AWS 安全最佳实践

2016 年 8 月

（请访问 **http://aws.amazon.com/security**
以查看此白皮书的最新版本）

版权声明

目录

摘要

本白皮书面向为在 Amazon Web Services (AWS) 中运行的应用程序设计安全基础设施和配置的现有客户和潜在客户。它所提供的安全最佳实践有助于您定义信息安全管理系统 (ISMS) 并为您的组织构建一组安全策略和流程，以便对 AWS 云中的数据和资产提供保护。本白皮书还概述不同安全主题，例如：对您在 AWS 上的资产进行标识、分类和保护，使用账户、用户和组来管理对 AWS 资源的访问，并针对您在云中对您的数据、操作系统和应用程序以及整体基础设施提供保护的方式提出建议。

本白皮书面向 IT 决策者和安全人员，并假定您熟悉网络、操作系统、数据加密和运行控制等方面的基本安全概念。

概述

对 Amazon Web Services (AWS) 客户而言，最重要的是信息安全。安全是一项核心功能要求，旨在防止关键任务信息被意外或故意窃取、泄露、完整性受损以及遭到删除。

在 AWS *责任共担模型* 下，AWS 提供全球安全基础设施和基础计算、存储、联网及数据库服务，以及更高级的服务。AWS 提供各种安全服务和功能供 AWS 客户用来保护其资产。AWS 客户负责保护其数据在云中的机密性、完整性和可用性，以及满足业务对于信息保护的特定要求。有关 AWS 安全功能的更多信息，请参阅安全过程概述白皮书。

本白皮书介绍您可用来构建和定义信息安全管理系统 (ISMS) 的最佳实践，信息安全管理系统 (ISMS) 是适用于贵组织的 AWS 资产的信息安全政策和流程的集合。有关 ISMS 的更多信息，请参阅 ISO 27001：http://www.27000.org/iso-27001.htm。尽管无需构建 ISMS 即可使用 AWS，但我们认为，基于广泛采用的全球安全方法基本构建块而构建的结构化信息安全管理方法将帮助您改进贵组织的整体安全态势。

我们讨论以下主题：

- AWS 和作为客户的您如何共同分担安全责任。
- 如何定义和分类您的资产
- 如何使用特权账户和组管理用户对您的数据的访问
- 保护您的数据、操作系统和网络的最佳实践
- 监控和警报如何帮助您实现安全目标

本白皮书在更高层面讨论这些领域的安全最佳实践。（它不提供“操作方法”配置指导。有关配置指导，请参阅 AWS 文档：
http://aws.amazon.com/documentation。）

了解 AWS 责任共担模型

Amazon Web Services 在云中提供安全的全球基础设施和服务。您可以将 AWS 作为基础构建您的系统，利用 AWS 功能构建 ISMS。

要在 AWS 中设计 ISMS，您必须首先熟悉 AWS 责任共担模型，这个模型要求 AWS 和客户合作共同实现安全目标。

AWS 提供安全的基础设施和服务，而作为客户的您负责保护操作系统、平台和数据。为确保全球基础设施的安全，AWS 需配置基础设施组件，提供服务和功能来增强安全性（例如 Identity and Access Management (IAM) 服务，您可以使用该服务管理 AWS 服务子集中的用户和用户权限）。为确保服务的安全，AWS 为我们提供的每种不同类型服务提供责任共担模型：

- 基础设施服务
- 容器服务
- 抽象服务

Amazon Elastic Compute Cloud (Amazon EC2) 等基础设施服务的责任共担模型规定，AWS 管理以下资产的安全：

- 设施
- 硬件的物理安全

- 网络基础设施
- 虚拟化基础设施

为了定义您的 ISMS 资产，考虑将 AWS 作为这些资产的所有者。利用这些 AWS 控制机制，将它们包含在您的 ISMS 中。

在此 Amazon EC2 示例中，作为客户，您负责以下资产的安全：

- Amazon 系统映像 (AMI)
- 操作系统
- 应用程序
- 传输中的数据
- 静态数据
- 数据存储
- 凭证
- 策略和配置

特定服务进一步界定您与 AWS 之间如何分担责任。有关更多信息，请参阅 http://aws.amazon.com/compliance/#third-party。

了解 AWS 安全全球基础设施

AWS 安全全球基础设施和服务由 AWS 管理，它们为企业级系统和各个单独的应用程序提供值得信赖的基础。AWS 为云信息安全制定了高标准，有一整套全面控制目标，范围从物理安全到软件采购，从开发到员工生命周期管理以及安全组织。AWS 安全全球基础设施和服务需要定期经受第三方合规性审计。有关更多信息，请参阅 Amazon Web Services 风险与合规性白皮书。（请参阅“参考文献与*延伸阅读*”。）

使用 IAM 服务

IAM 服务是本文讨论的 AWS 安全全球基础设施的一个组成部分。借助 IAM，您可以集中管理用户、安全凭证（如密码、访问密钥），以及对用户可以访问哪些 AWS 服务和资源进行控制的权限策略。

注册 AWS 时，您提供用户名（您的电子邮件地址）和密码创建一个 AWS 账户。通过用户名和密码，您可以登录 AWS 管理控制台，在这里您可以使用基于浏览器的界面来管理 AWS 资源。您还可以创建访问密钥（由访问密钥 ID 和私有访问密钥组成），当您使用命令行界面 (CLI)、AWS SDK 或 API 调用以编程方式调用 AWS 时需要用到它们。

通过 IAM，您可以在自己的 AWS 账户中创建各个用户，并为每个用户提供其自己的用户名、密码和访问密钥。这样，各个用户可使用特定于您账户的 URL 登录控制台。您还可以为各个用户创建访问密钥，使他们可以进行编程调用以访问 AWS 资源。IAM 用户执行的活动产生的所有费用均计入您的 AWS 账户。作为最佳实践，我们建议您为自己创建一个 IAM 用户，不要使用您的 AWS 账户凭证进行日常 AWS 访问。有关更多信息，请参阅 IAM 最佳实践。

区域、可用区和终端节点

您还应熟悉区域、可用区和终端节点，这些是 AWS 安全全球基础设施的组成部分。

使用 AWS 区域管理网络延迟和监管合规性。当您将数据保存在特定区域时，这些数据不会复制到该区域之外。如果您的业务需要跨区域复制数据，则由您负责执行此操作。AWS 提供有关每个区域所在的国家/地区和州/省（如果适用）的信息；您负责根据自己的合规性和网络延迟要求选择将存储数据的区域。

区域在设计时考虑到了可用性，由至少两个（通常更多）可用区组成。可用区旨在实现故障隔离。它们与多个 Internet 服务提供商 (ISP) 和不同电网相连。它们是使用高速链路互连的，因此应用程序可依赖局域网 (LAN) 连接在相同区域内实现可用区之间的通信。您需要认真选择自己的系统将驻留的可用区。系统可跨多个可用区，我们建议您将系统设计为在发生灾难时能够应对暂时或更长时间的可用区故障。

AWS 在 AWS 管理控制台中通过每项服务分别对应的控制台提供对相关服务的 Web 访问。AWS 通过应用程序编程接口 (API) 和命令行界面 (CLI) 提供对服务的编程访问。由 AWS 托管的服务终端节点提供管理（“背板”）访问。

分担 AWS 服务安全责任

AWS 提供多种不同的基础设施和平台服务。为了理解这些 AWS 服务的安全性和共担责任，我们将它们分为三个主要类别：基础设施、容器和抽象服务。根据您对功能的交互和访问方式，每个类别都有略微不同的安全责任模型

- **基础设施服务：**此类别包括计算服务（如 Amazon EC2）和相关服务（如 Amazon Elastic Block Store (Amazon EBS)、Auto Scaling 和 Amazon Virtual Private Cloud (Amazon VPC)）。通过这些服务，您可以使用与本地解决方案类似和大体兼容的技术设计和构建云基础设施。您控制操作系统，并配置和操作可访问虚拟化堆栈用户层的任何身份管理系统。
- **容器服务：**此类别的服务通常在单独的 Amazon EC2 或其他基础设施实例上运行，但有时您不管理操作系统或平台层。AWS 为这些应用程序“容器”提供托管服务。您负责设置和管理网络控制（如防火墙规则），负责从 IAM 单独管理平台级身份和访问管理。容器服务的示例包括 Amazon Relational Database Services (Amazon RDS)、Amazon Elastic Map Reduce (Amazon EMR) 和 AWS Elastic Beanstalk
- **抽象服务：**此类别包括高级存储、数据库和消息服务，如 Amazon Simple Storage Service (Amazon S3)、Amazon Glacier、Amazon DynamoDB、Amazon Simple Queuing Service (Amazon SQS) 和 Amazon Simple Email Service (Amazon SES)。这些服务抽象出平台或管理层，供您作为基础来构建和运行云应用程序。您使用 AWS API 访问这些抽象服务的终端节点，AWS 管理基础服务组件或它们所驻留的操作系统。您共享底层基础设施，抽象服务提供多租户平台，该平台以安全方式隔离您的数据，并提供与 IAM 之间的强有力集成。

我们更深入地讨论一下每个服务类型的责任共担模型。

基础设施服务的责任共担模型

Amazon EC2、Amazon EBS 和 Amazon VPC 等基础设施服务在 AWS 全球基础设施之上运行。它们在可用性和持久性目标方面各不相同，但始终在已启用了它们的特定区域中运行。通过在多个可用区中采用弹性组件，您构建的系统所实现的可用性目标可以超越 AWS 中各项单独服务的可用性目标。

图 1 介绍基础设施服务的责任共担模型的构建块。

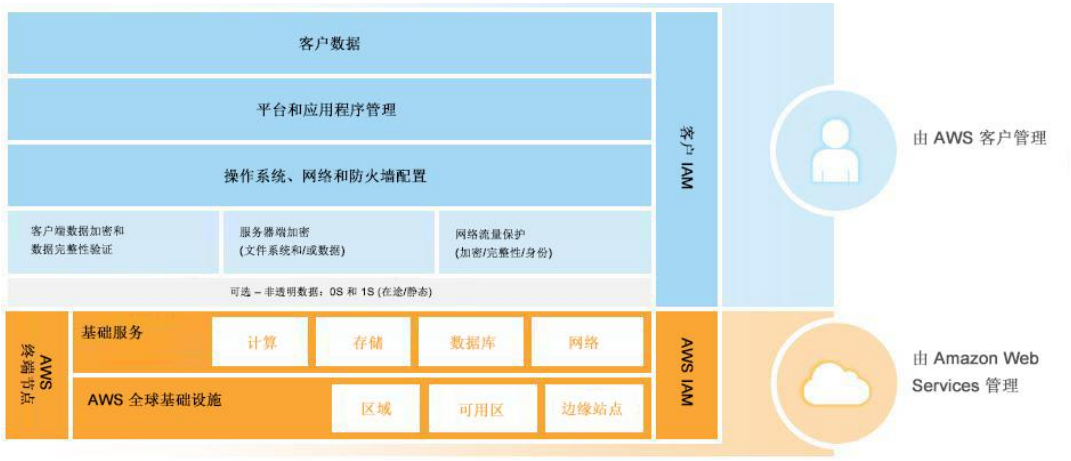

图 1：基础设施服务的责任共担模型

基于 AWS 安全全球基础设施构建，您在 AWS 云中安装和配置您的操作系统和平台，就像在自己的数据中心本地执行一样。然后，您在您的平台上安装应用程序。最后，您的数据驻留在您自己的应用程序中并由这些应用程序管理。除非您有更苛刻的业务或合规性要求，否则除 AWS 安全全球基础设施提供的保护层外，您无需引入额外的保护层。

对于某些合规性要求，您可能需要在 AWS 服务与您的操作系统及平台（存放应用程序和数据的地方）之间增加额外保护层。您可以施加额外控制（如静态数据保护和对传输中数据的保护），或者在 AWS 的服务与您的平台之间引入不透明层。不透明层可包括数据加密、数据完整性验证、软件与数据签名、安全时间戳等。

AWS 为您提供可用来保护静态和传输中数据的技术。有关更多信息，请参阅本白皮书中的“管理 Amazon EC2 实例的操作系统级访问”和“保护您的数据”部分。或者，您可以引入自己的数据保护工具，或利用 AWS 合作伙伴的产品。

上一节介绍了您可以通过哪些方式管理需要对 AWS 服务进行身份验证的资源的访问。不过，为了访问您 EC2 实例上的操作系统，您需要不同的凭证集。在责任共担模型中，您拥有操作系统凭证，但 AWS 帮助您引导对操作系统的初始访问。

当您从标准 AMI 启动新的 Amazon EC2 实例时，您可以使用安全的远程系统访问协议访问该实例，如安全外壳 (SSH) 或 Windows 远程桌面协议 (RDP)。您必须在操作系统级别成功进行身份验证，然后才能访问和配置 Amazon EC2 实例来满足的要求。在您进行身份验证并远程进入 Amazon EC2 实例后，您可以设置所需要的操作系统身份验证机制，其中可能包括 X.509 证书身份验证、Microsoft Active Directory 或本地操作系统账户。

为启用对 EC2 实例的身份验证，AWS 提供非对称密钥对，称为 Amazon EC2 密钥对。这些是业界标准 RSA 密钥对。每个用户可有多个 Amazon EC2 密钥对，可使用不同密钥对启动新实例。EC2 密钥对与 AWS 账户或先前讨论的 IAM 用户凭证无关。这些凭证控制对其他 AWS 服务的访问；EC2 密钥对仅控制对您特定实例的访问。

您可以选择使用 OpenSSL 等业界标准工具生成自己的 Amazon EC2 密钥对。您在安全、可信环境中生成密钥对，只有密钥对的公有密钥导入到 AWS 中；您安全地保存私有密钥。如果采用这种方法，建议您使用高质量的随机数字生成器。

您可以选择让 AWS 生成 Amazon EC2 密钥对。在这种情况下，当您首次创建实例时，系统会显示 RSA 密钥对的公有和私有密钥。您必须下载并安全地保存 Amazon EC2 密钥对的私有密钥。AWS 不存储私有密钥；如果丢失，您必须生成新的密钥对。

对于使用 **cloud-init** 服务的 Amazon EC2 Linux 实例，当从标准 AWS AMI 启动新实例时，Amazon EC2 密钥对的公有密钥会附加到初始操作系统用户的 **~/.ssh/authorized_keys** 文件。然后，通过将 SSH 客户端配置成使用正确 Amazon EC2 实例用户的名称作为其身份（例如 ec2-user），并提供用于用户身份验证的私有密钥文件，该用户将能够使用 SSH 客户端连接到 Amazon EC2 Linux 实例。

对于使用 **ec2config** 服务的 Amazon EC2 Windows 实例，当从标准 AWS AMI 启动新实例时，**ec2config** 服务会为该实例设置新的随机管理员密码，并使用相应 Amazon EC2 密钥对的公有密钥对其进行加密。通过使用 AWS 管理控制台或命令行工具，并提供相应的 Amazon EC2 私有密钥对密码进行解密，用户能够获得 Windows 实例密码。此密码连同 Amazon EC2 实例的默认管理账户可用于对 Windows 实例进行身份验证。

AWS 提供了一系列灵活实用的工具，用于管理 Amazon EC2 密钥，以及对新启动的 Amazon EC2 实例提供业界标准的身份验证。如果您具有更高的安全要求，可以实施 LDAP 或 Active Directory 身份验证等替代身份验证机制，并禁用 Amazon EC2 密钥对身份验证。

容器服务的责任共担模型

AWS 责任共担模型也适用于容器服务，例如 Amazon RDS 和 Amazon EMR。对于这些服务，AWS 管理底层基础设施和基础服务、操作系统和应用程序平台。例如，Amazon RDS for Oracle 是一种托管的数据库服务，在该服务中，AWS 管理容器的所有层，最高至 Oracle 数据库平台且包括此平台。对于 Amazon RDS 等服务，AWS 平台提供数据备份和恢复工具；但您负责配置和使用与业务连续性和灾难恢复 (BC/DR) 策略有关的工具。

对于 AWS 容器服务，您负责数据和防火墙规则，防火墙规则控制着对该容器服务的访问权限。例如，Amazon RDS 提供 RDS 安全组，Amazon EMR 可让您通过 Amazon EC2 安全组针对 Amazon EMR 实例管理防火墙规则。

图 2 介绍容器服务的责任共担模型。

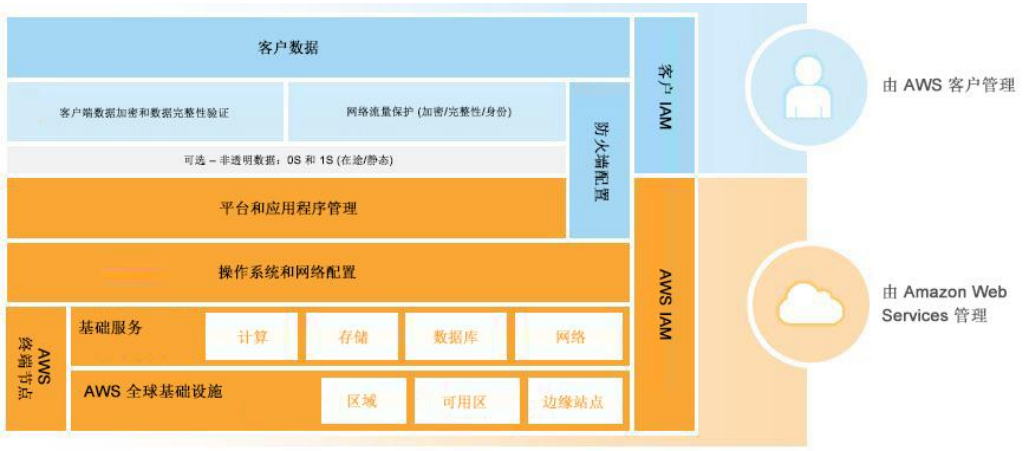

图 2：容器服务的责任共担模型

抽象服务的责任共担模型

对于抽象服务（例如 Amazon S3 和 Amazon DynamoDB），AWS 运行基础设施层、操作系统和平台，而您负责访问终端节点以存储和检索数据。Amazon S3 和 DynamoDB 与 IAM 紧密集成。您负责管理数据，包括对数据资产进行分类，以及使用 IAM 工具在平台级别向各个资源应用 ACL 类型权限，或者在 IAM 用户/组级别根据用户身份或用户责任应用权限。对于某些服务，例如 Amazon S3，您还可以使用平台提供的静态数据加密，或者平台提供的对您有效负载的 HTTPS 封装，以保护传入和传出该服务的数据。

图 3 概括了 AWS 抽象服务的责任共担模型：

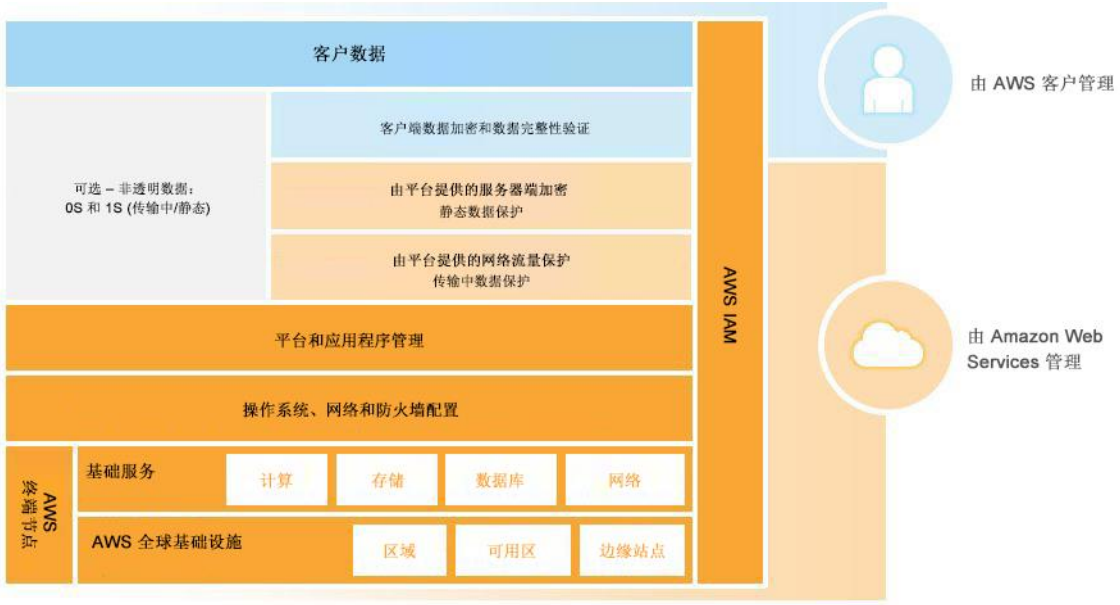

图 3：抽象服务的责任共担模型

使用 Trusted Advisor 工具

有些 AWS Premium Support 计划包括对 Trusted Advisor 工具的使用，该工具针对您的服务提供单一视图快照，并可帮助确定常见安全误配置、系统性能改进建议，以及未充分利用的资源。在本白皮书中，我们将介绍应用于 Amazon EC2 的 Trusted Advisor 安全方面。

Trusted Advisor 检查与以下安全建议的符合情况：

- 对常用管理端口的访问仅限于一小部分地址。这包括端口 22 (SSH)、23 (Telnet) 3389 (RDP) 和 5500 (VNC)。
- 限制对常用数据库端口的访问。这包括端口 1433 (MSSQL Server)、1434 (MSSQL Monitor)、3306 (MySQL)、Oracle (1521) 和 5432 (PostgreSQL)。
- 已配置 IAM 以帮助确保 AWS 资源的安全访问控制。
- 已启用多重身份验证 (MFA) 令牌，以便为 AWS 根账户提供双重身份验证。

定义和分类 AWS 上的资产

设计您的 ISMS 之前，应确定您需要保护的所有信息资产，然后为其设计一个在技术和财务上都可行的保护解决方案。可能难以从财务角度来量化每个资产，因此您可能发现使用定性指标（例如可忽略/低/中/高/极高）是一个更好的选择。

资产分为两大类：

- 基本要素，例如业务信息、流程和活动
- 支持基本要素的组成部分，例如硬件、软件、人员、站点及合作伙伴组织

表 1 显示了一个示例资产矩阵。

资产名称	资产所有者	资产类别	依赖关系	成本
面向客户的网站应用程序	电子商务团队	主要	EC2、Elastic Load Balancing、RDS、开发	部署、替换、维护、成本/损失后果
客户信用卡数据	E-C电子商务团队	主要	PCI 卡持有人环境、加密、AWS PCI 服务	
人员数据	COO	主要	Amazon RDS、加密提供者、开发和运营 IT、第三方	
数据存档	COO	主要	S3、Glacier、开发和运营 IT	
HR 管理系统	人力资源	主要	EC2、S3、RDS、开发和运营 IT、第三方	
AWS Direct Connect 基础设施	CIO	网络	网络运营、电信提供商、AWS Direct Connect	
商业智能基础设施	BI 团队	软件	EMR、Redshift、Dynamo DB、S3、开发和运营	
商业智能服务	COO	主要	BI 基础设施、BI 分析团队	
LDAP 目录	IT 安全团队	安全性	EC2、IAM、自定义软件、开发和运营	
Windows AMI	服务器团队	软件	EC2、补丁管理软件、开发和运营	
客户凭证	合规性团队	安全性	日常更新；存档基础设施	

表 1：示例资产矩阵

设计 ISMS 以保护您在 AWS 上的资产

确定了资产、类别和成本以后，应制定在 AWS 上实施、运行、监控、审核、维护及改进信息安全管理系统 (ISMS) 的标准。根据以下因素，每个组织的安全要求各不相同：

- 业务需求和目标
- 采用的流程
- 组织的规模和结构

所有这些因素均会随时间而改变，因此最好为所有这些信息构建周期性的管理流程。

表 2 给出了在 AWS 中设计和构建 ISMS 所建议采用的分阶段方法。如 ISO 27001 等标准框架对于 ISMS 的设计和实施可能会有所帮助。

阶段	标题	描述
1	**定义范围和边界。**	定义哪些区域、可用区、实例和 AWS 资源“在范围内”。若排除任何组件（例如，若设施由 AWS 管理，则可将其排除在您自己的管理系统之外），应明确说明具体的排除内容及原因。
2	**定义 ISMS 策略。**	包括以下内容： • 旨在为信息安全相关操作设定方向和原则的目标 • 法律、合同和法规要求 • 您的组织的风险管理目标 • 风险评测方式 • 管理层对计划的批准方式

3	**选择风险评估方法。**	根据组织中各小组关于以下因素的意见，选择风险评估方法： • 业务需求 • 信息安全要求 • 信息技术的功能和使用 • 法律要求 • 监管责任 因为公有云基础设施的运行方式与传统环境不同，因此设定接受风险及确定可接受的风险水平（风险容忍）的标准非常关键。 我们建议从风险评估开始，并尽可能充分利用自动化功能。AWS 风险自动化功能可缩小需要进行风险管理的资源范围。 有多种风险评估方法，包括 OCTAVE （运营方面的关键威胁、资产和漏洞评估）、ISO 31000:2009 风险管理、ENISA （欧洲网络信息安全机构）、IRAM（信息风险分析方法）和 NIST （美国国家标准与技术研究院） 特刊 (SP) 800-30 版本 1 风险管理指南。
4	**识别风险**	我们建议您创建一个风险登记单：将所有资产与各自面临的威胁相对应，然后根据漏洞评估和影响分析结果，为每个 AWS 环境创建新的风险矩阵。 以下为风险登记单的示例： • 资产 • 这些资产面临的威胁 • 这些威胁可以利用的漏洞 • 这些漏洞被利用时的后果
5	**分析和评估风险**	通过计算业务影响、可能性与盈利能力、风险等级，分析和评估风险。
6	**应对风险**	选择应对风险的选项。选项包括应用安全控制、接受风险、避免风险或转移风险。
7	**选择安全控制框架**	选择安全控制时，应使用框架，例如 ISO 27002、NIST SP 800-53、COBIT（信息及相关技术的控制目标）及 CSA-CCM （云安全联盟-云控制矩阵）。这些框架由一系列可重用的最佳实践组成，将帮助您选择相关控制措施。
8	**获得管理层批准**	即使实施了所有控制措施，仍会残存风险。我们建议您获得企业管理层的批准，确认所有残存风险，并获准实施和运行 ISMS。
9	**适用性声明**	创建包含以下信息的适用性声明： • 您选择了哪些控制措施及选择的理由 • 哪些控制措施已就位 • 哪些控制措施计划投入使用 • 您排除了哪些控制措施及排除的理由

表 2：ISMS 的构建阶段

管理 AWS 账户、IAM 用户、组和角色

确保用户具有相应级别的权限访问他们所需的资源，但不能超范围赋权，这是每个 ISMS 的重要部分。您可以借助 IAM 执行此功能。您在自己的 AWS 账户下*创建 IAM 用户*，然后直接向其分配权限，或者将其指定到已经分配权限的组。以下是有关 AWS 账户和 IAM 用户的更详细信息：

- **AWS 账户。**这是您在首次注册 AWS 时创建的账户。您的 AWS 账户代表着您与 AWS 之间的业务关系。您将使用自己的 AWS 账户管理所用的 AWS 资源和服务。AWS 账户对所有 AWS 资源和服务都有根权限，因此非常强大。请不要在与 AWS 之间的日常交互中使用根账户凭证。在某些情况下，您的组织可能选择使用多个 AWS 账户：

  为每个重要部门分别使用一个账户，然后在每个 AWS 账户下为相应的人员和资源创建 IAM 用户。

- **IAM 用户。**使用 IAM，您可以创建多个用户，每个用户都有单独的安全凭证，且所有用户都由同一个 AWS 账户控制。IAM 用户可以是需要通过管理控制台、CLI 或直接通过 API 访问您 AWS 资源的人员、服务或应用程序。最佳实践是为需要访问您 AWS 账户中的服务和资源的每个人都创建单独的 IAM 用户。您可以对您 AWS 账户下的资源创建精细的权限，将权限应用到您创建的组，然后将用户分配到这些组。这种最佳实践有助于确保用户拥有完成任务所需的最小特权。

使用多个 AWS 账户的策略

设计您的 AWS 账户策略，以便最大程度提高安全性并遵守您的业务和监管要求。表 3 讨论了各种可能的策略。

业务要求	建议的设计	说明
集中式安全管理	单个 AWS 账户	集中信息安全管理并最大程度降低开销。
生产、开发和测试环境的分离	三个 AWS 账户	创建三个 AWS 账户，分别用于生产服务、开发和测试。
多个自主部门	多个 AWS 账户	为组织的每个自主部门创建单独的 AWS 账户。您可以在每个账户下分配权限和策略。
多个自主独立项目的集中式安全管理	多个 AWS 账户	为通用项目资源（例如 DNS 服务、Active Directory、CMS 等）创建单一 AWS 账户。然后为每个项目创建单独的 AWS 账户。您可以在每个项目账户下分配权限和策略，并授予跨账户访问资源的权限。

表 3：AWS 账户策略

您可以在多个账户间配置整合账单关系，以便简化为每个账户管理不同账单的复杂性，并充分利用规模经济性。使用账单整合时，账户间并不共享资源和凭证。

管理 IAM 用户

具有相应权限级别的 IAM 用户可新建 IAM 用户，或者管理和删除现有用户。这种高特权 IAM 用户可为您组织中管理 AWS 配置或直接访问 AWS 资源的每个人员、服务或应用程序创建不同的 IAM 用户。我们强烈反对使用共享用户身份，也就是多个实体共享同样的凭证。

管理 IAM 组

IAM 组是一个 AWS 账户中的 IAM 用户集合。创建 IAM 组的依据可以是职能、组织或地理位置，也可以是项目，或是 IAM 用户需要访问类似 AWS 资源执行工作的其他任何情况。通过分配一个或多个 IAM 策略，您可以为每个 IAM 组提供访问 AWS 资源的权限。分配给 IAM 组的所有策略均由作为组成员的 IAM 用户继承。

例如，我们假设 IAM 用户 John 负责组织内的备份工作，并且需要访问 Amazon S3 存储桶 `Archives` 中的对象。您可以直接赋予 John 访问 `Archives` 存储桶的权限。但之后您的组织将 Sally 和 Betty 派入 John 所在的团队。尽管您能够单独为 John、Sally 和 Betty 分配用户权限，以使他们能够访问 `Archives` 存储桶，但为组分配这些权限并将 John、Sally 和 Betty 放入该组中将更容易管理和维护。如果其他用户需要相同的访问权限，您可以通过将他们添加到该组中将此权限赋予他们。当用户不再需要访问某资源时，可以将他们从能够访问该资源的组中移除。

IAM 组是一种管理对 AWS 资源的访问的强大工具。即使只有一个用户需要访问特定的资源，作为最佳实践，您也应为该访问确定或新建一个 AWS 组，通过组成员身份配置用户访问，并在组级别分配权限和策略。

管理 AWS 凭证

每个 AWS 账户或 IAM 用户都是唯一的身份，具有唯一的长期凭证。与这些身份相关联的凭证主要有两种类型：(1) 用于登录到 AWS 管理控制台和 AWS 门户页面的凭证，以及 (2) 用于以编程方式访问 AWS API 的凭证。

表 4 介绍两种类型的登录凭证。

登录凭证类型	详细信息
用户名称/密码	AWS 账户的用户名始终为电子邮件地址。IAM 用户名可实现更高灵活性。您的 AWS 账户密码可由您任意指定。可强制使 IAM 用户密码符合您定义的策略（即，您可以规定最短密码长度，或者要求使用非字母数字字符）。
多重身份验证 (MFA)	AWS 多重身份验证 (MFA)为登录凭证提供了额外的安全保护。启用 MFA 后，当用户登录 AWS 网站时，系统将要求他们输入用户名和密码（第一安全要素 — 用户已知），以及来自其 MFA 设备的身份验证代码（第二安全要素 — 用户已有）。您还可要求对想要删除 S3 对象的用户执行 MFA。我们建议您为 AWS 账户和您的 IAM 用户激活 MFA，以防止对您 AWS 环境的未授权访问。AWS 目前以智能手机应用程序的形式支持 Gemalto 硬件 MFA 设备以及虚拟 MFA 设备。

表 4：登录证书

表 5 介绍用于以编程方式访问 API 的凭证类型。

访问凭证类型	详细信息
访问密钥	访问密钥用于对向 AWS 服务发出的 API 调用进行数字签名。每个访问密钥凭证均由访问密钥 ID 和私有密钥组成。AWS 账户持有人或获分私有密钥的 IAM 用户必须妥善保护私有密钥部分。用户在任意时间都可拥有两组活动的访问密钥。作为最佳实践，用户应定期轮换他们的访问密钥。
针对 API 调用的 MFA	由多重身份验证 (MFA) 保护的 API 访问要求 IAM 用户输入有效的 MFA 代码，然后他们才能够使用某些功能，即 API。您在 IAM 中创建的策略将决定哪些 API 需要 MFA。由于 AWS 管理控制台调用 AWS 服务 API，因此您可以对 API 强制实施 MFA （无论通过控制台还是通过 API 访问）。

表 5：编程访问凭证

了解使用 IAM 角色和临时安全凭证的委托

在某些情况下，您需要向原本无权访问您 AWS 资源的用户或服务委托访问权限。下面的表 6 概述了委托此类访问权限的常用案例。

使用案例	描述
在 Amazon EC2 实例上运行的需要访问 AWS 资源的应用程序	运行于 Amazon EC2 实例上并且需要访问 AWS 资源（例如 Amazon S3 存储桶或 Amazon DynamoDB 表）的应用程序必须具有安全凭证才能向 AWS 发出编程请求。开发人员可将他们的凭证分发给每个实例，然后应用程序可使用这些凭证访问资源。然而，将长期凭证分发给每个实例难以管理，并且存在潜在的安全风险。
跨账户访问	要管理对资源的访问，可设置多个 AWS 账户 — 例如，将开发环境与生产环境隔离。但是，一个账户的用户可能需要访问另一个账户中的资源，例如，为了促进从开发环境到生产环境的更新。虽然在两个账户中工作的用户可以在每个账户中拥有单独的身份，但是管理多个账户的凭证为身份管理带来了难题。
联合身份	用户可能已具有 AWS 外部的身份，如在贵公司目录中。但是，这些用户可能需要使用 AWS 资源（或使用访问这些资源的应用程序）。如果是这样，这些用户还需要 AWS 安全凭证，以便向 AWS 发出请求。

表 6：常见委托使用案例

IAM 角色和临时安全凭证可满足这些使用案例的需要。通过 IAM 角色可以定义用户或服务所需的一组资源访问权限，但是该权限不能挂载到特定的 IAM 用户或组。但 IAM 用户、移动和基于 EC2 的应用程序或者 AWS 服务（例如 Amazon EC2）能够以编程方式担任一个角色。担任角色会返回临时安全凭证，供用户或应用程序用于对 AWS 提出编程请求。这些临时安全凭证具有可配置的过期日期，并且自动轮换。使用 IAM 角色和临时安全凭证意味着您不必始终为需要访问资源的每个实体管理长期凭证和 IAM 用户。

适用于 Amazon EC2 的 IAM 角色

适用于 Amazon EC2 的 IAM 角色是适用于表 6 中第一个使用案例的具体 IAM 角色实施。在下图中，开发人员正在 Amazon EC2 实例上运行一个应用程序，该应用程序需要访问名为 `photos` 的 Amazon S3 存储桶。管理员创建了 `Get-pics` 角色。该角色包含的策略将授予对该存储桶的读取权限，并允许开发人员随 Amazon EC2 实例启动该角色。在该实例中运行应用程序时，应用程序可以使用该角色的临时凭证访问 `photos` 存储桶。管理员无需授予开发人员访问 `photos` 存储桶的权限，开发人员也从不需要共享凭证。

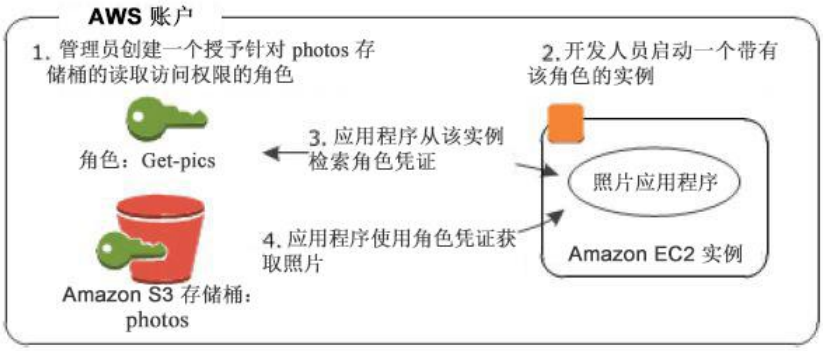

图 4：EC2 角色的工作原理

1. 管理员使用 IAM 创建 `Get-pics` 角色。在该角色中，管理员使用的策略指定只有 Amazon EC2 实例才可以担任该角色，并指定对 `photos` 存储桶的只读权限。
2. 开发人员启动 Amazon EC2 实例，并将 `Get-pics` 角色与该实例关联。
3. 应用程序在运行时将从 Amazon EC2 实例上的实例元数据中检索凭证。
4. 应用程序使用这些角色凭证以只读权限访问 `photo` 存储桶。

跨账户访问

使用 IAM 角色可以通过以下方式满足表 6 中第二个使用案例的需要：允许另一个 AWS 账户中的 IAM 用户访问您 AWS 账户中的资源。这一过程称为跨账户访问。通过跨账户访问，您可与其他 AWS 账户中的用户共同访问您的资源。

要建立跨账户访问，请在信任账户（账户 A）中创建一个 IAM 策略，该策略向可信账户（账户 B）授予对特定资源的访问权限。账户 B 随后可将该访问权限委托给其 IAM 用户。账户 B 向其 IAM 用户委托的访问权限不能超过账户 A 授予它的访问权限。

联合身份

使用 IAM 角色可以通过以下方式满足表 6 中第三个使用案例的需要：在您的公司用户与 AWS 资源之间创建一个身份代理来管理身份验证和授权流程，而无需在 AWS 中将您的所有用户均重新创建为 IAM 用户。

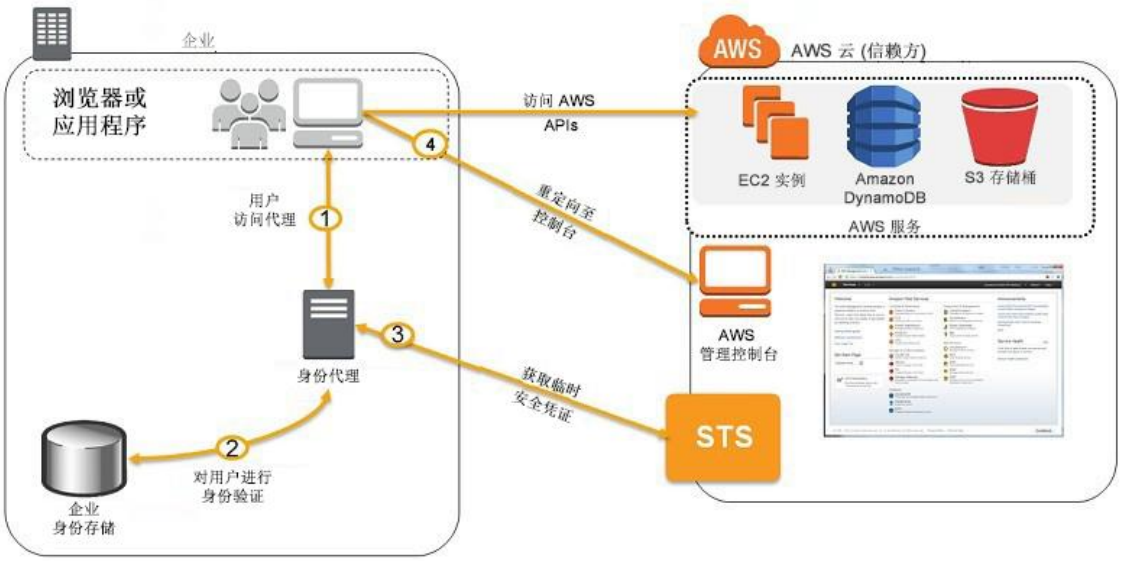

图 5:使用临时安全凭证的 AWS 联合身份

1. 企业用户访问身份代理应用程序。
2. 身份代理应用程序根据公司身份存储对用户进行身份验证。
3. 身份代理应用程序有权访问 AWS Security Token Service (STS) 以请求临时安全凭证。
4. 企业用户可获得一个临时 URL，通过该 URL 访问 AWS API 或管理控制台。AWS 提供了与 Microsoft Active Directory 结合使用的示例身份代理应用程序。

管理对 Amazon EC2 实例的操作系统级访问

上一节介绍了您可以通过哪些方式管理需要对 AWS 服务进行身份验证的资源的访问。不过，为了访问您 EC2 实例上的操作系统，您需要不同的凭证集。在责任共担模型中，您拥有操作系统凭证，但 AWS 帮助您引导对操作系统的初始访问。

当您从标准 AMI 启动新的 Amazon EC2 实例时，您可以使用安全的远程系统访问协议访问该实例，如安全外壳 (SSH) 或 Windows 远程桌面协议 (RDP)。您必须在操作系统级别成功进行身份验证，然后才能访问和配置 Amazon EC2 实例来满足的要求。在您进行身份验证并远程进入 Amazon EC2 实例后，您可以设置所需要的操作系统身份验证机制，其中可能包括 X.509 证书身份验证、Microsoft Active Directory 或本地操作系统账户。

为启用对 EC2 实例的身份验证，AWS 提供非对称密钥对，称为 Amazon EC2 密钥对。这些是业界标准 RSA 密钥对。每个用户可有多个 Amazon EC2 密钥对，可使用不同密钥对启动新实例。EC2 密钥对与 AWS 账户或先前讨论的 IAM 用户凭证无关。这些凭证控制对其他 AWS 服务的访问；EC2 密钥对仅控制对您特定实例的访问。

您可以选择使用 OpenSSL 等业界标准工具生成自己的 Amazon EC2 密钥对。您在安全、可信环境中生成密钥对，只有密钥对的公有密钥导入到 AWS 中；您安全地保存私有密钥。如果采用这种方法，建议您使用高质量的随机数字生成器。

您可以选择让 AWS 生成 Amazon EC2 密钥对。在这种情况下，当您首次创建实例时，系统会显示 RSA 密钥对的公有和私有密钥。您必须下载并安全地保存 Amazon EC2 密钥对的私有密钥。AWS 不存储私有密钥；如果丢失，您必须生成新的密钥对。

对于使用 **cloud-init** 服务的 Amazon EC2 Linux 实例，当从标准 AWS AMI 启动新实例时，Amazon EC2 密钥对的公有密钥会附加到初始操作系统用户的 **~/.ssh/authorized_keys** 文件。然后，通过将 SSH 客户端配置成使用正确 Amazon EC2 实例用户的名称作为其身份（例如 ec2-user），并提供用于用户身份验证的私有密钥文件，该用户将能够使用 SSH 客户端连接到 Amazon EC2 Linux 实例。

对于使用 **ec2config** 服务的 Amazon EC2 Windows 实例，当从标准 AWS AMI 启动新实例时，**ec2config** 服务会为该实例设置新的随机管理员密码，并使用相应 Amazon EC2 密钥对的公有密钥对其进行加密。通过使用 AWS 管理控制台或命令行工具，并提供相应的 Amazon EC2 私有密钥对密码进行解密，用户能够获得 Windows 实例密码。此密码连同 Amazon EC2 实例的默认管理账户可用于对 Windows 实例进行身份验证。

AWS 提供了一系列灵活实用的工具，用于管理 Amazon EC2 密钥，以及对新启动的 Amazon EC2 实例提供业界标准的身份验证。如果您具有更高的安全要求，可以实施 LDAP 或 Active Directory 身份验证等替代身份验证机制，并禁用 Amazon EC2 密钥对身份验证。

保护您的数据

此部分探讨如何保护 AWS 平台上的静态数据和传输中的数据。我们假设您已经确定并分类了您的资产，并根据资产的风险情况设定了资产保护目标。

资源访问授权

用户或 IAM 角色经过身份验证以后，可以访问他们已获权访问的资源。您依据用户是否需要对资源的控制权，以及是否需要取代单独的用户控制，通过资源策略或功能策略提供资源授权。

- **资源策略**适用于用户创建资源后想要允许其他用户访问这些资源的情况。在此模型中，该策略被直接挂载到资源，并描述谁能够对资源执行什么操作。用户对资源拥有控制权。您可以为 IAM 用户提供对资源的显式访问权限。根 AWS 账户始终具有管理资源策略的访问权限，是在该账户中创建的所有资源的所有者。或者，您也可以向用户授权，使其可以显式访问资源管理权限。
- **功能策略**（在 IAM 文档中称为“基于用户的权限”）通常用于推行公司范围的访问策略。功能策略直接或使用 IAM 组间接分配给 IAM 用户。这些策略也可分配给将在运行时担任的角色。功能策略定义允许或拒绝用户执行的功能（操作）。功能策略可通过显式拒绝基于资源的策略权限来取代它们。
- 可使用 IAM 策略将访问限制到特定 IP 地址范围，或者限制到特定几天或一天当中的特定时间段，以及根据其他条件设置限制。

- 资源策略和功能策略本质上具有累积性：单个用户的有效权限是资源策略与直接或通过组成员关系授予的功能权限的合集。

在云中存储和管理加密密钥

依赖加密的安全措施需要使用密钥。在云中如在本地系统中一样，保护您的密钥非常重要。

您可以使用现有流程在云中管理加密密钥，或者，您可以利用具有 AWS 密钥管理和存储功能的服务器端加密。

如果您决定使用自己的密钥管理流程，可以通过不同方法存储和保护密钥资料。我们强烈建议您将密钥存储在防篡改存储（例如硬件安全模块）中。Amazon Web Services 在云中提供 HSM 服务，称为 AWS CloudHSM。或者，您也可以使用在本地存储密钥的 HSM，并通过安全链接访问它们，例如连接到 Amazon VPC 的 IPSec 虚拟专用网络 (VPN)，或者采用 IPSec 的 AWS Direct Connect。

您可以使用本地 HSM 或 CloudHSM 支持各种使用案例和应用程序，例如，数据库加密、数字权限管理 (DRM)，以及包括验证和授权、文档签名和事务处理的公钥基础设施 (PKI)。CloudHSM 目前使用 SafeNet 提供的 Luna SA HSM。Luna SA 的设计符合联邦信息处理标准 (FIPS) 140-2 和 Common Criteria EAL4+ 标准，并支持各种行业标准加密算法。

注册 CloudHSM 时，您会收到 CloudHSM 设备的专用单租户访问权限。每个设备在 Amazon VPC 中显示为一项资源。CloudHSM 的加密域由您进行初始化和管理，而非由 AWS 完成。加密域是限制您的密钥访问权限的逻辑和物理安全边界。只有您可以控制自己的密钥和 CloudHSM 执行的操作。AWS 管理员将管理、维护和监控 CloudHSM 设备的运行状况，但没有加密域的访问权限。在您对加密域进行初始化后，可以在 EC2 实例上配置客户端，允许应用程序使用 CloudHSM 提供的 API。

您的应用程序可以使用 CloudHSM 支持的标准 API，例如 PKCS#11、MS CAPI 和 Java JCA/JCE （Java 加密架构/Java 加密扩展）。CloudHSM 客户端为您的应用程序提供 API，并使用经过相互身份验证的 SSL 连接来连接 CloudHSM 设备，实施每个 API 调用。

您可以在多个可用区（各可用区之间可进行复制）中实施 CloudHSM，以便实现更高的可用性和存储弹性。

保护静态数据

出于法规或业务要求原因，您可能想要进一步保护存储在 Amazon S3、Amazon EBS、Amazon RDS 或 AWS 其他服务中的静态数据。

表 7 列出了在 AWS 中对静态数据实施保护时需要考虑的问题。

问题	推荐的保护方法	策略
意外信息泄露	将数据指定为机密并限制能够访问这些信息的用户数目。使用 AWS 权限管理对用于 Amazon S3 等服务的资源的访问。使用加密保护 Amazon EBS 或 Amazon RDS 上的机密数据。	权限 文件、分区、卷或应用程序级加密
数据完整性受损	为确保数据完整性不因蓄意或意外的修改而受损，可使用资源权限来限制能够修改这些数据的用户的范围。即便使用了资源权限，特权用户的意外删除仍然是一个威胁（包括木马可能利用特权用户的凭证进行的攻击），这也显示了最小特权原则的重要性。应执行数据完整性检查，例如消息验证代码 (SHA-1/SHA-2) 或哈希消息验证代码 (HMAC)、数字签名或者验证加密 (AES-GCM)，以检测数据完整性受损情况。如果您检测到数据受损，则从备份恢复这些数据；或者，在使用 Amazon S3 的情况下，从先前的对象版本恢复这些数据。	权限 数据完整性检查（MAC/HMAC/数字签名/验证加密） 备份 版本控制 (Amazon S3)
意外删除	使用正确权限和最小特权规则是防范意外或恶意删除的最佳方式。对于 Amazon S3 等服务，您可以使用 MFA 删除功能要求对删除对象的操作进行多重身份验证，从而将对 Amazon S3 对象的访问限定于特权用户。如果您检测到数据受损，则从备份恢复这些数据；或者，在使用 Amazon S3 的情况下，从先前的对象版本恢复这些数据。	权限备份 版本控制 (Amazon S3) MFA 删除 (Amazon S3)
系统、基础设施、硬件或软件可用性	如果出现系统故障或发生自然灾害，则从备份或副本恢复您的数据。Amazon S3 和 Amazon DynamoDB 等某些服务提供区域内多个可用区之间的自动数据复制。 还有一些服务要求您配置复制或备份。	备份复制

表 7：对静态数据的威胁

分析适用于您的威胁情形，并采用“*表 1：示例资产矩阵设计* 您的 ISMS 以保护您的资产”部分概述的相关保护方法。

以下章节介绍如何配置 AWS 提供的不同服务以便保护静态数据。

保护 Amazon S3 上的静态数据

Amazon S3 提供了众多保护静态数据的安全功能，您可以视威胁情形选用。表 8 总结了这些功能：

Amazon S3 功能	描述
权限	将存储桶级或对象级权限与 IAM 策略一同使用，以防止资源遭受越权访问，并防止信息泄露、数据完整性受损或数据删除。
版本控制	Amazon S3 支持对象版本。默认情况下禁用版本控制。启用版本控制可以存储每个已修改或已删除对象的新版本，必要时您可以从这些新版本恢复受损的对象。
复制	Amazon S3 在相应区域内的所有可用区间复制每个对象。在发生系统故障时，复制可提供数据和服务可用性，但不会防止意外删除或数据完整性受损 – 其在保存副本的所有可用区间复制更改。Amazon S3 提供标准冗余和低冗余选项，这些选项具有不同的持久性目标和价位。
备份	Amazon S3 支持数据复制和版本控制，而不是自动备份。但您可以使用应用程序级技术将 Amazon S3 中存储的数据备份到其他 AWS 区域或本地备份系统中。
加密 – 服务器端	Amazon S3 支持用户数据的服务器端加密。服务器端加密对最终用户是透明的。AWS 为每个对象生成唯一加密密钥，然后使用 AES-256 加密对象。然后，结合使用 AES-256 和存储在安全位置的主密钥对该加密密钥本身进行加密。主密钥定期进行轮换。
加密 – 客户端	采用客户端加密时，您将创建和管理自己的加密密钥。您创建的密钥不会以明文形式导出到 AWS。在将数据提交到 Amazon S3 之前，您的应用程序会对其进行加密，并在从 Amazon S3 收到数据后会对其进行解密。数据以加密形式存储，密钥和算法只有您知道。尽管您可以使用任何加密算法，以及使用对称或非对称密钥对数据进行加密，但 AWS 提供的 Java 软件开发工具包提供了 Amazon S3 客户端加密功能。有关更多信息，请参阅*参考文献与其他读物*。

表 8：Amazon S3 静态数据保护功能

保护 Amazon EBS 上的静态数据

Amazon EBS 是 AWS 抽象数据块存储服务。您收到的每个 Amazon EBS 卷均采用未格式化的原始模式，就像新硬盘一样。您可以对 Amazon EBS 卷进行分区，创建软件 RAID 阵列，利用您选择的任何文件系统格式化这些分区，并最终保护 Amazon EBS 卷上的数据。针对 Amazon EBS 卷的所有这些决定和操作对 AWS 操作而言均不透明。

您可以将 Amazon EBS 卷挂载到 Amazon EC2 实例。

表 9 总结了通过在 Amazon EC2 实例上运行的操作系统保护静态 Amazon EBS 数据的功能。

Amazon EBS 功能	描述
复制	每个 Amazon EBS 卷均以文件的形式存储，AWS 创建 EBS 卷的两个副本以实现冗余。但这两个副本位于同一可用区中，因此 Amazon EBS 复制能够不受硬件故障的影响；这种方式不适合用作长期断电情况下或出于灾难恢复目的的可用性工具。我们建议您在应用程序级别复制数据，并且/或者创建备份。
备份	Amazon EBS 提供在特定时间点捕获 Amazon EBS 卷上存储的数据的快照。如果该卷受损（例如因系统故障）或其中的数据被删除，您可以从快照恢复该卷。 Amazon EBS 快照 AWS 对象，IAM 用户、组或角色可以获得访问这些对象的权限，因此只有授权用户才能够访问 Amazon EBS 备份。
加密：Microsoft Windows EFS	如果您正在 AWS 上运行 Microsoft Windows Server，并且需要额外的数据保密性级别，则可以实施加密文件系统 (EFS)，以进一步保护系统或数据分区上存储的敏感数据。EFS 是 NTFS 文件系统的扩展，可实现透明的文件和文件夹加密，并与 Windows 和 Active Directory 密钥管理设施以及 PKI 集成。您可以在 EFS 上管理自己的密钥。
加密：Microsoft	Windows BitLocker 是 Windows Server 2008 及更高操作系统上提供的卷（在单驱动器情况下为分区）加密解决方案。BitLocker 使用
Windows Bitlocker	AES 128 和 256 位加密。 默认情况下，BitLocker 需要使用受信任的平台模块 (TPM) 存储密钥；在 Amazon EC2 上不支持该模块。但您可以使用 BitLocker 保护 EBS 卷（如果您将其配置成使用密码）。有关更多信息，请参阅以下白皮书：Amazon 公司 IT 部门将 SharePoint 2010 部署到 Amazon Web Services 云。

Amazon EBS 功能	描述
加密：Linux dm- crypt	在运行内核 2.6 版或更高版本的 Linux 实例上，您可以使用 dm-crypt 在 Amazon EBS 卷和交换空间上配置透明数据加密。您可以使用各种密码以及 Linux Unified Key Setup (LUKS) 进行密钥管理。
加密：TrueCrypt	TrueCrypt 是一种第三方工具，它在 Amazon EBS 卷上提供透明的静态数据加密。TrueCrypt 同时支持 Microsoft Windows 和 Linux 操作系统。
加密和完整性验证：SafeNet ProtectV	SafeNet ProtectV 是一种第三方解决方案，可实现 Amazon EBS 卷的全磁盘加密以及 AMI 的预引导身份验证。SafeNet ProtectV 为数据和基础操作系统提供数据机密性和数据完整性验证。

表 9：Amazon EBS 静态数据保护功能

保护 Amazon RDS 上的静态数据

Amazon RDS 与 Amazon EC2 利用相同的安全基础设施。您可以使用无额外保护的 Amazon RDS 服务，但如果您出于合规性或其他目的需要对静态数据进行加密或执行数据完整性验证，则可以在应用层添加保护，或者使用 SQL 加密函数在平台层添加保护。

您可以在应用层添加保护，例如使用对所有敏感数据库字段进行加密的内置加密功能（使用应用程序密钥），然后再将这些字段存储在数据库中。应用程序可结合 PKI 基础设施使用对称加密，或者使用其他非对称密钥方法来管理密钥，以便提供主加密密钥。

您可以使用 MySQL 加密函数在平台上添加保护；这可采用语句的形式，例如：

```
INSERT INTO Customers (CustomerFirstName,CustomerLastName) VALUES
(AES_ENCRYPT('John',@key), AES_ENCRYPT('Smith',@key);
```

平台级加密密钥将在应用程序级别加以管理，例如应用程序级加密密钥。表 10 总结了 Amazon RDS 平台级保护选项。

Amazon RDS 平台	说明
MySQL	MySQL 加密函数包括用于加密、哈希和压缩的函数。有关更多信息，请参阅 https://dev.mysql.com/doc/refman/5.5/en/encryption- functions.html。
Oracle	在自带许可 (BYOL) 模式下，Amazon RDS for Oracle Enterprise Edition 上支持 Oracle 透明数据加密。
Microsoft SQL	Microsoft Transact-SQL 数据保护函数包括用于加密、签名和哈希的函数。有关更多信息，请参阅 http://msdn.microsoft.com/en-us/library/ms173744。

表 10：Amazon RDS 平台级静态数据保护

注意，SQL 范围查询不再适用于数据的加密部分。例如，对于诸如“John”、“Jonathan”和“Joan”等姓名，如果 `CustomerFirstName` 列的内容在应用或平台层进行了加密，则以下查询将不会返回预期结果：

```
SELECT CustomerFirstName, CustomerLastName from Customers WHERE
CustomerName LIKE 'Jo%';”
```

如下的直接比较将正常执行，并且对于 `CustomerFirstName` 完全匹配“John”的所有字段将返回预期结果。

```
SELECT CustomerFirstName, CustomerLastName FROM Customers WHERE
CustomerFirstName = AES_ENCRYPT('John', @key);
```

在未加密的字段上也将正常执行范围查询。例如，表中的 Date 字段可不加密，以便您能够在范围查询中使用该字段。

单向函数是模糊个人标识符的很好方式，例如社会保障号码或等同的个人 ID（在将它们作为唯一标识符时）。尽管您能够加密个人标识符，并在使用它们之前在应用或平台层对它们进行解密，但使用单向函数（例如加密 HMAC-SHA1）将个人标识符转换为固定长度的哈希值更加便利。个人标识符仍是唯一的，因为在商业 HMAC 中发生冲突的情况极为罕见。HMAC 不可逆向转换为原个人标识符，因此，除非您知道原个人 ID 并通过相同加密 HMAC 函数对其进行处理，否则无法通过这些数据反向追踪到原个人。

在所有区域中，Amazon RDS 均支持透明数据加密和本地网络加密，二者均为 Oracle Database 11g Enterprise Edition 的高级安全选项的组成部分。在自带许可 (BYOL) 模式下，Amazon RDS for Oracle 上提供 Oracle Database 11g Enterprise Edition。使用这些功能不收取任何额外费用。

Oracle 透明数据加密在将数据写入存储之前对数据进行加密，并在从存储读取数据时对数据进行解密。凭借 Oracle 透明数据加密，您能够使用高级加密标准 (AES) 和数据加密标准（三重 DES）等业界标准加密算法对表空间或特定表列进行加密。

保护 Amazon Glacier 上的静态数据

存储在 Amazon Glacier 上的所有数据均使用服务器端加密进行保护。AWS 为每个 Amazon Glacier 存档生成单独的唯一加密密钥，并使用 AES-256 对其进行加密。然后，结合使用 AES-256 和存储在安全位置的主密钥，对该加密密钥本身进行加密。主密钥定期进行轮换。如果您需要对静态信息提供更多保护，可以在将数据上传到 Amazon Glacier 之前对其进行加密。

保护 Amazon DynamoDB 上的静态数据

Amazon DynamoDB 是由 AWS 提供的共享服务。您可以在不添加保护的情况下使用 DynamoDB，但也可在标准 DynamoDB 服务基础上实施数据加密层。有关在应用层保护数据的注意事项，包括对范围查询的影响，请参阅上一节。

DynamoDB 支持数字、字符串和原始二进制数据类型格式。将加密字段存储在 DynamoDB 中时，最好使用原始二进制字段或 Base64 编码的字符串字段。

保护 Amazon EMR 上的静态数据

Amazon EMR 是云中的一种托管服务。AWS 提供运行 Amazon EMR 所需的 AMI，您不能使用自定义 AMI 或您自己的 EBS 卷。默认情况下，Amazon EMR 实例不对静态数据进行加密。

Amazon EMR 集群经常使用 Amazon S3 或 DynamoDB 作为持久性数据存储。Amazon EMR 集群在启动时能够将运行所需的数据从持久性存储复制到 HDFS，或者使用直接来自 Amazon S3 或 DynamoDB 的数据。

为提供更高级别的静态数据机密性或完整性，您可以采用表 11 中汇总的各种方法。

要求	描述
Amazon S3 服务器端加密 — 无 HDFS 副本	数据仅永久存储在 Amazon S3 上，从不复制到 HDFS。Hadoop 从 Amazon S3 提取数据，然后在本地处理数据，并不创建持久性本地副本。 有关 Amazon S3 服务器端加密的更多信息，请参阅*保护 Amazon S3 上的静态数据*部分。
Amazon S3 客户端加密	数据仅永久存储在 Amazon S3 上，从不复制到 HDFS。Hadoop 从 Amazon S3 提取数据，然后在本地处理数据，并不创建持久性本地副本。要应用客户端解密，您可以将自定义串行器/解串器 (SerDe) 与 Hive 或用于 Java Map Reduce 作业的 InputFormat 等产品一同使用。在每个单独的行或记录上应用加密，以便您能够拆分文件。 有关 Amazon S3 客户端加密的更多信息，请参阅*保护 Amazon S3 上的静态数据*部分。
应用程序级加密 — 整个文件加密	将数据存储在 Amazon S3 或 DynamoDB 中时，您可以在应用程序级别加密或保护数据的完整性（例如，通过使用 HMAC-SHA1）。 为解密数据，可将自定义 SerDe 与 Hive、脚本或引导操作一同使用，以便从 Amazon S3 中提取数据，对数据进行解密，将其加载到 HDFS，然后进行处理。由于已对整个文件进行了加密，您可能需要在单个结点上执行此操作，例如主节点。您可以将 S3Distcp 等工具与特殊编解码器一同使用。
应用程序级加密 — 单个字段加密/保持结构	Hadoop 可使用标准 SerDe，例如 JSON。数据解密可在 Hadoop 作业的映射阶段进行，您可以通过用于流式作业的自定义加密工具使用标准输入/输出重定向。
混合	您可能想要组合使用 Amazon S3 服务器端加密与客户端加密，以及应用程序级加密。

表 11：保护 Amazon EMR 上的静态数据

Gazzang 等 Amazon 软件合作伙伴为保护 Amazon EMR 上的静态和传输中的数据提供了专业化解决方案。

安全停用数据和介质

在云中停用数据的方式与在传统本地环境中不同。

当您要求 AWS 删除云中的数据时，AWS 不会停用基础物理介质，而是将存储块标记为未分配。AWS 使用安全的机制将这些存储块重新分配到别处。当您预配置数据块存储时，管理程序或虚拟机管理器 (VMM) 将跟踪您的实例已写入到哪些数据块中。当某个实例写入存储数据块时，上一个数据块被清零，然后由您的数据块覆盖。如果您的实例尝试从先前写入的数据块读取数据，则将返回您先前存储的数据。如果某个实例尝试从先前尚未写入的数据块读取数据，则管理程序会清零磁盘上的先前数据，并向该实例返回零。

当 AWS 确定介质已达到其使用寿命的终点，或者其遇到硬件故障时，作为停用流程的一部分，AWS 遵循美国国防部 (DoD) 5220.22-M （“国家工业安全计划操作手册”）或 NIST SP 800-88 （“存储介质清理指南”）中详细描述的方法来销毁数据。

有关删除云中数据的更多信息，请参阅 AWS 安全流程白皮书。（请参阅参考文献与延伸阅读。）

当您出于法规或业务原因要求进一步控制安全退役数据时，您可以使用未存储在云中的客户托管密钥实施静态数据加密。然后，除遵循先前的流程以外，您还要删除用于保护已退役数据的密钥，从而使其不可恢复。

保护传输中的数据

云应用程序通常通过公共链接（例如 Internet）进行通信，因此，当您运行云中的应用程序时，保护传输中的数据非常重要。这涉及到保护客户端与服务器之间的网络流量，以及服务器之间的网络流量。

表 12 列出了通过公共链接（如 Internet）通信时的常见问题。

问题	说明	推荐的保护措施
意外信息泄露	应限制对您的机密数据的访问。当数据穿越公共网络时，应通过加密防止数据泄露。	使用 IPSec ESP 和/或 SSL/TLS 加密传输中的数据。
数据完整性受损	无论是否为机密数据，您都应当知道数据完整性是否因蓄意或意外修改而受损。	使用 IPSec ESP/AH 和/或 SSL/TLS 验证数据完整性。
对等身份受损/身份欺骗/中间人	加密和数据完整性验证对于保护通信通道非常重要。对连接的远程端进行身份验证同样非常重要。如果远程端恰巧是攻击者，或者是将此连接中继到预定接收者的冒充者，则加密通道毫无价值。	将具有 IKE 的 IPSec 与预共享密钥或 X.509 证书一同使用对远程端进行身份验证。或者，根据服务器公用名 (CN) 或替代名称 (AN/SAN)，将 SSL/TLS 与服务器证书验证一同使用。

表 12：对传输中的数据的威胁

AWS 提供的服务对 IPSec 和 SSL/TLS 均提供支持，以保护传输中的数据。IPSec 是一种扩展 IP 协议栈的协议，通常用于网络基础设施中，其可使上层的应用程序安全地通信而不会遭到修改。另一方面，SSL/TLS 在会话层运行，尽管有第三方 SSL/TLS 包装程序，但它通常还需要应用层的支持。

以下章节提供了有关保护传输中的数据的详细信息。

管理应用程序以及对 AWS 公有云服务的管理访问

当访问在 AWS 公有云中运行的应用程序时，您的连接会跨越 Internet。在大多数情况下，您的安全策略将 Internet 视为不安全的通信媒体，并且要求保护传输中的应用程序数据。

表 13 概括了在访问公有云服务时保护传输中的数据的方法。

协议/方案	描述	推荐的保护方法
HTTP/HTTPS 流量（Web 应用程序）	HTTP 流量在默认情况下不受保护。对 HTTP 流量的 SSL/TLS 保护（也称为 HTTPS）是业界标准，受到 Web 服务器和浏览器的广泛支持。 HTTP 流量不仅包括对网页的客户端访问，还可包括 Web 服务（基于 REST 的访问）。	结合使用 HTTPS (HTTP over SSL/TLS) 与服务器证书验证。
HTTPS 卸载（Web 应用程序）	尽管通常建议使用 HTTPS，尤其是对于敏感数据，但 SSL/TLS 处理需要耗用 Web 服务器和客户端的更多 CPU 和内存资源。对于处理数千 SSL/TLS 会话的 Web 服务器，这可能会带来非常大的负载。对客户端的影响较小，因为仅终止有限数量的 SSL/TLS 连接。	卸载 Elastic Load Balancing 上的 HTTPS 处理可最大程度减少对 Web 服务器的影响，同时仍保护传输中的数据。可以使用 HTTP over SSL 等应用程序协议保护到实例的后端连接。
远程桌面协议 (RDP) 流量	访问公有云中 Windows 终端服务的用户通常使用 Microsoft 远程桌面协议 (RDP)。 在默认情况下，RDP 连接建立基础 SSL/TLS 连接。	为实现最佳保护，应向正被访问的 Windows 服务器发放可信 X.509 证书，以防止身份欺骗或中间人攻击。默认情况下，Windows RDP 服务器使用自签名证书，这些证书不受信任，应避免使用。
安全外壳 (SSH) 流量	SSH 是与 Linux 服务器建立管理连接的首选方法。SSH 是一种类似 SSL 的协议，它在客户端与服务器之间提供安全通信通道。此外，SSH 还支持隧道，隧道用于在 SSH 之上运行应用程序（如 X-Windows），并且保护正在传输的应用程序会话。	使用 SSH 2 版（使用非特权用户账户）。
数据库服务器流量	如果客户端或服务器需要访问云中的数据库，它们可能还需要遍历 Internet。	大多数新型数据库支持对本机数据库协议使用 SSL/TLS 包装程序。对于 Amazon EC2 上运行的数据库服务器，建议使用此方法保护传输中的数据。在某些情况下，Amazon RDS 提供 SSL/TLS 支持。 请参阅*保护正在传输到 Amazon RDS 的数据*一节，了解更多详细信息。

表 13：在访问公有云时保护正在传输的应用程序数据

在管理 AWS 服务时保护正在传输的数据

您可以使用 AWS 管理控制台或 AWS API 管理 AWS 中的服务，如 Amazon EC2 和 Amazon S3。服务管理流量的示例包括启动新的 Amazon EC2 实例，将对象保存到 Amazon S3 存储桶，或者修改 Amazon VPC 上的安全组。

AWS 管理控制台在客户端浏览器与控制台服务终端节点之间使用 SSL/TLS，以保护 AWS 服务管理流量。流量已加密，数据完整性已得到验证，并且客户端浏览器通过使用 X.509 证书对控制台服务终端节点进行了身份验证。在客户端浏览器与控制台服务终端节点之间建立 SSL/TLS 会话后，SSL/TLS 会话中的所有后续 HTTP 流量都受到保护。

此外，您可以使用 AWS API 直接从应用程序或第三方工具，或者通过 SDK 或 AWS 命令行工具管理 AWS 的服务。AWS API 是 HTTPS 上的 Web 服务 (REST)。根据使用的 API，SSL/TLS 会话在客户端与特定 AWS 服务终端节点之间建立，SSL/TLS 会话中的所有后续流量都受到保护，包括 REST 信封和用户有效负载。

保护正在传输到 Amazon S3 的数据

像 AWS 服务管理流量一样，通过 HTTPS 访问 Amazon S3。这包括所有 Amazon S3 服务管理请求以及用户有效负载，如正在从 Amazon S3 存储/检索的对象内容，以及关联的元数据。

当使用 AWS 服务控制台管理 Amazon S3 时，会在客户端浏览器与服务控制台终端节点之间建立 SSL/TLS 安全连接。所有后续流量都在该连接中受到保护。

当直接或间接使用 Amazon S3 API 时，会在客户端与 Amazon S3 终端节点之间建立 SSL/TLS 连接，所有后续 HTTP 和用户有效负载流量都封装在受保护的会话中。

保护正在传输到 Amazon RDS 的数据

如果您要从同一区域内的 Amazon EC2 实例连接到 Amazon RDS，您可以依赖 AWS 网络的安全性，但如果您要从 Internet 进行连接，可能需要使用 SSL/TLS 来提供额外保护。

对于客户端与服务器间的连接，SSL/TLS 通过服务器 X.509 证书、数据完整性验证和数据加密来提供对等身份验证。

对于与 Amazon RDS MySQL 和 Microsoft SQL 实例的连接，当前支持 SSL/TLS。对于这两个产品，Amazon Web Services 都提供与 MySQL 或 Microsoft SQL 侦听器关联的单一自签名证书。您可以下载此自签名证书并将其指定为可信。这可实现对等身份验证，防止服务器端的中间人或身份欺骗攻击。SSL/TLS 提供对客户端与服务器之间通信通道的本机加密和数据完整性验证。因为 AWS 上的所有 Amazon RDS MySQL 实例都使用同一自签名证书，并且 AWS 上的所有 Amazon RDS Microsoft SQL 实例都使用另一个单一自签名证书，所以对等身份验证不提供单独实例身份验证。如果要通过 SSL/TLS 进行单独服务器身份验证，可能需要利用 Amazon EC2 和自托管关系数据库服务。

Amazon RDS for Oracle 本机网络加密在数据移入和移除数据库时对数据进行加密。通过 Oracle 本机网络加密，您可以使用业界标准加密算法（如 AES 和三重 DES）对 Oracle Net Services 上传输的网络流量进行加密。

保护正在传输到 Amazon DynamoDB 的数据

如果要从同一区域内的其他 AWS 服务连接到 DynamoDB，您可以依赖 AWS 网络的安全性，但如果您要通过 Internet 连接到 DynamoDB，则应使用 SSL /TLS 上的 HTTP (HTTPS) 连接到 DynamoDB 服务终端节点。避免使用 HTTP 访问 DynamoDB，也要避免用于所有 Internet 连接。

保护正在传输到 Amazon EMR 的数据

Amazon EMR 包含大量应用程序通信路径，而其中的每一个通信路径都需要单独的机制来保护传输中的数据。表 14 列出了通信路径和我们建议的保护方法。

Amazon EMR 流量的类型	描述	推荐的保护方法
Hadoop 节点之间	Hadoop 主节点、辅助节点和核心节点都使用专有普通 TCP 连接互相通信。但 Amazon EMR 上的所有 Hadoop 节点都位于同一可用区中，并且在物理和基础设施层上按安全标准进行保护。	通常无需额外保护 — 所有节点都在同一设施中。
Hadoop 集群与 Amazon S3 之间	Amazon EMR 使用 HTTPS 在 DynamoDB 与 Amazon EC2 之间发送数据。有关更多信息，请参阅*保护正在传输到 Amazon S3 的数据*一节。	默认情况下使用 HTTPS。
Hadoop 集群与 Amazon DynamoDB 之间	Amazon EMR 使用 HTTPS 在 Amazon S3 与 Amazon EC2 之间发送数据。有关更多信息，请参阅*保护正在传输到 Amazon DynamoDB 的数据*一节。	默认情况下使用 HTTPS。
对 Hadoop 集群的用户或应用程序访问	客户端或本地应用程序可使用脚本（基于 SSH 的访问）、REST 或协议（如 Thrift 或 Avro）	使用 SSH 对应用程序进行交互式访问，或者在 SSH 中为其他协议创建隧道。
	通过 Internet 访问 Amazon EMR 集群。	如果使用 Thrift、REST 或 Avro，则使用 SSL/TLS。
对 Hadoop 集群的管理访问	Amazon EMR 集群管理员通常使用 SSH 管理集群。	将 SSH 用于 Amazon EMR 主节点。

表 14：保护正在传输到 Amazon EMR 的数据

保护您的操作系统和应用程序

通过 AWS 责任共担模型，您可以管理您的操作系统和应用程序的安全。Amazon EC2 提供真正的虚拟计算环境，您可以在其中使用 Web 服务接口，来启动具有多种操作系统和自定义预加载应用程序的实例。您可以标准化操作系统和应用程序构建，在单个安全的构建存储库中集中管理您的操作系统和应用程序的安全。您可以构建和测试预配置的 AMI，以符合您的安全要求。

建议包括：

- 禁用根 API 访问密钥和私有密钥
- 使用安全组限制只能从有限 IP 范围访问实例
- 用密码保护用户计算机上的 .pem 文件
- 当有人离开您的组织或不再需要访问权限时，从您实例上的 authorized_keys 文件中删除密钥
- 轮换凭证（DB、访问密钥）
- 定期运行最小特权检查，使用 IAM 用户访问顾问和 IAM 用户上次使用的访问密钥
- 使用防御主机强制实施控制和可见性

本节不是为了提供针对 AMI 的全面强化标准列表。行业认可的系统强化标准来源包括（但不限于）：

- Center for Internet Security (CIS)
- 国际标准化组织 (ISO)
- SysAdmin Audit Network Security (SANS) 协会
- 美国国家标准与技术研究院 (NIST)

建议您为所有系统组件开发配置标准。确保这些标准可应对所有已知的安全漏洞，并且与行业认可的系统强化标准一致。

如果已发布的 AMI 被发现违反最佳实践，或者给运行 AMI 的客户带来重大风险，则 AWS 保留采取措施将 AMI 从公共目录中移除并向发布者和 AIM 运行者通知调查结果的权利。

创建自定义 AMI

您可以创建符合贵组织特定要求的自有 AMI，然后发布它们，供内部（私有）或外部（公用）使用。作为 AMI 发布者，您负责您在生产中使用的系统映像的初始安全状况。您在 AMI 上应用的安全控制在特定时间点有效，它们不是动态的。您可以通过符合业务需求、不违反 AWS 可接受使用策略的任何方式配置私有 AMI。有关更多信息，请参阅 Amazon Web Services 可接受使用策略 (http://*aws.amazon.com/aup/*)。

但从 AMI 启动的用户可能不是安全专家，因此我们建议您符合某些最低安全标准。

在您发布 AMI 前，请确保所发布的软件是带有相关安全补丁的最新版本，并且执行表 15 中所列的清理和强化任务。

领域	推荐的任务
禁用不安全的应用程序	禁用在网络上以明文或以其他不安全的方式对用户进行身份验证的服务和协议。
将风险降至最低	在启动时禁用不必要的网络服务。应仅启动管理服务 (SSH/RDP) 和必不可少的应用程序所需的服务。
保护凭证	从磁盘和配置文件中安全删除所有 AWS 凭证。
保护凭证	从磁盘和配置文件中安全删除所有第三方凭证。
保护凭证	从系统中安全删除所有其他证书或密钥资料。
保护凭证	确保安装的软件不使用默认内部账户和密码。
采用良好的管控机制	确保系统不违反 Amazon Web Services 可接受使用策略。违反示例包括开放式 SMTP 中继或代理服务器。有关更多信息，请参阅 Amazon Web Services 可接受使用策略 (http://*aws.amazon.com/aup/*)。

表 15：发布 AMI 前清除任务

表 16 和 17 列出了操作系统特定的其他清理任务。表 16 列出了保护 Linux AMI 的步骤。

领域	强化活动
保护服务	将 sshd 配置为仅允许公有密钥身份验证。在 sshd_config 中将 **PubkeyAuthentication** 设置为 **Yes**，并将 **PasswordAuthentication** 设置为 **No**。
保护服务	在创建实例时生成唯一 SSH 主机密钥。如果 AMI 使用 **cloud-init**，它会自动对此进行处理。
保护凭证	移除并禁用所有用户账户的密码，使它们不能用于登录，并且没有默认密码。对每个账户运行 **passwd -l <USERNAME>**。
保护凭证	安全删除所有用户 SSH 公有和私有密钥对。
保护数据	安全删除包含敏感数据的所有外壳程序历史记录和系统日志文件。

表 16：保护 Linux/UNIX AMI

表 17 列出了保护 Windows AMI 的步骤：

领域	强化活动
保护凭证	在创建实例时，确保所有启用的用户账户都有随机生成的新密码。您可以将 EC2 Config 服务配置为在启动时对 Administrator 账户执行此操作，但您必须在绑定映像前显式执行此操作。
保护凭证	确保 Guest 账户已禁用。
保护数据	清除 Windows 事件日志。
保护凭证	确保 AMI 不属于 Windows 域。
将风险降至最低	不启用任何文件共享、打印后台处理程序、RPC，以及其他不必要但在默认情况下启用的 Windows 服务。

表 17：保护 Windows AMI

引导启动

对强化的 AMI 进行了实例化后，您仍可使用引导应用程序修改和更新安全控制。常用引导应用程序包括 Puppet、Chef、Capistrano、Cloud-Init 和 Cfn-Init。您还可运行自定义引导 Bash 或 Microsoft Windows PowerShell 脚本，无需使用第三方工具。

以下是要考虑的几个引导操作：

- 安全软件更新安装超出 AMI 补丁级别的最新补丁、服务包和关键更新。
- 除 AMI 中捕获的当前应用程序级测试版外，初始应用程序补丁还安装应用程序级更新。
- 通过上下文数据和配置，实例可应用特定于启动它们所在的环境的配置，例如，生产、测试或 DMZ/内部。
- 向远程安全监控和管理系统注册实例。

管理补丁

您负责您的 AMI 和实时实例的补丁管理。建议您实例化补丁管理并保留写入程序。

尽管您可以将第三方补丁管理系统用于操作系统和主要应用程序，但最好还是保留一份包含所有软件和系统组件的清单，以及将每个系统上安装的安全补丁的清单与最新供应商安全补丁清单进行比较，以便验证是否已安装了最新供应商补丁。

实施用于识别新安全漏洞并为这些漏洞分配风险排名的流程。至少将最关键、最高风险的漏洞排名为“高”。

控制公用 AMI 的安全

请注意，公开共享重要凭证时，不要将它们留在 AMI 上。有关更多信息，请参阅有关如何安全共享和使用公用 AMI 的教程：
http://aws.amazon.com/articles/0155828273219400。

保护您的系统以防恶意软件

和您保护传统基础设施不受病毒、蠕虫、特洛伊木马、Rootkit、僵尸网络和垃圾邮件等的威胁一样，保护您在云中的系统。

请务必理解单个实例以及整个云系统感染恶意软件的影响：当用户有意或无意地在 Linux 或 Windows 系统上执行某个程序时，可执行文件代入了该用户的特权（或者在某些情况下，冒充另一个用户）。该代码可执行启动它的用户有权执行的任何操作。用户必须确保他们仅执行可信代码。

如果您在自己的系统上执行一段不可信代码，则该系统不再是您的系统，它已属于他人。如果超级用户或具有管理特权的用户执行不可信程序，则执行该程序所在的系统不再可信，恶意代码可能更改操作系统的某些部分，安装 Rootkit，或者建立用于访问系统的后门。它可能删除数据或破坏数据完整性，或者影响服务可用性，或者以隐秘或公开的形式将信息泄露给第三方。

考虑执行代码所在的实例是否感染。如果感染的实例是单一登录环境的一部分，或者如果实例间存在隐式信任模型，则感染会快速传播到单个实例之外，进入整个系统或实现更大范围的传播。这种规模的感染会快速导致数据泄露，数据和服务受损，并且可能损害公司的声誉。还可能造成直接财务后果，例如，如果它损害了向第三方提供的服务，或者过度消耗云资源。您必须管理恶意软件的威胁。

表 18 概括了防止恶意软件的一些常用方法。

因素	常用方法
不可信 AMI	仅从可信 AMI 启动实例。可信 AMI 包括 AWS 提供的标准 Windows 和 Linux AMI，以及可信第三方提供的 AMI。如果您从标准和可信 AMI 获得自己的自定义 AMI，则您对其应用的所有其他软件和设置也必须可信。启动不可信第三方 AMI 会损害和感染您的整个云环境。
不可信软件	仅安装和运行可信软件提供商提供的可信软件。可信软件提供商是业界备受尊重的软件提供商，以安全、负责任的方式开发软件，不允许恶意代码进入其软件包中。开源软件也可能是可信软件，您应能够编译您自己的可执行文件。强烈建议您仔细进行代码审查，确保源代码不是恶意的。 可信软件提供商通常使用代码签名证书对其软件进行签名，或者提供他们产品的 MD5 或 SHA-1 签名，以便您验证所下载的软件的完整性。
不可信软件仓库	从可信来源下载可信软件。Internet 或网络其他地方的任意软件来源实际上可能将恶意软件分布在合法和高声誉软件包内部。这些不可信方可能提供内含恶意软件的衍生包的 MD5 或 SHA-1 签名，因此这些签名应是不可信的。 建议您建立自己的可信软件的内部软件仓库，供您的用户安装和使用。非常不建议用户采用从 Internet 上的任意来源下载和安装软件的危险做法。
最小特权原则	为用户提供执行其任务所需的最小特权。这样，即使用户意外启动受感染可执行文件，对实例和更广泛云系统的影响也会降至最低。
修补	修补面向外部的系统和内部系统，使其达到最新安全级别。蠕虫通常通过网络上的未修补系统传播。
僵尸网络	如果感染 — 无论是传统病毒、特洛伊木马还是蠕虫 - 传播到单个实例之外，导致更大范围的感染，则可能携带创建僵尸网络的恶意代码，僵尸网络是一种可由远程攻击者控制的受感染主机的网络。遵循所有前述建议，避免感染僵尸网络。
垃圾邮件	攻击者可使用受感染系统发送大量未经请求的邮件（垃圾邮件）。AWS 提供特殊的控制来限制 Amazon EC2 实例能够发送的电子邮件数量，但是首先您应防止感染。避免 SMTP 开放式中继，它可用于传播垃圾邮件，还可能违反 AWS 可接受使用策略。有关更多信息，请参阅 Amazon Web Services 可接受使用策略 (http://aws.amazon.com/aup/)。
病毒/反垃圾邮件软件	一定要在您的系统上使用声望较高的最新防病毒和反垃圾邮件解决方案。
基于主机的 IDS 软件	许多 AWS 客户安装基于主机的 IDS 软件，例如开源产品 OSSEC，这些软件包括文件完整性检查和 Rootkit 检测软件。使用这些产品来分析重要系统文件和文件夹，以及计算反映它们可信状态的校验和，然后定期查看这些文件是否已被修改，如果是，则提醒系统管理员。

表 18：恶意软件防护方法

如果实例已受感染，防病毒软件可能会检测到感染并删除病毒。我们建议采用最安全且广泛推荐的方法，意在保存所有系统数据，接着从可信来源重新安装所有系统、平台和应用程序可执行文件，然后仅从备份恢复数据。

减少损害和滥用

AWS 提供全球基础设施供客户构建解决方案，其中的许多解决方案面向 Internet。我们的客户解决方案不能以危害 Internet 社区其余部分的方式运行，即，必须避免滥用活动。

滥用活动是外部观察到的针对 AWS 客户实例或其他资源的恶意、冒犯性、非法行为，或者可能危害其他 Internet 站点的行为。

AWS 与您合作检测和处理针对您的 AWS 资源的可疑和恶意活动。针对您的资源的意外或可疑行为可能表明，您的 AWS 资源已受损，这向您的企业发出了潜在风险信号。

AWS 使用以下机制检测针对客户资源的滥用活动：

- AWS 内部事件监控
- 针对 AWS 网络空间的外部安全情报
- 针对 AWS 资源的 Internet 滥用投诉

尽管 AWS 滥用响应团队积极监控并关闭 AWS 上运行的恶意滥用程序或欺诈程序，但大多数滥用投诉指向在 AWS 具有合法业务的客户。非故意滥用活动的常见原因包括：

- **资源受损。**例如，未修补的 Amazon EC2 实例可能受到感染，而成为僵尸网络代理。
- **非故意滥用。**例如，过度激进的 Web 爬网程序可能被某些 Internet 站点分类为 DOS 攻击程序。
- **次要滥用。**例如，AWS 客户提供的服务的最终用户可能在公有 Amazon S3 存储桶上发布恶意软件文件。
- **虚假投诉。**Internet 用户可能将合法活动误认为滥用行为。

AWS 致力于与 AWS 客户合作，共同防止、检测和减少滥用，防范以后再出现滥用。当您收到 AWS 滥用警告时，您的安全和运营员工必须立即调查问题。拖延可能会使其他 Internet 站点也遭受破坏，导致声誉受损，且可能导致您承担法律责任。更重要的是，受牵涉的滥用资源可能被恶意用户损害，忽视这种损害可能会加大对您业务造成的破坏。

使用您 AWS 资源的恶意、非法或有害活动违反 AWS 可接受使用策略，可导致账户冻结。有关更多信息，请参阅 Amazon Web Services 可接受使用策略 (http://*aws.amazon.com/aup/)*。您负责维护 Internet 社区评估的良好服务。如果 AWS 客户没有解决所报告的滥用活动，AWS 将冻结其 AWS 账户，以保护 AWS 平台和 Internet 社区的完整性。

表 19 列出了能够帮助您对滥用事件做出响应的最佳实践：

最佳实践	描述
不要忽视 AWS 滥用通信。	当提交滥用案例时，AWS 会立即向客户的注册电子邮件地址发送电子邮件通知。您只需回复此滥用警告电子邮件，即可与 AWS 滥用响应团队交流信息。所有通信均保存在 AWS 滥用跟踪系统中，以供未来参考。 AWS 滥用响应团队致力于帮助客户了解投诉的性质。AWS 帮助客户减少和防止滥用活动。账户冻结是 AWS 滥用响应团队阻止滥用活动所采取的最后措施。 我们与客户合作，共同减少问题并避免不得不采取任何惩罚性措施。但您必须对滥用警告做出响应，采取措施停止恶意活动，防止再次出现滥用。客户不响应是造成实例和账户受阻的主要原因。
遵循安全最佳实践。	防止资源受损的最佳措施是遵循本文中概述的安全最佳实践。尽管 AWS 提供了某些安全工具来帮助您为云环境建立强大的防御措施，但您必须像对待自己数据中心内的服务器一样遵循安全最佳实践。始终采用简单的防御做法，例如应用最新的软件补丁，通过防火墙和/或 Amazon EC2 安全组限制网络流量，为用户提供最小特权访问权限。
减少损害。	如果您的计算环境已受损或已被感染，建议执行以下步骤恢复到安全状态： • 将任何已知受损的 Amazon EC2 实例或 AWS 资源视为不安全的。如果您的 Amazon EC2 实例正在生成您的应用程序使用情况无法解释的流量，则您的实例可能已受损或被恶意软件感染。关闭并完全重新构建该实例，以返回到安全状态。尽管在真实情况下完全重新启动可能具有挑战性，但在云环境中，这是第一个缓解方法。 • 您可能需要对受损的实例执行取证分析，检测根本原因。此类调查仅应由训练有素的安全专家执行，您应隔离受感染的实例，以防止在调查期间造成进一步破坏和感染。 要隔离 Amazon EC2 实例以进行调查，您可以设置限制性极高的安全组，例如，除用于接受来自单一 IP 地址的入站 SSH 或 RDP 流量的端口（取证调查员可从该端口安全地检查实例）外，关闭其他所有端口。 您还可以拍摄受感染实例的脱机 Amazon EBS 快照，将此脱机快照提供给取证调查员，以便进行深入的分析。 AWS 无权访问您实例或其他资源内的私有信息，因此我们无法检测来宾操作系统或应用程序级损害，如应用程序账户接管。如果您没有通过自己的工具记录信息（如访问日志、IP 流量日志或其他属性），则 AWS 无法以回溯方式提供这些信息。您负责执行大多数深入事件调查和缓解活动。
	在从受损的 Amazon EC2 实例中恢复时，您必须采取的最后一步是备份关键业务数据，完全终止受感染的实例，然后将它们作为全新资源重新启动。 为避免将来受损，建议您检查新启动的实例的安全控制环境。应用最新软件补丁和限制防火墙等简单步骤非常有帮助。
设置安全通信电子邮件地址。	AWS 滥用响应团队使用电子邮件发出滥用警告通知。在默认情况下，该电子邮件发送到您的注册电子邮件地址，但如果您是一家大型企业，您可能需要创建专用响应电子邮件地址。您可以在您的 **Personal Information** 页面的 **Configure Additional Contacts** 下设置其他电子邮件地址。

表 19：缓解滥用最佳实践

使用其他应用程序安全实践

以下是针对您操作系统和应用程序的其他一些一般安全最佳实践：

- 在创建新的 AMI 或部署新应用程序之前，始终更改供应商提供的默认设置，包括（但不限于）密码、简单网络管理协议 (SNMP) 社区字符串，以及安全配置。
- 移除或禁用不必要的用户账户。
- 在每个 Amazon EC2 实例上实施一个主要功能，以防需要不同安全级别的功能在同一服务器上共存。例如，在单独的服务器上分别实施 Web 服务器、数据库服务器和 DNS。
- 根据系统功能的需要，仅启用必需且安全的服务、协议、守护程序等。禁用所有不必要的服务，因为它们会增加实例以及整个系统的安全风险。
- 禁用或移除所有不必要的功能，如脚本、驱动程序、功能、子系统、EBS 卷和不必要的 Web 服务器。

按照安全最佳实践配置所有服务。对所有需要的服务、协议或守护程序均启用安全功能。选择 SSH 等服务，这些服务具有可在不太安全的同等服务（例如 Telnet）上实现用户/对等身份验证、加密和数据完整性验证的内置安全机制。使用 SSH 进行文件传输，而不是使用 FTP 等不安全的协议。如果您无法避免使用不太安全的协议和服务，则在它们周围引入额外安全层，例如可在网络层保护通信通道的 IPSec 或其他虚拟专用网 (VPN) 技术，或者可在应用层保护网络流量的 GSS-API、Kerberos、SSL 或 TLS。

尽管安全治理对所有组织都非常重要，但最佳实践是执行安全策略。尽量将系统安全参数配置为符合您的安全策略和指导原则，以免错误使用。

对于对系统和应用程序的管理访问，使用强加密机制对所有非控制台管理访问进行加密。使用 SSH、用户以及站点间 IPSec VPN 或 SSL/TLS 等技术进一步保护远程系统管理。

保护您的基础设施

本节提供保护 AWS 平台上的基础设施服务的建议。

使用 Amazon Virtual Private Cloud (VPC)

通过 Amazon Virtual Private Cloud (VPC)，您可以在 AWS 公有云中创建私有云。

每个客户 Amazon VPC 都使用按客户分配的 IP 地址空间。您可以对您的 Amazon VPC 使用私有 IP 地址（如 RFC 1918 的建议），在云中构建不会直接路由到 Internet 的私有云和关联网络。

Amazon VPC 不仅提供与私有云中其他客户的隔离，还提供与 Internet 的第 3 层（网络层 IP 路由）隔离。表 20 列出了在 Amazon VPC 中保护应用程序的选项：

问题	描述	推荐的保护方法
仅限 Internet	Amazon VPC 没有连接到您本地或其他位置的任何基础设施。您可能有或没有位于本地或其他位置的额外基础设施。 如果需要接受来自 Internet 用户的连接，您可以通过将弹性 IP 地址 (EIP) 仅分配给需要它们的那些 Amazon VPC 实例来提供入站访问权限。您可以通过将安全组或 NACL 仅用于特定端口和安全 IP 地址范围，进一步限制入站连接。 如果能够平衡来自 Internet 的入站流量的负载，则无需 EIP。您可以将实例放在 Elastic Load Balancing 后面。 对于出站（至 Internet）访问，例如获取软件更新或者访问 AWS 公有服务（如 Amazon S3）的数据，您可以使用 NAT 实例为出站连接提供伪装。无需 EIP。	使用 SSL/TLS 加密应用程序和管理流量，或者构建自定义用户 VPN 解决方案。 仔细计划在公有和私有子网中的路由和服务器布局。 使用安全组和 NACL。
Internet 上的 IPSec	AWS 为 VPC 提供业界标准和弹性 IPSec 终止基础设施。客户可建立从其本地或其他 VPN 基础设施到 Amazon VPC 的 IPSec 隧道。 IPSec 隧道建立在 AWS 与您的基础设施终端节点之间。在云中或本地运行的应用程序不需要任何修改，它们可直接受益于传输中 IPSec 数据保护。	使用标准 AWS VPN 设施（Amazon VPC VPN 网关、客户网关和 VPN 连接）建立使用 IKEv1 和 IPSec 的私有 IPSec 连接。 或者在云中和本地建立客户特定的 VPN 软件基础设施。
无 IPSec 的 AWS Direct Connect	通过 AWS Direct Connect，您可以使用专用链路上的 AWS 私有对等，在不使用 Internet 的情况下建立到 Amazon VPC 的连接。根据您的数据保护要求，这种情况下可以选择不使用 IPSec。	根据您的数据保护要求，私有对等可能不需要额外保护。

问题	描述	推荐的保护方法
采用 IPSec 的 AWS Direct Connect	您可以在 AWS Direct Connect 链路上使用 IPSec，以实现额外端到端保护。	请参阅上面的“Internet 上的 IPSec”。
混合	考虑综合使用这些方法。对所用的每个连接方法都采用充分的保护机制。	

表 20：访问 Amazon VPC 中的资源

您可以利用 Amazon VPC-IPSec 或 VPC-AWS Direct Connect 以安全方式在本地或其他托管基础设施中与您的 Amazon VPC 资源无缝集成。对于任一种方法，IPSec 连接保护传输中的数据，而 IPSec 上的 BGP 或者 AWS Direct Connect 链路集成您的 Amazon VPC 和本地路由域，以实现任何应用程序，甚至是不支持本地安全机制的应用程序的透明集成。

尽管 VPC-IPSec 为您的应用程序提供业界标准的透明保护，您可能还是需要使用其他级别的保护机制，如 VPC-IPSec 链路上的 SSL/TLS。

有关更多信息，请参阅 Amazon VPC 连接选项白皮书。

使用安全分区和网络分段

不同的安全要求必须使用不同的安全控制。将基础设施分成强制使用类似安全控制的多个区域是安全最佳实践。

尽管 AWS 底层基础设施大部分由 AWS 运营和安全团队管理，您还是可以构建自己的覆盖基础设施组件。Amazon VPC、子网、路由表、分段/分区的应用程序，以及自定义服务实例（如用户存储库、DNS 和时间服务器）补充了 AWS 托管云基础设施。

网络工程团队通常将分段解释为另一种基础设施设计组件，应用以网络为中心的访问控制和防火墙规则来管理访问。安全分区和网络分段是两个不同的概念，但是：网络分段仅将一个网络与另一个网络进行隔离，而安全分区创建一组安全级别类似于通用控制的系统组件。

在 AWS 上，您可以使用以下访问控制方法构建网络分段：

- 使用 **Amazon VPC** 为每个工作负载或组织实体定义隔离网络。
- 使用**安全组**管理对具有类似功能和安全要求的实例的访问；安全组是状态防火墙，为每个允许的和建立的 TCP 会话或 UDP 通信通道均启用双向防火墙规则。
- 使用允许 IP 流量无状态管理的**网络访问控制列表** (NACL)。NACL 与 TCP 和 UDP 会话无关，但它们允许对 IP 协议（例如 GRE、IPSec ESP、ICMP） 进行粒度控制，允许按源/目的地 IP 地址以及用于 TCP 和 UDP 的端口进行控制。NACL 与安全组协同工作，甚至在流量到达安全组之前也可以允许或拒绝流量。
- 使用**基于主机的防火墙**控制对每个实例的访问。
- 在流量流中创建**威胁保护层**，强制使所有流量遍历区域。
- **在其他层**（例如应用程序和服务）应用**访问控制**。

传统环境要求使用代表单独广播实体的单独网络区段，以便通过中心安全执行系统（如防火墙）路由流量。AWS 云的安全组概念使这一要求变得过时。安全组是实例的逻辑分组，它们还允许对这些实例执行入站和出站流量规则，无论这些实例位于哪个子网。

创建安全区域需要按网络区段进行额外控制，通常包括：

- **共享访问控制** — 中央 Identity and Access Management (IDAM) 系统。请注意，尽管可进行联合，但这通常与 IAM 相分离。
- **共享审计记录** — 事件分析和关联以及跟踪安全事件需要进行共享记录。
- **共享数据分类** — 请参阅“表 1：示例资产矩阵设计您的 ISMS 以保护您的资产”一节，了解更多信息。
- **共享管理基础设施** — 各个组件，如防病毒/反垃圾邮件系统、修补系统和性能监控系统。
- **共享安全（保密性/完整性）要求** — 通常结合数据分类加以考虑。

为评估您的网络分段和安全分区要求，请回答以下问题：

- 我是否控制区域间通信？我能否使用网络分段工具管理安全区域 A 与 B 之间的通信？通常，访问控制元素（如安全组、ACL 和网络防火墙）应在各安全区域之间建立一堵墙。默认情况下，Amazon VPC 构建区域间隔离墙。
- 我能否根据业务要求，使用 IDS/IPS/DLP/SIEM/NBAD 系统监控区域间通信？阻止访问和管理访问是不同的术语。安全区域之间的多孔通信要求在区域之间使用完善的安全监控工具。通过 AWS 实例的水平可扩展性，可在操作系统级别上对每个实例进行分区，利用基于主机的安全监控代理。
- 我能否应用每区域访问控制权限？分区的好处之一是控制出口访问。由资源控制访问在技术上是可能的，例如 Amazon S3 和 Amazon SMS 资源策略。
- 我能否使用专用管理通道/角色管理每个区域？针对特权访问的基于角色的访问控制是一项常见要求。您可以使用 IAM 在 AWS 上创建组和角色，以便创建不同的特权级别。您还可以模拟与应用程序和系统用户相同的方法。基于 Amazon VPC 的网络的主要新功能之一是支持多个弹性网络接口。安全工程师可使用双主机实例创建管理覆盖网络。
- 我可以应用每区域保密性和完整性规则吗？每区域加密、数据分类和 DRM 直接增强整体安全状况。如果安全要求根据每个安全区域而不同，则数据安全要求也必须不同。在每个安全区域使用不同的加密选项及轮换密钥始终是个好策略。

AWS 提供灵活的安全分区选项。安全工程师和架构师可以利用以下 AWS 功能，按 Amazon VPC 访问控制在 AWS 上构建隔离的安全区/区段：

- 每子网访问控制
- 每安全组访问控制
- 每实例访问控制（基于主机）
- 每 Amazon VPC 路由块
- 每资源策略 (S3/SNS/SMS)
- 每区域 IAM 策略
- 每区域日志管理

- 每区域 IAM 用户，管理用户
- 每区域日志源
- 每区域管理通道（角色、界面、管理控制台）
- 每区域 AMI
- 每区域数据存储资源（Amazon S3 存储桶或 Glacier 存档）
- 每区域用户目录
- 每区域应用程序/应用程序控制

凭借弹性云基础设施和自动部署，您可以跨所有 AWS 区域应用相同的安全控制机制。可重复的统一部署可以改进总体安全态势。

加强网络安全

AWS 遵循责任共担模型，以安全的方式配置数据中心网络、路由器、交换机和防火墙等基础设施组件。您负责控制对您云中系统的访问、在您的 Amazon VPC 中配置网络安全以及安全的入站和出站网络流量。

虽然应用身份验证和资源访问授权至关重要，但这无法阻止攻击者获得网络级别的访问和试图冒充合法用户。基于用户的网络位置控制对应用程序和服务的访问提供了额外的安全层。例如，具有强大用户身份验证功能的基于 Web 的应用程序也可从基于 IP 地址的防火墙（限制源流量进入特定范围的 IP 地址）和入侵防御系统（限制安全漏洞和最大限度地缩小应用程序潜在攻击面）获益。

AWS 云中的网络安全最佳实践包括：

- 始终使用安全组：它们可为 Amazon EC2 实例提供虚拟机管理程序级别的状态防火墙。您可以向单个实例和单个 ENI 应用多个安全组。
- 具有网络 ACL 的增强安全组：它们是无状态的，但提供快捷、高效的控制。网络 ACL 不特定于实例，因此，它们能够在安全组之外提供另一个控制层。您可以向 ACL 管理和安全组管理应用职责分离。
- 为到其他站点的受信连接使用 IPSec 或 AWS Direct Connect。使用虚拟网关 (VGW)，其中，基于 Amazon VPC 的资源需要远程网络连接。

- 保护传输中的数据，以确保数据的保密性和完整性以及通信各方的身份。
- 对于大规模部署，设计分层的网络安全。不要创建单一网络安全保护层，而应在外部、DMZ 和内部层应用网络安全。
- 利用 VPC 流日志这项功能，您可以进一步捕获有关传入和传出您的 VPC 中网络接口的 IP 流量的信息。

许多与您交互的 AWS 服务终端节点不提供本机防火墙功能或访问控制列表。AWS 通过当今最先进的网络和应用级控制系统来监控和保护这些终端节点。您可以借助 IAM 策略基于请求的源 IP 地址限制对您资源的访问。

保护外围系统：用户存储库、DNS、NTP

覆盖安全控制机制只在安全的基础设施上有效。DNS 查询流量是这种控制类型的绝佳示例。如果 DNS 系统不够安全，DNS 客户端流量可能会被截获，查询和响应中的 DNS 名称可能会被假冒。对于缺乏基本控制机制的基础设施来说，欺骗是一种简单但有效的攻击手段。SSL/TLS 可提供额外的防护。

某些 AWS 客户使用 Amazon Route 53 （一种安全的 DNS 服务）。如果您需要内部 DNS，则可在 Amazon EC2 实例上实施自定义 DNS 解决方案。DNS 是基础设施解决方案的重要组成部分，因此，它成为您的安全管理计划的一个重要组成部分。所有 DNS 系统以及其他重要的自定义基础设施组件都应该应用以下控制机制：

常见控制机制	描述
单独的管理级访问	实施角色分离和访问控制机制，以限制对此类服务的访问，往往与应用程序访问或访问基础设施的其他部分所需的访问控制机制分离。
监控、报警、审计跟踪	记录和监控授权及非授权的活动。
网络层访问控制	将网络访问限制到仅包括需要它的系统。如有可能，为所有网络级访问尝试应用协议实施（即，为 NTP 和 DNS 实施自定义的 RFC 标准）。
已打安全补丁的最新的稳定版软件	确保软件已打补丁，且不受任何已知漏洞或其他风险的影响。
持续的安全测试（评估）	确保定期测试基础设施。
所有其他安全控制流程均已到位	除特定于服务的自定义安全控制机制以外，还确保外围系统遵循您的信息安全管理体系 (ISMS) 最佳实践。

表 21：外围系统的控制

除了 DNS，其他的基础设施服务可能需要特定的控制机制。

集中式访问控制是管理风险的关键。IAM 服务为 AWS 提供了基于角色的身份和访问管理，但 AWS 并不为您的操作系统和应用程序提供 Active Directory、LDAP 或 RADIUS 之类的最终用户存储库。相反，除了身份验证授权审计 (AAA) 服务器（有时还包括专有的数据库表）以外，您还需要构建用户标识和身份验证系统。用于用户平台和应用程序的所有身份和访问管理服务器都对安全至关重要，需要特别注意。

时间服务器也是至关重要的自定义服务。它们在许多安全相关的事务（包括登录时间戳和证书验证）中必不可少。使用集中式时间服务器并使所有系统与同一个时间服务器同步非常重要。支付卡行业 (PCI) 数据安全标准 (DSS) 提出了一种极好的时间同步方法：

- 确认实施了时间同步技术并保持最新状态。
- 获得并审核在组织内获取、分配和存储正确时间的流程，并审核一个示例系统组件的时间相关系统参数设置。
- 确认仅指定的中央时间服务器可从外部源接收时间信号，并且来自外部源的时间信号基于国际原子时或通用协调时间 (UTC)。
- 确认指定的中央时间服务器相互之间对等以保持时间精确，且其他内部服务器仅从中央时间服务器接收时间。
- 审核系统配置和时间同步设置，以确认对时间数据的访问仅限于具有访问时间数据这一业务需求的人员。
- 审核系统配置和时间同步设置及流程，以确认对关键系统上时间设置的更改得到记录、监控和审核。
- 确认时间服务器接受来自行业认可的特定外部源的时间更新（这有助于防止个人恶意更改时钟）。您可以选择接收这些使用对称密钥加密的更新，也可以创建访问控制列表以指定将更新时间的客户端计算机的 IP 地址（这可防止未经授权而使用内部时间服务器）。

验证自定义基础设施的安全性是在云中管理安全的一个必不可少的组成部分。

构建威胁防护层

许多组织认为分层安全是保护网络基础设施的最佳实践。在云中，您可以借助 Amazon VPC、位于虚拟机管理程序层处的隐含防火墙规则以及网络访问控制列表、安全组、基于主机的防火墙和 IDS/IPS 系统的组合来创建网络安全分层解决方案。

虽然安全组、NACL 和基于主机的防火墙能够满足许多客户的需求，但如果您需要寻找深入的防御措施，则应内联部署网络级的安全控制设备，以拦截并分析流量，再将之转发到其最终目的地，如应用程序服务器。

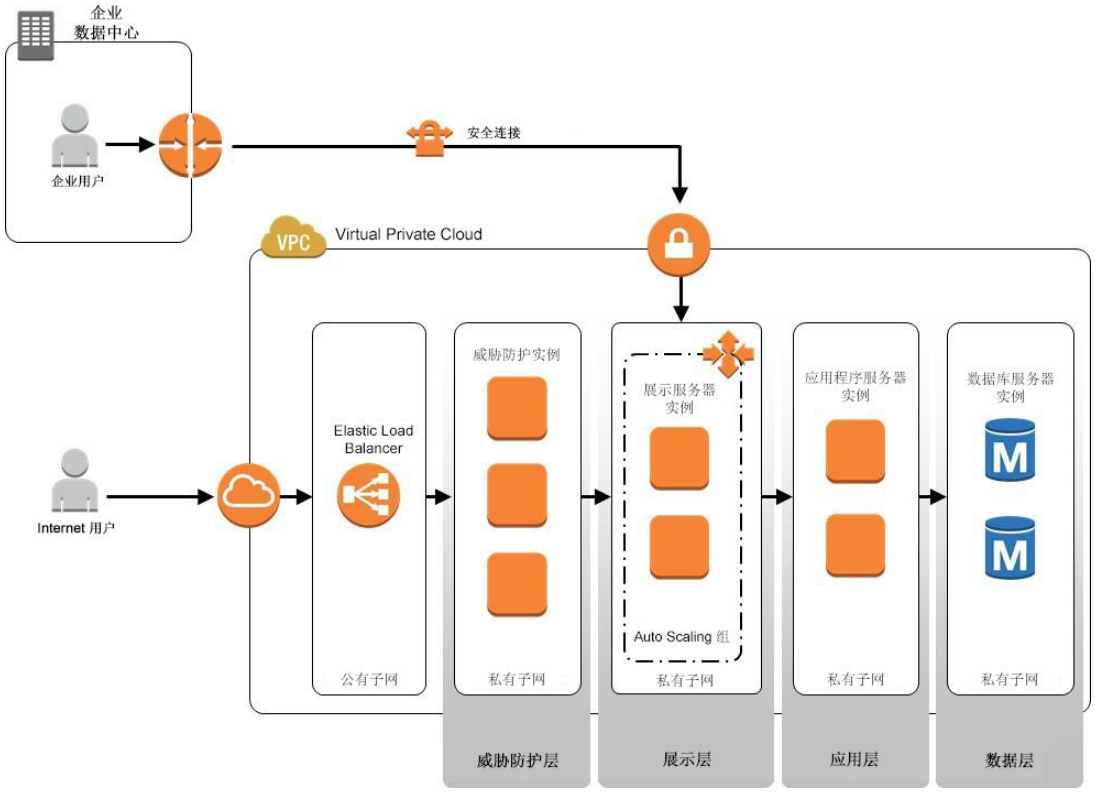

图 6：云中的分层式网络防御

内联威胁防护技术的示例包括：

- 安装在 Amazon EC2 实例上的第三方防火墙设备（也称作软刀片）。
- 统一威胁管理 (UTM) 网关
- 入侵防御系统

- 数据丢失管理网关
- 异常检测网关
- 高级持续性威胁检测网关

Amazon VPC 基础设施中的以下重要功能支持部署威胁防护层技术：

- **支持负载均衡器的多个层级：**当您使用威胁防护网关保护 Web 服务器、应用程序服务器或其他重要服务器的集群时，可扩展性是一个关键问题。AWS 参考架构强调部署内、外部负载均衡器，以实现威胁管理、内部服务器负载分配及高可用性。您可以利用 Elastic Load Balancing 或自定义的负载均衡器实例实现自己的多层设计。您必须在负载均衡器级别管理会话持久性，以实现有状态的网关部署。
- **支持多 IP 地址：**使用威胁防护网关保护包含多个实例（如 Web 服务器、电子邮件服务器、应用程序服务器等）的表示层时，多个此类实例必须使用多对一关系的安全网关。AWS 为单一网络接口提供了多 IP 地址的支持。
- **支持多个弹性网络接口 (ENI)：**威胁防护网关必须为双穴防范网关，且在许多情况下必须有多个接口（具体视网络的复杂性而定）。借助 ENI 的概念，AWS 支持多种不同实例类型上的多种网络接口，这使得它能够部署多区域安全功能。

延迟、复杂性等架构限制有时会导致无法实施内联威胁管理层，在这种情况下，您可以选择采用以下替代选项之一。

- **分布式威胁防护解决方案：**这种方法将在云中的各个实例上安装威胁防护代理。中央威胁管理服务器与所有基于主机的威胁管理代理通信，以实现日志收集、分析、关联和主动威胁响应的目的。
- **覆盖网络威胁防护解决方案：**利用 GRE 隧道、vtun 接口等技术在您的 Amazon VPC 上构建覆盖网络，或通过将另一个 ENI 上的流量转发到集中式网络流量分析和入侵检测系统来提供主动或被动的威胁响应。

测试安全性

所有 ISMS 都必须确保对安全控制和策略的有效性进行定期审查。为保证控制机制能够有效防范新的威胁和漏洞，客户需要确保基础设施能够抵御攻击。

验证现有控制机制需要进行测试。AWS 客户应采取一系列的测试方法：

- **外部漏洞评估：**由不了解或完全不清楚该基础设施及其组件的第三方评估系统漏洞；
- **外部渗透测试：**由不了解或完全不清楚该系统的第三方以受控的方式主动尝试攻破系统。
- **对应用程序和平台执行内部灰盒/白盒审核：**由了解或精通该系统的测试人员验证已就位的控制机制的有效性，或评估应用程序和平台是否存在已知漏洞。

AWS 的可接受使用策略概述了 AWS 云中允许和禁止的行为，并且定义了安全违例和网络滥用行为。AWS 支持在云中进行入站和出站渗透测试，但您必须请求许可才能执行渗透测试。有关更多信息，请参阅 Amazon Web Services 可接受使用策略 (http://aws.amazon.com/aup/)。

要请求对您的资源执行渗透测试，请填写并提交“AWS 漏洞渗透测试申请表”。您必须使用与需要进行测试的实例相关的凭证登录 AWS 管理控制台，否则表格将无法正确预先填入。对于第三方渗透测试，您必须自行填写表格，然后在获得 AWS 的批准后再通知第三方。

表格包含有关要测试的实例的信息、测试的预计开始和结束时间及测试时长，还要求您阅读并同意针对渗透测试及相应测试工具的使用的条款与条件。AWS 策略不允许测试 m1.small 或 t1.micro 实例类型。提交表格后，您会在一个工作日内收到回应，确认我们已收到您的请求。

如果您需要更多的时间进行其他测试，可以回复授权电子邮件，要求延长测试期。每个请求都需要单独的审批流程。

管理指标和改进

测量控制机制的有效性是每个 ISMS 不可分割的一部分。指标可让您了解控制机制保护环境的能力。风险管理往往取决于定性和定量指标。表 22 概括了测量和改进的最佳实践：

最佳实践	改进
监控和审核规程及其他控制机制	• 及时检测处理结果中的错误 • 及时发现失败和成功的安全违规及事故 • 使管理层能够确定委托给人员或通过信息技术实施的安全活动能否达到预期效果 • 利用指标帮助检测安全事件，从而防止安全事故 • 确定为解决安全违例而采取的措施是否有效
定期审查 ISMS 的有效性	• 考虑安全审计、事故和有效性测量的结果，以及有关各方的建议和反馈 • 确保 ISMS 符合政策和目标 • 审核安全控制机制
确保控制机制的有效性	• 确认安全要求已得到满足
按计划的时间间隔进行风险评估审查	• 审核残余风险及确定的风险可接受水平，同时考虑： • 组织、技术、业务目标和流程、已识别威胁的变化 • 已实施的控制机制的有效性 • 外部事件，如：法律或监管环境的变化、合同义务的变更、社会环境的转变
内部 ISMS 审计	• 由组织自身或其代表执行第一方审计（内部审计），以供内部使用。
定期管理评审	• 确保范围保持充裕 • 识别 ISMS 流程中的改进之处
更新安全计划	• 考虑监控和审查活动的结果 • 记录可能影响 ISMS 有效性或性能的行为和事件

表 22：测量和改进指标

缓解和防范 DoS 及 DDoS 攻击

运行 Internet 应用程序的组织认识到了由竞争对手、社会活动家或个人实施的拒绝服务 (DoS) 或分布式拒绝服务 (DDoS) 攻击带来的风险。风险状况取决于业务本质、最近发生的事件、政治局势以及公开的技术。缓解和防范技术与在本地采用的技术相似。

如果您关注 DoS/DDoS 攻击的防范和缓解，则我们强烈建议您注册 AWS 技术支持，以便主动和被动地将 AWS Support 服务加入到您缓解攻击的流程中，或遏制您在 AWS 上的环境中的持续性事故。

某些服务（例如 Amazon S3）使用共享基础设施，这意味着多个 AWS 账户会访问同一组 Amazon S3 基础设施组件中的数据并进行存储。在这种情况下，针对抽象服务发起的 DoS/DDoS 攻击可能会影响多名客户。AWS 会为来自 AWS 的抽象服务提供针对 DoS/DDoS 的缓解和保护控制，尽可能减少您在此类攻击事件中受到的影响。对于此类服务，您不需要提供额外的 DoS/DDoS 保护，但是我们强烈建议您遵守本白皮书中概述的最佳实践。

Amazon EC2 等其他服务使用共享的物理基础设施，但由您负责管理操作系统、平台和客户数据。对于此类服务，我们需要共同努力，以有效缓解和防范 DDoS 攻击。

AWS 采用专有技术来缓解和遏制针对 AWS 平台的 DoS/DDoS 攻击。为避免干扰到合法用户的流量并遵守责任共担模型，AWS 不提供缓解措施，也不主动阻止影响单个 Amazon EC2 实例的网络流量：只有您自己才能决定过高的流量是正常、良性的，还是遭受到了 DoS/DDoS 攻击。

虽然云中可以用于缓解 DoS/DDoS 攻击的方法有很多，但我们强烈建议您建立安全和性能基准，捕获正常情况下的系统参数，并尽可能地考虑到适用于您的业务的每日、每周、每年或其他模式。某些 DoS/DDoS 攻击防范技术（如统计和行为模型）可以与给定的正常操作基准模式比较并检测异常。例如，某个客户预计其网站在每天的特定时间通常会有 2000 个并发会话，则一旦当前并发会话数超过该值的两倍 (4000)，就可通过 Amazon CloudWatch 和 Amazon SNS 触发警报。

在云中构建安全堡垒时，可以考虑采用本地部署使用的组件。

表 23 概述了在云中缓解和防范 DoS/DDoS 攻击的常用方法。

方法	描述	防范 DoS/DDoS 攻击
防火墙：安全组、网络访问控制列表和基于主机的防火墙	传统的防火墙技术可限制潜在攻击者的攻击面，并拒绝进出攻击目标来源的流量。	• 管理允许的目标服务器和服务（IP 地址和 TCP/UDP 端口）的列表 • 管理允许的流量协议源的列表 • 显式暂时或永久拒绝来自特定 IP 地址的访问 • 管理允许的协议
Web 应用程序防火墙 (WAF)	Web 应用程序防火墙可提供针对 Web 流量的深度数据包检查。	• 特定于平台和应用程序的攻击 • 协议健全性攻击 • 未经授权的用户访问
基于主机或内联 IDS/IPS 系统	IDS/IPS 系统可以使用基于统计/行为或签名的算法来检测和遏制网络攻击及木马程序。	• 所有类型的攻击
流量整形/速率限制	通常，DoS/DDoS 攻击会耗尽网络和系统资源。限速是一项保护稀缺资源免遭过度消耗的良好技术。	• ICMP 泛洪 • 应用程序请求泛洪
初期会话限制	TCP SYN 泛洪攻击可按简单或分布形式发起。在任意一种情况下，如果您的系统存在基准数据，您就能够检测到半开（初期） TCP 会话数显著偏离常态，并丢弃特定来源的任何后续 TCP SYN 数据包。	• TCP SYN 泛洪

表 23：缓解和防御 DoS/DDoS 攻击的方法

除了传统的 DoS/DDoS 攻击缓解和防护方法，AWS 云还提供基于其弹性的功能。DoS/DDoS 攻击企图耗尽有限的计算、内存、磁盘或网络资源，这往往对本地基础设施有效。但是，根据定义，AWS 云具有弹性，在需要时，可以补充新的资源。例如，您可能受到来自僵尸网络的 DDoS 攻击（每秒产生数十万的请求，且这些请求与合法用户对您的 Web 服务器发起的请求混杂在一起而无法区分）。在使用传统的遏制技术时，您将开始拒绝特定来源的流量（通常是整个地理区域 — 假定该区域只有攻击者，没有有效的客户）。但这些假设和行动会导致拒绝为您自己的客户提供服务。

在云中，您可以选择吸收此类攻击。借助 Elastic Load Balancing、Auto Scaling 之类的 AWS 技术，您可以配置 Web 服务器在受到攻击（基于负载）时扩展，并在攻击停止后复原。即使遭受严重的攻击，Web 服务器也能通过利用云的弹性进行扩展，以执行和提供最佳的用户体验。吸收攻击方案会使您产生额外的 AWS 服务费用；但维持这样的攻击对攻击者而言是很大的财务负担，因此，攻击者不可能承受得住持久的攻击吸收。

此外，您还可以使用 Amazon CloudFront 吸收 DoS/DDoS 泛洪攻击。AWS WAF 与 AWS CloudFront 集成，可帮助保护 Web 应用程序免遭常见 Web 漏洞的攻击，这些漏洞会影响应用程序可用性、降低安全性或占用过多资源。试图攻击 CloudFront 背后内容的潜在攻击者很可能会向 CloudFront 边缘站点发送大多数或所有请求，在这些位置，AWS 基础设施会吸收多余的请求，而对后端的客户 Web 服务器基本不产生任何影响。再说明一下，吸收攻击会导致额外的 AWS 服务费用，但您应将此费用与攻击者维持攻击所需的成本进行比较。

为有效地缓解、遏制和全面管理您可能遭遇的 DoS/DDoS 攻击，您应构建分层防御模型（见本文其他地方的说明）。

管理安全监控、警报、审计跟踪和事故响应

责任共担模型需要您在操作系统及更高的层级监控和管理您的环境。您可能已在本地或其他环境中这样做了，因此，您可以调整现有的流程、工具和方法，使之可在云中使用。

有关安全监控的详细指南，请参阅 ENISA 采购安全白皮书。该白皮书概述在云中持续开展安全监控的概念（请参阅参考文献与延伸阅读）。

安全监控从回答以下问题开始：

- 我们应测量哪些参数？
- 我们应如何测量它们？
- 这些参数的阈值是什么？
- 上报流程的工作原理是什么？
- 数据保存在何处？

也许您必须回答的最重要的问题是“我需要记录些什么？”我们建议您为记录和分析配置以下几个方面：

- 由具有根权限或管理权限的任何个人进行的操作
- 对所有审计跟踪的访问
- 无效的逻辑访问尝试
- 标识与身份验证机制的使用
- 审计日志的初始化
- 系统级别对象的创建与删除

设计日志文件时，请牢记表 24 中的注意事项：

领域	注意事项
日志收集	记录如何收集日志文件。通常，由操作系统、应用程序或第三方/中间件代理收集日志文件信息。
日志传输	如果日志文件是集中式的，则以安全、可靠、及时的方式将它们传输到中心位置。
日志存储	集中来自多个实例的日志文件，以简化保留策略及分析和关联操作。
日志分类	以适合分析的格式显示不同类别的日志文件。
日志分析/关联	日志文件可提供安全情报（当您分析日志并关联其中的事件之后）。您可以实时或按预定的时间间隔分析日志。
日志保护/安全	日志文件非常敏感。请通过网络控制、身份和访问管理、加密、数据完整性验证和防篡改时间戳等手段保护它们。

表 24：日志文件注意事项

您可能有多种安全日志来源。防火墙、IDP、DLP、AV 系统、操作系统、平台、应用程序等各种网络组件都会生成日志文件。许多日志与安全相关，它们需要成为日志文件策略的一部分。与安全无关的其他日志最好从策略中排除。日志应包括所有用户活动、异常和安全事件，您应将它们保留预定的时间，以供日后调查之用。

要确定需要包含哪些日志文件，请回答以下问题：

- 云系统的用户是谁？他们如何注册？如何进行身份验证？如何获得访问资源的授权？

- 哪些应用程序需要访问云系统？它们如何获得凭证？如何进行身份验证？如何获得此类访问的授权？
- 哪些用户具有访问 AWS 基础设施、操作系统和应用程序的特权（管理级别的访问权限）？他们如何进行身份验证？如何获得此类访问的授权？

许多服务提供了内置的访问控制审计跟踪（例如，Amazon S3 和 EMR 都提供了这样的日志），但在某些情况下，您的日志记录业务需求可能高于本地服务日志可用的内容。这种情况下，可以考虑使用权限提升网关来管理访问控制日志和授权。

使用权限提升网关时，您可通过单一（集群）网关将针对系统的所有访问集中到一起。所有请求均由作为基础设施受信中介的代理系统执行，而不是直接调用 AWS 基础设施、您的操作系统或应用程序。通常，此类系统需要提供或执行以下功能：

- **自动化密码管理**（用于特权访问）：特权访问控制系统可根据自动使用 Microsoft Active Directory、UNIX、LDAP、MYSQL 等内置连接器的给定策略轮换密码和凭证。
- **定期运行最小特权检查**，使用 AWS IAM 用户访问顾问和 AWS IAM 用户上次使用的访问密钥
- **用户身份验证**（前端）和委派访问来自 AWS 的服务（后端）：通常为向所有用户提供单一登录的网站。基于用户的授权配置文件为用户分配访问权限。一种常见的方法是为该网站使用基于令牌的身份验证并获取用户配置文件中允许的对其他系统的点击式访问。
- 存储所有重要活动的**防篡改审计跟踪**。
- **共享账户的不同登录凭证**：有时，多个用户需要共享相同的密码。通过特权上报网关，可以进行远程访问而不泄露共享账户。
- 只允许对目标系统的访问，从而**限制跳点或远程桌面跳跃**。
- 可在会话期间使用的**管理命令**。对于 SSH 或设备管理或 AWS CLI 之类的互动会话，此类解决方案可通过限制可用命令和操作的范围来实施策略。
- **为基于终端和 GUI 的会话提供审计跟踪**，以用于合规性和安全相关目的。
- **记录一切内容**并根据策略的给定阈值报警。

使用变更管理日志

通过管理安全日志，您还能够跟踪变更。这些可能包括计划变更，计划变更可能是组织变更控制流程（有时也称作 MACD — 移动/添加/更改/删除）、临时变更或意外变更（如事件）的一部分。变更可能出现在系统的基础设施方面，也可能涉及其他类别，如代码存储库中的变更、黄金级映像/应用程序清单变更、流程和策略变更或文档变更。作为一项最佳实践，我们建议为所有上述变更类别采用防篡改日志存储库。关联和互连变更管理及日志管理系统。

您需要一位拥有特权的专门用户来删除或修改变更日志；对于大多数系统、设备和应用程序，变更日志应是防篡改的，普通用户不应具有管理日志的权限。普通用户应无法擦除变更日志中的证据。有时，AWS 客户会对日志使用文件完整性监控或变更检测软件，以确保更改现有日志数据会导致生成警报，而添加新条目不会生成警报。

至少每天审核一次系统组件的所有日志。日志审核必须包括执行安全功能的服务器，例如，入侵检测系统 (IDS) 和身份验证服务器、授权服务器和记账协议 (AAA) 服务器（例如，RADIUS）。为方便进行这一流程，您可以使用日志获取、分析和警报工具。

管理重要事务的日志

对于关键应用程序，所有“添加”、“更改”/“修改”和“删除”活动或事务都必须生成日志条目。每个日志条目应该包含以下信息：

- 用户标识信息
- 事件类型
- 日期和时间戳
- 成功或失败指示
- 事件起源
- 受影响数据、系统组件或资源的标识或名称

保护日志信息

日志记录设备和日志信息必须受到保护，避免篡改和未经授权的访问。管理员和操作员日志通常是擦除活动跟踪的目标。

保护日志信息的常见控制机制包括：

- 验证审计跟踪是否已针对系统组件启用并处于活动状态
- 确保仅具有任务相关需求的人员才能查看审计跟踪文件
- 确认当前审计跟踪文件是否通过访问控制机制、物理隔离和/或网络隔离等手段受到保护，不会遭到未经授权的修改
- 确保将当前审计跟踪文件及时备份到集中日志服务器或不易改动的媒介
- 确认面向外部的技术（例如，无线、防火墙、DNS、邮件）的日志已转移给或复制到安全的集中式内部日志服务器或介质
- 通过检查系统设置和监控的文件以及来自监控活动的结果，对日志使用文件完整性监控或更改检测软件
- 获取并检查安全策略和程序，以确认其包含至少每日审核安全日志的步骤并且需要跟踪异常
- 验证是否对所有系统组件执行定期日志审查
- 确保安全策略和程序包含审计日志保留策略并需要将审计日志保留一段时间（由业务和合规性要求定义）

日志记录故障

除监控 MACD 事件外，还需要监控软件或组件故障。故障可能是由硬件或软件故障所致，它们可能会影响到服务和数据的可用性，但可能与安全事件无关。或者，服务故障可能是故意的恶意活动所致，例如，拒绝服务攻击。在任何情况下，故障都应生成警报，之后，您应运用事件分析和关联技术确定故障的原因，以及是否应该触发安全响应。

结论

对于现代企业，AWS 云平台具备大量重要优势，如灵活性、弹性、公用事业账单，并且可缩短产品上市时间。它提供一系列可用于管理 AWS 中资产和数据安全的安全服务和功能。虽然 AWS 围绕基础设施或平台服务提供了优良的服务管理层，但企业仍负责保护其在云中的数据的机密性、完整性和可用性，并负责满足信息保护的特定业务需求。

传统的安全和法规遵从概念在云中仍然适用。我们建议您使用本白皮书中强调的各种最佳实践针对您的组织构建一套安全策略和流程，以便迅速、安全地部署应用程序和数据。

贡献者

- Dob Todorov
- Yinal Ozkan

参考文献与延伸阅读

- Amazon Web Services：安全过程概述 — http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
- Amazon Web Services 风险和合规性白皮书 — http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf
- 利用 Amazon Web Services 进行灾难恢复 — http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
- Amazon VPC 网络连接选项 — http://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf
- Active Directory 的联合身份验证示例应用程序使用案例 — http://aws.amazon.com/code/1288653099190193
- 用 Windows ADFS 单一登录到 Amazon EC2 .NET 应用程序 — http://aws.amazon.com/articles/3698?_encoding=UTF8&queryArg=searchQuery&x=20&y=25&fromSearch=1&searchPath=all&searchQuery=identity%20federation
- 通过令牌售卖机对 AWS 移动应用程序用户进行身份验证 — http://aws.amazon.com/articles/4611615499399490?_encoding=UTF8&queryArg=searchQuery&fromSearch=1&searchQuery=Token%20Vending%20machine
- 使用适用于 Java 的 AWS 开发工具包和 Amazon S3 进行客户端数据加密 – http://aws.amazon.com/articles/2850096021478074
- Amazon 公司的 IT 部门将 SharePoint 2010 部署到 Amazon Web Services 云 — http://media.amazonwebservices.com/AWS_Amazon_SharePoint_Deployment.pdf
- Amazon Web Services 可接受使用策略 — http://aws.amazon.com/aup/
- ENISA 采购安全：监控云合约中安全服务级别的指南 — http://www.enisa.europa.eu/activities/application-

security/cloud-computing/procure-secure-a-guide-to- monitoring-of- security-service-levels-in-cloud-contracts

- PCI 数据安全标准 — https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

  ISO/IEC 27001:2005 – http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103

- 针对 AWS 使用的审计安全核对清单 — http://media.amazonwebservices.com/AWS_Auditing_Security_Checklist.pdf