在 Amazon Web Services 上实现 Microsoft 应用程序现代化

如何开始您的旅程

2016 年 3 月

版权声明

目录

摘要

现在，云是大多数企业 IT 战略的核心。许多企业发现，妥善规划的云迁移策略（“简单地搬运”）能够带来直接的业务收益。本白皮书的目标受众是以 Microsoft 为中心的组织中的 IT 专家和业务决策者，他们希望将基于云的方法引入组织的 IT 实践中，因此必须对在 Microsoft Windows Server 和 Microsoft SQL Server 上构建的现有关键业务应用程序进行现代化。本白皮书介绍现代化 Amazon Web Services (AWS) 上的应用程序的优势以及如何开始您的这一旅程。

为什么要现代化应用程序？

对于许多 IT 组织来说，应用程序现代化都是一项重大举措，主要原因在于：

- **去除陈旧软件**

  避开维护陈旧软件和不支持的版本（Windows Server 2003、SQL Server 2003 和 SQL Server 2005）相关的时间、成本、性能及可靠性方面的难题。

- **开发运营计划**

  充分发挥新的开发运营和应用程序生命周期管理方法的优势。通过迁移到新的应用程序交付平台，公司能够加快创新步伐。

- **移动性计划**

  随着用户向移动设备迁移，IT 服务的使用量可能会增长一个或多个数量级。如果应用程序没有做好应对这种增长的准备，则会导致可扩展性方面的挑战。

- **新产品发布**

  新产品的推出可能会造成 IT 需求迅猛增加。基础应用程序（包括 Microsoft SQL Server 和 Microsoft SharePoint）必须做好准备，应对支持新品发布所需的扩展。

- **并购 (M&A) 活动**

  如果发生企业并购活动，复杂性会逐渐累积。在经历多次收购活动之后，公司会发现自己拥有成百上千的 SharePoint 站点、许多 Exchange 实例以及不计其数的 SQL Server 数据库。优化不同应用程序的管理往往是一项艰巨的任务。

为什么在 AWS 上运行 Microsoft 应用程序？

在最近的一项调查[1]中，International Data Corporation (IDC) 报告称有 50% 的受访者使用 AWS 来支持其生产力应用程序，如 Microsoft 开发的生产力应用程序。在这一数字中，65% 的受访者表示计划通过迁移现有应用程序或扩展已在 AWS 上运行的应用程序来增加对 AWS 的使用量。很明显，客户已经开始通过迁移来现代化其 Microsoft 应用程序。

面向企业应用程序的 AWS

客户可以通过在 AWS 云中运行基于 Microsoft Windows Server 构建的企业应用程序来提升其安全性及应用程序的性能和可靠性。例如，客户可在数小时内将可全球访问的 SharePoint 环境部署到 33 个 AWS 可用区中的任何一个可用区。为降低复杂性，客户可以使用与 Microsoft 管理和访问控制应用程序（如 System Center 和 Active Directory）集成的 AWS 工具。此外，客户还可以借助 AWS CloudFormation 模板可靠、重复地执行应用程序部署。

面向 LOB 应用程序和数据库的 AWS

业务线 (LOB) 所有者需要运行许多行业的应用程序，如石油和天然气勘探、零售终端 (POS)、金融、医疗、保险、制药、媒体和娱乐等。为加快部署，客户可以启动预配置的 Amazon 系统映像 (AMI) 模板，其中含有完全合规的 Microsoft Windows Server 和 Microsoft SQL Server 许可。

面向开发人员的 AWS

在 AWS 上进行开发工作的客户可以使用 Microsoft 开发工具，包括 Visual Studio、PowerShell 和 .NET 开发人员中心。通过这些工具，配以 AWS CodeDeploy、AWS Elastic Beanstalk (Elastic Beanstalk) 和 AWS OpsWorks 的可扩展性及敏捷性，客户能够更快地在 AWS 上完成代码并进行部署，且风险更低。

[1] http://www.idc.com/getdoc.jsp?containerId=256654

我可以在 AWS 上运行哪些 Microsoft 应用程序？

客户已在 AWS 云中成功部署几乎所有 Microsoft 应用程序，包括：

- Microsoft Windows Server
- Microsoft SQL Server
- Microsoft Active Directory
- Microsoft Exchange Server
- Microsoft Dynamics CRM 和 Dynamics AX、Dynamics ERP
- Microsoft SharePoint Server
- Microsoft System Center
- Skype for Business（以前称作 Microsoft Lync）
- Microsoft Project Server
- Microsoft Visual Studio Team Foundation Server
- Microsoft BizTalk Server
- Microsoft 远程桌面服务

如何入门？

对于企业来说，第一步是确定要在 50 多项 AWS 服务中选择哪些服务来支持其应用程序现代化计划。下图说明企业 IT 组织的典型职能与 AWS 产品之间的对应关系。本白皮书讨论该对应关系图中的部分重要服务，介绍它们在 Microsoft 应用程序现代化计划中的作用。

图 1：企业 IT 与 Amazon Web Services 之间的概念对应关系

安全性和访问权限

> 我们与 AWS 合作开发了一种安全模型，它使我们在 AWS 中的运营甚至比在我们自己的数据中心里还要安全。
>
> — Rob Alexander，Capital One 首席信息官

随着安全话题日益成为焦点以及社会各界对安全性的关注度日益增加，大多数客户的第一步是选择能够确保合规性和管控风险的服务。AWS 云采用与传统数据中心相同的安全隔离措施，包括物理安全性、网络隔离、服务器硬件隔离、存储隔离。AWS 已取得 ISO 27001 认证；同时根据支付卡行业 (PCI) 数据安全标准 (DSS)，已被确认为一级服务提供商。AWS 每年都会接受服务组织控制 (SOC) 1 审计，已成功获得美国联邦政府系统的“中级”评估认证，以及美国国防部 (DOD) 系统的国防部信息保障认证和鉴定流程 (DICAP) 的二级认证。

许多企业考虑采用适当的一组服务来确保安全性和管控权限，对于这类企业而言，Amazon Virtual Private Cloud、AWS Direct Connect 和 AWS Directory Services 是这一讨论的核心议题。通过 Amazon Virtual Private Cloud (Amazon VPC)，客户可以将 AWS 资源启动到自己定义的虚拟网络中。这个虚拟网络与本地数据中心的传统网络极其相似，但具有 AWS 可扩展基础设施的优势。

AWS Direct Connect 通过专用 1 Gb 或 10 Gb 以太网光缆将组织内部网络连接到 AWS。光缆的一端连接数据中心路由器，另一端连接 AWS Direct Connect 路由器。这一加密连接就绪后，客户可以绕过网络路径中的 Internet 服务提供商，创建直接通向 AWS 云（例如，Amazon Elastic Compute Cloud (Amazon EC2) 和 Amazon Simple Storage Service (Amazon S3)）和 Amazon VPC 的虚拟接口。

AWS Directory Service 是一项托管服务，您可以通过它方便地将 AWS 服务连接到现有本地 Microsoft Active Directory（通过 AD Connector），或在 AWS 云中设置和操作一个新目录（通过面向 AWS Directory Service 的 Simple AD 和 Microsoft Active Directory）。

正在传输（通过 SSL）的数据和静态数据的数据加密服务是通过服务器端和客户端加密实现的。AWS Certificate Manager (ACM)、AWS Key Management Service (AWS KMS) 和 AWS CloudHSM 可配合使用以确保提供密钥和证书管理服务，从而安全地生成、存储和管理用于数据加密的加密密钥。

最后，AWS WAF 提供 Web 应用程序防火墙服务以帮助 Web 应用程序防范常见的 Web 漏洞，这些漏洞可能会影响应用程序的可用性、危害安全性或占用过多资源。

计算：在 EC2 实例上运行的 Windows Server

> 我们没有时间重新设计应用程序。AWS 可以支持我们在 Windows Server 2003 上运行的旧 32 位应用程序、各种 Microsoft SQL Server 和 Oracle 数据库以及可靠的 Citrix 环境。
>
> — Jim McDonald，Hess 首席架构师

有了安全策略后，就该考虑要采用哪种基础设施来支持将要现代化的应用程序了。

Amazon EC2 是一项 Web 服务，可提供用于构建和托管软件系统的可扩展计算容量。要将 Windows 应用程序设计为在 Amazon EC2 上运行，客户可以根据不断变化的需求规划计算和存储资源的快速部署和快速缩减。当客户在 EC2 实例上运行 Windows Server 时，他们无需像对待本地 Windows Server 那样预置同样的系统包（包括硬件、虚拟化、软件和存储）。而是可以专注于使用各种云资源，以便提高 Windows 应用程序的可扩展性和总体性能。启动运行 Windows Server 的 Amazon EC2 实例之后，该实例的行为类似于运行 Windows Server 的传统服务器。例如，不管 Windows Server 是部署在本地还是 Amazon EC2 实例上，它都能运行 Web 应用程序，执行批处理，或管理需要大量计算的应用程序。通过远程桌面协议，客户可以直接远程进入 Windows Server 实例，管理非常方便。借助 Amazon EC2 Run Command，客户可以对单一 Windows Server 实例或整个实例队列运行 PowerShell 脚本。

为 Amazon EC2 构建的应用程序按需使用底层的计算基础设施。应用程序按需利用资源（如存储和计算资源）执行任务，并在任务完成后释放资源。此外，任务完成之后，它们通常会自动终止。处理过程中，应用程序会根据资源要求进行灵活扩展和缩小。Elastic Load Balancing 自动将传入的应用程序流量分配到云中的多个 Amazon EC2 实例。这使得客户能够实现更高的应用程序容错性能，从而无缝提供分配应用程序流量所需的负载均衡容量。

Auto Scaling 让客户能够非常密切地跟踪应用程序的需求曲线，减少提前手动预置容量的需求。例如，客户可以设置条件，当 Amazon EC2 队列的平均使用率较高时，按照增量向 Auto Scaling 组中添加新的 Amazon EC2 实例；同样，他们也可以设置条件，在 CPU 使用率较低时，以同样的量减少实例。

数据库：在 Amazon RDS 或 Amazon EC2 上运行的 SQL Server

> 通过 Amazon Relational Database Service (Amazon RDS)，我们的数据库管理员团队可以减少日常维护任务，有更多时间关注于改进工作。有了 Elastic Load Balancing，我们不必使用昂贵、复杂的负载均衡器，就能获得所需的功能。
>
> — Chad Marino，Kaplan 技术服务总监

现代化规划的另一个重要部分是选择数据库服务。需要在云中管理、扩展和优化 SQL Server 部署的客户可以使用 Amazon RDS，也可以在 Amazon EC2 上运行 SQL Server。

倾向于让 AWS 处理 SQL Server 数据库日常管理工作的客户可以选择 Amazon RDS，因为该服务能够让客户在云中轻松设置、操作和扩展关系数据库。Amazon RDS 能够自动执行安装、预置和管理磁盘、修补程序、升级次要版本、更换故障实例、备份和恢复 SQL Server 数据库等工作。此外，Amazon RDS 还提供跨多个可用区 (Multi-AZ) 的自动化同步复制，实现由 AWS 完全托管的高度可用和可扩展的环境。这使客户能够将精力集中于更高层次的任务上，如架构优化、查询优化、应用程序开发，而不必执行数据库维护和操作等这类毫无特色的工作。Amazon RDS for SQL Server 支持 Windows 身份验证，使客户能够更方便地访问和管理 Amazon RDS for SQL Server 实例。

Amazon RDS for SQL Server 支持 Microsoft SQL Server Express、Web、Standard 和 Enterprise 版本。SQL Server Express 没有额外的许可成本，适用于小型工作负载或概念验证部署。SQL Server Web 版本最适用于公用和可通过 Internet 访问的 Web 工作负载。SQL Server Standard 版本适用于大多数 SQL Server 工作负载，可在 Multi-AZ 模式下部署。SQL Server Enterprise 版本是功能最全的 SQL Server 版本，也能以 Multi-AZ 模式部署。

管理服务：Amazon CloudWatch、AWS CloudTrail、Run Command

> CSS 能够自动启动实例，这可减少约 75% 的项目启动时间。以前四天才能完成的工作，现在只需一天。我们并不总是从头开始重新构建 Web 和数据库服务器。我们可以克隆和复用映像。
>
> — Nick Morgan，Unilever 企业架构师

AWS 为企业提供全面的管理服务组合：

- **Amazon CloudWatch**：客户可以借助 Amazon CloudWatch 实时监控在 AWS 上运行的 AWS 资源和应用程序。CloudWatch 警报根据客户定义的规则发送通知或对所监控的资源自动进行更改。
- **AWS CloudTrail**：利用 AWS CloudTrail，客户通过获取其账户中的 AWS API 调用历史记录可以监控其在云上的 AWS 部署，包括通过 AWS 管理控制台、AWS 开发工具包、命令行工具、较高级 AWS 服务进行的 API 调用。此外，客户还能确定哪些用户和账户为支持 CloudTrail 的服务调用了 AWS API、调用方的 IP 地址和调用的发生时间。CloudTrail 可以集成到使用 API 的应用程序中，为组织自动创建跟踪、检查跟踪的状态和控制管理员启用和关闭 CloudTrail 日志记录的方式。
- **Amazon EC2 Run Command**：通过 Amazon EC2 Run Command 可以方便地运行 PowerShell 脚本，客户可借助它来自动执行常见的管理任务，如对数百个虚拟机应用补丁管理或配置更新。Run Command 与 AWS Identity and Access Management (IAM) 解决方案集成，可确保管理员能够访问仅针对其所有的设备的更新。所有更新均通过 AWS CloudTrail 的审计。

适用于 Microsoft System Center 的 AWS 加载项可扩展现有 System Center 实现的功能，能够配合 Microsoft System Center Operations Manager 及 Microsoft System Center Virtual Machine Manager 使用。安装后，客户可以使用相似的 System Center 界面查看和管理 AWS 云中的 Amazon EC2 for Microsoft Windows Server 资源，以及本地安装的 Windows Server。

通过 AWS Marketplace 完善解决方案

客户通常有首选 ISV 为其提供专用的软件解决方案，以增强客户安全、商业智能、存储等方面的能力。AWS Marketplace 是一个在线商店，客户通过它可以方便地发现、购买和部署其构建解决方案和运营其业务所需的软件和服务。AWS Marketplace 包含逾 35 个类别的 2600 多种软件和服务，简化了软件的许可和采购过程，客户可以通过简单的点击操作接受用户协议、选择定价选项、自动部署软件和相关的 AWS 资源。此外，AWS Marketplace 每月开一张发票，详细列明业务软件和 AWS 资源的使用情况，简化了客户的计费流程。AWS Marketplace 包含来自 SAP、Tableau、NetApp、Trend Micro、F5 Networks 等的产品。客户可通过 Marketplace 合作伙伴访问 Microsoft 应用程序，如 Microsoft Windows Server、Microsoft SQL Server、Microsoft SharePoint 自定义 AMI 等。

许可注意事项

客户可以选择在 AWS 云中使用新的或者现有 Microsoft 软件许可。对于新应用程序，客户可以购买包含许可的 Amazon EC2 或 Amazon RDS 实例。通过这种方法，客户直接从 AWS 获取新的、完全合规的 Windows Server 和 SQL Server 许可。客户可以按“即付即用”方式使用它们，无前期成本或长期投资。客户可以选择只包含 Microsoft Windows Server 的 AMI，或已安装 Windows Server 和 Microsoft SQL Server 的 AMI。包含客户端访问许可 (CAL)。

已购买 Microsoft 软件的客户具有“自带许可”(BYOL) 选项，Microsoft 通过软件保障计划依据 Microsoft 许可移动性政策授予客户这一选择权。Microsoft 的许可移动性计划允许已拥有 Windows Server 或 Microsoft SQL Server 许可的客户在 Amazon EC2 和 Amazon RDS 上运行其部署。此权益面向 Microsoft 批量许可 (VL) 客户提供，其 Windows Server 和 SQL Server 许可（当前包含 Standard 和 Enterprise 版本）由 Microsoft 软件保障合同涵盖。

如果客户的许可协议要求对套接字、核心或每个虚拟机进行控制，则客户可以使用 Amazon EC2 专用主机 — 为客户提供用于跟踪许可使用和合规情况并向 Microsoft 或 ISV 发送报告的硬件。

结论

本白皮书介绍了在 Amazon Web Services 上现代化应用程序的优势以及如何开始您的这一旅程。它说明了您可以如何受益于在 AWS 平台上运行企业应用程序、LOB 和数据库应用程序或为现代化计划开发新的应用程序。此外，若您要开始在 AWS 上现代化应用程序，我们推荐的 AWS 服务可供参考。