安全性支柱

AWS 架构完善的框架

2020 年7 月

声明

客户负责对本文档中的信息进行独立评估。本文档：(a) 仅供参考，(b) 代表 AWS 当前的产品服务和实践，如有变更，恕不另行通知，以及 (c) 不构成 AWS 及其附属公司、供应商或授权商的任何承诺或保证。AWS 产品或服务均“按原样”提供，没有任何明示或暗示的担保、声明或条件。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。

目录

摘要

本白皮书主要介绍架构完善的框架的安全性支柱。它提供了指导，以帮助您在安全 AWS 工作负载的设计、交付和维护过程中应用最佳实践和最新建议。

简介

AWS 架构完善的框架能够帮助理解您在 AWS 上构建工作负载时所做决策的权衡。通过使用此框架，您将了解有关在云中设计和运行可靠、安全、高效且经济实惠的工作负载的最新架构最佳实践。它提供了一种方法，使您能够根据最佳实践持续衡量工作负载，并确定需要改进的方面。我们相信，拥有架构完善的工作负载能够大大提高实现业务成功的可能性。

该框架基于五大支柱：

- 卓越运营
- 安全性
- 可靠性
- 性能效率
- 成本优化

本白皮书重点介绍安全性支柱。这样可以帮助您遵循最新的 AWS 建议，从而满足您的业务和法规要求。本白皮书面向技术岗位的人员，例如首席技术官 (CTO)、首席信息安全官 (CSO/CISO)、架构师、开发人员和运营团队成员。

阅读本白皮书后，您将了解可在设计注重安全的云架构时使用的 AWS 最新建议和策略。本白皮书不提供实施细节或架构模式，但会针对此类信息提供适当资源参考。通过采用本白皮书中的实践，您可以构建能够保护您的数据和系统、控制访问并自动响应安全事件的架构。

安全性

安全性支柱描述了如何利用云技术来保护数据、系统和资产，以改善您的安全状况。本白皮书提供了有关在 AWS 上构建安全工作负载的深度最佳实践指导。

设计原则

在云领域，有很多原则可帮助您提高工作负载的安全性：

- **实施强大的身份验证基础**：实施最小特权原则，并通过对每一次与 AWS 资源之间的交互进行适当授权来强制执行职责分离。集中进行身份管理，并努力消除对长期静态凭证的依赖。
- **实现可追溯性**：实时监控和审计对环境执行的操作和更改并发送警报。为系统集成日志和指标收集功能，以自动调查并采取措施。
- **在所有层面应用安全措施**：利用多种安全控制措施实现深度防御。应用到所有层面（例如网络边缘、VPC、负载均衡、每个实例和计算服务、操作系统、应用程序和代码）。
- **自动化安全性最佳实践**：借助基于软件的自动化安全机制，您能够以更为快速且更具成本效益的方式实现安全扩展。创建安全架构，包括实施可在版本控制模板中以代码形式定义和管理的控制措施。
- **保护传输中的数据和静态数据**：按敏感程度对您的数据进行分类，并根据情况采用加密、令牌和访问控制等适当机制。
- **限制对数据的访问**：利用相关机制和工具来减少或消除对于直接访问或手动处理数据的需求。这样可以降低处理敏感数据时数据处理不当、被修改以及人为错误的风险。
- **做好应对安全性事件的预案**：制定符合您组织要求的事件管理和调查政策和流程，做好应对事件的准备工作。开展事件响应模拟演练并使用具有自动化功能的工具来提高检测、调查和恢复的速度。

定义

云中的安全性包含五个方面：

1. Identity and Access Management
2. 检测
3. 基础设施保护
4. 数据保护
5. 事件响应

安全性和合规性是 AWS 与客户的共同责任。此责任共担模式有助于减轻您的运营负担。您应慎重选择服务，因为您承担的责任因您使用的服务、这些服务与您 IT 环境的集成以及适用的法律法规而异。这一责任共担的性质还提供了支持部署的灵活性和控制能力。

安全地操作您的工作负载

为了安全地操作您的工作负载，您必须对安全性的各个方面应用总体最佳实践。采用您在组织和工作负载层面的卓越运营中定义的要求和流程，并将它们应用到各个方面。及时了解最新的 AWS、行业建议以及威胁情报信息可帮助您改进您的威胁模型和控制目标。实现安全流程、测试和验证的自动化可扩展您的安全运营。

利用威胁模型发现风险并确定风险优先级：利用威胁模型发现潜在威胁，并维护一个最新的潜在威胁登记表。确定您的威胁优先级并调整您的安全控制措施，以进行防范、检测和响应。在不断变化的安全环境中，重新审视和维护此登记表。

确定并验证控制目标：根据您的合规性要求以及从威胁模型中发现的风险，获得并验证您需要应用于工作负载的控制目标和控制措施。持续验证控制目标和控制措施可帮助您衡量风险缓解措施的有效性。

及时了解最新的安全威胁：通过及时了解最新的安全威胁来识别攻击媒介，以帮助您定义并实施适当的控制措施。

及时了解最新的安全建议：及时了解最新的 AWS 和行业安全建议，以改善您的工作负载安全状况。

定期评估并实施新的安全服务和功能：评估并实施 AWS 和 APN 合作伙伴提供的安全服务和功能，以改善您的工作负载安全状况。

在管道中自动测试和验证安全控制措施：为您在构建管道和流程时测试并验证的安全机制建立可靠的基准和模板。利用工具和自动化功能，持续测试并验证所有的安全控制措施。例如，将机器映像和基础设施等项目作为代码模板进行扫描，以发现安全漏洞、异常以及与每个阶段的既定基准的偏差。

减少引入到生产环境中的安全性错误配置的数量至关重要——在构建过程中，可以执行的质量控制和可以减少的缺陷越多越好。设计持续集成和持续部署 (CI/CD) 管道，以便尽可能测试安全问题。CI/CD 管道提供了在构建和交付的每个阶段增强安全性的机会。还必须确保 CI/CD 安全工具始终是最新版本，以减轻不断变化的威胁。

资源

请参阅以下资源，以详细了解如何安全地操作您的工作负载。

视频

- 架构完善的安全性最佳实践
- 利用自动化和监管，支持大规模采用 AWS
- AWS Security Hub：管理安全警报和自动化合规性
- 在 AWS 上实现安全性自动化

文档

- 安全流程概述
- 安全公告
- 安全性博客
- AWS 的新增功能
- AWS 安全审计指导原则
- 在 AWS 上设置 CI/CD 管道

AWS 账户管理和分离

我们建议您根据函数、合规性要求或一组通用控制措施，在单独的账户和组账户中组织工作负载，而不是镜像您所在组织的报告结构。在 AWS 中，账户是供您的资源使用的硬边界、零信任容器。例如，强烈建议执行账户级分离，以使生产工作负载与开发和测试工作负载分离。

基于账户分离工作负载：从安全性和基础设施入手，随着工作负载的增长，使您的组织能够设置通用防护。这种方法在工作负载之间提供了边界和控制。强烈建议执行账户级分离，以使生产环境与开发和测试环境分离，或者在需要处理外部合规性要求（例如 PCI-DSS 或 HIPAA）所定义的各级敏感数据的工作负载与无需处理这些数据的工作负载之间提供强大的逻辑边界。

保护 AWS 账户：可以通过很多方法保护您的 AWS 账户，包括保护而不是使用根用户，并及时更新联系人信息。随着您的工作负载增长和扩展，您可以使用 AWS Organizations 集中管理和控制您的账户。AWS Organizations 可以帮助您管理账户、设置控制以及跨账户配置服务。

集中管理账户：AWS Organizations 自动创建和管理 AWS 账户，并在创建这些账户之后控制它们。当您通过 AWS Organizations 创建账户时，请务必考虑使用您的电子邮件地址，因为这将是允许重置密码的根用户。Organizations 允许您根据工作负载的要求和用途，将账户分组为代表不同环境的组织部门 (OU)。

集中设置控制：在适当的级别，只允许特定的服务、区域和服务操作，以控制您的 AWS 账户能够执行的操作。AWS Organizations 允许您使用服务控制策略 (SCP)，在组织、组织部门或账户级别应用权限防护机制，此操作适用于所有 AWS Identity and Access Management (IAM) 用户和角色。例如，您可以利用 SCP 禁止用户从您未明确允许的 AWS 区域启动资源。AWS Control Tower 能够以一种简化的方式设置和管理多个账户。它会自动在您的 AWS Organization 中设置账户、自动预置、应用防护机制（包括预防和检测），并提供一个仪表板以使您获得可见性。

集中配置服务和资源：AWS Organizations 可帮助您配置 AWS 服务，这些服务将应用于您的所有账户。例如，您可以使用 AWS CloudTrail 配置集中日志记录功能，以记录在您的组织中执行的所有操作，并禁止成员账户禁用日志记录功能。您也可以使用 AWS Config 集中聚合您定义的规则的数据，以便能够审计您的工作负载是否合规，并快速对变化做出反应。使用 AWS CloudFormation StackSets，您可以在您的组织中跨账户和 OU 集中管理 AWS CloudFormation 堆栈。这样，您就可以自动预置一个新账户，以满足您的安全要求。

资源

请参阅以下资源，以详细了解 AWS 对于部署和管理多个 AWS 账户的建议。

视频

- 使用 AWS Organizations 管理和监管多账户 AWS 环境
- AXA：使用全局登录区扩大采用规模
- 使用 AWS Control Tower 监管多账户 AWS 环境

文档

- 建立您的 AWS 最佳实践环境
- AWS Organizations
- AWS Control Tower
- 使用 AWS CloudFormation StackSets
- 如何使用服务控制策略设置您在 AWS Organizations 中的跨账户权限防护机制

动手实践

- 实验室：AWS 账户和根用户

Identity and Access Management

要使用 AWS 服务，您必须为您的用户和应用程序授予访问权限，以使他们/它们能够访问您 AWS 账户中的资源。当您在 AWS 上运行更多的工作负载时，您需要实施强大的身份管理和权限，以确保适当的人员在适当的条件下有权访问适当的资源。AWS 提供了大量的功能，以帮助您管理您的人员和机器身份及其权限。这些功能的最佳实践分为两个主要领域：

- 身份管理
- 权限管理

身份管理

在访问和运行安全的 AWS 工作负载时，您需要管理两种类型的身份。

人员身份：管理员、开发人员、操作员以及您的应用程序的消费者需要拥有身份，才能访问您的 AWS 环境和应用程序。他们可能是您的组织成员或与您协作的外部用户，也可能是通过 Web 浏览器、客户端应用程序、移动应用程序或交互式命令行工具与您的 AWS 资源交互的用户。

机器身份：您的工作负载应用程序、操作工具和组件需要拥有身份，才能向 AWS 服务发出请求以执行某种操作，例如读取数据。这些身份包括在 AWS 环境中运行的机器，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以管理需要访问权限的外部各方的机器身份。此外，您可能还有需要访问您 AWS 环境的 AWS 之外的机器。

依赖集中式身份提供商

对于员工身份，依赖身份提供商，使您能够在集中位置管理身份。这样，您就可以更轻松地管理跨多个应用程序和服务的访问权限，因为您在从单一位置创建、管理和撤销访问权限。例如，如果有人离开了您的组织，您可以从一个位置撤销此人对所有应用程序和服务（包括 AWS）的访问权限。这样就降低了对多个凭证的需求，并提供了与现有的人力资源 (HR) 流程集成的机会。

要与单独的 AWS 账户联合，您可以将用于 AWS 的集中身份与基于 SAML 2.0 并支持 AWS IAM 的提供程序结合使用。您可以使用与 SAML 2.0 协议兼容的任何提供程序 - 无论是由您在 AWS 中托管的提供程序、AWS 外部的提供程序还是由 AWS 合作伙伴网络 (APN) 提供的提供程序。您可以使用您的 AWS 账户与您选择的提供程序之间的联合，为用户或应用程序授予访问权限，以使

他们能够使用 SAML 断言获得临时安全凭证，以调用 AWS API 操作。也支持基于 Web 的单点登录，因此允许用户从您的登录门户登录到 AWS 管理控制台。

要与您的 AWS 组织中的多个账户联合，您可以在 AWS Single Sign-On (AWS SSO) 中配置您的身份源，并指定您的用户和组的存储位置。配置之后，您的身份提供程序将是您的事实来源，并可以使用跨域身份管理系统 (SCIM) v2.0 协议来同步信息。随后，您可以查找用户或组，并授予他们单点登录访问权限，以使他们能够访问 AWS 账户和/或云应用程序。

AWS SSO 与 AWS Organizations 集成，这样，您就可以配置您的身份提供程序，然后为您的组织中管理的现有账户和新账户授予访问权限。AWS SSO 为您提供了一个默认存储库，您可以使用它来管理您的用户和组。如果您选择使用 AWS SSO 存储库，请创建您的用户和组，并为他们分配对您的 AWS 账户和应用程序的访问权限级别，同时铭记最小特权最佳实践。您也可以选择使用 SAML 2.0 连接到您的外部身份提供程序，或者使用 AWS Directory Service 连接到您的 Microsoft AD 目录。配置之后，您可以通过您的中央身份提供程序进行身份验证，以登录到 AWS 管理控制台、命令行界面或 AWS 移动应用程序。

要管理您的工作负载的最终用户或消费者，例如移动应用程序，您可以使用 Amazon Cognito。它为您的 Web 和移动应用程序提供了身份验证、授权和用户管理功能。您的用户可以直接使用用户名和密码登录，也可以通过第三方（例如 Amazon、Apple、Facebook 或 Google）登录。

利用用户组和属性

随着您管理的用户数量不断增加，您需要确定如何组织这些用户，以便能够实现规模管理。将具有常见安全要求的用户置于由您的身份提供程序定义的组中，并建立机制以确保用于访问控制的用户属性（例如部门或位置）正确无误且已更新。使用这些组和属性（而不是单个用户）来控制访问权限。这样，您就可以通过使用权限集一次性更改用户的组成员身份或属性来集中管理访问，而不是在需要更改用户的访问权限时更新多个单独策略。您可以使用 AWS SSO 来管理用户组和属性。AWS SSO 支持最常用的属性，无论是在创建用户时手动输入的属性还是使用同步引擎自动预置的属性，例如跨域身份管理系统 (SCIM) 规范中定义的那些属性。

使用强大的登录机制

强制执行最小密码长度策略，并指导您的用户避免使用常见或重复使用过的密码。使用软件或硬件机制实施 Multi-Factor Authentication (MFA)，以提供一层额外的保护。例如，当使用 AWS SSO 作为身份源时，请为 MFA 配置“背景认知”或“始终开启”设置，并允许用户注册自己的 MFA 设备以加快采用。当使用外部身份提供程序 (IdP) 时，请为 MFA 配置您的 IdP。

使用临时凭证

需要身份以动态获取临时凭证。对于员工身份，使用 AWS SSO 或与 IAM 联合，以访问 AWS 账户。对于机器身份，例如 EC2 实例或 Lambda 函数，要求使用 IAM 角色，而不是拥有长期访问密钥的 IAM 用户。

对于使用 AWS 管理控制台的人员身份，要求用户获取临时凭证并联合到 AWS 中。为此，您可以使用 AWS SSO 用户门户，或者配置与 IAM 的联合。对于需要访问 CLI 的用户，请确保他们使用支持与 AWS Single Sign-On (AWS SSO) 直接集成的 AWS CLI v2。用户可以创建链接到 AWS SSO 账户和角色的 CLI 配置文件。CLI 会自动从 AWS SSO 检索 AWS 凭证，并代表您刷新这些凭证。这样就无需从 AWS SSO 控制台复制并粘贴临时 AWS 凭证。对于 SDK，用户应依靠 AWS STS 来代入角色，以接收临时凭证。在某些情况下，使用临时凭证可能并不现实。您应了解存储访问密钥的风险、经常轮换这些密钥，并尽可能要求使用 MFA 作为一项条件。

当您需要授权消费者访问您的 AWS 资源时，请使用 Amazon Cognito 身份池，并为他们分配一组临时有限特权凭证，以使他们能够访问您的 AWS 资源。通过您创建的 IAM 角色控制每个用户的权限。您可以定义规则，以根据用户的 ID 令牌中的声明，为每个用户选择角色。您可以为通过身份验证的用户定义一个默认角色。对于未通过身份验证的访客用户，您还可以定义一个拥有有限权限的单独 IAM 角色。

对于机器身份，您应依靠 IAM 角色授予对 AWS 的访问权限。对于 EC2 实例，您可以使用用于 Amazon EC2 的角色。您可以将 IAM 角色附加到您的 EC2 实例，以使您在 Amazon EC2 上运行的应用程序能够使用 AWS 创建的临时安全凭证，并自动进行轮换。要使用密钥或密码访问 EC2 实例，AWS Systems Manager 是一种更安全的方法，它允许您使用预安装的代理来访问和管理实例，而无需使用存储的密钥。此外，您也可以使用其他 AWS 服务（例如 AWS Lambda）来配置 IAM 服务角色，以授权此服务利用临时凭证执行 AWS 操作。

定期审计和轮换凭证

（最好通过自动化工具）定期验证，以确保实施正确的控制措施。对于人员身份，您应要求用户定期更改他们的密码并弃用访问密钥，以支持临时凭证。我们还建议您持续监控您的身份提供程序中的 MFA 设置。您可以设置 AWS Config 规则，以监控这些设置。对于机器身份，您应依靠使用 IAM 角色的临时凭证。当无法执行此操作时，需要经常审计和轮换访问密钥。

安全存储和使用密钥

对于并非 IAM 相关的凭证，如数据库登录，请使用一种专门用于处理密钥管理的服务，比如 AWS Secrets Manager。借助 AWS Secrets Manager，您可以使用支持的服务轻松管理、轮换和安全地存储加密密钥。为访问密钥而执行的调用将记录到 CloudTrail 中以进行审计，IAM 权限可以为它们授予最小特权访问权限。

资源

请参阅以下资源，以详细了解有关保护您的 AWS 凭证的 AWS 最佳实践。

视频

- 在每个层面掌握身份
- 使用 AWS SSO 大规模管理用户权限
- 有关大规模管理、检索和轮换密钥的最佳实践

文档

- AWS 账户根用户
- AWS 账户根用户凭证与 IAM 用户凭证
- IAM 最佳实践
- 为 IAM 用户设置账户密码策略
- AWS Secrets Manager 入门
- 使用实例配置文件

- 临时安全凭证
- 身份提供程序和联合

权限管理

管理权限以控制对需要访问 AWS 和您的工作负载的人员和机器身份的访问。权限用于控制哪些人可以在什么条件下访问哪些内容。为特定的人员身份和机器身份设置权限，以授权他们/它们访问特定资源上的特定服务操作。此外，为要授予的访问权限指定必须满足的条件。例如，您可以允许开发人员创建新的 Lambda 函数，但只能在特定的区域中创建。当大规模管理您的 AWS 环境时，请遵循以下最佳实践，以确保身份只拥有他们/它们所需的访问权限，而没有任何多余的权限。

为您的组织定义权限防护机制

当您在 AWS 中的工作负载增多并管理这些额外的工作负载时，您应使用账户分离这些工作负载，并使用 AWS Organizations 管理这些账户。我们建议您建立常用权限防护机制，以限制您所在组织中的所有身份的访问权限。例如，您可以限制对特定 AWS 区域的访问，或防止您的团队删除常见资源，例如您的核心安全团队使用的 IAM 角色。您可以首先实施服务控制策略示例，例如禁止用户禁用密钥服务。

您可以使用 AWS Organizations 将账户分组，并为每组账户设置常用控制措施。要设置这些常用控制措施，您可以使用与 AWS Organizations 集成的服务。具体来说，您可以使用服务控制策略 (SCP) 来限制账户组的访问权限。SCP 使用 IAM 策略语言，并允许您建立所有 IAM 委托人（用户和角色）都要遵循的控制措施。您可以限制对特定服务操作和资源的访问，并根据特定的条件限制访问，以满足您所在组织的访问控制需求。如有必要，您可以为您的防护机制定义异常情况。例如，您可以为账户中除特定管理员角色以外的所有 IAM 实体限制服务操作。

授予最小特权访问权限

建立最小特权原则可确保身份只能执行完成特定任务所需的最小功能集，同时实现可用性和效率的平衡。按照此原则进行操作可以限制意外访问，并有助于确保您能够审计哪些用户有权访问哪些资源。在 AWS 中，默认情况下，除根用户以外的身份没有任何权限，而根用户只能用于执行几项特定任务。

您可以使用策略来显式授予附加到 IAM 或资源实体的权限，例如联合身份或计算机所使用的 IAM 角色或者某些资源（例如 S3 存储桶）。当您创建并附加策略时，您可以指定服务操作、资源以及为使 AWS 允许访问而必须满足的条件。AWS 支持多种条件，以帮助您缩小访问权限范围。例如，使用 PrincipalOrgID 条件键时，将会验证 AWS Organizations 的标识符，以便能够授权在您的 AWS 组织内访问。您还可以使用 CalledVia 条件键控制 AWS 服务代表您发出的请求，例如要求 AWS CloudFormation 创建一个 AWS Lambda 函数。这样，您就可以在 AWS 中为您的人员身份和机器身份设置精细权限。

AWS 还允许您扩展权限管理，并遵循最小特权原则。

权限边界：您可以使用权限边界来设置管理员能够设置的最高权限。这样，您就可以为开发人员赋予创建和管理权限的能力，例如创建一个 IAM 角色，但限制他们可以授予的权限，以使他们无法利用他们创建的角色提升自己的权限。

基于属性的访问控制 (ABAC)：AWS 使您能够基于属性授予权限。在 AWS 中，这些属性称为标签。可以将标签附加到 IAM 委托人（用户或角色）和 AWS 资源。使用 IAM 策略时，管理员可以创建一个可重复使用的策略，以根据 IAM 委托人的属性来应用权限。例如，作为管理员，您可以使用一个 IAM 策略，授权您所在组织中的开发人员访问与这些开发人员的项目标签匹配的 AWS 资源。当这一组开发人员为项目添加资源时，会自动根据属性应用权限。这样就无需为每个新资源执行策略更新。

分析公共和跨账户访问

在 AWS 中，您可以授权访问另一个账户中的资源。您可以使用附加到资源的策略（例如 S3 存储桶策略）授予直接跨账户访问权限，也可以允许某个身份在另一个账户中代入 IAM 角色。当使用资源策略时，您希望确保授权身份在您的组织中进行访问，并有意识地公开资源。应当谨慎地公开资源，因为此操作将允许任何人访问资源。IAM Access Analyzer 使用数学方法（即可证明的安全性）来标识从账户的外部访问某个资源时的所有访问路径。它持续审核资源策略，并报告公开访问和跨账户访问的结果，以使您能够轻松分析可能非常宽泛的访问权限。

安全地共享资源

当您使用不同的账户管理工作负载时，您有时需要在这些账户之间共享资源。我们建议您使用 AWS Resource Access Manager (AWS RAM) 来共享资源。使用此服务，您可以轻松、安全地在您的 AWS 组织和组织部门内共享 AWS 资源。使用 AWS RAM，当账户移进和移出与之共享资源的组织或组织部门时，会自动授予或撤销对共享资源的访问权限。这样有助于您确保只与您的目标账户共享资源。

持续减少权限

当团队和项目刚刚起步时，您有时会选择授予宽泛的访问权限，以激励创新和敏捷性。我们建议您持续评估访问权限，将访问权限限制为所需的最低权限，并实现最小特权。AWS 提供了访问权限分析功能，以帮助您识别未使用的访问权限。为了帮助您识别未使用的用户和角色，AWS 会分析访问活动，并提供关于访问密钥和角色的上次使用情况的信息。您可以使用上次访问时间戳，以识别未使用的用户和角色并将它们移除。此外，您还可以查看关于服务和操作的上次访问情况的信息，并收紧特定用户和角色的权限。 例如，您可以使用关于上次访问情况的信息，以确定您的应用程序角色需要执行的特定 S3 操作，并只允许访问这些操作。控制台中提供了这些功能，您也可以对这些功能进行编程，以便将它们整合到您的基础设施工作流程和自动化工具中。

建立紧急访问流程

您应建立一个流程，以允许在遇到不太可能发生的自动化流程或管道问题时紧急访问您的工作负载，尤其是您 AWS 账户中的工作负载。此流程可能包含不同功能的组合，例如用于访问权限的紧急 AWS 跨账户角色，或者供管理员用来验证和批准紧急请求的特定流程。

资源

请参阅以下资源，以详细了解有关精细授权的最新 AWS 最佳实践。

视频

- 在最多 60 分钟的时间内成为 IAM 策略高手
- 职责分离、最小特权、委托和 CI/CD

文档

- 授予最小特权
- 使用策略
- 委派权限以管理 IAM 用户、组和凭证
- IAM Access Analyzer
- 移除不必要的凭证
- 在启用 MFA 的 CLI 中代入角色
- 权限边界
- 基于属性的访问控制 (ABAC)

动手实践

- 实验室：IAM 权限边界委派角色创建
- 实验室：基于 IAM 标签的 EC2 访问控制
- 实验室：Lambda 跨账户 IAM 角色代入

检测

使用检测功能，您可以识别潜在安全配置错误、威胁或意外行为。检测是安全生命周期的重要组成部分，可用于支持质量流程、法律或合规义务，还可以用于威胁识别和响应工作。检测机制分为多种不同的类型。例如，可以分析来自您工作负载的日志，以找到正在被利用的漏洞。您应定期查看与您的工作负载相关的检测机制，以确保符合内部和外部的策略和要求。自动化警报和通知应基于所定义的条件，以使您的团队或工具能够执行调查。这些机制都是重要的响应手段，可以帮助您的组织识别和了解异常活动的范围。

在 AWS 中，可以使用很多方法来解决检测性机制问题。以下部分介绍了如何使用这些方法：

- 配置
- 调查

配置

配置服务和应用程序日志记录：基本做法是在账户级别建立一套检测机制。这套基本机制的目的是记录和检测对您账户中的所有资源执行的多种操作。它们允许您构建全面的检测能力和一些用于添加功能的选项，包括自动修复和合作伙伴集成。

在 AWS 中，这套基本机制中的服务包括：

- AWS CloudTrail 可提供 AWS 账户活动的事件历史记录，包括通过 AWS 管理控制台、AWS 开发工具包、命令行工具和其他 AWS 服务执行的操作。
- AWS Config 监控和记录您的 AWS 资源配置，并允许您对照所需的配置自动执行评估和修复。
- Amazon GuardDuty 是一种威胁检测服务，可持续监控恶意活动和未经授权的行为，从而保护您的 AWS 账户和工作负载。
- AWS Security Hub 集中聚合、组织和优先处理来自多个 AWS 服务和可选第三方产品的安全警报或调查结果，以使您全面了解安全警报和合规性状态。

在账户级别构建基础时，很多核心 AWS 服务（例如 Amazon Virtual Private Cloud (VPC)）提供了服务级别的日志记录功能。您可以使用 VPC 流日志来捕获有关传入和传出网络接口的 IP 流量的信息，这些信息可提供对于连接历史记录的宝贵见解，并根据异常行为触发自动操作。

对于并非起源于 AWS 服务的 EC2 实例和基于应用程序的日志记录，可以使用 Amazon CloudWatch Logs 来存储和分析日志。代理将从正在运行的操作系统和应用程序收集日志，并自动存储这些日志。当这些日志在 CloudWatch Logs 中可用之后，您即可实时处理它们，或者使用 Insights 进行深入分析。

与收集和聚合日志同样重要的是，要能够从复杂的架构生成的大量日志和事件数据中提取有意义的见解。有关更多详细信息，请参阅可靠性支柱白皮书的*监控*部分。日志自身可能包含敏感数据——当应用程序数据以错误的方式进入 CloudWatch Logs 捕获的日志文件中，或者为日志聚合功能配置了跨区域日志记录并且在跨境传输某些类型的信息时需要注意一些法律事项时。

一种方法是使用在提供日志时触发的 Lambda 函数，以筛选和编辑日志数据，然后将其转发到中央日志记录位置，例如 S3 存储桶。可以将未编辑的日志保留在本地存储桶中，直到“合理的时间”结束（由法律和您的法律团队决定），届时 S3 生命周期规则会自动将它们删除。可以使用 S3 对象锁定功能在 Amazon S3 中进一步保护日志，在 Amazon S3 中，您可以使用“一次写入多次读取”(WORM) 模式来存储对象。

集中分析日志、调查结果和指标：安全运营团队依靠收集日志和使用搜索工具来发现需要关注的潜在事件，这些事件可能代表未经授权的活动或无意的更改。但是，仅仅分析收集的数据和手动处理信息不足以应对从复杂架构流出的大量信息。单凭分析和报告无法及时分配合适的资源来处理事件。

建立成熟的安全运营团队的最佳实践是将安全事件和调查结果的流程深度集成到通知和工作流系统中，例如票证系统、错误/问题系统或其他安全信息和事件管理 (SIEM) 系统。这样，工作流可以摆脱电子邮件和静态报告，让您能够路由、上报和管理事件或调查结果。许多组织也在逐步将安全警报集成到他们的聊天/协作和开发人员工作效率平台中。对于正在踏上自动化之旅的组织，一个由 API 驱动的低延迟票证系统能够在规划“首要自动化任务”时提供极高的灵活性。

这种最佳实践不仅适用于从描述用户活动或网络事件的日志消息生成的安全事件，还适用于在基础设施本身检测到的更改生成的安全事件。当面对一些更改，而且这些更改的不受欢迎程度足够微妙，以致于目前无法使用一组 IAM 和 Organizations 配置来防止这些更改发生时，为了保持和

验证安全架构，必须能够检测更改、确定更改是否适当，然后将这些信息路由到正确的修复工作流程。

GuardDuty 和 Security Hub 为日志记录提供了聚合、重复数据删除和分析机制，您也可以通过其他 AWS 服务提供这些机制。具体来说，GuardDuty 提取、聚合和分析来自 VPC DNS 服务的信息以及您也可以通过 CloudTrail 和 VPC 流日志查看的那些信息。Security Hub 能够提取、聚合和分析来自 GuardDuty、AWS Config、Amazon Inspector、Macie、AWS Firewall Manager 以及 AWS Marketplace 中提供的大量第三方安全产品的输出，如果您相应构建了自己的代码，还将包括这些代码。GuardDuty 和 Security Hub 都有一个主节点-成员模型，此模型可以跨多个账户聚合调查结果和见解，拥有本地 SIEM 的客户通常将 Security Hub 用作 AWS 端日志和警报预处理器和聚合器，随后即可通过基于 Lambda 的处理器和转发服务器从 Security Hub 中提取 Amazon EventBridge。

资源

请参阅以下资源，以详细了解有关捕获和分析日志的最新 AWS 建议。

视频

- 云中的威胁管理：Amazon GuardDuty 和 AWS Security Hub
- 集中监控资源配置和合规性

文档

- 设置 Amazon GuardDuty
- AWS Security Hub
- 入门：Amazon CloudWatch Logs
- Amazon EventBridge
- 配置 Athena 以分析 CloudTrail 日志
- Amazon CloudWatch
- AWS Config
- 在 CloudTrail 中创建跟踪

- 集中日志记录解决方案

动手实践

- 实验室：启用 Security Hub
- 实验室：自动部署检测性控制
- 实验室：Amazon GuardDuty 动手实践

调查

实施可行的安全事件：对于您的每个检测性机制，您还应调查一个以运行手册或行动手册形式存在的流程。例如，当您启用 Amazon GuardDuty 时，它会生成不同的调查结果。您的每个调查结果类型都应具有一个运行手册条目，例如，如果发现了特洛伊木马程序，您的运行手册的简单说明可以指示某个人员进行调查和修复。

自动响应事件：在 AWS 中，可以使用 Amazon EventBridge 调查感兴趣的事件以及自动化工作流程可能发生的意外变化的相关信息。此服务提供可扩展的规则引擎，可代理原生 AWS 事件格式（例如 CloudTrail 事件）以及您可以从应用程序中生成的自定义事件。Amazon EventBridge 还允许您将这些事件路由到构建事件响应系统 (Step Functions) 的工作流程系统中，或者路由到中央安全账户或存储桶中以执行进一步分析。

也可以使用 AWS Config 规则检测更改并将此信息路由到正确的工作流程。AWS Config 会检测对范围内服务的更改（尽管延迟要高于 Amazon EventBridge），并生成可使用 AWS Config 规则进行解析的事件，以便进行回滚、强制实施合规性策略以及将信息转发到相关系统（例如变更管理平台和运营票证系统）。除了编写您自己的 Lambda 函数以响应 AWS Config 事件，您还可以充分利用 AWS Config 规则开发工具包以及一组开源 AWS Config 规则。

资源

请参阅以下资源，以详细了解有关将审计控制与通知和工作流程集成的最新 AWS 最佳实践。

视频

- Amazon Detective
- 修复 Amazon GuardDuty 和 AWS Security Hub 调查结果

- 有关在 AWS 中管理安全操作的最佳实践
- 使用 AWS Config 实现连续合规性

文档

- Amazon Detective
- Amazon EventBridge
- AWS Config 规则
- AWS Config 规则存储库（开源）
- AWS Config 规则开发工具包

动手实践

- 解决方案：关于 AWS 账户活动的实时见解
- 解决方案：集中式日志记录

基础设施保护

基础设施保护包括满足最佳实践和组织、法律及监管义务所必需的控制方法（例如深度防御）。使用这些方法对于在云中持续成功运营至关重要。

基础设施保护是信息安全计划的关键组成部分之一。它可以确保您的工作负载中的系统和服务受到保护，防止意外和未经授权的访问以及潜在的漏洞对其造成危害。例如，您可以定义信任边界（例如网络边界和账户边界）、系统安全配置和维护（例如强化、最小化和修补）、操作系统身份验证和授权（例如用户、密钥和访问级别）以及其他适当的策略执行点（例如 Web 应用程序防火墙和/或 API 网关）。

在 AWS 中，有许多基础设施保护方法。以下部分介绍了如何使用这些方法：

- 保护网络
- 保护计算

保护网络

妥善规划和管理您的网络设计，这是为您工作负载中的资源提供分离和边界的基础。由于您工作负载中的很多资源都运行在 VPC 中并继承安全属性，因此必须使用由自动化作为后盾的检查和保护机制来支持设计。同样，对于在 VPC 之外运行的工作负载，当使用纯粹边缘服务和/或无服务器环境时，这些最佳实践适用于更加简化的方法。请参阅 AWS 架构完善的无服务器应用程序镜头，以获得有关无服务器安全性的特定指导。

创建网络层：具有相同可访问性要求的组件（例如 Amazon EC2 实例、Amazon RDS 数据库集群和 Amazon Lambda 函数）可细分为由子网构成的层。例如，应将 VPC 中的一个无需互联网访问的 Amazon RDS 数据库集群放在无法向/从互联网路由的子网中。此分层控制方法可减轻单层错误配置的影响，这种错误可能允许意外访问。对于 AWS Lambda，您可以在 VPC 中运行您的函数，以充分利用基于 VPC 的控制。

对于可能包含数千个 VPC、AWS 账户和本地网络的网络连接，您应使用 AWS Transit Gateway。它充当一个枢纽，以控制如何在类似于辐条的所有互联网络之间路由流量。Amazon VPC 与 AWS Transit Gateway 之间的流量保留在 AWS 私有网络中，可减少外部威胁媒介，例如分布式拒绝服务 (DDoS) 攻击和常见漏洞（SQL 注入、跨站点脚本、跨站点请求伪造或滥用损坏的身份验证代码等等）。AWS Transit Gateway 区域间对等也会对区域间流量加密，而且不会出现任何单点故障或带宽瓶颈。

在所有层控制流量：当构建您的网络拓扑时，您应检查每个组件的连接要求。例如，某个组件是否需要互联网可访问性（入站和出站）、连接到 VPC 的能力、边缘服务和外部数据中心。

使用 VPC，您可以使用您设置的私有 IPv4 地址范围或者 AWS 选择的 IPv6 地址范围来定义跨 AWS 区域的网络拓扑。对于入站和出站流量，您应采用深度防御方法应用多种控制，包括使用安全组（状态检测防火墙）、网络 ACL、子网和路由表。在 VPC 中，您可以在可用区中创建子网。每个子网都可以拥有一个关联的路由表，此表定义了用于管理流量在子网内所采用路径的路由规则。您可以将要连接到互联网或 NAT 网关的路由连接到 VPC 或使其经过另一个 VPC，以定义互联网可路由子网。

当在 VPC 内启动某个实例、RDS 数据库或其他服务时，它的每个网络接口都有自己的安全组。此防火墙位于操作系统层之外，可用于定义允许入站和出站流量的规则。您还可以定义安全组之间的关系。例如，通过参考对相关的实例应用的安全组，数据库层安全组中的实例仅接受来自应用程

序层内实例的流量。除非您在使用非 TCP 协议，否则不必在没有负载均衡器或 CloudFront 的情况下允许互联网直接访问 EC2 实例（甚至使用安全组禁止使用的端口）。这样有助于防止通过操作系统或应用程序问题进行意外访问。您还可以为子网附加网络 ACL，它将用作无状态防火墙。您应配置网络 ACL 以缩小各层之间允许的流量范围，但请注意，您需要定义入站和出站规则。

尽管某些 AWS 服务要求组件能够访问互联网以进行 API 调用（这是 AWS API 终端节点所在的位置），但其他服务会使用您 VPC 内的终端节点。很多 AWS 服务（包括 Amazon S3 和 Amazon DynamoDB）都支持 VPC 终端节点，并且 AWS PrivateLink 中已广泛使用此技术。对于需要出站连接到互联网的 VPC 资产，可以让它们通过 AWS 托管的 NAT 网关、仅出站的互联网网关或者您创建并管理的 Web 代理进行仅出站（单向）连接。

实施检查和保护：在每个层检查并筛选您的流量。对于通过基于 HTTP 的协议处理的组件，Web 应用程序防火墙可帮助防止常见的攻击。AWS WAF 是一个 Web 应用程序防火墙，可监控和拦截与转发到 Amazon API Gateway API、Amazon CloudFront 或 Application Load Balancer 的可配置规则匹配的 HTTP(s) 请求。要开始使用 AWS WAF，您可以将 AWS 托管规则与您自己的规则结合使用，也可以使用现有的合作伙伴集成。

要管理 AWS WAF、AWS Shield Advanced 保护以及跨 AWS Organizations 的 Amazon VPC 安全组，您可以使用 AWS Firewall Manager。它允许您跨账户和应用程序集中配置和管理防火墙规则，从而更轻松地扩展常见规则的实施。它还使用 AWS Shield Advanced 或者能够自动拦截向您的 Web 应用程序发送非必要请求的解决方案，以使您能够快速响应攻击。

自动化网络保护：自动运行保护机制，以提供基于威胁情报和异常检测的自我防御网络。例如可应对最新的威胁并减轻它们的影响的那些入侵检测和预防工具。您可以在 Web 应用程序防火墙等方面自动化网络保护，例如使用 AWS WAF Security Automations 解决方案 (https://github.com/awslabs/aws-waf-security-automations) 来自动拦截来自已知威胁媒介相关 IP 地址的请求。

资源

请参阅以下资源，以详细了解有关保护网络的 AWS 最佳实践。

视频

- 用于各种 VPC 的 AWS Transit Gateway 参考架构

- 使用 Amazon CloudFront、AWS WAF 和 AWS Shield 提供应用程序加速和保护
- 大规模 DDoS 攻击检测

文档

- Amazon VPC 文档
- AWS WAF 入门
- 网络访问控制列表
- 您的 VPC 的安全组
- 您的 VPC 的推荐网络 ACL 规则
- AWS Firewall Manager
- AWS PrivateLink
- VPC 终端节点
- Amazon Inspector

动手实践

- 实验室：自动部署 VPC
- 实验室：自动部署 Web 应用程序防火墙

保护计算

执行漏洞管理：频繁扫描和修补您的代码、依赖关系和基础设施中的漏洞，以帮助抵御新的威胁。

使用构建和部署管道，您可以自动执行很多漏洞管理工作：

- 使用第三方静态代码分析工具来发现常见安全问题，例如未检查的函数输入边界以及较新的 CVE。您可以对所支持的语言使用 Amazon CodeGuru。
- 使用第三方依赖关系检查工具，确定您的代码链接的库是否是最新版本、它们是否不含 CVE，并确保您拥有符合您软件策略要求的许可条件。

- 使用 Amazon Inspector，您可以针对您的实例对已知的常见弱点和漏洞 (CVE) 执行配置评估、根据安全基准执行评估以及实现缺陷通知完全自动化。Amazon Inspector 在生产实例或构建管道中运行，它会在发现结果时通知开发人员和工程师。您可以通过编程方式访问结果，并将您的团队引导至待办事项和错误跟踪系统。EC2 Image Builder 可通过自动化修补、AWS 提供的安全策略实施和其他自定义来维护服务器映像 (AMI)。
- 当使用容器时，在您的构建管道中对您的映像存储库定期实施 ECR 映像扫描，以便在您的容器中查找 CVE。
- 尽管 Amazon Inspector 和其他工具能够有效地确定配置和存在的任何 CVE，但也需要使用其他方法在应用程序级别测试您的工作负载。模糊是一种众所周知的查错方法，可自动将格式不正确的数据注入到您应用程序的输入字段和其他区域来查错。

很多这样的函数可以由 AWS 服务、AWS Marketplace 中的产品或开源工具来执行。

缩小攻击面：强化操作系统以及尽量减少所使用的组件、库和外部可用的服务，以缩小您的攻击面。为了缩小您的攻击面，您需要使用威胁模型来确定入口点和可能遇到的威胁。一种常见的缩小攻击面做法是首先减少未使用的组件，无论它们是操作系统程序包、应用程序等等（适用于基于 EC2 的工作负载）还是您代码中的外部软件模块（适用于所有工作负载）。对于常见的操作系统和服务器软件（例如互联网安全中心中的那些操作系统和服务器软件），您可以将很多强化和安全配置指南用作起点并进行迭代。

帮助人员远程执行操作：禁止交互式访问可以降低人为犯错的风险以及手动配置或管理的可能性。例如，利用变更管理工作流程，借助 AWS Systems Manager 等工具管理 EC2 实例，而不是允许直接访问或通过堡垒主机进行访问。AWS Systems Manager 可使用自动化工作流程、文档（行动手册）和运行命令等功能自动执行多种维护和部署任务。AWS CloudFormation 堆栈从管道进行构建，并能够自动执行您的基础设施部署和管理任务，而无需直接使用 AWS 管理控制台或 API。

实施托管服务：实施用于托管资源的服务，例如 Amazon RDS、AWS Lambda 和 Amazon ECS，以便在责任共担模式中减少安全维护任务。例如，Amazon RDS 可帮助您设置、操作和扩展关系数据库，并自动执行管理任务，例如硬件预置、数据库设置、修补和备份。这意味着您将有更多的空闲时间，因此可以专注于通过 AWS 架构完善的框架中所述的其他方法来保护您的应用程序。使用 AWS Lambda，无需使用预置或托管服务器即可运行代码，因此您只需在代码级别而不是基础设施或操作系统级别专注于连接、调用和安全性。

验证软件完整性：实施一些机制（例如代码签名），以确保工作负载中使用的软件、代码和库来自可信的来源且未被篡改。例如，您应验证二进制文件和脚本的代码签名证书以确认作者，并确保证书自作者创建以来未被篡改。此外，通过将您下载的软件的校验和与提供商提供的校验和进行对比，可帮助确保它未被篡改。

自动保护计算：自动化您的计算保护机制，包括漏洞管理、缩小攻击面和管理资源。此自动化将帮助您投入时间以保护工作负载的其他方面，并降低人为犯错的风险。

资源

请参阅以下资源，以详细了解有关保护计算的 AWS 最佳实践。

视频

- 有关 Amazon EC2 实例元数据服务的安全最佳实践
- 在 AWS 上保护您的数据块存储
- 保护无服务器和容器服务
- 在 Amazon EKS 上运行高安全性工作负载
- 在 Amazon EKS 中通过策略防护构建安全性

文档

- AWS Lambda 安全性概述
- Amazon EC2 中的安全性
- AWS Systems Manager
- Amazon Inspector
- 编写您自己的 AWS Systems Manager 文档
- 使用 Amazon EC2 Systems Manager 更换堡垒主机

动手实践

- 实验室：自动部署 EC2 Web 应用程序

数据保护

在为任何工作负载设计架构之前，您应确定可能影响安全性的基本实践。例如，数据分级提供了一种基于敏感程度对数据进行分类的方法，加密通过让未经授权的用户无法获知数据的真正内容来保护数据。这些方法非常重要，因为它们有助于实现诸如履行监管义务或避免处理不当等目标。

在 AWS 中，实施数据保护时可以使用很多不同的方法。以下部分介绍了如何使用这些方法：

- 数据分类
- 保护静态数据
- 保护传输中的数据

数据分类

数据分类提供了一种基于关键性和敏感度对组织数据进行分类的方法，以帮助您确定适当的保护和保留控制措施。

识别您工作负载内的数据：您需要了解您的工作负载正在处理的数据的类型和分类、相关的业务流程、数据所有者、适用的法律和合规性要求、数据的存储位置以及因此需要实施的控制措施。这可能包括用于指明数据是可公开访问、仅供内部使用（例如客户的个人可识别信息 (PII)）还是受到更加严格的访问限制（例如知识产权、法律特权数据或敏感数据等等）的分类。通过谨慎管理适当的数据分级系统以及每个工作负载的保护要求级别，您可以匹配适用于数据的控制和访问/保护级别。例如，公开内容可供任何人访问，而重要内容则以受保护的方式进行加密和存储，需要授权访问密钥才能解密。

定义数据保护控制：通过使用资源标签、根据敏感度（可能还包括附加说明/包体/感兴趣的社区）划分的单独 AWS 账户、IAM 策略、组织 SCP、AWS KMS 和 AWS CloudHSM，您可以定义并实施您的数据分类和加密保护策略。例如，如果您的项目具有包含极关键数据的 S3 存储桶或者处理机密数据的 EC2 实例，则可以使用“Project=ABC”标记对其进行标记。只有您的直属团队知道项目代码的含义，它提供了一种使用基于属性的访问控制措施的方法。您可以通过关键策略和授权定义对 AWS KMS 加密密钥的访问级别，以确保只有适当的服务可以通过安全机制访问敏

感内容。如果您正在根据标签做出授权决定，您应确保在 AWS Organizations 中使用标签策略适当定义对于标签的权限。

定义数据生命周期管理：您定义的生命周期策略应基于敏感性级别以及法律和组织要求。应考虑您的数据保留期限、数据销毁流程、数据访问管理、数据转换和数据共享等方面。当选择数据分类方法时，请平衡可用性与访问权限。您还应考虑多种访问级别及其细微差别，以便针对每个级别实施安全且有效的方法。始终采用深度防御方法并减少人工访问数据次数以及数据转换、删除或复制机制。例如，要求用户对应用程序执行严格身份验证，并为应用程序而不是用户授予执行“远程操作”的必要访问权限。 此外，确保用户来自可信网络路径并要求其获取解密密钥。使用控制面板和自动报告等工具为用户提供数据信息，而不是让他们直接访问数据。

自动识别和分类：自动识别和分类数据可帮助您实施正确的控制措施。在这方面实现自动化而不是允许人员直接访问，可以降低人为犯错和漏洞的风险。您应使用 AWS Macie 等工具执行评估，Amazon Macie 使用机器学习来自动发现和保护 AWS 中的敏感数据并对其分类。Amazon Macie 可以识别个人可识别信息 (PII) 或知识产权之类的敏感数据，并为您提供控制面板和警报，让您了解此类数据的访问或移动方式。

资源

请参阅以下资源，以详细了解数据分类。

文档

- 数据分类白皮书
- 标记 Amazon EC2 资源
- Amazon S3 对象标记

保护静态数据

静态数据代表您在工作负载期间的任意时间段内保留在非易失性存储器中的任何数据。其中包括数据块存储、对象存储、数据库、存档、IoT 设备和用来保留数据的任何其他存储介质。在实施了加密和适当的访问控制时，保护静态数据可以降低未经授权访问的风险。

加密和令牌化是两个重要但不同的数据保护方案。

*令牌化*是一个支持您定义令牌以表示其他敏感信息的过程（例如代表客户信用卡号的令牌）。令牌自身必须没有任何意义，而且不能是从它令牌化的数据衍生而来 – 因此，无法将加密摘要用作令牌。通过认真规划令牌化方法，您可以为内容提供额外保护，并确保满足合规性要求。例如，如果您使用令牌而不是信用卡号，就可以缩小信用卡处理系统的合规性范围。

*加密*可以将内容转换为这样一种形式：如果用户没有将这些内容解密为纯文本所需的密钥，就无法读取。令牌化和加密都可用于酌情保护信息。此外，可以使用掩码这种技术编辑数据的某个部分，以使剩余的数据不被视为敏感数据。例如，PCI-DSS 允许在合规性范围边界之外保留卡号的最后四位数字，以供索引使用。

实施安全密钥管理：通过定义加密方法，包括密钥存储、轮换和访问控制，有助于您防止内容被未经授权的用户访问或不必要地暴露给经过授权的用户。AWS KMS 可以帮助您管理加密密钥，并可与许多 AWS 服务集成。该服务可以为主密钥提供持久、安全和冗余的存储。您可以定义密钥别名以及密钥级策略。这些策略可以帮助您定义关键管理员以及关键用户。此外，AWS CloudHSM 是一个基于云的硬件安全模块 (HSM)，使您可以在 AWS 云上轻松生成和使用自己的加密密钥。它使用经 FIPS 140-2 第 3 级验证的 HSM，帮助您满足企业、合同和监管合规性要求，以确保数据安全。

实施静态加密：您应确保只以加密的方式存储数据。AWS KMS 与很多 AWS 服务无缝集成，使您能够更轻松地加密您的所有静态数据。例如，在 Amazon S3 中，您可以对存储桶设置默认加密，以自动加密所有的新对象。此外，Amazon EC2 还支持通过为整个区域设置默认加密选项来实施加密。

实施访问控制：各种控制措施，包括访问权限（使用最小特权）、备份（请参阅“可靠性”白皮书）、分离和版本控制，都可以帮助保护您的静态数据。您应使用本白皮书中前面介绍的检测性机制（包括 CloudTrail）和服务级别日志（例如 S3 访问日志），审计对您的数据进行的访问。您应清点可公开访问的数据，并计划如何随着时间的推移减少可用的数据量。Amazon S3 Glacier 文件库锁定和 S3 对象锁定这两项功能可提供强制访问控制——利用合规性选项锁定文件库策略之后，在锁定过期之前，即使根用户也无法对其进行更改。此机制符合 SEC、CFTC 和 FINRA 的图书和记录管理要求。有关更多详细信息，请参阅本白皮书。

审计加密密钥的使用：确保您了解并审计加密密钥的使用，以确保对密钥正确实施访问控制措施。例如，使用 AWS KMS 密钥的任何 AWS 服务都会在 AWS CloudTrail 中记录每次密钥使用。

随后，您可以使用 Amazon CloudWatch Insights 等工具查询 AWS CloudTrail，以确保您的密钥的所有使用都有效。

利用机制禁止人们访问数据：禁止所有用户直接访问正常运行环境中的敏感数据和系统。例如，利用变更管理工作流程，借助工具管理 EC2 实例，而不是允许直接访问或通过堡垒主机进行访问。这可以使用 AWS Systems Manager Automation 来实现，此功能将使用包含您的任务执行步骤的自动化文档。这些文档可以存储在源代码控制中、在运行之前接受对等审核，并接受全面测试以便最大程度降低风险（与 shell 访问相比）。企业用户可以使用一个仪表板而不是通过直接访问数据存储库来执行查询。当未使用 CI/CD 管道时，确定需要利用哪些控制措施和流程来充分提供通常禁用的 Break Glass 访问机制。

自动化静态数据保护：利用自动化工具持续验证和实施静态数据控制，例如确保只存在经过加密的存储资源。您可以使用 AWS Config 规则自动确认所有 EBS 卷都已经过加密。AWS Security Hub 还可以按照安全标准执行自动化检查，以验证多种不同的控制措施。此外，您的 AWS Config 规则可以自动修复不合规的资源。

资源

请参阅以下资源，以详细了解有关保护静态数据的 AWS 最佳实践。

视频

- AWS 中的加密原理
- 在 AWS 上保护您的数据块存储
- 使用 AWS CloudHSM 实现安全目标
- 使用 AWS Key Management Service 的最佳实践
- 深入了解 AWS 加密服务

文档

- 利用加密保护 Amazon S3 数据
- Amazon EBS 加密
- 加密 Amazon RDS 资源

- 利用加密保护数据
- AWS 服务如何使用 AWS KMS
- Amazon EBS 加密
- AWS Key Management Service
- AWS CloudHSM
- AWS KMS 加密详情白皮书
- 使用 AWS KMS 中的密钥策略
- 使用存储桶策略和用户策略
- AWS 加密工具

保护传输中的数据

传输中的数据是指从一个系统发送到另一个系统的任何数据。这包括您工作负载中的资源之间的通信以及其他服务与您的最终用户之间的通信。通过为传输中数据提供适当级别的保护，您就可以保护工作负载数据的机密性和完整性。

实施安全密钥和证书管理：安全地存储加密密钥和证书，并按照适当的时间间隔和使用严格的访问控制措施来轮换这些密钥和证书。实现这一目的的最佳方法是使用托管服务，例如 AWS Certificate Manager (ACM)。它能够让您轻松预置、管理和部署公有和私有传输层安全性 (TLS) 证书，以便与 AWS 服务和您的内部互联资源配合使用。TLS 证书用于保障网络通信的安全性、确立网站在互联网上的身份和资源在私有网络上的身份。ACM 与 Elastic Load Balancer、Amazon CloudFront 分配以及 API Gateway 上的 API 等 AWS 资源集成，还负责处理自动证书续订事宜。如果您使用 ACM 来部署私有根 CA 证书，则它可以提供要在 EC2 实例、容器等对象中使用的证书和私有密钥。

实施传输中加密：实施您根据适当的标准和建议定义的加密要求，以帮助您满足组织、法律和合规性要求。AWS 服务提供使用 TLS 的 HTTPS 终端节点进行通信，从而可以在与 AWS API 通信时提供传输中加密。可以使用安全组在 VPC 中审计和拦截不安全的协议，例如 HTTP。也可以在 Amazon CloudFront 中或 Application Load Balancer 上，将 HTTP 请求自动重定向到 HTTPS。

您可以完全控制计算资源，以便在整个服务中实施加密。您也可以利用 VPN 连接从外部网络连接到您的 VPC 中，以便于对流量进行加密。如果您有特殊要求，可以使用 AWS Marketplace 中提供的第三方解决方案。

验证网络通信：使用支持身份验证的网络协议，可以在双方之间建立信任。此功能将增强协议中使用的加密方法，以降低通信被篡改或拦截的风险。实施身份验证时常用的协议包括（很多 AWS 服务中使用的）传输层安全性 (TLS) 和（AWS 虚拟私有网络 (AWS VPN) 中使用的）IPsec。

自动检测意外数据访问：使用 Amazon GuardDuty 等工具，自动根据数据分类级别检测尝试将数据移到所定义的边界以外的行为，例如检测利用 DNS 协议将数据复制到未知或不可信的网络中的特洛伊木马程序。除了 Amazon GuardDuty 以外，还可以将负责捕获网络流量信息的 Amazon VPC 流日志与 Amazon EventBridge 配合使用，以检测已成功和被拒绝的异常连接。S3 Access Analyzer 可以帮助评估您的 S3 存储桶中的哪些数据可供哪些人访问。

资源

请参阅以下资源，以详细了解有关保护传输中的数据的 AWS 最佳实践。

视频

- 如何使用 AWS Certificate Manager 将网站的证书添加到 ELB?
- 深入了解 AWS Certificate Manager 私有 CA 证书

文档

- AWS Certificate Manager
- 适用于 Application Load Balancer 的 HTTPS 侦听器
- AWS VPN
- API Gateway 边缘优化

事件响应

即使采用极为成熟的预防和检测性控制措施，您的组织仍应实施机制来响应安全事件并缓解安全事件可能带来的影响。您的准备工作会极大地影响团队在事件发生期间采取有效行动、隔离和抑制问题并将运行状态恢复到已知良好状态的能力。在安全事件发生之前确保相关工具和访问权限部署到位，然后通过实际试用定期进行事件响应演练，这样有助于确保您有能力恢复并最大限度避免业务中断。

云响应的设计目标

尽管事件响应的一般流程和机制（例如《NIST SP 800-61 计算机安全事件处理指南》中定义的那些流程和机制）依然有效，但我们鼓励您评估这些与云环境中的安全事件响应相关的特定设计目标：

- **制定响应目标**：与您的利益相关方、法律顾问和组织领导合作，以确定事件响应目标。一些常见目标包括抑制和缓解问题、恢复受影响的资源、保留数据以供取证和确定归属。
- **制定计划**：制定计划，以帮助您响应事件、在事件期间进行沟通以及从事件中恢复。
- **利用云进行响应**：在发生事件和遇到数据时，实施您的响应模式。
- **了解您拥有和需要的证据**：将日志、快照和其他证据复制到中央安全云账户中，以保留这些证据。使用标签、元数据和保留策略实施机制。例如，您可以出于调查目的，选择使用 Linux dd 命令或相应的 Windows 命令为这些数据制作一个完整的副本。
- **使用部署机制**：如果安全异常可归因于一个配置错误，那么可能只需使用适当的配置重新部署资源以删除差异即可完成修复。如果可能，请确保您的响应机制能够安全地在处于未知状态的环境中多次发挥作用。
- **尽可能自动化**：当您发现问题或事件反复发生时，构建一些能够以编程方式确定并响应常见情况的机制。对于特殊事件、新事件和敏感事件，进行人为响应。
- **选择可扩展的解决方案**：尽量让您的组织采用的方法的可扩展性与云计算能力相匹配，并缩短检测与响应之间的时间差。
- **了解并改进您的流程**：当您发现您的流程、工具或员工的差距时，实施计划以弥补这些差距。模拟是找到差距和改进流程的安全方法。

在 AWS 中，实施事件响应时可以使用很多不同的方法。以下部分介绍了如何使用这些方法：

- **培训**您的安全运营和事件响应员工，以使他们了解云技术以及您的组织如何使用这些技术。
- **让**您的事件响应团队做好准备，以便在云中检测和响应事件、启用检测性功能并确保对必要的工具和云服务拥有适当的访问权限。此外，还应通过人工和自动化的方式准备必要的运行手册，以确保可靠且一致的响应。与其他团队合作，以确立预期的基准操作，并利用这些知识来发现与那些正常操作的偏差。
- **模拟**您云环境内的预期和意外安全事件，以了解您的准备工作的有效性。
- **迭代**您的模拟结果，以提高您的响应能力、缩短价值实现时间并进一步降低风险。

培训

使用自动化流程，组织将有更多的时间专注于能够提高工作负载安全性的措施。自动化事件响应还能够让人员关联事件、练习模拟、设计新的响应程序、执行研究、开发新技能以及测试或构建新的工具。即便提高了自动化程度，您的团队、专家以及安全组织内的响应者依然需要持续接受培训。

在获得一般性云体验之后，您需要大量投资于您的人员才能取得成功。通过提供额外的培训，以使您的员工学习编程技能、开发流程（包括版本控制系统和部署实践）和基础设施自动化，您的组织将会受益良多。最好的学习方法是通过举办事件响应实际试用来练习动手实践。这样，您团队中的专家即可在教导他人时完善各种工具和技术。

准备

在事件期间，您的事件响应团队必须能够访问事件所涉及的各种工具和工作负载资源。确保您的团队拥有适当的预置访问权限，以便能够在事件发生之前履行他们的职责。在事件发生之前，应记录并测试所有工具、访问权限和计划，以确保它们可提供及时的响应。

确定关键人员和外部资源：当您与其他团队（例如法律顾问、领导、业务利益相关方、AWS Support 服务等等）一起在云中定义您的事件响应方法时，您必须确定关键人员、利益相关

方和相关联系人。为了降低依赖性并缩短响应时间，请确保为您的团队、专家安全团队和响应者开展培训，以使他们了解您使用的服务并有机会练习动手实践。

我们鼓励您寻找外部 AWS 安全合作伙伴，他们应当能够为您带来外部专业知识和不同的视角，以增强您的响应能力。您的可靠安全合作伙伴可以帮助您发现您可能并不熟悉的潜在风险或威胁。

制定事件管理计划：制定计划，以帮助您响应事件、在事件期间进行沟通以及从事件中恢复。例如，您可以制定事件响应计划，从您的工作负载和组织最可能遇到的情况开始。在计划中说明如何在内部和外部进行沟通和上报。以行动手册的形式制定事件响应计划，从您的工作负载和组织最可能遇到的情况开始。这些事件可能是当前发生的事件。如果需要一个起点，您应考虑 AWS Trusted Advisor 和 Amazon GuardDuty 调查结果。 使用简单的格式，例如减价，以便在实现易维护性的同时确保包含重要的命令或代码片段，因此不必查找其他文档即可执行这些命令或代码片段。

从简单的事做起，然后进行迭代。与您的安全专家和合作伙伴密切合作，以确定可确保实施这些流程的必要任务。定义您执行的这些流程的手册说明。随后，测试这些流程并在运行手册模式中进行迭代，以改进您的响应的核心逻辑。确定异常以及这些场景的备用解决方案。例如，在开发环境中，您可能希望终止错误配置的 Amazon EC2 实例。但如果相同的事件发生在生产环境中，您不应终止实例，而应停止实例并向利益相关方核实关键数据不会丢失，而且终止是可接受的做法。在计划中说明如何在内部和外部进行沟通和上报。当您能够放心地人为响应流程时，请自动化此操作，以缩短解决问题的时间。

预置访问权限：确保事件响应者将正确的访问权限预置到 AWS 和其他相关系统中，以缩短调查到恢复的时间。在事件发生期间才确定如何为相关人员授予访问权限会延迟响应所需的时间，而且，如果是在压力下共享访问权限或未正确预置访问权限，还可能会引入其他安全漏洞。您必须了解您的团队成员所需的访问级别（例如他们可能采取哪些类型的操作），还必须提前预置访问权限。为了响应安全事件而以角色或用户的形式专门创建的访问权限通常是特权，目的是提供足够的访问权限。因此，应限制使用这些用户账户，而且不应使用这些账户来执行日常活动和将会触发警报的用途。

预部署工具：确保安全人员将适当的工具预先部署到 AWS 中，以缩短调查到恢复的时间。

要自动化安全工程和运营功能，您可以使用 AWS 提供的一整套 API 和工具。您可以完全自动执行身份管理、网络安全、数据保护和监控功能，并使用您已采用的常见软件开发方法交付这些功

能。当构建安全自动化时，您的系统可以监控、审核和启动响应，您不必安排人员监控您的安全位置并对事件做出人为响应。

如果您的事件响应团队继续以同样的方式响应警报，警报可能会让他们应接不暇。随着时间的推移，团队对警报的敏感性可能会下降，并可能在处理正常情况时犯错或者错过异常警报。利用一些功能自动处理重复和正常的警报，并将敏感、特殊的事件交由人员来处理，这样有助于避免疲于应对警报。

您可以通过编程方式自动执行此流程中的步骤，从而改进手动流程。为事件定义修复模式之后，您可以将此模式分解为可执行的逻辑，并编写代码以执行此逻辑。随后，响应者即可执行此代码以修复问题。随着时间的推移，您可以自动化越来越多的步骤，并最终自动处理各类常见事件。

对于在您的 EC2 实例的操作系统内运行的工具，您应使用 AWS Systems Manager Run Command 执行评估，它可以使用您安装在 Amazon EC2 实例操作系统中的代理，安全地远程管理实例。它需要使用 AWS Systems Manager 代理（SSM 代理），很多 Amazon 系统映像 (AMI) 中都默认安装了此代理。但请注意，一旦某个实例受损，此实例上运行的工具或代理所做出的任何响应都应被视为不可信赖的响应。

准备取证能力：确定并准备适当的取证调查能力，包括外部专家、工具和自动化。您的一些事件响应活动可能需要分析磁盘映像、文件系统、RAM 转储或者事件中涉及的其他构件。构建一个自定义的取证工作站，以使它们能够安装任何受影响的数据卷的副本。由于取证调查技术需要专家培训，因此您可能需要聘请外部专家。

模拟

开展实际试用：实际试用（也称为模拟或练习）是一些内部事件，可提供结构化机会，使您能够在逼真的场景中练习您的事件管理计划和流程。实际试用主要涉及做好准备，并以迭代方式提高您的响应能力。有些原因能够让您发现开展实际试用活动的价值，这些原因包括：

- 验证准备情况
- 建立信心 – 从模拟中学习以及开展员工培训
- 履行合规或合同义务
- 生成资格鉴定构件

- 敏捷 – 增量改进
- 速度更快并且不断改进的工具
- 优化沟通和上报
- 适应罕见和意外的情况

由于这些原因，通过参与 SIRS 活动而获得的价值能够让组织有效地应对压力重重的事件。开展既逼真又有益的 SIRS 活动可能是一项非常困难的练习。尽管对可处理常见事件的流程或自动化进行测试能够实现一些优势，但只有参与创造性的 SIRS 活动以测试您应对意外情况的能力并持续改进时，这些测试才能体现价值。

迭代

自动抑制和恢复能力：自动抑制事件并从事件中恢复，以缩短响应时间和减小对组织的影响。

当您从行动手册中创建并练习流程和工具之后，您可以将此逻辑解构到基于代码的解决方案中，很多响应者可以将此逻辑用作工具来自动进行响应，因此消除了响应者的分歧或猜测。这样可以加快响应的生命周期。下一个目标是允许此代码被警报或事件自身而不是被人类响应者调用以实现完全自动化，从而创建由事件驱动的响应。

使用由事件驱动的响应系统，检测性机制会触发一个响应机制，以自动修复事件。您可以使用由事件驱动的响应能力，以缩短检测机制与响应机制之间的价值实现时间。要创建这个由事件驱动的架构，您可以使用 AWS Lambda，这是一项无服务器计算服务，可运行您的代码以响应事件并为您自动管理底层计算资源。例如，假设您有一个 AWS 账户并为其启用了 AWS CloudTrail 服务。如果（通过 cloudtrail:StopLogging API 调用）禁用了 AWS CloudTrail，则您可以使用 Amazon EventBridge 监控特定的 cloudtrail:StopLogging 事件，并通过调用 AWS Lambda 函数来调用 cloudtrail:StartLogging，以重新启动日志记录功能。

资源

请参阅以下资源，以详细了解有关事件响应的最新 AWS 最佳实践。

视频

- 准备和响应 AWS 环境中的安全事件

- 自动化事件响应和取证
- 运行手册、事件报告和事件响应 DIY 指南

文档

- AWS 事件响应指南
- AWS Step Functions
- Amazon EventBridge
- CloudEndure 灾难恢复

动手实践

- 实验室：使用 AWS 控制台和 CLI 的事件响应
- 实验室：使用 Jupyter 的事件响应行动手册 – AWS IAM
- 博客：使用 AWS Step Functions 编排安全事件响应

结论

安全性是一项持续性的工作。事件发生时，应将其视为提高架构安全性的机会。拥有强大的身份控制、自动响应安全事件、在多个级别保护基础设施以及通过加密管理合理分类的数据，可以提供每个组织都应实施的深度防御。借助本白皮书中讨论的编程函数以及 AWS 功能和服务，您可以更加轻松地执行这项工作。

AWS 致力于帮助您构建和运营既能保护信息、系统和资产，又能提供业务价值的架构。

贡献者

以下是对本文档做出贡献的个人和组织：

- 架构完善的 Amazon Web Services 首席安全主管 Ben Potter
- Amazon Web Services 首席信息安全官办公室主任 Bill Shinn

- AWS Identity、Amazon Web Services 高级软件开发经理 Brigid Johnson
- Amazon Web Services 高级解决方案架构师 Byron Pogson
- Amazon Web Services 金融服务首席安全解决方案架构师 Darran Boyd
- Amazon Web Services 安全性和合规性首席专家解决方案架构师 Dave Walker
- Amazon Web Services 高级安全战略专家 Paul Hawkins
- Amazon Web Services 高级技术领导 Sam Elmalak

延伸阅读

如需更多帮助，请查阅以下资源：

- AWS 架构完善的框架白皮书

文档修订

日期	说明
2020 年 7 月	更新了有关账户、身份和权限管理的指导。
2020 年 4 月	更新以扩展每个方面的建议、新的最佳实践、服务和功能。
2018 年 7 月	更新以反映新的 AWS 服务和功能以及最新参考。
2017 年 5 月	更新了“系统安全配置和维护”一节，以反映新的 AWS 服务和功能。
2016 年 11 月	首次发布