卓越操作支柱

AWS 良好架构框架

2017 年 11 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

本份白皮书主要面向 Amazon Web Services（简称 AWS）良好架构框架当中的卓越操作支柱。其提供相关指导以帮助客户在立足 AWS 环境进行设计、交付与维护时，遵循最佳实践以实现卓越操作。

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

本份白皮书着眼于卓越操作支柱，旨在阐述如何将卓越操作纳入您的解决方案。卓越操作在传统本地数据中心中往往极具挑战性，这是因为操作通常被认为是一个隔离的职能，与其支持的业务线团队和开发团队不同。通过采用本份白皮书中提及的各项实践，您将能够建立起可以了解其状态、实现有效和高效操作及事件响应的架构方案，并且可以持续的优化和支持您的商业目标。

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 Amazon Web Services（简称 AWS）在设计卓越操作的云架构时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，文末将提供与此类信息相关的扩展资源。

卓越操作

卓越操作支柱包含运行并监控系统以交付商业价值，同时持续改进支持流程与规程的能力。

设计原则

在云环境当中，有五项设计原则帮助实现卓越操作：

- **利用代码执行操作：**在云环境中，您可以将您在应用代码中使用的工程学运用到整个环境中去。将整个工作负载（应用、基础设施，等等）定义为代码，并且通过代码对其进行更新。您可以将操作步骤形成脚本，通过事件响应来触发脚本的自动执行。通过代码来执行操作，可以减少人工错误并保证对事件响应的一致性。
- **注释文档：**在本地数据中心中，文档由手工创建，由人来使用，有任何变动时很难随时保持同步。在云环境中，您可以在每次构建后自动生成注释文档（或者自动对手工创建的文档生成注释）。注释文档可以被人以及系统来使用，您可以将注释文档作为您的操作代码的输入。
- **进行频繁、小型、可逆的变更：**应将工作负载设计成允许组件进行定期更新。更新应该是小型的、增量的，并且在失败的时候可逆（在可能的情况下不对客户造成影响）。
- **经常优化操作规程：**您在使用操作规程时，应寻找机会优化它们。当您的工作负载演变时，操作规程也应当进行相应的演变。组织定期的竞赛日活动来检验您的所有规程是否有效，并保证您的团队熟悉这些规程。
- **预见失败：**通过“预验”练习来找出潜在的失败源，从而消除或减少它们。针对您的失败场景进行测试，检验您对其影响的理解程度。针对您的响应规程进行测试，保证其有效性以及团队对其执行足够熟悉。组织定期的竞赛日活动来测试工作负载和团队对这些模拟事件的响应能力。
- **从操作失败中汲取经验：**通过从所有操作事件和失败中汲取经验来推动改进。将汲取的经验在团队内部，以及整个组织范围内进行分享。

定义

云环境下的卓越操作主要由以下三个方面组成：

1. 筹备
2. 操作
3. 演进

运维团队应当理解业务和客户需求，从而对业务产出进行有效和高效的支持。创建和使用规程来响应操作事件，并验证其对业务需求支持的有效性；同时也收集用于衡量业务成果实现情况的指标。一切都在不断变化——您的业务环境，业务优先级，客户需求等。因此，操作的设计需要能支持随时间不断发生的变化，并且能从其性能中吸取经验，这非常重要。

筹备

要为卓越操作做好筹备，您需要理解您的工作负载以及它们的预期表现。这样您才能设计和构建操作规程以支持您的工作负载。

在筹备卓越操作时，您需要考虑以下内容：

- 操作优先级
- 操作设计
- 操作就绪程度

操作优先级

您的团队需要对您的整个工作负载，他们在其中的角色，以及共享业务目标有一个共同的理解，从而设置能够帮助业务成功的操作优先级。您还需要考虑可能会影响您优先级的外部监管和合规要求。利用您的优先级将您的操作改进工作集中在最有影响的地方（例如，开发团队技能，提高工作负载性能，自动化运行手册或增强监控）。根据需求变化更新您的优先级。

AWS 可以帮助您向您的团队普及 AWS 及其服务，以增加他们对于操作选择如何影响工作负载的理解。

您应该使用 AWS Support（AWS Knowledge Center，AWS Discussion Forms 和 AWS Support Center）和 AWS Documentation 提供的资源来教育您的团队。通过 AWS 支持中心联系 AWS 支持部门，以获取有关 AWS 问题的帮助。

如果存在适用于您的组织的外部法规或合规要求，则您应使用 AWS Cloud Compliance 提供的资源来帮助教育您的团队，以便他们考虑对您的操作优先级的影响。

AWS Trusted Advisor 是一个工具，可以帮助您进行一系列重点检查，获得针对您环境的优化建议，以帮助确定优先级。商业支持（Business Support）和企业支持（Enterprise Support）客户可以获得额外的检查，重点关注安全性、可靠性、性能和成本优化，从而进一步帮助确定优先级。企业支持客户有资格参加“云操作评估”，旨在帮助他们确定其在云中操作方式的差距。他们还可以针对其关键任务工作负载进行良好架构（Well-Architected）的审查，以根据 AWS 最佳实践来评估其架构。这些跨团队的审查有助于建立对您的工作负载的共同理解，以及达成团队角色如何促进成功的共识。通过审查确定的需求可以帮助确定您的优先级。

您可能会发现，您希望在某个时间点强调一小部分操作优先级。从长远来看，使用平衡的方式来确保所需能力的发展。

关键性 AWS 服务

AWS Support 是支持您定义操作优先级的关键 AWS 服务。它提供了工具和专业知识的组合，可帮助您在 AWS 上定义自己的目标。以下服务与功能也起到重要作用：

- **AWS Cloud Compliance** 使您能够了解 AWS 上现有的强大控制措施，以便在云中维护安全和数据保护。
- **AWS Trusted Advisor** 提供实时指导，帮助您按照 AWS 最佳实践配置资源。
- **Business Support** 商业支持提供对全套 Trusted Advisor 检查和指导的访问，以遵循 AWS 最佳实践来部署资源。
- **Enterprise Support** 企业支持客户还可获得技术客户经理（TAM）的支持，他们作为指定的技术联系人提供指导，帮助您使用最佳实践来规划和构建解决方案，并主动帮助保持您的 AWS 环境的运行状况良好。

资源

请参阅以下资源，以了解更多针对操作优先级的 AWS 最佳实践信息。

文档

- AWS Trusted Advisor [2]
- AWS 云合规性 [3]
- AWS 良好架构框架 (Well Architected Framework) [4]
- AWS 商业支持 [5]
- AWS 企业支持 [6]
- AWS 企业支持权利 [7]
- AWS 支持云操作审查 [8]
- AWS 云采用框架 (Cloud Adoption Framework) [9]

操作设计

您工作负载的设计应包括如何部署、更新和运行。您希望实施符合减少缺陷和快速安全修复的工程实践。要了解架构内发生的事情，您需要通过日志记录、仪器、以及富有洞察力的业务和技术指标进行观察。

在 AWS 中，您可以将整个工作负载（应用程序，基础架构，策略，治理和操作）视为代码。可以全部通过代码进行定义和更新。这意味着您可以将用于应用程序代码的相同工程学准则应用于堆栈的每个元素。

您应该使用 AWS CloudFormation 为您的基础架构创建版本控制的模板。您应该使用 AWS 开发人员工具（例如 AWS CodeCommit，AWS CodeBuild，AWS CodePipeline，AWS CodeDeploy 和 AWS CodeStar）设置持续集成/连续部署（CI / CD）管道。采用可以让您及早发现缺陷的做法，并在生产中安全地修复或解决这些缺陷。当您的操作支持其他工作负载时，您可以使用 AWS CloudFormation 和 AWS 开发人员工具中的工件共享设计标准。您应该使用标签应用元数据，以便识别操作活动中的资源（例如，资源所有者、生命周期阶段和环境）。

在操作工作负载时，您需要记录日志或其他性能测量，以帮助您了解发生了什么，并能够了解系统的内部状态。您应该捕获 Amazon CloudWatch 中的日志（例如，AWS CloudTrail，AWS Lambda 和 Amazon VPC Flow Logs）。您应该使用自定义 CloudWatch 事件和 Amazon CloudWatch Logs API 将应用程序中的日志直接注入到 CloudWatch 中。对于系统级日志，请使用 CloudWatch Logs 代理和 AWS CLI。您应该使用此日志信息通过 CloudWatch 仪表板或第三方工具创建系统范围的操作状态视图。

要观察系统的内部状态，您的应用程序代码应该使用 CloudWatch 发布指标。确保您发布业务指标以及技术指标，因为这些指标可以帮助您了解客户的行为。AWS 可以使用 AWS X-Ray 对分布式应用程序进行检测，该应用程序可以在请求通过应用程序时提供端到端视图。

在检测工作负载时，需要捕获大量信息以感知情况（例如状态更改，用户活动，权限访问，利用率计数等），并知道您可以随时间不同过滤选择最有用的信息。为您的组织、成本核算、访问控制和自动化的执行进行资源标记。

关键性 AWS 服务

Amazon CloudWatch 是支持操作设计的关键 AWS 服务，它允许您监控 AWS 云资源和您在 AWS 上运行的应用程序。以下服务与功能也起到重要作用：

- **AWS CloudFormation** 允许您为您的基础架构创建版本控制的标准化模板。
- **AWS 开发人员工具** 是一组能够快速安全地交付软件的服务。
- **AWS X-Ray** 跟踪用户请求在整个应用程序中的传播情况，从而实现分布式应用程序的分析和调试。

资源

请参阅以下资源以了解更多与操作设计 AWS 最佳实践相关的细节信息。

视频

- AWS re:Invent 2016：使用 AWS CloudFormation 的基础架构持续交付（DEV313） [10]
- AWS re:Invent 2016：AWS 上的 DevOps：使用 AWS 开发人员工具加速软件交付（DEV201） [11]
- AWS CodeStar：快速开始在 AWS 上开发应用程序的集中体验

文档

- Amazon CloudWatch 入门 [12]
- 使用 Amazon CloudWatch 存储和监控操作系统和应用日志文件 [13]
- Amazon CloudWatch 高分辨率客户自定义指标和告警 [14]

- 使用 Amazon CloudWatch Events 监控 AWS 运行状况事件 [15]
- AWS CloudFormation 文档 [16]
- AWS 开发人员工具 [17]
- 在 AWS 上设置 CI / CD 管道 [18]
- AWS X-Ray [19]
- AWS 标记策略 [20]

操作就绪程度

您应该使用一致的流程（包括检查清单）来了解您何时准备好启动工作负载。这也将使您能够找到任何需要制定计划的地方。您需要拥有记录日常活动的运行手册和指导您解决问题的演练手册。您需要有足够的团队成员来负责操作活动（包括随时待命的），并提供有关 AWS、工作负载和操作工具的培训。您应该使用治理流程来启动工作负载以便了解情况做出决定。

AWS 允许您将操作视为代码，编写运行手册和演练手册活动以减少人为错误的风险。您可以在脚本中使用资源标记，以根据您定义的条件（例如，环境、所有者、角色或版本）选择性执行。您可以使用脚本程序，通过触发脚本来响应事件以实现自动化。通过将您的操作和工作负载视为代码，您还可以将对您环境的评估进行脚本化和自动化。

在 AWS 上，您可以创建临时的并行的环境，从而降低实验和测试的风险、工作量与成本。您应该测试您的程序，失败场景和您的成功响应，以识别您需要计划解决的领域（例如，在正式上线之前举行竞赛日活动并测试）。

您应该使用 Amazon EC2 Systems Manager 运行命令在您的实例上编写脚本程序，并使用 AWS Lambda 编写脚本来响应跨 AWS 服务 API 和您的自定义接口的事件。使用 CloudWatch Events 触发这些脚本来自动执行响应。您应该使用 AWS Config 制作基线来自动化工作负载配置测试，并使用 AWS Config 规则来检查您的配置。这些服务将有助于确定您的工作负载是否与最佳实践和标准保持一致。

确保您的团队具备成功操作工作负载的必要技能。AWS 提供了大量资源，包括 AWS 资源中心，AWS 博客和 AWS 在线技术会谈，这些资源都提供指导、示例和演练来培训您的团队。AWS 培训和认证提供一些免费的在线培训。此外，您可以注册讲师指导的培训，以支持您团队的 AWS 技能发展。

使用“预验证”来预测故障并在适当的时候创建程序。当您更改用于评估工作负载的检查清单时，请为您如何处理不再适用的线上系统做好计划。

关键性 AWS 服务

Amazon Lambda 是支持操作就绪的关键 AWS 服务，它可以将操作过程定义为可由您的环境中的事件触发的代码。以下服务与功能也起到重要作用：

- **AWS Config** 允许您跟踪对已部署的 CloudFormation 堆栈的更改。借助 AWS Config 规则，您可以评估您的 AWS 资源是否符合最佳实践。
- **Amazon EC2 Systems Manager** 是一组功能，可帮助您自动执行 Amazon Elastic Compute Cloud（Amazon EC2）实例上的管理任务。

资源

请参阅以下资源以了解更多与操作就绪 AWS 最佳实践相关的细节信息。

文档

- AWS Lambda [21]
- AWS EC2 System Manager [22]
- AWS Config Rules - 动态检查云资源合规性 [23]
- 如何使用 AWS Config 跟踪对 CloudFormation 堆栈的配置更改 [24]
- Amazon Inspector 博客更新文章 [25]
- AWS 活动和网络研讨会 [26]
- AWS 培训 [27]

操作

操作成功是通过您定义的结果和指标来衡量的。通过了解工作负载的运行状况，您可以确定它何时受到操作事件的影响并做出适当的响应。

要实现成功的操作，您需要考虑以下几点：

- 了解运行状况
- 事件响应

了解运行状况

您的团队应该能够掌握工作负载的运行状况。您将希望通过基于运行结果的指标来获取有用的见解。您应该使用这些指标来实施具有业务和技术观点的仪表盘，以帮助团队成员做出明智的决策。

AWS 可以更轻松地整合和分析您的工作负载和操作日志，以便您随时了解运行状态和情况。

您应该将日志数据发送到 CloudWatch Logs 并定义基线指标以建立正常的操作模式。创建 CloudWatch 仪表板，以展示系统级别和业务级别指标的视图。

您还可以将 CloudWatch Logs 日志数据注入 Amazon Elasticsearch Service（Amazon ES）中，然后使用内置支持的 Kibana 创建仪表板，实现运行状况的可视化（例如订单费率，连接用户和交易时间）。

在 AWS 责任共担模型中，部分监控通过 AWS 服务健康仪表板（SHD）和个人健康仪表板（PHD）提供给您。当 AWS 遇到可能会影响您的事件时，这些仪表板会提供警报和修复指导。拥有商业和企业支持订阅的客户还可以访问 PHD API，从而实现与他们的事件管理系统的集成。

AWS 还通过 AWS 服务 API 和 SDK 支持第三方日志分析系统和商业智能工具（例如 Grafana，Kibana 和 Logstash）。

关键性 AWS 服务

Amazon CloudWatch 是帮助您了解运行状况的关键 AWS 服务，通过其功能集（包括指标和仪表板）来实现。以下服务与功能也起到重要作用：

- **Amazon CloudWatch Logs** 允许您监控和存储来自 EC2 实例、AWS CloudTrail 和其他来源的日志。
- **Amazon ES** 可以轻松部署，保护，运行和扩展 Elasticsearch 以进行日志分析和应用程序监控。
- **Personal Health Dashboard** 在 AWS 遇到可能会影响您的事件时，会提供警报和修复指导。
- **Service Health Dashboard** 提供有关 AWS 服务可用性的最新信息。

资源

请参阅以下资源以了解更多与了解运行状况 AWS 最佳实践相关的细节信息。

视频

- AWS re:Invent 2015：使用 Amazon CloudWatch 记录，监控和分析您的 IT（DVO315） [28]
- AWS re:Invent 2016：Amazon CloudWatch 日志和 AWS Lambda：完美搭档（DEV301） [29]

文档

- 使用 Amazon CloudWatch 存储和监控操作系统和应用程序日志文件 [30]
- 新增 - 针对 Amazon CloudWatch 仪表板的 API 和 CloudFormation 支持 [31]
- AWS Answers：集中化日志记录 [32]

事件响应

你应该预见操作事件，包括计划内事件（例如，销售促销，部署和故障测试）和计划外事件（例如，利用率波动和组件故障）。当您响应警报时，您应该使用现有的运行手册和演练手册来实施一致的结果。应由负责响应和升级的角色或团队来负责已定义的警报。您还需要了解系统组件对您业务的影响，并在需要时将其作为目标。您应该在事件发生后执行根本原因分析（RCA）防止故障重复出现，或记录变通方法。

AWS 提供支持工作负载和操作即代码的各个方面的工具，以简化事件响应。这些工具允许您编写对操作事件的响应脚本，通过响应监控数据触发它们的执行。在 AWS 中，您可以通过用已知的良好版本替换失败的组件来改善恢复时间，而不是尝试修复它们。然后您可以在非生产环境对失败的资源进行分析。

有多种方法可以自动执行 AWS 上的运行手册和演练手册操作。要响应您的 AWS 资源状态更改或您自己的自定义事件中的事件，您应该创建 CloudWatch 规则以通过 CloudWatch 目标（例如，Lambda 函数、Amazon Simple Notification Service（Amazon SNS）主题和 Amazon EC2 容器服务（Amazon ECS）任务）来触发响应。要响应超过资源阈值的指标（例如等待时间），您应该创建 CloudWatch 警报，以使用 Amazon EC2 操作、Auto Scaling 操作执行一个或多个操作，或将通知发送到 Amazon SNS 主题。如果您需要执行自定义操作来响应警报，请通过 Amazon SNS 通知调用 Lambda。使用 Amazon SNS 发布事件通知和升级消息以通知相关人员。

AWS 还通过 AWS 服务 API 和 SDK 支持第三方系统。合作伙伴和第三方提供了许多工具，可以实现监控、通知和响应。其中一些工具是 New Relic，Splunk，Loggly，SumoLogic 和 Datadog。

需要知晓在采取行动之前何时需要做出人为的决定。如有可能，在需要采取行动之前做出该决定。您应该保留关键的手动步骤以便在自动程序失败时使用。

关键性 AWS 服务

Amazon Lambda 是帮助您实现自动化事件响应的关键 AWS 服务，它可以将操作过程定义为可由您的环境中的事件触发的代码。以下服务与功能也起到重要作用：

- **AWS CloudWatch** 用于收集日志和指标，它启用对响应的触发执行。
- **Amazon CloudWatch Events** 提供近乎实时的系统事件流，可与您定义的规则相匹配以触发自动响应。
- **Amazon SNS** 是一种灵活的、完全托管的发布订阅消息传递和移动通知服务，用于协调向订阅终端和客户端传递消息。它使您可以调用 Lambda 响应警报。
- **Auto Scaling** 可帮助您保持应用程序可用性，并允许您根据您定义的条件对 Amazon EC2 的容量进行动态自动伸缩。
- **Amazon EC2 Systems Manager** 是一组功能，可帮助您自动执行 EC2 实例上的管理任务。

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 2016：自动执行安全事件响应，理念、代码与执行（SEC313） [33]

文档

- 什么是 Amazon CloudWatch 事件 [34]
- 如何自动标记 Amazon EC2 资源以响应 API 事件 [35]
- EC2 运行命令现在可作为 CloudWatch 事件目标 [36]
- 新增 - Amazon CloudWatch 高分辨率自定义指标和警报 [37]

演进

演进是随着时间的推移而不断改进的循环。根据从您的操作活动中汲取的经验教训，实施频繁的小增量的更改。

要随着时间的推移演进您的操作，您需要考虑以下几点：

- 从经验中学习
- 分享学习收获

从经验中学习

当出现故障时，您将希望确保您的团队以及您的大型工程社区能够从这些失败中汲取经验。您应该分析失败情况，以确定经验教训并制定改进计划。您将希望定期与其他团队一起回顾学到的经验教训，以验证您的见解。定期提供时间进行分析、实验和改进是至关重要的。

在 AWS 上，您可以轻松聚合所有操作活动、工作负载和基础架构的日志，以创建详细的活动历史记录。然后，您可以使用 AWS 工具分析您的操作（例如，识别趋势，将事件和活动与结果相关联，并在环境和系统之间进行比较和对比），以揭示改进的机会。

在 AWS 上，您可以创建临时环境副本，降低实验和测试的风险、工作量和成本。这些重复的环境可用于测试您的分析、实验结果，以及开发和测试计划中的改进。

您应该使用 CloudTrail 跟踪 API 活动（通过 AWS 管理控制台，CLI，SDK 和 API）以了解您的账户中发生的情况。使用 CloudTrail 和 CloudWatch 跟踪您的 AWS 开发人员工具的部署活动。这会将部署的详细活动历史记录及其结果添加到 CloudWatch Logs 日志数据中。

您还应该将 CloudWatch Logs 日志数据注入 Amazon ES，然后使用内置支持的 Kibana 进行可视化，并对您的操作进行一段时间的回顾分析。

或者，您可以将 CloudWatch 数据导出到 Amazon Simple Storage Service（Amazon S3），使用 Amazon Athena 进行分析，并使用 Amazon QuickSight 执行分析，创建可视化界面并获得更深入的了解。

AWS 还通过 AWS 服务 API 和 SDK 支持第三方日志分析系统和商业智能工具（例如 Grafana，Kibana 和 Logstash）。

让业务人员、开发人员和其他运营团队参与讨论和验证见解并确定需要改进的领域，实现跨团队审查。寻找机会改进您的所有环境（例如，开发、测试和生产）。

关键性 AWS 服务

Amazon ES 是帮助您从经验中学习的关键 AWS 服务，它允许您分析您的日志数据以快速安全地获取可操作的见解。以下服务与功能也起到重要作用：

- **Amazon QuickSight** 是一项业务分析服务，可轻松构建可视化，执行临时分析并快速从数据中获取洞察。
- **Amazon Athena** 是无服务器交互式查询服务，可以轻松分析 Amazon S3 中的数据。
- **Amazon S3** 可用于日志的收集和存档保留。
- **Amazon CloudWatch** 用于收集日志和指标并创建仪表板。

资源

请参阅以下资源以了解更多与从经验中学习的 AWS 最佳实践相关的细节信息。

视频

- 无服务器大数据分析 - Amazon Athena 和 Amazon QuickSight [38]

文档

- 查看 Amazon CloudWatch 控制台中的 AWS CodeDeploy 日志 [39]
- 使用 Amazon Kinesis Firehose，Amazon Athena，Amazon QuickSight 分析 VPC 流日志 [40]

分享学习收获

您应该分享您团队的学习收获，以增加整个组织的收益。您需要共享信息和资源以防止可避免的错误并简化开发工作。这将使您能够专注于交付功能。

在 AWS 上，可以使用代码方法来定义和管理应用程序、计算、基础架构和操作。这使得发布，共享和采用变得轻松。许多 AWS 服务和资源旨在跨账户共享，使您能够在团队中共享产品和知识。

使用 AWS Identity and Access Management（IAM）来定义权限，以便对您希望在账户内和跨账户共享的资源进行访问控制。您应该使用版本控制的 AWS CodeCommit 存储库来共享应用程序库、脚本程序、程序文档和其他系统文档。通过共享 AMI 访问权限和授权跨账户使用 Lambda 功能来共享您的计算标准。您还应该将您的基础架构标准通过 CloudFormation 模板共享。当您发布新资源或更新时，请使用 Amazon SNS 发布通知。订阅用户可以使用 Lambda 获取新版本。

通过 AWS API 和 SDK，您可以集成外部和第三方工具和存储库（例如，GitHub、BitBucket 和 SourceForge）。

在共享您学习和开发的内容时，请注意构建权限以确保共享存储库的完整性。

关键性 AWS 服务

AWS IAM 是帮助您分享学习收获的关键 AWS 服务，它允许您管理账户内和跨账户的资源分享。以下服务与功能也起到重要作用：

- **Amazon SNS** 支持向订阅用户发布资源的基于事件的通知。
- **AWS CodeCommit** 为您操作即代码提供版本控制的存储库，并可通过 IAM 进行共享。
- **AWS Lambda** 支持将操作过程定义为可以跨账户共享的代码。
- **AWS CloudFormation** 允许您为基础设施创建版本控制的标准化模板。
- **Amazon Machine Images**（AMI）是您的 EC2 计算环境的预定义操作系统模板。

资源

请参阅以下资源以了解更多与分享学习收获的 AWS 最佳实践相关的细节信息。

视频

- AWS re:Invent 2014 |（SEC302）委托访问您的 AWS 环境 [41]

文档

- 共享 AWS CodeCommit 存储库 [42]
- 轻松授权 AWS Lambda 函数 [43]
- 与特定的 AWS 账户共享 AMI [44]
- 通过 CloudFormation Designer URL 加速模板共享 [45]
- 将 AWS Lambda 与 Amazon SNS 结合使用 [46]

结论

卓越操作是一项持续的工作。每一次操作事件和失败都应该被视为对您架构的操作进行改善的机会。通过了解工作负载的需求，预定义日常活动的运行手册和指导解决问题的演练手册，在 AWS 上利用代码执行操作，并维持对运行情况的感知，您的操作将在事件发生时做好准备并作出响应。通过聚焦基于业务优先级的渐进式改进，以及从事件响应和回顾分析中吸取的经验教训，您将能提高操作的效率和有效性从而实现业务的成功。

AWS 致力于帮助您构建和运行体系结构，从而在构建高响应性和自适应部署的同时最大限度地提高效率。为了使您的工作负载真正实现卓越操作，您应该使用在本文中讨论的最佳实践。

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
- Brian Carlson，Amazon Web Services 良好架构运营主管
- Jon Steele，Amazon Web Services 高级技术客户经理
- Ryan King，Amazon Web Services 技术项目经理

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 [47]

备注

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

[2] https://aws.amazon.com/premiumsupport/trustedadvisor/

[3] https://aws.amazon.com/compliance/

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

[5] https://aws.amazon.com/premiumsupport/business-support/

[6] https://aws.amazon.com/premiumsupport/enterprise-support/

[7] https://aws.amazon.com/blogs/aws/aws-enterprise-support-update-training-credits-operations-review-well-architected/

[8] https://aws.amazon.com/about-aws/whats-new/2016/04/aws-support- introduces-operations-reviews-recommendations-and-reporting-available- through-enterprise-support-plan/

[9] https://aws.amazon.com/professional-services/CAF/

[10] https://www.youtube.com/watch?v=TDalsML3QqY

[11] https://www.youtube.com/watch?v=-ddpq2VQNxo

[12] https://aws.amazon.com/cloudwatch/getting-started/

[13] https://aws.amazon.com/blogs/aws/cloudwatch-log-service/

[14] https://aws.amazon.com/blogs/aws/new-high-resolution-custom-metrics-and-alarms-for-amazon-cloudwatch/

[15] http://docs.aws.amazon.com/health/latest/ug/cloudwatch-events-health.html

16 http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html

17 https://aws.amazon.com/products/developer-tools/

18 https://aws.amazon.com/getting-started/projects/set-up-ci-cd-pipeline/

19 https://aws.amazon.com/cn/xray/

20 https://aws.amazon.com/answers/account-management/aws-tagging- strategies/

21 https://aws.amazon.com/lambda/

22 https://aws.amazon.com/ec2/systems-manager/

23 http://aws.amazon.com/blogs/aws/aws-config-rules-dynamic-compliance-checking-for-cloud-resources/

24 https://aws.amazon.com/cn/blogs/mt/how-to-track-configuration-changes-to-cloudformation-stacks-using-aws-config/

25 http://aws.amazon.com/blogs/aws/category/amazon-inspector/

26 https://aws.amazon.com/about-aws/events/

27 https://aws.amazon.com/training/

28 https://www.youtube.com/watch?v=ZaOR-ybLJF0&t=1232s

29 https://www.youtube.com/watch?v=xaFaVeoA9V8

30 https://aws.amazon.com/blogs/aws/cloudwatch-log-service/

31 https://aws.amazon.com/blogs/aws/new-api-cloudformation-support-for- amazon-cloudwatch-dashboards/

32 https://aws.amazon.com/answers/logging/centralized-logging/

33 https://www.youtube.com/watch?v=x4GkAGe65vE

34

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

35 https://aws.amazon.com/blogs/security/how-to-automatically-tag-amazon-ec2-resources-in-response-to-api-events/

36 https://aws.amazon.com/blogs/aws/ec2-run-command-is-now-a-cloudwatch-events-target/

37 https://aws.amazon.com/blogs/aws/category/amazon-cloud-watch/

38 https://www.youtube.com/watch?v=m1HTL_SJHrE

39 https://aws.amazon.com/blogs/devops/view-aws-codedeploy-logs-in-amazon-cloudwatch-console/

40 https://aws.amazon.com/blogs/big-data/analyzing-vpc-flow-logs-with-amazon-kinesis-firehose-amazon-athena-and-amazon-quicksight/

41 https://www.youtube.com/watch?v=0zJuULHFS6A&t=849s

42 http://docs.aws.amazon.com/codecommit/latest/userguide/how-to-share-repository.html

43 https://aws.amazon.com/blogs/compute/easy-authorization-of-aws-lambda-functions/

44 http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html

45 https://aws.amazon.com/blogs/devops/speed-template-sharing-with-an-aws-cloudformation-designer-url/

46 http://docs.aws.amazon.com/lambda/latest/dg/with-sns-example.html

47 https://aws.amazon.com/well-architected