在企业环境中部署适用于 NetApp ONTAP 的 Amazon FSx

AWS 规范指引

AWS 规范指引: 在企业环境中部署适用于 NetApp ONTAP 的 Amazon FSx

Table of Contents

在企业环境中部署适用于 NetApp ONTAP 的 Amazon FSx

Luigi Seregni、Antonio Aga Rossi 和 Giulio Dipace，Amazon Web Services（AWS）

2023 年 8 月（文档历史记录）

将工作负载迁移到云可以支持组织发展，并帮助您适应不断变化的市场格局。云功能和特性可以提供可扩展性、敏捷性和韧性，从而提高应用程序的服务水平。

每年都会推出新的规则和条例，例如新的《国际财务报告准则（IFRS）》标准。不断演变的标准通常需要更高的计算能力，而这可能很难在本地实现。对存储吞吐量要求极高的高性能计算（HPC）应用程序是迁移到云或混合云环境的理想选择。

适用于 NetApp ONTAP 的 Amazon FSx 是一项云服务，它支持这些 HPC 应用程序的高吞吐量要求，并且向后兼容本地 ONTAP 工作负载。使用本指南，您可以在企业环境中部署功能齐全的适用于 ONTAP 的 FSx 解决方案。企业环境意味着本指南并不只关注适用于 ONTAP 的 FSx 服务。相反，它采用了整体视图，并提供了在复杂环境中部署此类文件系统的注意事项。

本指南还回顾了常见的部署挑战，例如 Active Directory 集成、服务账户部署、ONTAP 命令行问题排查和存储虚拟机（SVM）配置。

该指南提供了四个不同的部分：

- 架构：本章概述了使用适用于 ONTAP 的 FSx 的可能企业架构，描述了不同组件之间的交互以及合适的使用模式。
- 创建文件系统：本节列出了创建完全运行的适用于 ONTAP 的 FSx 环境的所有操作。我们提供了手动部署解决方案的分步准则。
- 最佳实践：本章根据在企业环境中部署适用于 ONTAP 的 FSx 期间吸取的经验教训提供建议和最佳实践。
- 常见问题：本节包含一系列问题，用于解决有关该技术的常见问题。

目标受众

本指南旨在帮助需要部署支持 HPC 工作负载和 Active Directory 集成的适用于 ONTAP 的 FSx 解决方案的云管理员和架构师。

目标

本指南可以帮助您和您的组织执行以下操作：

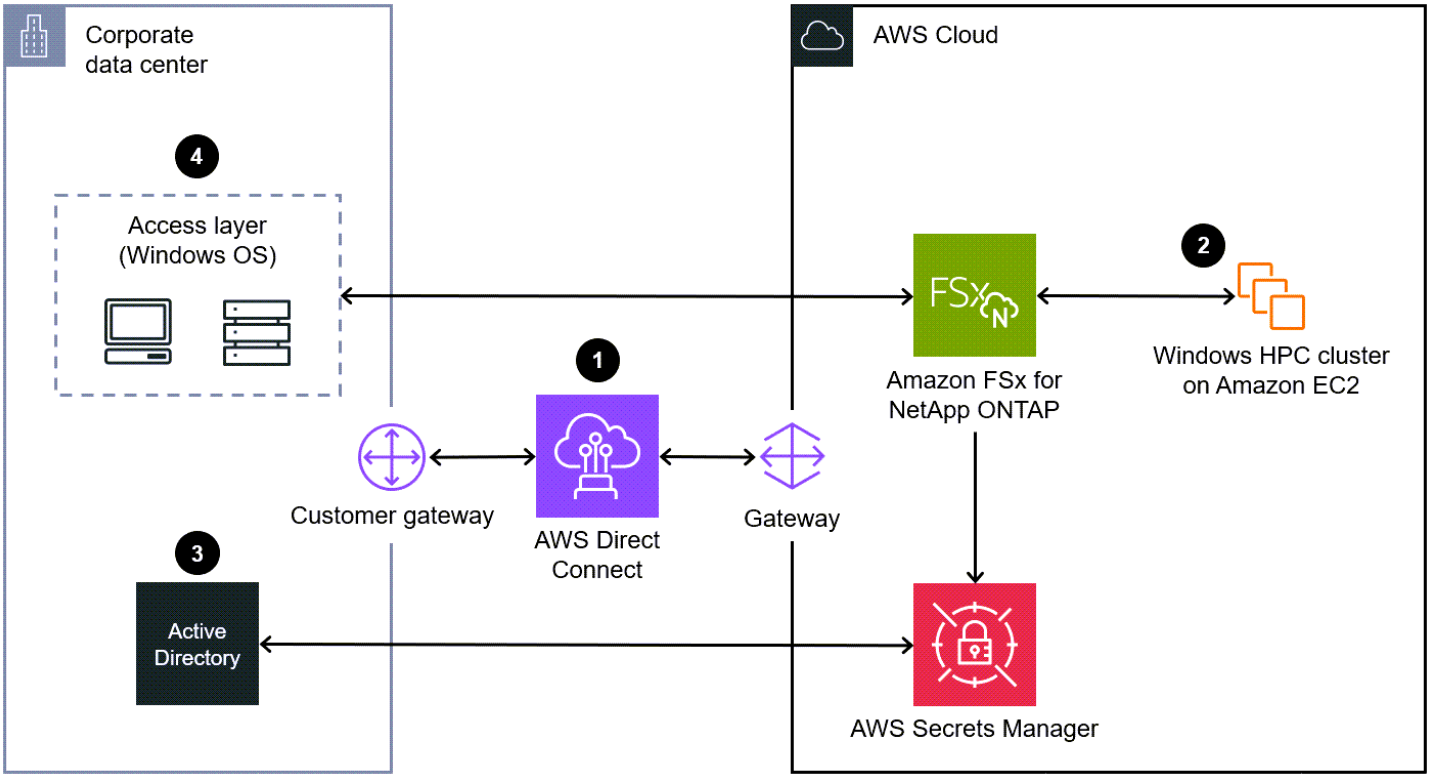
- 了解架构并在企业环境中部署功能齐全的适用于 ONTAP 的 FSx 解决方案
- 将适用于 ONTAP 的 FSx 与 Active Directory 集成
- 创建服务账户以在生产环境中将适用于 ONTAP 的 FSx 连接到 Active Directory
- 管理 Amazon FSx 的存储层
- 通过 ONTAP 命令行进行问题排查
- 排查存储虚拟机（SVM）的配置问题（NetApp 文档）
- 使用服务消息块（SMB）协议访问适用于 ONTAP 的 FSx 文件系统中的数据

在企业环境中部署适用于 ONTAP 的 FSx 的架构

适用于 NetApp ONTAP 的 Amazon FSx 是一种托管式存储服务，可帮助您在 AWS 云中启动和运行完全托管式 NetApp ONTAP 文件系统。适用于 ONTAP 的 FSx 支持 Windows 或 Linux 操作系统（OS），并且可以通过行业标准协议访问，例如网络文件系统（NFS）、服务器消息块（SMB）和互联网小型计算机系统接口（iSCSI）。此外，此文件系统支持压缩和重复数据删除，这可以降低存储成本。

本指南重点介绍 Windows 工作负载的部署。例如，您可以使用适用于 ONTAP 的 FSx 作为由数百个 Windows 节点组成的 HPC 第三方解决方案的共享存储。这些节点具有极高的写入和读取吞吐量要求，且已连接到网格调度器。

下图描述了在混合云环境中部署企业 HPC 工作负载和适用于 ONTAP 的 FSx 的典型示例。本指南中通篇引用了此架构。



以下是此架构的功能：

1. 本地数据中心和云环境通过使用 AWS Direct Connect 进行连接。
2. 运行 Windows 的 HPC 工作负载部署在 AWS 云中。
3. Active Directory 部署在本地环境中。

4. 在 Windows 上运行的访问层系统部署在本地环境中。

客户访问层

通过客户访问层，最终用户可以访问 AWS 云中的工作负载。Amazon WorkSpaces 或 Citrix 通常用于通过使用 SMB 挂载来访问应用程序和访问 Amazon FSx 中的数据。

Active Directory

通常，微软 Active Directory 是在本地安装和管理的。许多组织希望将适用于 ONTAP 的 FSx SVM 加入 Active Directory 域，以便在文件和文件夹级别提供用户身份验证和访问控制。然后，SMB 客户端可以使用其在 Active Directory 中的现有用户身份自行进行身份验证并访问 SVM 卷。有关更多信息，请参阅在适用于 ONTAP 的 FSx 中使用 Microsoft Active Directory。您必须制定适当的网络规则，以确保 SVM 可以到达 Active Directory 域。

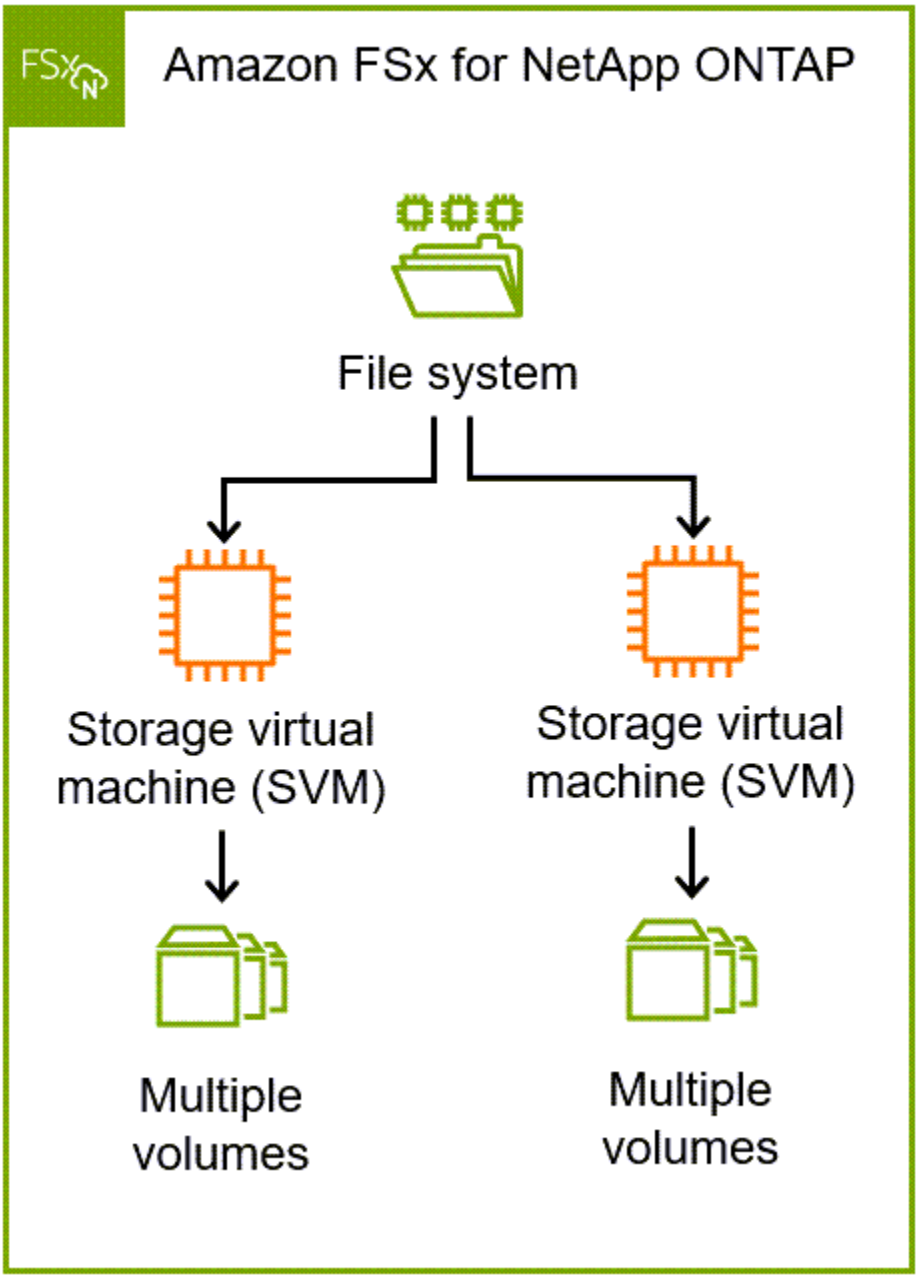
要允许 Amazon FSx 文件系统在托管式卷上创建、编辑和删除文件，您需要为 Active Directory 域创建一个服务账户。有关更多信息，请参阅向 Amazon FSx 服务账户委托权限。Active Directory 是许多企业组织的核心组件，部署新账户（即使权限有限）可能需要相当长的时间。

Amazon FSx 资源

以下是适用于 ONTAP 的 FSx 中的主要资源类型：

- 文件系统是主要的适用于 ONTAP 的 FSx 资源，类似于本地 NetApp ONTAP 集群。要进行问题排查，您可以使用 NetApp CLI 命令与文件共享端点建立 SSH 连接。本指南后面部分将提供有关排查命令问题的更多信息。
- 存储虚拟机（SVM）是一种独立的虚拟文件服务器，具有自己的管理和数据访问端点。适用于 ONTAP 的 FSx 与 Active Directory 域之间的集成在 SVM 级别进行管理。因此，如果您遇到有关 Active Directory 的错误，那么 SVM 是进行问题排查的好起点。
- 卷是用于组织数据和对数据进行分组的虚拟资源。这些是逻辑容器，其中存储的数据会消耗文件系统的物理容量。卷托管在 SVM 上。您可以为每个卷配置不同的分层策略。分层策略是功能强大的工具，可通过定义数据存储在性能优化的 SSD 层中还是存储在成本优化的容量层中，来帮助您管理性能和成本。

下图解释了适用于 ONTAP 的 FSx 文件系统的资源结构。Amazon FSx 完全管理所有组件。



您可以使用连接路径将多个卷加入单个逻辑命名空间（NetApp 文档）。对客户端而言，连接点看起来就像一个普通的目录。连接路径提供了使用多个卷的好处（例如对快照和迁移选项的精细控制），并且可以方便地通过单个接入点访问多个卷中的数据。

Amazon EC2 上的 Windows HPC 集群

就本指南而言，Amazon FSx 充当由 Amazon Elastic Compute Cloud（Amazon EC2）实例组成的关键、高吞吐量 Windows HPC 集群的存储层。在 Amazon EC2 上设置 HPC 集群有多种方法。有关示例方法，请参阅 Amazon EC2 文档中的教程：在 Amazon EC2 上设置 Windows HPC 集群。HPC 集

群计算节点（也称为 Worker 节点）通过 SMB 共享与 Amazon FSx 文件系统进行交互。您可以在计算节点上自动或手动创建 SMB 共享。

AWS Secrets Manager

企业架构通常使用基础设施即代码（IaC）工具来部署，例如 HashiCorp Terraform。安全最佳实践是不在 IaC 脚本中包含任何敏感信息。AWS Secrets Manager 通常用于存储敏感信息，例如 Active Directory 服务账户的密码。

创建已加入 Active Directory 的适用于 ONTAP 的 FSx 文件系统

本节包含有关在企业环境中创建适用于 NetApp ONTAP 的 Amazon FSx 文件系统并将存储虚拟机（SVM）加入本地数据中心的 Active Directory 域的部署说明。本章介绍以下高级流程：

- 预调配 Active Directory 服务账户：要允许文件系统在托管卷上创建、编辑和删除文件，您需要为 Active Directory 域创建一个服务账户。
- 设置适用于 ONTAP 的 FSx 文件系统：您可以设置适用于 ONTAP 的 FSx 文件系统、SVM 和卷。
- 监控适用于 ONTAP 的 FSx：您可以为适用于 ONTAP 的 FSx 使用情况和活动配置日志记录和监控。

预调配 Active Directory 服务账户

如果您想将适用于 NetApp ONTAP 的 Amazon FSx SVM 加入您的本地 Active Directory 域，则必须在 Amazon FSx 文件系统的整个生命周期内保持有效的 Active Directory 服务账户。Amazon FSx 必须能够完全管理文件系统并执行需要取消加入和重新加入 Active Directory 域的任务，例如更换出现故障的文件 SVM 或修补 NetApp ONTAP 软件。请确保 Amazon FSx 中的 Active Directory 配置（包括服务账户凭证）保持最新。

此服务账户必须在 Active Directory 中拥有以下权限：

- 将计算机加入域的权限
- 在您要加入文件系统的组织单元（OU）中，拥有以下权限：
  - 重置密码
  - 限制账户读取和写入数据
  - 写入 DNS 主机名
  - 写入服务主体名称
  - 创建和删除计算机对象
  - 读取和写入账户限制

Active Directory 域管理员可以使用 Active Directory 用户和计算机 MMC 管理单元手动创建服务账户。有关说明，请参阅适用于 ONTAP 的 FSx 文档中的向您的 Amazon FSx 服务账户委派权限。您也可以通过编程方式配置此账户。例如，您可以使用 PowerShell，如以下示例所示。

```
param(
    [string] $DomainName,
    [string] $Username, #Service Account username
    [string] $Firstname, #Service Account Firstname
    [string] $Lastname, #Service Account Lastname
    [string] $saOU, #OU where Service Account is created
    [string] $delegateOrganizationalUnit #OU where Service Account has delegation
)

#Retrieve Active Directory domain credentials of a Domain Admin
$DomainCredential = ...

#Import Active Directory PowerShell module
...

#Create Service Account in specified OU
New-Active DirectoryUser -Credential $DomainCredential -SamAccountName $Username -
UserPrincipalName "$Username@$DomainName" -Name "$Firstname $Lastname" -GivenName
 $Firstname -Surname $Lastname -Enabled $True -ChangePasswordAtLogon $False -
DisplayName "$Lastname, $Firstname" -Path $saOU -CannotChangePassword $True -
PasswordNotRequired $True
$user = Get-Active Directoryuser -Identity $Username
$userSID = [System.Security.Principal.SecurityIdentifier] $user.SID

#Connect to Active Directory drive
Set-Location Active Directory:

$ACL = Get-Acl -Path $delegateOrganizationalUnit
$Identity = [System.Security.Principal.IdentityReference] $userSID

#GUID of Active Directory Class
$Computers = [GUID]"bf967a86-0de6-11d0-a285-00aa003049e2"
$ResetPassword = [GUID]"00299570-246d-11d0-a768-00aa006e0529"
$ValidatedDNSHostName = [GUID]"72e39547-7b18-11d1-adef-00c04fd8d5cd"
$ValidatedSPN = [GUID]"f3a64788-5306-11d1-a9c5-0000f80367c1"
$AccountRestrictions = [GUID]"4c164200-20c0-11d0-a768-00aa006e0529"

#Delegation list
$rules = @()
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($Identity,
 "CreateChild, DeleteChild", "Allow", $Computers, "All"))
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($Identity,
 "ExtendedRight", "Allow", $ResetPassword, "Descendents", $Computers))
```

```
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($Identity,
 "ReadProperty, WriteProperty", "Allow", $AccountRestrictions, "Descendents",
 $Computers))
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($userSID,
 "Self", "Allow", $ValidatedDNSHostName, "Descendents", $Computers))
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($userSID,
 "Self", "Allow", $ValidatedSPN, "Descendents", $Computers))

#Set delegation
foreach($rule in $rules) {
    $ACL.AddAccessRule($rule)
}
Set-Acl -Path $delegateOrganizationalUnit -AclObject $ACL
```

设置适用于 ONTAP 的 FSx 文件系统

适用于 NetApp ONTAP 的 Amazon FSx 文档包含有关在 AWS 管理控制台中使用快速创建或标准创建选项设置文件共享的说明。本指南包含针对需要支持 HPC 工作负载和 Active Directory 集成的企业的更多建议和指引。

有关在 AWS 管理控制台中创建适用于 ONTAP 的 FSx 文件系统的说明，请参阅创建适用于 ONTAP 的 FSx 文件系统。在每个部分中，请注意以下针对企业环境的设置建议和注意事项。

文件系统详细信息部分

1. 对于部署类型，请选择以下选项之一：
   - 为生产工作负载选择多可用区。此选项有助于在无法访问可用区时保持数据可用性。
   - 选择单可用区可用于灾难恢复、非生产工作负载，或者应用程序层中已内置复制功能且不需要额外存储级冗余的工作负载。对于这些类型的工作负载，此选项具有成本效益。

   有关配置部署类型的更多信息和建议，请参阅本指南的最佳实践部分中的选择可用区部署选项的最佳实践。
2. 对于预调配 SSD IOPS，请选择以下选项之一：
   - 如果您希望 Amazon FSx 自动为每 GiB SSD 存储预调配 3 IOPS，每个文件系统最多可预调配 16 万 SSD IOPS，请选择自动。
   - 如果要指定 IOPS 数，请选择用户预调配模式。如果预调配更高的 IOPS 级别，您需要为高于当月所含费率的平均预调配 IOPS 付费，以 IOPS 月数为单位。

有关更多信息，请参阅适用于 ONTAP 的 FSx 文档中的存储容量和 IOPS、更新存储空间和 IOPS 时的注意事项和存储容量对性能的影响。

默认存储虚拟机配置部分

1. 对于根卷安全风格，请选择下列选项之一：
   - 如果您计划主要从基于 Linux 的客户端（NFS 协议）访问文件系统，请选择 Unix。
   - 如果您计划主要从基于 Windows 的客户端（SMB 协议）访问文件系统，请选择 NTFS。
   - 如果您计划从基于 Linux 和基于 Windows 的客户端平等访问文件系统，请选择混合。此为高级设置。

   有关这些设置的更多信息，请参阅安全风格及其影响（NetApp 文档）。
2. 对于 Active Directory，选择加入 Active Directory。
3. 对于 NetBIOS 名称，将为您的 SVM 创建的 Active Directory 计算机对象的 NetBIOS 名称。这通常与 SVM 名称相同，但可能有所不同。NetBIOS 名称不超过 15 个字符。
4. 对于 Active Directory 域名，请输入 Active Directory 的完全限定域名。域名不超过 255 个字符。
5. 对于 DNS 服务器 IP 地址，请输入域的 DNS 服务器的 IPv4 地址。您最多可以输入三个 IP 地址。
6. 对于服务账户用户名和服务账户密码，请输入现有 Active Directory 中服务账户的用户名和密码。这是您之前在本指南的预调配 Active Directory 服务账户中设置的服务账户。
7. 对于组织单元（OU），请输入要将文件系统加入的组织单元的可分辨路径名。
8. 对于委托文件系统管理员组，输入您的 Active Directory 中可以管理您的文件系统的组的名称。默认组为 `Domain Admins`。

“默认卷配置”部分

1. 对于卷名称，输入卷的名称。名称不能超过 203 个字符，接受字母数字和下划线（_）字符。
2. 对于连接路径，请输入要将卷挂载到文件系统内的位置。该名称中必须包含前导正斜杠，例如 `/vol1`。有关更多信息，请参见本指南的 Amazon FSx 资源 部分。
3. 对于卷大小，请输入卷的存储容量，以兆字节（MiB）为单位。输入 20–104857600（100 TiB）范围内的任意整数。
4. 对于存储效率，选择是否启用存储效率功能，例如重复数据删除、压缩和紧凑化。有关更多信息，请参阅适用于 ONTAP 的 FSx 文档中的存储效率。如果这些效率功能与您的 HPC 工作负载兼容，我们建议在企业环境中使用这些功能。

5. 对于容量池分层策略，请为卷选择分层策略。有关分层策略的更多信息和建议，请参阅本指南的最佳实践部分中的存储层和分层策略的最佳实践。

监控适用于 ONTAP 的 FSx

记录和监控适用于 NetApp ONTAP 的 Amazon FSx 使用情况和活动是一种最佳实践，因为它可以帮助您了解文件系统的状态。您可以使用日志数据对影响系统可靠性、操作和效率的任何问题进行问题排查。这在企业环境中尤其重要，因为文件系统的问题可能会危及任务处理结果、产生不准确的结果，或违反服务等级协议。这可能会导致 HPC 工作负载所有者被罚款，或者导致使用不正确的数据做出决策。有关监控企业环境的最佳实践，请参阅本指南中的监控适用于 ONTAP 的 FSx 文件系统的最佳实践。

您可以使用各种 AWS 和第三方工具与服务来记录及监控适用于 ONTAP 的 FSx 使用情况和活动。例如，您可以使用 Amazon CloudWatch、ONTAP 中的事件管理系统（EMS）、NetApp Cloud Insights 服务、NetApp Harvest、NetApp Grafana 和 AWS CloudTrail。有关更多信息，请参阅监控适用于 NetApp ONTAP 的 Amazon FSx。

企业环境中适用于 ONTAP 的 FSx 部署的最佳实践

本节提供在企业环境中部署和运行适用于 NetApp ONTAP 的 Amazon FSx 的最佳实践和注意事项。这些建议是根据 AWS 专业服务团队的经验提出的。

除了本指南中的建议外，请遵循以下最佳实践：

- 使用 Active Directory 的最佳实践（适用于 ONTAP 的 FSx 文档）
- 数据保护（适用于 ONTAP 的 FSx 文档）
- IAM 中的安全最佳实践 [AWS Identity and Access Management（IAM）文档]
- NetApp ONTAP FlexGroup 卷的最佳实践和实施指南（NetApp 文档）

存储层和分层策略的最佳实践

存储层是适用于 NetApp ONTAP 的 Amazon FSx 文件系统的物理存储介质。提供以下存储层：

- SSD 层是专为活跃数据而设计的高性能固态硬盘（SSD）存储，您可以为此层选择存储大小。
- 容量池层是完全弹性的存储，针对不常访问的数据进行了成本优化。SSD 层的速度明显快于容量池层。适用于 ONTAP 的 FSx SSD 存储可提供亚毫秒级的文件操作延迟，容量池层可提供数十毫秒的延迟。

有关这些层的更多信息，请参阅适用于 ONTAP 的 FSx 存储层。

您在卷级别配置的分层策略决定 SSD 层中存储的数据是否以及何时过渡到容量池层。适用于 ONTAP 的 FSx 提供四种不同的分层策略：仅限快照、自动、全部和无。有关每个策略的更多信息，请参阅适用于 ONTAP 的 FSx 文档中的分层策略。

在为文件共享中的卷设置分层策略时，考虑以下建议：

- HPC 工作负载应访问 SSD 层中的数据，以防止出现性能瓶颈。对于 HPC 工作负载访问的卷，我们建议将分层策略设置为无或仅限快照。
- 将数据迁移到文件共享时，我们建议将目标卷分层策略设置为全部。这降低了成本，因为所有数据都会迁移到 SSD 层，然后立即迁移到容量池层。此外，如果 SSD 层容量使用率达到 98% 或更高，则将停止向该层写入数据。将分层策略设置为全部可防止在迁移期间达到此分层阈值。迁移完成后，您可以更改分层策略以平衡性能和成本。有关更多信息，请参阅 Migrating file shares to Amazon FSx for NetApp ONTAP using AWS DataSync（AWS 博客文章）。

使用 NetApp ONTAP 最大目录大小的最佳实践

maxdirsize（NetApp 文档）是一项 NetApp ONTAP 设置，它决定了每个目录中可以存储的最大文件数。此设置适用于卷，因此卷中的所有目录都具有相同的 `maxdirsize` 设置。默认值为 320 MB，这允许您在每个目录中最多存储 430 万个文件。

您可以增加 `maxdirsize` 值以支持更大的目录。增加该值后，如果不重新创建目录，就无法减少该值。由于目录是在内存中加载的，因此需要在目录的大小和文件系统的性能之间进行权衡。您只能通过测试来验证自定义设置。NetApp 建议您将此值保留为默认值。有关更多信息，请参阅 NetApp ONTAP FlexGroup 卷的最佳实践和实施指南（NetApp 文档）。

如果您自定义 `maxdirsize` 设置，则可以使用以下公式来确定单个文件夹中可以容纳的文件数。

```
max number of files in each directory = maxdirsize in MB × 53 × 0,25
```

监控适用于 ONTAP 的 FSx 文件系统的最佳实践

与其他 AWS 服务类似，适用于 ONTAP 的 FSx 已与 Amazon CloudWatch 集成。CloudWatch 可帮助您近乎实时地监控 AWS 资源的指标。文件系统和卷级别提供了指标，这些资源的详细监控指标可帮助您通过更精细的报告详细信息对其进行分析。有关更多信息，请参阅适用于 ONTAP 的 FSx 文档中的使用 Amazon CloudWatch 进行监控。使用 CloudWatch 监控适用于 ONTAP 的 FSx 时，请考虑以下建议：

- 我们建议您使用 `StorageUsed` 文件系统指标，以便您可以按存储层筛选监控结果。
- 使用 `StorageCapacity` 文件系统指标配置 CloudWatch 告警，该告警会在固态硬盘层容量使用率超过 80% 时通知您。这可确保卷的分层功能正常运行，并有助于保持处理新数据的容量。有关更多信息，请参阅分层阈值。

选择可用区部署选项的最佳实践

您可以在单可用区或多可用区配置中部署适用于 NetApp ONTAP 的 Amazon FSx。每个选项均提供不同级别的可用性和持久性。有关这些部署选项的更多信息，请参阅适用于 ONTAP 的 FSx 文档中的可用性和持久性。

多可用区以主动-被动配置部署适用于 ONTAP 的 FSx 文件系统。因此，所有连接到文件共享的服务器仅使用主可用区中的端点。辅助可用区中的端点仅用于失效转移，除非主可用区出现故障，否则不会用于读取或写入。

创建适用于 ONTAP 的 FSx 文件系统后，您无法更改可用区部署选项。要更改可用区配置，您必须创建一个新的文件系统，然后将数据迁移到新的文件系统。

但是，即使您使用单可用区选项部署了文件共享，仍然可以从其他可用区访问该文件共享。您的网络配置（例如安全组和网络访问控制列表）必须允许客户端连接到文件系统端点。使用此方法，每个方向的跨可用区流量（读取和写入）都会产生费用。有关更多信息，请参阅适用于 NetApp ONTAP 的 Amazon FSx 定价。

选择部署选项时，您必须在多可用区配置的韧性和单可用区配置的性能之间选择。如果适合您的使用案例，我们建议您选择多可用区选项，因为它可提供高可用性。但是，单可用区选项可能更具成本效益，且可以减少延迟。考虑 HPC 工作负载及其能否承受额外的延迟。

常见问题

对于适用于 ONTAP 的 FSx 卷而言，精简预调配意味着什么？

一般而言，精简预调配意味着系统使用虚拟化技术显示的可用资源多于实际预调配的资源。它就像银行的现金储备一样，实际存放在银行的金额少于银行账户的总金额。在适用于 NetApp ONTAP 的 Amazon FSx 中创建卷时，不会提前预留存储空间。当您向其添加数据时，它的大小会逐渐增加。有关更多信息，请参阅适用于 ONTAP 的 FSx 存储层。

适用于 ONTAP 的 FSx 支持哪些协议？

适用于 ONTAP 的 FSx 文件系统可通过网络文件系统（NFS）、服务器消息块（SMB）和互联网小型计算机系统接口（iSCSI）协议进行访问。有关更多信息，请参阅适用于 ONTAP 的 FSx 文档中的访问数据。

我在 Windows 环境中使用适用于 ONTAP 的 FSx。启用与 Active Directory 的集成是否有任何先决条件？

是，您需要在 Active Directory 域上创建一个服务账户。有关更多信息，请参阅本指南中的预调配 Active Directory 服务账户。您还需要确保网络连接正常。设置文件系统时，请勿忘记指定要加入的组织单位（OU）。有关更多信息，请参阅适用于 ONTAP 的 FSx 文档中的将 SVM 加入自行管理的 Microsoft AD 的先决条件。

我是否可以更改卷分层策略？

是，您可以随时更改分层策略。有关更多信息，请参阅 Amazon FSx 文档中的设置卷的分层策略。

文件系统上的分层策略和写入操作不起作用，指标显示 SSD 存储层利用率大于 98%。我应该怎么办？

当 SSD 存储层的利用率达到或高于 98% 时，所有分层功能和写入操作都会停止。有关更多信息，请参阅 Amazon FSx 文档中的分层阈值。要恢复操作，请增加 SSD 存储容量。考虑更改分层策略，以在 SSD 层中保留更少的数据。有关更多信息，请参阅 Amazon FSx 文档中的管理卷存储容量和设置卷的分层策略。

多可用区部署是否支持主动-主动配置？

否，多可用区部署是一种主动-被动配置。有关更多信息，请参阅本指南中的选择可用区部署选项的最佳实践。

适用于 ONTAP 的 FSx 的单可用区和多可用区部署的价格是否相同？

否，多可用区配置的成本大约是单可用区配置的两倍。对于单可用区部署，跨可用区流量会发生更改。有关更多信息，请参阅适用于 NetApp ONTAP 的 Amazon FSx 定价。

资源

适用于 NetApp ONTAP 的 Amazon FSx 文档

- 存储层
- 支持的客户端
- 管理卷
- 管理 SMB 共享
- 将适用于 ONTAP 的 FSx SVM 加入 Active Directory 域的最佳实践
- 卷数据分层和阈值
- 用于 Amazon CloudWatch 监控的文件系统指标
- TieringPolicy（API 参考）

其他 AWS 资源

- 选择 AWS 存储服务
- 适用于 NetApp ONTAP 的 Amazon FSx 定价
- Migrating file shares to Amazon FSx for NetApp ONTAP using AWS DataSync（AWS 博客文章）

NetApp 资源

- NetApp ONTAP FlexGroup 卷：最佳实践和实施指南（NetApp PDF）
- 什么是连接路径（NetApp 知识库）
- 什么是 maxdirsize（NetApp 知识库）

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
初次发布	—	2023 年 8 月 29 日

AWS 规范指引术语表

以下是《AWS 规范指引》提供的策略、指南和模式中常用的术语。若要推荐词条，请使用术语表末尾的提供反馈链接。

数字

7 R

将应用程序迁移到云中的 7 种常见迁移策略。这些策略以 Gartner 于 2011 年确定的 5 R 为基础，包括以下内容：

- 重构/重新架构：充分利用云原生功能来提高敏捷性、性能和可扩展性，以迁移应用程序并修改其架构。这通常涉及到移植操作系统和数据库。示例：将本地 Oracle 数据库迁移到 Amazon Aurora PostgreSQL 兼容版。
- 更换平台：将应用程序迁移到云中，并进行一定程度的优化，以利用云功能。示例：将本地 Oracle 数据库迁移到 AWS 云中的 Amazon Relational Database Service（Amazon RDS）for Oracle。
- 重新购买：转换到其他产品，通常是从传统许可转向 SaaS 模式。示例：将客户关系管理（CRM）系统迁移到 Salesforce.com。
- 重新托管（直接迁移）：将应用程序迁移到云中，无需进行任何更改即可利用云功能。示例：将本地 Oracle 数据库迁移到 AWS 云中 EC2 实例上的 Oracle。
- 重新放置（虚拟机监控器级直接迁移）：将基础设施迁移到云中，无需购买新硬件、重写应用程序或修改现有操作。您将服务器从本地平台迁移到同一平台的云服务中。示例：将 Microsoft Hyper-V 应用程序迁移到 AWS。
- 保留（重访）：将应用程序保留在源环境中。其中可能包括需要进行重大重构的应用程序，并且您希望将工作推迟到以后，以及您希望保留的遗留应用程序，因为迁移它们没有商业上的理由。
- 停用：停用或删除源环境中不再需要的应用程序。

A

ABAC

请参阅基于属性的访问控制。

抽象服务

请参阅托管服务。

ACID

请参阅原子性、一致性、隔离性、持久性。

主动-主动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步（通过使用双向复制工具或双写操作），两个数据库都在迁移期间处理来自连接应用程序的事务。这种方法支持小批量、可控的迁移，而不需要一次性割接。它比主动-被动迁移更灵活，但工作量更大。

主动-被动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步，但在将数据复制到目标数据库时，只有源数据库处理来自连接应用程序的事务。目标数据库在迁移期间不接受任何事务。

聚合函数

一种 SQL 函数，它对一组行进行操作并计算该组的单个返回值。聚合函数的示例包括 SUM 和 MAX。

AI

请参阅人工智能。

AIOps

请参阅人工智能运营。

匿名化

永久删除数据集中个人信息的过程。匿名化可以帮助保护个人隐私。匿名化数据不再被视为个人数据。

反模式

一种用于解决反复出现的问题的常用解决方案，而在这类问题中，此解决方案适得其反、无效或不如替代方案有效。

应用程序控制

一种安全方法，仅允许使用经批准的应用程序，以帮助保护系统免受恶意软件的侵害。

应用程序组合

有关组织使用的每个应用程序的详细信息的集合，包括构建和维护该应用程序的成本及其业务价值。这些信息是产品组合发现和分析过程的关键，有助于识别需要进行迁移、现代化和优化的应用程序并确定其优先级。

人工智能（AI）

计算机科学领域致力于使用计算技术执行通常与人类相关的认知功能，例如学习、解决问题和识别模式。有关更多信息，请参阅什么是人工智能？

人工智能运营（AIOps）

使用机器学习技术解决运营问题、减少运营事故和人为干预以及提高服务质量的过程。有关如何在 AWS 迁移策略中使用 AIOps 的更多信息，请参阅运营集成指南。

非对称加密

一种加密算法，使用一对密钥，一个公钥用于加密，一个私钥用于解密。您可以共享公钥，因为它不用于解密，但对私钥的访问应受到严格限制。

原子性、一致性、隔离性、持久性（ACID）

一组软件属性，即使在出现错误、电源故障或其他问题的情况下，也能保证数据库的数据有效性和操作可靠性。

基于属性的访问权限控制（ABAC）

根据用户属性（如部门、工作角色和团队名称）创建精细访问权限的做法。有关更多信息，请参阅 AWS Identity and Access Management（IAM）文档中的有关 AWS 的 ABAC。

权威数据源

存储主要数据版本的位置，被认为是最可靠的信息源。您可以将数据从权威数据源复制到其他位置，以便处理或修改数据，例如对数据进行匿名化、编辑或假名化。

可用区

一个 AWS 区域 中的不同位置，用于与其他可用区的故障隔离，并向同一区域中的其他可用区提供低成本、低延迟的网络连接。

AWS 云采用框架（AWS CAF）

AWS 的准则和最佳实践框架，旨在帮助组织制定高效且有效的计划来成功迁移到云。AWSCAF 将指导原则分为六个重点领域（角度）：业务、人员、治理、平台、安全和运营。业务、人员和治理角度侧重于业务技能和流程；平台、安全和运营角度侧重于技术技能和流程。例如，人员角度针对

的是负责人力资源（HR）、人员配置职能和人员管理的利益相关者。从这个角度来看，AWS CAF 为人员发展、培训和沟通提供了指导，帮助组织为成功采用云做好准备。有关更多信息，请参阅 AWS CAF 网站和 AWS CAF 白皮书。

AWS Workload Qualification Framework（AWS WQF）

一种评估数据库迁移工作负载、推荐迁移策略并提供工作量估算的工具。AWSWQF 包含在 AWS Schema Conversion Tool（AWS SCT）中。它用来分析数据库架构和代码对象、应用程序代码、依赖关系和性能特征，并提供评测报告。

B

恶意机器人

一种旨在扰乱或伤害个人或组织的机器人。

BCP

请参阅业务连续性计划。

行为图

一段时间内资源行为和交互的统一交互式视图。您可以使用 Amazon Detective 的行为图来检查失败的登录尝试、可疑的 API 调用和类似的操作。有关更多信息，请参阅 Detective 文档中的行为图中的数据。

大端序系统

一个先存储最高有效字节的系统。另请参阅字节顺序。

二进制分类

一种预测二进制结果（两个可能的类别之一）的过程。例如，您的 ML 模型可能需要预测诸如“该电子邮件是否为垃圾邮件？”或“这个产品是书还是汽车？”之类的问题

bloom 筛选条件

一种概率性、内存高效的数据结构，用于测试元素是否为集合的成员。

蓝/绿部署

一种部署策略，您可以创建两个独立但完全相同的环境。在一个环境中运行当前应用程序版本（蓝色），在另一个环境中运行新应用程序版本（绿色）。此策略可帮助您在影响最小的情况下快速回滚。

自动程序

一种通过互联网运行自动任务并模拟人类活动或交互的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的 Web 爬网程序。还有一些被称为恶意机器人的机器人，其目的是扰乱或伤害个人或组织。

僵尸网络

被恶意软件感染并受单方（称为僵尸网络控制者或僵尸网络操作者）控制的僵尸网络。僵尸网络是最著名的扩展机器人及其影响力的机制。

分支

代码存储库的一个包含区域。在存储库中创建的第一个分支是主分支。您可以从现有分支创建新分支，然后在新分支中开发功能或修复错误。为构建功能而创建的分支通常称为功能分支。当功能可以发布时，将功能分支合并回主分支。有关更多信息，请参阅关于分支（GitHub 文档）。

紧急（break-glass）访问

在特殊情况下，通过批准的流程，用户可以快速访问他们通常没有访问权限的 AWS 账户。有关更多信息，请参阅 AWS Well-Architected 指引中的 Implement break-glass procedures 指标。

棕地策略

您环境中的现有基础设施。在为系统架构采用棕地策略时，您需要围绕当前系统和基础设施的限制来设计架构。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

缓冲区缓存

存储最常访问的数据的内存区域。

业务能力

企业如何创造价值（例如，销售、客户服务或营销）。微服务架构和开发决策可以由业务能力驱动。有关更多信息，请参阅在 AWS 上运行容器化微服务白皮书中的围绕业务能力进行组织部分。

业务连续性计划（BCP）

一项计划，旨在应对大规模迁移等破坏性事件对运营的潜在影响，并使企业能够快速恢复运营。

C

CAF

请参阅 AWS Cloud Adoption Framework。

金丝雀部署

缓慢而渐进地向最终用户发布版本。当您确信无误后，即可部署新版本，并完全替换当前版本。

CCoE

请参阅云卓越中心。

CDC

请参阅更改数据捕获。

更改数据捕获（CDC）

跟踪数据来源（如数据库表）的更改并记录有关更改的元数据的过程。您可以将 CDC 用于各种目的，例如审计或复制目标系统中的更改以保持同步。

混沌工程

故意引入故障或破坏性事件来测试系统的韧性。您可以使用 AWS Fault Injection Service（AWS FIS）来执行实验，对您的 AWS 工作负载施加压力并评估其响应。

CI/CD

请参阅持续集成和持续交付。

分类

一种有助于生成预测的分类流程。分类问题的 ML 模型预测离散值。离散值始终彼此不同。例如，一个模型可能需要评估图像中是否有汽车。

客户端加密

在目标 AWS 服务 接收数据之前，在本地对数据进行加密。

云卓越中心（CCoE）

一个多学科团队，负责推动整个组织的云采用工作，包括开发云最佳实践、调动资源、制定迁移时间表、领导组织完成大规模转型。有关更多信息，请参阅 AWS 云企业战略博客上的 CCoE 文章。

云计算

通常用于远程数据存储和 IoT 设备管理的云技术。云计算通常连接到边缘计算技术。

云运营模型

在 IT 组织中，一种用于构建、完善和优化一个或多个云环境的运营模型。有关更多信息，请参阅构建您的云运营模型。

云采用阶段

组织迁移到 AWS 云中时通常会经历四个阶段：

- 项目 - 出于概念验证和学习目的，开展一些与云相关的项目
- 基础 - 进行基础投资以扩大云采用率（例如，创建登录区、定义 CCoE、建立运营模型）
- 迁移 - 迁移单个应用程序
- 重塑 - 优化产品和服务，在云中创新

Stephen Orban 在 AWS 云企业战略博客上发表的博客文章 The Journey Toward Cloud-First & the Stages of Adoption 中对这些阶段进行了定义。有关它们与 AWS 迁移策略的关系的信息，请参阅迁移准备指南。

CMDB

请参阅配置管理数据库。

代码存储库

通过版本控制过程存储和更新源代码和其他资产（如文档、示例和脚本）的位置。常见的云存储库包括 GitHub 或 Bitbucket Cloud。每个版本的代码都称为一个分支。在微服务结构中，每个存储库都专门用于一个功能。单个 CI/CD 管线可以使用多个存储库。

冷缓存

一种空的、填充不足或包含过时或不相关数据的缓冲区缓存。这会影响性能，因为数据库实例必须从主内存或磁盘读取，这比从缓冲区缓存读取要慢。

冷数据

很少访问的数据，且通常是历史数据。查询此类数据时，通常可以接受慢速查询。将这些数据转移到性能较低且成本更低的存储层或类别可以降低成本。

计算机视觉（CV）

AI 的一个领域，它使用机器学习来分析和提取数字图像和视频等视觉格式中的信息。例如，Amazon SageMaker AI 为 CV 提供图像处理算法。

配置漂移

对于工作负载而言，一种偏离预期状态的配置更改。这可能会导致工作负载变得不合规，且通常是渐进的，不是故意的。

配置管理数据库（CMDB）

一种存储库，用于存储和管理有关数据库及其 IT 环境的信息，包括硬件和软件组件及其配置。您通常在迁移的产品组合发现和分析阶段使用来自 CMDB 的数据。

合规性包

一系列 AWS Config 规则和修复操作，您可以将其组合起来以自定义合规性和安全性检查。您可以使用 YAML 模板，将合规性包作为单个实体部署到 AWS 账户 区域中，或者跨组织部署。有关更多信息，请参阅 AWS Config 文档中的合规性包。

持续集成和持续交付（CI/CD）

自动执行软件发布过程的源代码、构建、测试、暂存和生产阶段的过程。CI/CD 通常被描述为管线。CI/CD 可以帮助您实现流程自动化、提高工作效率、改善代码质量并加快交付速度。有关更多信息，请参阅持续交付的优势。CD 也可以表示持续部署。有关更多信息，请参阅持续交付与持续部署。

CV

请参阅计算机视觉。

D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

根据网络中数据的关键性和敏感性对其进行识别和分类的过程。它是任何网络安全风险管理策略的关键组成部分，因为它可以帮助您确定对数据的适当保护和保留控制。数据分类是 AWS Well-Architected Framework 中安全支柱的一个组成部分。有关详细信息，请参阅数据分类。

数据漂移

生产数据与用来训练机器学习模型的数据之间的有意义差异，或者输入数据随时间推移的有意义变化。数据漂移可能降低机器学习模型预测的整体质量、准确性和公平性。

传输中数据

在网络中主动移动的数据，例如在网络资源之间移动的数据。

数据网格

一种架构框架，可提供分布式、去中心化的数据所有权以及集中式管理和治理。

数据最少化

仅收集并处理绝对必要数据的原则。在 AWS 云 中践行数据最少化可以降低隐私风险、成本和您的分析碳足迹。

数据边界

AWS 环境中的一组预防性护栏，可帮助确保只有可信身份才能访问来自预期网络的可信资源。有关更多信息，请参阅在 AWS 上构建数据边界。

数据预处理

将原始数据转换为 ML 模型易于解析的格式。预处理数据可能意味着删除某些列或行，并处理缺失、不一致或重复的值。

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

一种支持商业智能（例如分析）的数据管理系统。数据仓库通常包含大量历史数据，通常用于查询和分析。

数据库定义语言（DDL）

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言（DML）

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

请参阅数据库定义语言。

深度融合

组合多个深度学习模型进行预测。您可以使用深度融合来获得更准确的预测或估算预测中的不确定性。

深度学习

一个 ML 子字段使用多层人工神经网络来识别输入数据和感兴趣的目标变量之间的映射。

深度防御

一种信息安全方法，经过深思熟虑，在整个计算机网络中分层实施一系列安全机制和控制措施，以保护网络及其中数据的机密性、完整性和可用性。当您在 AWS 上采用此策略时，您可以在 AWS Organizations 结构的不同层添加多种控制措施，来保护资源。例如，深度防御方法可能将多因素身份验证、网络分段和加密结合起来。

委托管理员

在 AWS Organizations 中，兼容服务可以注册 AWS 成员账户来管理组织的账户，并管理该服务的权限。此账户被称为该服务的委托管理员。有关更多信息和兼容服务列表，请参阅 AWS Organizations 文档中使用 AWS Organizations 的服务。

后

使应用程序、新功能或代码修复在目标环境中可用的过程。部署涉及在代码库中实现更改，然后在应用程序的环境中构建和运行该代码库。

开发环境

请参阅环境。

侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出提醒。这些控制是第二道防线，提醒您注意绕过现有预防性控制的安全事件。有关更多信息，请参阅在 AWS 上实施安全控制中的侦测性控制。

开发价值流映射（DVSM）

用于识别对软件开发生命周期中的速度和质量产生不利影响的限制因素并确定其优先级的流程。DVSM 扩展了最初为精益生产实践设计的价值流映射流程。其重点关注在软件开发过程中创造和转移价值所需的步骤和团队。

数字孪生

真实世界系统的虚拟再现，如建筑物、工厂、工业设备或生产线。数字孪生支持预测性维护、远程监控和生产优化。

维度表

星型架构中的一种较小的表，其中包含事实表中定量数据的数据属性。维度表属性通常是文本字段或行为类似于文本的离散数字。这些属性通常用于查询约束、筛选和结果集标注。

灾难

阻止工作负载或系统在其主要部署位置实现其业务目标的事件。这些事件可能是自然灾害、技术故障或人为操作的结果，例如无意的配置错误或恶意软件攻击。

灾难恢复（DR）

您用来最大程度地减少由灾难造成的停机时间和数据丢失的策略和流程。有关更多信息，请参阅 AWS 上工作负载的灾难恢复：AWS Well-Architected Framework 中的云中恢复。

DML

请参阅数据库操作语言。

领域驱动设计

一种开发复杂软件系统的方法，通过将其组件连接到每个组件所服务的不断发展的领域或核心业务目标。Eric Evans 在其著作领域驱动设计：软件核心复杂性应对之道（Boston: Addison-Wesley Professional, 2003）中介绍了这一概念。有关如何将领域驱动设计与 strangler fig 模式结合使用的信息，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

DR

请参阅灾难恢复。

漂移检测

跟踪与基准配置的偏差。例如，您可以使用 AWS CloudFormation 来检测系统资源中的漂移，也可以使用 AWS Control Tower 来检测登录区中可能会影响监管要求合规性的更改。

DVSM

请参阅开发价值流映射。

E

EDA

请参阅探索性数据分析。

EDI

请参阅电子数据交换。

边缘计算

该技术可提高位于 IoT 网络边缘的智能设备的计算能力。与云计算比较时，边缘计算可以减少通信延迟并缩短响应时间。

电子数据交换（EDI）

组织之间业务文件的自动交换。有关更多信息，请参阅什么是电子数据交换。

加密

一种将人类可读的纯文本数据转换为加密文字的计算流程。

加密密钥

由加密算法生成的随机位的加密字符串。密钥的长度可能有所不同，而且每个密钥都设计为不可预测且唯一。

字节顺序

字节在计算机内存中的存储顺序。大端序系统先存储最高有效字节。小端序系统先存储最低有效字节。

端点

请参阅服务端点。

端点服务

一种可以在虚拟私有云（VPC）中托管，与其他用户共享的服务。您可以使用 AWS PrivateLink 创建端点服务，并将权限授予其他 AWS 账户 或 AWS Identity and Access Management（IAM）主体。这些账户或主体可通过创建接口 VPC 端点来私密地连接到您的端点服务。有关更多信息，请参阅 Amazon Virtual Private Cloud（Amazon VPC）文档中的创建端点服务。

企业资源规划（ERP）

一种自动化和管理企业关键业务流程（例如会计、MES 和项目管理）的系统。

信封加密

用另一个加密密钥对加密密钥进行加密的过程。有关更多信息，请参阅 AWS Key Management Service（AWS KMS）文档中的信封加密。

环境

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

- 开发环境 — 正在运行的应用程序的实例，只有负责维护应用程序的核心团队才能使用。开发环境用于测试更改，然后再将其提升到上层环境。这类环境有时称为测试环境。

- 下层环境 — 应用程序的所有开发环境，比如用于初始构建和测试的环境。
- 生产环境 — 最终用户可以访问的正在运行的应用程序的实例。在 CI/CD 管线中，生产环境是最后一个部署环境。
- 上层环境 — 除核心开发团队以外的用户可以访问的所有环境。这可能包括生产环境、预生产环境和用户验收测试环境。

epic

在敏捷方法学中，有助于组织工作和确定优先级的功能类别。epics 提供了对需求和实施任务的总体描述。例如，AWS CAF 安全操作说明包括身份和访问管理、侦测性控制、基础设施安全、数据保护和事件响应。有关 AWS 迁移策略中 epics 的更多信息，请参阅计划实施指南。

ERP

请参阅企业资源规划。

探索性数据分析（EDA）

分析数据集以了解其主要特征的过程。您收集或汇总数据，并进行初步调查，以发现模式、检测异常并检查假定情况。EDA 通过计算汇总统计数据和创建数据可视化得以执行。

F

事实表

星型架构中的中心表。它存储有关业务运营的定量数据。通常，事实表包含两种类型的列：包含度量的列和包含维度表外键的列。

快速失效机制

一种使用频繁且增量式的测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

在 AWS 云中，诸如可用区、AWS 区域、控制面板或数据面板之类的边界，它限制了故障的影响并有助于提高工作负载的韧性。有关更多信息，请参阅 AWS 故障隔离边界。

功能分支

请参阅分支。

特征

您用来进行预测的输入数据。例如，在制造环境中，特征可能是定期从生产线捕获的图像。

特征重要性

特征对于模型预测的重要性。这通常表示为数值分数，可以通过各种技术进行计算，例如 Shapley 加法解释（SHAP）和积分梯度。有关更多信息，请参阅使用 AWS 实现机器学习模型的可解释性。

功能转换

为 ML 流程优化数据，包括使用其他来源丰富数据、扩展值或从单个数据字段中提取多组信息。这使得 ML 模型能从数据中获益。例如，如果您将“2021-05-27 00:15:37”日期分解为“2021”、“五月”、“星期四”和“15”，则可以帮助学习与不同数据成分相关的算法学习精细模式。

少样本提示

在要求 LLM 执行类似任务之前，先向其提供少量示例，以演示任务和预期输出。此技术是上下文内学习的一种应用，其中模型可以从提示中嵌入的示例（样本）中学习。对于需要特定格式、推理或领域知识的任务，少样本提示可能非常有效。另请参阅零样本提示。

FGAC

请参阅精细访问控制。

精细访问控制（FGAC）

使用多个条件允许或拒绝访问请求。

快闪迁移

一种数据库迁移方法，通过更改数据捕获使用连续数据复制，在极短的时间内迁移数据，而非使用分阶段方法。目标是将停机时间降至最低。

FM

请参阅基础模型。

基础模型（FM）

一个大型深度学习神经网络，它已使用海量的通用和未标注数据集进行训练。FM 能够执行各种常规任务，例如理解语言、生成文本和图像以及使用自然语言进行对话。有关更多信息，请参阅什么是基础模型。

G

生成式人工智能

AI 模型的一个子集，这些模型已经过大量数据训练，可以使用简单的文本提示来创建新的内容和构件，例如图像、视频、文本和音频。有关更多信息，请参阅什么是生成式人工智能。

地理阻止

请参阅地理限制。

地理限制（地理阻止）

Amazon CloudFront 中的一个选项，用于阻止特定国家/地区的用户访问内容分发。您可以使用允许列表或阻止列表来指定已批准和已禁止的国家/地区。有关更多信息，请参阅 CloudFront 文档中的限制内容的地理分发。

GitFlow 工作流程

一种方法，在这种方法中，下层和上层环境在源代码存储库中使用不同的分支。Gitflow 工作流程被认为是传统的工作流程，而基于中继的工作流程则是现代的、首选的方法。

黄金映像

系统或软件的快照，用作部署该系统或软件的新实例的模板。例如，在制造业中，黄金映像可用于在多个设备上预调配软件，并有助于提高设备制造操作的速度、可扩展性和生产效率。

全新策略

在新环境中缺少现有基础设施。在对系统架构采用全新策略时，您可以选择所有新技术，而不受对现有基础设施（也称为棕地）兼容性的限制。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

护栏

一种高级规则，用于跨组织单位（OU）管理资源、策略和合规性。预防性护栏会执行策略以确保符合合规性标准。它们是使用服务控制策略和 IAM 权限边界实现的。侦测性护栏会检测策略违规和合规性问题，并生成提醒以进行修复。它们是使用 AWS Config、AWS Security Hub CSPM、Amazon GuardDuty、AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 检查实现的。

H

HA

请参阅高可用性。

异构数据库迁移

将源数据库迁移到使用不同数据库引擎的目标数据库（例如，从 Oracle 迁移到 Amazon Aurora）。异构迁移通常是重新架构工作的一部分，而转换架构可能是一项复杂的任务。AWS 提供了 AWS SCT 来帮助实现架构转换。

高可用性（HA）

在遇到挑战或灾难时，工作负载无需干预即可连续运行的能力。HA 系统旨在自动进行故障转移、持续提供良好性能，并以最小的性能影响处理不同负载和故障。

历史数据库现代化

一种用于实现运营技术（OT）系统现代化和升级以更好满足制造业需求的方法。历史数据库是一种用于收集和存储工厂中各种来源数据的数据库。

保留数据

从用于训练机器学习模型的数据集中保留的一部分标注的历史数据。通过将模型预测与保留数据进行比较，您可以使用保留数据来评估模型性能。

同构数据库迁移

将源数据库迁移到共享同一数据库引擎的目标数据库（例如，从 Microsoft SQL Server 迁移到 Amazon RDS for SQL Server）。同构迁移通常是更换主机或更换平台工作的一部分。您可以使用本机数据库实用程序来迁移架构。

热数据

经常访问的数据，例如实时数据或近期的转化数据。这些数据通常需要高性能存储层或存储类别才能提供快速的查询响应。

修补程序

针对生产环境中关键问题的紧急修复。由于其紧迫性，修补程序通常在典型的 DevOps 发布工作流程之外进行。

hypercare 周期

割接之后，迁移团队立即管理和监控云中迁移的应用程序以解决任何问题的时间段。通常，这个周期持续 1-4 天。在 hypercare 周期结束时，迁移团队通常会将应用程序的责任移交给云运营团队。

我

IaC

请参阅基础设施即代码。

基于身份的策略

附加到一个或多个 IAM 主体的策略，用于定义它们在 AWS 云 环境中的权限。

空闲应用程序

90 天内平均 CPU 和内存使用率在 5% 到 20% 之间的应用程序。在迁移项目中，通常会停用这些应用程序或将其保留在本地。

IIoT

请参阅工业物联网。

不可变基础设施

一种模型，可为生产工作负载部署新的基础设施，而不是更新、修补或修改现有基础设施。不可变基础设施本质上比可变基础设施更一致、更可靠、更可预测。有关更多信息，请参阅 AWS Well-Architected Framework 中的使用不可变基础设施进行部署最佳实践。

入站（入口）VPC

在 AWS 多账户架构中，一种用于接受、检查和路由来自应用程序外部的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

增量迁移

一种割接策略，在这种策略中，您可以将应用程序分成小部分进行迁移，而不是一次性完整割接。例如，您最初可能只将几个微服务或用户迁移到新系统。在确认一切正常后，您可以逐步迁移其他微服务或用户，直到停用遗留系统。这种策略降低了大规模迁移带来的风险。

工业 4.0

该术语由 Klaus Schwab 在 2016 年提出，指的是通过连接、实时数据、自动化、分析和 AI/ML 的进步来实现制造流程的现代化。

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码（IaC）

通过一组配置文件预调配和管理应用程序基础设施的过程。IaC 旨在帮助您集中管理基础设施、实现资源标准化和快速扩展，使新环境具有可重复性、可靠性和一致性。

工业物联网（IIoT）

在工业领域使用联网的传感器和设备，例如制造业、能源、汽车、医疗保健、生命科学和农业。有关更多信息，请参阅制定工业物联网（IIoT）数字化转型策略。

检查 VPC

在 AWS 多账户架构中，一种用于管理 VPC（相同或不同的 AWS 区域）、互联网和本地网络之间的网络流量检查的集中式 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

物联网（IoT）

由带有嵌入式传感器或处理器的连接物理对象组成的网络，这些传感器或处理器通过互联网或本地通信网络与其他设备和系统进行通信。有关更多信息，请参阅什么是 IoT？

可解释性

它是机器学习模型的一种特征，描述了人类可以理解模型的预测如何取决于其输入的程度。有关更多信息，请参阅使用 AWS 实现机器学习模型的可解释性。

IoT

请参阅物联网。

IT 信息库（ITIL）

提供 IT 服务并使这些服务符合业务要求的一套最佳实践。ITIL 是 ITSM 的基础。

IT 服务管理（ITSM）

为组织设计、实施、管理和支持 IT 服务的相关活动。有关将云运营与 ITSM 工具集成的信息，请参阅运营集成指南。

ITIL

请参阅 IT 信息库。

ITSM

请参阅 IT 服务管理。

L

基于标签的访问控制（LBAC）

强制访问控制（MAC）的一种实施方式，其中明确为用户和数据本身分配了安全标签值。用户安全标签和数据安全标签之间的交集决定了用户可以看到哪些行和列。

登录区

登录区是一个架构完善、可扩展且安全的多账户 AWS 环境。这是一个起点，您的组织可以从这里放心地在安全和基础设施环境中快速启动和部署工作负载和应用程序。有关登录区的更多信息，请参阅设置安全且可扩展的多账户 AWS 环境。

大语言模型（LLM）

一种基于大量数据进行预训练的深度学习 AI 模型。LLM 可以执行多项任务，例如回答问题、总结文档、将文本翻译成其他语言以及完成句子。有关更多信息，请参阅什么是 LLM。

大规模迁移

迁移 300 台或更多服务器。

LBAC

请参阅基于标签的访问控制。

最低权限

授予执行任务所需的最低权限的最佳安全实践。有关更多信息，请参阅 IAM 文档中的应用最低权限许可。

直接迁移

请参阅 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参阅字节顺序。

LLM

请参阅大语言模型。

下层环境

请参阅环境。

M

机器学习（ML）

一种使用算法和技术进行模式识别和学习的人工智能。ML 对记录的数据（例如物联网（IoT）数据）进行分析和学习，以生成基于模式的统计模型。有关更多信息，请参阅机器学习。

主分支

请参阅分支。

恶意软件

旨在危害计算机安全或隐私的软件。恶意软件可能会破坏计算机系统、泄露敏感信息或获得未经授权的访问权限。恶意软件的示例包括病毒、蠕虫、勒索软件、木马、间谍软件和键盘记录器。

托管服务

AWS 服务（其中 AWS 运营基础设施层、操作系统和平台，而您可访问端点存储和检索数据）。Amazon Simple Storage Service（Amazon S3）和 Amazon DynamoDB 就是托管服务的示例。这些服务也称为抽象服务。

制造执行系统（MES）

一种软件系统，用于跟踪、监控、记录和控制在车间将原材料转化为成品的生产过程。

MAP

请参阅迁移加速计划。

机制

一个完整的过程，您可以在其中创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运作过程中自我强化和改善的循环。有关更多信息，请参阅 AWS Well-Architected Framework 中的构建机制。

成员账户

除管理账户外，属于 AWS Organizations 中的组织的所有 AWS 账户。一个账户一次只能作为一个组织的成员。

MES

请参阅制造执行系统。

消息队列遥测传输（MQTT）

一种基于发布/订阅模式的轻量级机器对机器（M2M）通信协议，适用于资源受限的 IoT 设备。

微服务

一种小型独立服务，通过明确定义的 API 进行通信，通常由小型独立团队拥有。例如，保险系统可能包括映射到业务能力（如销售或营销）或子域（如购买、理赔或分析）的微服务。微服务的好处包括敏捷性、灵活扩展、易于部署、可重复使用的代码和韧性。有关更多信息，请参阅使用 AWS 无服务器服务集成微服务。

微服务架构

一种使用独立组件构建应用程序的方法，这些组件将每个应用程序进程作为微服务运行。这些微服务使用轻量级 API 通过明确定义的接口进行通信。该架构中的每个微服务都可以更新、部署和扩展，以满足对应用程序特定功能的需求。有关更多信息，请参阅在 AWS 上实现微服务。

迁移加速计划（MAP）

一项提供咨询支持、培训和服务的 AWS 计划，旨在帮助组织为迁移到云奠定坚实的运营基础，并抵消迁移的初始成本。MAP 提供了一种以系统的方式执行遗留迁移的迁移方法，以及一套用于自动执行和加速常见迁移场景的工具。

大规模迁移

将大部分应用程序组合分波迁移到云中的过程，在每一波中以更快的速度迁移更多应用程序。本阶段使用从早期阶段获得的最佳实践和经验教训，实施由团队、工具和流程组成的迁移工厂，通过自动化和敏捷交付简化工作负载的迁移。这是 AWS 迁移策略的第三阶段。

迁移工厂

跨职能团队，通过自动化、敏捷的方法简化工作负载迁移。迁移工厂团队通常包括运营、业务分析师和所有者、迁移工程师、开发人员和从事 sprint 工作的 DevOps 专业人员。20% 到 50% 的企业应用程序组合由可通过工厂方法优化的重复模式组成。有关更多信息，请参阅本内容集中有关迁移工厂的讨论和云迁移工厂指南。

迁移元数据

有关完成迁移所需的应用程序和服务器的信息。每种迁移模式都需要一套不同的迁移元数据。迁移元数据的示例包括目标子网、安全组和 AWS 账户。

迁移模式

一种可重复的迁移任务，详细列出了迁移策略、迁移目标以及所使用的迁移应用程序或服务。示例：使用 AWS Application Migration Service 将主机迁移到 Amazon EC2。

迁移组合评测（MPA）

一种在线工具，提供了用于验证迁移到 AWS 云的业务案例的信息。MPA 提供了详细的组合评测（服务器规模调整、定价、TCO 比较、迁移成本分析）以及迁移计划（应用程序数据分析和数据

收集、应用程序分组、迁移优先级排序和波次规划）。MPA 工具（需要登录）向所有 AWS 顾问和 APN 合作伙伴顾问免费提供。

迁移准备情况评测（MRA）

使用 AWS CAF 深入了解组织的云就绪状态，找出优势和劣势，并制定行动计划来弥补发现的差距。有关更多信息，请参阅迁移准备指南。MRA 是 AWS 迁移策略的第一阶段。

迁移策略

将工作负载迁移到 AWS 云的方法。有关更多信息，请参见术语表中的 7 R 词条，以及 Mobilize your organization to accelerate large-scale migrations。

ML

请参阅机器学习。

现代化

将过时的（原有的或单体）应用程序及其基础设施转变为云中敏捷、弹性和高度可用的系统，以降低成本、提高效率和利用创新。有关更多信息，请参阅 Strategy for modernizing applications in the AWS 云。

现代化准备情况评估

一种评估方式，有助于确定组织应用程序的现代化准备情况；确定收益、风险和依赖关系；确定组织能够在多大程度上支持这些应用程序的未来状态。评估结果是目标架构的蓝图、详细说明现代化进程发展阶段和里程碑的路线图以及解决已发现差距的行动计划。有关更多信息，请参阅 Evaluating modernization readiness for applications in the AWS 云。

单体应用程序（单体式）

作为具有紧密耦合进程的单个服务运行的应用程序。单体应用程序有几个缺点。如果某个应用程序功能的需求激增，则必须扩展整个架构。随着代码库的增长，添加或改进单体应用程序的功能也会变得更加复杂。若要解决这些问题，可以使用微服务架构。有关更多信息，请参阅将单体分解为微服务。

MPA

请参阅迁移组合评测。

MQTT

请参阅消息队列遥测传输。

多分类器

一种帮助为多个类别生成预测（预测两个以上结果之一）的过程。例如，ML 模型可能会询问“这个产品是书、汽车还是手机？”或“此客户最感兴趣什么类别的产品？”

可变基础设施

一种为生产工作负载更新和修改现有基础设施的模型。为了提高一致性、可靠性和可预测性，AWS Well-Architected Framework 建议使用不可变基础设施作为最佳实践。

O

OAC

请参阅来源访问控制。

OAI

请参阅来源访问身份。

OCM

请参阅组织变革管理。

离线迁移

一种迁移方法，在这种方法中，源工作负载会在迁移过程中停止运行。这种方法会延长停机时间，通常用于小型非关键工作负载。

OI

请参阅运营集成。

OLA

请参阅运营级别协议。

在线迁移

一种迁移方法，在这种方法中，源工作负载无需离线即可复制到目标系统。在迁移过程中，连接工作负载的应用程序可以继续运行。这种方法的停机时间为零或最短，通常用于关键生产工作负载。

OPC-UA

请参阅开放流程通信 – 统一架构。

开放流程通信 – 统一架构（OPC-UA）

一种用于工业自动化的机器对机器（M2M）通信协议。OPC-UA 提供了具有数据加密、身份验证和授权方案的互操作性标准。

运营级别协议（OLA）

一项协议，阐明了 IT 职能部门承诺相互交付的内容，以支持服务水平协议（SLA）。

运营准备情况审查（ORR）

一份问题核对清单和关联的最佳实践，可帮助您了解、评估、预防或缩小事件和可能的故障的范围。有关更多信息，请参阅 AWS Well-Architected Framework 中的运营准备情况审查（ORR）。

运营技术（OT）

与物理环境配合使用以控制工业运营、设备和基础设施的硬件和软件系统。在制造业中，OT 和信息技术（IT）系统的集成是工业 4.0 转型的关键重点。

运营整合（OI）

在云中实现运营现代化的过程，包括就绪计划、自动化和集成。有关更多信息，请参阅运营整合指南。

组织跟踪

由 AWS CloudTrail 创建的跟踪，用于记录 AWS Organizations 中的组织的所有 AWS 账户 事件。该跟踪是在每个 AWS 账户 中创建的，属于组织的一部分，并跟踪每个账户的活动。有关更多信息，请参阅 CloudTrail 文档中的为组织创建跟踪。

组织变革管理（OCM）

一个从人员、文化和领导力角度管理重大、颠覆性业务转型的框架。OCM 通过加快变革采用、解决过渡问题以及推动文化和组织变革，帮助组织为新系统和战略做好准备和过渡。在 AWS 迁移策略中，这个框架称为人员加速，因为云采用项目需要快速的变革。有关更多信息，请参阅 OCM 指南。

来源访问控制（OAC）

CloudFront 中的一个增强选项，用于限制访问以保护您的 Amazon Simple Storage Service（Amazon S3）内容。OAC 支持所有 AWS 区域 中的 S3 存储桶、使用 AWS KMS 的服务器端加密（SSE-KMS）以及对 S3 存储桶的动态 PUT 和 DELETE 请求。

来源访问身份（OAI）

CloudFront 中的一个选项，用于限制访问以保护您的 Amazon S3 内容。当您使用 OAI 时，CloudFront 会创建一个主体，供 Amazon S3 进行身份验证。经过身份验证的主体只能通过特

定的 CloudFront 分发访问 S3 存储桶中的内容。另请参阅 OAC，其中提供了更精细和增强的访问控制。

ORR

请参阅运营准备情况审查。

OT

请参阅运营技术。

出站（出口）VPC

在 AWS 多账户架构中，一种用于处理从应用程序内部启动的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

P

权限边界

附加到 IAM 主体的 IAM 管理策略，用于设置用户或角色可以拥有的最大权限。有关更多信息，请参阅 IAM 文档中的权限边界。

个人身份信息（PII）

直接查看其他相关数据或与之配对时可用于合理推断个人身份的信息。PII 的示例包括姓名、地址和联系信息。

PII

请参阅个人身份信息。

playbook

一套预定义的步骤，用于捕获与迁移相关的工作，例如在云中交付核心运营功能。playbook 可以采用脚本、自动化运行手册的形式，也可以是操作现代化环境所需的流程或步骤的摘要。

PLC

请参阅可编程逻辑控制器。

PLM

请参阅产品生命周期管理。

policy

一个对象，可以定义权限（请参阅基于身份的策略）、指定访问条件（请参阅基于资源的策略）或定义 AWS Organizations 的组织中所有账户的最大权限（请参阅服务控制策略）。

多语言持久性

根据数据访问模式和其他要求，独立选择微服务的数据存储技术。如果您的微服务采用相同的数据存储技术，它们可能会遇到实现难题或性能不佳。如果微服务使用最适合其需求的数据存储，则可以更轻松地实现微服务，并获得更好的性能和可扩展性。有关更多信息，请参阅在微服务中实现数据持久性。

组合评测

一个发现、分析和确定应用程序组合优先级以规划迁移的过程。有关更多信息，请参阅评估迁移准备情况。

谓词

返回 `true` 或 `false` 的查询条件，通常位于 `WHERE` 子句中。

谓词下推

一种数据库查询优化技术，可在传输之前筛选查询中的数据。这将减少从关系数据库检索和处理的数据量，并提高查询性能。

预防性控制

一种安全控制，旨在防止事件发生。这些控制是第一道防线，帮助防止未经授权的访问或对网络的意外更改。有关更多信息，请参阅在 AWS 上实施安全控制中的预防性控制。

主体

AWS 中可执行操作并访问资源的实体。该实体通常是 AWS 账户、IAM 角色或用户的根用户。有关更多信息，请参阅 IAM 文档中角色术语和概念中的主体。

隐私设计

一种在整个开发过程中都考虑隐私的系统工程方法。

私有托管区

私有托管区就是一个容器，其中包含的信息说明您希望 Amazon Route 53 如何响应一个或多个 VPC 中的某个域及其子域的 DNS 查询。有关更多信息，请参阅 Route 53 文档中的私有托管区的使用。

主动控制

一种安全控制，旨在防止部署不合规资源。这些控制会在资源预调配之前对其进行扫描。如果资源与控件不兼容，则不会对其进行预调配。有关更多信息，请参阅 AWS Control Tower 文档中的控制参考指南，并参阅在 AWS 上实施安全控制中的主动控制。

产品生命周期管理（PLM）

对产品在其整个生命周期内的数据和流程的管理，从设计、开发和发布，到增长和成熟，再到衰退和淘汰。

生产环境

请参阅环境。

可编程逻辑控制器（PLC）

在制造业中，一种高度可靠、适应性强的计算机，用于监控机器并实现制造过程自动化。

提示串接

使用一个 LLM 提示的输出作为下一个提示的输入，以生成更好的响应。该技术用于将复杂的任务分解为子任务，或者迭代地完善或扩展初步响应。它有助于提高模型响应的准确性和相关性，并允许获得更精细的个性化结果。

假名化

用占位符值替换数据集中个人标识符的过程。假名化可以帮助保护个人隐私。假名化数据仍被视为个人数据。

发布/订阅（pub/sub）

一种支持微服务间异步通信的模式，可提高可扩展性和响应能力。例如，在基于微服务的 MES 中，微服务可以将事件消息发布到其他微服务可以订阅的频道。系统可以在不更改发布服务的情况下添加新的微服务。

Q

查询计划

一系列用于访问 SQL 关系数据库系统中的数据的步骤，类似于指令。

查询计划回归

当数据库服务优化程序选择的最佳计划不如数据库环境发生特定变化之前时。这可能是由统计数据、约束、环境设置、查询参数绑定更改和数据库引擎更新造成的。

R

RACI 矩阵

请参阅责任、问责、咨询和知情（RACI）。

RAG

请参阅检索增强生成。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI 矩阵

请参阅责任、问责、咨询和知情（RACI）。

RCAC

请参阅行列访问控制。

只读副本

用于只读目的的数据库副本。您可以将查询路由到只读副本，以减轻主数据库的负载。

重新架构

请参阅 7 R。

恢复点目标（RPO）

自上一个数据恢复点以来可接受的最长时间。这决定了从上一个恢复点到服务中断之间可接受的数据丢失情况。

恢复时间目标（RTO）

服务中断和服务恢复之间可接受的最大延迟。

重构

请参阅 7 R。

区域

地理区域中的 AWS 资源集合。每个 AWS 区域 是孤立的，独立于其他的区域，以提供容错能力、稳定性和韧性。有关更多信息，请参阅指定您的账户可以使用的 AWS 区域。

回归

一种预测数值的 ML 技术。例如，要解决“这套房子的售价是多少？”的问题 ML 模型可以使用线性回归模型，根据房屋的已知事实（如建筑面积）来预测房屋的销售价格。

重新托管

请参阅 7 R。

版本

在部署过程中，推动生产环境变更的行为。

重新放置

请参阅 7 R。

更换平台

请参阅 7 R。

重新购买

请参阅 7 R。

韧性

应用程序抵御中断或从中断中恢复的能力。在 AWS 云中规划韧性时，高可用性和灾难恢复是常见的考虑因素。有关更多信息，请参阅 AWS 云韧性。

基于资源的策略

一种附加到资源的策略，例如 AmazonS3 存储桶、端点或加密密钥。此类策略指定了允许哪些主体访问、支持的操作以及必须满足的任何其他条件。

责任、问责、咨询和知情（RACI）矩阵

定义参与迁移活动和云运营的所有各方的角色和责任的矩阵。矩阵名称源自矩阵中定义的责任类型：负责（R）、问责（A）、咨询（C）和知情（I）。支持（S）类型是可选的。如果包括支持，则该矩阵称为 RASCI 矩阵，如果将其排除在外，则称为 RACI 矩阵。

响应性控制

一种安全控制，旨在推动对不良事件或偏离安全基线的情况进行修复。有关更多信息，请参阅在 AWS 上实施安全控制中的响应性控制。

保留

请参阅 7 R。

停用

请参阅 7 R。

检索增强生成（RAG）

一种生成式人工智能技术，其中 LLM 在生成响应之前引用其训练数据来源之外的权威数据来源。例如，RAG 模型可以对组织的知识库或自定义数据执行语义搜索。有关更多信息，请参阅什么是 RAG。

轮换

定期更新机密密钥以使攻击者更难访问凭证的过程。

行列访问控制（RCAC）

使用已定义访问规则的基本、灵活的 SQL 表达式。RCAC 由行权限和列掩码组成。

RPO

请参阅恢复点目标。

RTO

请参阅恢复时间目标。

运行手册

执行特定任务所需的一套手动或自动程序。它们通常是为了简化重复性操作或高错误率的程序而设计的。

S

SAML 2.0

众多身份提供者（IdP）使用的开放标准。此功能可实现联合单点登录（SSO），因此用户可以登录 AWS 管理控制台 或调用 AWS API 操作，而无需在 IAM 中为组织中的每个人都创建用户。有关基于 SAML 2.0 的联合身份验证的更多信息，请参阅 IAM 文档中的关于基于 SAML 2.0 的联合身份验证。

SCADA

请参阅监督控制和数据采集。

SCP

请参阅服务控制策略。

机密密钥

在 AWS Secrets Manager 中，您以加密形式存储的机密或受限信息，例如密码或用户凭证。它由机密密钥值及其元数据组成。机密密钥值可以是二进制、单个字符串或多个字符串。有关更多信息，请参阅 Secrets Manager 文档中的什么是 Secrets Manager 机密密钥？。

设计安全

一种在整个开发过程中都考虑安全的系统工程方法。

安全控制

一种技术或管理护栏，可防止、检测或降低威胁行为体利用安全漏洞的能力。安全控制有以下四种类型：预防性、检测性、响应性和主动性。

安全固化

缩小攻击面，使其更能抵御攻击的过程。这可能包括删除不再需要的资源、实施授予最低权限的最佳安全实践或停用配置文件中不必要的功能等操作。

安全信息和事件管理（SIEM）系统

结合了安全信息管理（SIM）和安全事件管理（SEM）系统的工具和服务。SIEM 系统会收集、监控和分析来自服务器、网络、设备和其他来源的数据，以检测威胁和安全漏洞，并生成提醒。

安全响应自动化

一种预定义的程序化操作，旨在自动响应或修复安全事件。这些自动化可作为检测性或响应性安全控制措施，帮助您实施 AWS 安全最佳实践。自动响应操作的示例包括修改 VPC 安全组、修补 Amazon EC2 实例或轮换凭证。

服务器端加密

由接收数据的 AWS 服务 在目的地对数据进行加密。

服务控制策略（SCP）

一种策略，用于集中控制 AWS Organizations 的组织中所有账户的权限。SCP 为管理员可以委托给用户或角色的操作定义了护栏或设定了限制。您可以将 SCP 用作允许列表或拒绝列表，指定允许或禁止哪些服务或操作。有关更多信息，请参阅 AWS Organizations 文档中的服务控制策略。

服务端点

AWS 服务 的入口点的 URL。您可以使用端点，通过编程方式连接到目标服务。有关更多信息，请参阅 AWS 一般参考 中的 AWS 服务 端点。

服务水平协议（SLA）

一份协议，阐明了 IT 团队承诺向客户交付的内容，比如服务正常运行时间和性能。

服务水平指标（SLI）

对服务性能方面的衡量，例如错误率、可用性或吞吐量。

服务水平目标（SLO）

代表服务运行状况的目标指标，由服务水平指标衡量。

责任共担模式

一种描述您在云安全性和合规性方面与 AWS 共担的责任模型。AWS 负责云的安全，而您则负责云中的安全。有关更多信息，请参阅责任共担模式。

SIEM

请参阅安全信息和事件管理系统。

单点故障（SPOF）

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

请参阅服务水平协议。

SLI

请参阅服务水平指标。

SLO

请参阅服务水平目标。

split-and-seed 模式

一种扩展和加速现代化项目的模式。随着新功能和产品发布的定义，核心团队会拆分以创建新的产品团队。这有助于扩展组织的能力和服务，提高开发人员的工作效率，支持快速创新。有关更多信息，请参阅 Phased approach to modernizing applications in the AWS 云。

SPOF

请参阅单点故障。

星型架构

一种数据库组织结构，它使用一个大型事实表来存储事务数据或测量数据，并使用一个或多个较小的维度表来存储数据属性。此结构专为在数据仓库中使用或用于商业智能目的而设计。

strangler fig 模式

一种通过逐步重写和替换系统功能直至可以停用原有的系统来实现单体系统现代化的方法。这种模式用无花果藤作为类比，这种藤蔓成长为一棵树，最终战胜并取代了宿主。该模式是由 Martin Fowler 提出的，作为重写单体系统时管理风险的一种方法。有关如何应用此模式的示例，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

监督控制和数据采集（SCADA）

在制造业中，一种使用硬件和软件来监控实物资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

以模拟用户交互的方式测试系统，以检测潜在问题或监控性能。您可以使用 Amazon CloudWatch Synthetics 来创建这些测试。

系统提示

一种为 LLM 提供上下文、说明或准则以指导其行为的技术。系统提示有助于设置上下文并制定与用户交互的规则。

T

tags

充当元数据的键值对，用于组织 AWS 资源。标签有助于您管理、识别、组织、搜索和筛选资源。有关更多信息，请参阅标记您的 AWS 资源。

目标变量

您在监督式 ML 中尝试预测的值。这也被称为结果变量。例如，在制造环境中，目标变量可能是产品缺陷。

任务列表

一种通过运行手册用于跟踪进度的工具。任务列表包含运行手册的概述和要完成的常规任务列表。对于每项常规任务，它包括预计所需时间、所有者和进度。

测试环境

请参阅环境。

训练

为您的 ML 模型提供学习数据。训练数据必须包含正确答案。学习算法在训练数据中查找将输入数据属性映射到目标（您希望预测的答案）的模式。然后输出捕获这些模式的 ML 模型。然后，您可以使用 ML 模型对不知道目标的新数据进行预测。

中转网关

中转网关是网络中转中心，您可用它来互连 VPC 和本地网络。有关更多信息，请参阅 AWS Transit Gateway 文档中的什么是中转网关。

基于中继的工作流程

一种方法，开发人员在功能分支中本地构建和测试功能，然后将这些更改合并到主分支中。然后，按顺序将主分支构建到开发、预生产和生产环境。

可信访问权限

为您指定的服务授予权限，让其代表您在 AWS Organizations 的组织中及其账户中执行任务。当需要服务相关的角色时，受信任的服务会在每个账户中创建一个角色，为您执行管理任务。有关更多信息，请参阅 AWS Organizations 文档中的将 AWS Organizations 与其他 AWS 服务一起使用。

优化

更改训练过程的各个方面，以提高 ML 模型的准确性。例如，您可以通过生成标签集、添加标签，并在不同的设置下多次重复这些步骤来优化模型，从而训练 ML 模型。

双披萨团队

一个小型 DevOps 团队，两个披萨就能养活。双披萨团队的规模可确保在软件开发过程中充分协作。

U

不确定性

这一概念指的是不精确、不完整或未知的信息，这些信息可能会破坏预测式 ML 模型的可靠性。不确定性有两种类型：认知不确定性是由有限的、不完整的数据造成的，而偶然不确定性是由数据中固有的噪声和随机性导致的。有关更多信息，请参阅量化深度学习系统中的不确定性指南。

无差别任务

也称为繁重工作，即创建和运行应用程序所必需的工作，但不能为最终用户提供直接价值或竞争优势。无差别任务的示例包括采购、维护和容量规划。

上层环境

请参阅环境。

V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC 对等连接

两个 VPC 之间的连接，允许您使用私有 IP 地址路由流量。有关更多信息，请参阅 Amazon VPC 文档中的什么是 VPC 对等连接。

漏洞

损害系统安全的软件缺陷或硬件缺陷。

W

热缓存

一种包含经常访问的当前相关数据的缓冲区缓存。数据库实例可以从缓冲区缓存读取，这比从主内存或磁盘读取要快。

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

一种对与当前记录有某种关联的一组行执行计算的 SQL 函数。窗口函数对于处理任务很有用，例如计算移动平均值或根据当前行的相对位置访问行的值。

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

迁移项目中负责一组特定任务的职能小组。每个工作流都是独立的，但支持项目中的其他工作流。例如，组合工作流负责确定应用程序的优先级、波次规划和收集迁移元数据。组合工作流将这些资产交付给迁移工作流，然后迁移服务器和应用程序。

WORM

请参阅一次写入多次读取。

WQF

请参阅 AWS 工作负载资格鉴定框架。

一次写入多次读取（WORM）

一种存储模型，可一次写入数据并防止数据被删除或修改。授权用户可以根据需要多次读取数据，但无法对其进行更改。此数据存储基础设施被认为不可变。

Z

零日漏洞利用

一种利用零日漏洞的攻击，通常为恶意软件。

零日漏洞

生产系统中不可避免的缺陷或漏洞。威胁主体可能利用这种类型的漏洞攻击系统。开发人员经常因攻击而意识到该漏洞。

零样本提示

为 LLM 提供执行任务的说明，但没有可以帮助指导的示例（样本）。LLM 必须使用预先训练的知识来处理任务。零样本提示的有效性取决于任务的复杂性和提示的质量。另请参阅少样本提示。

僵尸应用程序

平均 CPU 和内存使用率低于 5% 的应用程序。在迁移项目中，通常会停用这些应用程序。