使用。挂载后，文件系统中的所有文件都可供应用程序使用，而无需任何其他交互。但是，将这些文件存储在磁盘上时会对其进行加密。

设备映射器 是 Linux 2.6 和 3.x 内核中的基础设施，它提供了创建块储存设备虚拟层的通用方法。该设备映射器 crypt 目标使用内核加密 API 提供块储存设备的透明加密。本文中的解决方案将 dm-crypt 与由逻辑卷管理器（LVM）映射到逻辑卷的磁盘备份文件系统结合使用。LVM 为 Linux 内核提供逻辑卷管理。

通过设计保护数据以及默认情况

每当用户或应用程序尝试使用 AWS Management Console、AWS API 或 AWS CLI 时，都会向 AWS 发送请求。AWS 服务收到请求后执行一组步骤，根据特定策略评估逻辑确定是允许还是拒绝该请求。默认情况下，除根凭证请求外，AWS 上的所有请求都被拒绝（应用默认拒绝策略）。这意味着会拒绝一切未明确允许的策略。在策略定义中，并且作为最佳实践，AWS 建议您应用最小特权原则，这意味着每个组件（例如用户、模块或服务）必须只能访问完成其任务所需的资源。

此方法遵守 GDPR 第 25 条规定，控制者“应实施适当的技术和组织措施，确保在默认情形下，仅处理为实现每个特定目的而必需的个人数据。”

AWS 还提供了实施基础设施即代码的工具，这是从架构设计开始就重视安全性的强大机制。AWS CloudFormation 提供了一种通用语言来描述和预置所有基础设施资源（包括安全策略和流程）。借助这些工具和实践，安全性已成为代码的一部分，您可以根据组织要求进行版本控制、监控和修改（使用版本控制系统）。这可实现通过设计保护数据，因为安全流程和策略可以包含在您的架构定义中，并且还可以通过您组织中的安全措施连续监控。

AWS 如何提供帮助

表 1 – AWS 如何帮助您了解 GDPR 合规性

区域	说明	AWS 服务和工具
强合规性框架	适当的技术和组织措施可能需要包含“确保处理系统和服务的持续机密性、完整性、可用性和弹性的能力。”	SOC 1/SSAE 16/ISAE 3402（以前是 SAS 70）/SOC 2/SOC 3 PCI DSS 1 级 ISO 9001/ISO 27001/ISO 27017/ISO 27018 NIST FIPS 140-2 常见云计算控制目录（C5）
数据访问控制	控制者“…应实施适当的技术和组织措施以确保在默认情形下，仅处理为实现特定目的而必需的个人数据。”	AWS Identity and Access Management (IAM) Amazon Cognito AWS Shield 和 AWS WAF AWS Resource Access Manager Amazon CloudFront AWS Organizations AWS CloudTrail
监控和日志记录	“所有控制者及其代表（如适用）应保留其职责范围内的处理活动记录。”	AWS Config Amazon CloudWatch AWS Control Tower Amazon GuardDuty

区域	说明	AWS 服务和工具
	“...控制者和处理者应采取适当的技术和组织性措施以确保达到与风险相称的安全级别 [...]”	Amazon Inspector Amazon Macie AWS Systems Manager AWS Security Hub AWS 工具和开发工具包
在 AWS 上保护您的数据	组织必须“实施适当的技术和组织措施，以确保具有可避免风险的适当安全级别，包括对个人数据进行假名和加密处理。”	AWS Certificate Manager AWS CloudHSM AWS Key Management Service

贡献者

本文档的贡献者包括：

- Amazon Web Services 技术行业专家 Tim Anderson
- Amazon Web Services 公共部门解决方案架构师 Carmela Gambardella
- Amazon Web Services 安全保证经理 Giuseppe Russo
- Amazon Web Services 高级项目经理 Marta Taggart
- Amazon Web Services 公共部门解决方案架构师 Luca Iannario

文档修订

日期	说明
2017 年 11 月	首次发布
2020 年 12 月	更新包含新的 AWS 服务和功能。

声明

客户负责对本文档中的信息进行独立评估判断。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实践，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户承担的责任和义务受 AWS 协议制约，本文档不是 AWS 与客户直接签订的协议的一部分，也不构成对该协议的修改。