aws partner network | competency

AWS 零售能力
技术合作伙伴验证清单

2019 年 12 月
版本 1.0

目录

简介

AWS 能力计划旨在认可在专业解决方案领域拥有出色的技术能力和经过实证的客户成功经验的 AWS 合作伙伴网络合作伙伴（以下简称“APN 合作伙伴”）。“能力合作伙伴验证清单”（以下简称“清单”）适用于有意申请 AWS 能力的 APN 合作伙伴。该清单提供了在 AWS 能力计划中获得称号需要达到的标准。在 APN 合作伙伴申请特定能力后，我们会对他们的能力进行审计。AWS 会利用内部专业知识和第三方公司来促进审计顺利进行。AWS 保留随时对本文档进行更改的权利。

对合作伙伴的期望

希望 APN 合作伙伴在申请 AWS 能力计划前仔细阅读本文档，即使满足所有先决条件也应如此。如果本文档中的内容不清楚且需要进一步说明，请先联系您的 AWS 合作伙伴拓展代表 (PDR) 或 AWS 合作伙伴拓展经理 (PDM)。如果需要进一步帮助，您的 PDR/PDM 将会联系计划办公室。

准备好提交计划申请时，APN 合作伙伴应填写本文档中所列清单中的“合作伙伴自我评估”栏。

要提交申请，请执行以下操作：

1. 以联盟领导身份登录 APN 合作伙伴网络门户 (https://partnercentral.awspartner.com/)
2. 选择页面左侧的“View My APN Account”
3. 滚动到“Program Details”部分
4. 选择您要申请的 AWS 能力旁边的“Update”
5. 填写计划申请，然后单击“Submit”
6. 通过电子邮件将完成的自我评估发送至 competency-checklist@amazon.com。
    - 自我评估必须包括：
        - 解决方案类别（客户参与度；企业采购和规划；供应链和分销；实体、数字和虚拟商店；高级零售数据科学；以及核心零售业务应用程序）
        - 部署类型（SaaS 或在 AWS 上部署的客户）
        - 有关 AWS 案例研究的文档（定义见下文）

如对上述说明有任何疑问，请联系您的 PDR/PDM。
AWS 将在五个工作日内查看申请并回复任何问题，以启动审计计划或请求其他信息。

APN 合作伙伴应查看清单，使用清单填写自我评估，收集和整理客观证明材料以便在审计当天与审计人员分享，从而为审计做好准备。

AWS 建议 APN 合作伙伴在审计期间安排深入了解相关要求的人员。最佳实践是 APN 合作伙伴应为审计安排好以下人员：一名或多名技术水平较高的 AWS 认证工程师/架构师、一名负责运营和支持服务的运营经理、一名负责介绍概况的业务拓展主管。APN 合作伙伴应确保在安排审计之前，拥有与审计人员（无论是 AWS 还是第三方）分享客观证明材料或任何演示中包含的所有信息的必要批准。

AWS 零售能力计划

AWS 零售能力计划合作伙伴就零售领域的以下类别提供解决方案：客户参与度；企业采购和规划；供应链和分销；实体、数字和虚拟商店；高级零售数据科学；以及核心零售业务应用程序

零售能力类别

APN 合作伙伴还必须明确其解决方案适用的细分类别：

- **客户参与度：**有关忠诚度、社交渠道管理、客户关系管理 (CRM)、呼叫中心、广告（数字和直邮）、SEO 和受众参与度的解决方案，旨在使零售营销领导者能够在购买前和购买后积极吸引和留住客户。
- **企业采购和规划：**有关采购、补货、分类计划、平面和空间规划、促销和定价优化、类别管理以及供应商合作的解决方案，供企业采购和规划团队使用。
- **供应链和分销：**供应链和分销解决方案涵盖仓库管理系统 (WMS)、企业资源规划 (ERP)、仓库自动化、进出口、运输和物流。
- **实体、数字和虚拟商店：**旨在转变线上或线下购物体验的解决方案，包括 POS、订单管理系统 (OMS)、统一商务、电子商务、最后一英里配送、无限（无摩擦）商店体验、数字创新（AR/VR、ESL、物联网、信标、语音、识别、数字信息亭、智能后视镜、交互式显示器）、数字资产管理 (DAM) 和支付。
- **高级零售数据科学：**有关零售数据湖、人工智能/机器学习和分析的解决方案，旨在提高运营效率和客户参与度，并获得客户见解。
- **核心零售业务应用程序：**面向高级管理人员、财务、采购、人力资源、员工管理、法律和 IT 的核心零售企业解决方案。

APN 合作伙伴还必须确定哪种交付类别适用于其解决方案：

1. **SaaS：**通过共享 AWS 基础设施为多个客户提供服务。所有 AWS 账户均由 APN 合作伙伴管理。
2. **客户部署：**部署在客户 AWS 环境中。所有 AWS 账户均由客户管理

AWS 零售能力计划先决条件

AWS 能力计划经理会对以下各项进行验证；在安排技术验证审核之前，必须解决信息缺失或不完整问题。

1.0 APN 计划成员资格		是否满足
1.1 技术合作伙伴级别	APN 合作伙伴在申请零售能力计划之前必须阅读计划指南和定义。单击此处了解计划详情	
1.2 技术合作伙伴级别	APN 合作伙伴必须成为高级 APN 技术合作伙伴，然后才能申请 AWS 零售能力计划。	
1.3 解决方案类别	APN 合作伙伴明确其解决方案的细分类别： □ **客户参与度** □ **企业采购和规划** □ **供应链和分销** □ **实体、数字和虚拟商店** □ **高级零售数据科学** □ **核心零售业务应用程序** APN 合作伙伴明确其解决方案的交付类别： □ **SaaS** □ **客户部署**	
1.4 客户采用	APN 合作伙伴描述利用其解决方案的客户总数。	
2.0 案例研究		**是否满足**
2.1 特定于零售的案例研究	对于接受审核的每个零售解决方案，APN 合作伙伴必须进行 4 项案例研究。在这 4 个案例研究中，每个案例研究都必须与六个细分类别（客户参与度；企业采购和规划；供应链和分销；实体、数字和虚拟商店；高级零售数据科学；以及核心零售业务应用程序）之一中使用的 APN 合作伙伴解决方案示例相关。 拥有 AWS 数字客户体验 (DCX)、数据和分析、物联网、迁移和/或机器学习能力的 APN 合作伙伴可以重复使用最多 4 项客户案例研究，用于针对特定行业的挑战提供具有高度针对性的解决方案的项目，以及提供特定于零售业的独特细分领域知识的咨询服务。 APN 合作伙伴必须针对每个案例研究提供以下信息： ▪ 客户名称 ▪ 客户网站 ▪ 客户面临的挑战 ▪ 如何部署解决方案以应对挑战 ▪ 使用的第三方应用程序或解决方案 ▪ 客户参考进入生产阶段的日期 ▪ 成果/结果 ▪ 特定架构图、部署指南和其他材料，具体取决于解决方案类型，如下一节所述。 APN 合作伙伴平台中的计划申请流程会要求提供这一信息。包含在此案例研究中的信息可能是私人信息，不会公开。 我们会在技术验证的文档审核阶段检查您提供的所有 AWS 案例研究。如果 APN 合作伙伴不能按照清单所列项目提供评估案例研究所需的文档，或者存在未能满足的清单项目，则相应案例研究将不会被纳入针对相应能力的案例研究范围内。 案例研究必须描述过去 18 个月内执行的部署，并且必须针对已经由客户投入生产的项目，而不是处于试点或概念验证阶段的项目。	

2.2 公开案例研究	在批准合作伙伴的能力申请后，AWS 会使用公开案例研究来根据可衡量的 KPI 展示 APN 合作伙伴解决方案的成功经验，并且让客户相信 APN 合作伙伴拥有根据客户目标来开发和交付解决方案的经验和知识。 APN 合作伙伴必须将与案例研究相关的 4 项客户部署中的 2 项作为公开案例研究发布。这些公开案例研究可以采用正式案例研究、白皮书或博客文章的形式。	
	公开案例研究必须能够从 APN 合作伙伴的网站轻松找到，例如必须能够从 APN 合作伙伴的主页导航到公开案例研究，并且 APN 合作伙伴必须在应用程序中提供指向这些公开案例研究的链接。	
	公开案例研究必须包括以下内容： ▪ 客户名称、APN 合作伙伴名称和 AWS 的参考 ▪ 客户面临的挑战 ▪ 如何部署解决方案以应对挑战 ▪ AWS 服务如何用作解决方案的一部分 ▪ 成果/结果	
3.0 AWS 零售网络形象和思想领导力		**是否满足**
3.1 APN 合作伙伴的 AWS 登录页面	APN 合作伙伴为其 AWS 零售解决方案创建的网络形象要让客户对 APN 合作伙伴在零售方面的能力和经验有信心。 APN 合作伙伴必须有 AWS 登录页面，该页面描述其 AWS 零售解决方案，提供指向其公开案例研究的链接，列举技术合作伙伴关系，并且提供能够证明 APN 合作伙伴拥有零售方面的专业知识以及突出与 AWS 的合作的任何其他相关信息。 必须能够从 APN 合作伙伴的主页访问特定的 AWS 零售页面。主页本身不能作为 AWS 登录页面，除非 APN 合作伙伴是专门的零售技术公司，并且主页反映出 APN 合作伙伴对零售的关注。	
3.2 零售思想领导力	AWS 零售能力合作伙伴在零售方面拥有深厚的专业知识，并开发了利用 AWS 服务的创新解决方案。 APN 合作伙伴必须拥有面向公众的材料（例如博客文章、新闻报道、视频等），以展示 APN 合作伙伴对零售的关注及所具备的零售专业知识。合作伙伴必须提供过去 12 个月内发布的材料示例的链接。	
4.0 业务要求		
4.1 准备就绪的工具包	APN 合作伙伴必须有准备就绪的文档和卖家工具包，包括明确的产品价值主张；可以通过确定能否赢得客户的所有相关信息（例如销售素材、演示文稿和客户用例）来向 AWS 销售组织清楚地表达这一价值主张。 证据必须采用销售素材的形式，包括演示文稿、单页和用例清单。	
4.2 产品支持/帮助平台	APN 合作伙伴通过网络聊天、电话或电子邮件支持向客户提供产品支持。 必须通过描述针对产品或解决方案为客户提供的支持的形式来提供证据。	
4.3 产品在 AWS Marketplace 上销售	APN 合作伙伴通过 AWS Marketplace 提供解决方案。 □ 是 □ 否 如果“是”，则 APN 合作伙伴必须提供指向 AWS Marketplace 列表的链接。如果“否”，则无需更多信息。	

4.4 针对联合卖出的 AWS 产品/服务的销售报酬	APN 合作伙伴为其卖家提供与 AWS 联合销售的销售报酬计划。 □ 是 □ 否 □ 说明：_____ 必须提供对面向 APN 合作伙伴卖家的报酬计划的简要说明作为证明材料。	
4.5 AWS/APN 合作伙伴联合共赢	APN 合作伙伴具备记录和公开联合共赢情况的流程。 通过口头描述过程的形式提供证明材料。	
5.0 APN 合作伙伴自我评估		**是否满足**
5.1 AWS 能力合作伙伴计划验证清单自我评估	APN 合作伙伴必须进行自我评估，以便确定自己是否满足“AWS 零售技术合作伙伴验证清单”中的要求。 ▪ APN 合作伙伴必须填写该清单中的所有部分。 ▪ 必须通过电子邮件并按照以下电子邮件主题行约定将完成的自我评估发送到 **competency-checklist@amazon.com**：“[APN 合作伙伴名称]，零售能力技术合作伙伴完成的自我评估。” ▪ 建议 APN 合作伙伴先让其合作伙伴解决方案架构师、合作伙伴拓展代表 (PDR) 或合作伙伴拓展经理 (PDM) 审核完成的自我评估，然后再将其提交给 AWS。这样做是为了确保 APN 合作伙伴的 AWS 团队能够参与其中并在审核之前提供建议，从而确保带来积极的审核体验。	

零售能力技术合作伙伴验证清单

第三方审核人员和/或 AWS 合作伙伴解决方案架构师会对以下各项进行验证；在安排技术验证审核之前，必须解决信息缺失或不完整问题。

技术验证		适用于： SaaS	适用于： AWS 上部署的客户	是否满足
架构图	根据部署类别，需要一个或多个架构图。 每个架构图必须： □ 显示架构的主要元素，以及这些元素如何结合，以便向客户提供合作伙伴解决方案 □ 使用适当的 AWS 服务图标显示使用的所有 AWS 服务。 □ 显示 AWS 服务的部署方式，包括 Amazon Virtual Private Cloud (VPC)、可用区 (AZ)、子网和到 AWS 外部系统的连接。 □ 包括在 AWS 外部部署的元素，例如本地组件或硬件设备。	是 – 整个解决方案一个，每个案例研究一个。	是 – 每个案例研究一个。	
部署指南	部署指南必须提供在 AWS 上部署合作伙伴解决方案的最佳实践，并包括“部署指南的基准要求”中概述的所有部分	否	是 – 解决方案一个。	
已完成的验证清单	对于为合作伙伴解决方案提供的 4 项案例研究，APN 合作伙伴必须提供以下清单的完成版本，表明满足了哪些清单项目。	是	是	
1.0 安全性 **安全性支柱侧重于保护信息和系统。关键主题包括数据的机密性和完整性，标识和管理哪些人员可以通过权限管理进行哪些操作，保护系统以及建立控制机制来检测安全事件。**				
1.1 不使用 AWS 账户根用户进行日常活动	AWS 账户根用户不得用于进行日常活动。创建 AWS 账户后，您应该立即创建 AWS Identity and Access Management (IAM) 用户账户，并且使用这些 IAM 用户账户进行所有日常活动。创建 IAM 用户账户后，您应该安全地存储 AWS 根账户凭证，并仅将其用于执行需要 AWS 账户根用户的少量账户和服务管理任务。有关如何设置 IAM 用户账户和群组以供日常使用的更多信息，请参阅创建您的首个 IAM 管理用户和群组。	是	否	
1.2 已为 AWS 账户根用户启用 Multi-Factor Authentication (MFA)	您必须为 AWS 账户根用户启用 Multi-Factor Authentication (MFA)。因为 AWS 账户根用户可以在 AWS 账户中执行敏感操作，所以添加额外的身份验证可以帮助您更好地保护您的账户。我们提供多种类型的 MFA，包括虚拟 MFA 设备和硬件 MFA 设备。	是	否	
1.3 将 IAM 用户账户用于所有日常活动	在不需要的情况下，不得将 AWS 账户根用户用于任何任务。而是应该为每个需要管理员访问权限的人创建一个新的 IAM 用户。然后，通过将用户放入您附加了管理员访问管理策略的管理员组，让这些用户成为管理员。之后，管理员组中的用户应该针对 AWS 账户设置组和用户等内容。将来要进行的所有交互都应该通过 AWS 账户的用户和他们自己的密钥而不是根用户来进行。但是，要执行某些账户和服务管理任务时，您必须使用根用户凭证登录。	是	否	
1.4 为所有交互式 IAM 用户启用 Multi-Factor Authentication (MFA)	您必须为所有交互式 IAM 用户启用。使用 MFA，用户就有了一个可以生成唯一身份验证码（一次性密码或称为 OTP）的设备。用户必须同时提供常规凭证（用户名和密码）和 OTP。MFA 设备可以是一个特殊的硬件，也可以是一个虚拟设备（例如，它可以在智能手机上的应用程序中运行）。	是	否	
1.5 IAM 凭证定期轮换	您必须定期更改密码和访问密钥，并确保您账户中的所有 IAM 用户也这样做。这样，如果在您不知情的情况下密码或访问密钥被盗用，则您可以限制使用凭证访问您的资源的时间。您可以对账户应用密码策略，要求所有 IAM 用户轮换其密码，而且您可以选择用户必须轮	是	否	

	换密码的频率。有关轮换 IAM 用户的访问密钥的更多信息，请参阅轮换访问密钥。			
1.6 为 IAM 用户配置了强密码策略	您必须为 IAM 用户配置强密码策略。如果允许用户更改其自己的密码，则您应该要求他们创建强密码并要求他们定期轮换密码。您可以在 IAM 控制台的“账户设置”页面创建适用于您的账户的密码策略。您可以使用密码策略来定义密码要求，例如最小长度、是否需要非字母字符和轮换频率等。有关更多信息，请参阅为 IAM 用户设置账户密码策略。	是	否	
1.7 IAM 凭证不在多个用户之间共享	您必须为需要访问您账户的所有人创建单独的 IAM 用户账户。您还需要为自己创建一个 IAM 用户，向该用户授予管理权限，并使用该 IAM 用户来执行所有工作。通过为访问您帐户的人员创建单独的 IAM 用户，您可以为每个 IAM 用户提供一组唯一的安全凭证。您还可以向每个 IAM 用户授予不同的权限。如有必要，您可以随时更改或撤销 IAM 用户的权限。（如果您将根用户凭证提供给他人，就可能很难撤回，而且无法限制获得这些凭证的人员的权限。）	是	否	
1.8 将 IAM 策略设置为只授予最低权限	您必须遵循授予最低权限这一标准的安全建议。这意味着只授予执行任务所需的权限。确定用户需要执行的任务，然后制定让用户只执行这些任务的策略。最开始只授予最低权限，然后根据需要授予其他权限。这样做比一开始授予过于宽松的权限而后再尝试收紧权限更为安全。定义适当的权限之前需要进行一些研究。确定执行特定任务需要具备的条件、特定服务支持哪些操作以及执行这些操作所需的权限。	是	否	
1.9 不使用硬编码凭证（例如访问密钥）	您必须遵循有关管理 AWS 访问密钥的最佳实践，并避免使用硬编码凭证。以编程方式访问 AWS 时，您使用访问密钥来验证您的身份和应用程序的身份。拥有您的访问密钥的任何人将与您拥有相同的 AWS 资源访问权限级别。因此，AWS 全力保护您的访问密钥，而且按照责任共担模式的要求，您也应该这样做。	是	是	
1.10 对所有凭证进行静态加密	基准要求是确保对所有凭证都进行静态加密。	是	是	
1.11 AWS 访问密钥仅供交互式用户使用	除以下情况外，不得使用 AWS 访问密钥：1. 特定人员使用 AWS 访问密钥来访问 AWS 服务，并且将密钥安全地存储在由其控制的设备上。2. 某项服务使用 AWS 访问密钥来访问其他 AWS 服务，但仅限于以下情况：a) 无法使用 Amazon EC2 实例角色、Amazon Elastic Container Service (Amazon ECS) 任务角色或类似机制，b) AWS 访问密钥至少每周轮换一次，以及 c) 具备严格的 IAM 策略，以便：i) 仅允许访问特定的方法和目标，并且 ii) 限制访问子网（在该子网上或从该子网访问资源）。	是	是	
1.12 为每个区域的所有 AWS 账户启用了 AWS CloudTrail	必须为每个区域的所有 AWS 账户启用 AWS CloudTrail。了解 AWS 账户活动是一项关键的安全与运营最佳实践。您可以使用 AWS CloudTrail 查看、搜索、下载、存档、分析和响应 AWS 基础设施中的账户活动。您可以确定谁或什么程序执行了什么操作、操作了哪些资源、事件发生的时间以及其他详细信息，从而帮助您分析和响应 AWS 账户中的活动。	是	否	
1.13 CloudTrail 日志存储在其他 AWS 账户所有的 S3 存储桶中	AWS CloudTrail 日志必须存储在访问权限极其有限（例如仅限审计与恢复）的其他 AWS 账户拥有的存储桶中。	是	否	
1.14 CloudTrail S3 日志存储桶启用了版本控制	必须使用版本控制功能或 MFA 删除功能保护 AWS CloudTrail 日志存储桶的内容。	是	否	

功能或 MFA 删除功能				
1.15 Amazon EC2 安全组具备严格的访问限制	所有 Amazon EC2 安全组都应该尽可能地限制访问。至少要：1. 实施安全组来限制互联网和 Amazon VPC 之间的流量，2. 实施安全组来限制 Amazon VPC 内的流量，3. 在所有情况下都只使用限制性最高的设置。	是	是	
1.16 为您账户中的 Amazon S3 存储桶设置了适当的访问权限	您必须确保制定了适当的控制措施来控制对每个 Amazon S3 存储桶的访问。使用 AWS 时，最佳实践是只向确实需要访问您的资源的人员授予访问权限（最低权限原则）。	是	是	
1.17 Amazon S3 存储桶没有错误配置为允许公开访问。	您必须确保正确配置了不允许公开访问的存储桶，以便防止公开访问。默认情况下，所有 Amazon S3 存储桶都是私有的，只能由获得显式授权的用户访问。除非使用 Amazon S3 托管公有资产（例如，托管在公有网站上使用的映像），否则大多数使用案例不需要广泛的公有访问权限来从 Amazon S3 存储桶读取文件；最佳实践是永远不向公众开放访问权限。	是	是	
1.18 具备监控机制来检测 S3 存储桶或对象被公开访问的情况	您必须具备监控或提醒机制，以便发现 Amazon S3 存储桶被公开访问的情况。一种选择是使用 AWS Trusted Advisor。AWS Trusted Advisor 可以检查 Amazon S3 中具有开放访问权限的存储桶。如果向每个人授予“列出”权限，那么当存储桶中的对象被非预期用户频繁列出时，费用可能会超出预期。如果向每个人授予“上传/删除”权限，那么任何人都可以向存储桶添加项目或者修改或删除存储桶中的项目，这样会产生潜在的安全漏洞。Trusted Advisor 可以检查明确的存储桶权限和可能替代存储桶权限的相关存储桶策略。	是	否	
1.19 具备监控机制来检测 Amazon EC2 实例和容器中的更改	对 Amazon S3 实例或容器的更改可能表示存在未经授权的活动，并且必须至少将这些更改记录到一个持久的位置，以便将来进行取证调查。为此制定的机制必须至少能够：1. 检测对解决方案中使用的 Amazon S3 实例或容器中的操作系统或应用程序文件的任何更改。2. 将记录以上更改的数据存储到 Amazon S3 实例或容器之外的一个持久的位置。合适的机制包括：a. 通过计划的配置管理（例如 Chef、Puppet 等）或专用工具（例如 OSSEC、Tripwire 或类似工具）部署文件完整性检查，或 b. 扩展配置管理工具来验证 Amazon S3 主机配置，并且通过配置“Canary”（记录无操作）事件以便在关键配置文件或软件包有更新时发出提醒，从而确保服务在运行时在所有范围内主机上保持运行，或 c. 部署主机型入侵检测系统，例如使用 ElasticSearch 和 Kibana 的 OSSEC 等开源解决方案，或者使用合作伙伴解决方案。请注意，以下机制不符合要求：频繁循环 Amazon S3 实例或容器。	是	否	
1.20 对所有数据进行了分类	考虑在工作负载中处理和存储的所有客户数据并对其进行分类，以便确定数据的敏感性以及处理这些数据时使用的适当方法。	是	是	
1.21 所有敏感数据都经过加密	归类为敏感数据的所有客户数据都经过静态加密和动态加密。	是	是	
1.22 安全地管理加密密钥	对所有加密密钥进行静态加密和动态加密，并且使用 AWS Key Management Service (KMS) 等 AWS 解决方案或 HashiCorp Vault 等合作伙伴解决方案控制对密钥的访问。	是	是	
1.23 所有传输中的数据都经过加密	Amazon Virtual Private Cloud 边界上的所有传输数据都经过加密。	是	是	

1.24 已经确定并演练过安全事故响应流程	必须制定安全事件响应流程来处理 AWS 账户被盗用等事件。必须通过演练事故响应流程（例如安全演练）对该流程进行测试。必须在过去 12 个月内进行演练，以便确认：a. 相关人员拥有访问环境的权限。b. 具备适当的工具。c. 相关人员知道如何响应计划中提到的各种安全事故。	是	否	
1.25 支付卡行业 (PCI) 数据安全标准 (DSS) – 认证或 SAQ	对于存在持卡人数据的电子商务、统一商务和销售点应用程序，建立了一个流程，用于对工作负载的支付卡行业 (PCI) 数据安全标准 (DSS) 范围执行年度评估。根据范围评估，视需要执行 PCI DSS 认证或 SAQ。证明材料必须采用 PCI DSS 认证合规报告或完成的自我评估问卷 (SAQ) 的形式。	是	是	
1.26 端到端 PCI 数据加密	对于存在持卡人数据的电子商务、统一商务和销售点应用程序，会对传输中的数据进行加密，即使是位于 Amazon VPC 中。	是	是	
1.27 针对分布式拒绝服务 (DDoS) 攻击的保护措施已准备就绪	提供可缓解开放系统互连 (OSI) 模型各层中分布式拒绝服务 (DDoS) 攻击的基础设施和服务。	是	否	
1.28 缓解开放 Web 应用程序安全项目 (OWASP) 十大攻击的机制已准备就绪	提供可缓解开放 Web 应用程序安全项目 (OWASP) 漏洞的基础设施和服务。	是	否	
2.0 可靠性 可靠性支柱侧重于预防故障和快速从故障中恢复以便满足业务和客户需求的能力。关键主题包括设置相关的基本要素、跨项目要求、恢复计划以及我们如何处理变更。				
2.1 网络连接高度可用	解决方案的网络连接必须高度可用。如果使用 VPN 或 AWS Direct Connect 连接到客户网络，则解决方案必须支持冗余连接，即使客户并不是一直使用。	是	是	
2.2 基础设施扩展机制符合业务需求	基础设施扩展机制必须符合业务需求，具体方式如下：1. 在架构的每一层实施自动扩展机制，或 2. 确认当前的业务需求（包括成本需求和预计用户增长）不需要自动扩展机制，并且手动扩展程序已经被充分记录并频繁测试。	是	是	
2.3 AWS 和应用程序日志集中管理	应用程序和 AWS 基础设施中的所有日志信息都应该合并到一个单独的系统中。	是	否	
2.4 AWS 和应用程序监控和报警集中管理	必须集中监控应用程序和 AWS 基础设施，并且生成警报并将其发送给相应的操作人员。	是	否	
2.5 实现了基础设施配置和管理的自动化	解决方案必须使用 AWS CloudFormation 或 Terraform 等自动化工具来配置和管理 AWS 基础设施。不得使用 AWS 控制台对生产 AWS 基础设施进行常规更改。	是	是	
2.6 持续进行定期数据备份	您必须定期将数据备份到持久存储服务。备份可以确保您能够从管理错误、逻辑错误或物理错误中恢复。Amazon S3 和 Amazon Glacier 是理想的备份和存档服务。Amazon S3 和 Amazon Glacier 都是持久且低成本的存储平台。两者都可以提供无限容量，而且即便备份数据量不断增长也不需要进行卷管理或媒体管理。Amazon S3 和 Amazon Glacier 采用按用量付费模式，且每月每 GB 的成本较低，所以非常适合用于数据保护。	是	是	
2.7 定期对恢复机制进行测试，并在架构	您必须定期测试恢复机制和恢复流程，并在对云环境进行重大更改后进行测试。AWS 可以提供大量资源帮助您管理数据备份和恢复。	是	否	

发生重大更改后进行测试				
2.8 解决方案可以灵活应对可用区服务中断	在单个可用区内的所有服务都中断的情况下，解决方案必须能够继续运行。	是	是	
2.9 已经对解决方案的弹性进行了测试	已经在过去 12 个月内通过演练对基础设施应对单个可用区服务中断的能力进行了测试。	是	否	
2.10 已经制定了灾难恢复 (DR) 计划	明确的灾难恢复计划应该包含恢复点目标 (RPO) 和恢复时间目标 (RTO)。您必须针对所有范围内的服务确定 RPO 和 RTO，并且 RTO 必须与您与客户签订的 SLA 的要求一致。	是	是	
2.11 恢复时间目标 (RTO) 少于 24 小时	对于核心服务，基准要求是 RTO 少于 24 小时。	是	否	
2.12 灾难恢复 (DR) 计划已经过充分测试	必须对照恢复点目标 (RPO) 和恢复时间目标 (RTO) 定期测试灾难恢复计划，并在进行重要更新后测试灾难恢复计划。在 AWS APN 高级合作伙伴申请获得批准之前，必须至少进行一次灾难恢复测试。	是	否	
2.13 灾难恢复 (DR) 计划涵盖恢复到另一个区域	您的灾难恢复计划必须包含恢复到另一个 AWS 区域的策略，而且必须针对这种情况进行定期恢复测试。您必须在过去 12 个月内至少完成一次灾难恢复计划的全面测试，并且至少要恢复到另一个 AWS 区域。注意：虽然将数据还原到测试环境或为用户导出数据可以有效地验证备份，但这些过程无法满足对另一个 AWS 区域进行全面恢复测试的要求。	是	否	
3.0 卓越运营 卓越运营支柱侧重于运行和监控系统以便实现业务价值，以及不断改进流程和程序。关键主题包括管理和实现变更自动化、响应事件以及定义标准，以便成功管理日常操作。				
3.1 实现了代码更改部署自动化	解决方案必须支持将代码自动部署到 AWS 基础设施。不得使用交互式安全外壳 (SSH) 或远程桌面协议 (RDP) 会话在 AWS 基础设施中部署更新。	是	否	
3.2 编制了运行手册并确定了上报流程	必须编制运行手册，确定响应各种应用程序和 AWS 事件时使用的标准程序。必须确定上报流程，用于处理系统生成的提醒和报警，并响应客户报告的事故。上报流程还必须包括在适当情况下上报至 AWS Support。	是	否	
3.3 已经为 AWS 账户启用 AWS 商业支持	必须启用商业支持。商业支持（或更高级别）是针对高级技术合作伙伴的 AWS 合作伙伴网络要求。要获得高级技术合作伙伴资格，您必须至少为一个 AWS 账户启用商业支持。	是	否	
4.0 性能效率 性能效率支柱侧重于有效使用 IT 和计算资源。关键主题包括根据工作负载要求选择正确的资源类型和规模、监控性能，并根据业务需求的变化做出明智的决策以便维持效率。				
4.1 部署后启用性能测试	定义可衡量的性能目标，并在发布到生产环境之前进行性能测试，以验证是否达到性能目标。	是	是	
4.2 监控阈值已准备就绪	监控应用程序性能并准备好适当的机制，以在超出阈值时触发警报。	是	是	

AWS 资源：

标题	描述
如何构建实践登录页面	提供有关如何构建满足计划先决条件的实践/解决方案页面的指导。
如何编写公共案例研究	提供有关如何构建满足计划先决条件的公共客户案例研究的指导。
如何构建架构图	提供有关如何构建满足计划先决条件的架构图的指导。
合作伙伴准备文档	提供有关计划先决条件的指导和最佳实践示例。
AWS 架构完善的网页	涵盖架构完善的最佳实践