安全性支柱

AWS 良好架构框架

2017 年 5 月

通告

本文档所提供的信息仅供参考，且仅代表截至本文件发布之日时 AWS 的当前产品与实践情况，若有变更恕不另行通知。客户有责任利用自身信息独立评估本文档中的内容以及任何对 AWS 产品或服务的使用方式，任何“原文”内容不作为任何形式的担保、声明、合同承诺、条件或者来自 AWS 及其附属公司或供应商的授权保证。AWS 面向客户所履行之责任或者保障遵循 AWS 协议内容，本文件与此类责任或保障无关，亦不影响 AWS 与客户之间签订的任何协议内容。

目录

摘要

本文档详细介绍良好架构框架中的安全性，旨在帮助客户在 AWS 云环境中的最佳安全设计、交付和维护。

内容简介

在 Amazon Web Services (简称 AWS)，我们充分意识到为客户传递架构设计与运营最佳实践的重要意义，特别是在云端可靠性、安全性、效率以及成本效率等层面的积极作用。作为这项工作中的关键性组成部分，我们建立起 AWS 良好架构框架 [1]（AWS Well-Architected Framework），其将帮助大家立足 AWS 构建系统的同时，明确把握自身决策中的优势与弊端。我们认为，良好架构系统的存在将能够极大提升您的企业实现商业成功的机率。

此套框架基于五大支柱性因素：

- 安全性
- 可靠性
- 性能效率
- 成本优化
- 卓越操作

本份白皮书着眼于安全性支柱，旨在阐述如何将安全性纳入您的解决方案。安全性保障工作在传统内部解决方案当中往往极具挑战性，这是因为您需要面临复杂的流程、脆弱的安全架构以及缺乏有效审计等一系列难题。通过采用本份白皮书中提及的各项实践，您将能够建立起保护数据安全保护、系统访问控制以及攻击自动化响应的安全架构方案。

本份白皮书主要面向各技术类职能角色，具体包括首席技术官（简称 CTO）、架构师、开发人员以及运营团队成员。在阅读本文之后，您将能够了解云架构安全性设计工作中需要遵循的最佳实践及战略思路。本份白皮书并不提供任何具体实施细节或者架构模式，但文末将提供与此类信息相关的扩展资源。

安全性

安全性支柱的核心在于为信息、系统以及资产提供保护的同时，通过风险评估及安全策略交付价值。本份白皮书将立足 AWS 为安全系统的架构设计工作提供深层次最佳实践指导。

设计原则

在云环境当中，大家可以利用多项基本原则帮助自身强化系统安全性：

- **将安全引入一切层面：**相较于立足基础设施边界运行安全方案（例如防火墙），您应将防火墙及其它安全控制机制引入全部资源（例如每套虚拟服务器、负载均衡器以及网络子网）。
- **实际可追溯性：**对您环境当中的一切操作与变更进行记录与审计。
- **执行最低权限原则：**确保授权水平符合每一项与 AWS 资源之间的交互需求，同时直接面向资源实施强逻辑访问控制。
- **专注于保护您的系统：**在 AWS 责任分担模型 [2]的帮助下，您能够专注于保护自己的应用程序、数据以及操作系统，而 AWS 则负责保护基础设施与服务。
- **自动化安全最佳实践：**基于软件的安全机制能够帮助您以更为快速且具备成本效益的方式实现安全扩展。创建并保存安装有补丁并经过安全强化的虚拟服务器镜像，而后自动利用此镜像完成各套新服务器的启动。另外，创建一套完整的可信架构，同时利用版本控制机制通过模板对其进行定义与管理。最后，以自动化方式响应安全事件的发现与解决。

定义

云环境下的安全性主要由以下五个方面组成：

1. 身份与访问管理
2. 检测控制
3. 基础设施保护
4. 数据保护
5. 事件响应

AWS 责任分担模型允许各企业利用云平台实现自身安全性与合规性目标。由于 AWS 保护用于支持各项云服务的物理基础设施，AWS 客户可将注意力集中在利用服务实现具体目标身上。AWS 云亦提供出色的安全数据访问机制以及用于响应安全事件的自动化方案。

身份与访问管理

身份与访问管理属于信息安全规划当中的核心组成部分，负责确保仅经过验证及授权的用户方可以符合预期的方式访问您的资源。举例来说，您可定义各相关主体（包括用户、组、服务与角色对您帐户采取的具体操作）、制定与这些主体相统一的策略，同时实施强大的访问控制管理机制。这些权限管理因素将共同构成业务系统内验证与授权的核心。

在 AWS 上，大家可以利用多种不同方法实现身份与访问管理，以下部分详尽阐述了这些方法的具体使用方式：

- 保护 AWS 凭证
- 细粒度授权

保护 AWS 凭证

对于凭证访问活动的精心管理正是您保护云端资源的基础所在。由于您面向 AWS 作出的每一项交互皆需要进行认证，因此建立适当的凭证管理实践及模式将帮助您充分的管理安全的生命周期，最终确保仅针对您的帐户中最适当的部分采取行动。

当您打开一个 AWS 帐户时，您的初始身份能够访问该帐户内的全部 AWS 服务与资源。您可利用此身份在 AWS 身份与访问管理（简称 IAM）服务当中建立低权限用户或者基于角色的访问机制。然而，此初始帐户（即 root 用户）并不适用于日常任务。这些凭证应谨慎配合多因素身份验证（简称 MFA）加以保护，同时在该初始帐户设置完成后删除一切相关访问密钥。

对于该 root 帐户，您应严格遵循最佳实践，要求仅利用其创建其它初始 IAM 用户及用户组以实现长期身份管理。这些高权限 IAM 用户应接受严格监控与约束，其可利用联合认证（通过 SAML 2.0 或者 Web 身份机制）体系获得现有身份供应方的信任。利用联合认证机制，您将能够有效降低 IAM 当中的用户创建需求，同时继续利用现有身份、凭证以及基于角色的访问机制。

对于全部 IAM 用户，您应采用适当的策略以强制执行强验证。您可以在 AWS 帐户当中设置一套密码策略，对各 IAM 用户使用的密码作出最小长度与复杂性要求。大家也可以通过设置强制性轮询策略要求 IAM 用户定期更改密码内容。对于一切可利用密码访问 AWS 管理控制台的 IAM 用户，您还应要求其使用多因素验证机制。

IAM 用户还可能需要访问直接来自命令行工具（简称 CLI）的命令，或者使用软件开发套件（简称 SDK）。在这类情况下，联合认证机制往往并不实用，因此需要发布访问密钥 ID 与机密密钥，用以代替传统密码机制。这些凭证应受到严格

保护，同时尽可能仅发布临时凭证。需要特别注意的是，避免立足不正确的安全位置进行密码存储及访问，或者无意中将此类凭证提交至源代码存储库。

对于各类不适用联合认证机制的用例，例如大量服务到服务验证场景，您可以利用面向 Amazon EC2 实例的 IAM 实例配置文件及/或 AWS 安全令牌服务（AWS Security Token Service，简称 STS）以生成并管理各类临时性凭证，进而利用其在软件当中实现 AWS API 验证。

关键性 AWS 服务

AWS 服务凭证保护层面的关键为 AWS 身份与访问管理（简称 IAM）。此项服务允许您管理各类凭证并为其应用管理策略。以下服务与功能亦在此层面发挥有重要作用：

- **AWS 安全令牌服务**允许您请求临时性、权限受限的凭证，用以通过其它 AWS API 的验证机制。
- **向 EC2 实例的 IAM 实例**配置文件 允许大家利用 Amazon 弹性计算云（简称 EC2）元数据服务与临时性托管凭证访问其它 AWS API。

资源

请参阅以下资源以了解更多与 AWS 凭证保护 AWS 最佳实践相关的细节信息。

视频

- AWS re:Invent 2015 SEC202 IAM 最佳实践概述 [3]
- AWS re:Invent 2015 SEC307 AWS IAM 联动选项纵览：从角色到 SAML 再到定制化身份中间人 [4]

说明文档

- Root 帐户凭证对 IAM 用户凭证 [5]
- 帐户 Root 用户 [6]
- 为 IAM 用户设置一套帐户密码策略
- 为 IAM 用户管理访问密钥 [7]
- 使用实例配置文件 [8]
- 临时性安全凭证 [9]

细粒度授权

建立最低权限原则能够确保各经过验证的身份仅具备执行特定任务所必需的最小权限集，同时在可用性与效率之间寻求最佳平衡点。采取这项原则能够有效控制有效凭证遭到滥用所引发的**影响半径**或潜在危害，确保您切实拆分监督责任并显著简化资源使用权限的审计难度。

企业应当为用户及应用程序定义与 AWS 交互相关的角色与责任，同时采取细粒度授权机制以保障这些角色。

细粒度授权可在 AWS 当中通过使用 IAM 角色及策略的方式实现。角色是由用户或者其它 AWS 服务所设立的另一 IAM“主体”，其将被赋予临时性凭证并配合受限权限集。IAM 策略则属于正式记录在案的单一或者多项权限条件。策略可被附加至用户、组以及角色当中，借以建立起极具鲁棒性的访问管理框架。

关键性 AWS 服务

细粒度授权支持层面的关键 AWS 服务为 AWS 身份与访问管理，其提供极为灵活的策略语言以批准或拒绝各项操作、为这些操作设定条件并将不同操作限制于具体主体或者资源范畴之内。

资源

请参阅以下资源以了解更多与细粒度授权 AWS 最佳实践相关的细节信息。

说明文档

- 策略使用指南 [10]
- 将权限分配至管理员：IAM 用户、组以及凭证 [11]
- 受控策略与内联策略 [12]
- 策略使用指南 [13]

检测控制

您可以利用检测控制机制识别潜在的安全事件。此类控制手段属于治理框架当中的重要组成部分，可用于支持质量流程、法律或者合规性义务以及威胁识别与响应行动。检测控制分为多种不同类型，例如用于进行资产清单及其详尽属性整理以促进高效决策（与生命周期控制），进而帮助建立运营基准等等。或者，您也可以采取内部审计机制——即对与信息系统相关之控制方案加以检查，从而确保各项实践满足策略与要求，这部分明确定义的条件将成为进一步设置自动化警报通知机制的基础。这些控制手段皆属于极为重要的反应性因素，能够帮助企业有效识别并理解异常活动的影响范围。

在 AWS 当中，您可以考虑使用多种不同方案以实现检测控制。以下部分描述了这些方案的具体使用方法：

- 日志收集与分析
- 将审计控制与通知同工作流进行整合

日志收集与分析

在传统数据中心架构当中，日志的汇总与分析工作通常要求在服务器上安装代理、精心配置网络设备以将日志消息定向至收集点，同时将应用程序日志转发至搜索及规则引擎。相比之下，云环境凭借着两项能力极大简化了此类汇总工作。

首先，由于资产及实例可以编程化方式描述且无需依赖于代理运行状态，因此资产管理工作的难度将大大降低。举例来说，相较于以手动方式更新资产数据库并利用实际安装库进行记录，大家可以在云环境中通过数次 API 调用轻松完成资产元数据收集。这部分数据在准确度与及时性方面远超 CMDB 当中的发现扫描与人工输入方式，同时亦优于使用可能因自身问题导致报告停滞的代理方案。

第二，您可以利用原生 API 驱动型服务收集、过滤并分析日志内容，且无需对日志记录后端亲自加以维护及规模控制。您可以直接指向存储桶内对象存储中的日志，或者将各事件定向至流式端点，这意味着您可在显著降低容量规划所耗费的时间，并充分确保后端记录及搜索架构的可用性。

在 AWS 当中，最佳实践要求利用 AWS CloudTrail 及其它特定服务日志记录机制以收集全局 API 活动并对数据进行集中化存储与分析。您可以将 AWS CloudTrail 日志记录定向至 Amazon CloudWatch 日志内或者其它端点处，从而以统一化格式跨越计算、存储及应用程序进行事件捕捉。

对于基于服务器以及应用程序等并非源自服务本身的日志记录，您仍然需要使用传统方法加以处理——包括利用代理进行事件收集与路由（包括系统日志、第三方解决方案乃至本地操作系统日志等），但 AWS 同样提供更优解决方案。利用 AWS CloudFormation、AWS OpsWorks 或者 Amazon 弹性计算云（简称 EC2）用户数据等服务及功能，系统管理员能够确保各实例当中始终切实安装有必要代理。

与收集并汇总日志同样重要的是：您需要从现代、高复杂度架构所生成的大规模日志及事件数据当中提取有价值信息。架构师应当考虑采取端到端检测控制机制。您不应单纯生成并存储日志，而应为信息安全功能提供强大的分析与检索能力，从而真正获取安全相关活动中的分析结论。AWS 提供的各类面向大数据工作负载的解决方案非常适合执行安全数据的解析与分析任务。

关键性 AWS 服务

活动信息收集层面的关键 AWS 服务有 AWS CloudTrail，其提供丰富且详尽的 AWS 帐户内 API 调用信息。以下服务与功能亦在此层面发挥有重要作用：

- **AWS Config** 为您提供一套 AWS 资源、配置历史以及配置变更通知清单，可用于支持安全及治理保障工作。
- **Amazon Elasticsearch Service** 负责对开源搜索及分析引擎 Elasticsearch 集群进行管理与规模控制。您可以利用这套解决方案实现对安全数据的索引、搜索与渲染。
- **AWS CloudWatch** 允许您以集中化方式将日志信息纳入数据流，并同 VPC Flow 日志以及 AWS CLoudTrail 等功能及服务进行原生整合。CloudWatch 日志亦可通过扩展实现日志提取，且您无需为此管理任何传统基础设施。
- **Amazon EMR** 允许您编写各类应用程序以实现日志信息的规模化解析与分析，而且完全不需要为此管理 Hadoop 或者其它任何数据分析集群。
- **Amazon 简单存储服务(简称 S3) 与 Amazon Glacier** 可用于以集中化方式实现日志数据的存储与长期归档。

将审计控制与通知同工作流进行整合

安全运营团队依靠日志收集与搜索工具以发现各类值得关注的潜在事件，具体可能包括未经授权的活动或者计划外变更。然而，单纯以手动方式分析并处理收集到的数据并不足以提供能够与现代、高复杂度基础设施相匹配的信息。具体而言，单凭分析与报告机制无法及时为工作事件分配正确的资源。要建立成熟的安全体系，相关最佳实践要求运营团队深入整合安全事件及调查结果，并将其引入通知与工作流系统——包括申请系统、bug/问题系统或者其它安全信息与事件管理（简称 SIEM）系统。这意味着工作流将摆脱电子邮件以及静态报告的束缚，允许您随时对事件或发现进行路由、升级以及管理。目前，相当一部分 DevOps 组织开始将安全警报机制集成至其沟通/互联网中继沟通（简称 IRC）工具或者其它协作及开发者生产力平台当中。

相关最佳实践不仅要求从用户活动或者网络事件生成的日志信息内提取安全事件线索，同时亦需要着眼于基础设施本身中出现的变更。这种检测变更、衡量变更是否适当并随后将相关信息路由至正确修理工作流当中的能力，对于安全架构的维护与验证无疑至关重要。

在 AWS 当中，大家可以利用 Amazon CloudWatch 将值得关注的事件及可能反映不必要变更的信息路由至理想的工作流当中。这项服务提供一套可扩展规则引擎，用于向中间人描述原生 AWS 事件格式（例如 AWS CloudTrail 事件）以及您自主建立的定制化事件。您制定的规则可用于解析事件、在必要时进行事件传递，而后将其路由至 AWS Lambda 函数、Amazon 简单通知服务（Amazon Simple Notification Service ， 简称 SNS）通知或者其它目标处。

您可以利用 AWS Config 规则变更检测并将相关信息路由至正确的工作流处。AWS Config 会检测范围内服务的变更情况并生成可供 AWS Config 规则加以解析并据此执行回滚的事件，实施合规性策略，并最终将信息转发至变更管理平台及运营申请系统等系统处。

对于生产环境而言，减少安全配置错误数量可谓至关重要，这意味着您需要在构建流程当中尽可能增加质量控制因素并削减执行缺陷。现代持续集成与持续部署（简称 CI/CD）管道应在设计当中尽可能对安全问题加以测试。利用 Amazon Inspector，您能够面向各类已知安全漏洞及缺陷（CVE）执行配置评估、根据安全基准审查您的实例并以全面自动化方式实现缺陷通知。Amazon Inspector 可运行在生产实例当中或者 build 管道之内，且能够在发现问题时向开发人员及工程师发送通知。您可通过编程化方式访问发现结果并将其定向至库存及 bug 追踪系统处。

关键性 AWS 服务

面向通知与工作流系统的审计控制集成层面的关键 AWS 服务为 Amazon CloudWatch 事件，其允许您将事件路由至一套强大的规则引擎当中。各规则随后将对输入事件进行检查，解析输入值并据此将各事件路由至任意数量目标处——包括电子邮件或移动设备、申请队列以及问题管理系统等。以下服务与功能亦在此层面中发挥有重要作用：

- **AWS Config 规则**允许您创建能够自动检查由 AWS Config 记录之 AWS 资源配置条目的相关规则。
- 必须启用 **Amazon CloudWatch** 以快速收集事件，并利用 CloudWatch 事件实现信息路由。
- **Amazon CloudWatch API 与 AWS SDK** 可用于在您的应用程序当中创建定制化事件，并将其注入至 CloudWatch 事件内以实现基于规则的处理与路由。

- **Amazon Inspector** 提供一种编程化方式，旨在发现存在于操作系统及应用程序当中的各类安全缺陷以及配置错误。由于您可利用 API 调用方式访问评估流程以及评估结果，因此亦可轻松将相关结果纳入工作流以及通知系统当中。DevOps 团队能够将 Amazon Inspector 添加至其 CI/CD 管道并借此发现各类原本即存在或者新近出现的问题。

资源

请参阅以下资源以了解更多与将审计控制与通知同工作流进行整合 AWS 最佳实践相关的细节信息。

视频

- Amazon CloudWatch 事件 [14]
- 要点：AWS Config 规则介绍 [15]
- Amazon Inspector 介绍 [16]

说明文档

- Amazon CloudWatch 事件 [17]
- AWS Config 规则 [18]
- AWS Config 规则库（GitHub 上的开源资源） [19]
- Amazon Inspector [20]

基础设施保护

基础设施保护工作当中包含多种控制方法，例如纵深防御以及多因素验证，这些已经成为实现最佳实践并满足行业或监管义务的必要前提。对于这些方法的运用亦属于立足云端或者内部环境实现成功持续运营的关键性条件。

基础设施保护属于信息安全计划当中的一大重要组成部分。其能够确保系统之内的系统与服务受到严格保护，从而避免由计划外及未授权访问与潜在安全缺陷的影响。举例来说，您可定义信任边界（例如网络边界及数据包过滤机制）、系统安全配置与维护（例如强化与补丁安装）、操作系统验证与授权（例如用户、密钥以及访问层级）以及其它适用的策略贯彻点（例如 Web 应用程序防火墙以及/或者 API 网关）。

在 AWS 当中，您可以利用多种不同方案实现基础设施保护。以下部分描述了这些方案的具体使用方式：

- 保护网络与主机级边界
- 系统安全配置与维护
- 实施服务级保护

保护网络与主机级边界

对于网络拓扑结构以及设计方案等环境内资源隔离与边界划分实现手段的精心管理是安全保障的重中之重。由于您环境当中的资源会直接继承底层网络的安全属性，因此大家必须建立起适当的网络设计方案，旨在确保各类工作负载仅拥有运行所必需的网络路径与路由机制。您可以建立多套多层保护机制以实现控制冗余能力，并借此缓解单层配置错误可能引发的不当访问活动。

在定义网络拓扑结构时，请考虑到系统当有哪些组件需要进行公开——例如面向客户的负载均衡器。另外，当您进行网络连接设计时，请考虑是否需要在数据中心与 AWS 之间经由私有网络建立连接。为您的虚拟私有云（简称 VPC）、子网、路由表、网络访问列表（简称 NACL）、网关以及安全组采取适当的配置方案，从而切实实现网络路由以及主机级保护能力。

利用 Amazon 虚拟私有云服务创建的 VPC 允许您配合指定的 IP 地址范围在同一 AWS 服务区内定义网络拓扑结构。在 VPC 当中，您可以立足当前可用区创建多个子网。每套子网皆拥有与之匹配的路由表，用于定义该子网之内用于管理流量路径的具体规则。您亦可设定一套指向 VPC 附加互联网网关的路由方案，用于定义公开可路由子网。未接入互联网网关的路由体系能够防止各实例受到来自互联网的直接访问。再有，子网内亦可添加网络访问列表（无状态防火墙）。您可配置一套 ACL 以缩小所允许流量的范围。举例来说，您可在子网托管数据库内仅允许接收来自数据库引擎端口的访问。

当在 VPC 当中启动一台主机时，其将拥有自己的安全组（有状态防火墙）。该防火墙独立于操作系统层之外，且可用于为各获准流量定义具体规则。您也可以在各安全组之间定义彼此关系。举例来说，某一数据库层安全内的各实例仅可接受来自同一应用层中实例的流量。

在采用 VPC 设计方案时，请认真考量为 VPC 选择 IP 地址范围时需要遵循的指导原则。尽量使用与其它 VPC 或者数据中心不存在交集的 IP 地址。而在设计 NACL 规则时，需要注意其属于一套无状态防火墙，因此必须根据您的实际需要同时定义出站与入站规则。

关键性 AWS 服务

网络与主机级边界保护层面的关键 AWS 服务为 Amazon 虚拟私有云（简称 VPC）。这项服务允许您在 AWS 之上创建自己的虚拟私有网络。以下服务与功能亦在此层面中发挥有重要作用：

- **Amazon VPC 安全组：**提供一套每主机有状态防火墙，允许您指定流量规则并定义其与其它安全组间的关系。
- **AWS Direct Connect：**允许您在自有数据中心与 VPC 之间建立起专用直通连接。

资源

请参阅以下资源以了解更多与网络及主机级边界保护 AWS 最佳实践相关的细节信息。

视频

- Amazon VPC 深度剖析 [21]

说明文档

- Amazon VPC 说明文档 [22]
- Amazon VPC 网络访问控制列表 [23]
- 为您的 VPC 建立安全组 [24]
- 面向 VPC 的网络 ACL 规则推荐 [25]

系统安全配置与维护

对于环境内运行系统的安全配置进行管理是强大、安全且可扩展系统的根本性基础。系统的安全性水平直接体现在利用基于操作系统的防火墙、CVE 与安全漏洞扫描工具、病毒扫描工具以及其它一切能够验证并维护操作系统完整性之工具保障自主控制能力之上。这类控制手段亦为您的深层防御策略建立起额外保障层。

当您定义一套系统安全保护方案时，请考虑到系统所需要的访问级别并采取最低权限原则（例如仅开放通信所必要的商品，借此确保操作系统得到强化且禁用一切不必要的工具及/或许可配置）。您应在操作系统当中采取适当的配置机制，包括强大的授权机制。

您应以自动化方式进行部署并降低操作人员访问数量，从而缩小攻击面。您可利用 EC2 运行命令实现这项目标。另外，您应评估自身基准安全性水平，并在更新

或部署过程当中执行常规安全漏洞评估。Amazon Inspector 等常规安全漏洞及缺陷（CVE）扫描工具可用于实现这项目标，并以集中化方式汇总安全分析与修复意见。您还需要确保您的操作系统及应用程序得到妥善配置与及时更新，包括防火墙设置以及反恶意软件定义。您可利用 EC2 状态管理器定义并维护操作系统配置的一致性。利用 EC2 清单以收集并查询与各实例及所安装软件相关的配置信息。最后，利用 EC2 补丁管理器等自动化补丁安装工具以自动化方式跨越众多实例组实现操作系统与软件补丁 部署。

关键性 AWS 服务

系统保护支持层面的关键 AWS 服务为 Amazon VPC 安全组每实例防火墙。以下服务与功能亦在此层面中发挥有重要作用：

- **Amazon Inspector** 可用于在您的客户操作系统及应用程序中发现安全漏洞或有违最佳实践的状况。
- **EC2 运行命令**提供一种简单的自动化任务管理方法，包括通过远程执行 shell 脚本或 PowerShell 以实现具备细粒度访问控制与可见性要求的命令，旨在安装软件更新或者变更操作系统配置。
- **EC2 状态管理器**能够帮助您定义并维护操作系统配置一致性，具体包括防火墙设置以及反恶意软件定义等。
- **EC2 清单**可帮助您收集并查询与各实例及其中所安装之软件相关的配置及清单信息。
- **EC2 补丁管理器**可帮助您跨越众多实例组以自动化方式选择并部署操作系统及软件补丁。

资源

请参阅以下资源以了解更多与系统安全配置与维护 AWS 最佳实践相关的细节信息。

说明文档

- EC2 系统管理器 [26]
- EC2 运行命令 [27]
- EC2 状态管理器 [28]
- EC2 清单 [29]
- EC2 补丁管理器 [30]

- 利用 Amazon EC2 系统管理器取代堡垒主机 [31]

执行服务层保护

对于服务端点配置安全性的保护是保障端点授权访问以及安全性的根本所在。立足这一安全层级，您需要确保用户与/或自动化系统具备适当访问等级以执行相关任务（且配合最低权限）。

您可以利用 IAM 定义各项策略以保护 AWS 服务端点。IAM 能够帮助您面向服务及操作访问定义各类策略。然而，对于某些特定服务，您亦可定义细粒度控制机制以指定服务内的具体资源。另外，某些资源拥有自己的资源层级策略。举例来说，Amazon S3 拥有存储桶策略，用于定义面向各对象及/或整体存储桶的访问级别; AWS 密钥管理服务（简称 KMS）中的策略则用于定义该密钥管理服务之内的密钥管理员及用户。利用 IAM 以及各资源策略可为资源定义出一套强大的保护模式。

在定义服务层保护方案时，请确保采用最低权限方法并据此设置服务级访问策略。

关键性 AWS 服务

服务层保护的关键 AWS 服务为 AWS 身份与访问管理（简称 IAM），其允许您面向各类 AWS 资源定义具体策略。以下服务与功能亦在这一层面发挥着重要作用：

- **AWS 密钥管理服务(简称 KMS)** 允许您立足个别密钥设置管理策略。
- **Amazon 简单存储服务(简称 S3)** 允许您面向各 Amazon S3 存储桶设置存储桶策略。

资源

请参阅以下资源以了解更多与执行服务级保护 AWS 最佳实践相关的细节信息。

说明文档

- VPC 安全组 [32]
- 在 AWS KMS 当中使用密钥策略 [33]
- 使用存储桶策略与用户策略 [34]
- Amazon Inspector [35]

数据保护

在为任何系统设计架构之前，我们首先应当确定可能影响安全性的各项基础实践。举例来说，**数据保密**提供的保密方法以敏感度为基础，旨在帮助企业立足不同**加密**级别对数据提供保护，确保其不会受到未经授权之访问活动的影响。这些工具与技术非常重要，能够有效支持预防经济损失或者遵循监管义务等目标。

在 AWS 当中，您可考虑利用多种不同方案实现数据保护，以下部分描述了这些方案的具体使用方式：

- 数据分级
- 加密/令牌
- 保护静态数据
- 保护处理状态数据
- 数据备份/复制/恢复

数据分级

数据分级提供一种基于企业内信息敏感性水平进行数据分级的方法。其中包括了解可用数据类型、数据所在位置以及数据的访问级别与保护措施（例如采取加密或者访问控制机制）。通过精心建立并管理数据分级系统以及各层保护要求，您将能够将适合的控制与访问/保护级别与具体数据加以匹配。举例来说，面向公众的内容可供任何人访问，而关键性内容则被加密并以受保护方式进行存储——即需要密钥方可解密。

通过利用资源标签、IAM 策略、AWS KMS 以及 AWS CloudHSM，您能够定义并实现各项数据分级策略。举例来说，如果您拥有多套存放有关键性数据的 Amazon S3 存储桶或者负责处理保密数据的 EC2 实例，则可将其标记为“DataClassification=CRITICAL”。您可通过密钥策略定义这些加密密钥的访问级别，从而确保只有适当服务能够访问到这些敏感内容。

数据分级亦可通过托管在 AWS 之上的第三方以及开源解决方案实现。您也可以利用 IAM 策略为不同资源定义访问级别，或者利用应用级控制为各操作方定义资源访问权限。

在考量数据分级方法时，您需要在实效性与访问性之间寻求平衡点。另外，您还应考虑引入多级访问与微调机制，从而在保障安全性的同时继续保证其在某一层级上可供正常使用。另外，您应始终采取纵深防御策略。举例来说，要求用户通过强授权方可实现应用程序访问，同时保证用户来自受信网络路径且需要解密密钥。

关键性 AWS 服务

AWS 数据分级支持层面的关键功能为资源标记，其允许您为各类资源应用不同的定制化标签。以下服务与功能亦在这一层面中发挥着重要作用：

- **AWS 密钥管理服务(简称 KMS):** 允许您定义加密密钥以及与之对应的访问策略。

资源

请参阅以下资源以了解更多与数据分级 AWS 最佳实践相关的细节信息。

说明文档

- 利用标签标记您的 Amazon EC2 资源 [36]
- 在 AWS KMS 当中使用密钥策略 [37]
- 使用存储桶策略与用户策略 [38]

加密/令牌

加密与令牌属于两项重要但又互不相同的数据保护方案。**令牌化**属于一项流程，允许您定义令牌以表达信息中的某一敏感片段（例如通过令牌表达客户的信用卡号）。令牌内容必须毫无意义。**加密**则是一种基于内容的方法，旨在将内容转换为不可读形式，且无法在不具备密钥的情况下将其解密为普通文本。令牌与加密机制均可用于实现内容保护，您应视具体需求酌情选择。

通过精心定义您的令牌化方案，大家能够为内容提供额外的保护能力，同时确保满足各类合规性要求。举例来说，在处理信用卡的场景下，您可以在系统中利用令牌替代明文信用卡号。您亦可立足加密 Amazon 关系数据库服务（简称 RDS）数据库或者 Amazon DynamoDB 数据库创建查找表以定义自己的令牌化方案，并向您的最终应用程序发布令牌。

通过定义加密方法，您将能够避免受保护内容不会被未授权用户的窥探、亦不会遭到授权用户的无意曝光。AWS 针对加密密钥管理需求提供一项密钥管理服务（AWS KMS），此项服务能够为您的主钥提供持久、安全且具备冗余保障的存储机制。您可以定义自己的密钥别称以及密钥级策略。此项策略将帮助您定义密钥管理员以及密钥用户。举例来说，您可要求仅允许密钥管理系统访问可解密各存储内容的主角。

另外，AWS CloudHSM 服务可帮助您在 AWS 云内使用专用硬件安全模块（HSM）方案，从而满足企业、合同以及合规性中列出的数据安全保障要求。利用 AWS CloudHSM，您将能够有针对性地控制加密密钥以及 HSM 所执行的密码操作。

在定义加密/令牌方案时，请考虑您所定义的数据分级模式以及各类内容所需要的访问级别。另外，请考虑到合规性要求、内容管理需求以及如何严格执行相关方案。再有，请认真考量令牌化与加密机制之间的差异与用例契合度。最后，关注交付至用户处的实际密钥策略以及访问级别。

关键性 AWS 服务

加密支持层面的关键 AWS 服务为 AWS 密钥管理服务（简称 AWS KMS），其提供易于使用、安全且具备冗余机制的密钥管理能力。以下服务与功能亦在这一层面发挥着重要作用：

- **AWS CloudHSM:** 提供一套用于管理密钥的硬件安全模块。
- **Amazon DynamoDB:** 提供一种快速实现 NoSQL 数据库的方式。其可用于为您的令牌存储加密内容。

资源

请参阅以下资源以了解更多与加密/令牌 AWS 最佳实践相关的细节信息。

视频

- AWS 中的加密与密钥管理 [39]

说明文档

- 利用加密机制保护数据 [40]
- AWS 密钥管理服务 [41]
- AWS CloudHSM [42]
- AWS KMS 密码细节白皮书 [43]

保护静态数据

静态数据，是指那些您在任意持续时间内所持续拥有的任何内容，具体包括块存储、对象存储、数据库、归档以及任何其它驻留有数据的存储介质。通过保护您的静态数据，大家可以避免未授权访问，并配合强大的加密密钥防止内容遭遇意外泄露。

多种 AWS 服务皆提供与 AWS 密钥管理服务（简称 KMS）的内置集成能力，允许您通过复选框快速对持久存储内容进行加密。Amazon S3 允许您选择 KMS 以加密所上传的对象内容，Amazon 弹性块存储（简称 EBS）则允许您选择主密钥以加密块存储分卷。Amazon 关系数据库服务（简称 RDS）允许您选择密钥以加密静态下的数据库实例存储内容（包括备份）。

您亦可选择采用自己的静态数据处理方案。举例来说，您可以对内容进行本地加密，并存储加密后的内容。Amazon S3 允许您上传已经加密的对象，同时亦允许您将对象与内存内加密密钥一同上传以实现对象加密。为了实现这一目标，您必须保证提供同一个密钥。

在实施静态数据保护方案时，您应考虑使用数据分级模式以确保内容保护机制能够确切反映您的内部目标。另外，请认真考量各项合规性或者监管要求。最后，请确保您为各密钥、存储介质以及计算资源等能够访问存储内容的因素配置正确的访问级别。

关键性 AWS 服务

静态数据保护层面的关键 AWS 服务为 AWS 密钥管理服务，其提供易于使用、安全且具备冗余机制的密钥管理能力。以下服务与功能亦在这一层面发挥着重要作用：

- **Amazon S3:** 提供一项对象存储服务，可与 KMS 相集成并允许您自行提供密钥。
- **Amazon 弹性块存储(简称 EBS):** 提供可与 AWS KMS 相集成的块存储服务，但您亦可凭借操作系统工具或者其它第三方解决方案使用块级加密机制。
- **Amazon Glacier:** 提供一套长期数据归档解决方案，且对静态内容进行加密。

资源

请参阅以下资源以了解更多与静态数据保护 AWS 最佳实践相关的细节信息。

视频

- AWS 中的加密与密钥管理 [44]

说明文档

- 利用加密机制保护 Amazon S3 数据 [45]
- Amazon EBS 加密 [46]

保护传输中数据

传输中数据是指一切由某一系统传输至另一系统的内容。其中包括环境之内各服务器间的通信内容，以及各服务与最终用户间的通信内容。通过为您的传输中数据提供适合的保护级别，您将能够更具信心地保护最终用户内容。在保护传输中数据时，业界通常会选择可实现传输层安全（简称 TLS）的协议并将此作为标准化方案。

AWS 各服务面向通信提供 HTTPS 端点，因此能够在利用 AWS API 进行通信时对传输中数据提供加密支持。您可对各项计算资源进行全面控制，从而实现跨服务间传输内容的加密效果。另外，AWS 证书管理器（简称 ACM）服务亦允许您为自己的域管理并部署证书。

再有，您也可以在单一 VPC 或者多个 VPC 之间使用 VPN 连接，以便于实现流量加密。

在大规模数据传输时，请认真考量您的加密方案并在加密与易用性之间寻求平衡点。考虑在内部数据中心与 AWS 之间使用 VPN 连接，同时尽可能通过 HTTPS 以安全方式实现应用到应用间通信。您可利用弹性负载均衡、Amazon CloudFront 以及 Amazon 证书管理器生成、部署并管理可供 TLS 加密机制使用的证书。

关键性 AWS 服务

传输中数据保护层面的关键 AWS 服务为 **AWS 证书管理器**，其可帮助您生成证书以实现系统间加密传输体系的建立。以下服务与功能亦在这一层面发挥着重要作用：

- **弹性负载均衡：经典弹性负载均衡器与应用程序负载均衡器** 可帮助您利用安全端点部署并管理各负载均衡器。
- **Amazon CloudFront:** 为您的内容分发任务支持加密端点。

资源

请参阅以下资源以了解更多与传输中数据保护 AWS 最佳实践相关的细节信息。

说明文档

- AWS 证书管理器 [47]
- 如何满足传输中数据加密相关 PCI 要求 [48]
- 利用 HTTPS 监听程序创建一套经典负载均衡器 [49]

数据备份/复制/恢复

通过定义您的数据备份、复制与恢复方案，您可以保护自身免受数据删除或破坏问题的影响。理想的数据备份与复制方案能够帮助您顺利应对灾难状况。合理安全的保护一级与二级数据源则可保证业务的持续运营。

AWS 为您提供多种功能与特性，旨在实现数据备份与复制需求。Amazon S3 是一项可提供“十一个九”持久性水平的对象存储服务，其允许您为内容创建可复制至其它位置以提供额外保护能力的内容副本。Amazon RDS 负责为您的数据库实例进行备份，且允许您将这些实例复制至其它位置。您亦可为 Amazon EBS 分卷保存快照并将其复制至各个服务区。另外，大家还能够利用自动化任务与计划内任务进行资源备份。请考虑利用 AWS Lambda 函数以特定间隔执行备份。

Amazon Glacier 是一项安全、持久且成本极低的云存储服务，主要用于数据归档与长期备份。您可利用这项服务实现极具成本效益的备份副本存储。这些副本可在必要时随时进行恢复，从而满足测试、监管或者灾难场景下的具体需求。

在定义备份/复制/恢复方法时，请确保您在其中纳入希望受到保护的一切场景与相关细节。举例来说，Amazon RDS 会复制一切意外变更，因此凭借这套备份，您将能够免受恶意活动所造成的意外错误影响。请确保您建立起一套面向内容恢复的流程。您应规划灾备演练活动，旨在确保现有方案能够行之有效地应对灾难事件。另外，请考虑将各备份副本利用不同凭证组存储在不同帐户当中，以防主帐户发生安全问题。

关键性 AWS 服务

数据备份、复制与恢复支持层面的关键 AWS 服务为 Amazon S3。以下服务与功能亦在数据的备份与复制层面发挥着重要作用：

- **Amazon S3 跨区域副本**属于一项 Amazon S3 存储桶级功能，可实现对象在不同 AWS 服务区内各存储桶间的自动同步。
- **Amazon S3 生命周期策略与版本控制**允许您建立一套备份策略以满足保留需求。
- **Amazon 弹性块存储快照操作**允许您对附加至 EC2 实例的分卷进行备份。

资源

请参阅以下资源以了解更多与数据备份、复制与恢复 AWS 最佳实践相关的细节信息。

说明文档

- Amazon S3 跨服务区复制 [50]
- Amazon S3 对象生命周期管理 [51]
- Amazon S3 对象版本控制 [52]
- Amazon EBS 快照 [53]
- Amazon Glacier 上手指南 [54]
- 配合计划内事件使用 AWS Lambda [55]

事件响应

即使拥有非常成熟的预防与检测控制机制，企业仍然有必要建立相关流程以响应并缓解由安全事件引发的潜在影响。您工作负载的具体架构将极大影响到团队在事件发生期间采取行动，进而隔离或系统并将运行状态恢复至已知良好状态的能力。首先我们应当在安全事件发生前将工具部署到位，而后定期演练安全事件响应方案并及时更新架构，以确保在必要时其能够顺利完成调查取证与恢复任务。

在 AWS 当中，您可以考虑利用多种不同方案以实现事件响应。以下清洁室部分内容将描述这些方案的具体使用方式。

清洁室

在各类事件当中，保持态势感知能力无疑是最为重要的原则性要求之一。通过利用标签以确切描述您的 AWS 资源，事件响应人员将能够快速对事件的潜在影响作出判断。举例来说，根据申请系统中的拥有者或者工作队列对实例及其它资产进行标记，将使得响应团队快速派出正确的处理人员。利用数据分级或者关键性属性对系统进行标记，则可更为准确地评估事件影响。

在事件过程当中，正确的处理人员需要对事件进行隔离与遏制，而后进行取证以快速发现其根本原因。在部分案例当中，事件响应小组还需要主动参与到整治以及恢复工作当中。事件过程中，判断如何为正确的处理人员提供访问能力将直接决定响应工作所需要的时间；如果在这类压力场景下存在访问失效或者配置不当问题，则很可能引发系统中存在的其它安全性缺陷。请确保您的团队成员提前获得必要的访问权限，而后定期评估访问级别是否合理，以及其能否在必要时立即或者轻松实现触发。

在 AWS 当中，您可以利用 API 的自动执行各类事件响应过程及后续取证调查中需要完成的相关任务。举例来说，您可以通过变更与某一实例相关联的安全组对该实例进行隔离，或者在负载均衡器中将其移除出轮换清单之外。利用 Auto Scaling 对工作负载进行架构调整能够在不影响应用程序可用性的前提下，将该节点从容量中顺利移除。

为了获取磁盘镜像或者操作系统配置“原本”，响应团队可利用 Amazon EBS 快照以及 Amazon EC2 Amazon Machine Image（简称 AMI）API 以捕捉系统数据与状态。将这些快照及相关事件因素存储于 Amazon S3 或者 Amazon Glacier 之内，从而确保该数据始终可用且得到适当保留。

在事件过程当中，我们往往很难在不了解根本原因并已经顺利遏制事件影响的情况下对非受信环境进行调查。作为 AWS 的一项独有能力，安全相关人员可以利用 AWS CloudFormation 快速创建一套新的受信环境，并立足于此进行深入调查。CloudFormation 模板将在这套经过预配置的独立环境当中包含全部必要工具实例，帮助取证团队确定引发事件的原因。这不仅减少了收集必要工具所需要的时间，更能够切实实现对目标系统的隔离，同时确保响应团队始终在清洁室环境下工作。

关键性 AWS 服务

成熟的事件响应能力需要以下关键 AWS 服务与功能的配合与支持：

- **Amazon 身份与访问管理(简称 IAM)** 应被用于为事件响应团队提供适当的授权。
- **AWS CloudFormation** 可用于创建一套受信环境，用以实施深入调查。

- **Amazon EC2 API** 可用于进行实例隔离，同时缓解安全事件造成的后续影响。

资源

请参阅以下资源以了解更多与事件响应 AWS 最佳实践相关的细节信息。

视频

- AWS re:Invent 2015 (SEC308) 云环境下的安全事件整理 [56]
- AWS re:Invent 2014 (SEC404) 云环境下的事件响应 [57]

说明文档

- AWS 上的安全事件响应与取证 [58]

结论

安全保障是一项持续性工作。当相关事件发生时，我们应将其视为提升架构安全性水平的机遇。强大的认证与授权控制机制、自动化安全事件响应方案、多层次基础设施保护能力以及分类数据的加密管理手段将切实满足各类业务应用对于纵深防御的实际需求。凭借着灵活的 API 调用能力以及本文所提及的各项 AWS 服务与功能，您将能够更为轻松地实现安全保障目标。

AWS 致力于帮助您构建并运营能够切实保护信息、系统以及资产，同时交付商业价值的架构设计方案。为了保障架构安全性，您应充分利用本份白皮书中提及的各类工具与技术选项。

贡献者

以下个人及组织为本份白皮书的编撰作出贡献：

- Philip Fitzsimons，Amazon Web Services， 良好架构高级经理
- Bill Shinn，Amazon Web Services 首席安全解决方案架构师
- Sam Elmalak，Amazon Web Services 解决方案架构师

扩展阅读

如果需要获取更多帮助，请参阅以下资料：

- AWS 良好架构框架白皮书 [59]

文件修订历史

2017 年 5 月 26 日。更新系统安全配置与维护章节以纳入更多 AWS 新服务与功能。

备注

[1] https://aws.amazon.com/architecture/well-architected/

[2] https://aws.amazon.com/compliance/shared-responsibility-model/

[3] https://www.youtube.com/watch?v=_wiGpBQGCjU&feature=youtu.be

[4] https://www.youtube.com/watch?v=-XARG9W2bGc&feature=youtu.be

[5] http://docs.aws.amazon.com/general/latest/gr/root-vs-iam.html

[6] http://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

[7] http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

[8] http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2_instance-profiles.html

[9] http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html

[10] http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage.html

[11] http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_delegate-permissions.html

[12] http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html

[13] http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage.html

[14] https://www.youtube.com/watch?v=v1c9eYT6EWM

[15] https://www.youtube.com/watch?v=SpXZtN0Pjzw

[16] https://www.youtube.com/watch?v=ddz0JmCTTsU

[17] http://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html

[18] http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html

[19] https://github.com/awslabs/aws-config-rules

[20] https://aws.amazon.com/inspector/

[21] https://www.youtube.com/watch?v=HexrVfuIY1k

[22] https://aws.amazon.com/documentation/vpc/

[23] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

[24] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

[25] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_NACLs.html

[26] https://aws.amazon.com/ec2/systems-manager/

[27] https://aws.amazon.com/ec2/systems-manager/run-command/

[28] https://aws.amazon.com/ec2/systems-manager/state-manager/

[29] https://aws.amazon.com/ec2/systems-manager/inventory/

[30] https://aws.amazon.com/ec2/systems-manager/patch-manager/

[31] https://aws.amazon.com/blogs/mt/replacing-a-bastion-host-with-amazon-ec2-systems-manager/

[32] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

[33] http://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

[34] http://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html

[35] https://aws.amazon.com/documentation/inspector/

[36] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

[37] http://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

[38] http://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html

[39] https://www.youtube.com/watch?v=uhXalpNzPU4

[40] http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html

[41] https://aws.amazon.com/kms/

[42] https://aws.amazon.com/cloudhsm/

[43] https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf

[44] https://www.youtube.com/watch?v=uhXalpNzPU4

[45] http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html

[46] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

[47] http://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html

[48] https://aws.amazon.com/blogs/security/how-to-address-the-pci-dss-requirements-for-data-encryption-in-transit-using-amazon-vpc/

[49] http://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html

[50] http://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html

[51] http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

[52] http://docs.aws.amazon.com/AmazonS3/latest/dev/ObjectVersioning.html

[53] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

[54] http://docs.aws.amazon.com/amazonglacier/latest/dev/amazon-glacier-getting-started.html

[55] http://docs.aws.amazon.com/lambda/latest/dg/with-scheduled-events.html

[56] https://www.youtube.com/watch?v=uc1Q0XCcCv4

[57] https://www.youtube.com/watch?v=nzSrRvADh6g

[58] https://www.slideshare.net/AmazonWebServices/security-incident-response-and-forensics-on-aws

[59] https://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf