SAP 指南

一般 SAP 指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

一般 SAP 指南: SAP 指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

主页 1
概览 2
关于本指南 2
AWS 概述 2
AWS 服务 2
AWS 全球基础设施 6
AWS 安全与合规 6
AWS 配置和管理 7
SAP AWS 概述 8
开启的 SAP 软件和许可证 AWS 8
SAP Support on AWS 9
在上部署 SAP 系统 AWS 9
适用于 SAP 的合作伙伴服务 AWS 11
SAP 谈 AWS 规划 11
SAP 笔记 11
AWS 架构上的 SAP 12
选择 AWS 区域和可用区 13
网络和连接 14
遵循安全最佳实践 6
EC2 SAP 的实例类型 16
操作系统 17
数据库 19
SAP 安装媒体 21
SAProuter 和 SAP 解决方案经理 21
文档修订 22
亚马逊 EC2 实例类型 23
实例类型可用性 23
SAP NetWeaver 支持的实例 23
SAP 的当前一代实例 NetWeaver 24
上一代 SAP 实例 NetWeaver 46
SAP HANA 认证和非认证实例 48
最新一代认证实例 49
上一代认证实例 56
非认证实例 57

SAP Business One 认证实例，SAP HANA 版本 58
在 SAP 上记录实例类型的历史记录 AWS 60
AWS 数据提供商 62
简介 62
定价 63
技术要求 64
亚马逊 VPC 网络拓扑 64
Amazon VPC 端点 65
IAM 角色 66
DataProvider 4.3 68
正在安装 DataProvider 4.3 69
正在更新到 DataProvider 4.3 87
正在卸载旧版本 91
故障排除 92
在 Linux 系统上 92
Windows 上的问题排查 96
为 SAP 定制 AWS 数据提供器 100
配置文件的语法规则 101
用户可配置的 EC2 实例类型 101
用户可配置的 EBS 卷类型 103
在 SAP 系统监控中验证 SAP AWS 的数据提供者 103
使用 SAP 操作系统收集器 (SAPOSCOL) 检查指标 104
使用 SAP CCMS 交易检查指标 105
捕获的指标示例 108
版本历史记录 113
成本估算 118
AWS 区域 118
计算 118
存储 119
Amazon EBS 119
Amazon EFS 120
FSx 适用于 Windows 文件服务器的亚马逊 120
FSx 适用于 NetApp ONTAP 的亚马逊 120
Amazon S3 121
网络 121
Amazon VPC 121

AWS Site-to-Site VPN 122
AWS 直接连接 122
Elastic Load Balancing 123
数据传输定价 123
自动化 125
Backup、还原和恢复 125
AWS 适用于 SAP HANA 的 Backint Agent 125
AWS 弹性灾难恢复 125
Amazon EBS 快照 126
迁移 126
Migration Hub Orchestrator 126
AWS DataSync 126
监控 126
AWS 数据提供商 127
CloudWatch 适用于 SAP HANA 的 Amazon 应用程序见解 127
Amazon CloudWatch 127
AWS CloudTrail 127
Amazon VPC 流日志 127
操作系统许可证 128
Red Hat 128
SUSE 128
Windows 129
甲骨文企业 Linu 129
AWS Marketp 129
AWS Support 130
架构指导 131
概览 131
先决条件 131
专业知识 131
推荐读物 132
简介 132
SAP NetWeaver 架构单点故障 132
高可用性和灾难恢复 133
本地部署模式与云部署模式 134
架构指导方针和决策 136
区域和可用区 136

AWS 账户 138
计算 139
网络连接 141
存储 144
监控和审计 147
架构模式 147
故障场景 147
模式 148
摘要 166
微软 SQL 168
模式 168
比较矩阵 168
单区域模式 169
多区域模式 171
使用弹性灾难恢复实现灾难恢复 177
场景 178
参考信息 178
SLAs 和许可证 178
恢复时间目标（RTO） 179
恢复点目标 (RPO) 179
恢复一致性目标 (RCO) 180
SAP 许可证 180
网络、存储和计算 180
网络 181
存储 182
计算 184
场景 186
AWS 区域内灾难恢复 186
AWS 跨区域灾难恢复 188
除了 AWS 灾 AWS 难恢复 190
共享存储弹性 192
AWS 区域内灾难恢复 193
AWS 跨区域灾难恢复 193
除了 AWS 灾 AWS 难恢复 194
实施 194
SAP 应用程序层 194

SAP 数据库层 195
与 SAP 一起崛起 198
连接 199
建立与 RISE 的连接的角色和责任 200
从本地网络连接到 RISE 200
从您的 AWS 账户连接到 RISE 212
通过最近的 Di AWS rect Connect POP（包括 AWS 本地区域）连接到 RISE 225
连接到 RISE 的决策树 227
其他考虑因素 228
安全性 236
单点登录 — SAP 云身份服务和 AWS IAM 身份中心 237
单点登录 — SAP 云身份服务和微软 Entra（以前是 Azure AD） 238
单点登录 — SAPGUI 前端 239
使用 SAP 的 RISE AWS 服务实现高级安全性 240
将 SAP 密钥管理服务 (SAP KMS) 与 AWS 密钥管理服务 (AWS KMS) 集成 249
AWS Nitro 如何通过 SAP 帮助保护 RISE？ 252
Amazon WorkSpaces 是 RISE 与 SAP 合作的远程访问解决方案 255
可靠性 259
扩展 263
性能 264
数据集成 267
数据分析 272
应用程序集成 276
存档和文档管理 277
开发和扩展 281
安全扩展 283
人工智能 288
..... ccxcv

SAP 通用指南

本节涵盖以下指南。

- 概述
- Amazon EC2 实例类型
- 估计
- AWS 数据提供商
- 架构指导
- 使用 AWS 弹性灾难恢复实现灾难恢复
- 借助 SAP 在 AWS 云端崛起

关于 AWS 文档的其他 SAP

- SAP HANA 开启 AWS
- SAP NetWeaver 开启 AWS
- 适用于 SAP 应用程序的数据库 AWS
- AWS SAP 版 Launch Wizard
- AWS SAP 版 Systems Manager
- AWS 适用于 SAP 的 SDK ABA
- SAP BusinessObjects 开启 AWS
- AWS Migration Hub 协调器

SAP 谈 AWS 概述和规划

Amazon Web Services 的 SAP 专家

最后更新时间：2023 年 1 月

本指南为正在考虑实施 SAP 环境或系统或将其迁移到 Amazon Web Services 云的 SAP 客户和合作伙伴提供了概述和规划信息。

本指南适用于以前在传统本地基础架构上安装、迁移和操作 SAP 环境和系统的用户。它由三个主要部分组成：

- AWS 云和 AWS 服务概述，面向刚接触云的读者。
- SAP 概述 AWS，包括软件和许可证、支持选项以及合作伙伴服务。
- 有助于您规划和充分利用 SAP 环境@@ 的技术注意事项 AWS。

> **Note**
>
> 要访问本指南中引用的 SAP Note，您必须拥有 SAP ONE Support Launchpad 用户账户。有关详细信息，请参阅 SAP 支持网站。

关于本指南

本指南是内容系列的一部分，该系列提供了有关在 AWS 云中托管、配置和使用 SAP 技术的详细信息。有关该系列的其他指南（从概述到高级主题），请参阅 https://aws.amazon.com/sap/doc s/。

AWS 概述

AWS 提供一系列基于云的全球服务，包括计算、存储、联网、物联网 (IoT) 等。这些服务可帮助组织更快地行动、降低 IT 成本并支持可扩展性。 AWS 深受大型企业和知名初创企业的信赖，可以为各种工作负载提供支持，例如 Web 和移动应用程序、游戏开发、数据处理和仓储、存储和存档。

AWS 服务

AWS 提供 200 多种云服务，您可以根据您的业务或组织需求量身定制组合使用这些服务。有关所有 AWS 服务的信息，请参阅亚马逊 Web Services 云平台文档。

本节介绍与 SAP 解决方案的部署和操作最相关的 AWS 服务。以下列表简要描述了每项服务及其在 SAP 系统中的用途。要查看单个服务的功能、定价和文档，请点击说明后面的详细信息链接。

区域图	服务	描述	SAP 的用户
计算	亚马逊弹性计算云（亚马逊 EC2）	云端安全、可调整大小的计算容量。（详情）	用于安装和操作 SAP 系统的虚拟服务器和裸机服务器。
存储	Amazon Elastic Block Store（Amazon EBS)	用于 EC2 实例的永久性块存储卷。（详情）	SAP 软件的文件系统（例如/usr/sap）、SAP 数据库日志和数据文件以及 SAP 本地备份。
	Amazon Simple Storage Service（Amazon S3）	对象存储服务，提供极其耐用、高度可用且可无限扩展的数据存储基础架构。（详情）	用于文件备份、数据库备份、存档数据、数据湖等的高度持久存储。
	Amazon Elastic File System (Amazon EFS)	简单、可扩展的弹性文件系统，适用于基于 Linux 的工作负载，可与 AWS 云服务和本地资源一起使用。（详情）	SAP 应用程序服务器的共享文件系统（例如/sapmnt）。
	FSx 适用于 Windows 文件服务器的亚马逊	完全托管、高度耐用且可用的 Microsoft Windows 原生文件系统。（详情）	SAP 应用程序服务器的共享文件系统（例如/sapmnt）。
	FSx 适用于 NetApp ONTAP 的亚马逊	基于 NetApp ONTAP 文件系统构建的完全托管、高度可靠、可扩展、高性能的文件存储（详细信息）	SAP 应用程序服务器的共享文件系统（例如/sapmnt）。

区域图	服务	描述	SAP 的用户
联网	亚马逊虚拟计算云（亚马逊 VPC）	AWS 云中逻辑上隔离的部分，您可以在其中启动您定义的虚拟网络中的 AWS 资源。（详情）	SAP 资源的网络。您可以控制您的 EC2 实例与其他网络、实例和本地网络资源（例如生产和非生产环境中的资源）的隔离级别。
	亚马逊 Site-to-Site VPN	使您能够将本地网络或分支机构站点安全地连接到您的 VPC。（详情）	本地系统/用户与 SAP 系统之间的网络连接。 AWS
	AWS 直接 Connect	允许您在数据中心、办公室或 AWS 主机托管环境之间建立私有网络连接。（详情）	本地系统/用户与 SAP 系统或环境之间的私有网络连接。 AWS
	Amazon Route 53	高度可用且可扩展的云域名系统 (DNS) Web 服务。（详情）	上运行的 SAP 系统的名称和地址解析 AWS。
	Amazon 时间同步	高度准确和可靠的时间参考，可以从 EC2 实例本地访问。(Linux | Windows)	EC2 实例上的 SAP 系统的时间同步。
管理和操作工具	AWS 管理控制台	用于配置和管理 AWS 资源的简单 Web 界面。（详情）	为您的 SAP 环境调配和管理 AWS 资源 AWS。
	AWS 命令行界面 (AWS CLI)	用于配置和管理 AWS 资源的命令行工具集。（详情）	创建脚本以自动为你的 SAP 环境调配和管理 AWS 资源 AWS。

区域图	服务	描述	SAP 的用户
	AWS CloudFormation	一种创建相关 AWS 资源集合并以有序且可预测的方式配置这些资源的简便方法。（详情）	为新的 SAP 环境、灾难恢复环境和其他用例自动调配 AWS 资源。
	Amazon CloudWatch	监控 AWS 云资源和您运行的应用程序 AWS：收集和跟踪指标、收集和监控日志文件以及设置警报。（详情）	AWS 使用 A mazon CloudWatch 应用程序见解监控正在运行的 SAP 系统。
	AWS CloudTrail	记录在您的账户上进行的活动并将日志文件传输到您的 S3 存储桶。（详情）	您 AWS 账户内的审计功能，例如使用 Amazon EC2 API。
	AWS SAP 版 Launch Wizard	AWS Launch Wizard for SAP 是一项服务，可指导您完成 SAP 应用程序的大小、配置和部署 AWS。（详情）	设置和配置 SAP 部署所需的资源。
	AWS 适用于 SAP HANA 的 Backint Agent	SAP 认证的解决方案，用于将 SAP HANA 数据库备份到亚马逊 S3 以及从中恢复 SAP HANA 数据库。（详情）	用于将 SAP HANA 数据库备份存储到亚马逊 S3 的备份解决方案。

区域图	服务	描述	SAP 的用户
安全、身份和合规性	AWS Identity and Access Management (IAM)AWS	安全地管理对 AWS 服务和资源的访问。使用 AWS IAM，您可以创建和管理 AWS 用户和群组，并使用权限来允许和拒绝他们访问 AWS 资源。（详情）	使用权限最低的安全模型进行精细的访问控制，以访问特定的 AWS 服务和操作；例如，允许 SAP BASIS 资源在不终止 EC2 实例的情况下启动、停止和启动实例。

AWS 全球基础设施

AWS 云基础架构是围绕区域和可用区构建的。 AWS 区域是提供多个物理分隔且相互隔离的可用区域的物理位置。每个可用区都由一个或多个数据中心组成，这些数据中心通过低延迟、高吞吐量和高度冗余的网络连接。这些可用区为设计和操作应用程序和数据库提供了一种更简单、更有效的方式，与传统的单一或多数据中心基础架构相比，它们具有更高的可用性、容错性和可扩展性。

有关可用 AWS 区域的列表以及有关 AWS 全球基础设施的更多信息，请参阅 AWS 网站上的全球基础设施。

AWS 安全与合规

安全性

在 AWS，安全是我们的首要任务。作为 AWS 客户，您将受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。云端的安全性与本地数据中心的安全性非常相似，但无需支付维护设施和硬件的成本。在云中，您无需管理物理服务器或存储设备。相反，您可以使用基于软件的安全工具来监控和保护进出云资源的信息流。

作为 AWS 客户，您可以继承 AWS 政策、架构和运营流程的所有最佳实践，这些最佳实践旨在满足我们对安全最敏感的客户的需求，并获得您在安全控制方面所需的灵活性和敏捷性。

AWS 云支持责任共担模式。在 AWS 管理云安全的同时，您也要负责云中的安全。这意味着您可以控制自己选择实施的安全措施，以保护自己的数据、平台、应用程序、系统和网络，这与在现场数据中心中的安全措施没有什么不同。

要了解有关 AWS 安全的更多信息，请参阅 AWS 网站上的AWS 云安全。

合规

AWS 提供强大的控件，帮助维护云端的安全性和数据保护。由于系统建立在 AWS 云基础架构之上，因此将分担合规责任。通过将以治理为中心、便于审计的服务功能与适用的合规或审计标准相结合，AWS 合规推动者建立在传统计划的基础上，帮助您在安全控制环境中运营。 AWS

向其客户 AWS 提供的 IT 基础架构的设计和管理符合最佳安全实践和各种 IT 安全标准。以下是 AWS 符合条件的部分保障计划清单：

- SOC 1/ISAE 3402、SOC 2、SOC 3
- FISMA、FIPS、DIACAP 和 FedRAMP
- PCI DSS 等级 1
- ISO 9001、ISO 27001、ISO 27017、ISO 27701、ISO 27018

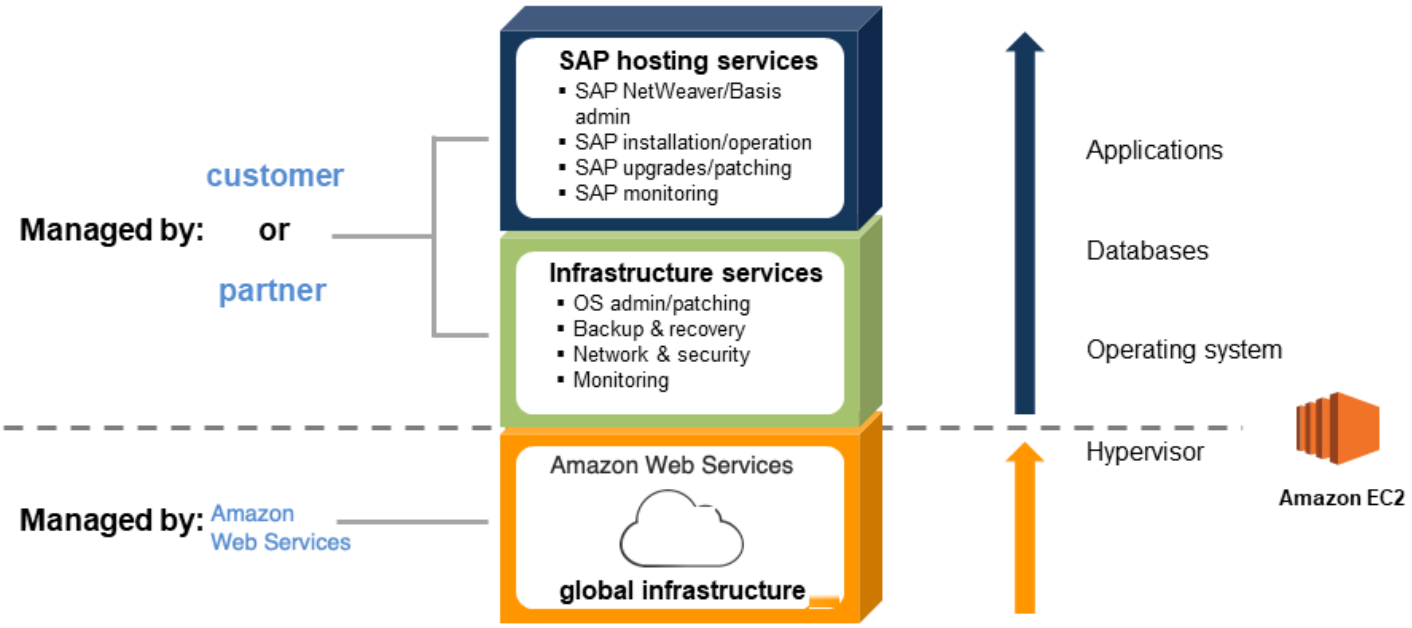
有关更多信息，请参阅 AWS 合规性计划。

AWS 配置和管理

AWS 服务和资源的配置和管理使用由客户或合作伙伴管理的自助服务模式。有关可用于配置和管理的工具的概述，请参阅 “AWS 服务” 部分中的管理工具。

图 1 显示了 SAP 由客户或合作伙伴管理的 AWS 服务和由客户或合作伙伴管理的服务。

图 1：适用于 SAP 的托管服务 AWS



SAP AWS 概述

AWS 自 2011 年以来一直与 SAP 合作，帮助客户部署和迁移他们的 SAP 应用程序 AWS，SAP 支持在上运行绝大多数可用的 SAP 应用程序 AWS。

开启的 SAP 软件和许可证 AWS

本节介绍可用于 SAP 软件和许可证的选项 AWS。

自带软件和许可证

大多数可以运行的 SAP 解决方案都 AWS 使用 bring-your-own-software和 bring-your-own-license (BYOL) 模型。在上面运行 SAP 系统 AWS 不需要特殊或新的 SAP 许可证。如果你是 SAP 的现有客户，则可以在上运行 SAP 时使用现有的 SAP 许可证 AWS。您有责任获得有效的 SAP 许可证，并且必须确保自己符合 SAP 许可政策。 AWS 不提供或销售 SAP 许可证。

AWS Marketp

AWS Marketplace 是一个数字目录，其中包含来自独立软件供应商的数千个软件清单，可让您轻松查找、测试、购买和部署在其上运行的软件 AWS。要查看 AWS Marketplace 中提供的与 SAP 相关的产品，请点击以下链接：Mark AWS etplace 中的 SAP。

SAP 试用版和开发人员许可证

S AP 云设备库提供对最新预配置 SAP 解决方案的在线存储库的访问权限。您可以使用自动部署 AWS 的启动向导快速部署这些解决方案。SAP 云设备库中提供的某些解决方案附带免费试用版或开发者版许可证。

SAP 硬件密钥生成

EC2 实例上的 SAP 硬件密钥生成使用取决于 SAP 内核补丁级别的特定过程。如果在将 SAP 内核修补到适当级别之前生成了硬件密钥，并且稍后更新了内核，则硬件密钥可能会发生变化，从而使已安装的许可证失效。有关如何在 EC2 实例上生成 SAP 硬件 ID 以及所需的 SAP 内核补丁级别的详细信息，请参阅以下 SAP 注释（需要访问 SAP One Support Launchpad）：

- SAP Note 2327159 — 虚拟和环境中的 SAP NetWeaver 许可证行为 CLoud
- SAP Note 1178686 — Linux：生成 SAP 硬件密钥的替代方法
- SAP Note 2327159 — 虚拟和云环境中的 SAP NW 许可证行为
- SAP Note 1697114 — 确定亚马逊云中的硬件 ID
- SAP Note 2113263 — 硬件 ID 的额外公钥 AWS

- SAP Note 2823805 — 硬件 ID 的其他公钥 AWS
- SAP Note 2319387 — 调整中国的执照检查 AWS

SAP Support on AWS

AWS 和 SAP 密切合作，确保无论你是在本地还是在本地运行 SAP 系统，都能通过相同的支持渠道获得相同 AWS 级别的支持。

支持 SAP 解决方案 AWS

大多数在传统本地基础架构上运行的 SAP 解决方案都由 SAP on 提供完全支持 AWS。有关支持的 SAP 解决方案的完整列表 AWS，请参阅 SAP Note 1656099 以及该说明中引用的其他注释。

SAP Support on AWS

为了确保 SAP 在 AWS 环境中全面支持你的 SAP 和 AWS，你必须遵守 SA P Note 1656 250 中的指导方针和要求。以下是为确保在 AWS 环境中支持 SAP 而必须遵循的主要要求：

- 对每个 EC2 实例启用 Amaz CloudWatch on 的详细监控，确保每隔一分钟提供所需的 AWS 指标。有关亚马逊的更多信息 CloudWatch，请参阅 https://aws.amazon.com/cloudwatch。
- 在每个 EC2 实例上安装、配置和运行适用于 SAP AWS 的数据提供器。 AWS 数据提供商从各种来源（包括亚马逊 EC2 API、Amazon EC2 实例元数据和亚马逊）收集所需的性能和配置数据 CloudWatch，并将其与 SAP 应用程序共享，以帮助监控和提高业务交易的性能。
- 你用于运行 SAP 系统的任何 AWS 账户都必须有商业AWS 支持或企业支持的支持计划。

在上部署 SAP 系统 AWS

本节介绍可用于配置 AWS 基础架构和在上安装 SAP 系统的不同选项 AWS。

手动部署

支持的大多数 SAP 解决方案 AWS 都可以通过手动配置所需的 AWS 基础架构资源，然后按照相关的 SAP 安装文档进行安装 AWS。

自动部署

AWS Launch Wizard for SAP 是一项服务，可指导您完成 SAP 应用程序的大小、配置和部署 AWS。AWS Launch Wizard 缩短了在上面部署 SAP 应用程序所需的时间 AWS。您在服务控制台上输入应用

程序要求，包括 SAP HANA 设置、SAP 环境设置和部署详细信息，然后 La AWS unch Wizard 会确定部署和运行 SAP 应用程序的相应 AWS 资源。

有关更多信息，请参阅适用于 SAP 的 AWS Launch Wizard 的工作原理。

预建镜像

某些 SAP 解决方案 AWS 以预先构建的系统映像形式提供，其中包含预安装和预配置的 SAP 系统。预构建的 SAP 系统映像使您能够快速配置新的 SAP 系统，而不必花费传统手动 SAP 安装所需的时间和精力。

预构建的 SAP 系统映像可从以下来源获得：

- AWS Marketp
- SAP 云设备库

SAP 解决方案	部署选项
SAP 商务套件（ERP、CRM 等）	手册 | SAP CAL
SAP NetWeaver	手册 | SAP AWS 版 Launch Wizard | SAP CAL
SAP S/4HANA	手册 | SAP AWS 版 Launch Wizard | SAP CAL
SAP BW/4HANA	手册 | SAP CAL
SAP HANA	手册 | SAP AWS 版 Launch Wizard | SAP CAL
SAP BusinessObjects BI	手册 | AWS Marketplace | SAP
SAP 商务部（Hybris）	手动
SAP 商业一号，适用于 SAP HANA 的版本	手册 | SAP CAL
SAP 商业一号，适用于微软 SQL Server 的版本	手动

从 APN 合作伙伴那里获得帮助

有些 AWS 合作伙伴网络 (APN) 合作伙伴在部署和运营 SAP 解决方案方面经验丰富，可以帮助您处理 SAP 工作负 AWS载。有关更多信息，请参阅以下部分。

适用于 SAP 的合作伙伴服务 AWS

AWS 合作伙伴网络 (APN) 是一个由提供各种服务和产品的公司组成的社区。 AWS APN SAP 合作伙伴可以提供特定于 SAP 的服务，以帮助您最大限度地发挥在上运行 SAP 解决方案的好处。 AWS

适用于 SAP 的合作伙伴服务和解决方案的类型 AWS

- 云评估服务 — 咨询服务可帮助您为云采用之旅制定高效、有效的计划。典型的服务包括财务/TCO（总拥有成本）、技术、安全和合规以及许可。
- Proof-of-concept 服务 — 帮助您测试 SAP 的服务 AWS；例如：SAP ERP/ECC migration to SAP HANA or SAP S/4HANA, SAP Business Warehouse (BW) migration to SAP HANA or SAP BW/4HANA, SAP OS/DB 迁移、新的 SAP 解决方案实施。
- 迁移服务 — 用于将现有 SAP 环境或系统迁移到的服务 AWS；例如：All-on-AWS SAP 迁移 (PRD/QAS/DEV), hybrid SAP migrations (QAS/DEV)、单个 SAP 系统（例如 SAP BW）迁移。
- 托管服务 — 针对 SAP 环境的托管服务 AWS，包括： AWS 账户和资源管理、操作系统管理/修补、备份和恢复、SAP Basis 和 SAP。 NetWeaver
- 打包解决方案 — SAP 合作伙伴提供的捆绑软件和服务产品，将 SAP 软件、许可证、实施和托管服务结合在一起 AWS，例如 SAP S/4HANA、SAP BusinessObjects BI 等。
- ISV 软件解决方案 — 合作伙伴软件解决方案，用于迁移、集成和运行 SAP 解决方案 AWS；例如：系统迁移、高可用性、备份和恢复、数据复制、自动扩展、灾难恢复。

如何在 SAP 上找到合作伙伴解决方案 AWS

AWS SAP Partner Sol utions 提供了一个集中式平台，供您搜索、发现值得信赖的 APN 合作伙伴并与之建立联系，这些合作伙伴提供解决方案和服务，帮助您的企业更快地实现价值，并最大限度地发挥运行 SAP 解决方案的优势。 AWS有关更多信息，请参阅 AWS SAP 能力合作伙伴。

SAP 谈 AWS 规划

如果你是一位经验丰富的 SAP Basis 或 SAP 管理 NetWeaver 员，那么有许多与计算配置、存储、安全、管理和监控相关的 AWS特定注意事项可以帮助你充分利用 SAP 环境。 AWS本节提供了在运行 SAP 解决方案时实现最佳性能、可用性和可靠性以及降低总拥有成本 (TCO) 的指导方针。 AWS

SAP 笔记

在迁移或实施 SAP 环境之前 AWS，应阅读并遵循相关的 SAP 注意事项。从 SAP Note 1656099 开始获取一般信息，然后点击其他相关 SAP 笔记的链接（需要访问 SAP One Support Launchpad）。

AWS 架构上的 SAP

本节介绍了 SAP 上的两种主要架构模式 AWS：所有系统开启 AWS 和混合模式。

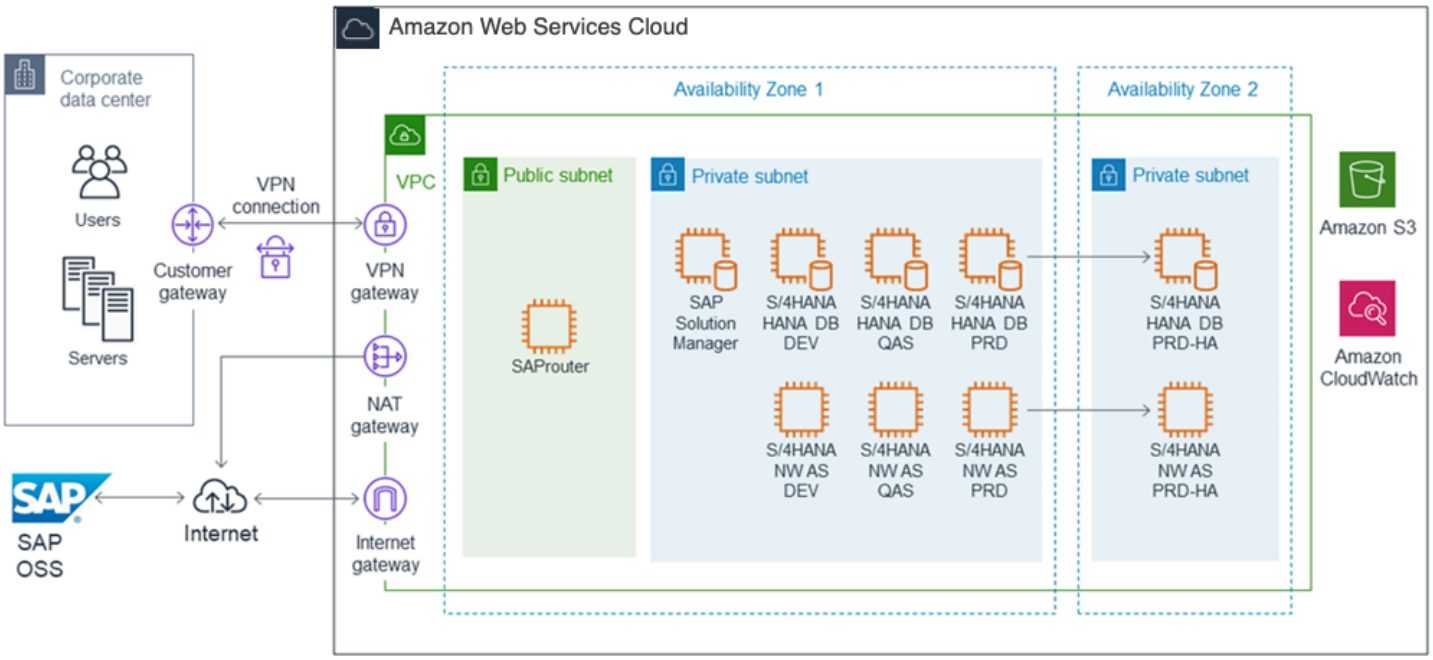
全能架构AWS

借助 SAP All-on AWS 架构，您的 SAP 环境的所有系统和组件都托管在其上 AWS。此类架构的示例场景包括：

- 在上实施一个完整的、全新 SAP 环境 AWS
- 将完整的现有 SAP 环境迁移到 AWS

图 3 描绘了 SAP 全能架构。AWS 运行的 SAP 环境通过 VPN 连接或通过 Di AWS rect AWS s Connect 的专用网络连接与本地系统和用户集成。 SAProuter 部署在公有子网中，并分配了一个可从互联网访问的公有 IP 地址，以便能够通过安全网络通信 (SNC) 连接与 SAP OSS 网络集成。网络地址转换 (NAT) 网关使私有子网中的实例能够连接到 Internet 或其他 AWS 服务，但可以防止实例接收 Internet 上某人发起的入站流量。有关更多信息，请参阅 “配置网络和连接” 部分。

图 3：SAP 全能架构AWS



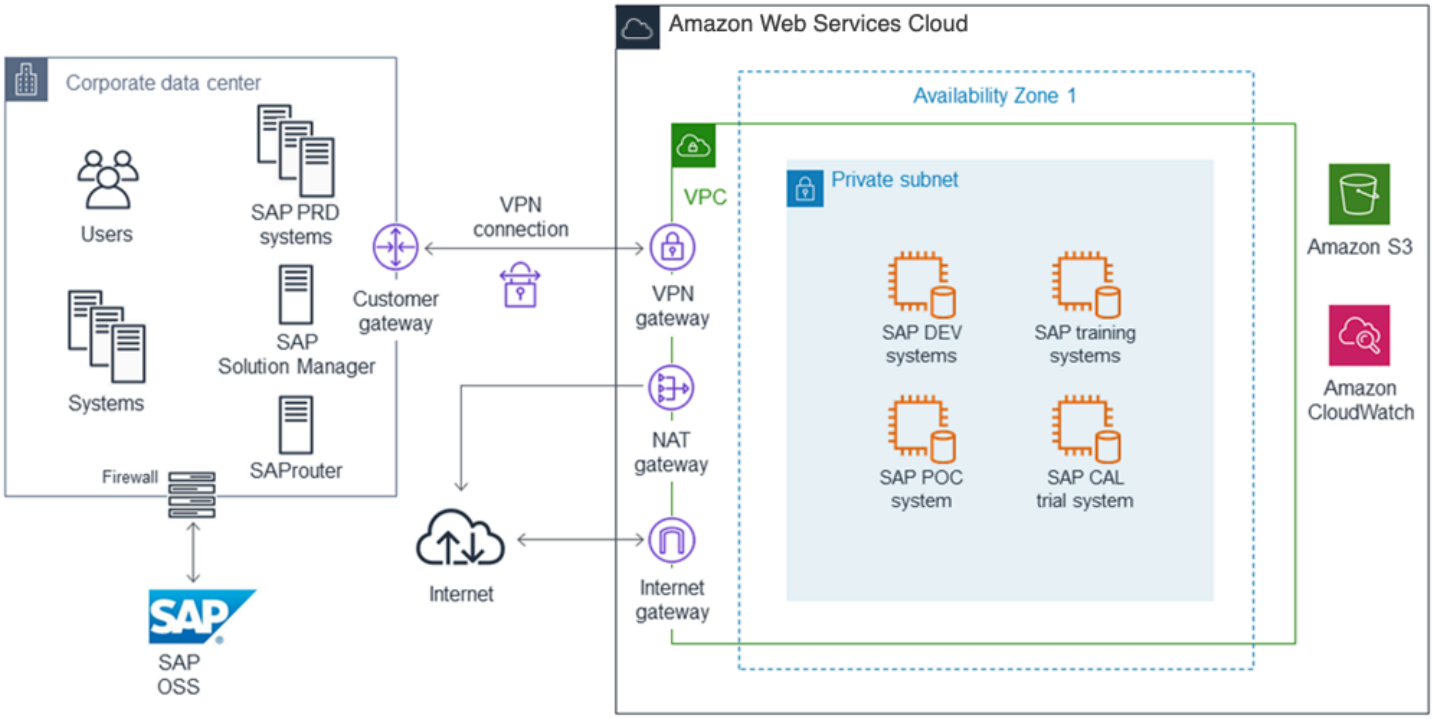
混合 AWS 架构

使用 SAP 混合 AWS 架构，一些 SAP 系统和组件托管在您的本地基础架构上，而另一些则托管在 AWS 基础架构上。此类架构的示例场景包括：

- 在上运行 SAP 测试、试用、培训 proof-of-concept (PoC) 和类似系统 AWS
- 在上面运行非生产 SAP 环境（例如 DEV 和 QAS） AWS，与本地运行的 SAP 生产环境集成
- 在现有的 SAP 本地环境上实施新的 SAP 应用程序 AWS 并将其集成到现有的 SAP 本地环境中

图 4 描绘了 SAP 混合 AWS 架构，其中包含 SAP 开发和 QAS 环境以及 SAP 测试、培训和 PoC 系统。 AWS这些系统与企业网络上的 SAP 系统和用户集成。VPC 和公司网络之间的连接通过 VPN 连接或 Directs Conn AWS ect 连接提供。企业网络上运行的现有 SAProuter 和 SAP 解决方案管理器用于管理在 VPC 中运行的 SAP 系统。

图 4：SAP 混合 AWS 架构



选择 AWS 区域和可用区

有关 AWS 区域和可用区的信息，请参阅本指南的AWS 全球基础设施部分。

选择区域

在选择要在 AWS 其中部署 SAP 环境的区域时，请考虑以下因素：

- 靠近您的本地数据中心、系统和最终用户，以最大限度地减少网络延迟。
- 数据驻留和监管合规要求。

- 您计划在该地区使用的 AWS 产品和服务的可用性。有关按地区划分 AWS 的产品和服务的详细列表，请参阅 AWS 网站上的区域表。
- 您计划在该地区使用的 EC2 实例类型的可用性。要查看特定实例类型的 AWS 区域可用性，请参阅适用于 SAP 的 Amazon EC2 实例类型网页。

选择可用区

在为 SAP 部署选择可用区时，无需特别考虑 AWS。所有 SAP 应用程序（SAP ERP、CRM、SRM 等）和系统（SAP 数据库系统、SAP 中央服务系统和 SAP 应用程序服务器）都应部署在同一个可用区中。如果需要高可用性 (HA)，请使用多个可用区。有关更多信息，请参阅上的 SAP 可用性和可靠性架构指南 AWS。

网络和连接

Amazon VPC

Amazon VPC 使您能够在 AWS 云中自己的、逻辑上隔离的区域中定义虚拟网络。您可以将您的 AWS 资源（例如实例）启动到您的 VPC 中。您的 VPC 与您可能在自己的数据中心运行的传统网络非常相似，其优势在于使用 AWS 可扩展的基础架构。您可以配置您的 VPC；您可以选择它的 IP 地址范围、创建子网并配置路由表、网关和安全设置。您可以将您的 VPC 中的实例连接到网络。您可以将 VPC 连接到您自己的企业数据中心，并使 AWS 云成为数据中心的扩展。要保护各个子网中的资源，您可以利用多种安全层，包括安全组和网络访问控制列表。有关更多信息，请参阅《Amazon VPC 用户指南》。

有关设置和配置 VPC 以及您的网络与 VPC 之间连接的详细说明，请参阅 Amazon VPC 文档。

网络连接选项

有多种选项可用于在本地用户和运行 SAP 系统的系统之间提供网络连接 AWS，包括直接互联网连接、硬件 VPN 和专用网络连接。

私有网络连接

AWS Di@@ rects Connect 可以轻松建立从您的场所到 AWS. 使用 D AWS irects Connect，您可以在数据中心、办公室或主机托管环境之间 AWS 建立私有连接。在许多情况下，这可以降低您的网络成本，增加带宽吞吐量，并提供比基于互联网的连接更稳定的网络体验。有关更多信息，请参阅 Directs AWS Connect 用户指南。

用例：建议要求比硬件 VPN 更高的带宽和更低延迟的客户使用。

有关更多信息，请参阅 Amazon 虚拟计算云连接选项。

直接连接互联网

连接到运行的 SAP 系统的最快、最简单的方法是使用具有单个公有子网和互联网网关的 VPC 来实现通过互联网进行通信。 AWS 有关更多信息，请参阅 Amazon VPC 用户指南中的场景 1：仅包含公有子网的 VPC。

用例：最适合不包含敏感数据的 SAP 演示、训练和测试型系统。

Site-to-Site /硬件 VPN

AWS Site-to-Site VPN 通过互联网协议安全 (IPsec) 隧道将您的数据中心或分支机构扩展到云端，并支持连接到虚拟专用网关和 T AWS ransit Gateway。您可以选择通过 IPsec 隧道运行边界网关协议 (BGP)，以获得高可用性的解决方案。有关更多信息，请参阅 Amazon VPC 用户指南中的向您的 VPC 添加硬件虚拟私有网关。

用例：建议用于需要与本地用户和系统集成的任何 SAP 环境。 AWS

Client VPN

AWS Client VPN 提供完全托管的 VPN 解决方案，通过互联网连接和兼容 OpenVPN 的客户端，可以从任何地方进行访问。它具有弹性，可自动扩展以满足您的需求，并允许您的用户同时 AWS 连接到本地网络。 AWS Client VPN 可与您的现有 AWS 基础设施（包括 Amazon VPC 和 AWS Directory Service）无缝集成，因此您无需更改网络拓扑。

用例：为您的远程员工和业务合作伙伴提供快速、轻松的连接。

遵循安全最佳实践

为了提供 end-to-end安全和 end-to-end隐私，根据安全最佳实践 AWS 构建服务，在这些服务中提供适当的安全功能，并记录如何使用这些功能。此外， AWS 客户必须使用这些功能和最佳实践来构建适当安全的应用程序环境。让客户能够确保其数据的机密性、完整性和可用性对于保持信任和信心至关重要。 AWS

责任共担环境

作为客户的您与客户之间存在一种共担责任模式 AWS。 AWS 操作、管理和控制从主机操作系统和虚拟化层到服务运行设施的物理安全的组件。反过来，您负责并管理客户机操作系统（包括更新和安全补丁）、其他相关应用程序软件、Amazon VPC 设置和配置以及 AWS提供的安全组防火墙的配置。有关 AWS 安全性的更多信息，请访问AWS 云安全页面并查看那里提供的各种安全资源。

Amazon VPC

SAP 环境安全的基础 AWS 是使用 Amazon VPC 提供整体隔离。Amazon VPC 包含安全细节，您必须设置这些详细信息才能正确访问和限制您的资源。Amazon VPC 提供的功能可用于帮助提高和监控 VPC 的安全：

- 安全组充当关联 EC2 实例的防火墙，在实例级别控制入站和出站流量。
- 网络访问控制列表 (ACLs) 充当关联子网的防火墙，在子网级别控制入站和出站流量。
- 路由表由一组称为路由的规则组成，用于确定网络流量的定向位置。在您的 VPC 中的每个子网必须与一个路由表关联；路由表控制子网的路由。
- 流日志会捕获有关进出您的 VPC 中网络接口的 IP 流量的信息。

有关如何在 VPC 内设置和管理安全的详细文档，请参阅 Amazon VPC 用户指南的安全部分。

EC2 SAP 的实例类型

Amazon EC2 提供多种经过优化的实例类型，以适应不同的用例。实例类型包括 CPU、内存、存储和网络容量的不同组合，便于您灵活选择适合应用程序的资源组合。每种实例类型都包含一个或多个实例大小，您可以根据目标工作负载的要求扩展资源。

部署在上面需要 AWS 来自 SAP 支持的 SAP 系统必须在已通过 SAP 认证的 EC2 实例类型上运行。本节介绍在哪里可以找到有关已通过 SAP 认证的 EC2 实例类型的详细信息以及特定 SAP 解决方案的其他信息。

NetWeaver基于 SAP 的解决方案

基于 SAP NetWeaver 平台且使用 SA P 应用程序性能标准 (SAPS) 进行规模调整的 SAP 解决方案必须在特定的 EC2 实例类型子集上运行，才能获得 SAP Support 的支持。有关详细信息，请参阅：

- SAP Note 1656099
- 适用于 SAP 的 Amazon EC2 类型

SAP HANA

在 SAP HANA 数据库之上运行的 SAP HANA 平台和 SAP 解决方案（例如 HANA 上的 SAP Suite、HANA 上的 SAP S/4HANA、HANA 上的 SAP Business Warehouse (BW)、SAP BW/4HANA — 需要已通过 SAP HANA 认证的特定 EC2 实例类型。有关更多信息，请参阅上的 Amazon SAP EC2 实例类型 AWS。

SAP 商业一号，适用于 SAP HANA 的版本

有关通过 SAP Business One（适用于 SAP HANA 的版本）认证的 EC2 实例类型的信息，请参阅：

- SAP Note 2058870
- SAP Business on AWS

操作系统

受支持的操作系统

EC2 实例在基于英特尔 x86 指令集的 64 位虚拟处理器上运行。以下 64 位操作系统和版本可用并支持上 AWS的 SAP 解决方案。

- SUSE Linux 企业服务器 (SLES)
- 适用于 SAP 应用程序的 SUSE Linux 企业服务器（适用于 SAP 的 SLES）
- 红帽企业 Linux (RHEL)
- 适用于 SAP 解决方案的红帽企业 Linux（适用于 SAP 的 RHEL）
- Microsoft Windows Server
- 甲骨文企业 Linu

有关上支持 SAP 的操作系统的更多信息 AWS，请参阅 SAP Note 1656250。

SAP 的 SLES 和 SAP 的 RHEL

SUSE 和 Red Hat 提供特定于 SAP 的操作系统版本，具有以下优势：

- SAP 的配置和调整
- 扩展版本支持
- 适用于 SAP 的高可用性扩展
- 专门的支持渠道

> **Note**
>
> 由于这些好处，我们强烈建议在部署时使用适用于 SAP 的 SLES 或具有高可用性 (HA) 和更新服务 (美国) 的 SAP 版 RHEL。 AWS

要详细了解 SUSE 和红帽的 SAP 操作系统版本，请参阅 SLES 和红帽网站上的以下信息。

SLES for SAP

- 一般信息
- SUSE 开启 AWS 适用于 SAP 应用程序

RHEL for SAP

- 一般信息
- 公共云中的红帽
- 红帽云接入
- 如何在亚马逊上找到红帽 Cloud Access 金牌图片 EC2
- 公共云中的红帽云访问和红帽企业 Linux 按需订阅有什么区别？

操作系统许可证

这些操作系统许可选项可用于 SAP 系统，网址 AWS为：

- 按需 — 操作系统软件和许可证捆绑在 Amazon 系统映像 (AMI) 中。操作系统许可证的费用包含在按需实例小时费用或该实例类型的预留实例费用中。
- 自带许可证/订阅 (BYOL)-将您现有的操作系统许可证或订阅带到云端。 AWS
- AWS Marketplace — 从 Mark AWS etplace 购买操作系统许可证和订阅。

下表列出了适用于每个操作系统和版本的许可选项。要了解有关每个选项的更多信息，请点击表格中的链接。

操作系统	许可证/订阅选项
SLES	点播 | BYOL
适用于 SAP 的 SLES	AWS 市场 | BYOL
RHEL	点播 | BYOL
带有 HA 和 US 的 SAP 版 RHEL	AWS 市场 | BYOL

操作系统	许可证/订阅选项
Windows	点播 | BYOL
Oracle Linux	BYOL

数据库

支持的数据库

SAP 还支持 SAP 为本地基础架构支持的所有数据库平台和版本 AWS。有关上特定 SAP 解决方案支持的数据库的详细信息 AWS，请参阅 SA P Note 165 6099。

数据库安装和管理

亚马逊上的客户托管数据库 EC2

大多数 SAP 解决方案在 Amazon EC2 上都使用客户托管模式。数据库的安装、配置、管理、备份和恢复均由客户或合作伙伴完成。

以下 SAP 解决方案在 Amazon EC2 上使用自我管理的数据库模型：

- SAP 商务套件和 NetWeaver基于 SAP 的应用程序
- SAP HANA
- SAP S/4HANA
- SAP BW/4HANA
- SAP BusinessObjects BI
- SAP 商业一号

Amazon RDS

Amazon Relational Database Service（Amazon RDS）是一项托管服务，可以轻松地在云中设置、操作和扩展关系数据库。它提供经济实惠且可调整大小的容量，同时管理耗时的数据库管理任务，让您可以腾出时间专注于应用程序和业务。以下 SAP 解决方案目前支持 Amazon RDS：

- SAP BusinessObjects BI

- SAP 商务（以前称为 SAP Hybris Commerce）

Amazon Aurora

Amazon Aurora（Aurora）是专为云构建的兼容 MySQL 和 PostgreSQL 的关系数据库。它将传统企业数据库的性能和可用性与开源数据库的简单性和成本效益相结合。以下 SAP 解决方案目前支持 Aurora MySQL：

- SAP 商务（以前称为 SAP Hybris Commerce）

数据库许可证

这些数据库许可选项可用于 SAP 系统，网址 AWS为：

- 按需 — 数据库软件和许可证捆绑在 Amazon 系统映像 (AMI) 中。数据库许可证费用包含在按需实例小时费用或该实例类型的预留实例费用中。
- 自带许可证 (BYOL)-将您现有的数据库许可证带到 AWS 云端。
- AWS Marketplace — 从 Mar AWS ketplace 购买数据库软件和许可证。

下表列出了每个数据库 AWS 的可用许可选项。有关更多信息，请访问许可选项列中的链接。

数据库	许可选项
SAP HANA	BYOL
SAP 自适应服务器企业版 (ASE) (SAP ASE)	BYOL
Microsoft SQL Server	BYOL *
IBM DB2	BYOL
Oracle	BYOL
Amazon Aurora	按需

- 从 SAP 购买的 SQL Server 运行时许可证需要微软软件保障或亚马逊 EC2 专用主机才能获得这些许可证 AWS。有关更多信息，请参阅：

- SAP Note 2139358——SQL Server 许可条款变更的影响
- 微软许可开启 AWS

SAP 安装媒体

大多数 SAP 解决方案都 AWS 使用 bring-your-own-software模型。将 SAP 安装媒体复制到 AWS：

- 从 SAP 软件下载中心下载到 Amazon EC2。从您的 EC2 实例连接到 SAP 软件下载中心并下载所需的安装媒体。此选项很可能是获取 SAP 安装媒体的最快方法 AWS，因为 EC2 实例与互联网的连接速度非常快。您可以创建专用 Amazon EBS 卷来存储安装媒体，然后根据需要将该卷连接到不同的实例。您还可以创建 Amazon EBS 卷的快照，并创建多个可以并行连接到多个实例的卷。
- 从您的网络复制到 Amazon EC2。如果您已经将所需的 SAP 安装媒体下载到网络上的某个位置，则可以将媒体从网络直接复制到 EC2 实例。

SAProuter 和 SAP 解决方案经理

以下各节介绍在上运行 SAP 解决方案时 SAProuter 和 SAP 解决方案管理器的选项 AWS。

适用于 SAP 的全能架构AWS

在开启 SAP 环境时 AWS，您需要设置 SAP Solution Manager 系统并 SAProuter 连接到 SAP 支持网络，就像使用任何基础架构一样。有关插图，请参见全能AWS 架构图 (the section called “图 3：SAP 全能架构AWS”)。

设置 SAProuter 和 SAP 支持的网络连接时，请遵循以下准则：

- 将安装 SAProuter 软件的实例启动到 VPC 的公有子网中，并为其分配弹性 IP 地址。
- 使用必要的规则为 SAProuter 实例创建特定的安全组，以允许所需的入站和出站访问 SAP 支持网络。
- 使用安全网络通信 (SNC) 类型的互联网连接。有关更多信息，请参阅 https://service.sap.com/internet connection。

适用于 SAP 混合 AWS 架构

当使用 AWS 作为 IT 基础设施的扩展时，您可以使用在数据中心运行的现有 SAP Solution Manager 系统来管理在 VPC AWS 中运行的 SAP 系统。 SAProuter 有关更多信息，请参阅混合架构图（图 4）。

文档修订

日期	更改	位置
2023年1月	更新	整个指南中的更改
2019年5月	更新	整个指南中的更改
2018年8月	初次发布	–

适用于 SAP 的 Amazon EC2 实例类型 AWS

Amazon Elastic Compute Cloud (Amazon EC2) 提供多种针对不同用例进行了优化的实例类型。CPU、内存、存储和网络容量的不同组合为应用程序选择资源提供了灵活性。您可以选择满足您的工作负载要求的实例类型。

AWS 已与 SAP 密切合作，针对 AWS 解决方案对 SAP 的 Amazon EC2 实例类型进行了测试和认证。有关更多信息，请参阅 SAP Note 1656099——SAP 应用程序，网址 AWS为：支持的产品和 DB/OS 亚马逊 EC2 产品（需要访问 SAP 门户）以及 SA P 认证和支持的 SAP HANA 硬件目录。

主题

- 实例类型可用性
- SAP NetWeaver 支持的实例
- SAP HANA 认证和非认证实例
- SAP Business One 认证实例，SAP HANA 版本
- 在 SAP 上记录实例类型的历史记录 AWS

实例类型可用性

Amazon EC2 实例类型的可用性取决于您选择的区域。有关您所在地区的可用实例类型的更多信息，请参阅亚马逊 EC2 实例类型指南中的按地区划分的亚马逊 EC2 实例类型。

> **Note**
>
> 某些 Amazon EC2 实例系列，例如 X1、x2iDN、x2iDN 和高内存，可能无法在一个地区的所有可用区域中使用。在规划时，您必须确认 SAP 工作负载所需的实例类型是否在目标可用区中可用。

您还可以使用describe-instance-type-offerings命令来确定某个区域及其可用区中某个实例类型的可用性。有关示例，请参阅 Amazon EC2 用户指南中的使用 AWS CLI 查找实例类型。

SAP NetWeaver 支持的实例

完全支持适用于 SAP NetWeaver 的上一代 Amazon EC2 实例，并且这些实例类型保留了相同的特性和功能。我们建议使用最新一代的 Amazon EC2 实例进行新的 SAP NetWeaver 实施或迁移。

主题

- SAP 的当前一代实例 NetWeaver
- 上一代 SAP 实例 NetWeaver

SAP 的当前一代实例 NetWeaver

Example

General Purpose

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
m5.large	2	8	2,817	高	最多 4,750	18,750
m5.xlarge	4	16	5,535	高	最多 4,750	18,750
m5.2xlarge	8	32	11,269	高	最多 4,750	18,750
m5.4xlarge	16	64	22,538	高	4750	18,750
m5.8xlarge	32	128	45,077	10	6800	30000
m5.12xlarge	48	192	67,615	10	9500	40000
m5.16xlarge	64	256	90,153	20	13600	60000
m5.24xlarge	96	384	135,230	25	19000	80,000
m5.metal	96	384	142,000	25	19000	80,000
m6a.large	2	8	3,023	最多 12.5	最高 10,000	40000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
m6a.xlarge	4	16	6,046	最多 12.5	最高 10,000	40000
m6a.2xlarge	8	32	12,093	最多 12.5	最高 10,000	40000
m6a.4xlarge	16	64	24,185	最多 12.5	最高 10,000	40000
m6a.8xlarge	32	128	48,370	12.5	10000	40000
m6a.12xlarge	48	192	72,555	18.75	15000	60000
m6a.16xlarge	64	256	96,740	25	20000	80,000
m6a.24xlarge	96	384	145,110	37.5	30000	120,000
m6a.32xlarge	128	512	193,480	50	40000	160000
m6a.48xlarge	192	768	290,220	50	40000	240,000
m6i.large	2	8	3,095	最多 12.5	最高 10,000	40000
m6i.xlarge	4	16	6,190	最多 12.5	最高 10,000	40000
m6i.2xlarge	8	32	12,380	最多 12.5	最高 10,000	40000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
m6i.4xlarge	16	64	24,760	最多 12.5	最高 10,000	40000
m6i.8xlarge	32	128	49,520	12.5	10000	40000
m6i.12xlarge	48	192	74,280	18.75	15000	60000
m6i.16xlarge	64	256	99,040	25	20,600	80,000
m6i.24xlarge	96	384	148,560	37.5	30000	120,000
m6i.32xlarge	128	512	198,080	50	40000	160000
m6id.large	2	8	3,095	最多 12.5	最高 10,000	40000
m6id.xlarge	4	16	6,190	最多 12.5	最高 10,000	40000
m6id.2xlarge	8	32	12,380	最多 12.5	最高 10,000	40000
m6id.4xlarge	16	64	24,760	最多 12.5	最高 10,000	40000
m6id.8xlarge	32	128	49,520	12.5	10000	40000
m6id.12xlarge	48	192	74,280	18.75	15000	60000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
m6id.16xlarge	64	256	99,040	25	20,600	80,000
m6id.24xlarge	96	384	148,560	37.5	30000	120,000
m6id.32xlarge	128	512	198,080	50	40000	160000
m6idn.large	2	8	3,095	最多 25	最多 25,000	100000
m6idn.xlarge	4	16	6,190	最多 30	最多 25,000	100000
m6idn.2xlarge	8	32	12,380	最多 40	最多 25,000	100000
m6idn.4xlarge	16	64	24,760	最多 50	最多 25,000	100000
m6idn.8xlarge	32	128	49,520	50	25000	100000
m6idn.12xlarge	48	192	74,280	75	37,500	15万
m6idn.16xlarge	64	256	99,040	100	50000	200,000
m6idn.24xlarge	96	384	148,560	150	75000	300,000
m6idn.32xlarge	128	512	198,080	200	100000	400,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
m6in.large	2	8	3,095	最多 25	最多 25,000	100000
m6in.xlarge	4	16	6,190	最多 30	最多 25,000	100000
m6in.2xlarge	8	32	12,380	最多 40	最多 25,000	100000
m6in.4xlarge	16	64	24,760	最多 50	最多 25,000	100000
m6in.8xlarge	32	128	49,520	50	25000	100000
m6in.12xlarge	48	192	74,280	75	37,500	15万
m6in.16xlarge	64	256	99,040	100	50000	200,000
m6in.24xlarge	96	384	148,560	150	75000	300,000
m6in.32xlarge	128	512	198,080	200	100000	400,000
m7a.medium	1	4	2,238	最多 12.5	最高 10,000	最多 40,000
m7a.large	2	8	4,476	最多 12.5	最高 10,000	最多 40,000
m7a.xlarge	4	16	8,952	最多 12.5	最高 10,000	最多 40,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
m7a.2xlarge	8	32	17,904	最多 12.5	最高 10,000	最多 40,000
m7a.4xlarge	16	64	35,808	最多 12.5	最高 10,000	最多 40,000
m7a.8xlarge	32	128	71,616	12.5	10000	40000
m7a.12xlarge	48	192	107,424	18.75	15000	60000
m7a.16xlarge	64	256	143,232	25	20000	80,000
m7a.24xlarge	96	384	214,848	37.5	30000	120,000
m7a.32xlarge	128	512	286,464	50	40000	160000
m7a.48xlarge	192	768	429,720	50	40000	240,000
m7i.large	2	8	4,218	最多 12.5	最高 10,000	最多 40,000
m7i.xlarge	4	16	8,435	最多 12.5	最高 10,000	最多 40,000
m7i.2xlarge	8	32	16,870	最多 12.5	最高 10,000	最多 40,000
m7i.4xlarge	16	64	33,740	最多 12.5	最高 10,000	最多 40,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
m7i.8xlarge	32	128	67,480	12.5	10000	40000
m7i.12xlarge	48	192	101,200	18.75	15000	60000
m7i.16xlarge	64	256	123,300	25	20000	80,000
m7i.24xlarge	96	384	167,470	37.5	30000	120,000
m7i.48xlarge*	192	768	306,202	50	40000	240,000

Compute Optimized

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
c5.large	2	4	2,650	最多 10	最多 4,750	20000
c5.xlarge	4	8	5,300	最多 10	最多 4,750	20000
c5.2xlarge	8	16	10,600	最多 10	最多 4,750	20000
c5.4xlarge	16	32	21,200	最多 10	4750	20000
c5.9xlarge	36	72	47,700	10	9500	40000
c5.18xlarge	72	144	95,400	25	19000	80,000
c5a.large	2	4	2,746	最多 10	最多 3,170	13300
c5a.xlarge	4	8	5,493	最多 10	最多 3,170	13300

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
c5a.2xlarge	8	16	10,986	最多 10	最多 3,170	13300
c5a.4xlarge	16	32	21,973	最多 10	最多 3,170	13300
c5a.8xlarge	32	64	43,943	10	3,170	13300
c5a.12xlarge	48	96	65,915	12	4750	20000
c5a.16xlarge	64	128	87,887	20	6,300	26700
c5a.24xlarge	96	192	131,830	20	9500	40000
c5n.large	2	5	2,650	最多 25	最多 4,750	20000
c5n.xlarge	4	11	5,300	最多 25	最多 4,750	20000
c5n.2xlarge	8	21	10,600	最多 25	最多 4,750	20000
c5n.4xlarge	16	42	21,200	最多 25	4750	20000
c5n.9xlarge	36	96	47,700	50	9500	40000
c5n.18xlarge	72	192	95,400	100	19000	80,000
c6a.large	2	4	2,864	最多 12.5	最高 10,000	40000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
c6a.xlarge	4	8	5,727	最多 12.5	最高 10,000	40000
c6a.2xlarge	8	16	11,454	最多 12.5	最高 10,000	40000
c6a.4xlarge	16	32	22,908	最多 12.5	最高 10,000	40000
c6a.8xlarge	32	64	45,817	12.5	10000	40000
c6a.12xlarge	48	96	68,725	18.75	15000	60000
c6a.16xlarge	64	128	91,633	25	20000	80,000
c6a.24xlarge	96	192	137,450	37.5	30000	120,000
c6a.32xlarge	128	256	183,267	50	40000	160000
c6a.48xlarge	192	384	274,900	50	40000	240,000
c6i.large	2	4	2,950	最多 12.5	最高 10,000	40000
c6i.xlarge	4	8	5,899	最多 12.5	最高 10,000	40000
c6i.2xlarge	8	16	11,799	最多 12.5	最高 10,000	40000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
c6i.4xlarge	16	32	23,598	最多 12.5	最高 10,000	40000
c6i.8xlarge	32	64	47,195	12.5	10000	40000
c6i.12xlarge	48	96	70,793	18.75	15000	60000
c6i.16xlarge	64	128	94,390	25	20,600	80,000
c6i.24xlarge	96	192	141,585	37.5	30000	120,000
c6i.32xlarge	128	256	188,780	50	40000	160000
c6id.large	2	4	2,950	最多 12.5	最高 10,000	40000
c6id.xlarge	4	8	5,899	最多 12.5	最高 10,000	40000
c6id.2xlarge	8	16	11,799	最多 12.5	最高 10,000	40000
c6id.4xlarge	16	32	23,598	最多 12.5	最高 10,000	40000
c6id.8xlarge	32	64	47,195	12.5	10000	40000
c6id.12xlarge	48	96	70,793	18.75	15000	60000
c6id.16xlarge	64	128	94,390	25	20,600	80,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
c6id.24xlarge	96	192	141,585	37.5	30000	120,000
c6id.32xlarge	128	256	188,780	50	40000	160000

Memory Optimized

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
r5.large	2	16	2,891	最多 10	最多 4,750	18,750
r5.xlarge	4	32	5,782	最多 10	最多 4,750	18,750
r5.2xlarge	8	64	11,564	最多 10	最多 4,750	18,750
r5.4xlarge	16	128	23,128	最多 10	4750	18,750
r5.8xlarge	32	256	46,257	10	6800	30000
r5.12xlarge	48	384	69,385	10	9500	40000
r5.16xlarge	64	512	92,513	20	13600	60000
r5.24xlarge	96	768	138,770	25	19000	80,000
r5.metal	96	768	143,230	25	19000	80,000
r5b.large	2	16	2,891	最多 10	最高 10,000	43333

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
r5b.xlarge	4	32	5,782	最多 10	最高 10,000	43333
r5b.2xlarge	8	64	11,564	最多 10	最高 10,000	43333
r5b.4xlarge	16	128	23,128	最多 10	10000	43333
r5b.8xlarge	32	256	46,257	25	20000	86667
r5b.12xlarge	48	384	69,385	50	30000	130,000
r5b.16xlarge	64	512	92,513	75	40000	173333
r5b.24xlarge	96	768	138,770	100	60000	260000
r5b.metal	96	768	143,230	100	60000	260000
r5n.large	2	16	2,891	最多 25	最多 4,750	18,750
r5n.xlarge	4	32	5,782	最多 25	最多 4,750	18,750
r5n.2xlarge	8	64	11,564	最多 25	最多 4,750	18,750
r5n.4xlarge	16	128	23,128	最多 25	4750	18,750
r5n.8xlarge	32	256	46,257	25	6800	30000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
r5n.12xlarge	48	384	69,385	50	9500	40000
r5n.16xlarge	64	512	92,513	75	13600	60000
r5n.24xlarge	96	768	138,770	100	19000	80,000
r5n.metal	96	768	143,230	100	19000	80,000
r6a.large	2	16	2,984	最多 12.5	最高 10,000	40000
r6a.xlarge	4	32	5,968	最多 12.5	最高 10,000	40000
r6g.2xlarge	8	64	11,935	最多 12.5	最高 10,000	40000
r6a.4xlarge	16	128	23,871	最多 12.5	最高 10,000	40000
r6a.8xlarge	32	256	47,742	12.5	10000	40000
r6a.12xlarge	48	384	71,613	18.75	15000	60000
r6a.16xlarge	64	512	95,483	25	20000	80,000
r6a.32xlarge	128	1024	190,967	50	40000	160000
r6a.24xlarge	96	768	143,225	37.5	30000	120,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
r6a.48xlarge	192	1,536	286,450	50	40000	240,000
r6i.large	2	16	3,063	最多 12.5	最高 10,000	40000
r6i.xlarge	4	32	6,127	最多 12.5	最高 10,000	40000
r6i.2xlarge	8	64	12,253	最多 12.5	最高 10,000	40000
r6i.4xlarge	16	128	24,506	最多 12.5	最高 10,000	40000
r6i.8xlarge	32	256	49,013	12.5	10000	40000
r6i.12xlarge	48	384	73,519	18.75	15000	60000
r6i.16xlarge	64	512	98,025	25	20000	80,000
r6i.24xlarge	96	768	147,038	37.5	30000	120,000
r6i.32xlarge	128	1024	196,050	50	40000	160000
r6i.metal	128	1024	203,600	50	40000	160000
r6id.large	2	16	3,063	最多 12.5	最高 10,000	40000
r6id.xlarge	4	32	6,127	最多 12.5	最高 10,000	40000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
r6gd.2xlarge	8	64	12,253	最多 12.5	最高 10,000	40000
r6id.4xlarge	16	128	24,506	最多 12.5	最高 10,000	40000
r6id.8xlarge	32	256	49,013	12.5	10000	40000
r6id.12xlarge	48	384	73,519	18.75	15000	60000
r6id.16xlarge	64	512	98,025	25	20000	80,000
r6id.24xlarge	96	768	147,038	37.5	30000	120,000
r6id.32xlarge	128	1024	196,050	50	40000	160000
r6idn.large	2	16	3,063	最多 25	最多 25,000	100000
r6idn.xlarge	4	32	6,127	最多 30	最多 25,000	100000
r6idn.2xlarge	8	64	12,253	最多 40	最多 25,000	100000
r6idn.4xlarge	16	128	24,506	最多 50	最多 25,000	100000
r6idn.8xlarge	32	256	49,013	50	25000	100000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
r6idn.12xlarge	48	384	73,519	75	37,500	15万
r6idn.16xlarge	64	512	98,025	100	50000	200,000
r6idn.24xlarge	96	768	147,038	150	75000	300,000
r6idn.32xlarge	128	1024	196,050	200	100000	400,000
r6id.metal	128	1024	203,600	50	40000	160000
r6in.large	2	16	3,063	最多 25	最多 25,000	100000
r6in.xlarge	4	32	6,127	最多 25	最多 25,000	100000
r6in.2xlarge	8	64	12,253	最多 25	最多 25,000	100000
r6in.4xlarge	16	128	24,506	最多 25	最多 25,000	100000
r6in.8xlarge	32	256	49,013	12.5	25000	100000
r6in.12xlarge	48	384	73,519	18.75	37,500	15万
r6in.16xlarge	64	512	98,025	25	50000	200,000
r6in.24xlarge	96	768	147,038	37.5	75000	300,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
r6in.32xlarge	128	1024	196,050	200	100000	400,000
r7a.medium	1	8	2,255	最多 12.5	最高 10,000	最多 40,000
r7a.large	2	16	4,510	最多 12.5	最高 10,000	最多 40,000
r7a.xlarge	4	32	9,020	最多 12.5	最高 10,000	最多 40,000
r7a.2xlarge	8	64	18,040	最多 12.5	最高 10,000	最多 40,000
r7a.4xlarge	16	128	36,080	最多 12.5	最高 10,000	最多 40,000
r7a.8xlarge	32	256	72,160	12.5	10000	40000
r7a.12xlarge	48	384	108,240	18.75	15000	60000
r7a.16xlarge	64	512	144,320	25	20000	80,000
r7a.24xlarge	96	768	216,480	37.5	30000	120,000
r7a.32xlarge	128	1024	288,640	50	40000	160000
r7a.48xlarge	192	1536	432,980	50	40000	240,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
r7i.large	2	16	4,155	最多 12.5	最高 10,000	40000
r7i.xlarge	4	32	8,310	最多 12.5	最高 10,000	40000
r7i.2xlarge	8	64	16,620	最多 12.5	最高 10,000	40000
r7i.4xlarge	16	128	33,240	最多 12.5	最高 10,000	40000
r7i.8xlarge	32	256	66,480	12.5	10000	40000
r7i.12xlarge	48	384	99,720	18.75	15000	60000
r7i.16xlarge	64	512	105,500	25	20000	80,000
r7i.24xlarge	96	768	158,250	37.5	30000	120,000
r7i.48xlarge*	192	1536	296,200	50	40000	240,000
u-3tb1.56xlarge	224	3,072	237,750	50	19000	80,000
u-6tb1.56xlarge	224	6,144	380770	100	38,000	160000
u-6tb1.112xlarge	448	6,144	475,500	100	38,000	160000
u-6tb1.metal	448	6,144	480,600	100	38,000	160000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
u-9tb1.112xlarge	448	9,216	475,500	100	38,000	160000
u-9tb1.metal	448	9,216	480,600	100	38,000	160000
u-12tb1.112xlarge	448	12,288	475,500	100	38,000	160000
u-12tb1.metal	448	12,288	480,600	100	38,000	160000
u-18tb1.112xlarge	448	18432	520,330	100	38,000	160000
u-18tb1.metal	448	18432	534,130	100	38,000	160000
u-24tb1.112xlarge	448	24576	508,720	100	38,000	160000
u-24tb1.metal	448	24576	517,480	100	38,000	160000
u7i-6tb.112xlarge	448	6,144	642,850	100	60000	420,000
u7i-8tb.112xlarge	448	8192	645,230	100	60000	420,000
u7i-12tb.224xlarge	896	12,288	1,254,030	100	60000	420,000
u7in-16tb.224xlarge	896	16,384	1,281,620	200	100000	420,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
u7in-24tb.224xlarge	896	24576	1,225,250	200	100000	420,000
u7inh-32tb.480xlarge	1,920	32,768	不适用	200	160000	840,000
x1.16xlarge	64	976	65,750	10	7,000	40000
x1.32xlarge	128	1,952	131,500	25	14,000	80,000
x1e.xlarge	4	122	4,109	最多 10	500	3,700
x1e.2xlarge	8	244	8,219	最多 10	1000	7,400
x1e.4xlarge	16	488	16,437	最多 10	1,750	10000
x1e.8xlarge	32	976	32,875	最多 10	3,500	20000
x1e.16xlarge	64	1,952	65,750	10	7,000	40000
x1e.32xlarge	128	3,904	131,500	25	14,000	80,000
x2idn.16xlarge	64	1024	98,025	50	40000	15万
x2idn.24xlarge	96	1,536	147,038	75	60000	200,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
x2idn.32xlarge	128	2,048	196,050	100	80,000	300,000
x2iedn.xlarge	4	128	5,906	最多 25	最多 20,000	12,500
x2iedn.2xlarge	8	256	11,813	最多 25	最多 20,000	25000
x2iedn.4xlarge	16	512	23,625	最多 25	最多 20,000	50000
x2iedn.8xlarge	32	1024	47,250	25	20000	75000
x2iedn.16xlarge	64	2,048	94,500	50	40000	15万
x2iedn.24xlarge	96	3,072	141,750	75	60000	200,000
x2iedn.32xlarge	128	4,096	189,000	100	80,000	300,000
x2iezn.2xlarge	8	256	14,170	最多 25	3,170	13,333
x2iezn.4xlarge	16	512	28,340	最多 25	4,175	20000
x2iezn.6xlarge	24	768	42,510	50	9500	40000
x2iezn.8xlarge	32	1024	56,680	75	12000	55,000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
x2iezn.12xlarge	48	1,536	85,020	100	19000	80,000

Storage Optimized

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
i3en.xlarge	4	32	5,782	最多 25	最多 4,750	20000
i3en.2xlarge	8	64	11,564	最多 25	最多 4,750	20000
i3en.3xlarge	12	96	17,346	最多 25	最多 4,750	20000
i3en.6xlarge	24	192	34,693	25	4750	20000
i3en.12xlarge	48	384	69,385	50	9500	40000
i3en.24xlarge	96	768	138,770	100	19000	80,000
i3en.metal	96	768	143,230	100	19000	80,000
i4i.large	2	16	3,063	最多 10	最高 10,000	40000
i4i.xlarge	4	32	6,127	最多 10	最高 10,000	40000
i4i.2xlarge	8	64	12,253	最多 12.5	最高 10,000	40000

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	最大 IOPS
i4i.4xlarge	16	128	24,506	最多 25	最高 10,000	40000
i4i.8xlarge	32	256	49,013	18.75	10000	40000
i4i.12xlarge	48	384	73,519	28.125	15000	60000
i4i.16xlarge	64	512	98,025	37.5	20000	80,000
i4i.24xlarge	96	768	147,038	56.25	30000	120,000
i4i.32xlarge	128	1024	196,050	75	40000	160000
i4i.metal	128	1024	203,600	75	40000	160000

*Windows 2016 及更高版本、SLES 15 及更高版本以及 RHEL 8.6 及更高版本支持 m7i.48xlarge 和 r7i.48xlarge。 SP3

上一代 SAP 实例 NetWeaver

Example

General Purpose

实例类型	vCPU	内存 (GiB)	SAPS
cc2.8xlarge	32	60.5	90,330
cr1.8xlarge	32	244	30,430
m2.2xlarge	4	32.2	3,700

实例类型	vCPU	内存 (GiB)	SAPS
m2.4xlarge	8	68.4	7,400
m4.large	2	8	2,366
m4.xlarge	4	16	4,732
m4.2xlarge	8	32	9,464
m4.4xlarge	16	64	18,928
m4.10xlarge	40	160	47,320
m4.16xlarge	64	256	75,770

Compute Optimized

实例类型	vCPU	内存 (GiB)	SAPS
c3.large	2	3.75	1,995
c3.xlarge	4	7	3,990
c3.2xlarge	8	15	7,980
c3.4xlarge	16	30	15,915
c3.8xlarge	32	60	31,830
c4.large	2	3.75	2,379
c4.xlarge	4	7.5	4,758
c4.2xlarge	8	15	9,515
c4.4xlarge	16	30	19,030
c4.8xlarge	36	60	37,950

Memory Optimized

实例类型	vCPU	内存 (GiB)	SAPS
r3.large	2	15	1,995
r3.xlarge	4	30.5	3,990
r3.2xlarge	8	61	7,980
r3.4xlarge	16	122	15,960
r3.8xlarge	32	244	31,920
r4.large	2	15.25	2,387
r4.xlarge	4	30.5	4,775
r4.2xlarge	8	61	9,550
r4.4xlarge	16	122	19,100
r4.8xlarge	32	244	38,200
r4.16xlarge	64	488	76,400

SAP HANA 认证和非认证实例

AWS 已与 SAP 密切合作，针对 AWS 解决方案对 SAP 的 Amazon EC2 实例类型进行了测试和认证。

完全支持适用于 SAP HANA 的上一代 Amazon EC2 实例，并且这些实例类型保留了相同的特性和功能。我们建议使用最新一代的 Amazon EC2 实例进行新的 SAP HANA 实施或迁移。

适用于 SAP HANA 的所有当前和上一代 Amazon EC2 实例类型都可用于运行非生产工作负载。欲了解更多信息，请参阅 SAP Note 2271345。

内容

- 最新一代认证实例
  - SAP HANA OLTP 和 OLAP 向上扩展
  - SAP HANA OLTP 和 OLAP 横向扩展

- 上一代认证实例
  - SAP HANA OLTP 和 OLAP 向上扩展
  - SAP HANA OLTP 和 OLAP 横向扩展
- 非认证实例

最新一代认证实例

SAP HANA OLTP 和 OLAP 向上扩展

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	SAP HANA OLAP prod	SAP HANA OLAP 规模调整	FSx 适用于 ONTAP
r5.8xlar e	32	256	46,257	10	6800	✓	Standar	✓	Standar	✗
r5.12xla ge	48	384	69,385	10	9500	✓	Standar	✓	Standar	✗
r5.16xla ge	64	512	92,513	20	13600	✓	Standar	✓	Standar	✗
r5.24xla ge	96	768	138,77C	25	19000	✓	Standar	✓	Standar	✗
r5.meta	96	768	143,23C	25	19000	✓	Standar	✓	Standar	✗
r5b.8xla ge	32	256	46,257	25	20000	✓	Standar	✓	Standar	✗
r5b.12xl rge	48	384	69,385	50	30000	✓	Standar	✓	Standar	✗
r5b.16xl rge	64	512	92,513	75	40000	✓	Standar	✓	Standar	✗

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	SAP HANA OLAP prod	SAP HANA OLAP 规模调整	FSx 适用于 ONTAP
r5b.24xl rge	96	768	138,77(	100	60000	✓	Standar	✓	Standar	✗
r5b.met	96	768	143,23(	100	60000	✓	Standar	✓	Standar	✗
r6i.8xlar ge	32	256	49,013	12.5	10000	✓	Standar	✗	不适用	✗
r6i.12xla rge	48	384	73,519	18.75	15000	✓	Standar	✓	Standar	✓
r6i.16xla rge	64	512	98,025	25	20000	✓	Standar	✓	Standar	✓
r6i.24xla rge	96	768	147,038	37.5	30000	✓	Standar	✓	Standar	✓
r6i.32xla rge	128	1024	196,05(	50	40000	✓	Standar	✓	Standar	✓
r7i.8xlar ge	32	256	66,480	12.5	10000	✓	Standar	✓	Standar	✓
r7i.12xla rge	48	384	99,720	18.75	15000	✓	Standar	✓	Standar	✓
r7i.16xla rge	64	512	105,50(	25	20000	✓	Standar	✓	Standar	✓
r7i.24xla rge	96	768	158,25(	37.5	30000	✓	Standar	✓	Standar	✓

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	SAP HANA OLAP prod	SAP HANA OLAP 规模调整	FSx 适用于 ONTAP
r7i.48xla rge	192	1536	296,200	50	40000	✓	Standar	✓	Standar	✓
u-3tb1.5 xlarge	224	3,072	237,750	50	19000	✓	Standar	✓	工作负载	✓
u-6tb1.5 xlarge	224	6,144	380770	100	38,000	✓	Standar	✓	工作负载	✓
u-6tb1.1 2xlarge	448	6,144	475,500	100	38,000	✓	Standar	✓	Standar	✓
u-6tb1.r tal	448	6,144	480,600	100	38,000	✓	Standar	✓	Standar	✗
u-9tb1.1 2xlarge	448	9,216	475,500	100	38,000	✓	Standar	✓	工作负载	✓
u-9tb1.r tal	448	9,216	480,600	100	38,000	✓	Standar	✓	工作负载	✗
u-12tb1 12xlarge	448	12,288	475,500	100	38,000	✓	Standar	✓	工作负载	✓
u-12tb1 etal	448	12,288	480,600	100	38,000	✓	Standar	✓	工作负载	✗
u-18tb1 12xlarge	448	18432	520,330	100	38,000	✓	工作负载	✓	工作负载	✓
u-18tb1 etal	448	18432	534,130	100	38,000	✓	工作负载	✓	工作负载	✗

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	SAP HANA OLAP prod	SAP HANA OLAP 规模调整	FSx 适用于 ONTAP
u-24tb1 12xlarge	448	24576	508,720	100	38,000	✓	工作负载	✗	不适用	✓
u-24tb1 etal	448	24576	517,480	100	38,000	✓	工作负载	✗	不适用	✗
u7i-6tb. 12xlarge	448	6,144	642,850	100	60000	✓	Standar	✓	Standar	✓
u7i-8tb. 12xlarge	448	8192	645,230	100	60000	✓	Standar	✓	Standar	✓
u7i-12tb 224xlarg	896	12,288	1,254,0	100	60000	✓	Standar	✓	Standar	✓
u7in-16t .224xlar e	896	16,384	1,281,6	200	100000	✓	Standar	✓	Standar	✓
u7in-24t .224xlar e	896	24576	1,225,1	200	100000	✓	工作负载	✓	工作负载	✓
u7inh-3 b.480xla ge	1,920	32,768	不适用	200	160000	✓	Standar	✓	Standar	✓
x1.16xla ge	64	976	65,750	10	7,000	✓	Standar	✓	Standar	✗
x1.32xla ge	128	1,952	131,500	25	14,000	✓	Standar	✓	Standar	✗

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	SAP HANA OLAP prod	SAP HANA OLAP 规模调整	FSx 适用于 ONTAP
x1e.32x rge	128	3,904	131,50(	25	14,000	✓	Standar	✓	工作负载	✗
x2idn.1(large	64	1024	98,025	50	40000	✓	Standar	✓	工作负载	✓
x2idn.2(large	96	1,536	147,038	75	60000	✓	Standar	✓	工作负载	✓
x2idn.3(large	128	2,048	196,05(	100	80,000	✓	Standar	✓	Standar	✓
x2iedn.(xlarge	96	3,072	141,75(	75	60000	✓	Standar	✓	工作负载	✓
x2iedn.(xlarge	128	4,096	189,00(	100	80,000	✓	Standar	✓	工作负载	✓

SAP HANA OLTP 和 OLAP 横向扩展

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	OLTP 最大节点数	SAP HANA OLAP prod	SAP HANA OLAP 规模调整	OLAP 最大节点数	FSx 适用于 ONTAP
r5.24x ge	96	768	138,77	25	19000	✗	不适用	不适用	✓	Standa	16	✗
r6i.24x rge	96	768	147,03	37.5	30000	✗	不适用	不适用	✓	Standa	16	✓

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	OLTP 最大节点数	SAP HANA OLAP prod	SAP HANA OLAP 规模调整	OLAP 最大节点数	FSx 适用于 ONTAP
r6i.32x rge	128	1024	196,05	50	40000	✗	不适用	不适用	✓	Standa	16	✓
u-6tb1 xlarge	224	6,144	38077	100	38,000	✓	Standa	4	✓	工作负载	16	✓
u-6tb1 2xlarg	448	6,144	475,50	100	38,000	✓	Standa	4	✓	Standa	16	✓
u-6tb1 tal	448	6,144	480,60	100	38,000	✓	Standa	4	✓	Standa	16	✗
u-9tb1 2xlarg	448	9,216	475,50	100	38,000	✓	Standa	4	✓	工作负载	16	✓
u-12tb 12xlar	448	12,288	475,50	100	38,000	✓	Standa	4	✓	工作负载	16	✓
u-12tb etal	448	12,288	480,60	100	38,000	✓	Standa	4	✗	不适用	不适用	✗
u7i-6tb 12xlar	448	6,144	642,85	100	60000	✗	不适用	不适用	✓	Standa	16	✗
u7i-8tb 12xlar	448	8192	645,23	100	60000	✗	不适用	不适用	✓	Standa	16	✗
u7in-1 .224xla e	896	12,288	1,254,	100	60000	✓	Standa	4	✓	Standa	8	✓

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	OLTP 最大节点数	SAP HANA OLAP prod	SAP HANA OLAP 规模调整	OLAP 最大节点数	FSx 适用于 ONTAP
u7in-1 .224xl e	896	16,384	1,281,	200	10000	✓	Standa	4	✓	Standa	8	✓
u7in-2 .224xl e	896	24576	1,225,	200	10000	✓	工作负载	4	✓	工作负载	8	✓
u7inh- b.480x ge	1,920	32,768	不适用	200	16000	✓	Standa	4	✓	工作负载	8	✗
x1.16x ge	64	976	65,750	10	7,000	✗	不适用	不适用	✓	Standa	7	✗
x1.32x ge	128	1,952	131,50	25	14,000	✗	不适用	不适用	✓	Standa	25	✗
x1e.32 rge	128	3,904	131,50	25	14,000	✗	不适用	不适用	✓	工作负载	25	✗
x2idn. large	64	1024	98,025	50	40000	✗	不适用	不适用	✓	Standa	16	✓
x2idn. large	96	1,536	147,03	75	60000	✗	不适用	不适用	✓	工作负载	16	✓
x2idn. large	128	2,048	196,05	100	80,000	✗	不适用	不适用	✓	工作负载	16	✓
x2iedn xlarge	96	3,072	141,75	75	60000	✗	不适用	不适用	✓	工作负载	16	✓

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	OLTP 最大节点数	SAP HANA OLAP prod	SAP HANA OLAP 规模调整	OLAP 最大节点数	FSx 适用于 ONTAP
x2iedn xlarge	128	4,096	189,0(	100	80,00(	✗	不适用	不适用	✓	工作负载	16	✓

上一代认证实例

SAP HANA OLTP 和 OLAP 向上扩展

实例类型	vCPU	内存 (GiB)	SAPS	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	SAP HANA OLAP prod	SAP HANA OLAP 规模调整
r3.2xlarge	8	61	7,980	✗	Standard	✗	Standard
r3.4xlarge	16	122	15,960	✗	Standard	✗	Standard
r3.8xlarge	32	244	31,920	✓	Standard	✓	Standard
r4.8xlarge	32	244	38,200	10	7,000	✓	Standard
r4.16xlarge	64	488	76,400	25	14,000	✓	Standard

SAP HANA OLTP 和 OLAP 横向扩展

实例类型	vCPU	内存 (GiB)	SAPS	SAP HANA OLTP 产品	SAP HANA OLTP 规模调整	SAP HANA OLAP prod	SAP HANA OLAP 规模调整
r3.8xlarge	32	244	31,920	✗	不适用	✓	Standard

非认证实例

下表中的 Amazon EC2 实例未经过生产使用认证。您可以使用它们来运行非生产工作负载。有关更多信息，请参阅 SAP Note 2271345 — 成本优化的 SAP HANA 硬件，用于非生产用途（需要访问 SAP 门户）。

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	FSx 适用于 ONTAP
r4.2xlarge	8	61	9,550	最多 10	1,700	✗
r4.4xlarge	16	122	19,100	最多 10	3,500	✗
r5.2xlarge	8	64	11,564	最多 10	最多 4,750	✗
r5.4xlarge	16	128	23,128	最多 10	4750	✗
r5b.2xlarge	8	64	11,564	最多 10	最高 10,000	✗
r5b.4xlarge	16	128	23,128	最多 10	10000	✗
r6i.2xlarge	8	64	12,253	最多 12.5	最高 10,000	✗
r6i.4xlarge	16	128	24,506	最多 12.5	最高 10,000	✗

实例类型	vCPU	内存 (GiB)	SAPS	网络 (Gbps)	存储空间 (Mbps)	FSx 适用于 ONTAP
x1e.xlarge	4	122	4,109	最多 10	500	✗
x1e.2xlarge	8	244	8,219	最多 10	1000	✗
x1e.4xlarge	16	488	16,437	最多 10	1,750	✗
x2iedn.xlarge	4	128	5,906	最多 25	最多 20,000	✗
x2iedn.2xlarge	8	256	11,813	最多 25	最多 20,000	✗
x2iedn.4xlarge	16	512	23,625	最多 25	最多 20,000	✗
x2iedn.8xlarge	32	1024	47,250	25	20000	✗
x2iedn.16xlarge	64	2,048	94,500	50	40000	✗

SAP Business One 认证实例，SAP HANA 版本

AWS 已与 SAP 密切合作，针对 AWS 解决方案对 SAP 的 Amazon EC2 实例类型进行了测试和认证。

Example

Current Generation

实例类型	vCPU	内存 (GiB)	SAPS	最大并发用户数
r5.2xlarge	8	64	11,564	25
r5.4xlarge	16	128	23,128	50

实例类型	vCPU	内存 (GiB)	SAPS	最大并发用户数
r5.12xlarge	48	384	69,385	150
r5.24xlarge	96	768	138,770	250
r6i.2xlarge	8	64	12,253	25
r6i.4xlarge	16	128	24,506	50
r6i.8xlarge	32	256	49,013	100
r7i.2xlarge	8	64	16,620	25
r7i.4xlarge	16	128	33,240	50
r7i.8xlarge	32	256	66,480	100
r7i.12xlarge	48	384	99,720	150
x1.16xlarge	64	976	65,750	200

Previous Generation

实例类型	vCPU	内存 (GiB)	SAPS	最大并发用户数
c3.8xlarge	32	60	31,830	25
m4.10xlarge	40	160	47,320	50
m4.16xlarge	64	256	75,770	100
r3.8xlarge	32	244	31,920	50

在 SAP 上记录实例类型的历史记录 AWS

更改	日期
添加了对 u7inh-32tb.480xlarge 的横向扩展 (OLAP) 支持	2025 年 6 月
在 SAP NetWeaver 和 SAP HANA 中添加了 U7i	2024 年 5 月
将 R7i 添加到 SAP Business One	2024 年 1 月
在 SAP 中添加了 m7i 和 R7i NetWeaver	2023 年 10 月
将 R7a 添加到 SAP NetWeaver	2023 年 9 月
将 m7a 添加到 SAP NetWeaver	2023 年 8 月
将 R6i 添加到 SAP Business One	2023 年 2 月
在 SAP 中添加了 r6id、r6in、r6iDn、m6iD、m6in 和 m6iDN NetWeaver	2023 年 1 月
添加了 ONTAP FSx 对 u-18tb1.112 和 u-24tb1.112 的支持	2023 年 1 月
在 SAP HANA 和 SAP 中添加了 u-24tb1 和 u-18tb1 NetWeaver	2022 年 10 月
将 i4i 添加到 SAP NetWeaver	2022 年 9 月
添加了 FSx ONTAP 对 SAP HANA 的支持	2022 年 9 月
将 R6a 添加到 SAP NetWeaver	2022 年 7 月
在 SAP 中添加了 c6i、c6id 和 c6a NetWeaver	2022 年 7 月
在 SAP HANA OLAP 横向扩展中添加了 x2iDN 和 R6i	2022 年 6 月

更改	日期
初次发布	2022 年 4 月

AWS 适用于 SAP 的数据提供商

AWS 适用于 SAP 的数据提供程序是一种从 AWS 服务中收集与性能相关的数据的工具。它使这些数据可用于 SAP 应用程序，以帮助监控和改善业务交易的性能。SAP 要求客户按照 SAP 注释 1656250 中所述安装代理（需要登录凭据）。

适用于 SAP AWS 的数据提供商使用与 SAP 基础架构运行最相关的操作系统、网络和存储数据。其数据源包括亚马逊弹性计算云 (Amazon EC2) 和亚马逊 CloudWatch。本指南提供了 Linux 和 Windows 上适用于 SAP AWS 的数据提供程序的安装、配置和故障排除信息。

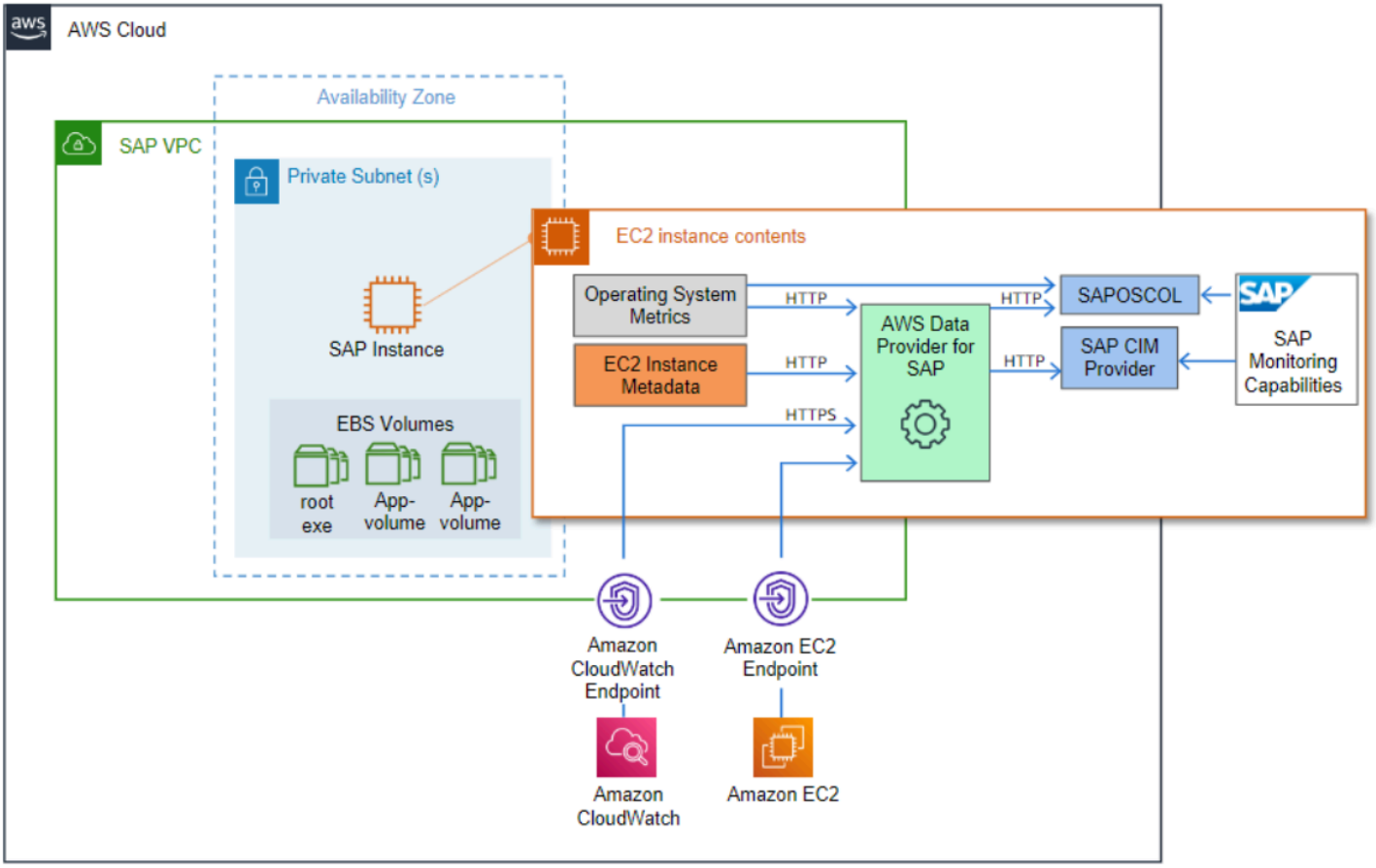
简介

许多不同规模的组织都选择在亚马逊 Web Services 云中托管关键 SAP 系统。使用 AWS，您可以快速配置 SAP 环境。此外， AWS 云的弹性特性使您能够根据需要向上和向下扩展计算资源。因此，您的企业可以将更多的资源（包括人员和资金）投入到创新上。

许多 SAP 系统处理日常业务事务，对业务功能至关重要。作为 SAP 客户，您需要能够跟踪这些事务的性能并对其进行故障排除。适用于 SAP AWS 的数据提供程序是一种在亚马逊弹性计算云 (Amazon EC2) 实例上收集关键性能数据的工具，SAP 应用程序可以使用这些数据来监控 SAP 构建的交易。数据是从您的 AWS 云端操作环境中的各种来源收集的，包括亚马逊 EC2 和亚马逊 CloudWatch。这些数据包括与您的 SAP 基础架构相关的操作系统、网络和存储的信息。来自 SAP AWS 数据提供程序的数据由 SAP 操作系统收集器 (SAPOSCOL) 和 SAP CIM 提供程序读取。

该图简要说明了 SAP AWS 的数据提供者、其数据源和输出。

适用于 SAP AWS 的数据提供程序的数据源



本指南的目的是帮助您：

- 了解安装和运行 SAP AWS 数据提供程序所需的技术要求和组件。
- 安装适用于 SAP AWS 的数据提供程序。
- 了解 SAP AWS 数据提供程序的更新流程。
- 对安装问题进行故障排除。

定价

DataProvider 代理是免费提供的。但是，由于 SAP 要求按特定的时间间隔交付监控数据，因此运行代理会产生间接成本。这会 DataProvider 导致频繁GetMetric调用亚马逊 CloudWatch 和亚马逊 EC2 API 来检索指标数据。这些调用的预期费用约为每个系统每月 20.00 美元到 40.00 美元，并将根据连接到 Amazon 实例的磁盘数量而有所不同。 EC2

示例：在美国东部（弗吉尼亚北部）地区使用 DataProvider 代理的每月费用。

已修复：

- 运行 2 个必需的 Amazon VPC 终端节点（监控、亚马逊 EC2）的费用约为 14.00 美元+ 0.01 美元，每处理一个 GB 数据。

> **Note**
>
> 这些端点只需创建一次，即可由整个环境共享。如果您已经在使用这些终端节点，则无需再次创建它们。

每个系统：

- 预计每个实例每天大约有 70,000 个 API 调用（附有 6 个磁盘）。按每千次通话 0.0 1美元计算，约为每月 21.00美元。API 调用次数根据连接的磁盘数量增加或减少。

技术要求

在创建 SAP 实例之前，请确保满足以下技术要求。

主题

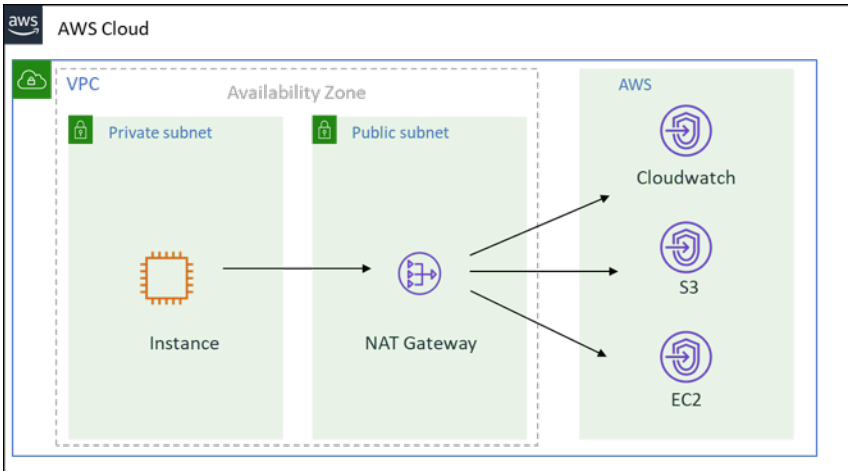
- 亚马逊 VPC 网络拓扑
- Amazon VPC 端点
- IAM 角色

亚马逊 VPC 网络拓扑

您需要在亚马逊虚拟私有云（亚马逊 VPC）中部署从 SAP AWS 数据提供商那里接收信息的 SAP 系统。您可以使用以下网络拓扑之一来启用到基于 Internet 的终端节点的路由：

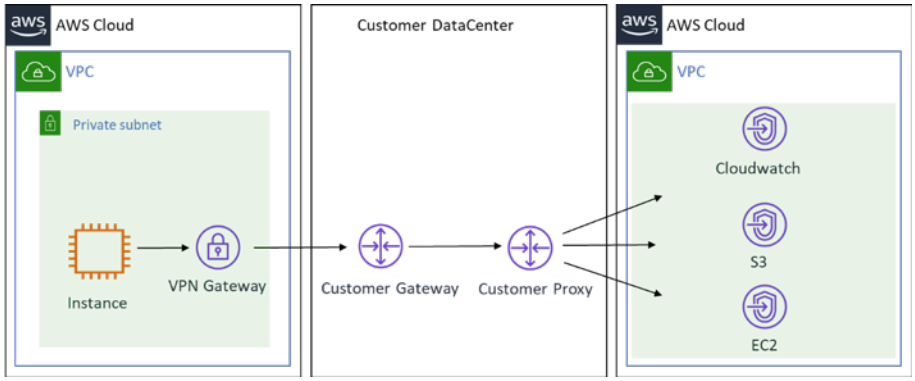
- 第一个拓扑结构配置通过 Amazon VPC 内的 NAT 网关直接进入 AWS 云的路由和流量。有关互联网网关的更多信息，请参阅AWS 文档。

通过互联网网关连接到 AWS 云端



- 第二种拓扑将流量从 Amazon VPC 路由到贵组织的本地数据中心，然后返回 AWS 云端。有关此拓扑的更多信息，请参阅什么是 AWS Site-to-Site VPN？

通过本地数据中心连接至亚马逊 Web Services 云



Amazon VPC 端点

为 DataProvider 使用的以下服务创建终端节点：

- 监控
- Amazon EC2

要在 AWS 控制台中创建数据端点，请对两个端点分别使用以下步骤：

1. 登录 Amazon VPC 控制台，导航到终端节点，然后选择创建终端节点。
2. 在下一个屏幕上，搜索服务名称，然后选择相应的 VPC 和路由表，然后选择创建终端节点。
3. 创建完所有三个终端节点后，您应该会在终端节点列表中看到它们，如下所示：

IAM 角色

您需要向 SAP AWS 的数据提供商授予对亚马逊 CloudWatch、亚马逊简单存储服务 (Amazon S3) Semple S3 Service 和 EC2 亚马逊服务的只读访问权限，这样您才能使用它们。 APIs为此，您可以为 EC2 亚马逊实例创建 AWS 身份和访问管理 (IAM) 角色并附加权限策略。

使用以下过程创建 IAM 角色并向您的 Amazon EC2 实例授予权限：

1. 登录AWS 管理控制台并打开 IAM 控制台。
2. 在导航窗格中，选择角色，然后选择创建角色。
3. 选择 AWS 服务角色类型，然后选择EC2。
4. 选择EC2作为用例，然后选择 “下一权限”。
5. 选择创建策略，然后选择 JSON。
6. 将以下策略复制并粘贴到输入字段中，替换所有现有文本，然后选择 Review P olic y。

> **Note**
>
> 如果您的 Amazon EC2 实例在北京和宁夏运行，则必须使用正确的区域更新资源行。

请参阅以下基于您所在 AWS 地区的政策示例。

AWS 地区（ AWS GovCloud （美国东部）、 AWS GovCloud （美国西部）、北京和宁夏除外）

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "EC2:DescribeInstances",
                "cloudwatch:GetMetricStatistics",
                "EC2:DescribeVolumes"
            ],
            "Resource": "*"
        },
        {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
```

```
          "Action": "s3:GetObject",
          "Resource": [
           "arn:aws:s3:::aws-sap-dataprovider-<us-east-1>/config.properties"
             ]
        }
    ]
}
```

北京和宁夏

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "EC2:DescribeInstances",
                "cloudwatch:GetMetricStatistics",
                "EC2:DescribeVolumes"
            ],
            "Resource": "*"
        },
        {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
         "Action": "s3:GetObject",
         "Resource": [
          "arn:aws-cn:s3:::aws-sap-dataprovider-<cn-north-1>/config.properties"
            ]
        }
    ]
}
```

AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
```

```
            "Action": [
                "EC2:DescribeInstances",
                "cloudwatch:GetMetricStatistics",
                "EC2:DescribeVolumes"
            ],
            "Resource": "*"
        },
        {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
         "Action": "s3:GetObject",
         "Resource": [
          "arn:aws-us-gov:s3:::aws-sap-dataprovider-<us-gov-west-1>/
config.properties"
            ]
        }
    ]
}
```

7. 提供角色的名称和描述，然后选择创建策略。
8. 选择 Create Policy (创建策略)。IAM 控制台使用类似于以下内容的消息确认新策略。
9. 导航到 “创建角色” 页面，刷新屏幕，搜索新创建的角色，然后选择策略。
10选择 “下一步：标签”。
11如果需要，可以添加任何标签，否则请选择 “下一步：查看”。
12为角色提供一个名称，然后选择创建角色。

DataProvider 4.3

如果您不熟悉适用于 SAP AWS 的数据提供程序，请参阅安装 DataProvider 4.3。

如果您需要更新或卸载 DataProvider 4.3，请参阅更新到 DataProvider 4.3。

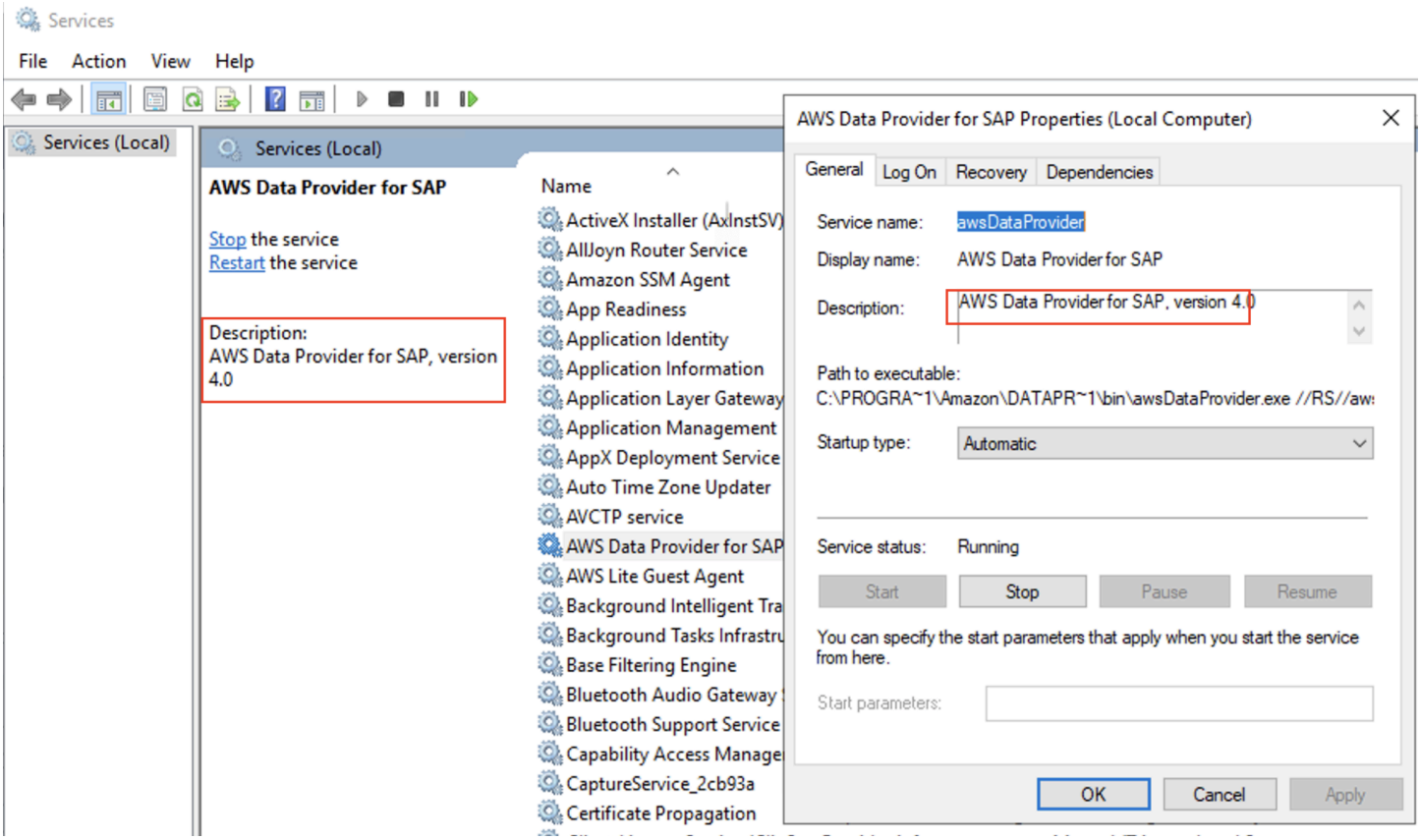
如果您的系统上有旧版本，请参阅卸载旧版本。

> **Important**
>
> 的所有先前版本（v1、v2、v3）均 DataProvider 已弃用，将不再接收更新。要进行新 DataProvider 安装，必须使用 SSM 发行版安装 DataProvider 4.3。

运行以下命令以检查系统 DataProvider 上的当前版本。

```
rpm -qa | grep aws-sap
```

要 DataProvider 在 Windows 上查看的当前版本，请转到 “服务（本地）”，选择 “适用于 SAP AWS 的数据提供器”，然后打开 “属性”。您可以在 “描述” 字段中看到当前版本。



正在安装 DataProvider 4.3

适用于 SAP AWS 的数据提供程序作为一项服务运行，该服务在启动时自动启动，并收集、聚合指标并将其公开给 SAP 主机代理。指标来自各种提供商，这些提供商从平台的相关领域提取指标。SAP AWS 的数据提供程序旨在继续运行，无论其提供商是否具有连接或访问他们所请求的 AWS 服务指标的权限。无法达到他们正在收集的指标的提供商会返回空值。

例如，如果您的亚马逊 EC2 实例没有与之关联的 IAM 角色来授予对 Amazon CloudWatch GetMetricStatisticsAPI 的显式访问权限，则 CloudWatch 提供商将无法对亚马逊 EC2 实例执行GetMetricStatistics操作并返回空值。

需要在每个 SAP 生产系统上安装该提供商，才有资格获得 SAP 支持。您一次只能在系统上安装一个提供程序实例。

适用于 SAP AWS 的数据提供程序旨在自动更新自身，以便为你提供最新的指标。当 SAP AWS 的数据提供程序启动时，内置更新服务会从 AWS 托管 Amazon S3 存储桶中检索其组件和指标定义的最新版本。如果 SAP AWS 的数据提供程序无法访问更新服务，它将继续按原样运行。

使用 SSM 分销商安装 — DataProvider 4.3（推荐）

DataProvider 4.3 版本允许您通过 SSM 发行商安装软件包。 AWS 建议使用这种方法进行安装，你可以 DataProvider 使用 Linux 或 Windows 平台进行安装。

DataProvider 使用 SSM 分发服务器安装的先决条件

SSM-Agent

必须先在实例上`ssm-agent`安装了，然后才能使用 SSM 分发服务器安装 DataProvider 代理。使用以下 AWS Systems Manager 用户指南`ssm-agent`在您的实例上安装。

- RHEL：在红帽企业 Linux 实例上手动安装 SSM 代理
- SUSE：在 SUSE Linux 企业服务器实例上手动安装 SSM 代理
- 甲骨文：在 Oracle Linux 实例上手动安装 SSM 代理
- Windows：在适用于 Windows 服务器的亚马逊 EC2 实例上手动安装 SSM 代理

Java 运行时

DataProvider 是一个 Java 应用程序，需要在实例上安装 Java 运行时才能运行。

如果您的实例尚未安装 Java 运行时，则可以使用 Amazon Corretto 提供的 OpenJDK 来安装 Java 运行时。

DataProvider 4.3 支持以下 Java 运行时版本：

- 亚马逊 Corretto 8 或 OpenJDK 8
- 亚马逊 Corretto 11 或 OpenJDK 11
- 亚马逊 Corretto 17 或 OpenJDK 17

有关如何在您的亚马逊 EC2 实例上下载和安装 JDK 的更多信息，请参阅 Amazon C orretto 文档。

在终端中，运行以下命令以验证安装。

```
java -version
```

例如，Coretto-8.252.09.1 的预期输出应如下所示：

```
openjdk version "1.8.0_252"OpenJDK Runtime Environment Corretto-8.252.09.1 (build
 1.8.0_252-b09)OpenJDK 64-Bit Server VM Corretto-8.252.09.1 (build 25.252-b09, mixed
 mode)
```

GPG 密钥

如果您是 SUSE 用户，则必须下载 DataProvider GPG 密钥并在安装前将其导入。

- GPG 密钥网址：G PG 密钥
- 登录您的 SUSE 实例并运行以下命令来导入密钥：

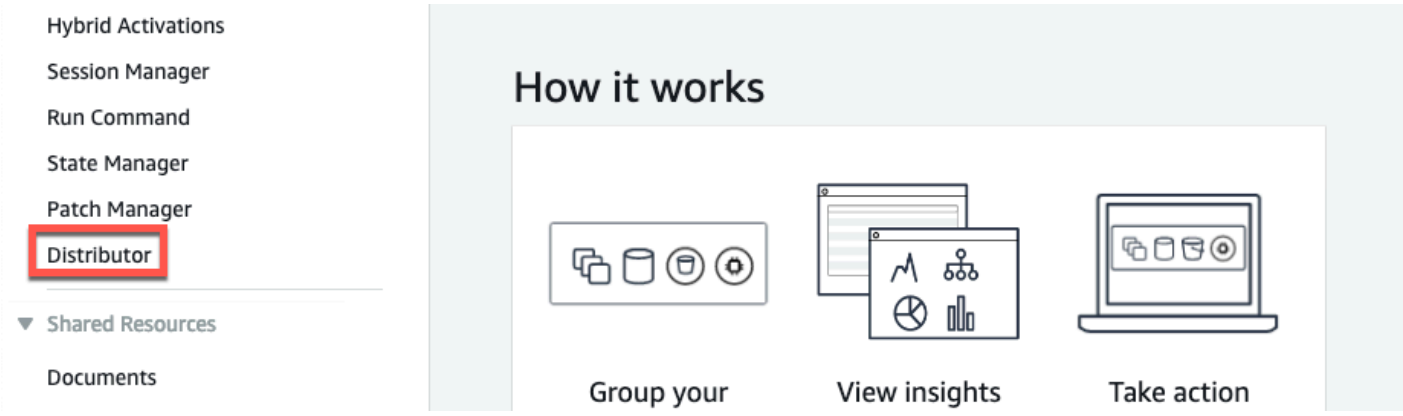
```
wget https//<url to GPG key>
```

```
rpm --import RPM-GPG-KEY-AWS
```

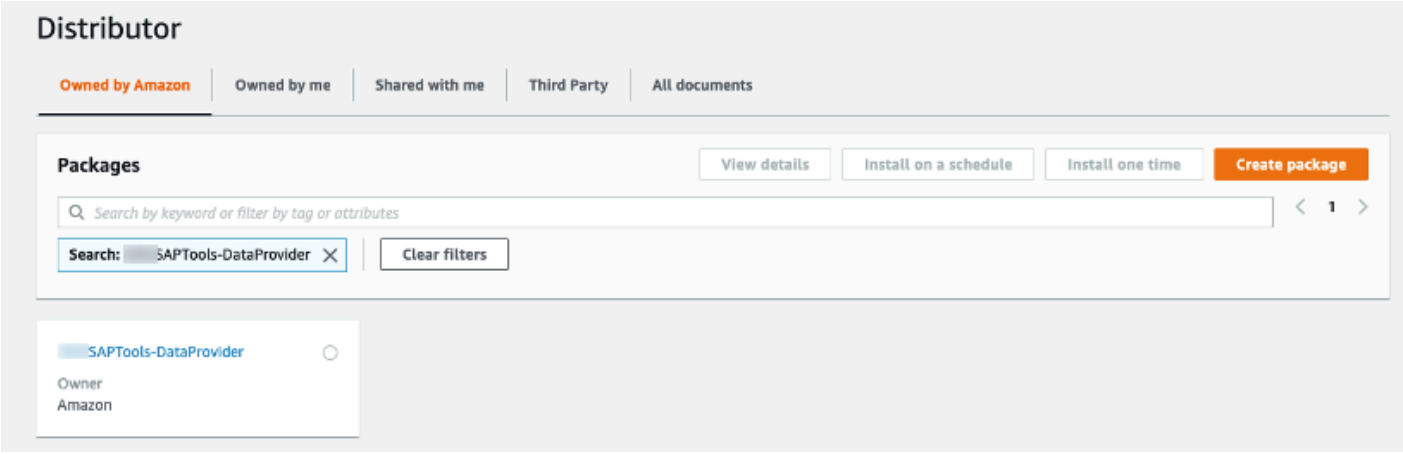
使用 SSM 分发服务器安装 DataProvider 代理

使用以下步骤安装 DataProvider 4.3。

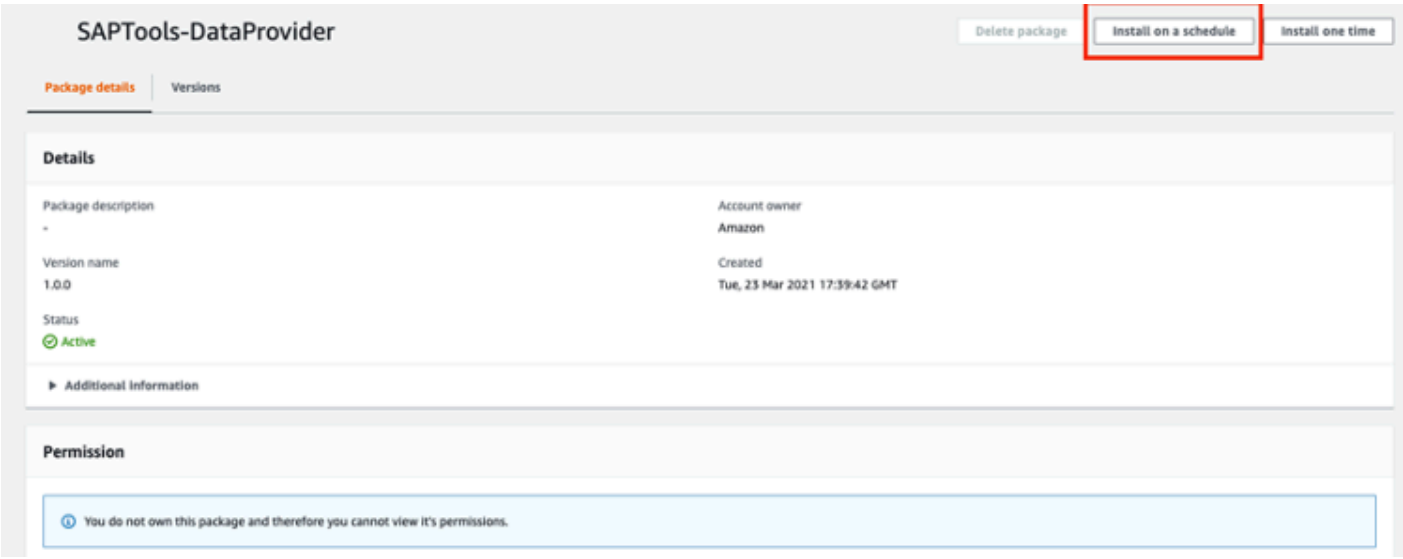
1. 打开 Systems Manager 控制台。
2. 在左侧导航窗格的 “节点管理” 部分下，选择 Distrib utor。



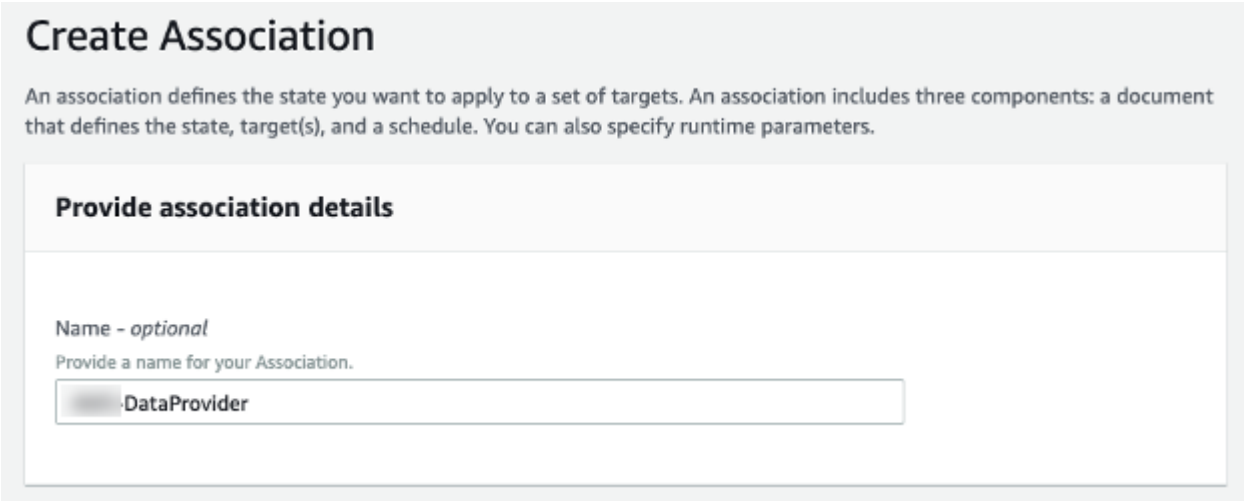
3. 在搜索栏中 AWSSAPTools-DataProvider，键入并选择软件包。



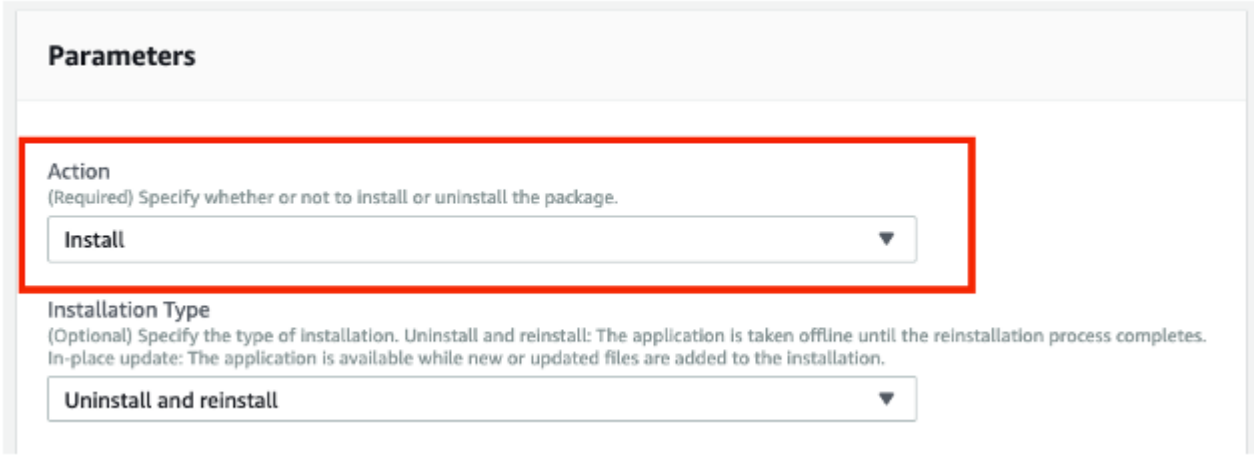
4. 要在新版本发布 DataProvider 时接收自动更新，请选择 “按计划安装”。



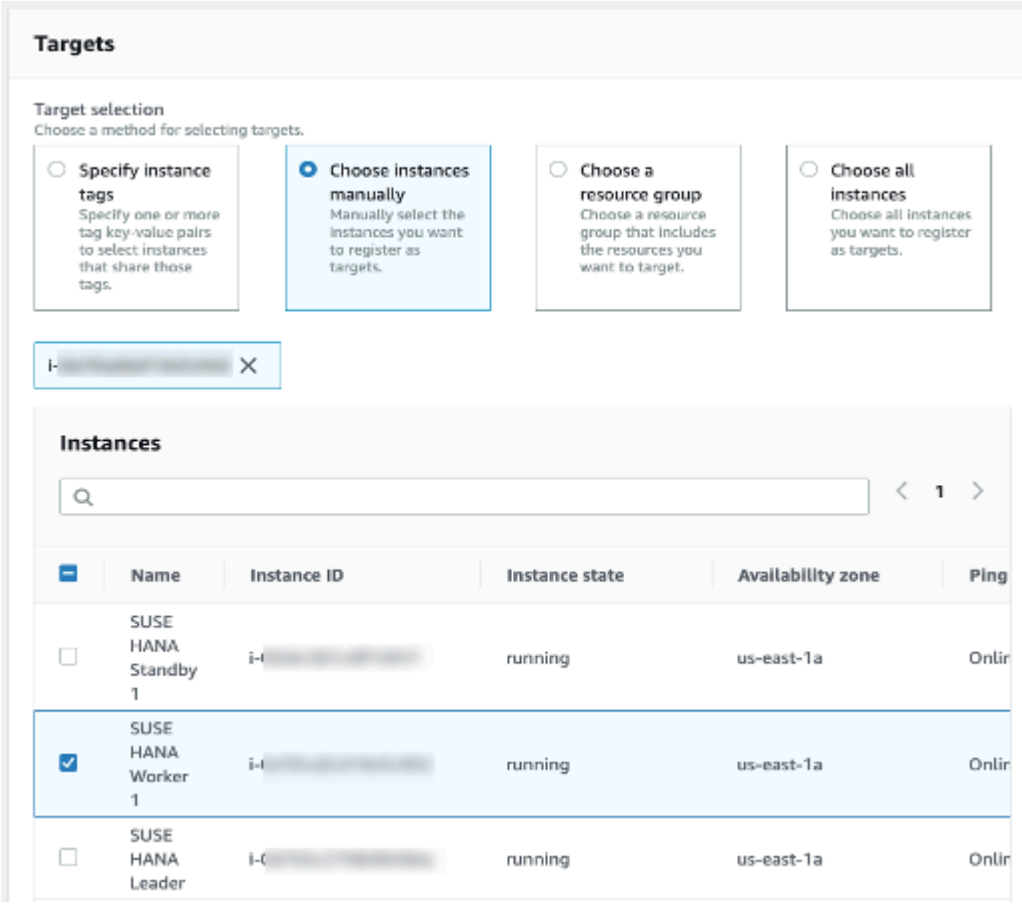
5. 在 “创建关联” 页面上，键入关联的名称。



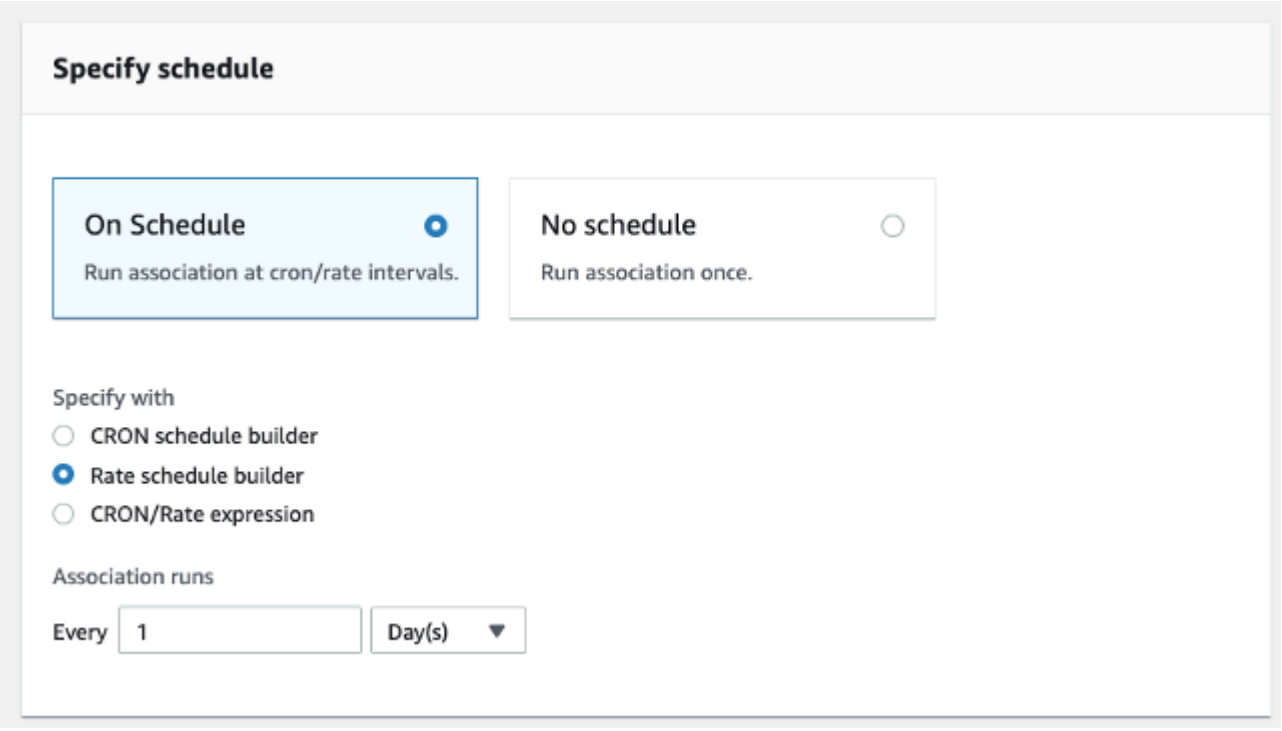
6. 在 “参数” 部分的 “操作” 中，选择 “安装”。



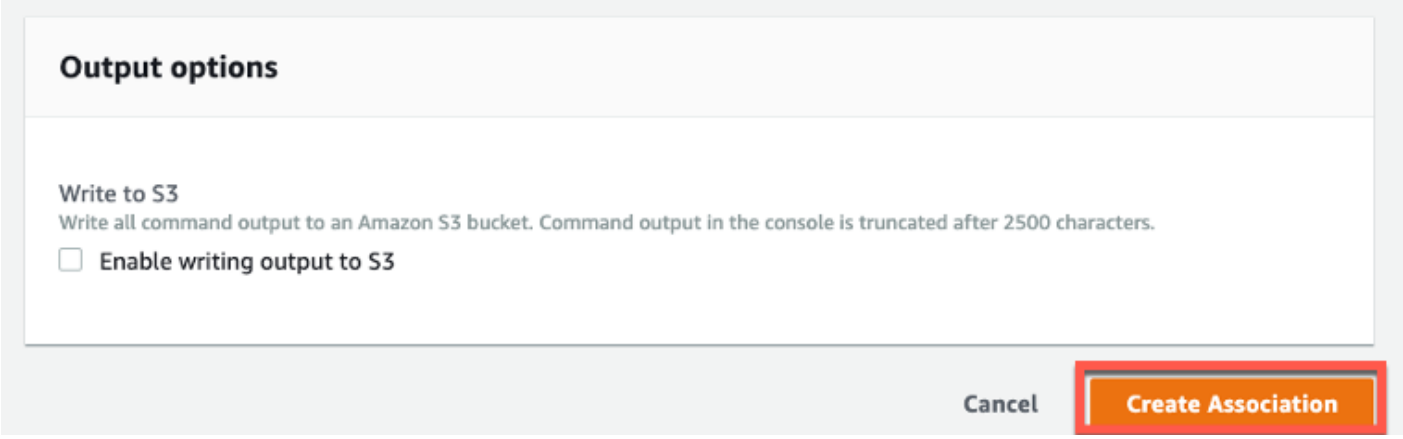
7. 在 “> 目标” 部分中，在 “目标选择” 中，选择 “手动选择实例”。然后，选择要安装的实例 DataProvider。



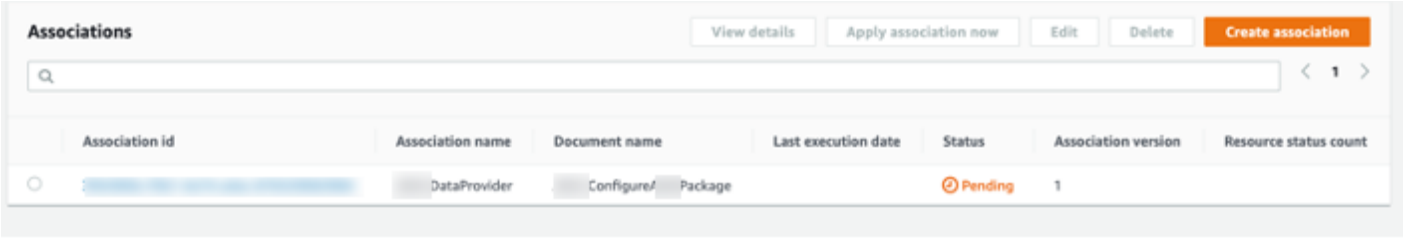
8. 在 “指定日程安排” 部分中，进行以下选择：
   - 选择 “按计划”
   - 对于 “指定方式”，选择 “费率明细表生成器”。
   - 对于助理跑步，请选择 30 天。（AWS 建议 30 天）



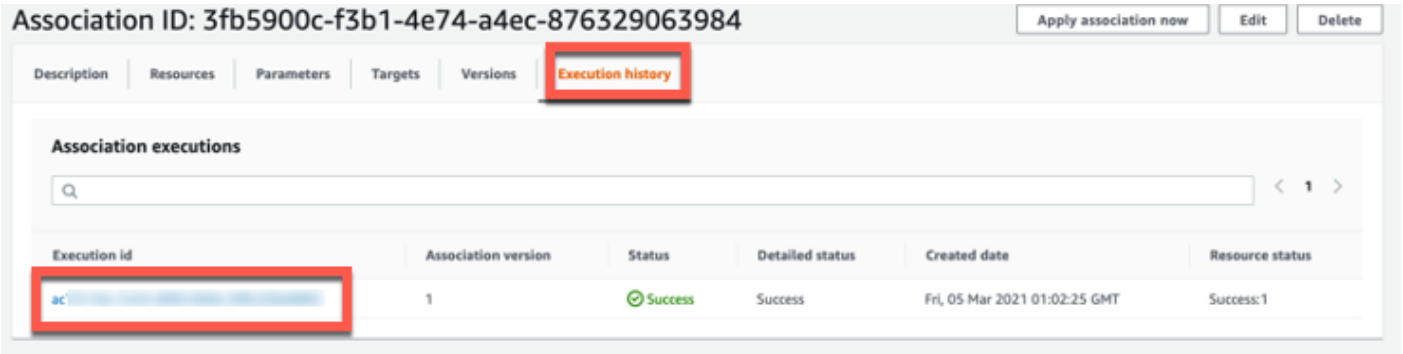
9. 在 “输出选项” 部分，选择 “创建关联”。



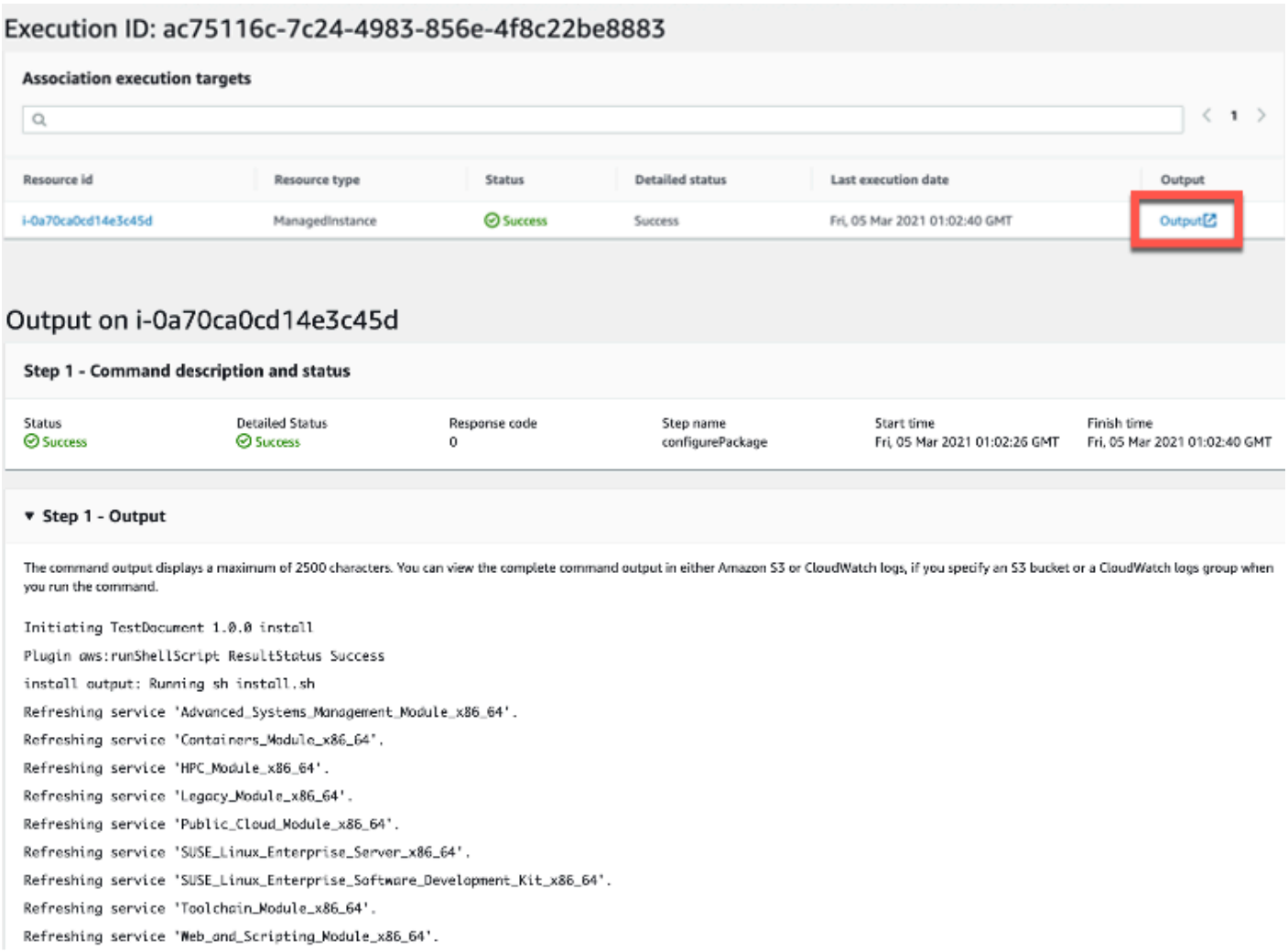
10.创建关联后，选择关联 ID。



11选择 “执行历史记录” 选项卡。然后，选择执行 ID。



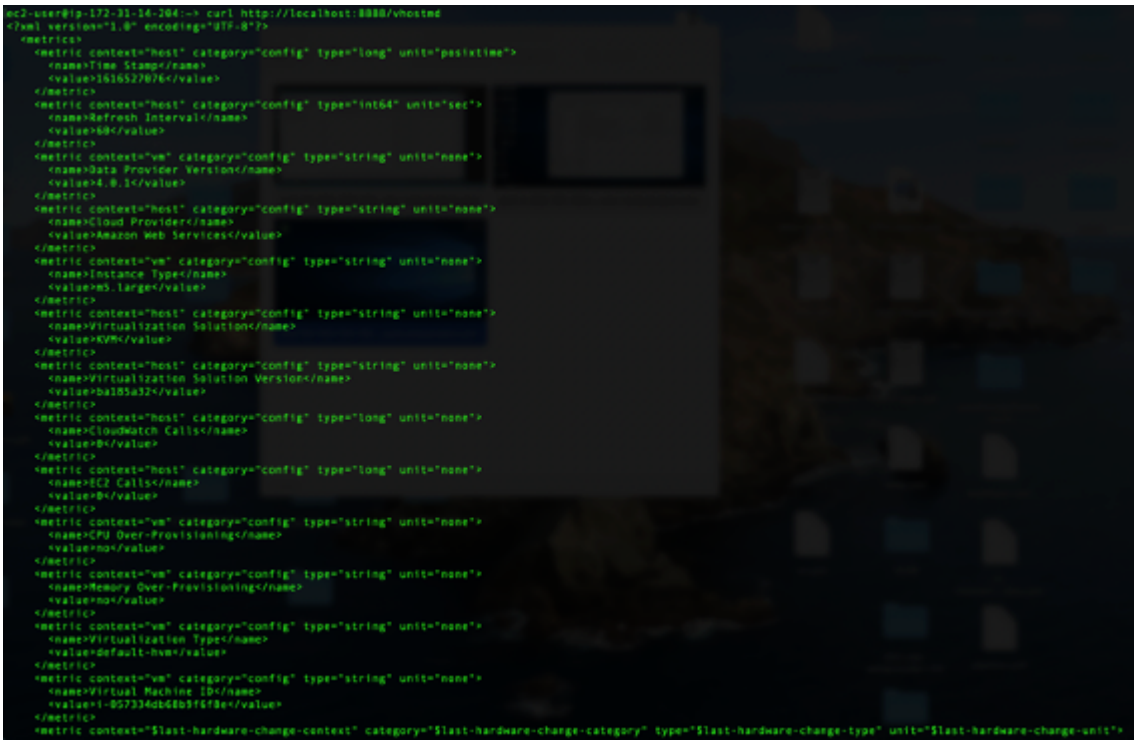
12.在 “执行 ID” 页面上，选择 “输出” 以查看安装结果。



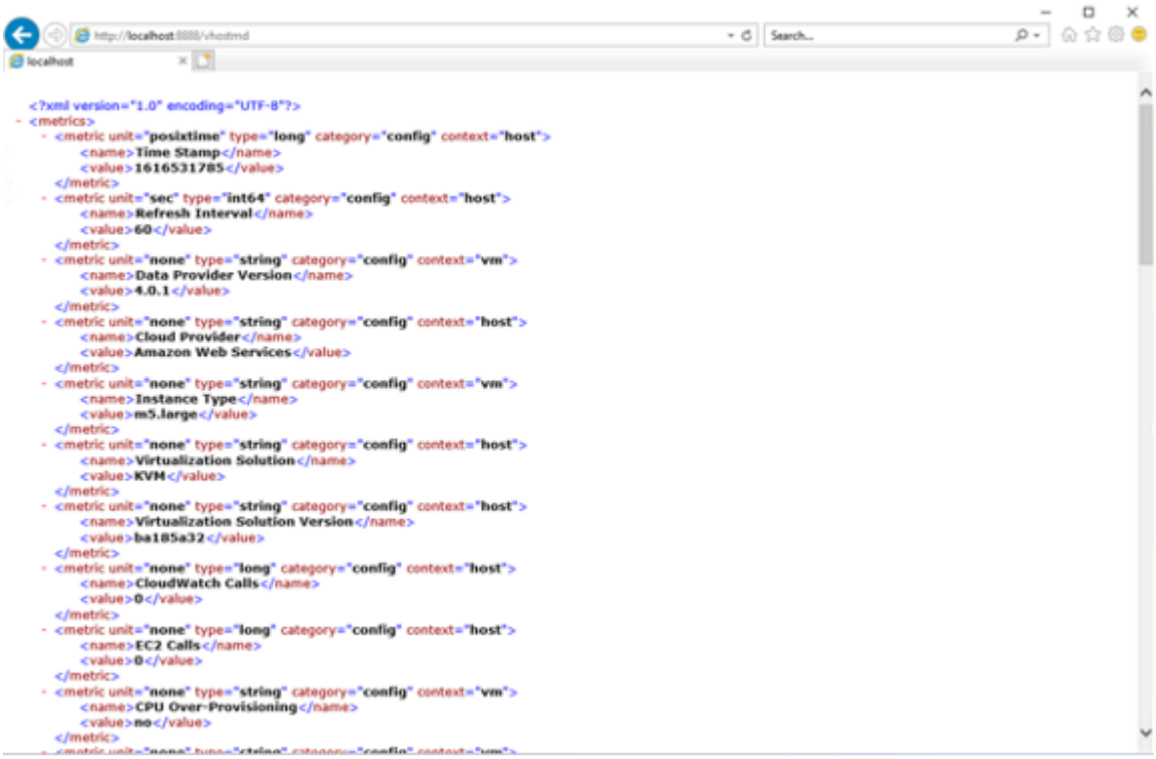

```
The following NEW package is going to be installed:
aws-sap-dataprovider-standalone

The following package has no support information from it's vendor:
aws-sap-dataprovider-standalone

1 new package to install.
Overall download size: 28.0 MiB. Already cached: 0 B. After the operation, additional 28.0 MiB will be used.
Continue? [y/n/...? shows all options] (y): y
Retrieving package aws-sap-dataprovider-standalone-4.0-1.amzn2.x86_64 (1/1), 28.0 MiB ( 28.0 MiB unpacked)

Checking for file conflicts: [...done]
(1/1) Installing: aws-sap-dataprovider-standalone-4.0-1.amzn2.x86_64 [............done]
Additional rpm output:
Will install a SYSTEMD service.

Installing prerequisites.
Done installing prerequisites (SYSTEMD)
*****
Starting the aws-dataprovider service as systemd

*****
Important: Verify log files in /var/log/aws-dataprovider!
*****
Installer completed, exiting.
```

13安装完成后，登录实例，然后 http://localhost:8888/vhostmd [调用端点] DataProvider 以允许获取指标。

- Linux 示例



- Windows 示例



使用可下载的安装程序进行安装 — 4.3 DataProvider

如果您选择不使用 SSM 安装 DataProvider 4.3，则 DataProvider 可以使用以下步骤手动安装。

> **Note**
>
> 在开始手动安装之前，必须安装 “先决条件” 部分中列出的项目。您无需安装SSM-Agent. 可下载内容 DataProvider 不提供自动更新，要获得最新版本，您必须手动检查和下载新版本。

为您的环境下载以下文件。默认情况下，文件将在 us-east-1 区域下载，如果您想将文件下载到其他区域，请在下载之前更改默认区域。

- Red Hat https://aws-sap-dataprovider-us-east-1.s3.us-east-1.amazonaws.com/v4/ installers/linux/RHEL/aws-sap-dataprovider-rhel-standalone .x 86_64.rpm
- SUSE https://aws-sap-dataprovider-us-east-1.s3.us-east-1.amazonaws.com/v4/ installers/linux/SUSE/aws-sap-dataprovider-sles-standalone .x86_64.rpm
- 甲骨文 Linux https://aws-sap-dataprovider-us-east-1.s3.us-east-1.amazonaws.com/v4/ installers/linux/ORACLE/aws-sap-dataprovider-oel-standalone. x86_64.rpm
- Windows https://aws-sap-dataprovider-us-east-1.s3.us-east-1.amazonaws.com/v4/ installers/win/aws-data-provider-installer-win-x64-Standalone.exe
- GPG Key GPG 密钥：安装程序/rp m-gpg-k ey-aws https://aws-sap-dataprovider-us-east-1.s3.us-east-1.amazonaws.com/v4/

在 Linux 上安装

在 Linux 上，数据提供程序以 RPM 包的形式提供。

SUSE Linux Enterprise Server

要在 SUSE Linux 企业服务器 (SLES) 上安装适用于 SAP AWS 的数据提供程序，请下载以下文件：

- 标准：aws-sap-dataprovider-sles.x86_6 4.rpm 和 GPG Key
- 中国 aws-sap-dataprovider-sles ：.x86_64.rpm 和 GPG Key

这些文件完全相同，但由于在中国工作时可能出现连接问题，因此 AWS 提供了这两个位置选项。

要安装数据提供器，请运行以下命令：

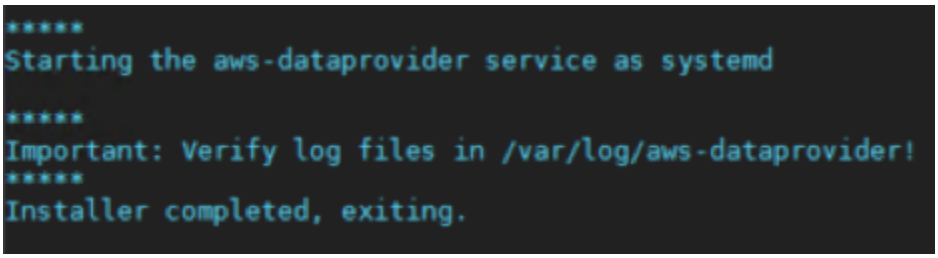
```
wget https://<url to rpm package>
wget https://<url to GPG key>
rpm --import RPM-GPG-KEY-AWS
zypper install -y <rpm package>
```

示例：

```
wget https://aws-sap-dataprovider-us-east-1.s3.us-east-1.amazonaws.com/v4/installers/
linux/SUSE/aws-sap-dataprovider-sles-standalone.x86_64.rpm
wget https://aws-sap-dataprovider-us-east-1.s3.us-east-1.amazonaws.com/v4/installers/
RPM-GPG-KEY-AWS
rpm --import RPM-GPG-KEY-AWS
zypper install -y aws-sap-dataprovider-sles-standalone.x86_64.rpm
```

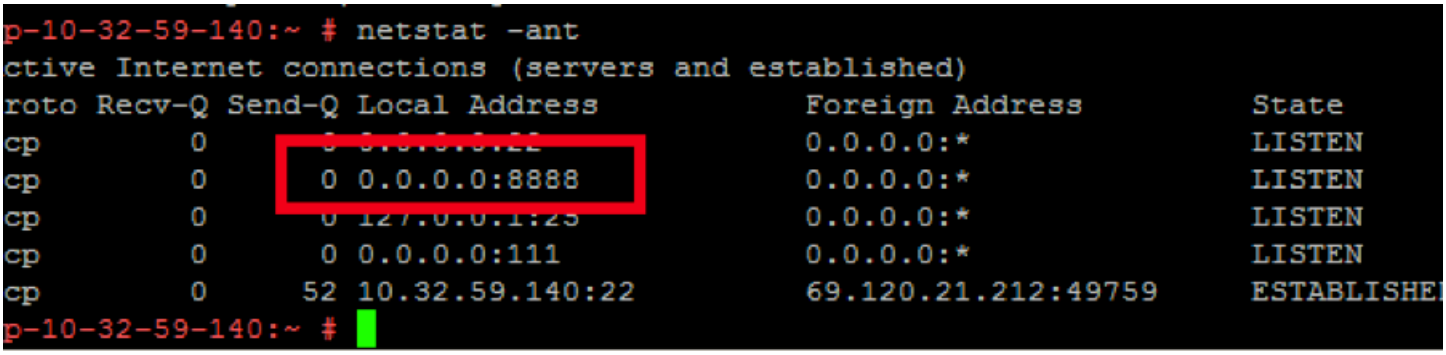
安装 RPM 软件包后，代理会作为守护程序启动，如下图所示。

RPM 软件包安装



通过调用`netstat -ant`确定侦听器是否在 localhost 端口 8888 上运行，验证服务是否正在运行。

在 Linux 上验证安装情况



您还应该在上查看日志文件`/var/log/aws-dataprovider/messages.0`，以确保守护程序具有访问所需指标的适当连接和授权。

在 Linux 上验证连接和授权

```
I 0001C Agent has started with version 4.2.0 : Tue Aug 25 18:13:00 UTC 2020
I 0000C Agent log level has been set to INFO
I 10001 Read in jar configuration; read on board configuration
I 10002 Is there a local, optional configuration file at /usr/local/ec2/aws-dataprovider/config.properties ?
I 10003 Read local, optional configuration file from /usr/local/ec2/aws-dataprovider/config.properties
I 03002 vhostmd agent is listening on localhost
I 0000D Agent is starting the vhostmd provider
I 08001  ** Running Diagnostics **
I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access
I 08009 Diagnostic : Passed
I 0800A Diagnostic : EC2 API Connectivity & Access
I 0800D Diagnostic : Passed
I 08010 Diagnostic: Data Collector API
I 08011 Diagnostic : Passed
I 0800E ** Diagnostics Complete **
```

启动时，监视代理会运行三组诊断：

- AWS 连接诊断可确保与 Amazon S3 的网络连接，从而自动获取 SAP AWS 数据提供程序的更新。
- 第二个诊断测试访问权限 CloudWatch。此授权需要使用允许访问的 IAM 策略为您正在运行的 Amazon EC2 实例分配一个 IAM 角色 CloudWatch。有关详细信息，请参阅本指南前面的 IAM 角色。
- 第三个诊断测试访问亚马逊的授权 EC2，还需要一个与亚马逊 EC2 实例关联的 IAM 角色。

适用于 SAP AWS 的数据提供程序设计为在有或没有连接的情况下运行，但是如果没有连接，您就无法获得更新。如果您没有适当的授权，Amazon CloudWatch 和 Amazon EC2 将返回空值。

您也可以直接致电 SAP AWS 的数据提供商来查看指标。调用`wget http://localhost:8888/vhostmd` 会返回一个包含指标的文件。您可以查看文件内部以查看返回的指标，如下所示。

在 Linux 上查看指标

```
ip-10-32-59-140:~ # wget http://localhost:8888/vhostmd
--2012-10-09 17:10:28--  http://localhost:8888/vhostmd
Resolving localhost... 127.0.0.1, ::1
Connecting to localhost|127.0.0.1|:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/xml]
Saving to: `vhostmd'

    [ <=>                                                   ] 7,58

2012-10-09 17:10:31 (385 MB/s) - `vhostmd' saved [7589]

ip-10-32-59-140:~ # cat vhostmd
<?xml version="1.0" encoding="UTF-8"?>
  <metrics>
    <metric context="host" category="config" type="long" unit="posixtime"
      <name>Time Stamp</name>
      <value>1349802629284</value>
    </metric>
    <metric context="host" category="config" type="int64" unit="sec">
      <name>Refresh Interval</name>
      <value>60</value>
    </metric>
    <metric context="host" category="config" type="string" unit="none">
      <name>Cloud Provider</name>
      <value>Amazon Web Services</value>
    </metric>
    <metric context="host" category="config" type="string" unit="none">
      <name>Instance Type</name>
      <value>m1.large</value>
    </metric>
```

现在，每次操作系统启动时，适用于 SAP AWS 的数据提供程序都会自动启动。您也可以使用以下命令手动停止并重新启动 SAP AWS 数据提供器，具体取决于您的操作系统版本：

- SLES 11、Oracle Linux 6 和红帽 Linux 6：

```
service aws-dataprovider [start|stop]
```

- SLES 12、SLES 15、Oracle Linux 7、甲骨文 Linux 8、Red Hat Linux 7 和红帽 Linux 8。

```
systemctl [start|stop] aws-dataprovider
```

如果您对互联网没有透明 HTTP/HTTPS 访问权限，则可以将 AWS 数据提供者配置为使用代理。

1. 停止 SAP AWS 的数据提供商。
2. 在位于的文件中输入代理信息（如下所示）`/usr/local/ec2/aws-dataprovider/proxy.properties`。

```
#proxy.properties
#used to set web proxy settings for the {aws} Data Provider for SAP
#Https is the only supported proxy method
#Blank values for everything means no proxy set

https.proxyHost=
https.proxyPort=
https.proxyDomain=
https.proxyUsername=
https.proxyPassword=
```

3. 启动适用于 SAP AWS 的数据提供程序。

在红帽和甲骨文企业 Linux 上安装

对于 Red Hat 和 Oracle Enterprise Linux，安装步骤与上述 SLES 的安装步骤相同，但是 RPM 文件和安装 RPM 软件包的命令有所不同。

- Red Hat

  默认值：aws-sap-dataprovider-rhel.x 86_64.rpm
- 甲骨文企业 Linu

  默认值：aws-sap-dataprovider-oel.x 86_64.rpm

要安装数据提供器，请运行以下命令：

```
wget https://<url to rpm package>
yum -y install <rpm package>
```

示例：

```
wget https://aws-sap-data-provider.s3.amazonaws.com/Installers/aws-sap-dataprovider-
rhel.x86_64.rpm
```

```
yum -y install aws-sap-dataprovider-rhel.x86_64.rpm
```

在 Windows 上安装

在 Windows 上，安装程序以 NSIS（Nullsoft 脚本安装系统）可执行文件的形式提供。

1. 打开 Web 浏览器并下载安装程序：
   - 默认：aws-data-provider-installer-win-x64.exe
2. 运行下载的 exe 文件。
3. 验证安装。
   - 安装完成后，您可以在`C:\Program Files\Amazon\DataProvider`目录中看到该文件。
   - 安装还会创建并启动一项名为 “适用于 SAP AWS 的数据提供器” 的 Windows 服务。
   - 在 Web 浏览器中输入 http://localhost:8888/vhostmd 以验证服务是否正在运行。如果安装成功，该页面会返回来自 SAP AWS 数据提供商的指标。
4. 如果您对互联网没有透明 HTTP/HTTPS 访问权限，则可以将 AWS 数据提供者配置为使用代理。
   a. 停止 SAP AWS 的数据提供商。
   b. 在位于的文件中输入代理信息（如下所示）`C:\Program Files\Amazon\DataProvider\proxy.properties`。

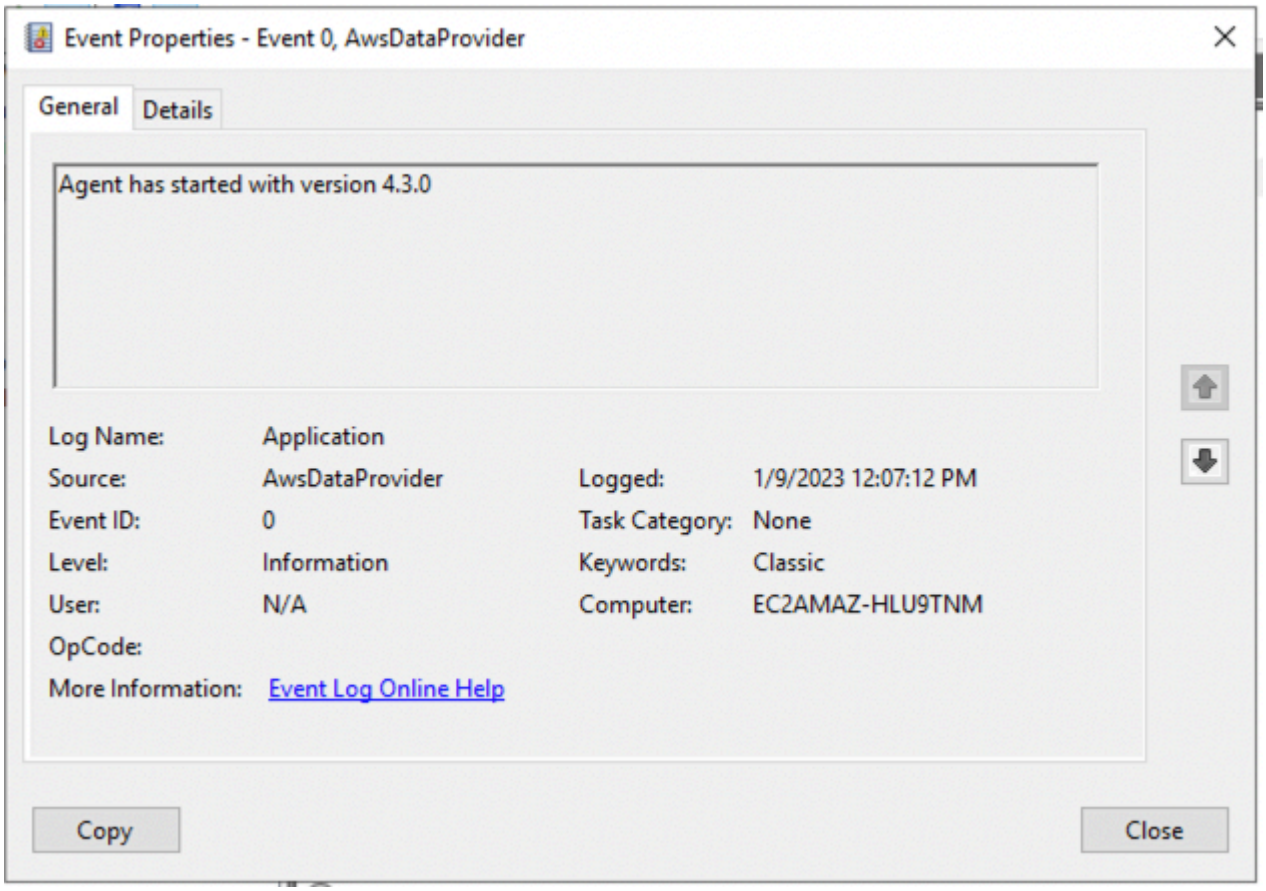
   ```
   #proxy.properties
   #used to set web proxy settings for the {aws} Data Provider for SAP
   #Https is the only supported proxy method
   #Blank values for everything means no proxy set

   https.proxyHost=
   https.proxyPort=
   https.proxyDomain=
   https.proxyUsername=
   https.proxyPassword=
   ```

   c. 启动适用于 SAP AWS 的数据提供程序。
5. 通过`netstat -ant`从命令窗口或 Windows PowerShell 脚本调用，以确定侦听器是否在本地主机端口 8888 上运行，验证服务是否正在运行。

```
PS C:\Users\Administrator\Desktop> netstat -ant

Active Connections

  Proto  Local Address          Foreign Address        State           Offload S
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:8888           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       InHost
  TCP    10.191.175.27:139      0.0.0.0:0              LISTENING       InHost
  TCP    10.191.175.27:3389     69.120.21.212:50796    ESTABLISHED     InHost
  TCP    10.191.175.27:49511    23.63.240.60:443       CLOSE_WAIT      InHost
  TCP    10.191.175.27:49555    74.125.228.104:80      TIME_WAIT       InHost
  TCP    10.191.175.27:49556    74.125.228.103:80      ESTABLISHED     InHost
  TCP    10.191.175.27:49558    169.254.169.254:80     CLOSE_WAIT      InHost
```

在 Windows 上验证安装情况

6. 导航到 Windows 事件日志，然后从 SAP AWS 数据提供程序中查找启动事件的应用程序日志。检查诊断信息。



在 Windows 上检查诊断程序

启动时，监视代理会运行三组诊断：

- AWS 连接诊断可确保与 Amazon S3 的网络连接，从而自动获取 SAP AWS 数据提供程序的更新。
- 第二个诊断测试访问授权 CloudWatch，这需要使用允许访问的 IAM 策略为您正在运行的 EC2 实例分配一个 IAM 角色 CloudWatch。有关详细信息，请参阅本指南前面的 IAM 角色。
- 第三个诊断测试访问亚马逊的授权 EC2，还需要一个与亚马逊 EC2 实例关联的 IAM 角色。

适用于 SAP AWS 的数据提供程序设计为在有或没有连接的情况下运行，但是如果没有连接，您就无法获得更新。如果您没有适当的授权，Amazon CloudWatch 和 Amazon 会 EC2 返回空值。

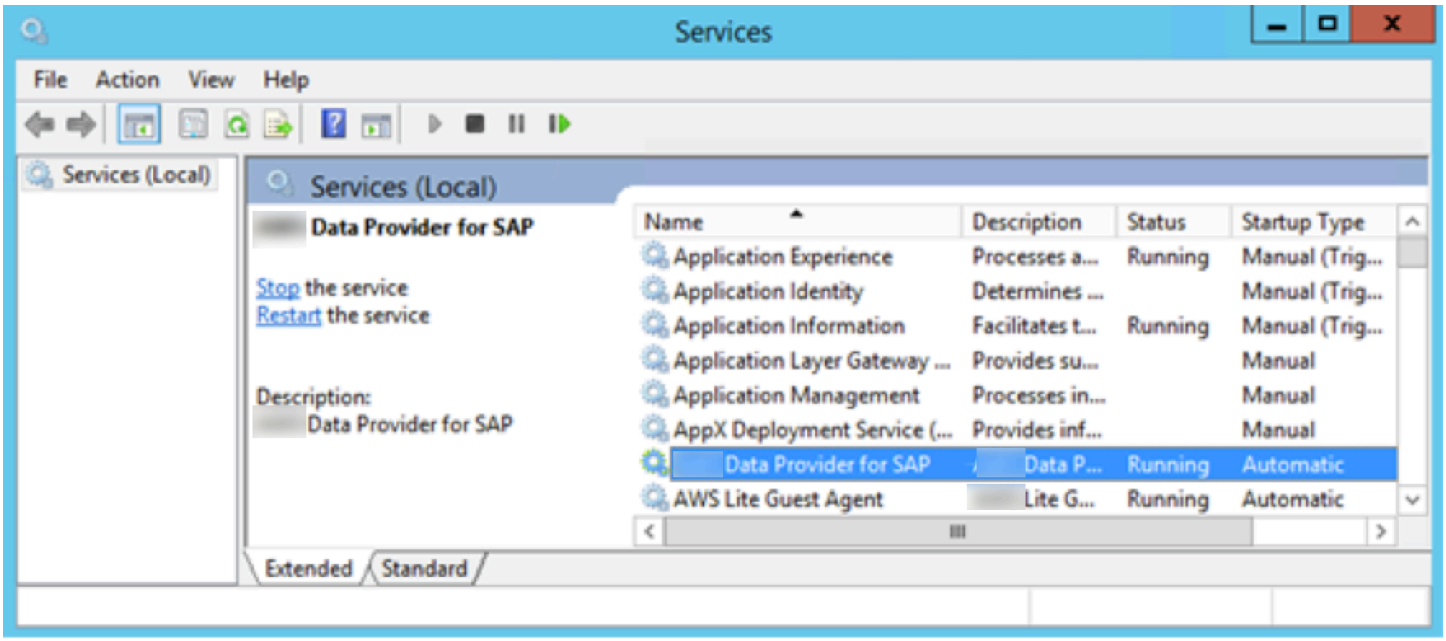
您也可以直接从 Web 浏览器调用 SAP AWS 数据提供程序来查看指标，如图所示。

在 Windows 上查看指标

```
- <metrics>
  - <metric context="host" category="config" type="long" unit="posixtime">
      <name>Time Stamp</name>
      <value>1349813196225</value>
    </metric>
  - <metric context="host" category="config" type="int64" unit="sec">
      <name>Refresh Interval</name>
      <value>60</value>
    </metric>
  - <metric context="host" category="config" type="string" unit="none">
      <name>Cloud Provider</name>
      <value>Amazon Web Services</value>
    </metric>
  - <metric context="host" category="config" type="string" unit="none">
      <name>Instance Type</name>
      <value>m1.xlarge</value>
    </metric>
```

AWS 现在，每次操作系统启动时，适用于 SAP 的数据提供程序都会自动启动。您也可以手动停止和重启适用于 SAP AWS 的数据提供程序，就像停止并重新启动任何其他 Windows 服务一样。

在 Windows 上停止并重新启动适用于 SAP AWS 的数据提供器



要配置代理设置，可以将自定义`proxy.properties`文件放在 Windows 的临时目录中，该目录由 Windows 系统变量 %TEMP% 指定。

订阅 AWS 数据提供者代理以获取通知

当 AWS 数据提供程序代理的新版本发布时，Amazon 简单通知服务可以通知您。使用以下步骤设置此订阅。

1. 打开 https://console.aws.amazon.com/sns/v3/home。
2. 确保您位于美国弗吉尼亚北部 (us-east-1) 区域。
3. 在左侧导航窗格中，选择订阅 > 创建订阅。
4. 根据您使用 AWS 数据提供器代理的 AWS 区域添加主题 ARN。

区域	ARN
默认	`arn:aws:sns:us-east-1:804845276281:AWS-DataProvider-SAP-Update`

区域	ARN
AWS GovCloud （美国西部）和 AWS GovCloud （美国东部）	`arn:aws-us-gov:sns:us-gov-west-1:140982767562:AWS-Data Provider-SAP-Update`
中国（北京）区域和中国（宁夏）区域	`arn:aws-cn:sns:cn-north-1:001645243879:AWS-DataProvider-SAP-Update`

5. 协议-选择电子邮件或短信。
   - 电子邮件-在 “终端节点” 字段中输入您想要接收通知的电子邮件地址。

     > **Note**
     >
     > 要启用电子邮件通知，您必须按照提供的电子邮件地址上收到的说明确认您的电子邮件订阅。

   - 短信 — 在 “终端节点” 字段中输入您想要接收通知的电话号码。
6. 选择创建订阅。现在，无论何时发布新版本 AWS 的数据提供者代理，您都可以收到通知。

要取消订阅通知，请按以下步骤操作。

1. 打开 https://console.aws.amazon.com/sns/v3/home。
2. 在左侧导航窗格中，选择 “订阅”。
3. 从您的订阅列表中选择订阅，然后选择 “删除”。

正在更新到 DataProvider 4.3

如果您之前安装了 DataProvider 2.0 或 3.0，并且想要更新到 DataProvider 4.3，则需要先卸载正在运行的版本，然后再安装 DataProvider 4.3。

使用 SSM 分销商软件包更新到 DataProvider 4.3

当您通过 SSM 发行版安装 DataProvider 4.3 时，它将在新版本上自动更新已安装的软件包。有关更多信息，请参阅安装或更新软件包。

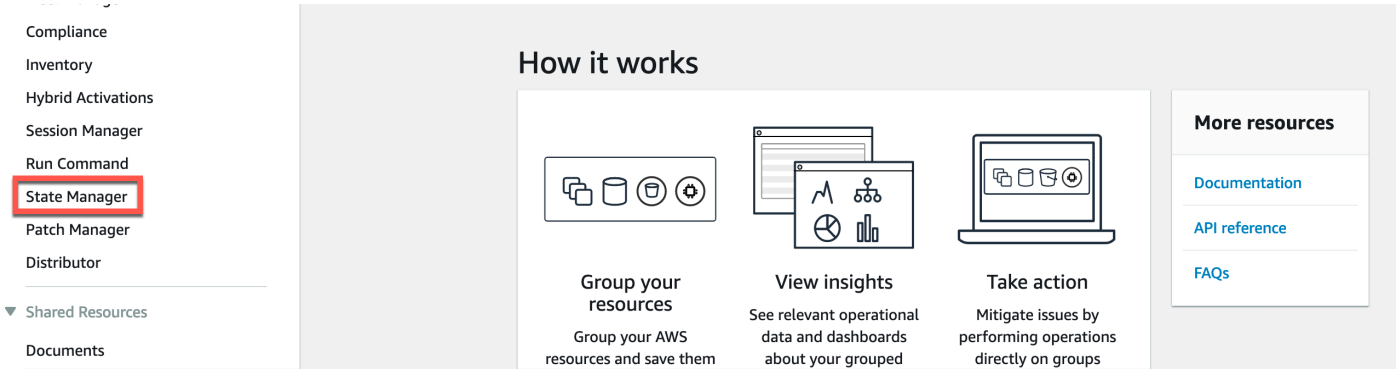
要手动更新 DataProvider 4.3，必须先卸载正在运行的版本，然后安装更新的版本。

DataProvider 4.3 不支持以下操作：

- 如果 DataProvider 已使用 SSM 发行版安装了 RPM 软件包，则手动更新 RPM 软件包。
- 如果是使用 RPM 手动安装的， DataProvider 则通过 SSM 发行商自动更新。
- 在任何情况下都可以手动更新 RPM 软件包。

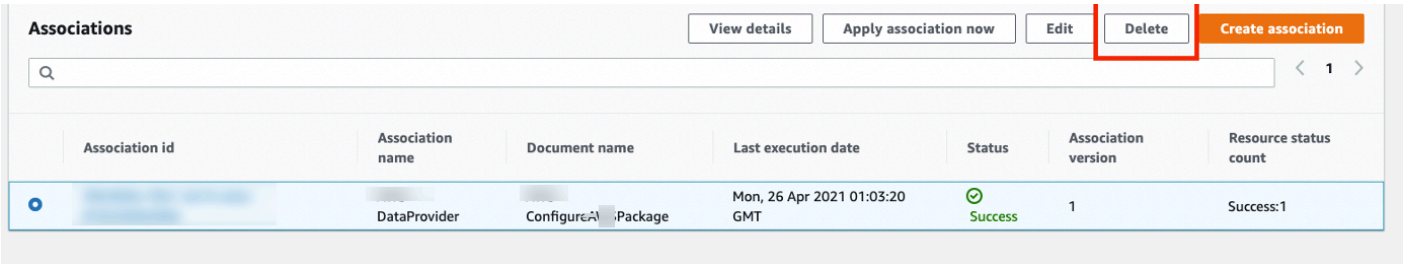
使用 SSM 发行版卸载 DataProvider 4.3

1. 打开 AWS Systems Manager 控制台，在左侧导航窗格中，选择状态管理器。

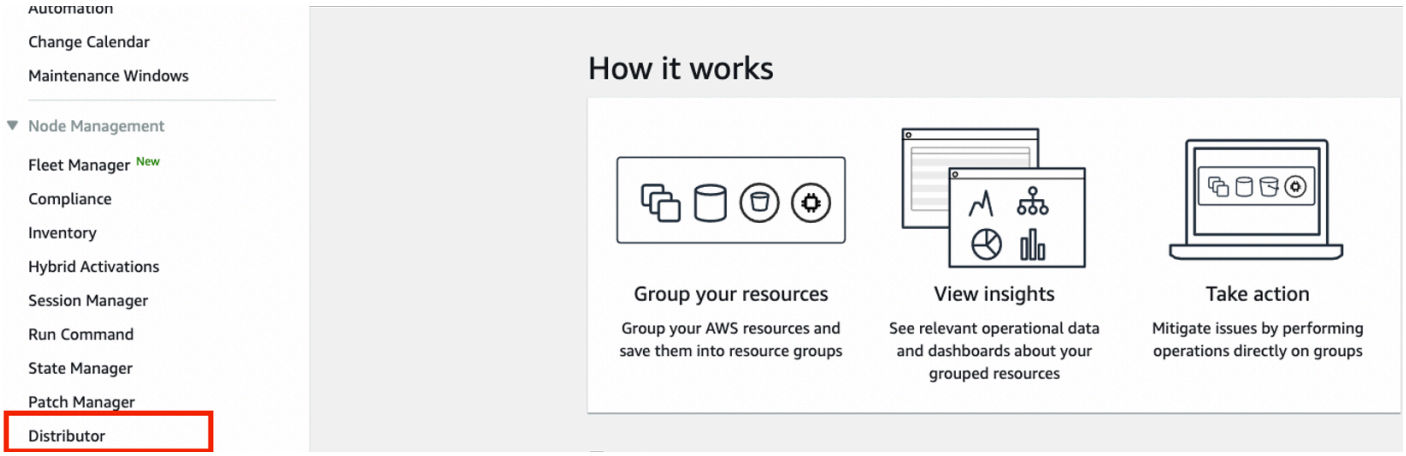


2. 在 “关联” 页面上，选择关联 ID。然后选择 Delete(删除)。

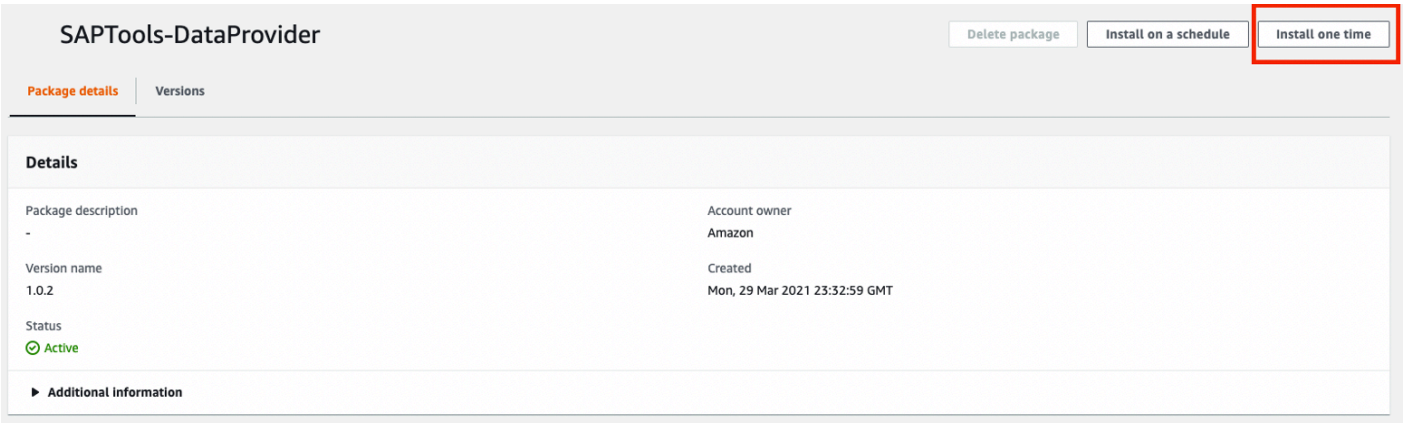
   删除成功后，自动更新将停止。



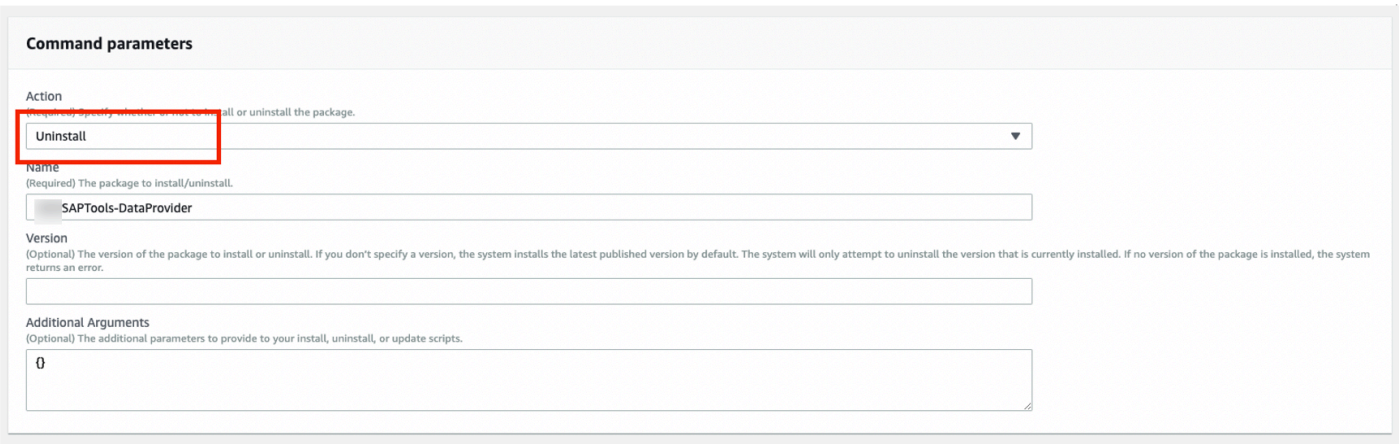
3. 在主页的左侧导航页中，选择分销商。



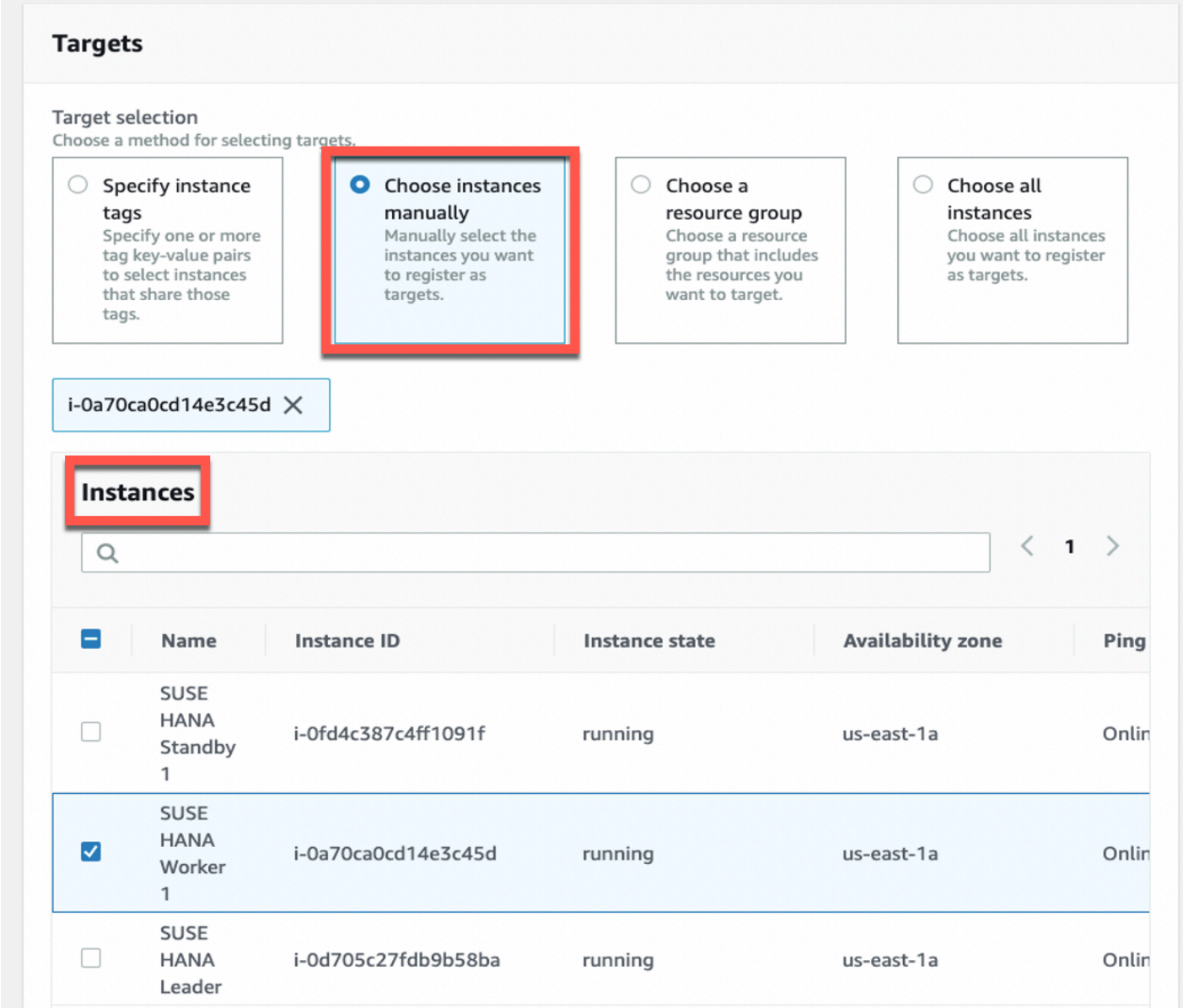
4. 选择分AWSSAPTools-DataProvider销商软件包，然后选择一次安装。



5. 在 “命令参数” 部分中，选择 “卸载”。



6. 在目标部分中，选择手动选择实例。然后选择要卸载的实例 DataProvider。



7. 选择 “运行” 开始卸载。

手动卸载 DataProvider 4.3

RedHat

```
yum erase aws-dataprovider-standalone
```

SUSE

```
zypper rm aws-dataprovider-standalone
```

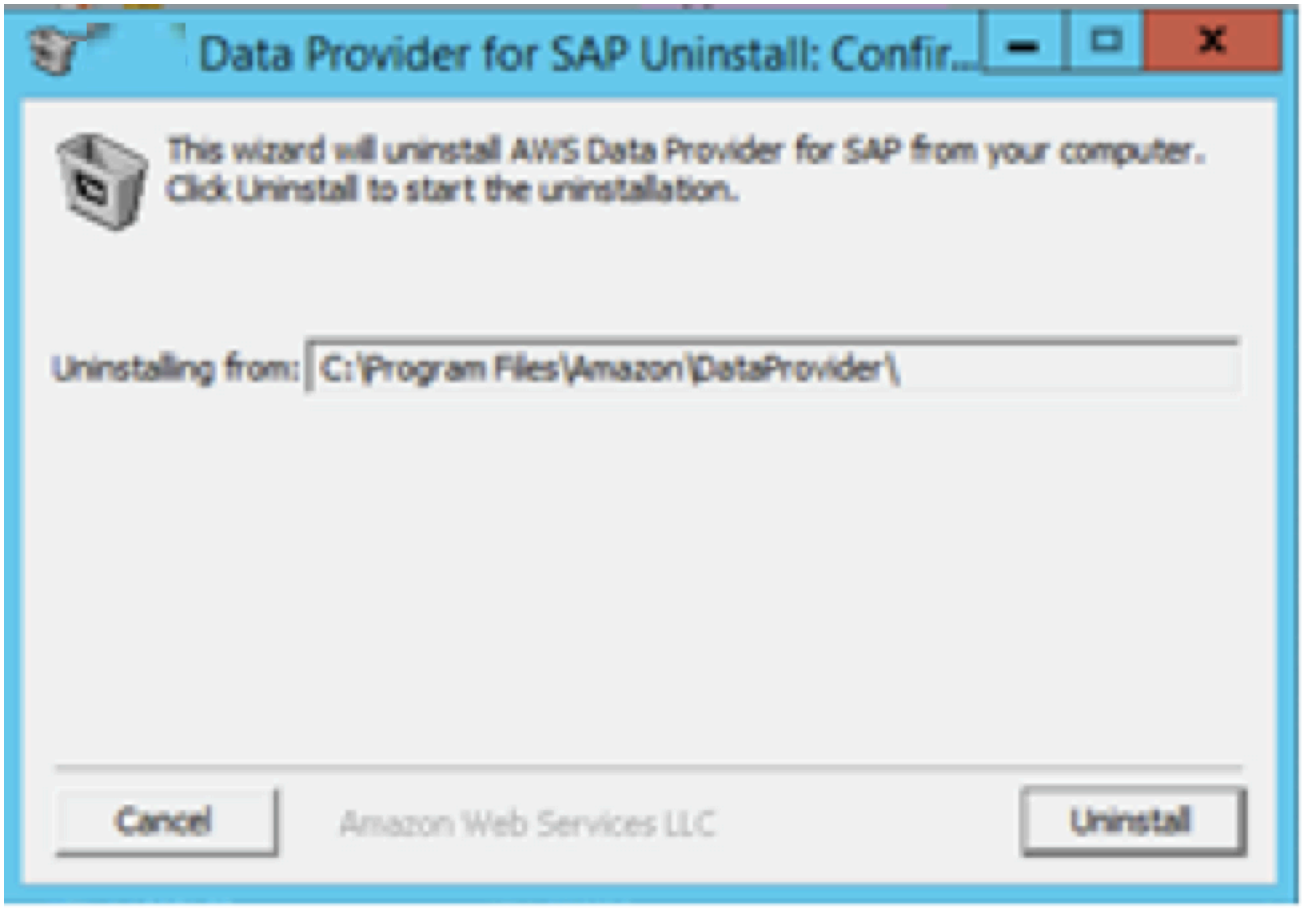
Windows

1. 运行卸载程序。

```
C:\Program Files\AmazonA\DataProvider\uninstall.exe
```

2. 出现提示时，选择 “卸载”。

在 Windows 上卸载适用于 SAP AWS 的数据提供器



正在卸载旧版本

卸载适用于 SAP AWS 的数据提供程序不需要 SAP 停机，并且可以在线完成。唯一的影响将是系统上安装时指标监控信息的缺口。 DataProvider

卸载 DataProvider 3.0

Linux

1. 以超级用户身份登录 Linux，例如 root。
2. DataProvider 使用以下命令停止并删除。

SLES

```
zypper remove -y aws-sap-dataprovider
```

RHEL/OEL

```
yum -y erase aws-sap-dataprovider
```

Windows

```
“C:\Program Files\Amazon\DataProvider\uninstall.exe“
```

卸载 DataProvider 2.0

Linux

1. 以超级用户身份登录 Linux，例如 root。
2. DataProvider 使用以下命令停止并删除。

```
/usr/local/ec2/aws-agent/bin/aws-agent_uninstall
```

Windows

```
“C:\Program Files\Amazon\DataProvider\uninstall.exe“
```

故障排除

本节为分析安装问题提供了帮助。

在 Linux 系统上

问题：安装失败，我不确定我的文件是否处于一致状态。

使用以下命令停止并移除数据提供器。

销售：

```
zypper remove -y aws-sap-dataprovider
```

RHEL/ OEL:

```
yum -y erase aws-sap-dataprovider
```

问题：SAP AWS 的数据提供程序在安装过程结束时无法启动。

请查看日志文件/var/log/aws-dataprovider以获取有关未按预期进行的事情的提示。如果需要，请卸载并重新安装数据提供程序。如果重新安装适用于 SAP AWS 的数据提供程序不能解决问题，则可以通过编辑/usr/local/ec2/aws-dataprovider/bin/aws-dataprovider文件来收集有关 SAP AWS 数据提供器的调试信息。

在 Linux 上调试安装

```
### BEGIN INIT INFO
# Provides:          aws-dataprovider
# Required-Start:    $local_fs $network
# Required-Stop:     $local_fs
# Default-Start:     3 5
# Default-Stop:      0 1 6
# Short-Description: aws-dataprovider
### END INIT INFO

## Determine Download bucket by region
REGION="$(wget --no-proxy -q -O /dev/stdout http://169.254.169.254/latest/dynamic/instance-identity/document | awk -F\" '/region/ {
print $4}' )"
if [[ $REGION == *"cn"* ]]
then
   REGIONENDPOINT="s3.cn-northwest-1.amazonaws.com.cn"
   MYBUCKET="aws-sap-data-provider-china"
else
   REGIONENDPOINT="s3.amazonaws.com"
   MYBUCKET="aws-sap-data-provider"
fi
MYS3="https://${REGIONENDPOINT}/${MYBUCKET}"

DAEMON="/usr/local/ec2/aws-dataprovider/bin/jsvc"
DAEMONOPTS="-jvm server -home /usr/local/ec2/aws-dataprovider/jre/amazon-corretto-8.242.08.1-linux-x6[illegible]-pidfile /tmp/aws-dataprovi
der.pid -cp /usr/local/ec2/aws-dataprovider/lib/installer.jar:/usr/local/ec2/aws-dataprovider/lib/comm[illegible]s-daemon-1.0.10/commons-dae
mon-1.0.10.jar -Dcom.amazon.aws.aws-dataprovider.proxypath=/usr/local/ec2/aws-dataprovider -Dcom.amazon.aws.aws-dataprovider.access
=${MYS3} com.amazon.aws.dataprovider.AwsDataProvider /usr/local/ec2/aws-dataprovider -vhostmd -LogLevel=INFO"
```

现在，如果你运行服务aws-dataprovider-start或systemctl start aws-dataprovider，你会得到很多调试输出，这些输出可能会帮助你诊断问题的根本原因。

Linux 上的调试信息

```
Java VM created successfully
Class org/apache/commons/daemon/support/DaemonLoader found
Native methods registered
java_init done
Daemon loading...
Daemon loaded successfully
java_load done
18:05:28.561 I 06002 Starting the data collector engine

18:05:29.230 I 00001 ****** AWS SAP Data Collector Agent is Starting ******

18:05:29.237 I 00002 Software Version: 1.0.47 : Fri Sep 21 22:22:00 UTC 20

18:05:29.239 I 0000C Agent log level has been set to FINE

18:05:29.241 I 08001  ** Running Diagnostics **

18:05:29.241 I 08002 Diagnostic : AWS Connectivity

18:05:30.078 I 08005 Diagnostic : Passed

18:05:30.078 I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access

18:05:30.803 I 08009 Diagnostic : Passed

18:05:30.803 I 0800A Diagnostic : EC2 API Connectivity & Access

18:05:31.082 I 0800D Diagnostic : Passed

18:05:31.083 I 0800E ** Diagnostics Complete **

18:05:31.282 I 03002 vhostmd agent is listening on localhost

18:05:31.282 I 0000D Agent is starting the vhostmd provider

18:05:31.282 I 00003 ************************************************
```

问题：当我查看日志时，我注意到我的安装未通过所有诊断。

Linux 上互联网连接问题的症状

```
14:32:15.862 I 08001  ** Running Diagnostics **

14:32:15.862 I 08002 Diagnostic : AWS Connectivity

14:33:19.362 W 08003 Diagnostic : Failed

14:33:19.362 I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access

14:33:19.515 W 08007 Diagnostic : Failed

14:33:19.516 I 0800A Diagnostic : EC2 API Connectivity & Access

14:33:19.542 W 0800B Diagnostic : Failed

14:33:19.542 I 0800E ** Diagnostics Complete **
```

如果所有诊断均失败，则表明您的互联网出站连接存在问题。你可以通过 ping 一个知名的互联网位置（例如 www.am azon.com）来确认这一点。路由问题的最常见原因是 VPC 网络配置，它需要有互联网网关或通过互联网路由与您的数据中心建立 VPN 连接。有关详细信息，请参阅本指南前面的 Amazon VPC 网络拓扑。

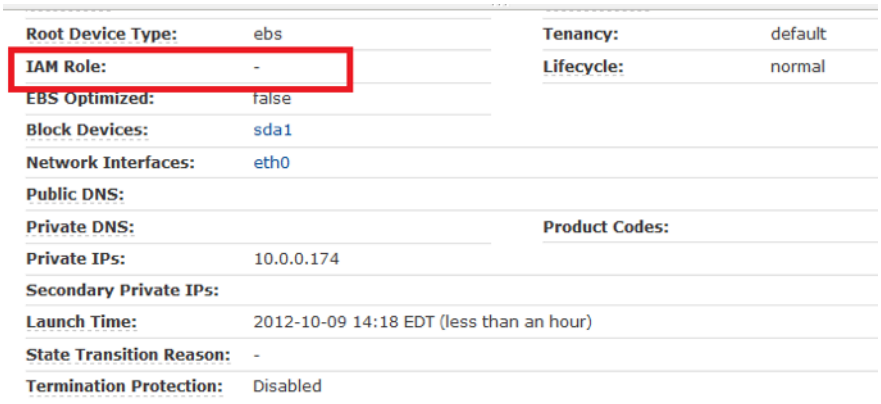
问题：当我查看日志时，我注意到我无法访问 CloudWatch 和Amazon EC2，但我确实通过了第一次 AWS 连接诊断。

Linux 上出现授权问题的症状

```
14:38:57.467 I 08001  ** Running Diagnostics **

14:38:57.468 I 08002 Diagnostic : AWS Connectivity

14:38:58.182 I 08005 Diagnostic : Passed

14:38:58.182 I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access

14:38:58.325 W 08007 Diagnostic : Failed

14:38:58.325 I 0800A Diagnostic : EC2 API Connectivity & Access

14:38:58.357 W 0800B Diagnostic : Failed

14:38:58.357 I 0800E ** Diagnostics Complete **
```

这清楚地表明您在尝试访问 CloudWatch 和Amazon时遇到了授权问题 EC2。此问题的常见原因是没有与您的实例关联的 IAM 角色，该角色包含本指南前面的 I AM 角色中指定的 IAM 策略。您可以通过在 Amazon EC2 控制台中查看相关的 Amazon EC2 实例并验证 IAM 角色来快速诊断此问题。

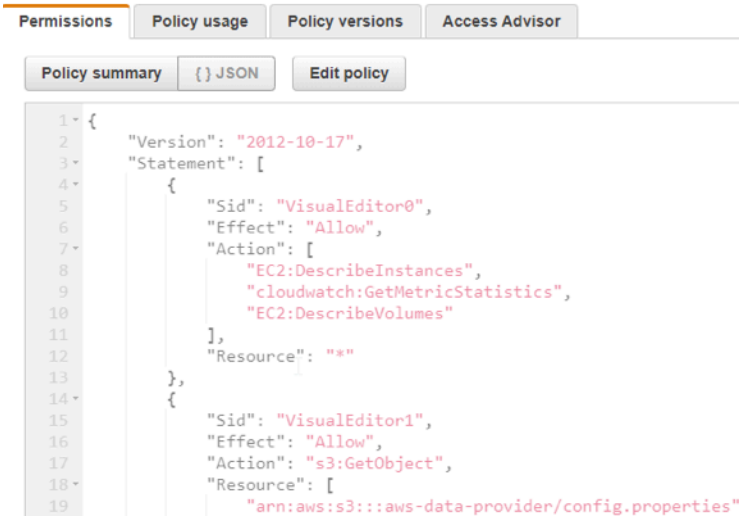
验证 EC2 实例的 IAM 角色



如果 IAM 角色不存在，则按照本指南前面介绍的 IAM 角色中指定的方式创建该角色。

如果您确实为该实例分配了 IAM 角色，请前往 IAM 控制台，选择 IAM 角色名称，然后展开策略。验证您是否拥有本指南前面的 IAM 角色中指定的必需策略。

验证 IAM 角色的策略



问题：我想为数据提供程序配置/更新**JAVA_HOME**。

打开`/usr/local/ec2/aws-dataprovider/env`文件并更新`JAVA_HOME`变量。更新后，使用以下命令重新启动数据提供器。

```
sudo systemctl daemon-reload
sudo systemctl start aws-dataprovider
```

Windows 上的问题排查

问题：安装失败，我不确定我的文件是否处于一致状态。

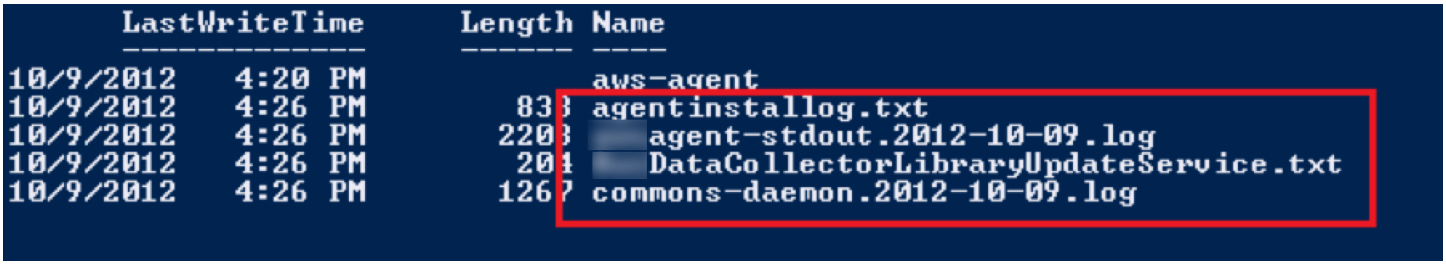
根据系统的 DataProvider 版本，按照更新到 DataProvider 4.3 或卸载旧版本中的步骤进行操作。

问题：SAP AWS 的数据提供程序在安装过程结束时无法启动。

如果重新安装适用于 SAP AWS 的数据提供程序不能解决问题，则可以通过查看`C:\Program Files \Amazon\DataProvider`目录中的日志文件来收集有关 SAP AWS 数据提供器的调试信息。

这些日志文件包括安装日志、服务安装日志以及 SAP AWS 数据提供程序本身的输出。

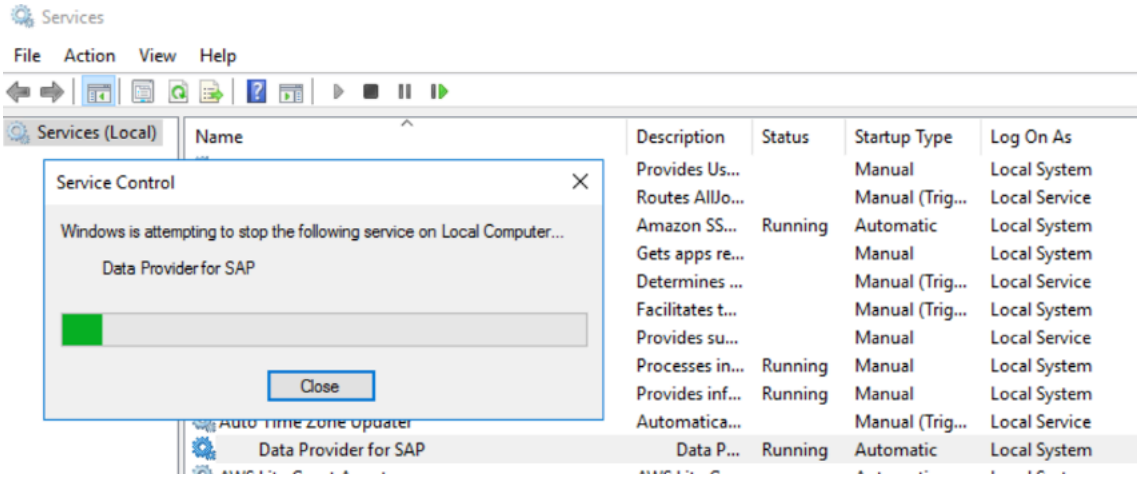
Windows 上的日志文件



问题：我想从数据提供者那里获得更详细的日志信息。

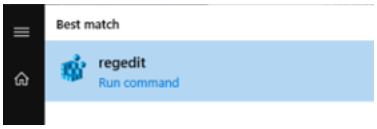
首先停止数据提供者服务。

在 Windows 上停止服务



打开注册表编辑器，方法是单击左下角的 Windows 徽标`regedit`并键入，然后单击屏幕上显示的选项：

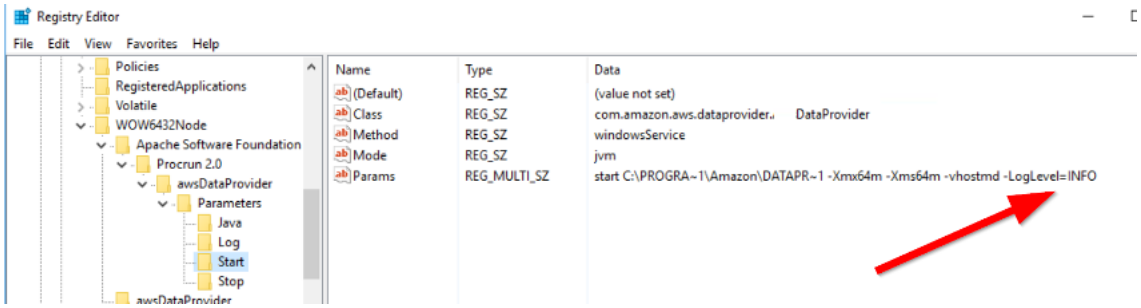
开始 **`regedit`**



在注册表中，导航到密钥：

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun
 2.0\awsDataProvider\Start
```

日志设置



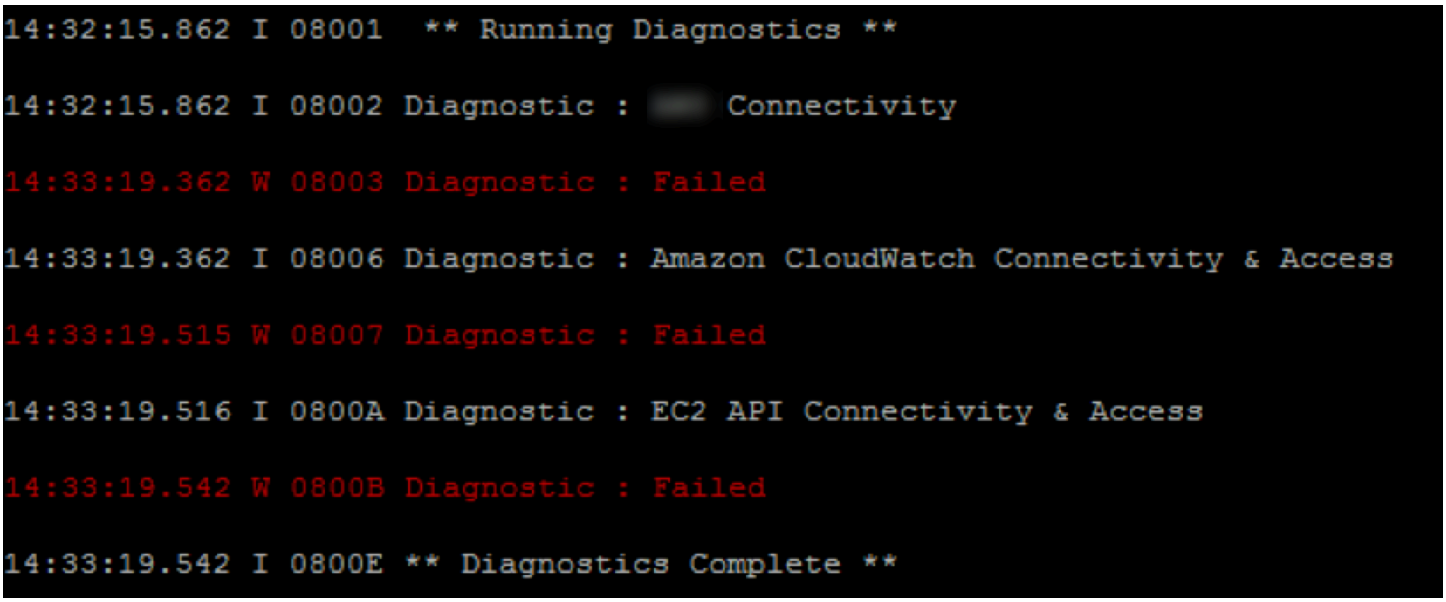
数据提供器接受两个日志级别：INFO 和 FINE。FINE 将生成更详细的日志记录，这在调试问题时非常有用。建议在完成故障排除后将其重新设置为 INFO，以避免日志占用不必要的磁盘空间。

问题：我想从头开始重新安装适用于 SAP AWS 的数据提供程序。

根据系统的 DataProvider 版本，按照更新到 DataProvider 4.3 或卸载旧版本中的步骤进行操作。

问题：当我查看日志时，我注意到我的安装未通过所有诊断。

Windows 上出现互联网连接问题的症状



如果所有诊断均失败，则表明您的互联网出站连接存在问题。你可以通过 ping 一个知名的互联网位置（例如 www.am azon.com）来确认这一点。路由问题的最常见原因是 VPC 网络配置，它需要有互联网网关或通过互联网路由与您的数据中心建立 VPN 连接。

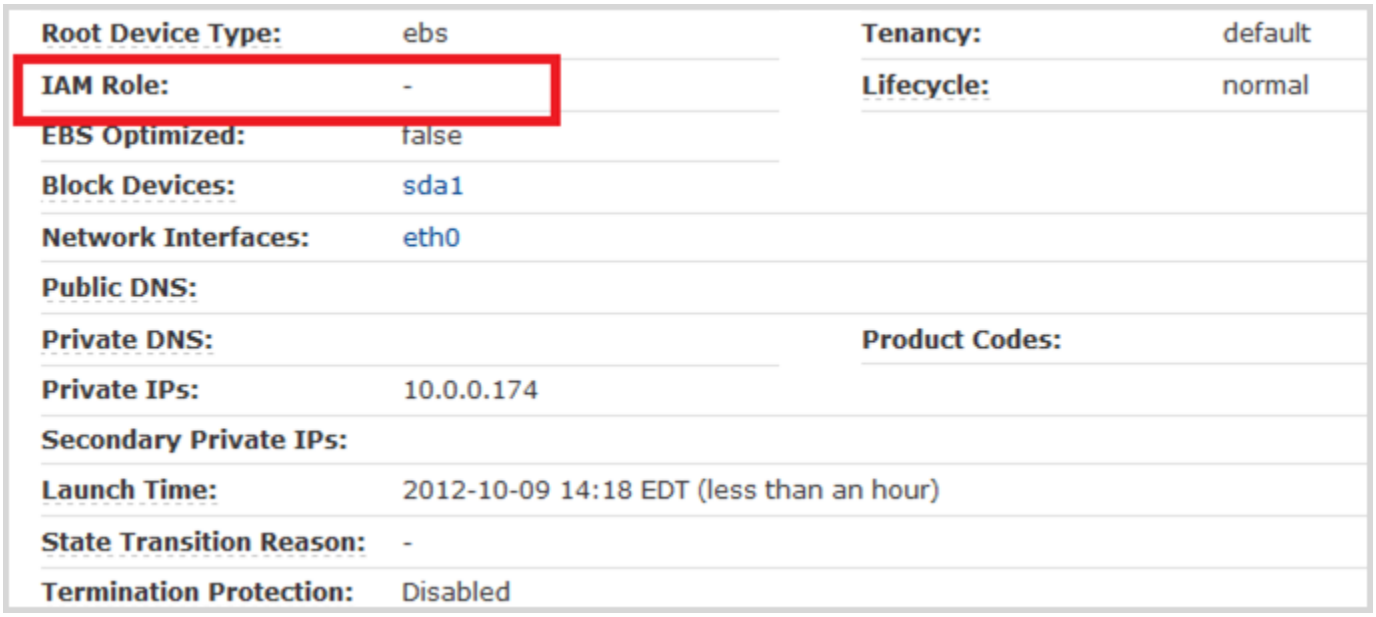
问题：当我查看日志时，我注意到我无法访问 CloudWatch 和 Amazon EC2，但我确实通过了第一次 AWS 连接诊断。

Windows 上出现授权问题的症状

```
14:38:57.467 I 08001  ** Running Diagnostics **

14:38:57.468 I 08002 Diagnostic : AWS Connectivity

14:38:58.182 I 08005 Diagnostic : Passed

14:38:58.182 I 08006 Diagnostic : Amazon CloudWatch Connectivity & Access

14:38:58.325 W 08007 Diagnostic : Failed

14:38:58.325 I 0800A Diagnostic : EC2 API Connectivity & Access

14:38:58.357 W 0800B Diagnostic : Failed

14:38:58.357 I 0800E ** Diagnostics Complete **
```

这清楚地表明您在尝试访问Amazon CloudWatch 和Amazon时遇到了授权问题 EC2。此问题的常见原因是没有与包含 IAM 策略的 IAM 策略的 IAM 角色关联的 IAM 角色，如本指南前面的 IAM 角色所述。您可以通过在 Amazon EC2 控制台中查看特定 EC2 实例并验证 IAM 角色来快速诊断此问题。

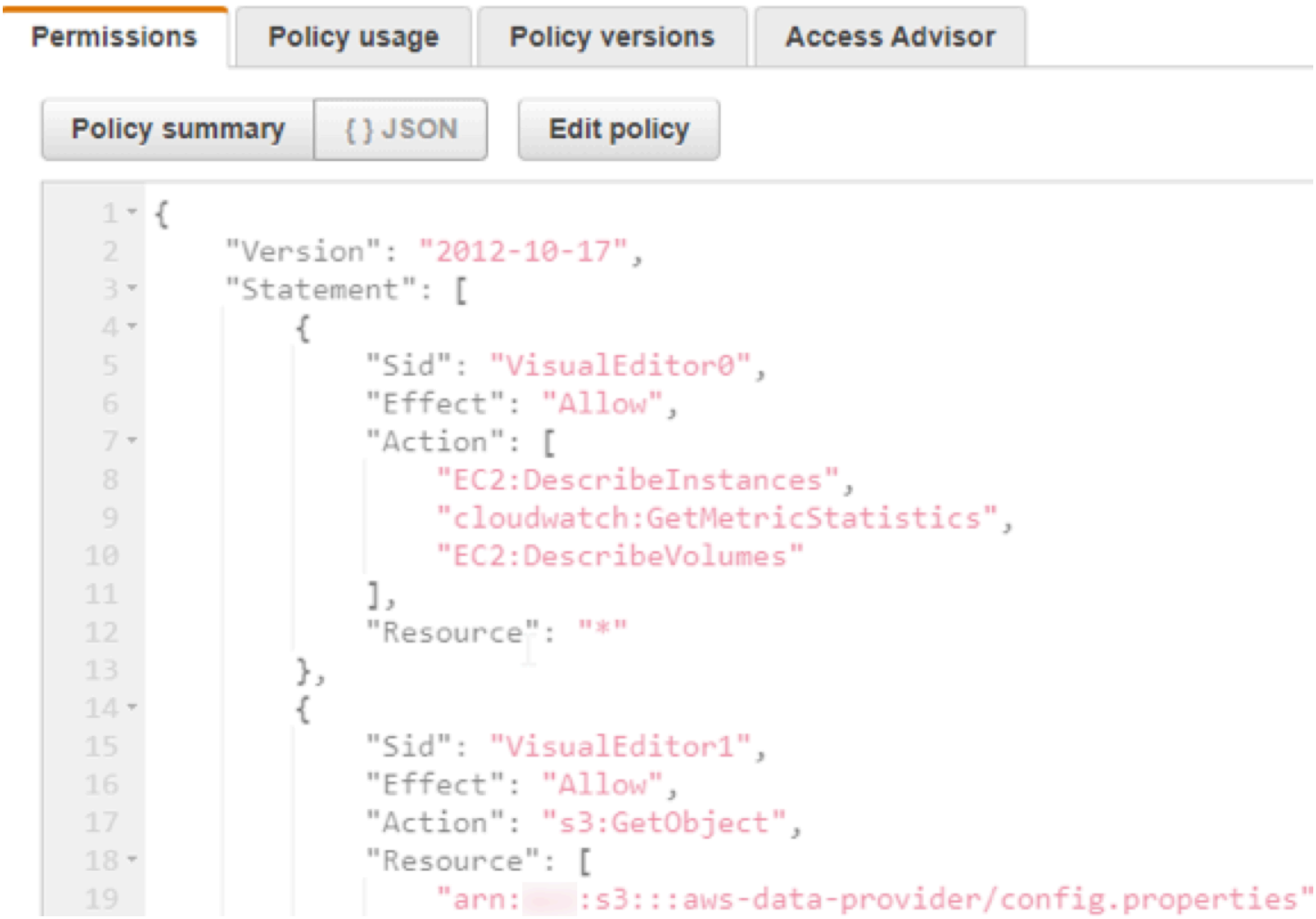
验证 EC2 实例的 IAM 角色



如果 IAM 角色不存在，则按照本指南前面介绍的 IAM 角色中的指定进行创建。

如果您确实为该实例分配了 IAM 角色，请前往 IAM 控制台，选择 IAM 角色名称，然后选择显示。确认您拥有在 IAM 角色中指定的必需策略。

验证 IAM 角色的策略



为 SAP 定制 AWS 数据提供器

有些设置在适用于 SAP AWS 的数据提供程序中进行了硬编码。您可以覆盖现有设置或添加新设置。例如，在 AWS 添加新的实例类型时，您可以将其添加到 AWS Data Provider for SAP 配置中。

适用于 SAP AWS 的数据提供器通过从可用文件中读取配置信息来创建数据库`config.properties`，顺序如下：

- 数据提供器应用程序的 JAR（Java 存档）文件。
- 安装目录。只有在要覆盖或扩展当前配置时才需要此文件。默认目录如下：
  - Linux — `/usr/local/ec2/aws-dataprovider/config.properties`
  - Windows — `C:\Program Files\Amazon\DataProvider\config.properties`
- 区域 S3 存储桶。<region>替换为该地区的地区代码（例如，`us-east-1`）。

```
https://aws-sap-dataprovider-<region>.s3.<region>.amazonaws.com/config.properties
```

配置文件的语法规则

- 配置文件需要在每行的最后一个值后面加一个逗号。
- 字符串中不会忽略空格。逗号之间的整个字符串（包括任何空格）都被接受为值。
- 如果有多行具有相同实例类型，则该类型的现有值将被覆盖。
- 字符串的大小写区分大小写。

用户可配置的 EC2 实例类型

适用于 SAP AWS 的数据提供商维护着一个包含适用于 SAP 的所有相关 Amazon EC2 实例类型的数据库。

EC2 实例类型的条目必须采用逗号分隔的列表，如下所示：

ec2type、i-type、cpu、core、threads、t-ecu、ecu、hthread、l-map、w-map、speed、p-ecu、

例如：

```
ec2type,r3.8xlarge,2,16,2,32,1,thread,eth0,lan2,10000,true,
```

以下情况适用：

字段名称	内容	示例	类型	描述
关键字	ec2type	—	字符串	用于标识带有 EC2 实例描述的记录的令牌
i-type（实例类型）	参见清单	r3.8xlarge	字符串	实例类型，必须匹配 EC2 实例元数据字符串
中央处理器 (CPUs)	1 | 2	2	整数	插槽数量

字段名称	内容	示例	类型	描述
核心（核心）	integer	16	整数	处理器内核总数
线程（每个内核的线程数）	1 | 2	2	整数	每核心线程数
t-ecu（总欧洲货币单位价值）	integer	32	双精度	具有 ECU 评级的上一代实例类型的 ECU 值；ECU 之后的实例类型的内核数
ecu（每内核 ECU）	双倍	1	双精度	1 表示所有 ECU 之后的实例类型；总计 ECU 除以具有 ECU 额定值的前一代实例类型的内核
hthread（超线程）	话题 | 核心	线程	字符串	线程用于超线程实例类型；核心用于非超线程实例类型
l-map（Linux 网卡映射）	eth0	eth0	字符串	网络接口的 Linux 映射
w-map（Windows 网卡映射）	eth0	lan2	字符串	网络接口的 Windows 映射
速度（网络接口速度）	1000 | 2000 | 10000	100000	整数	网络接口的最大速度，以 KB 为单位
p-ecu（后 ECU）	真 | 假	true	布尔值	对于没有 ECU 评级的现代实例来说是正确的

用户可配置的 EBS 卷类型

适用于 SAP AWS 的数据提供程序维护着一个包含 SAP 所有相关的 EBS 卷类型的数据库。

EBS 卷类型的条目必须采用逗号分隔的列表，如下所示：

voltype、ebs-type、采样时间、

例如：

```
voltype,io1,60,
```

以下情况适用：

字段名称	内容	示例	类型	描述
关键字	voltyp	—	字符串	用于标识带有 EBS 卷描述的记录的标记
ebs-type（EBS 型）	io1 | gp2 | sc1 | st1	io1	字符串	EBS 类型，必须与 EBS 卷元数据字符串匹配
采样时间	60 | 300	60	整数	CloudWatch 采样时间，以秒为单位

Important

根据SAP监控要求校准EBS指标需要抽样时间。采样时间的变化将导致 SAP 监控系统中的 EBS 指标不正确。

在 SAP 系统监控中验证 SAP AWS 的数据提供者

SAP AWS 的数据提供程序通过给定系统的 http://localhost:8888/vhostmd 的 XML 页面公开 AWS特定指标。

本节说明哪些指标会向 SAP 系统公开，以及如何访问这些指标以进行 SAP 系统监控。

使用 SAP 操作系统收集器 (SAPOSCOL) 检查指标

SAP AWS 数据提供程序提供的信息由 SAP 操作系统收集器 (S APOSCO L) 读取。您可以使用 SAPOSCOL 的交互模式来验证这两个工具是否可以正常协作。以下示例显示了在 Windows 下进行的查找。Linux 下的查询方式非常相似。

1. 打开 Windows 命令外壳并将外壳指向该目录`C:\Program Files\SAP\hostctrl\exe`。从`-d`选项`saposcol.exe`开始。

   启动 SAPOSCOL

   ```
   PS C:\Users\Administrator> cd 'C:\Program Files'
   PS C:\Program Files> cd .\SAP\hostctrl\exe
   PS C:\Program Files\SAP\hostctrl\exe> .\saposcol.exe -d
   ************************************************************************
   * This is Saposcol Version COLL 22.10 721 - 21.45 NT 15/02/04
   * Please use 'help' to see the usage.
   ************************************************************************
   ```

2. SAPOSCOL 现在处于交互模式。键入`dump ccm`并按 Enter 键以列出收集到的所有值。SAPOSCOL 将显示一长串指标，如下所示。

   来自 SAPOSCOL 的指标

   ```
   PS C:\Program Files\SAP\hostctrl\exe> .\saposcol.exe -d
   ************************************************************************
   * This is Saposcol Version COLL 22.10 721 - 21.45 NT 15/02/04
   * Please use 'help' to see the usage.
   ************************************************************************
   Collector > dumpc ccm
   dumpc ccm
   Name    Snap    1Min    5Min    15Min   60Min   Unit
   SysInfo_General\Manufacturer    Xen
   SysInfo_General\Model   HVM domU
   Virtualization_Configuration\Cloud Provider     Amazon Web Services
   Virtualization_Configuration\Cloud Instance Type        c4.4xlarge
   Virtualization_Configuration\Data Provider Version      1.3.1   1.3.1
   Virtualization_Configuration\Enhanced Monitoring Access TRUE
   Virtualization_Configuration\Enhanced Monitoring Details        ACTIVE
   Virtualization_Configuration\Virtual Machine ID i-f485da0b
   Virtualization_Configuration\Solution   Xen
   Virtualization_Configuration\Solution Version   ba185a32        ba185a32
   Virtualization_Configuration\Last Hardware Change       Wed Jun 10 15:07:43 2015        Wed Jun 10 15:07:43 2015
   ```

   以下两个指标表明 SAPOSCOL 正在与 SAP AWS 数据提供商成功合作：

   - 增强型监控访问权限 TRUE
   - 增强监控详情已激活

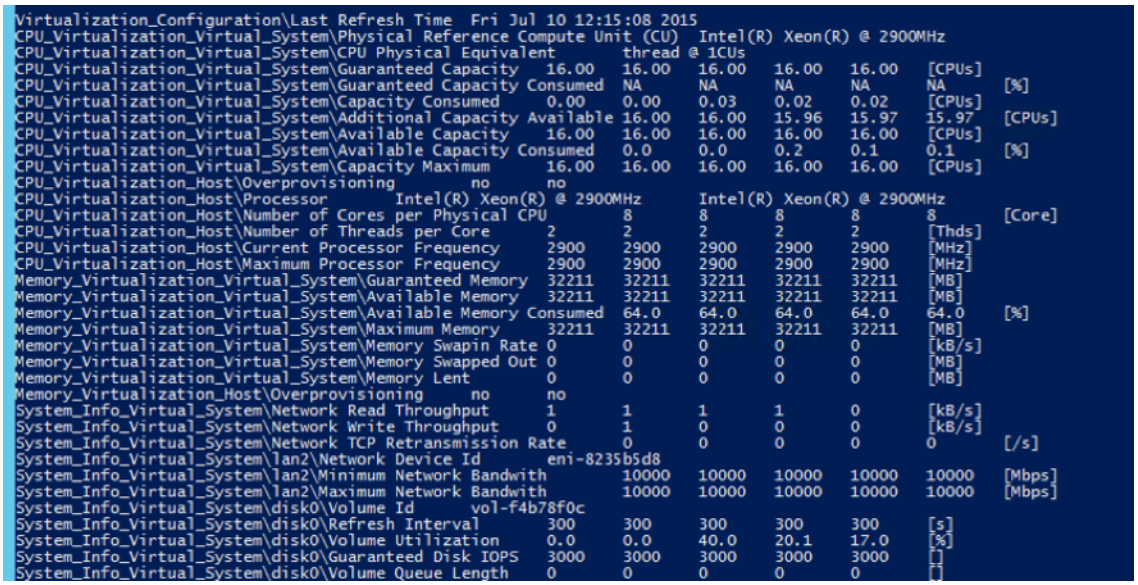
   AWS特定指标以以下字符串开头：

   +

   - 虚拟化_配置
   - CPU_虚拟化_虚拟化_系统
   - 内存_虚拟化_虚拟化_虚拟系统

- 系统信息_虚拟化_系统

AWS特定指标



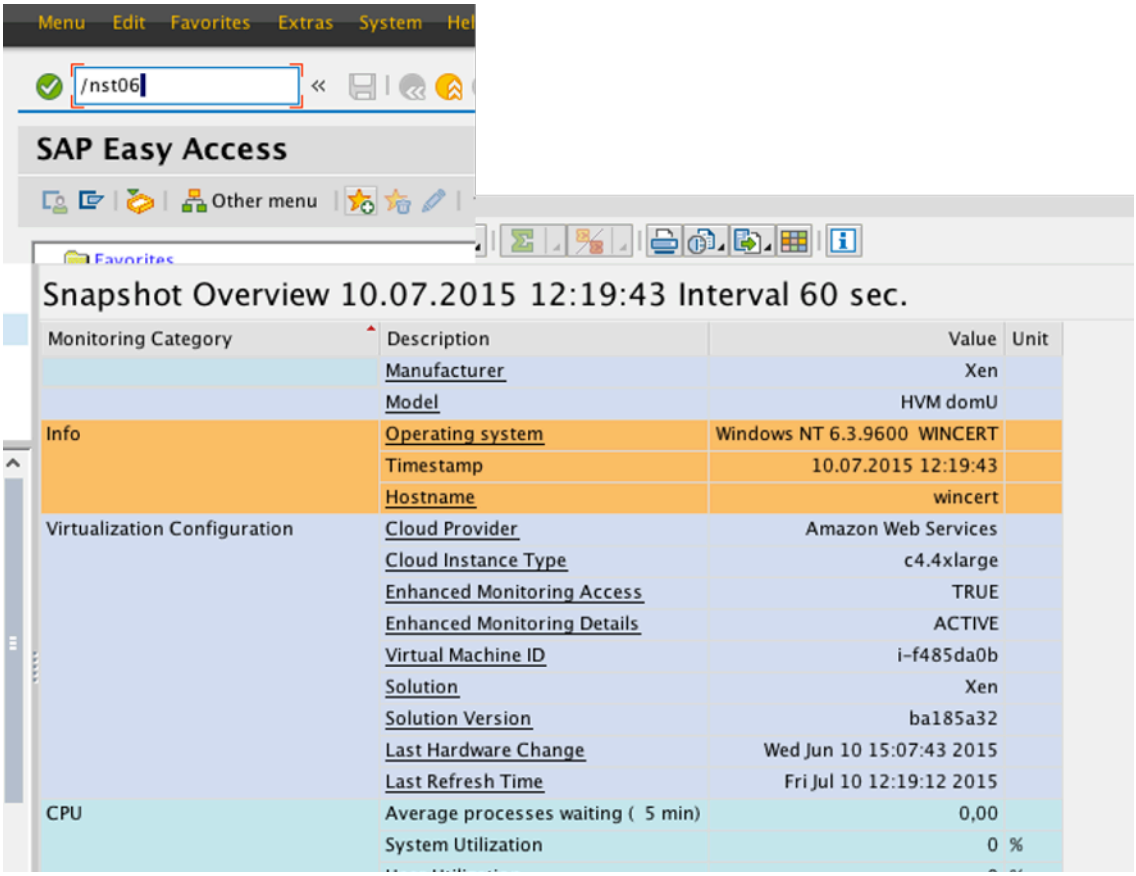
```
Virtualization_Configuration\Last Refresh Time  Fri Jul 10 12:15:08 2015
CPU_Virtualization_Virtual_System\Physical Reference Compute Unit (CU)  Intel(R) Xeon(R) @ 2900MHz
CPU_Virtualization_Virtual_System\CPU Physical Equivalent       thread @ 1CUs
CPU_Virtualization_Virtual_System\Guaranteed Capacity   16.00   16.00   16.00   16.00   16.00   [CPUs]
CPU_Virtualization_Virtual_System\Guaranteed Capacity Consumed  NA      NA      NA      NA      NA      [%]
CPU_Virtualization_Virtual_System\Capacity Consumed     0.00    0.00    0.03    0.02    0.02    [CPUs]
CPU_Virtualization_Virtual_System\Additional Capacity Available 16.00   16.00   15.96   15.97   15.97   [CPUs]
CPU_Virtualization_Virtual_System\Available Capacity    16.00   16.00   16.00   16.00   16.00   [CPUs]
CPU_Virtualization_Virtual_System\Available Capacity Consumed   0.0     0.0     0.2     0.1     0.1     [%]
CPU_Virtualization_Virtual_System\Capacity Maximum      16.00   16.00   16.00   16.00   16.00   [CPUs]
CPU_Virtualization_Host\Overprovisioning        no      no
CPU_Virtualization_Host\Processor       Intel(R) Xeon(R) @ 2900MHz      Intel(R) Xeon(R) @ 2900MHz
CPU_Virtualization_Host\Number of Cores per Physical CPU        8       8       8       8       8       [Core]
CPU_Virtualization_Host\Number of Threads per Core      2       2       2       2       2       [Thds]
CPU_Virtualization_Host\Current Processor Frequency     2900    2900    2900    2900    2900    [MHz]
CPU_Virtualization_Host\Maximum Processor Frequency     2900    2900    2900    2900    2900    [MHz]
Memory_Virtualization_Virtual_System\Guaranteed Memory  32211   32211   32211   32211   32211   [MB]
Memory_Virtualization_Virtual_System\Available Memory   32211   32211   32211   32211   32211   [MB]
Memory_Virtualization_Virtual_System\Available Memory Consumed  64.0    64.0    64.0    64.0    64.0    [%]
Memory_Virtualization_Virtual_System\Maximum Memory     32211   32211   32211   32211   32211   [MB]
Memory_Virtualization_Virtual_System\Memory Swapin Rate 0       0       0       0       0       [kB/s]
Memory_Virtualization_Virtual_System\Memory Swapped Out 0       0       0       0       0       [MB]
Memory_Virtualization_Virtual_System\Memory Lent        0       0       0       0       0       [MB]
Memory_Virtualization_Host\Overprovisioning     no      no
System_Info_Virtual_System\Network Read Throughput      1       1       1       1       0       [kB/s]
System_Info_Virtual_System\Network Write Throughput     0       1       0       0       0       [kB/s]
System_Info_Virtual_System\Network TCP Retransmission Rate      0       0       0       0       0       [/s]
System_Info_Virtual_System\lan2\Network Device Id       eni-8235b5d8
System_Info_Virtual_System\lan2\Minimum Network Bandwith        10000   10000   10000   10000   10000   [Mbps]
System_Info_Virtual_System\lan2\Maximum Network Bandwith        10000   10000   10000   10000   10000   [Mbps]
System_Info_Virtual_System\disk0\Volume Id      vol-f4b78f0c
System_Info_Virtual_System\disk0\Refresh Interval       300     300     300     300     300     [s]
System_Info_Virtual_System\disk0\Volume Utilization     0.0     0.0     40.0    20.1    17.0    [%]
System_Info_Virtual_System\disk0\Guaranteed Disk IOPS   3000    3000    3000    3000    3000    []
System_Info_Virtual_System\disk0\Volume Queue Length    0       0       0       0       0       []
```

使用 SAP CCMS 交易检查指标

SAPOSCOL 将 AWS增强型统计数据以及其他特定于操作系统的指标交给 SAP 系统。您还可以在 SAP CCMS 中查看 AWS增强型统计信息。您可以在 SAP GUI 的左上角事务字段中输入事务 st06（或 /nst06），以便快速访问这些数据。

> **Note**
>
> 您需要获得相应的授权才能查询此信息。

SAP CCMS 中的统计数据（标准视图）



在此屏幕上，您可以验证核心 AWS 信息，例如：

- 云提供商
- 实例类型
- 增强监控访问的状态（必须为 TRUE）
- 增强监控详细信息的状态（必须处于活动状态）
- 虚拟机标识符

> **Important**
>
> 增强的 AWS 指标不显示在标准视图中。

要查看增强的 AWS 统计数据，请选择左上角的标准视图按钮。它变为专家视图并显示增强的 AWS 统计数据。出现的列表很全面。它显示了处理器的详细信息。

增强的 AWS 统计数据（专家视图）

CPU Virtualization Host	Overprovisioning	no	
	Processor	Intel(R) Xeon(R) @ 2900MHz	
	Number of Cores per Physical CPU	8	Core
	Number of Threads per Core	2	Thds
	Current Processor Frequency	2.900	MHz
	Maximum Processor Frequency	2.900	MHz
CPU Virtualization Virtual System	Physical Reference Compute Unit (CU)	Intel(R) Xeon(R) @ 2900MHz	
	CPU Physical Equivalent	thread @ 1CUs	
	Guaranteed Capacity	16,00	CPUs
	Capacity Consumed	0,00	CPUs
	Additional Capacity Available	16,00	CPUs
	Available Capacity	16,00	CPUs
	Available Capacity Consumed	0,0	%
	Capacity Maximum	16,00	CPUs

它还显示有关内存子系统（主内存和磁盘）和网络接口的详细信息。

内存和网络统计信息（专家视图）

Memory Virtualization Host	Overprovisioning	no	
	Network Read Throughput	5	kB/s
	Network Write Throughput	4	kB/s
	Network TCP Retransmission Rate	0	/s
	lan2\Network Device Id	eni-8235b5d8	
	lan2\Minimum Network Bandwith	10.000	Mb...
	lan2\Maximum Network Bandwith	10.000	Mb...
	disk0\Volume Id	vol-f4b78f0c	
	disk0\Refresh Interval	300	s
	disk0\Volume Utilization	0,0	%
	disk0\Guaranteed Disk IOPS	3.000	
	disk0\Volume Queue Length	0	
	disk0\Volume Read Response Time	0	msec
	disk0\Volume Write Response Time	0	msec
	disk0\Volume Read Throughput	1	kB/s
	disk0\Volume Write Throughput	15	kB/s
	disk0\Volume Read Ops	0	/s
	disk0\Volume Write Ops	2	/s
	disk1\Volume Id	vol-89676771	
	disk1\Refresh Interval	300	s
	disk1\Volume Utilization	0,0	%
	disk1\Guaranteed Disk IOPS	300	
	disk1\Volume Queue Length	0	
	disk1\Volume Read Response Time	0	msec
	disk1\Volume Write Response Time	0	msec
	disk1\Volume Read Throughput	0	kB/s
	disk1\Volume Write Throughput	0	kB/s
	disk1\Volume Read Ops	0	/s
	disk1\Volume Write Ops	0	/s

> **Note**
>
> 图 37—39 中的屏幕插图取自 SAP NetWeaver 7.4 SP08。此版本在 “内存虚拟化” 部分显示了增强的 AWS 统计信息。SAP 已在更高版本中修复了此问题 NetWeaver。

捕获的指标示例

以下显示了示例指标。您的系统指标可能略有不同。

```
<metrics>
<metric context="host" category="config" type="long" unit="posixtime">
<name>Time Stamp</name>
<value>1584376572</value>
</metric>
<metric context="host" category="config" type="int64" unit="sec">
<name>Refresh Interval</name>
<value>60</value>
</metric>
<metric context="vm" category="config" type="string" unit="none">
<name>Data Provider Version</name>
<value>3.0.139</value>
</metric>
<metric context="host" category="config" type="string" unit="none">
<name>Cloud Provider</name>
<value>Amazon Web Services</value>
</metric>
<metric context="vm" category="config" type="string" unit="none">
<name>Instance Type</name>
<value>m5.large</value>
</metric>
<metric context="host" category="config" type="string" unit="none">
<name>Virtualization Solution</name>
<value>KVM</value>
</metric>
<metric context="host" category="config" type="string" unit="none">
<name>Virtualization Solution Version</name>
<value>ba185a32</value>
</metric>
<metric context="host" category="config" type="long" unit="none">
<name>CloudWatch Calls</name>
<value>12</value>
```

```
</metric>
<metric context="host" category="config" type="long" unit="none">
<name>EC2 Calls</name>
<value>4</value>
</metric>
<metric context="vm" category="config" type="string" unit="none">
<name>CPU Over-Provisioning</name>
<value>no</value>
</metric>
<metric context="vm" category="config" type="string" unit="none">
<name>Memory Over-Provisioning</name>
<value>no</value>
</metric>
<metric context="vm" category="config" type="string" unit="none">
<name>Virtualization Type</name>
<value>default-hvm</value>
</metric>
<metric context="vm" category="config" type="string" unit="none">
<name>Virtual Machine ID</name>
<value>i-##################</value>
</metric>
<metric context="vm" category="config" type="long" unit="posixtime">
<name>Last Hardware Change</name>
<value>1572284007</value>
</metric>
<metric context="host" category="cpu" type="string" unit="none">
<name>Processor Type</name>
<value>Intel(R) Xeon(R) @ 2500MHz</value>
</metric>
<metric context="host" category="cpu" type="int64" unit="none">
<name>Number of Cores per CPU</name>
<value>1</value>
</metric>
<metric context="host" category="cpu" type="int64" unit="none">
<name>Number of Threads per Core</name>
<value>2</value>
</metric>
<metric context="host" category="cpu" type="int64" unit="MHz">
<name>Max HW Frequency</name>
<value>2500</value>
</metric>
<metric context="host" category="cpu" type="int64" unit="MHz">
<name>Current HW Frequency</name>
<value>2500</value>
```

```
</metric>
<metric context="vm" category="cpu" type="string" unit="none">
<name>Reference Compute Unit (CU)</name>
<value>Intel(R) Xeon(R) @ 2500MHz</value>
</metric>
<metric context="vm" category="cpu" type="string" unit="none">
<name>vCPU Mapping</name>
<value>thread</value>
</metric>
<metric context="vm" category="cpu" type="long" unit="cu">
<name>Phys. Processing Power per vCPU</name>
<value>1</value>
</metric>
<metric context="vm" category="cpu" type="int64" unit="cu">
<name>Guaranteed VM Processing Power</name>
<value>2</value>
</metric>
<metric context="vm" category="cpu" type="int64" unit="cu">
<name>Current VM Processing Power</name>
<value>2</value>
</metric>
<metric context="vm" category="cpu" type="int64" unit="cu">
<name>Max. VM Processing Power</name>
<value>2</value>
</metric>
<metric context="vm" category="cpu" type="double" unit="percent">
<name>VM Processing Power Consumption</name>
<value>3.00</value>
</metric>
<metric context="vm" category="memory" type="long" unit="MB">
<name>Guaranteed Memory assigned</name>
<value>8274</value>
</metric>
<metric context="vm" category="memory" type="long" unit="MB">
<name>Current Memory assigned</name>
<value>8274</value>
</metric>
<metric context="vm" category="memory" type="long" unit="MB">
<name>Max Memory assigned</name>
<value>8274</value>
</metric>
<metric context="vm" category="memory" type="double" unit="percent">
<name>VM Memory Consumption</name>
<value>29.00</value>
```

```
</metric>
<metric context="vm" category="memory" type="int64" unit="KB/sec">
<name>Memory SwapIn Rate</name>
<value>0</value>
</metric>
<metric context="vm" category="memory" type="int64" unit="MB">
<name>Memory Swapped Out</name>
<value>0</value>
</metric>
<metric context="vm" category="memory" type="int64" unit="MB">
<name>Memory Lent</name>
<value>0</value>
</metric>
<metric context="vm" category="memory" type="int64" unit="MB">
<name>Total Visible Memory</name>
<value>-1</value>
</metric>
<metric context="vm" category="memory" type="int64" unit="percent">
<name>Visible Memory Consumed</name>
<value>-1</value>
</metric>
<metric context="vm" category="memory" type="int64" unit="KB/sec">
<name>Visible Memory SwapIn Rate</name>
<value>0</value>
</metric>
<metric context="vm" category="memory" type="int64" unit="MB">
<name>Visible Memory Swapped Out</name>
<value>0</value>
</metric>
<metric context="vm" category="network" type="int64" unit="bytes">
<name>Network Read Bytes</name>
<value>54110386</value>
</metric>
<metric context="vm" category="network" type="int64" unit="bytes">
<name>Network Write Bytes</name>
<value>1330726</value>
</metric>
<metric context="vm" category="network" type="int64" unit="none">
<name>TCP Packets Retransmitted</name>
<value>396480</value>
</metric>
<metric context="vm" category="network" type="int64" unit="Mbps" device-id="eni--
##################</">
<name>Minimum Network Bandwidth</name>
```

```
<value>10000</value>
</metric>
<metric context="vm" category="network" type="int64" unit="Mbps" device-id="eni--
##################</">
<name>Maximum Network Bandwidth</name>
<value>10000</value>
</metric>
<metric context="vm" category="network" type="string" unit="none" device-id="eni--
##################</">
<name>Mapping</name>
<value>lan2</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="msec" device-id="vol--
##################</">
<name>Volume Idle Time</name>
<value>58489</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="none" device-id="vol--
##################</">
<name>Volume Queue Length</name>
<value>0</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="bytes" device-id="vol--
##################</">
<name>Volume Read Bytes</name>
<value>9878528</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="none" device-id="vol--
##################</">
<name>Volume Read Ops</name>
<value>144</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="msec" device-id="vol--
##################</">
<name>Volume Read Time</name>
<value>246</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="msec" device-id="vol--
##################</">
<name>Volume Write Time</name>
<value>8266</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="bytes" device-id="vol--
##################</">
```

```
<name>Volume Write Bytes</name>
<value>282332160</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="none" device-id="vol--
##################</">
<name>Volume Write Ops</name>
<value>3090</value>
</metric>
<metric context="vm" category="disk" type="string" unit="none" device-id="vol--
##################</">
<name>Volume Type</name>
<value>gp2</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="none" device-id="vol--
##################</">
<name>Guaranteed IOps</name>
<value>180</value>
</metric>
<metric context="vm" category="disk" type="int64" unit="sec" device-id="vol--
##################</">
<name>Interval</name>
<value>300</value>
</metric>
<metric context="vm" category="disk" type="string" unit="none" device-id="vol--
##################</">
<name>Mapping</name>
<value>disk0</value>
</metric>
</metrics>
```

版本历史记录

版本 4.3.2 (2023 年 8 月)

- 错误修复：针对解决 CVE-2022-45688 的安全更新。

版本 4.3.1（2023 年 6 月）

- 错误修复：数据提供器现已设置为成功安装 SAP JVM。

版本 4.3（2023 年 1 月）

- 增加了对 JDK 17 的支持
- 添加了从远程 Amazon S3 存储桶读取配置信息的新增功能

版本 4.2（2022 年 11 月）

- 增加了对甲骨文和 Linux 的支持
- 增加了与 Linux `logrotate` 功能的集成
- RPM 软件包版本的更新。

版本 4.1.1 (2022 年 9 月)

- 增加了对新 Amazon EC2 实例类型的支持。

版本 4.1.0 (2022 年 1 月)

- 增加了对 JDK 11 的支持。
- 增加了对新 Amazon EC2 实例类型的支持。

版本 4.0.3（2021 年 12 月）

- 错误修复：移除了 Log4j 依赖关系。

版本 4.0.2（2021 年 12 月）

- 错误修复：Log4j2 问题的安全更新 (CVE-2021-44228)。

版本 4.0（2021 年 4 月）

- 4.0 版本的初始版本。
- Support 支持 SSM 软件包安装。
- Support fo IMDSv2 r.

版本 3.0（2020 年 4 月）

- 3.0 版本的初始版本。

- 将 Java 运行时从 Oracle 切换到了 Amazon Corretto。

版本 2.9（2017 年 8 月 30 日）

- 增加了对中国区域的支持。
- 添加了 Linux 卸载程序。
- 可以自定义 Linux 安装程序，使其从自定义 S3 存储桶进行安装。
- 适用于 Windows 的静默安装程序（不需要任何输入）。
- 改进了接入点的确定。
- 对 X1E 实例系列的支持。

版本 2.8（2017 年 3 月 1 日）

- SLES 12、Red Hat 7 和 Oracle Linux 7 现在将使用 SYSTEMD 来管理守护程序。
- 对适用于 SAP 的 SLES 和 SLES 的支持 12. SP2
- 尝试安装 AWS 数据提供程序时，SLES 12 SP1 系统将从 Linux 服务迁移到 SYSTEMD，而无需先将其卸载。
- 日志文本有细微变化。
- 支持 R4 和 M4 实例类型。
- 更新了 Windows 安装验证。

版本 2.7（2016 年 12 月 21 日）

- Support 支持加拿大（中部）、美国东部（俄亥俄州）和欧洲（伦敦）区域。
- 添加了常见 AWS 区域的默认接入点分辨率。

版本 2.6（2016 年 9 月 1 日）

- 错误修复：安装脚本会检查 wget 是否存在
- 支持 Oracle Linux。

版本 2.5（2016 年 5 月 2 日）

- 错误修复：2.2-2.4 版本中的安全性和稳定性修复。

- 新增：支持新的 Amazon EBS 卷类型：
  - 吞吐量优化的硬盘 (st1)
  - 冷硬盘 (sc1)
- 新增：对 Amazon EC2 X1 实例系列的支持。

版本 2.1（2016 年 1 月 20 日）

- Support 支持亚太地区（首尔）区域。
- 错误修复：版本 2.0 从错误的 S3 存储桶中提取文件进行安装。在安装 2.1 版本之前，需要先卸载 2.0 版。

版本 2.0（2015 年 12 月 22 日）

- 新增：sdb 到 sdzz 范围内的 Windows 设备已正确分配了 SCSI 设备。 IDs
- 新增：Java 虚拟机的使用量现在限制为最大堆大小 64 MB。

版本 1.3.1（2015 年 7 月 14 日）

- 错误修复：安全修复。
- 新增：支持 C4、D2 和 M4 实例类型。使用已安装 1.3 代理迁移实例的用户将通过 Web 上更新的配置数据库自动获得对新实例类型的支持。

版本 1.3（2015 年 2 月 17 日）

- 新增：支持新的 Amazon EC2 C4 实例系列。
- 安全补丁：将 Linux 和 Windows 版本升级到 JRE 8u31。
- 错误修复：现在可以正确报告 c3.8xlarge 实例的相对性能。
- 新增： CloudWatch 和 Amazon EC2 指标接入点：
  - 增加了对欧洲（法兰克福）区域的支持。
  - 接入点可由用户配置。您无需安装新产品版本即可添加有关新 AWS 区域的信息。
  - 接入点现在可以从基于互联网的数据库文件进行更新。您可以通过更新基于 Web 的配置文件然后重新启动守护程序/服务来添加新 AWS 区域。
- 新增：Linux 上提供了占用固定磁盘空间的消息日志文件。
- 新增：用户可配置的 EC2 实例类型可用。

- 新增：增加了对未来 EC2 实例类型的 Web 更新支持，无需产品更新。
- 错误修复： GP2 体积现在可以报告正确的采样间隔时间。
- 新增：用户可配置的新 EBS 体积类型的采样时间现已推出。
- 新增：SAP AWS 的数据提供程序现在会报告 EC2 实例的虚拟化类型。

版本 1.2.2（2014 年 10 月 1 日）

- Windows 错误修复：安装程序可执行文件从正确的 Amazon S3 存储桶中提取安装内容。
- Windows 错误修复：适用于 SAP AWS 的数据提供程序现在使用以下名称报告 Windows EBS 卷的正确磁盘映射：xvd [a-z] [a-z] [a-z]。

版本 1.2.1（2014 年 9 月 29 日）

- 错误修复：EBS 卷现在报告卷类型的正确属性类型（“字符串”）。

版本 1.2（2014 年 9 月 16 日）

- 新增：对 T2、R3 和 C3 实例系列的支持。
- 新增：对后 ECU（EC2 计算单元）实例类型的 Support：
  - 新的实例类型不再具有 ECU 值。
  - 这些实例类型的参考计算能力是给定处理器的硬件线程。CPU 的总功耗等于给定实例类型的 v CPUs 数。
- 新增：支持新的 EBS GP2 卷类型。
  - 现在，每个卷都标有 EBS 卷类型。
- 新增：EBS 一分钟交易量统计报告。
  - 现在，EBS 体积在单独的属性中报告其各自的采样间隔。
- 错误修复：Windows 设备的 EBS 卷映射现在会报告正确的名称。
- 错误修复：已修复通过 HTTP/HTTPS 代理进行安装、更新和操作。
- 新增：已在 Linux 上添加了 JRE 8 支持。

SAP 谈 AWS 成本估算

最后更新时间：2023 年 5 月

AWS 提供 pay-as-you-go定价。您只需为所使用的服务付费，只要您使用这些服务即可。没有长期合同或复杂的许可要求。欲了解更多信息，请参阅AWS 定价和 https://calculator.aws/#/。

以下概述了经常用于在上部署和运行 SAP 系统的 AWS 服务的定价特征 AWS。

主题

- AWS 区域
- 计算
- 存储
- 网络
- 自动化
- Backup、还原和恢复
- 迁移
- 监控
- 操作系统许可证
- AWS Marketp
- AWS Support

AWS 区域

AWS 服务定价因 AWS 地区而异。您必须选择要在其中部署 SAP 系统的区域才能开始创建估算。有关更多信息，请参阅区域和可用区。

计算

Amazon Elastic Compute Cloud (Amazon EC2) 提供多种实例类型，可提供 CPU、内存、存储、I/O 和联网功能的不同组合。每个正在运行的实例按小时收费。有关更多信息，请参阅 Amazon EC2 定价。

Amazon EC2 提供多种购买选项，让您可以灵活地优化成本。有关更多信息，请参阅实例购买选项。

存储

以下 AWS 服务是灵活、经济实惠且适用于您的 SAP 系统的 easy-to-use数据存储选项。各选项都具有独特的性能和耐久性。有关更多信息，请参阅上的 “云存储” AWS。

主题

- Amazon EBS
- Amazon EFS
- FSx 适用于 Windows 文件服务器的亚马逊
- FSx 适用于 NetApp ONTAP 的亚马逊
- Amazon S3

Amazon EBS

Amazon Elastic Block Store (Amazon EBS) 为亚马逊实例提供永久的块级存储卷。 EC2 每个运行 SAP 环境的 Amazon EC2 实例都需要一个或多个 Amazon EBS 卷来存储系统组件，例如操作系统、SAP 软件、SAP 数据库数据和日志文件以及本地备份存储。

使用 Amazon Elastic Block Store，您只需为自己配置的内容付费。有关更多信息，请参阅 Amazon EBS 定价。

Amazon EBS 快照

Amazon EBS 快照是存储在亚马逊 EBS 卷中的区块数据的 point-in-time副本。标准层中的 Amazon EBS 快照以增量方式存储，这意味着您只需为存储的更改区块付费。存档层中的 Amazon EBS 快照是您的区块数据的完整副本，这意味着您需要为存储的所有区块付费，而不仅仅是更改的区块。

您也可以启用回收站功能以防止意外删除。回收站中的 Amazon EBS 快照按相同的费率计费。

适用于 SAP 工作负载的 Amazon EBS 快照的另一个功能是快速快照恢复 (FSR)。此功能使您能够从快照中快速恢复完全配置的 Amazon EBS 卷，无论卷或快照的大小如何。FSR 按每个快照和启用该快照的每个可用区按数据服务单位小时数 (DSU 小时数) 收费。 DSUs 表示按分钟计费，最少为一小时。

Amazon EBS 快照既可以用于 SAP 系统的根卷和二进制卷，也可以用于数据库卷。

Amazon EFS

亚马逊 Elastic File System（亚马逊 EFS）提供无服务器文件存储。您无需配置或管理存储容量和性能即可共享文件数据。Amazon EFS 可在不中断应用程序的情况下按需扩展到 PB 级，并可在您添加和移除文件时自动扩涨或收缩。您可以快速轻松地创建和配置文件系统。

Amazon EFS 将每个对象存储在多个可用区中，使其具有很高的可用性。它支持网络文件系统版本 4（NFSv4.1 和 NFSv4 .0）协议。它已通过 SAP 文件共享认证，还可用于在 SAP 环境中存储数据文件。

使用 Amazon EFS，您只需为文件系统使用的存储空间付费，并且没有最低费用或安装成本。有关更多信息，请参阅 Amazon S3 定价。

FSx 适用于 Windows 文件服务器的亚马逊

亚马逊 FSx 版 Windows 文件服务器提供完全托管的微软 Windows 文件服务器，由完全原生 Windows 文件系统提供支持。它支持 Windows 文件系统功能和通过网络访问文件存储的行业标准服务器消息块 (SMB) 协议。

FSx 适用于 Windows File Server 已通过认证 AWS，可在 SAP 环境中使用 SAP 工作负载，也可以用于基于 Windows 的数据文件共享。

对 FSx 于 Windows File Server，您只需为使用的资源付费，并且没有最低费用或安装成本。有关更多信息，请参阅亚马逊 Window FSx s 文件服务器版定价。

FSx 适用于 NetApp ONTAP 的亚马逊

Amazon FSx f NetApp or ONTAP 是一项完全托管的服务，它基于广受欢迎的 ONTAP 文件系统提供高度可靠、可扩展、高性能和功能丰富的文件存储。 NetApp

FSx 适用于 ONTAP 已通过 SAP 工作负载认证。 AWS

您需要根据以下类别为您使用的文件系统付费。

- 固态硬盘存储容量（GB/月）
- 您预置的 SSD IOPS 超过 3IOPS/GB（IOPS/月）
- 吞吐容量（每兆字节每秒 [MBps]-月）
- 容量池存储消耗量（GB/月）

- 容量池请求（每次读取和写入）
- 备份存储消耗（GB/月）

有关更多信息，请参阅 Amazon f FSx or NetApp ONTAP 定价。

Amazon S3

Amazon Simple Storage Service (Amazon S3) 是一项对象存储服务，可提供业界领先的可扩展性、数据可用性、安全性和性能。您可以使用 Amazon S3 来暂存媒体、存储备份和存档数据。Amazon S3 提供一系列适合不同使用案例的存储类。

Amazon S3 仅按照您的实际使用容量收费，没有任何隐性收费和超容量收费。这种模式为您提供了一种可变成本的服务，该服务可以随着您的业务而增长，同时为您提供基础架构的成本优势。 AWS 有关更多信息，请参阅 Amazon S3 定价。

网络

AWS 提供多种强大而安全的网络服务。

主题

- Amazon VPC
- AWS Site-to-Site VPN
- AWS 直接连接
- Elastic Load Balancing
- 数据传输定价

Amazon VPC

借助 Amazon Virtual Private Cloud（亚马逊 VPC），您可以在您定义的逻辑隔离的虚拟网络中启动 AWS 资源。该虚拟网络与您在自己的数据中心中运行的传统网络非常相似，其优点是使用的可扩展基础架构。 AWS

使用 Amazon VPC 无需支付额外费用。某些组件需要付费，例如 NAT 网关、IP 地址管理器、流量镜像、Reachability Analyzer 和网络访问分析器。有关更多信息，请参阅 Amazon VPC pricing。

使用以下选项在您的本地网络和 Amazon VPC 之间建立安全连接。

- AWS T@@ ransit Gateway 是一个网络传输中心，可用于互连虚拟私有云 (VPCs) 和本地网络。随着您的云基础设施在全球扩展，区域间对等互连使用 AWS 全球基础设施将中转网关连接在一起。您的数据会自动加密，永远不会在公共互联网上传输。

  您需要按小时为中转网关上的每个挂载付费，并且需要为在中转网关上处理的流量付费。有关更多信息，请参阅 AWS Transit Gateway 定价。
- NAT 网关是一项网络地址转换 (NAT) 服务。您可以使用 NAT 网关，以便私有子网中的实例可以连接到 VPC 外部的服务，但外部服务无法启动与这些实例的连接。

  当您预置 NAT 网关时，NAT 网关可用的每个小时及其处理的每个 GB 数据都需支付费用。有关更多信息，请参阅 Amazon VPC pricing。
- AWS PrivateLink 是一项高度可用的可扩展技术，可用于将 VPC 私密地连接到服务，如同这些服务就在您自己的 VPC 中一样。您无需使用互联网网关、NAT 设备、公有 IP 地址、 AWS Direct Connect 连接或 AWS Site-to-Site VPN 连接即可允许从您的私有子网与服务进行通信。因此，您可以控制可从 VPC 访问的特定 API 端点、站点和服务。

  有关 VPC 终端节点定价的信息，请参阅AWS PrivateLink 定价。

AWS Site-to-Site VPN

默认情况下，您在 Amazon VPC 中启动的实例无法与您自己的（远程）网络通信。您可以创建 VP AWS Site-to-Site N (VP Site-to-Site N) 连接并配置路由以通过该连接传递流量，从而允许从 VPC 访问您的远程网络。

您需要为预置并且可用的 VPN 连接按 VPN 连接小时数付费。有关更多信息，请参阅 AWS Site-to-Site VPN 和加速 Site-to-Site VPN 连接定价。

您需要支付从 Amazon EC2 向互联网传输数据的费用。有关更多信息，请参阅数据传输。

当您创建加速 VPN 连接时，我们将代表您创建和管理两个加速器。您需要按小时为每个加速器付费，并支付数据传输费。有关更多信息，请参阅AWS 全球加速器定价。

AWS 直接连接

AWS Direct Connect 通过标准的以太网光纤电缆将您的内部网络连接到 AWS Direct Connect 位置。电缆的一端连接到您的路由器，另一端连接到 Di AWS rect Connect 路由器。通过此连接，您可以绕过网络路径中的互联网服务提供商，直接创建与公共 AWS 服务（例如 Amazon S3 或 Amazon VPC）的虚拟接口。 AWS Direct Connect 位置允许 AWS 访问与其关联的区域。您可以使用公共区域或 AWS GovCloud （美国）中的单个连接访问所有其他公共区域的公共 AWS 服务。

AWS Direct Connect 有两个计费要素：端口时长和出站数据传输。有关更多信息，请参阅 AWS Direct Connect 定价。

Elastic Load Balancing

Elastic Load Balancing 会自动将您的传入流量分配到一个或多个可用区域中的多个目标，例如亚马逊 EC2 实例、容器和 IP 地址。它会监控已注册目标的运行状况，并仅将流量传输到运行状况良好的目标。弹性负载均衡将会扩展负载均衡器容量，以响应传入流量中的变化。

使用 Elastic Load Balancing 在上设置高可用性的 SAP 环境 AWS。

利用负载均衡器，您可以按实际用量付费。有关更多信息，请参阅 Elastic Load Balancing 定价。

数据传输定价

数据传输定价因架构模式和用例而异。它仅占SAP工作负载总成本的一小部分 AWS，即1-5%。

下表汇总了适用于您的 SAP 环境的常见数据传输场景。

场景	架构	数据传输费用	定价指南	其他费用
入境至 AWS	全部	否		
从出站 AWS 到互联网	全部	是	基于所使用的服务	
同一 AWS 地区的服务	互联网网关	否		
同一 AWS 地区的服务	NAT 网关	否		每 GB 处理费用，请参阅 Amazon VPC 定价
同一 AWS 地区的服务	AWS PrivateLink/VPC 终端节点	否		请参阅 AWS PrivateLink 定价
不同 AWS 地区的服务	全部	是	区域间数据传输的每 GB 费用，	

场景	架构	数据传输费用	定价指南	其他费用
			请参阅 Amazon EC2 定价	
同一可用区中的组件	全部	否		
不同可用区域中的组件	AWS Transit Gate	否		AWS Transit Gateway 手续费，请参阅 AWS Transit Gate
不同可用区域中的组件	Amazon VPC 对等连接	是	区域间数据传输的每 GB 费用，请参阅 Amazon EC2 定价	
不同 AWS 地区的组件	AWS Transit Gate	是	区域间数据传输的每 GB 费用，请参阅 Amazon EC2 定价	AWS Transit Gateway 处理
不同 AWS 地区的组件	Amazon VPC 对等连接	是	区域间数据传输的每 GB 费用，请参阅 Amazon EC2 定价	
转移到本地或公司网络	AWS VPN	是	按每 GB 的数据传输收费，请参阅 Amazon EC2 定价	AWS VPN 和 AWS Transit Gatewa
转移到本地或公司网络	AWS 直接连接	是	根据位置和提供商向外传输数据的每 GB 费用，请参阅 Amazon EC2 定价	AWS 直接连接和 T AWS ransit Gateway 收费

自动化

使用适用于 SAP 的 S AWS ystems Manager，你可以使用 Backup 在亚马逊 EC2 上 AWS 备份和恢复 SAP HANA 数据库。

AWS 您可以免费使用适用于 SAP 的 Systems Manager。您只需为为管理和运营 SAP 环境而配置的 AWS 资源付费。

Backup、还原和恢复

借助这些服务，您可以快速有效地备份、还原和恢复 SAP 工作负载。

主题

- AWS 适用于 SAP HANA 的 Backint Agent
- AWS 弹性灾难恢复
- Amazon EBS 快照

AWS 适用于 SAP HANA 的 Backint Agent

AWS 适用@@ 于 SAP HANA 的 Backint Agent AWS （ Backint 代理）是一款经过 SAP 认证的备份和还原应用程序，适用于在云端 EC2 亚马逊实例上运行的 SAP HANA 工作负载。 AWS Backint 代理作为独立应用程序运行，可与您的现有工作流程集成，将 SAP HANA 数据库备份到 Amazon S3 和 AWS 备份。

AWS Backint 代理是一项免费服务。您只需为所使用的基础 AWS 服务（例如 Amazon S3 或 AWS Backup）付费。有关更多信息，请参阅以下参考资料。

- Amazon S3 定价
- AWS Backup 定价

AWS 弹性灾难恢复

AWS Elastic 灾难恢复（Elastic Dasaster Recovery）使用经济实惠的存储、最少的计算和恢复，快速、可靠地 point-in-time恢复本地和基于云的应用程序，最大限度地减少停机和数据丢失。

您只需为主动复制到 AWS的服务器付费。有关更多信息，请参阅 AWS Elastic 灾难恢复定价。

Amazon EBS 快照

请参阅 A mazon EBS 部分。

迁移

以下服务使您能够快速移动应用程序和文件。

主题

- Migration Hub Orchestrator
- AWS DataSync

Migration Hub Orchestrator

AWS M@@ igration Hub Orchestrator 简化并自动将服务器和企业应用程序迁移到。 AWS它提供了运行和跟踪迁移的单个位置。

AWS Migration Hub Orchestrator 可供您使用，无需支付额外费用。您只需为为迁移预置的 AWS 资源付费。

AWS DataSync

AWS DataSync是一项在线数据移动和发现服务，可简化数据迁移，并帮助您快速、轻松、安全地将文件或对象数据移入存储服务、移出存储服务或在 AWS 存储服务之间移动。

您只需根据您所在 AWS 地区的每千兆字节固定费用为迁移的数据量付费。有关更多信息，请参阅AWS DataSync 定价。

监控

通过使用以下服务，您可以监控您的 SAP 工作负载 AWS。

主题

- AWS 数据提供商
- CloudWatch 适用于 SAP HANA 的 Amazon 应用程序见解
- Amazon CloudWatch
- AWS CloudTrail
- Amazon VPC 流日志

AWS 数据提供商

AWS 适用于 SAP 的数据提供程序是一种从 AWS 服务中收集与性能相关的数据的工具。它使这些数据可用于 SAP 应用程序，以帮助监控和改善业务交易的性能。

有关成本的信息，请参阅适用于 SAP AWS 的数据提供商定价。

CloudWatch 适用于 SAP HANA 的 Amazon 应用程序见解

Amazon App CloudWatch lication Insights 可帮助您监控使用亚马逊 EC2 实例以及其他应用程序资源的应用程序。

CloudWatch Application Insights 使用 CloudWatch 指标、日志和事件为选定的应用程序资源设置推荐的指标和日志，以通知检测到的问题。这些功能将根据 Amazon CloudWatch 定价从您的 AWS 账户中扣款。有关更多信息，请参阅《CloudWatch 应用见解》定价。

Amazon CloudWatch

Amazon 会实时 CloudWatch监控您的资源和正在运行 AWS 的应用程序。您可以收集和跟踪资源和应用程序的指标。

有关 CloudWatch 定价的信息，请参阅以下资源。

- CloudWatch 账单和成本
- 亚马逊 CloudWatch 定价

AWS CloudTrail

AWS CloudTrail是一项 AWS 服务，可帮助您实现 AWS 账户的运营和风险审计、治理和合规性。用户、角色或 AWS 服务采取的操作将作为事件记录在中 CloudTrail。

CloudTrail 按使用量收费，没有最低费用。有关更多信息，请参阅AWS CloudTrail 定价。

Amazon VPC 流日志

利用 VPC 流日志这项功能，您可以捕获有关传入和传出您的 VPC 中网络接口的 IP 流量的信息。

发布流日志时，将收取已出售日志的数据摄取和存档费用。有关发布销售日志时定价的更多信息，请打开 Amazon CloudWatch 定价，选择日志 > Vended Logs。

操作系统许可证

您可以自带自己选择的操作系统的许可证，也可以从 AWS Marketplace 购买许可证。

主题

- Red Hat
- SUSE
- Windows
- 甲骨文企业 Linu

Red Hat

红帽提供两个 Linux 发行版来运行 SAP 工作负载。如需了解更多详情，您可以查看红帽文档 — 适用于 SAP 解决方案的红帽企业 Linux (RHEL) 订阅概述。

您可以从 AWS Marketplace 或 Red Hat Cloud Access 使用这些选项。当您从中购买红帽操作系统时 AWS，您的 Support 计划包括操作系统支持。

如果您想启动带有 RHEL for SAP 应用程序的 Amazon EC2 实例，则必须订阅红帽云访问计划。在 RHEL 8 中，需要用于 SAP 解决方案的 RHEL 或适用于 SAP 应用程序的 RHEL 才能在生产环境中运行 SAP 应用程序。

Marketpl@@ AWS ace 上的 RHEL SAP Solut ions 按小时费率或按年付费提供。适用于 SAP 解决方案的 RHEL 专为运行 SAP 工作负载而设计。它包括更长的生命周期支持，以及扩展更新支持 (E4S)，为特定的次要版本提供自正式发布之日起四年的支持。它还提供了配置基于 Pacemaker 的集群所需的所有必要软件包，从而确保关键生产服务的可靠性和可用性。

> **Note**
>
> AWS Marketplace 定价显示 RHEL 的软件成本。RHEL 的额外费用已包含在亚马逊的 EC2 定价中。

SUSE

SUSE 提供了两个用于运行 SAP 工作负载的 Linux 发行版 — SUSE Linux 企业服务器 (SLES) 和适用于 SAP 应用程序的 SUSE Linux 企业服务器（适用于 SAP 的 SLES）

您可以从 AWS Marketplace 或 SUSE 使用这些选项。当您从中购买 SUSE 操作系统时 AWS，您的 Support 计划包括操作系统支持。

当您自带订阅时，Amazon 的支持取决于您 EC2 的 SUSE 购买协议。

Amazon EC2 的 SLES 按小时费率或按年度承诺提供。适用于 SAP 解决方案的 RHEL 专为运行 SAP 工作负载而设计。它包括更长的生命周期支持，以及扩展更新支持 (E4S)，为特定的次要版本提供自正式发布之日起四年的支持。它还提供了配置基于 Pacemaker 的集群所需的所有必要软件包，从而确保关键生产服务的可靠性和可用性。

AWS Marketplace 上的 SAP SLES 按小时费率或按年度承诺提供。SLES 订阅的价格包含在您的亚马逊 EC2 实例成本中，并且基于亚马逊 EC2 实例CPUs 的 v。适用于 SAP 的 SLES 专为运行 SAP 工作负载而设计。它包括更长的生命周期支持，以及提供 4.5 年总支持的 Extended Service Pack Overlap Support。SLES for SAP 还提供软件组件和服务，例如 SAP HANA 高可用性资源代理和集群连接器。

> **Note**
>
> SAP 版 SLES 的定价是软件的成本，SLES 不收取额外费用。

Windows

亚马逊上的 Windows 服务器 EC2 可以按固定的小时费率使用，无需承诺（按需），也可以通过一次性付款（Savings Plan 或预留实例）使用。就具有这两种选项的Windows操作系统而言，成本没有区别。您也可以自带驾照。有关更多信息，请参阅上的 Microsoft 许可 AWS。

甲骨文企业 Linu

SAP 要求你订阅 Oracle Linux Premier Support 才能使用 Oracle 企业 Linux 操作系统。有关更多信息，请查看以下来自 Oracle 和 SAP 的资源。

- 甲骨文商店
- SAP Note 2069760-Oracle Linux 7.x SAP 安装和升级（需要访问 SAP 门户）

AWS Marketp

AWS Marketplace 是一个精心策划的数字目录，客户可以使用它来查找、购买、部署和管理第三方软件、数据和服务，以构建解决方案和运营业务。

在 AWS Marketplace 中，产品可以免费使用，也可以收取相关费用。有关更多信息，请参阅产品定价。

AWS Support

AWS Support 提供不同级别的支持。有关更多信息，请参阅 Supp AWS ort 计划定价。

在运行 SAP 工作负载时，SAP 要求您至少获得业务级别的支持 AWS。要了解有关 SAP 先决条件的更多信息，请参阅 SA P Note 1656250-SAP，网址为：Su AWS pport 先决条件（需要访问 SAP 门户）。

SAP 上可用性和可靠性的架构指南 AWS

2021 年 8 月

本指南是内容系列的一部分，该系列提供了有关在 Amazon Web Services (AWS) 云中托管、配置和使用 SAP 技术的详细信息。有关更多信息，请参阅 SAP 上的 “ AWS 技术文档”。

概览

本指南提供了一套架构指南、策略和决策，用于部署具有高可用性和可靠配置 NetWeaver的基于 SAP 的系统 AWS。

在本指南中，我们将介绍：

- SAP 高可用性和可靠性简介
- 架构指南和决策考虑
- 架构模式和推荐用法

本指南适用于以前具有为 SAP 设计高可用性和灾难恢复 (HADR) 架构经验的用户。

本指南不涵盖确定 HADR 需求的业务需求和/或特定合作伙伴或客户解决方案的实施细节。

先决条件

专业知识

在按照本指南中的配置说明进行操作之前，我们建议您熟悉以下 AWS 服务。（如果您不熟悉 AWS，请参阅入门 AWS。）

- Amazon EC2
- Amazon EBS
- Amazon VPC
- Amazon EFS
- Amazon S3

推荐读物

在阅读本文档之前，我们建议您了解以下指南中的关键概念和最佳实践：

- SAP 谈 AWS 概述和规划
- 云端架构 SAP 入 AWS 门

简介

几十年来，SAP 客户通过两种常见模式在内部保护 SAP 工作负载：高可用性和灾难恢复。云计算的出现为使用现代架构和技术重新思考 SAP 的 HADR 功能提供了机会。

让我们回顾一下作为 SAP n 层架构一部分的 SAP 系统设计和单点故障。

SAP NetWeaver 架构单点故障

图 1：SAP 单点故障

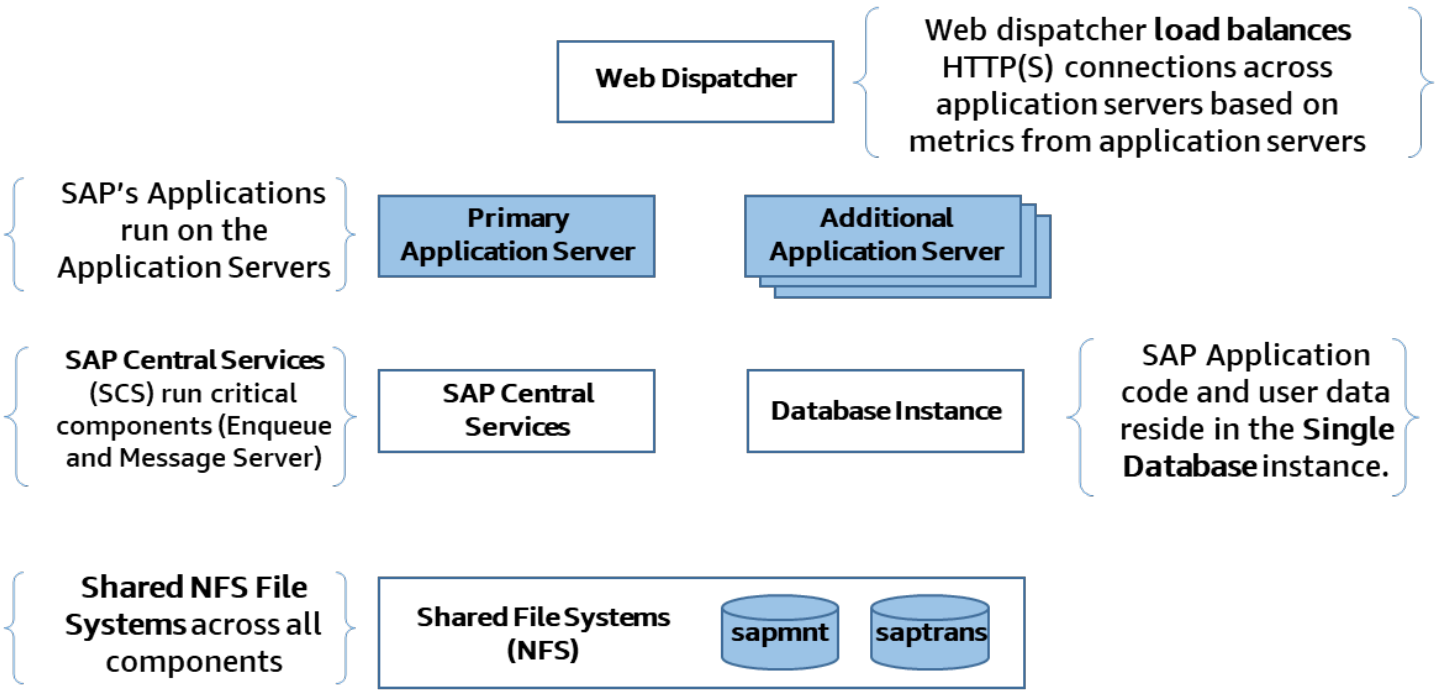


图 1 显示了典型的 SAP NetWeaver 架构，它有几个单点故障，如下所示：

- SAP 中央服务（消息服务器和入队进程）
- SAP 应用程序服务器

- NFS（共享存储）
- 数据库
- SAP 网络调度器

对于 SAP 中央服务和数据库，可以通过部署更多主机来增加保护。例如，另一台运行 SAP 复制入队的主机可以防止应用程序级锁定（入队锁）丢失，而另一台运行辅助数据库实例的主机可以防止数据丢失。

但是，这些单点故障的固有设计限制了轻松利用云原生功能来提供高可用性和可靠性的能力。

Amazon 弹性文件服务 (Amazon EFS) 是一项高度可用且持久的托管 NFS 服务，可在多个物理位置（AWS 可用区）主动运行。此服务可以帮助保护 SAP 的其中一个单点故障。

高可用性和灾难恢复

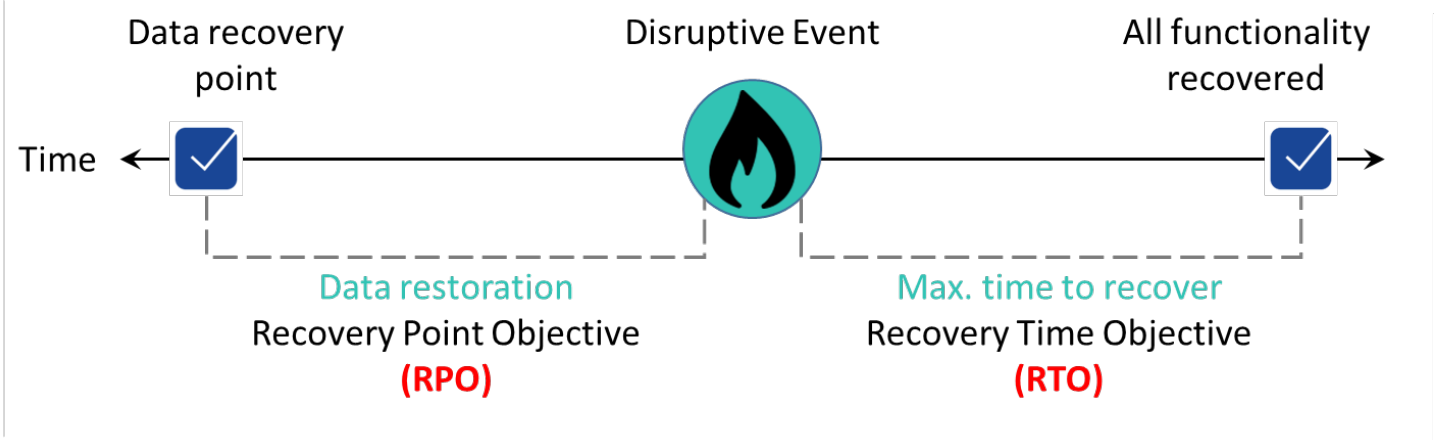
高可用性 (HA) 是系统的属性，它可以在定义的时间段内以可接受或商定的水平提供服务，并掩盖最终用户的计划外中断。这通常是通过使用群集服务器来实现的。这些服务器提供自动故障检测、恢复或高弹性硬件、强大的测试以及问题和变更管理。

灾难恢复 (DR) 通过在不同的硬件和/或物理位置进行可靠且可预测的恢复，防止计划外重大中断（例如站点灾难）。由于损坏或恶意软件导致的数据丢失被视为逻辑灾难事件。它通常在单独的解决方案中解决，例如从最新的备份或存储快照中恢复。逻辑灾难恢复并不一定意味着故障转移到另一个设施。

从记录在案和可测量的数据点的角度来看，HADR 要求通常按以下方式定义：

- 正常运行时间百分比是给定时段（每月或每年）内正常运行时间的百分比。
- 平均恢复时间 (MTTR) 是从故障中恢复所需的平均时间。
- 恢复服务 (RTS) 是指为用户恢复系统服务所花费的时间。
- 恢复时间目标 (RTO) 是系统或服务可能停机的最长时间、解决方案恢复所需的时间以及服务重新可用所需的时间。
- 恢复点目标 (RPO) 是指企业愿意丢失多少数据，用时间表示。这是从故障到恢复点之间的最长时间。

图 1：SAP 单点故障



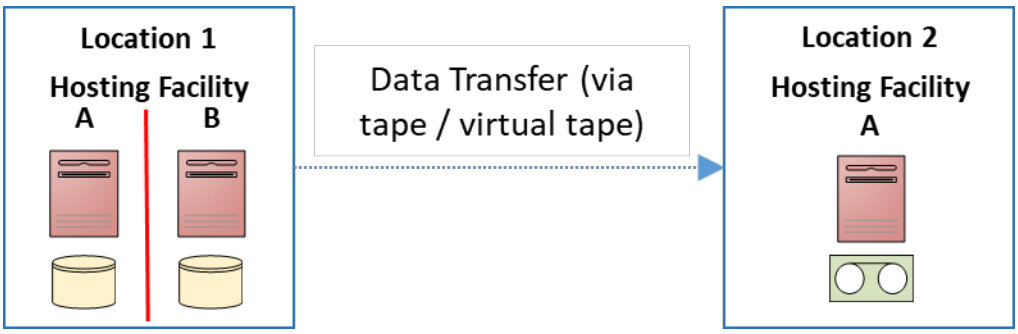
≈

本地部署模式与云部署模式

传统上，具有高可用性要求的客户会将其主要计算能力部署在单个数据中心或托管设施中，通常是在两个独立的房间或数据中心大厅中，这些房间或数据中心大厅具有不同的冷却和电源以及高速网络连接。有些客户会近距离运行两个托管设施，计算能力是分开的，但又足够近，不会受到网络延迟的影响。

为了满足灾难恢复需求（前面的情景意味着不可预见的位置故障风险更高），许多客户会扩展其架构，将数据副本所在的辅助位置包括在内，并增加空闲计算容量。主位置和辅助位置之间的距离常常导致需要异步传输数据，这会影响恢复点目标。对于许多运行 SAP 的行业和公司来说，这是用于高可用性和灾难恢复的标准且普遍接受的架构模式。

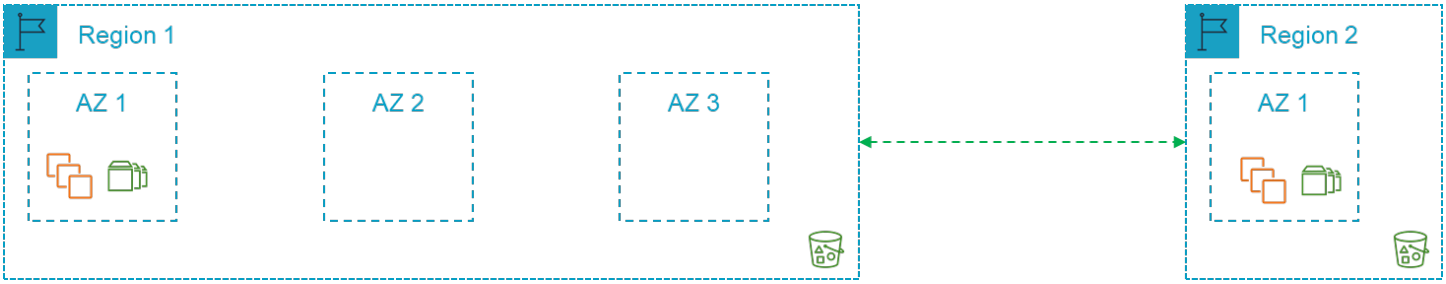
图 3：本地灾难恢复



在图 3 中，我们举例说明了客户经常在内部使用的方法。在 L ocation 1 中，客户有两个托管设施，通常将房间或大厅分隔在同一个数据中心中，他们在那里为 SAP 单点故障部署高可用性架构。地点 2 是灾难恢复地点，在地点 1 的两个托管设施都出现严重故障时，SAP 系统将在其中恢复。

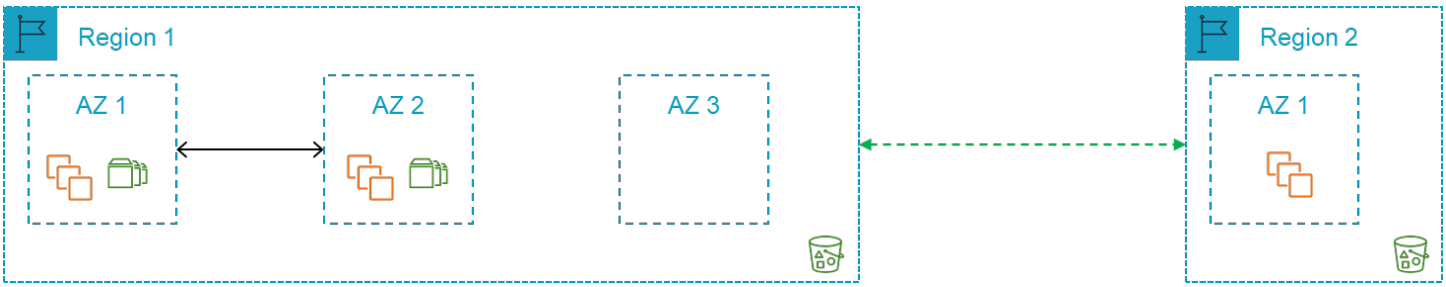
将 SAP 工作负载迁移到云提供商的客户仍会恢复到该架构，并将其映射到 AWS 区域和可用区 (AZs)，如图 4 所示。虽然这种架构可以在您的环境中运行，但它不遵循Well-Architecte AWS d Framework，该框架可帮助云架构师为其应用程序构建安全、高性能、弹性和高效的基础架构。

图 4：本地到 AWS 区域的映射方法



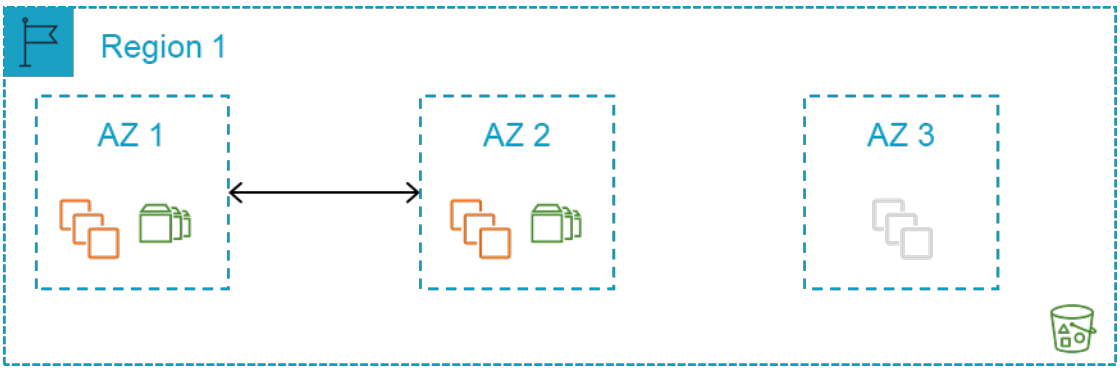
AWS 在区域和可用区中按地理位置隔离设施。多可用区方法提供距离，同时保持主计算容量的性能。这种方法（图 5）大大降低了定位故障的风险。

图 5：本地与 AWS 区域映射的替代方法



由于主计算容量的位置故障风险显著降低，因此可以根据业务需求评估第二个区域的需求。您可以使用在相同或不同的区域快速部署所需的容量 AWS。闲置硬件不再是问题。利用跨区域复制，数据备份可以存储在亚马逊简单存储服务 (Amazon S3) 的 AWS 单个区域或 AWS 多个区域中。这种架构可以简化并随时可用（图 6）。

图 6：单 AWS 区域方法



除了考虑基础设施或托管设施故障的影响外，还需要考虑的另一种情况是由于意外或恶意的技术活动而导致业务数据丢失。

意外或恶意技术活动导致的业务数据丢失称为逻辑灾难恢复。它需要决定从一个好的本地副本恢复业务数据。为此，需要就数据的存储位置以及逻辑灾难恢复时如何使用数据做出决定。

在本指南中，我们将详细介绍关键架构指南、架构模式以及为满足可用性和可靠性要求而需要考虑的决策。

架构指导方针和决策

本节将简要概述通常用于 SAP 工作负载的 AWS 服务，以及在设计托管 SAP 的架构时需要了解的一些要点 AWS。如果您已经熟悉这些 AWS 服务，则可以跳过本节。

区域和可用区

AWS 全球基础设施由AWS 区域和可用区 (AZs) 组成。 有关 AWS 全球基础设施的更多详细信息，请参阅区域和可用区。

区域

AWS 业务遍及全球，可确保为世界各地的客户提供服务。 AWS 在北美、南美、欧洲、亚太和中东维护多个区域。

AWS 区域是地理区域中的 AWS 资源集合。每个区域都是孤立和独立的。有关区域名称和代码的列表，请参阅区域终端节点。

区域提供容错能力、稳定性和弹性。它们使您能够创建冗余资源，在不太可能发生的停机事件中，这些资源仍然可用且不受影响。

AWS 区域由多个可用区 (AZs) 组成，通常为 3。可用区是 AWS 基础设施中完全隔离的分区。它由分散的数据中心组成，这些数据中心位于不同的设施中，具有冗余电源、网络和连接。

您保留对数据实际所在 AWS 区域的完全控制权和所有权，从而可以轻松满足地区合规性和数据驻留要求。

可用区

可用区 (AZs) 使客户能够运行比单个数据中心更高的可用性生产应用程序和数据库。将应用程序分布在多个区域中，使您能够在面对大多数故障模式（包括自然灾害或系统故障）时保持弹性。

每个可用区可以是多个数据中心。全面而言，它可以包含数十万台服务器。它们是 AWS 全球基础架构中完全隔离的分区。凭借其自身强大的基础架构，可用区与任何其他区域在物理上是分开的。有几千米的距离，尽管所有距离都在100千米以内（彼此相距60英里）。此距离可以隔离可能影响数据中心的最常见灾害（即洪水、火灾、暴风雨、地震等）。

区域内的所有可用区 (AZs) 都通过完全冗余的专用城域光纤与高带宽和低延迟网络互连。这可确保区域间的高吞吐量、低延迟联网。网络性能足以完成可用区之间的同步复制。

AWS 可用区 (AZs) 使我们的客户能够以高度可用的方式运行其应用程序。为了实现高可用性，应用程序需要在多个位置同时运行完全相同的数据，从而允许在发生灾难时以最少的停机时间进行无缝故障转移。

服务

我们的一般政策是，根据客户需求、延迟、数据主权和其他因素，在正式上市后的 12 个月内向所有 AWS 地区提供 AWS 服务、功能和实例类型。您可以联系AWS 销售代表，分享您对本地区域交付的兴趣，索取服务路线图信息，或者深入了解服务相互依存关系（根据保密协议）。

由于服务的性质，某些 AWS 服务是在全球而不是按地区交付的，例如53号公路、Amazon Chime、亚马逊 WorkDocs、亚马逊和 WorkMail亚马逊 WorkSpaces。 WorkLink

其他服务，例如亚马逊弹性计算云（亚马逊 EC2）和亚马逊弹性区块存储（Amazon EBS）Elastic Block Store（Amazon EBS），均为区域服务。在创建用于启动的 Amazon EC2 或 Amazon EBS 资源时，需要在某个区域内指定所需的可用区。

选择 AWS 区域

在为 SAP 环境部署选择 AWS 区域时，应考虑以下几点：

- 靠近本地数据中心、系统和最终用户，以最大限度地减少网络延迟。
- 数据驻留和合规性要求。
- 您计划在该地区使用的 AWS 产品和服务的可用性。有关更多详细信息，请参阅区域表。
- 您计划在该地区使用的 Amazon EC2 实例类型的可用性。有关更多详细信息，请参阅适用于 SA P 的 Amazon EC2 实例类型。
- 不同 AWS 地区之间的定价差异。有关更多详细信息，请参阅 SAP 关于 AWS 定价和优化的指南。

多区域注意事项

在多个区域部署时，一个重要的考虑因素是每个区域所需的核心服务（例如网络、安全和审计服务）的相关成本和管理工作。

网络延迟

如果您决定采用多区域方法，则应考虑从本地位置到次要区域的网络延迟增加所产生的影响。

跨区域数据传输

AWS 提供了几种在区域之间传输数据的方法。在设计用于灾难恢复的 SAP 架构时，这些方法非常重要。在将数据传输到其他 AWS 区域时，您应考虑任何数据驻留要求、与数据传输（跨区域对等互连和/或 Amazon S3 复制）相关的成本，以及次要区域的存储。

0 级服务

使用 AWS 区域时，在部署 SAP 工作负载之前，您需要许多第 0 层服务。这些产品包括 DNS、Active Directory 和/或 LDAP 以及任何 AWS 或 ISV 提供的安全与合规产品和服务。

AWS 账户

虽然没有关于特定客户应拥有多少 AWS 账户的 one-size-fits-all答案，但大多数组织都希望创建一个以上的 AWS 账户。多个账户可提供最高级别的资源和账单隔离。

在 SAP 工作负载的背景下，客户通常在单独的 AWS 账户中部署生产环境。它有助于将生产环境与 SAP 环境的其余部分隔离开来。

AWS O rganizations 是一项账户管理服务，可让您将多个 AWS 账户整合到一个由您创建和集中管理的组织中。 AWS Organizations 包括账户管理和整合账单功能。它使您能够更好地满足业务的预算、安全和合规需求。作为组织的管理员，您可以在组织中创建账户并邀请现有账户加入组织。

AWS Landing Zon e 是一种解决方案，可帮助客户根据 AWS 最佳实践更快地设置安全的多账户 AWS 环境。您可以通过自动设置运行安全和可扩展工作负载的环境来节省时间，同时通过创建核心账户和资源来实现初始安全基准。它还为开始使用多账户架构、Identity and Access Managem AWS ent、治理、数据安全、网络设计和日志提供了一个基准环境。

注意：Lan AWS ding Zone AWS 解决方案由解决方案架构师或专业服务顾问提供，用于创建 AWS 客户、网络和安全策略的自定义基准。

如果您希望通过 Active Directory 等自定义插件设置具有丰富自定义选项的可配置着陆区，并通过代码部署和配置管道进行变更管理，请考虑使用 Landing Zone 解决方案。 AWS

AWS Cont@@ rol Tower 基于与数千家企业合作建立的最佳实践，提供了设置和管理安全、合规的多账户 AWS 环境的最简单方法。借助 C AWS ontrol Tower，您的分散团队可以快速配置新 AWS 帐户。同时，您的中央云管理员将知道所有账户都与集中制定的公司范围内的合规性政策保持一致。

可以考虑使用 AWS 控制塔（Control Tower）在带有预配置蓝图的着陆区基础上设置一个新 AWS 环境。您可以使用预先配置的护栏以交互方式管理您的账户。

计算

亚马逊弹性计算云 (Amazon EC2) 在亚马逊网络服务 (AWS) 云中提供可扩展的计算容量。亚马逊 EC2 实例在指定亚马逊虚拟私有云 (Amazon VPC) 内的特定可用区启动。

当 Amazon EC2 实例部署在单个区域内的两个或多个可用区域时，服务级别 AWS协议为 99.99%。

实例类型

SAP 支持一系列 A mazon EC2 实例类型。在为 SAP 工作负载选择实例类型时，应考虑哪些层可以灵活使用所用实例（应用程序层）。另外，根据计算、内存、存储吞吐量和许可证合规性要求，考虑哪些层需要使用特定的实例类型（数据库层）。

对于具有特定实例类型要求且在故障情况下无法灵活更改的等级，请考虑在所需的可用区和实例将要运行的区域内使用预留实例或按需容量预留进行容量预留。这种方法称为静态稳定性。有关更多信息，请参阅使用可用区的静态稳定性。

预留实例

与按需@@ 实例定价相比，预留实例可显著节省您的 Amazon EC2 成本。预留实例不是物理实例。它们是对账户中使用的按需实例所应用的账单折扣。要享受 discount 优惠，这些按需实例必须匹配某些属性，例如实例类型和区域。

当您 EC2 跨多个可用区部署 Amazon 以实现高可用性时，我们建议您使用区域预留实例。除了比按需实例定价节省之外，区域预留实例还可在指定可用区内提供容量预留。这样可以确保所需的容量随时可用。

出于计费目的，Organizations 的整合账单功能将组织中的所有账户视为一个账户。 AWS 这意味着，组织中的所有账户都可以享受到任何其他账户购买的预留实例的小时成本优惠。

节省计划

S@@ avin gs Plans 是一种灵活的定价模式，可为您的 AWS 计算使用量节省高达 72%。无论 EC2 实例系列、大小、租期或 AWS 地区如何，它都提供更低的 Amazon 实例使用价格。Savings Plan 模式也适用于 AWS Fargate 和 Lambda AWS 的使用。

与按需相比，Savings Plans 可节省大量费用，就像亚马逊 EC2 预留实例一样，以换取承诺在一年或三年内使用特定数量的计算能力（以美元/小时计）。

按需容量预留

按需容量预留允许您为特定可用区域中的 Amazon EC2 实例预留任意持续时间的容量。这使您能够独立创建和管理容量预留，并享受 Savings Plans 或区域预留实例提供的账单折扣。您可以随时创建容量预留，确保只要需要，您就可以随时访问Amazon EC2 容量。您随时可以创建容量预留，而无需作出一年或三年期限承诺，并且可以立即使用该容量。当您不再需要预留时，我们建议您取消容量预留以停止为此产生费用。

跨可用区域的实例系列可用性

某些 Amazon EC2 实例系列（例如 X1 和高内存）不适用于某个区域内的所有可用区。您应确认 SAP 工作负载所需的实例类型，并检查目标可用区中是否有这些实例类型。

Amazon EC2 自动恢复

Amazon a EC2 uto recovery 是一项 Amazon EC2 功能，当实例由于底层硬件故障或需要 AWS 参与修复的问题而受损时，它会自动恢复同一可用区内的实例。

您可以通过创建监控 EC2 实例状态的亚马逊 CloudWatch 警报来启用亚马逊实例的自动恢复。导致系统状态检查出现故障的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上影响到网络连接状态的硬件问题

尽管失败的实例通常需要不到 15 分钟的时间才能重启，但 Amazon a EC2 uto Recovery 不提供 SLA。因此，如果故障主机上运行的应用程序的恢复至关重要（例如，SAP 数据库或 SAP Central Services），则应考虑使用跨两个可用区的群集来帮助确保高可用性。

高内存裸机专用主机

Amazon EC2 内存增强型实例专为运行大型内存数据库（例如 SAP HANA）而设计。高内存裸机实例可在 Amazon EC2 专用主机上使用，预留期为一年或三年。

内存增强型实例支持专用主机恢复。如果在您的专用主机上检测到故障，主机恢复会自动在新的替换主机上重启您的实例。主机恢复减少了手动干预的需求，并降低了专用主机意外故障时的操作负担。

我们建议您在所选区域的不同可用区中使用内存第二高的实例，以防出现区域故障。

亚马逊 EC2 维护

AWS 维护实例的底层主机时，它会安排实例的维护时间。维护事件有两种类型：

- 在网络维护期间，计划的实例会在短时间内失去网络连接。在维护完成后，将恢复与实例的正常网络连接。
- 在电源维护期间，计划的实例将短时间脱机，然后重启。执行重启后，您的实例的所有配置设置都将保留。

此外，我们经常升级我们的 Amazon EC2 队列，许多补丁和升级都以透明的方式应用于实例。但是，有些更新需要短暂的重启。这样的重启应该很少发生，但对于应用可增强我们的安全性、可靠性和操作性能的升级是必要的。

作为 Amazon EC2 定期维护的一部分，可能需要进行两种类型的重启：

- 实例重启是虚拟实例的重启，相当于操作系统的重启。
- 系统重启需要重启托管实例的底层物理服务器。

您可以在 AWS 管理控制台中或使用 API 工具或命令行查看您的实例即将发生的任何计划事件。

如果您不采取任何措施，则两种情况下对您的实例的影响都是一样的：在您的计划维护时段内，您的实例将经历重启，在大多数情况下需要几分钟。

或者，您可以通过在实例上执行停止和启动操作，将您的实例迁移到新主机。有关更多信息，请参阅停止和启动实例。您可以自动化立即停止并启动以响应计划维护事件。

网络连接

亚马逊 Virtual Private Cloud 和子网

亚马逊虚拟私有云（Amazon VPC）是专用于您的 AWS 账户的虚拟网络。它在逻辑上与 AWS 云中的其他虚拟网络隔离。您可以将您的 AWS 资源（例如 Amazon EC2 实例）启动到您的 VPC 中。

创建 VPC 时，必须以无类域间路由 (CIDR) 块的形式为 VPC 指定 IPv4 地址范围，例如 10.0.0.0/16。这是您的 VPC 的主要 CIDR 块。

您可以在所选 AWS 区域内创建 VPC，它将在该区域内的所有可用区域中可用。

要向您的 VPC 添加新子网，您必须在 VPC 范围内为该子网指定一个 IPv4 CIDR 块。您可以指定要在其中放置子网的可用区。您可以在同一个区域中拥有多个子网，但单个子网不能跨越多个区域。

为了提供 future 的灵活性，我们建议您的子网和连接设计支持您账户在该区域内的所有可用区域，无论您最初计划在一个区域内使用多少个可用区。

跨可用区域的延迟

所有可用区 (AZs) 都通过完全冗余的专用城域光纤与高带宽、低延迟的网络互连。这会导致同一区域中不同可用区的资源之间出现个位数毫秒的延迟。

为了获得高可用性，我们建议跨多个可用区（包括 SAP 应用程序服务器层）部署生产 SAP 工作负载。如果您有涉及大量数据库调用的 SAP 事务或批处理作业，我们建议您在与数据库位于同一可用区的 SAP 应用程序服务器上运行这些事务，并对最终用户使用 SAP 登录组 (SMLG)，对后台处理作业使用批处理服务器组 (SM61)。这可确保 SAP 工作负载中对延迟敏感的部分在正确的应用程序服务器上运行。

从本地到 AWS 连接

您可以通过 Site-to-Site虚拟专用网络 (VPN) 或 Di AWS rect Connect 从本地连接到您的 VPC。 AWS Direct Connect 提供的服务级别协议高达 99.99%， Site-to-SiteVPN 提供的 S LA 为 99.95%

Site-to-Site VPN 连接是指向特定区域。对于基于直接连接的连接，Di rect Connect Gateway 允许您连接到多个区域。

在与 AWS 本地建立连接时，请确保通过使用多个 Direct Connect Link、多个 VPN 连接或两者的组合来实现弹性连接。

Di AWS rect Connect 弹性工具包提供了一个包含多个弹性模型的连接向导。这些模型可帮助您订购专用连接以实现您的 SLA 目标。

VPC 端点

VPC 终端节点以私密方式将您的 VPC 连接到支持的 AWS 服务和由提供支持的 VPC 终端节点服务AWS PrivateLink。它不需要通过互联网网关、NAT 设备、VPN 连接或 Di AWS rect Connect 连接访问互联网。您的 VPC 中的实例不需要公有 IP 地址即可与 AWS 服务中的资源通信。您的 VPC 与其他服务之间的流量不会离开亚马逊网络。

VPC 终端节点可用于支持基于 SAP 的工作负载所需的所有核心 AWS 服务，包括亚马逊 EC2 API、Amazon S3 和亚马逊 Elastic File System。

跨区域对等互连

Amazon Virtual Private Cloud（亚马逊 VPC）支持不同区域的两个 VPCs 区域之间的区域间对等互连。这可用于允许网络流量（例如数据库复制流量）在不同区域的两个 Amazon EC2 实例之间流动。区域间对等互连会产生数据传输成本。

AWS T@@ ransit Gateway 是一个网络传输中心，您可以使用它通过 Di AWS rect Connect 或 VPN 将一个 AWS 区域内的虚拟私有云 (VPC) 与其他 AWS 区域的其他云以及本地网络互连。 VPCs 使用 Transit Gateway 将产生 Tr ansit Gateway 费用。AWS Tran sit Gateway 在一个区域内提供了 99.95% 的 SL A。

负载均衡

Elastic Loa d Balancing 支持四种类型的负载均衡：应用程序负载均衡器、网络负载均衡器、网关负载均衡器和经典负载均衡器。

Network Load Balancer 可用于支持跨多个可用区部署 SAP Web 调度器和/或 SAP 中央服务的高可用性。有关更多详细信息，请参阅使用 Network Load Balancer 叠加 IP 路由。

负载均衡器是客户端的单一联系点。负载均衡器将传入流量分配到多个目标，例如 Amazon EC2 实例。

监听器使用您配置的协议和端口检查来自客户端的连接请求，并将请求转发到目标组。

每个目标组使用 TCP 协议和指定的端口号将请求路由到一个或多个注册目标，例如 Amazon EC2 实例。您可以对每个目标组配置运行状况检查。在注册到目标组 (它是使用负载均衡器的侦听器规则指定的) 的所有目标上，执行运行状况检查。

对于 TCP 流量，Network Load Balancer 使用基于协议、源 IP 地址、源端口、目标 IP 地址、目标端口和 TCP 序列号的流哈希算法选择目标。每个单独的 TCP 连接在连接的有效期内路由到单个目标。

DNS

Amazon Route 53 是一种可用性高、可扩展性强的域名系统（DNS）Web 服务。您可以使用 Route 53 以任意组合执行三个主要功能：域注册、DNS 路由和运行状况检查。53 号公路提供的 SLA 为 100%。

Amazon Route 53 Resolver 提供了一组功能，允许在本地和 AWS 通过私有连接进行双向查询。

存储

对象存储

Amazon 简单存储服务 (Amazon S3) 是一项对象存储服务，可提供业界领先的可扩展性、数据可用性、安全性和性能。Amazon S3 是一项跨区域内所有可用区域的区域服务，其设计持久性为 99.999999999%（11 9），服务级别协议为 99.9%。

为了防止数据丢失，您可以对 Amazon S3 执行备份（例如数据库备份或文件备份）。此外，亚马逊 EBS 快照和亚马逊系统映像 (AMIs) 存储在 Amazon S3 中。

Amazon S3 复制支持跨亚马逊 S3 存储桶自动异步复制对象。为对象复制配置的存储桶可以归同一个 AWS 账户所有，也可以由不同的账户拥有。

亚马逊 S3 复制

您可以在相同或不同的 AWS 区域之间复制对象。

- 跨区域复制 (CRR) 用于跨不同区域的 Amazon S3 存储桶复制对象。 AWS
- 同区域复制 (SRR) 用于跨同一区域的 Amazon S3 存储桶复制对象。 AWS

跨区域复制会产生以下成本：

- 在第一和第二 AWS 区域之间传输的数据收取数据传输费用
- Amazon S3 对存储在两个不同 AWS 区域的 Amazon S3 中的数据收费

此外，您还可以通过跨区域复制启用 Amazon S3 复制时间控制。Amazon S3 复制时间控制 (Amazon S3 RTC) 可帮助您满足数据复制的合规性或业务要求，并提供对 Amazon S3 复制时间的可视性。Amazon S3 RTC 可在几秒钟内复制您上传到 Amazon S3 的大部分对象，并在 15 分钟内复制其中 99.99% 的对象。

除了上面列出的跨区域复制费用外，Amazon S3 RTC 还会产生以下费用：

- Amazon S3 RTC 管理功能-按每 G B 定价
- CloudWatch 亚马逊 Amazon S3 指标-按指标数量定价

同区域复制会产生以下成本：

- 存储在 Amazon S3 中的数据的费用

数据块存储

Amazon Elastic Block Store (Amazon EBS) 提供块级存储卷，用于亚马逊 EC2 实例。Amazon EBS 卷的行为类似于原始、未格式化的块储存设备。您可以将这些卷作为设备挂载在实例上。你可以在这些卷之上创建文件系统，也可以像使用块储存设备（如硬盘）一样使用它们。您可以动态更改连接到实例的卷的配置。

Amazon EBS 卷放置在特定的可用区中，在那里它们会被自动复制，以保护您免受单个组件故障的影响。所有 Amazon EBS 卷类型都提供持久的快照功能，在多可用区配置下，每个卷的可用性为 99.999%，服务可用性为 99.99%。需要使用数据库复制功能、块级复制解决方案或 Amazon EBS 快照，才能保证存储在 Amazon EBS 上的 SAP 数据跨多个可用区的持久性。

Amazon EBS 卷的设计年故障率 (AFR) 在 0.1%-0.2% 之间，其中故障是指卷完全或部分丢失，具体取决于卷的大小和性能。这使得 Amazon EBS 卷的可靠性是普通商用磁盘驱动器的 20 倍，后者出现故障，AFR 约为 4%。例如，如果您有 1,000 个 Amazon EBS 卷运行 1 年，那么您应该预计 1 到 2 个卷会出现故障。

Amazon EBS 提供多种不同的卷类型。它必须用于存储 SAP 数据库相关的数据，必须使用通用固态硬盘 (gp2) 或预配置 IOPS 固态硬盘 (io1)。吞吐量和 IOPS 要求将决定是需要 gp2 还是 io1。

借助 Amazon EBS Multi-Attach，您可以将单个预配置 IOPS 固态硬盘 (io1) 卷连接到位于同一可用区域的多达 16 个AWS 基于 Nitro 的实例。您可以将多个启用多重挂载的卷附加到一个实例或一组实例。卷附加到的每个实例都对共享卷拥有完全读取和写入权限。启用多重挂载的卷不支持 I/O 隔离栏。I/O 隔离栏协议控制共享存储环境中的写入访问，以保持数据一致性。您的应用程序必须为附加的实例提供写入顺序，以保持数据一致性。

Amazon EBS 快照

您可以通过拍摄 point-in-time快照将 Amazon EBS 卷上的数据备份到 Amazon S3。快照属于增量 备份，这意味着仅保存设备上在最新快照之后更改的数据块。由于无需复制数据，这将最大限度缩短创建快照所需的时间和增加存储成本节省。删除快照时，仅会删除该快照特有的数据。每张快照都包含将数据（从拍摄快照的那一刻起）恢复到新 Amazon EBS 卷所需的所有信息。

Amazon EBS 快照可以复制（复制）到其他地区和/或与其他 AWS 账户共享。

跨区域复制快照会产生以下费用：

- 在第一和第二 AWS 区域之间传输的数据收取数据传输费用
- Amazon EBS 快照对存储在两个不同 AWS 区域的 Amazon S3 中的数据收费

还原快照

根据现有 Amazon EBS 快照创建的新卷会在后台延迟加载。这意味着，从快照创建卷后，无需等待所有数据从 Amazon S3 传输到您的 Amazon EBS 卷，您连接的实例就可以开始访问该卷及其所有数据。

此初步操作需要时间，并且会显著增加 I/O 操作的延迟。如果您的实例访问尚未加载的数据，则该卷会立即从 Amazon S3 下载请求的数据，然后继续在后台加载其余卷数据。

快速快照还原

Amazon EBS 快速快照还原允许您根据创建时已完全初始化的快照创建卷。这会消除首次访问块时对其执行 I/O 操作的延迟。使用快速快照还原创建的卷可以立即交付其所有预配置性能。要使用快速快照还原，请在特定可用区中为特定快照启用此功能。对于启用快速快照还原功能的每个区域，按数据服务单位小时数 (DSUs) 收费。 DSUs 按分钟计费，最少 1 小时。

文件存储

Amazon EFS

Amazon Elastic Fil e System（亚马逊 EFS）提供基于 NFS 版本 4 的可扩展文件存储，供基于 Linux 的 EC2 亚马逊使用（基于 Windows 的亚马逊实例不支持 EC2 亚马逊 EFS）。 该服务旨在实现高度可扩展性、可用性和耐用性。Amazon EFS 文件系统跨一个 AWS 区域的多个可用区存储数据和元数据。亚马逊 EFS 提供的 SLA 为 99.99%。

Amazon EFS 文件系统可以在同一区域或不同区域 VPCs内跨账户共享，这使得 Amazon EFS 成为 SAP 全局文件系统 (/sapmnt) 和 SAP 传输目录 (/usr/sap/trans) 的理想选择。

AWS DataSync支持 Amazon EFS 到 Amazon EFS 在区域和不同 AWS 账户之间传输，允许跨区域复制基于 SAP 文件的关键数据。AWS 备份还可用于跨区域复制 Amazon EFS 文件系统的备份。

Amazon FSx

亚马逊 FSx 版 Windows 文件服务器提供完全托管的微软 Windows 文件服务器，由完全原生 Windows 文件系统提供支持。Amazon FSx 提供 99.9% 的 SLA，同时支持单可用区和多可用区文件系统。

使用单可用区文件系统，Amazon FSx 会自动在可用区内复制您的数据，持续监控硬件故障，并在出现故障时自动更换基础设施组件。亚马逊 FSx 还使用存储在Amazon S3中的Windows卷影复制服务，每天对您的文件系统进行高度持久的备份。您可以随时进行其他备份。

多可用区文件系统支持单可用区文件系统的所有可用性与持久性功能。此外，它们旨在为数据提供持续可用性，即使在可用区不可用时也是如此。在多可用区部署中，Amazon FSx 会自动在不同的区域预配置和维护备用文件服务器。写入文件系统磁盘的任何更改都会跨可用区同步复制到备用磁盘中。

Amazon FSx 文件系统可以在同一区域或不同区域 VPCs内跨账户共享，这使得 Amazon FSx 不仅可以用于 SAP 全球文件系统，还可以用于 SAP 传输目录。

此外，亚马逊还 FSx 可用于为微软 SQL Server 提供持续可用 (CA) 文件共享。

监控和审计

Amazon CloudWatch

Amazon CloudWatch 是一项专为 DevOps 工程师、开发人员、站点可靠性工程师 (SREs) 和 IT 经理构建的监控和可观察性服务。 CloudWatch 为您提供数据和切实可行的见解，以监控您的应用程序、响应系统范围的性能变化、优化资源利用率并获得统一的运营状况视图。 CloudWatch 以日志、指标和事件的形式收集监控和操作数据，为您提供在服务器上和本地服务器上运行的 AWS 资源、应用程序 AWS 和服务的统一视图。您可以使用 CloudWatch 来检测环境中的异常行为、设置警报、并排可视化日志和指标、采取自动操作、解决问题以及发现见解，以保持应用程序平稳运行。

AWS CloudTrail

AWS CloudTrail 是一项支持对您的 AWS 账户进行治理、合规、运营审计和风险审计的服务。借CloudTrail助，您可以记录、持续监控和保留与整个 AWS 基础架构中的操作相关的账户活动。CloudTrail 提供您的 AWS 账户活动的事件历史记录，包括通过 AWS 管理控制台 AWS SDKs、命令行工具和其他 AWS 服务执行的操作。此事件历史记录简化了安全分析、资源变更跟踪和故障排除。此外，您还可以使用 CloudTrail 来检测 AWS 账户中的异常活动。这些功能有助于简化操作分析和故障排除。

架构模式

在本节中，我们将详细介绍您可以根据可用性和恢复要求选择的架构模式。我们还会分析故障场景，帮助您为 SAP 系统选择正确的模式。

故障场景

对于以下故障场景，主要考虑因素是可用区内计算和/或存储容量的物理不可用。

可用区故障

可用区故障可能是由于您的资源在该可用区内使用的一项或多项 AWS 服务的可用性显著降级所致。例如：

- 有些 Amazon EC2 实例因系统状态检查错误而失败，或者无法访问且无法重启。
- 几个出现卷状态检查错误的亚马逊 Elastic Block Store (Amazon EBS) 卷出现故障。

Amazon 弹性区块存储失败

丢失连接到单个 Amazon EC2 实例的一个或多个 Amazon EBS 卷可能会导致 SAP 系统的关键组件（即数据库）不可用。

亚马逊 EC2 失败

丢失单个 Amazon EC2 实例可能会导致 SAP 系统的关键组件（即数据库或 SAP 中央服务）不可用。

逻辑数据丢失

如果底层硬件容量仍然存在，但数据的主副本已损坏或丢失，则还应考虑逻辑数据丢失的可能性。这种数据丢失可能是由于您 AWS 账户内的恶意活动或人为错误造成的。

为了防止逻辑数据丢失，建议将数据的常规副本备份到 Amazon S3 存储桶。此存储桶会被复制（使用单区域或跨区域复制）到另一个由单独 AWS 账户拥有的 Amazon S3 存储桶。通过在 AWS 两个账户之间进行适当的 AWS 身份和访问管理 (IAM) 管理 (IAM) 控制，此策略可确保并非所有数据副本都因恶意活动或人为错误而丢失。

模式

在本节中，我们将研究可用于处理上述故障场景的架构模式。

在选择满足组织特定业务需求的模式时，需要考虑两个关键参数：

- 针对 SAP 单点故障的计算可用性
- Amazon EBS 上仍保持 SAP 数据的可用性

这些参数决定了从故障场景中恢复所需的时间，即 SAP 系统恢复服务所花费的时间。

架构模式的类型

架构模式分为单区域和多区域模式。区别因素将是：

1. 如果您要求数据始终仅位于特定的地理位置（AWS 区域）（例如，数据驻留要求）。

   或

2. 如果您要求数据始终驻留在两个特定的地理位置（AWS 区域）（例如，为了合规起见，两个 SAP 数据的副本必须相隔至少 500 英里）。

如果您的生产系统对您的业务至关重要，并且在出现故障时需要尽量减少停机时间，则应选择多区域模式，以确保您的生产系统始终保持高可用性。在部署多区域模式时，您可以使用自动化方法（例如集群解决方案）在可用区之间进行故障切换，从而最大限度地减少总体停机时间并消除人为干预的需求，从而从中受益。多区域模式不仅提供高可用性，还提供灾难恢复，从而降低总体成本。

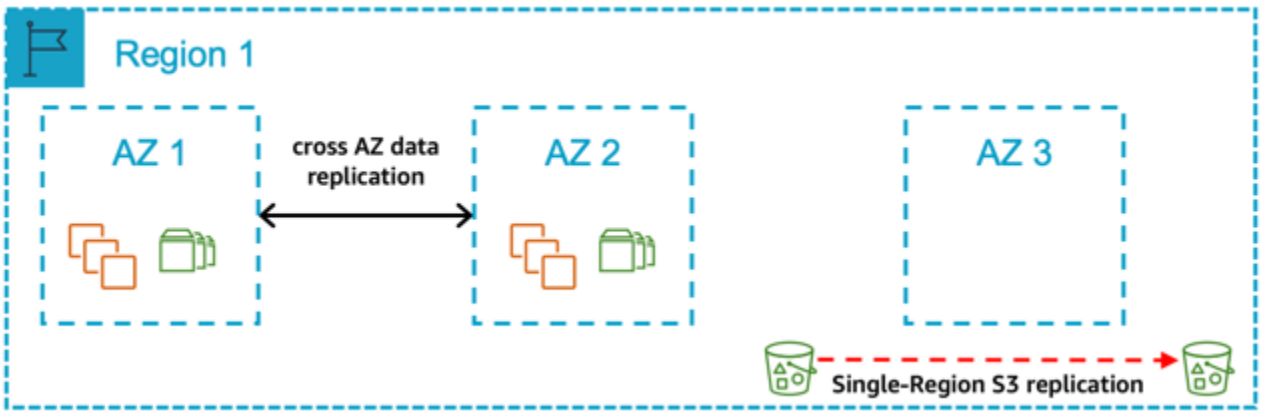
单一区域架构模式

在以下情况下，选择单个区域模式：

- 您要求数据始终仅位于特定的地理AWS 区域（区域）
- 您希望避免与多区域方法相关的潜在网络延迟注意事项
- 您希望避免与多区域方法相关的成本影响或差异，包括：
  - AWS 不同 AWS 地区的服务定价
  - 跨区域数据传输成本

模式 1：单个区域，有两个 AZs 用于生产

图 7：具有两个生产可用区的单个区域



在这种模式下，您可以将所有生产系统部署在两个可用区中。在两个可用区中，为生产 SAP 数据库和中央服务层部署的计算大小相同，可在区域出现故障时自动进行故障转移。SAP 应用程序层所需的计

算在两个区域之间以 50/50 的比例分配。您的非生产系统与您的生产系统的大小不相同，而是部署在该区域内的相同区域或不同的可用区中。

在以下情况下选择此模式：

- 您需要一个明确的时间窗口来完成生产恢复，并需要保证另一个可用区中生产 SAP 数据库和中央服务层的计算容量可用性。
- 您可以接受跨两个可用区为生产 SAP 数据库和中央服务层部署所需的计算和存储的额外成本。
- 您的非生产环境与生产环境的规模不同，因此在可用区出现故障或亚马逊 EC2 服务严重降级时，不能将其用作生产的牺牲容量。
- 您可以接受跨可用区域的数据复制（需要数据库复制功能或块级复制解决方案）和相关成本。
- 您可以接受，可用区之间的自动故障转移需要第三方集群解决方案。
- 您可以接受所需的可变持续时间（包括剩余可用区域中所需计算容量的可用性延迟），以便在区域出现故障时将应用程序层的容量恢复到 100%。

关键设计原则

- 100% 的计算容量部署在可用区 1 和可用区 2，用于生产 SAP 数据库和中央服务层。
- 生产应用程序层（主动/主动）的计算容量部署在可用区 1 和可用区 2 中。如果可用区出现故障，则需要扩展应用程序层，使其在剩余区域内恢复到 100% 的容量。
- 使用数据库复制功能或块级复制解决方案，将 SAP 数据库保存在 Amazon EBS 上的两个可用区中。
- Amazon a EC2 uto recovery 针对所有实例进行了配置，以防范底层硬件故障，但受第三方集群解决方案保护的实例除外。
- Amazon EFS 用于 SAP 全球文件系统。
- SAP 数据库会定期备份到亚马逊 S3。
- Amazon S3 单区域复制配置为保护逻辑数据丢失。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照。

优点

- 低平均恢复时间 (MTTR)
- 可预测的恢复服务 (RTS)
- 能够通过将数据库和中央服务层故障转移到可用区 2，防止可用区严重降级或整体故障

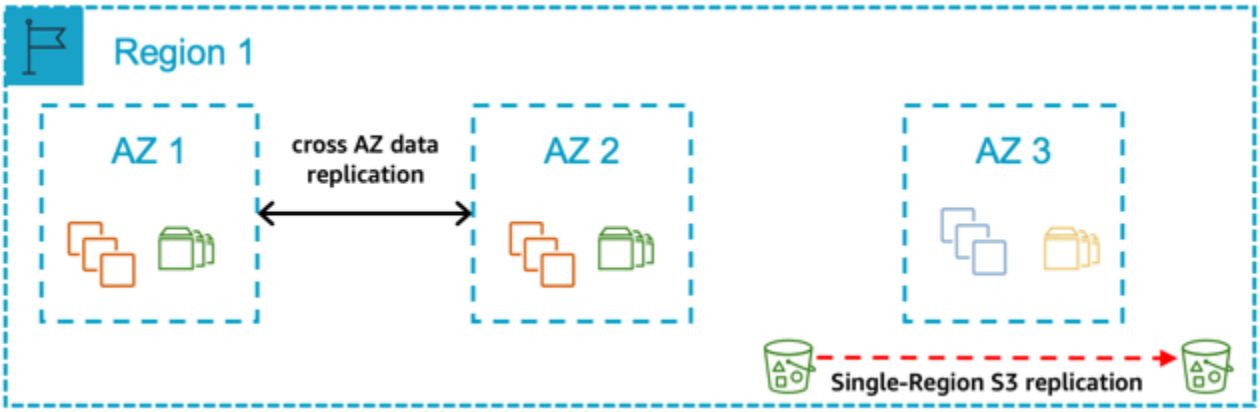
- 如果出现可用区或 Amazon EBS 故障，则无需从 Amazon S3 恢复数据

注意事项

- 在可用区之间进行自动故障切换需要有据可查和测试的流程。
- 维护自动故障转移解决方案需要经过充分记录和测试的流程。
- 如果可用区出现故障或 Amazon EC2 服务严重降级，则需要经过充分记录和测试的流程来扩展 AWS 资源，使应用程序层恢复到所需的容量。

模式 2：在第三个 AZ 中有一个区域，其中两个 AZs 用于生产，生产规模的非生产

图 8：一个区域在第三个可用区中有两个可用区，用于生产规模和生产规模的非生产环境



在这种模式下，您可以将所有生产系统部署在两个可用区中。在两个可用区中，为生产 SAP 数据库和中央服务层部署的计算大小相同，可在区域出现故障时自动进行故障转移。SAP 应用程序层所需的计算在两个可用区之间以 50/50 的比例分配。您的非生产系统的大小与您的生产系统相同，并且部署在第三个可用区中。如果您的生产系统所在的可用区出现故障，则会重新分配非生产容量，以使生产恢复到多可用区模式。

在以下情况下选择此模式：

- 如果该区域内的可用区出现故障，您需要能够继续为生产配置多可用区。
- 您需要一个明确的时间窗口来完成生产恢复，并确保另一个可用区中生产 SAP 数据库和中央服务层的计算容量可用性。
- 您可以接受跨两个可用区为生产 SAP 数据库和中央服务层部署所需的计算和存储的额外成本。
- 您可以接受跨可用区域的数据复制（需要数据库复制功能或块级复制解决方案）和相关成本。
- 您可以接受，可用区之间的自动故障转移需要第三方集群解决方案。

- 在可用区出现故障时，您可以接受所需的可变持续时间（包括剩余可用区域中所需计算容量的可用性延迟），以使应用程序层的容量恢复到 100%。

关键设计原则

- 100% 的计算容量部署在可用区 1 和可用区 2 中，用于生产 SAP 数据库和中央服务层。
- 100% 的生产计算能力（数据库和中央服务）部署在第三个可用区，供非生产人员在正常操作中使用。
- 生产应用程序层（主动/主动）的计算容量部署在可用区 1 和可用区 2 中。如果可用区出现故障，则需要扩展应用程序层，使其在剩余区域内恢复到 100% 的容量。
- Amazon a EC2 uto reco very 针对所有实例进行了配置，以防范底层硬件故障，但受第三方集群解决方案保护的实例除外。
- 使用数据库复制功能或块级复制解决方案，将 SAP 数据库保存在 Amazon EBS 上的两个可用区中。
- Amazon EFS 用于 SAP 全球文件系统。
- SAP 数据库会定期备份到亚马逊 S3。
- Amazon S3 单区域复制配置为防止逻辑数据丢失。
- 所有服务器的 Amazon Machine Image/Amazon EBS 快照都是定期拍摄的。

优点

- 低平均恢复时间 (MTTR)
- 可预测的恢复服务 (RTS)
- 能够通过将数据库和中央服务层故障转移到可用区 2，防止可用区严重降级或整体故障
- 在可用区出现故障或 Amazon EBS 故障时，无需从 Amazon S3 恢复数据
- 可选择将数据保存在 Amazon EBS 上的三个不同可用区中，具体取决于数据库或块级复制解决方案的功能
- 如果可用区出现严重降级或完全出现故障，则使用非生产计算容量在两个可用区中恢复生产

注意事项

- 在可用区之间进行自动故障切换需要有据可查和测试的流程。
- 维护自动故障转移解决方案需要经过充分记录和测试的流程。

- 如果可用区出现故障或 Amazon EC2 服务严重降级，则需要经过充分记录和测试的流程来扩展 AWS 资源，使应用程序层恢复到所需的容量。
- 如果可用区故障影响生产，则需要经过充分记录和测试的流程，才能将非生产计算容量重新分配为在两个可用区之间运行的恢复生产。

模式 3：单个区域，其中一个可用区用于生产，另一个可用区用于非生产

图 9：单个区域，其中一个可用区用于生产，另一个可用区用于非生产

在这种模式下，您将所有生产系统部署在一个可用区中，将所有非生产系统部署到另一个可用区。您的非生产系统的规模与您的生产系统相当。

在以下情况下选择此模式：

- 您需要一个明确的时间窗口来完成生产恢复，并确保 SAP 数据库和中央服务层的另一个可用区域的计算容量可用性。
- 您可以接受将计算容量从非生产重新分配到生产所需的额外时间，作为恢复生产的总体时间窗口的一部分。
- 您可以接受将数据从另一个可用区的 Amazon S3 恢复到 Amazon EBS 所需的时间作为恢复生产的整个时间窗口的一部分。
- 您可以接受在可用区出现故障（包括剩余可用区所需计算容量的可用性出现任何延迟）后将应用程序层恢复到 100% 容量所需的可变持续时间。
- 您可以接受一段时间，即在可用区出现故障或 Amazon 服务严重降级时，只为生产 SAP 数据库和中央 EC2 服务层部署一组计算。

关键设计原则

- 100% 的计算容量部署在可用区 1 中，用于生产 SAP 数据库和中央服务层。
- 100% 的计算容量部署在可用区 1 中，用于生产 SAP 应用程序层。
- 100% 的生产计算容量（SAP 数据库和中央服务）部署在可用区 2 中，供非生产部门在正常操作中使用。
- 为所有实例配置了 Amazon a EC2 uto Recovery，以防出现底层硬件故障。
- SAP 数据库仅保存在单个可用区的 Amazon EBS 上，不会复制到其他可用区。
- Amazon EFS 用于 SAP 全球文件系统。
- SAP 数据库数据会定期备份到 Amazon S3。
- Amazon S3 单区域复制配置为防止逻辑数据丢失。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照。

优点

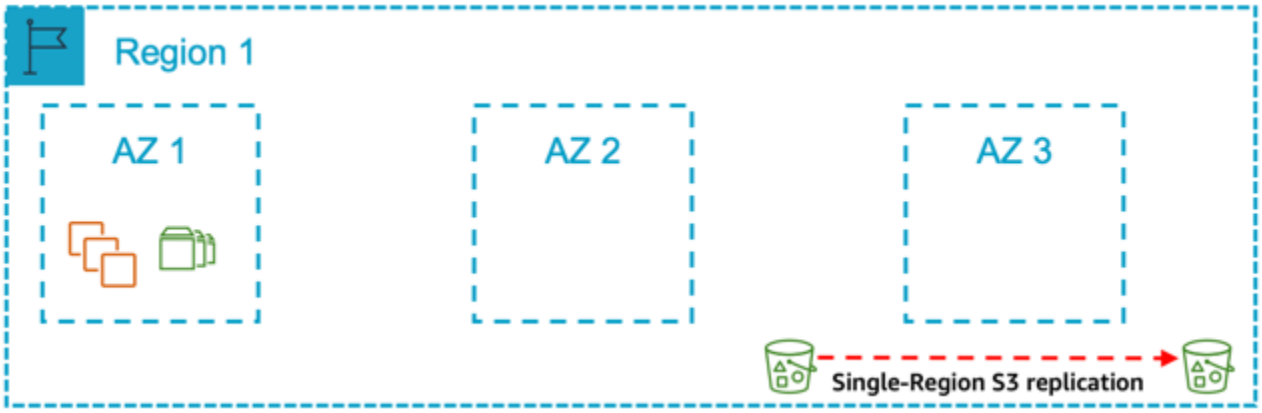
- 通过在生产可用区出现故障时使用非生产容量来优化成本
- 在两个可用区部署所需的计算容量，以实现更可预测的恢复时间

注意事项

- 为了确保可恢复性，需要经过充分记录和测试的流程，用于将所需的计算容量从非生产重新分配到生产以及将数据恢复到不同的可用区。
- 如果可用区故障影响生产，则可能会丢失非生产环境。
- 由于两个可用区之间缺乏高可用性，因此在出现计算故障或可用区故障时恢复生产所需的时间会增加。

模式 4：具有用于生产的单一可用区的单一区域

图 10：具有单个生产可用区的单个区域



在这种模式下，您将所有生产系统部署在一个可用区中，将所有非生产系统部署在同一个可用区或另一个可用区中。您的非生产系统与您的生产系统的大小不同。 *

在以下情况下选择此模式：

- 如果可用区出现故障或 Amazon EC2 服务严重降级，您可以接受与在其他可用区重新创建 AWS 资源并将永久数据恢复到 Amazon EBS 所需的可变时间长度（包括剩余可用区中所需计算容量可用性的任何延迟）相关的风险。
- 您希望通过多可用区方法避免成本影响，并接受生产 SAP 系统停机的相关风险。

关键设计原则

- 100% 的计算容量部署在可用区 1 中，用于生产 SAP 数据库和中央服务层。
- 100% 的计算容量部署在可用区 1 中，用于生产 SAP 应用程序层。
- Amazon EC2 已针对所有实例进行了配置，以防出现底层硬件故障。
- 部署的非生产计算容量低于为生产 SAP 数据库和中央服务层部署的计算容量的 100%。
- SAP 数据库仅保存在单个可用区的 Amazon EBS 上，不会复制到其他可用区。
- Amazon EFS 用于 SAP 全球文件系统。
- SAP 数据库会定期备份到亚马逊 S3。
- Amazon S3 单区域复制配置为防止逻辑数据丢失。
- 所有服务器的 Amazon Machine Image/Amazon EBS 快照都是定期拍摄的。

优点

- 最低成本

- 最简单的设计
- 最简单的操作

注意事项

- 为确保可恢复性，需要在不同可用区扩展 AWS 资源和恢复数据的流程有据可查、经过测试。

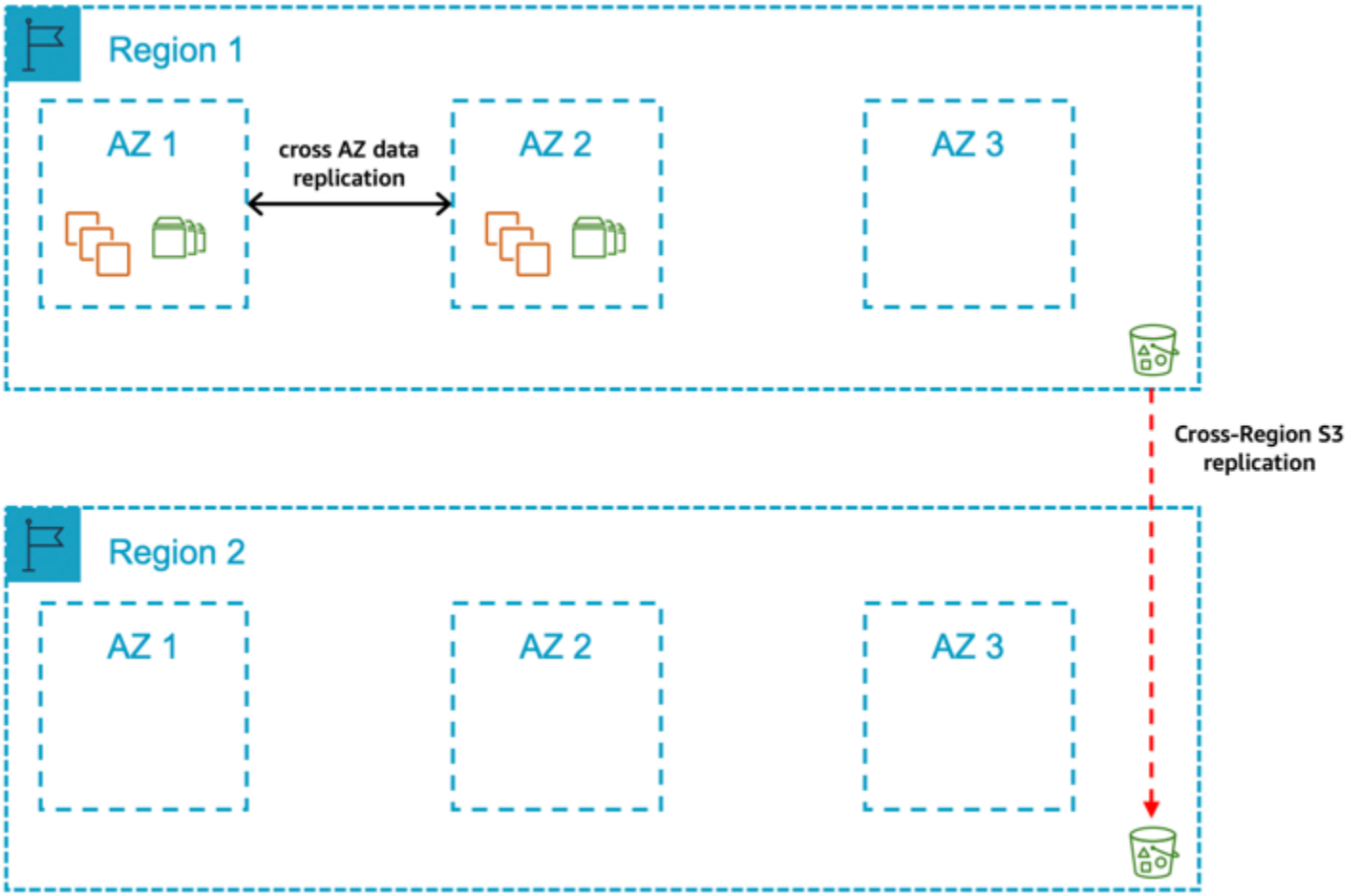
多区域架构模式

如果您需要以下内容，则应选择多区域架构：

- 您要求数据始终位于两个特定的地理 AWS 区域。
- 您可以接受与多区域方法相关的潜在网络延迟注意事项。
- 您可以接受与多区域方法相关的复杂性增加。
- 您可以接受与多区域方法相关的成本影响/差异，包括：
  - AWS 不同 AWS 地区的@@ 服务定价（例如 Amazon EC2）
  - 跨区域数据传输成本
- 第二个区域的额外计算和/或存储成本。

模式 5：一个主区域，其中两个 AZs 用于生产，一个包含备份副本的辅助区域 AMIs

图 11：一个包含两个生产可用区的主区域和一个包含备份副本的辅助区域 AMIs



在这种模式下，您可以在主区域的两个可用区中部署生产系统。在两个可用区中，为生产 SAP 数据库和中央服务层部署的计算大小相同，可在可用区出现故障时自动进行故障转移。SAP 应用程序层所需的计算在两个可用区之间以 50/50 的比例分配。此外，存储在 Amazon S3、Amazon EBS 快照和亚马逊系统映像中的生产数据库备份会复制到辅助区域。如果区域完全出现故障，生产系统将从第二个区域的最后一组备份中恢复。

在以下情况下选择此模式：

- 您需要一个确定的时间窗口来完成生产恢复，并保证主区域内另一个可用区的计算容量可用性，用于生产 SAP 数据库和中央服务层。
- 您可以接受在主区域内的两个可用区为生产 SAP 数据库和中央服务层部署所需的计算和存储的额外成本。
- 您可以接受与跨可用区相关的数据复制费用。
- 您可以接受，可用区之间的自动故障转移需要第三方集群解决方案。

- 如果可用区出现故障或 Amazon EC2 出现重大故障，您可以允许一段时间内只为 SAP 数据库和中央服务部署一组计算。
- 您可以接受，跨可用区进行数据复制需要数据库复制功能或块级复制解决方案。
- 您可以接受所需的可变持续时间（包括剩余可用区中所需计算容量的可用性延迟），以使应用程序层恢复到 100% 的容量。
- 您可以接受在区域出现故障时完成生产恢复所需的可变持续时间。
- 您可以接受与多区域方法相关的复杂性和成本的增加。
- 您可以接受需要手动操作才能在第二个区域恢复生产。

关键设计原则

- 100% 的计算容量部署在可用区 1 和可用区 2 中，用于生产 SAP 数据库和中央服务层。
- 计算容量部署在可用区 1 和可用区 2 中，用于生产 SAP 应用程序层（主动/主动），需要在可用区出现故障或 Amazon EC2 服务严重降级时进行扩展。
- Amazon a EC2 uto reco very 针对所有实例进行了配置，以防范底层硬件故障，但受第三方集群解决方案保护的实例除外。
- Amazon EBS 上与 SAP 数据库相关的数据使用数据库复制功能或块级复制解决方案在可用区之间复制。
- Amazon EFS 用于 SAP 全球文件系统，并在辅助区域进行复制。
- SAP 数据库数据会定期备份到 Amazon S3。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照
- 为了保护逻辑数据丢失，Amazon S3 数据（数据库备份）、Amazon EBS 快照和亚马逊系统映像被复制/复制到辅助区域。

优点

- Amazon EC2 或可用区出现故障时的平均恢复时间 (MTTR) 较低
- Amazon EC2 或可用区出现故障时可预测的恢复服务 (RTS)
- 通过数据库复制功能或块级复制解决方案，将与数据库相关的数据保存在两个可用区的不同 Amazon EBS 卷集上
- 在主区域的两个可用区中部署所需的计算容量
- 在主区域出现可用区故障时，无需依赖从 Amazon S3 恢复数据

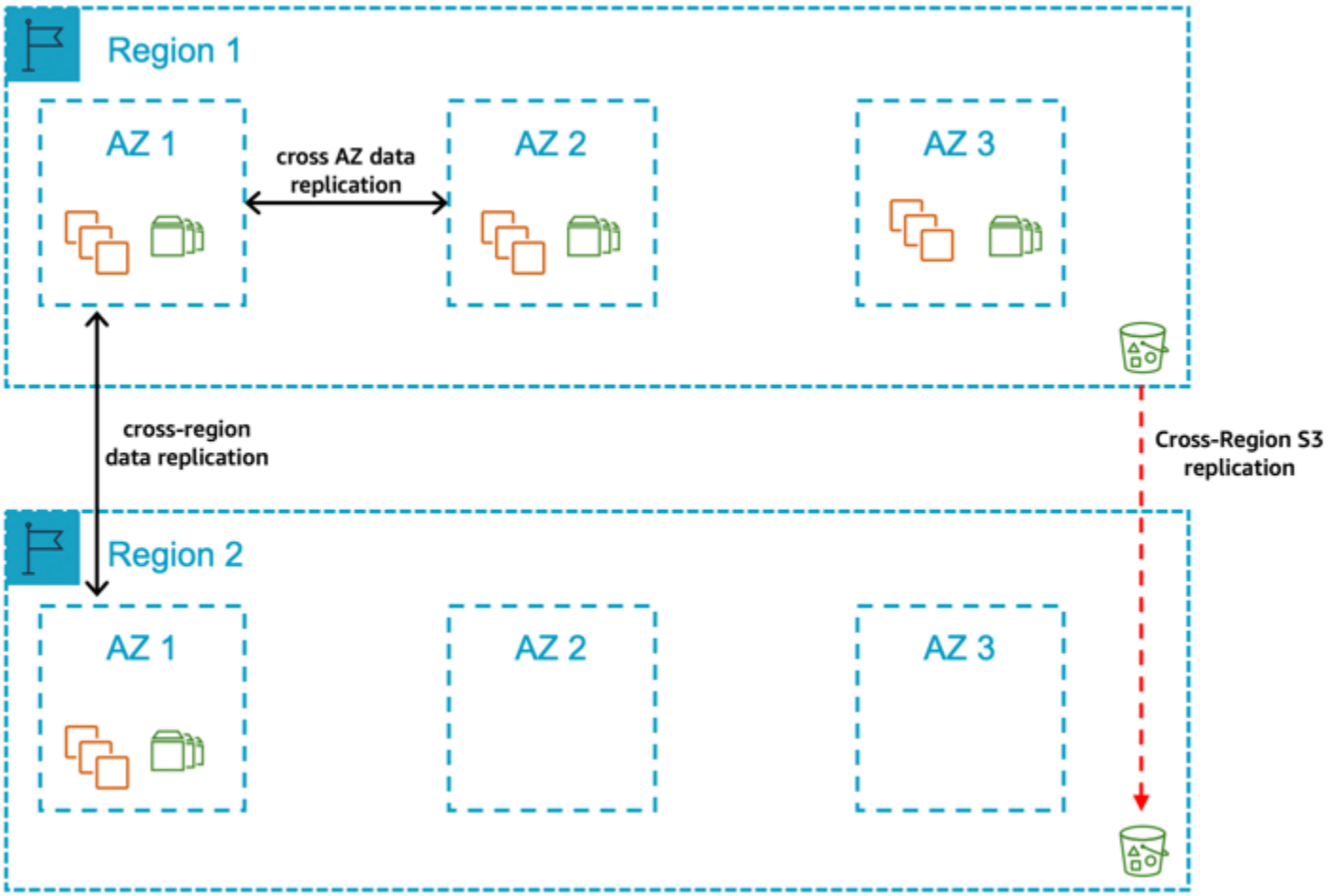
- 能够通过故障转移到数据库和中央服务层的可用区 2 来防范严重降级或可用区整体故障
- 能够通过故障转移到辅助区域来防范严重退化或整个区域故障

注意事项

- 在可用区之间进行自动故障切换需要有据可查和测试的流程。
- 维护自动故障转移解决方案需要经过充分记录和测试的流程。
- 如果可用区出现故障或 Amazon EC2 服务严重降级，则需要经过充分记录和测试的流程来扩展 AWS 资源以使应用程序层恢复到最大容量。
- 扩展 AWS 资源、恢复数据以及将生产转移到次要区域需要有据可查和测试的流程。
- 从您的本地位置到辅助 AWS 区域的网络延迟较高，可能会影响最终用户的性能。

模式 6：一个主区域，其中两个 AZs 用于生产，一个在单个可用区中部署计算和存储容量的辅助区域

图 12：具有两个生产可用区的主区域和一个在单个可用区中部署计算和存储容量的辅助区域



在这种模式下，您可以将所有生产系统部署在主区域的两个可用区中。在两个可用区中，为生产 SAP 数据库和中央服务层部署的计算大小相同，可在可用区出现故障时自动进行故障转移。SAP 应用程序层所需的计算在两个可用区之间以 50/50 的比例分配。您的非生产系统的规模与您的生产系统不相等，并且部署在该区域内的不同可用区中。此外，计算容量部署在辅助区域的可用区 1 中，用于生产 SAP 数据库和中央服务层。使用数据库复制功能或块级复制解决方案将生产数据库复制到辅助区域。

存储在 Amazon S3、Amazon EBS 快照和亚马逊系统映像中的生产数据库备份将复制到辅助区域。如果区域完全出现故障，则将使用数据库层的复制数据以及 SAP 中央服务和应用程序层的最后一组备份，在辅助区域中恢复生产系统。

在以下情况下选择此模式：

- 您需要一个确定的时间窗口来完成生产恢复，并保证主区域内另一个可用区的计算容量可用性，用于生产 SAP 数据库和中央服务层。
- 您可以接受在主区域内的两个可用区为生产 SAP 数据库和中央服务层部署所需的计算和存储的额外成本。
- 您可以接受在主区域的两个可用区为生产 SAP 数据库和中央服务层部署所需的计算和存储而增加的成本。
- 您可以接受与跨可用区相关的数据复制费用。
- 您可以接受，可用区之间的自动故障转移需要第三方集群解决方案。
- 如果可用区出现故障或 Amazon EC2 出现重大故障，您可以允许一段时间内只为 SAP 数据库和中央服务部署一组计算。
- 您可以接受，跨可用区复制数据库相关数据需要数据库复制功能或块级复制解决方案。
- 您可以接受所需的可变持续时间（包括剩余可用区中所需计算容量的可用性延迟），以使应用程序层恢复到 100% 的容量。
- 在区域出现故障时，您需要一个明确的时间窗口才能完成生产恢复。
- 您可以接受与多区域方法相关的复杂性和成本的增加。
- 您需要在辅助区域的单个可用区中为生产 SAP 数据库和中央服务层保证计算容量的可用性。
- 您可以接受在辅助区域的一个可用区的两个可用区中为生产 SAP 数据库和中央服务层部署所需的计算和存储的成本增加。
- 您可以接受需要手动操作才能在区域之间进行故障切换。

关键设计原则

- 100% 的计算容量部署在可用区 1 和可用区 2 中，用于生产 SAP 数据库和中央服务层。

- 100% 的计算容量部署在辅助区域的可用区 1 中，用于生产 SAP 数据库和中央服务层。
- 计算容量部署在可用区 1 和可用区 2 中，用于生产 SAP 应用程序层（主动/主动），需要在可用区出现故障或 Amazon EC2 服务严重降级时进行扩展。
- Amazon a EC2 uto reco very 针对所有实例进行了配置，以防范底层硬件故障，但受第三方集群解决方案保护的实例除外。
- Amazon EBS 上与数据库相关的数据使用数据库复制功能或块级复制解决方案在可用区之间复制。
- Amazon EBS 上与 SAP 数据库相关的数据使用数据库复制功能或块级复制解决方案在区域之间复制。
- Amazon EFS 用于 SAP 全球文件系统并复制到辅助区域。
- SAP 数据库数据会定期备份到 Amazon S3。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照
- 为了防止逻辑数据丢失，Amazon S3 数据（数据库备份）、Amazon EBS 快照和亚马逊系统映像被复制/复制到辅助区域。

优点

- Amazon EC2、可用区或区域出现故障时的平均恢复时间 (MTTR) 较低
- 可预测的恢复服务 (RTS)
- 通过数据库复制功能或块级复制解决方案，将数据库相关数据保存在主区域两个可用区的不同的 Amazon EBS 卷和辅助区域可用区的一组卷上
- 在主区域的两个可用区和辅助区域的一个可用区中部署所需的计算容量
- 在可用区出现故障或区域故障时，无需依赖从 Amazon S3 恢复数据
- 能够通过故障转移到数据库和中央服务层的可用区 2 来防范严重降级或可用区整体故障
- 能够通过故障转移到辅助区域来防范严重退化或整个区域故障

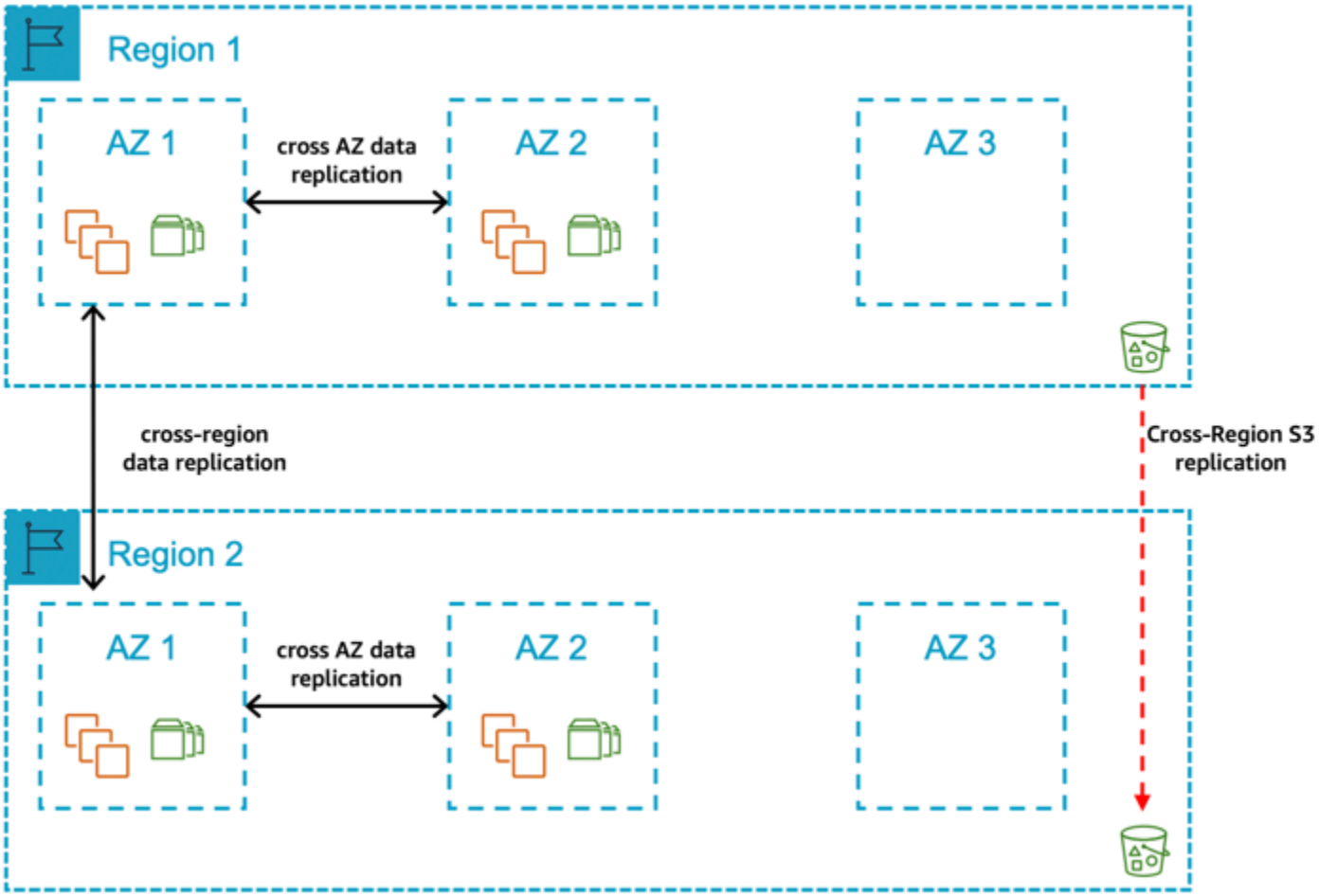
注意事项

- 在可用区之间进行自动故障切换需要有据可查和测试的流程。
- 维护自动故障转移解决方案需要经过充分记录和测试的流程。
- 如果可用区出现故障或 Amazon EC2 服务严重降级，则需要经过充分记录和测试的流程来扩展 AWS 资源以使应用程序层恢复到最大容量。
- 将生产转移到次要区域需要有据可查和经过测试的流程。
- 从您的本地位置到辅助 AWS 区域的网络延迟较高，可能会影响最终用户的性能。

- 在两个不同的区域保持相同的软件版本和补丁级别（操作系统、数据库、SAP）会产生开销。

模式 7：一个主区域，其中两个 AZs 用于生产，另一个是部署计算和存储容量并在两个区域之间进行数据复制的辅助区域 AZs

图 13：具有两个生产可用区的主区域和一个部署了计算和存储容量并在两个可用区之间复制数据的辅助区域



在这种模式下，您可以将所有生产系统部署在主区域的两个可用区中。在两个可用区中，为生产 SAP 数据库和中央服务层部署的计算大小相同，可在可用区出现故障时自动进行故障转移。SAP 应用程序层所需的计算在两个可用区之间以 50/50 的比例分配。此外，您在辅助区域的可用区 1 和可用区 2 中为生产 SAP 数据库和中央服务层部署了计算容量，并且使用数据库复制功能或块级复制解决方案将生产数据库复制到辅助区域。存储在 Amazon S3、Amazon EBS 快照和亚马逊系统映像中的生产数据库备份将复制到辅助区域。如果区域完全出现故障，生产系统将手动移至辅助区域。

在以下情况下选择此模式：

- 您需要一个确定的时间窗口来完成生产恢复，并保证主区域内另一个可用区的计算容量可用性，用于生产 SAP 数据库和中央服务层。
- 您可以接受在主区域内的两个可用区为生产 SAP 数据库和中央服务层部署所需的计算和存储的额外成本。
- 如果可用区出现故障或 Amazon EC2 出现重大故障，您可以允许一段时间内只为 SAP 数据库和中央服务部署一组计算。
- 您可以接受，跨可用区复制数据库相关数据需要数据库复制功能或块级复制解决方案。
- 您可以接受与跨可用区相关的数据复制费用。
- 您可以接受，可用区之间的自动故障转移需要第三方集群解决方案。
- 您可以接受所需的可变持续时间（包括剩余可用区中所需计算容量的可用性延迟），以使应用程序层恢复到 100% 的容量。
- 在区域出现故障时，您需要一个明确的时间窗口才能完成生产恢复。
- 您需要在辅助区域的两个可用区域中确保生产 SAP 数据库和中央服务层的计算容量可用性。
- 您可以接受在辅助区域的两个可用区为生产 SAP 数据库和中央服务层部署所需的计算和存储的额外成本。
- 您可以接受与多区域方法相关的复杂性和成本的增加。
- 您可以接受需要手动操作才能在区域之间进行故障切换。

关键设计原则

- 100% 的计算容量部署在主区域的可用区 1 和可用区 2 中，用于生产 SAP 数据库和中央服务层。
- 100% 的计算容量部署在辅助区域的可用区 1 和可用区 2 中，用于生产 SAP 数据库和中央服务层。
- 计算容量部署在主区域 1 和可用区 2 中，用于生产 SAP 应用程序层（主动/主动），并且需要在可用区故障或 Amazon EC2 服务严重降级时进行扩展。
- Amazon a EC2 uto recovery 针对所有实例进行了配置，以防范底层硬件故障，但受第三方集群解决方案保护的实例除外。
- Amazon EBS 上与 SAP 数据库相关的数据使用数据库复制功能或块级复制解决方案在可用区之间复制。
- Amazon EBS 上与 SAP 数据库相关的数据使用数据库复制功能或块级复制解决方案在区域之间复制。
- Amazon EFS 用于 SAP 全球文件系统，并在辅助区域进行复制。
- SAP 数据库数据定期备份到 Amazon S3 上。
- 所有服务器的 Amazon Machine Image/Amazon EBS 快照都是定期拍摄的。

- 为了防止逻辑数据丢失，Amazon S3 数据（数据库备份）、Amazon EBS 快照和亚马逊系统映像被复制/复制到辅助区域。

优点

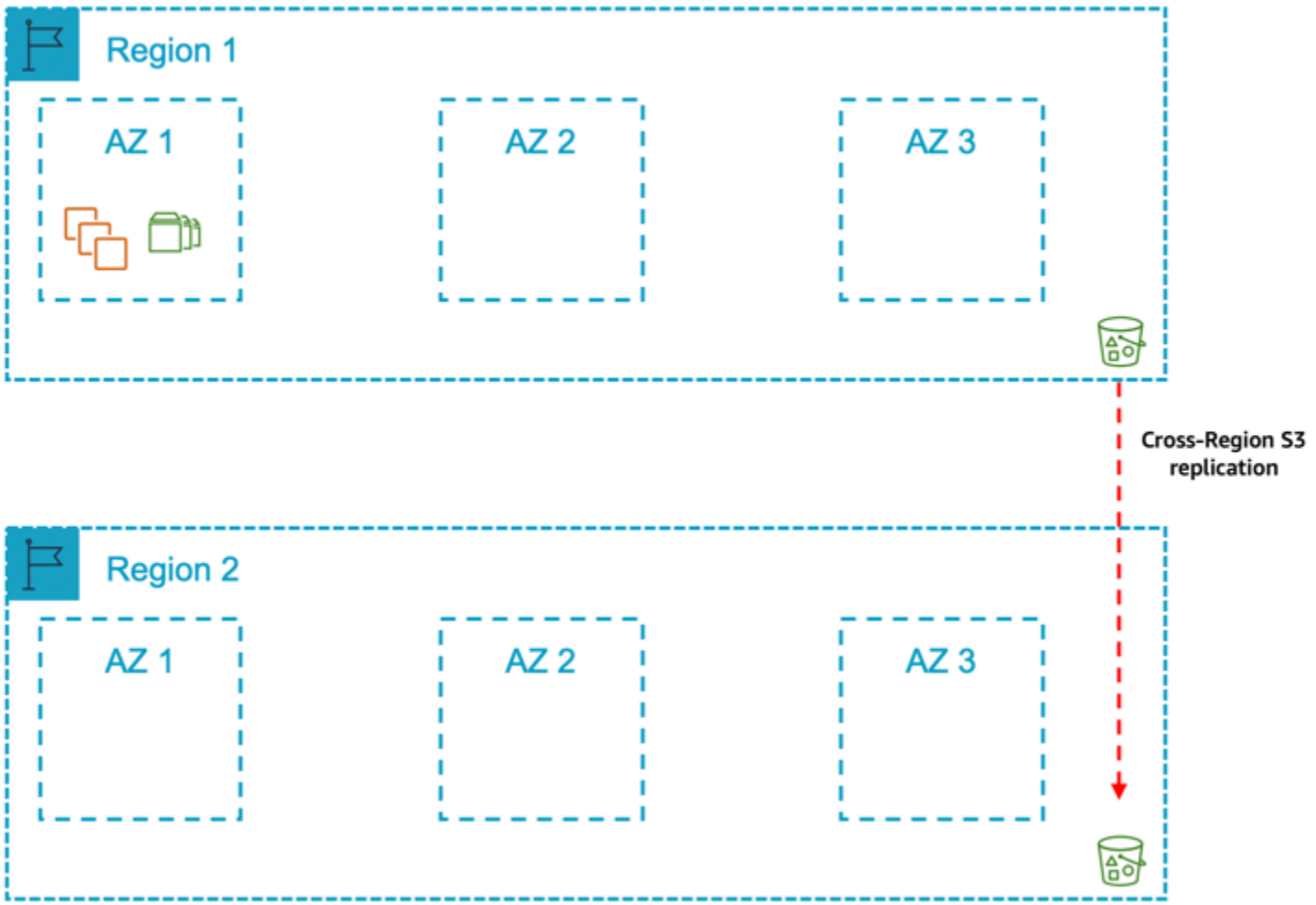
- Amazon EC2、可用区或区域出现故障时的平均恢复时间 (MTTR) 较低
- 可预测的恢复服务 (RTS)
- 通过数据库复制功能或块级复制解决方案，将数据库相关数据保存在主区域两个可用区的不同 Amazon EBS 卷和辅助区域两个可用区的不同 Amazon EBS 卷集上
- 在主区域的两个可用区和辅助区域的两个可用区中部署所需的计算容量
- 在可用区或区域出现故障时，无需依赖从 Amazon S3 恢复数据
- 能够通过故障转移到数据库和中央服务层的可用区 2 来防范严重降级或可用区整体故障
- 能够通过故障转移到辅助区域来防范严重退化或整个区域故障

注意事项

- 在可用区之间进行自动故障切换需要有据可查和测试的流程。
- 维护自动故障转移解决方案需要经过充分记录和测试的流程。
- 如果可用区出现故障或 Amazon EC2 服务严重降级，则需要经过充分记录和测试的流程来扩展 AWS 资源以使应用程序层恢复到最大容量。
- 将生产转移到次要区域需要有据可查和经过测试的流程。
- 从您的本地位置到辅助 AWS 区域的网络延迟较高，可能会影响最终用户的性能。
- 在两个不同的区域保持相同的软件版本和补丁级别（操作系统、数据库、SAP）会产生开销。

模式 8：一个主区域，其中一个用于生产的可用区，一个包含备份副本的辅助区域 AMIs

图 14：一个主区域，其中一个用于生产的可用区，一个包含备份副本的辅助区域 AMIs



在这种模式下，您可以在主区域的一个可用区中部署生产系统。您的非生产系统的规模与您的生产系统不相等，并且部署在该区域内的相同可用区或不同的可用区中。

此外，存储在 Amazon S3、Amazon EBS 快照和亚马逊系统映像中的生产数据库备份会复制到辅助区域。如果区域完全出现故障，生产系统将从第二个区域的最后一组备份中恢复。

在以下情况下选择此模式：

- 如果可用区出现故障或 Amazon EC2 服务严重降级，您可以接受与在其他可用区重新创建 AWS 资源并将永久数据恢复到 Amazon EBS 所需的可变时间长度（包括剩余可用区中所需计算容量可用性的任何延迟）相关的风险。
- 在区域出现故障时，您可以接受与完成生产恢复所需的可变持续时间相关的风险。
- 您希望通过多可用区方法避免成本影响，并接受生产 SAP 系统停机的相关风险。
- 您可以接受与多区域方法相关的复杂性和成本的增加。
- 您可以接受需要手动操作才能恢复辅助区域的生产。

关键设计原则

- 100% 的计算容量部署在可用区 1 中，用于生产 SAP 数据库和中央服务层。
- 100% 的计算容量部署在可用区 1 中，用于生产 SAP 应用程序层。
- 为所有实例配置了 Amazon a EC2 uto Reco very，以防出现底层硬件故障。
- 部署的非生产计算容量低于为生产 SAP 数据库和中央服务层部署的计算容量的 100%。
- SAP 数据库仅保存在单个可用区的 Amazon EBS 上，不会使用数据库复制功能或块级复制解决方案复制到其他可用区。
- Amazon EFS 用于 SAP 全球文件系统。
- SAP 数据库会定期备份到 Amazon S3。
- Amazon S3 的配置是为了防止逻辑数据丢失。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照。
- 为了防止逻辑数据丢失，Amazon S3 数据（数据库备份）、Amazon EBS 快照和亚马逊系统映像被复制/复制到辅助区域。

优点

- 与多可用区相比，成本更低
- 能够通过故障转移到辅助区域来防范严重退化或整个区域故障

注意事项

- 如果可用区出现故障或 Amazon EC2 服务严重降级，则需要经过充分记录和测试的流程来扩展 AWS 资源，使 SAP 应用程序层恢复到最大容量。
- 扩展 AWS 资源、恢复数据以及将生产转移到次要区域需要有据可查和测试的流程。
- 从您的本地位置到辅助 AWS 区域的网络延迟较高，可能会影响最终用户的性能。
- 如果由于两个可用区之间缺乏高可用性而导致计算、可用区或区域出现故障，则恢复生产所需的时间会增加。

摘要

下表汇总了这些模式及其主要特征。

#	单个区域	多区域	单可用区主可用区	多可用区主可用区	单个 AZ 第二区域	多可用区第二区域	第 2 个亚利桑那州的生产能力	非生产能力的使用	跨区域数据复制
1	是	否	否	是	否	否	是	否	否
2	是	否	否	是	否	否	是	是	否
3	是	否	是	否	否	否	否	是	否
4	是	否	是	否	否	否	否	否	否
5	否	是	否	是	是	否	是	否	是
6	否	是	否	是	是	否	是	否	是
7	否	是	否	是	否	是	是	否	是
8	否	是	是	否	是	否	否	否	是

表 1：模式摘要

借助 AWS 云的灵活性和敏捷性，您可以选择本指南中描述的任何模式。您可以选择最能满足 SAP 系统业务需求的模式。它使您免于选择最高要求并将其应用于所有生产系统的麻烦。

例如，如果您需要在另一个可用区中为核心 ERP 系统的生产 SAP 数据库和中央服务层以及 BW 系统提供高度可用的计算容量，则可以接受在不同的可用区中重新创建 AWS 资源并恢复永久数据所需的可变持续时间。在这种情况下，您可以为 ERP 选择模式 3，为 BW 选择模式 1 以降低总体拥有成本。

如果您的需求随着时间的推移而发生变化，则无需进行大量重新设计即可转移到不同的模式。例如，在实施项目的早期阶段，您可能不需要其他可用区的高可用计算容量，但可以在上线前几周将容量部署到第二个可用区。

在选择运行 SAP 系统的架构模式时，应考虑以下几点 AWS：

- 数据的地理驻留地
- 生产 SAP 系统停机对组织的影响

- 恢复时间目标
- 恢复点目标
- 成本概况

SAP 谈微软 SQL 服务器的 AWS 架构模式

本文档提供了有关在 Microsoft SQL 服务器上的 AWS 云端部署 SAP 工作负载的架构模式的信息。在考虑恢复时间和恢复点目标的同时，这些模式提供了高可用性和弹性的实施选项。

从业务需求向后推进，定义一种满足 SAP 系统和数据可用性目标的方法。对于每种故障场景，弹性要求、可接受的数据丢失和平均恢复时间都必须与组件和支持的业务应用程序的关键程度成正比。

您可以根据自己的特定业务标准自定义这些模式。在选择模式时，您应该考虑每种故障类型的风险和影响，以及缓解成本。

主题

- 模式
- 比较矩阵
- 微软 SQL 服务器的单区域架构模式
- 微软 SQL 服务器的多区域模式

模式

架构模式分为两类。

- 单区域模式
- 多区域模式

比较矩阵

下表对进一步讨论的所有架构模式进行了比较。

图案	业务需求			解决方案特征		实施详情	
	弹性类型	恢复点目标	恢复时间目标	成本	复杂性	SQL AlwaysOn	亚马逊 S3 复制

图案 1	单区域灾难恢复	接近零*	低	中	中	2 层	不适用
图案 2		中	高	非常低	非常低	不适用	不适用
图案 3	多区域灾难恢复	中	高	中	中	2 层	跨区域
图案 4		接近零*	低	高	高	3 层	跨区域
图案 5		中	高	低	低	不适用	跨区域
图案 6		低	低	中	中	不适用	不适用

*要实现接近零的恢复点目标，必须在同一 AWS 区域内以同步数据提交模式设置数据库复制。

微软 SQL 服务器的单区域架构模式

单区域架构模式可帮助您避免网络延迟，因为您的 SAP 工作负载组件位于同一区域内的近距离位置。每个 AWS 区域通常都有三个可用区。有关更多信息，请参阅AWS 全球基础设施地图。

当您需要确保 SAP 数据位于数据主权法律规定的区域边界内时，您可以选择这些模式。

以下是两种单一区域架构模式。

模式

- 模式 1：具有两个生产可用区的单一区域
- 模式 2：具有一个生产可用区的单一区域

模式 1：具有两个生产可用区的单一区域

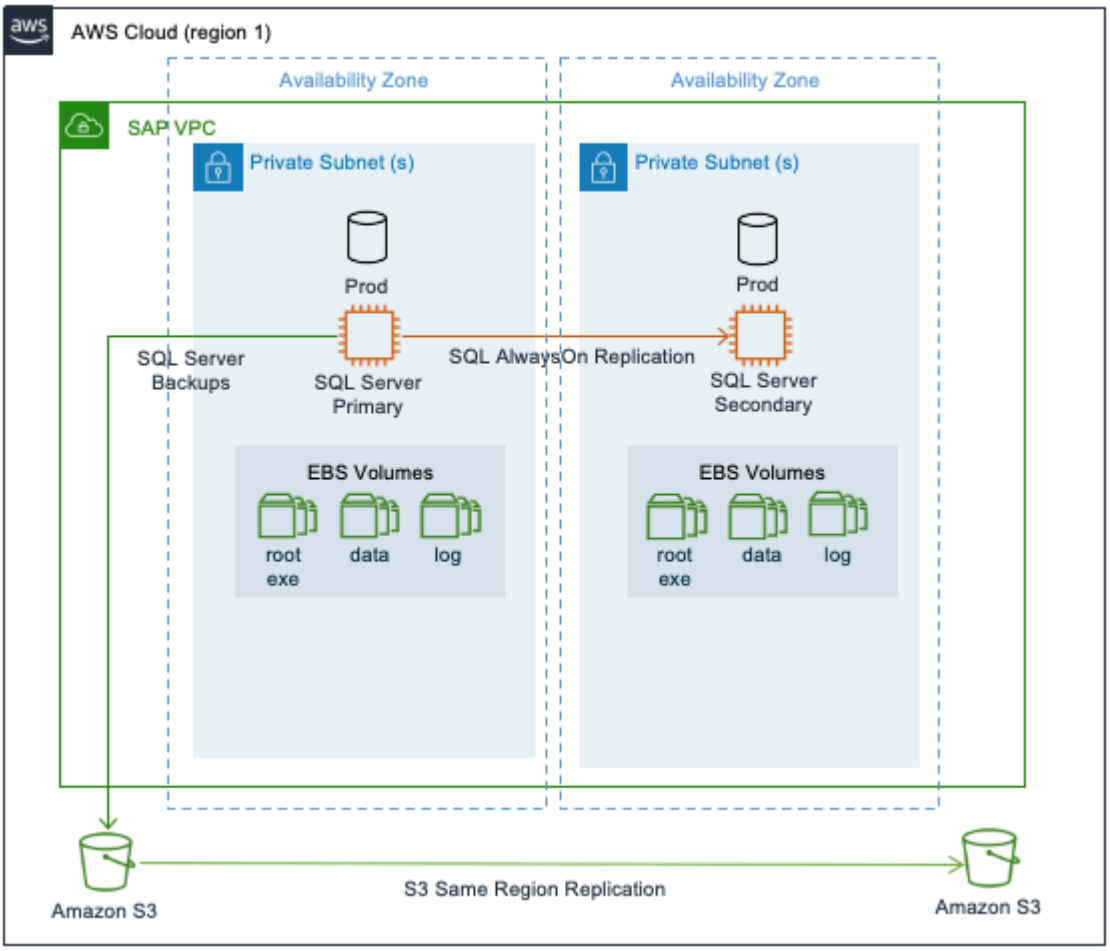
在这种模式下，你的 Microsoft SQL 服务器部署在两个可用区中，两个实例上都 AlwaysOn 进行了配置。主实例和辅助实例的实例类型相同。辅助实例可以在active/passive or active/active模式下部署。我们建议使用同步复制模式实现两个可用区之间的低延迟连接。

如果您正在寻找用于自动故障转移的高可用性群集解决方案，以实现接近零的恢复点和时间目标，则这种模式是基础。 AlwaysOn 带有 Windows 群集的 SQL 可实现自动故障转移，可针对故障情况（包括罕见的可用区丢失）提供弹性。

您需要考虑 AlwaysOn 配置许可的额外成本。此外，将生产等效实例类型配置为备用实例会增加总拥有成本。

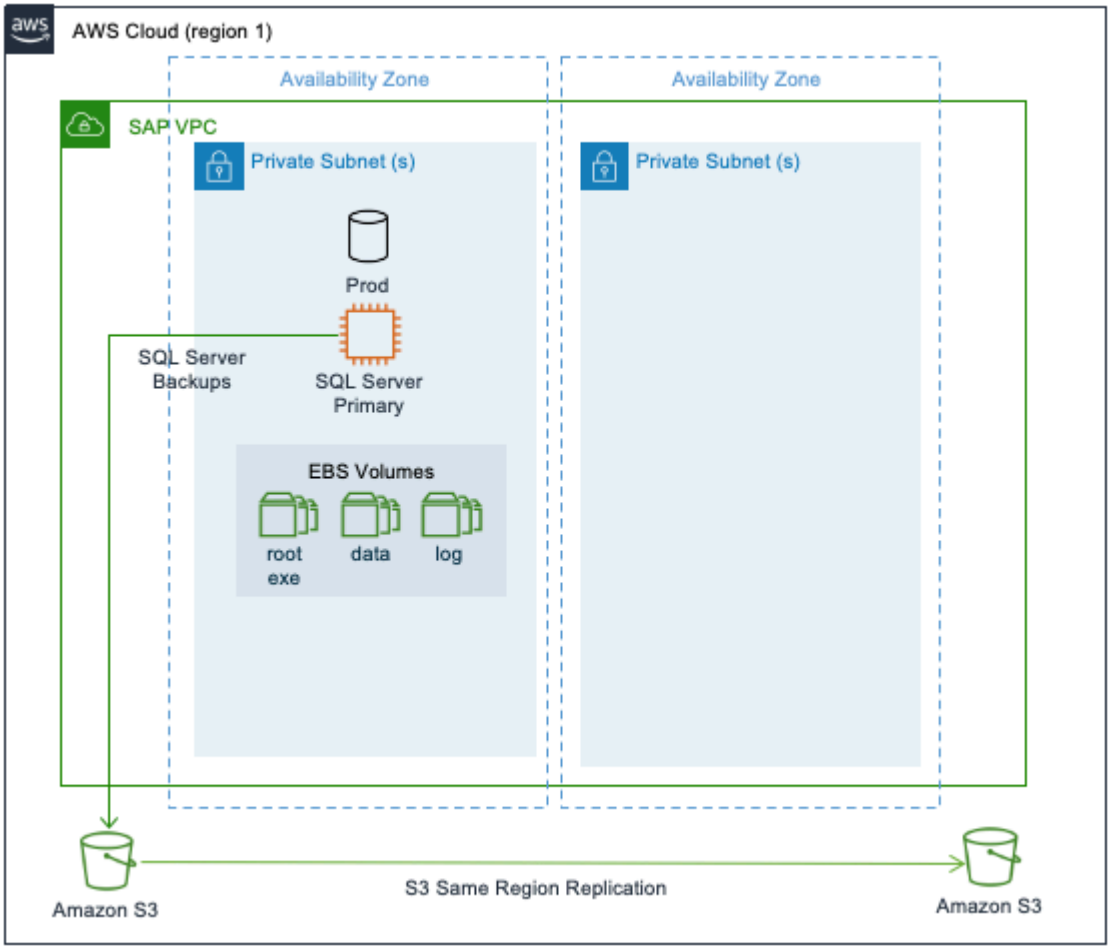
微软 SQL 服务器备份可以存储在亚马逊 S3 存储桶中。Amazon S3 对象自动存储在多个设备上，跨越一个区域中至少三个可用区。为了防止逻辑数据丢失，您可以使用 Amazon S3 的同区域复制功能。

通过同区域复制，您可以在单独的 AWS 账户中设置自动复制 Amazon S3 存储桶。此策略可确保并非所有数据副本都因恶意活动或人为错误而丢失。要设置同区域复制，请参阅设置复制。



模式 2：具有一个生产可用区的单一区域

在这种模式下，Microsoft SQL Server 作为独立安装进行部署，没有用于复制数据的目标系统。这是最基本、最具成本效益的部署选项。在故障情况下，可用来恢复业务运营的选项有 Amazon a EC2 uto recovery（在实例出现故障时），或者在出现影响可用区的重大问题时，通过从最新有效的备份中恢复和恢复。



微软 SQL 服务器的多区域模式

AWS 全球基础设施横跨全球多个地区，而且这种足迹在不断增加。有关最新更新，请参阅AWS 全球基础架构。如果您希望在任何给定时刻将 SAP 数据驻留在多个区域，以确保在出现故障时提高可用性并最大限度地减少停机时间，则应选择多区域架构模式。

在部署多区域模式时，您可以从使用集群解决方案等自动化方法中获益，在可用区之间进行故障转移，从而最大限度地减少总体停机时间并消除人为干预的需求。多区域模式不仅提供高可用性，还提供灾难恢复，从而降低总体成本。所选区域之间的距离会直接影响延迟，因此，在多区域模式中，在整体设计中必须考虑这一点。

跨区域复制或数据传输还会产生额外的成本影响，这些影响也需要考虑在解决方案的总体定价中。不同地区的定价各不相同。

以下是四种多区域架构模式。

模式

- 模式 3：主区域有两个生产可用区，辅助区域带有备份副本/ AMIs
- 模式 4：主区域有两个生产可用区，辅助区域将计算和存储容量部署在单个可用区中
- 模式 5：主区域有一个用于生产的可用区和一个带有备份副本的辅助区域 AMIs
- 模式 6：使用 Ela AWS stic 灾难恢复在区块级别复制的主区域，一个用于生产的可用区和一个辅助区域

模式 3：主区域有两个生产可用区，辅助区域带有备份副本/ AMIs

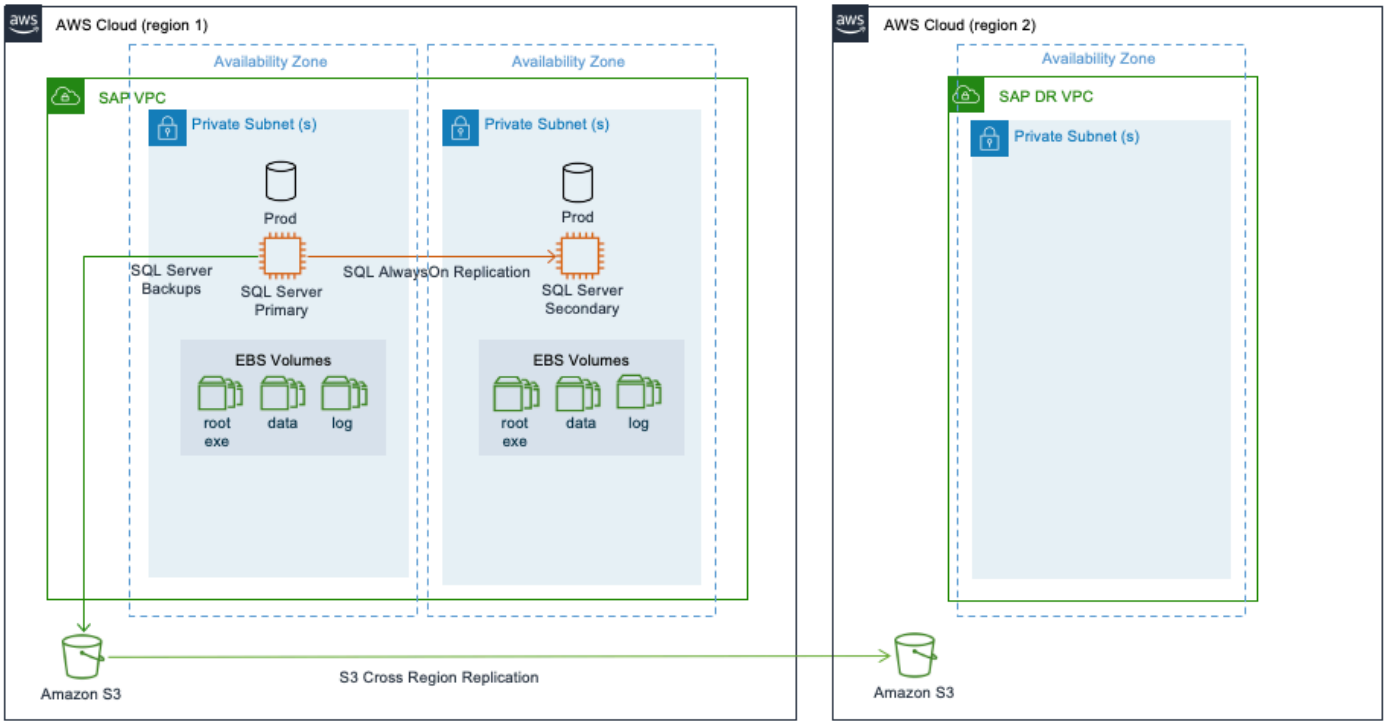
这种模式与模式 1 类似，在这种模式中，你的 Microsoft SQL 服务器具有高可用性。您可以使用在主区域的两个可用区中部署生产实例 AlwaysOn。您可以使用存储在 Amazon S3、Amazon EBS 和亚马逊系统映像 (AMIs) 中的备份副本在辅助区域中恢复 SQL 数据库。

通过跨区域复制存储在 Amazon S3 中的文件，存储在存储桶中的数据会自动（异步）复制到目标区域。可以在区域之间复制 Amazon EBS 快照。有关更多信息，请参阅复制 Amazon EBS 快照。您可以使用 AWS CLI、 AWS 管理控制台或 Amazon 在区域内 AWS SDKs 或跨区域复制 AMI EC2 APIs。有关更多信息，请参阅复制 AMI。您还可以使用 AWS Backup 来计划和运行跨区域的快照和复制。

如果区域完全失败，则需要使用 AMI 在辅助区域中构建生产 SQL 服务器。您可以使用 AWS CloudFormation 模板自动启动新 SQL Server。实例启动后，您可以从 Amazon S3 下载最后一组备份，将您的 SQL 服务器恢复到灾难事件发生 point-in-time前的状态。在辅助区域恢复并恢复 SQL 服务器后，您可以使用 DNS 将客户端流量重定向到新实例。

此架构为您提供了跨多个可用区实施 SQL Server 的优势，并且能够在出现故障时立即进行故障转移。对于主区域之外的灾难恢复，恢复点目标受您在 Amazon S3 存储桶中存储 SQL 备份文件的频率以及将 Amazon S3 存储桶复制到目标区域所花费时间的限制。您可以使用 Amazon S3 复制时间控制进行有时限的复制。有关更多信息，请参阅启用 Amazon S3 复制时间控制。

您的恢复时间目标取决于在辅助区域中构建系统以及从备份文件恢复操作所需的时间。时间长短将根据数据库的大小而有所不同。此外，在没有预留实例容量的情况下，获得恢复过程的计算容量所需的时间可能会更长。当您需要在一个区域内实现尽可能低的恢复时间和恢复点目标，而在主区域之外进行灾难恢复需要较高的恢复点和时间目标时，这种模式非常适合。



模式 4：主区域有两个生产可用区，辅助区域将计算和存储容量部署在单个可用区中

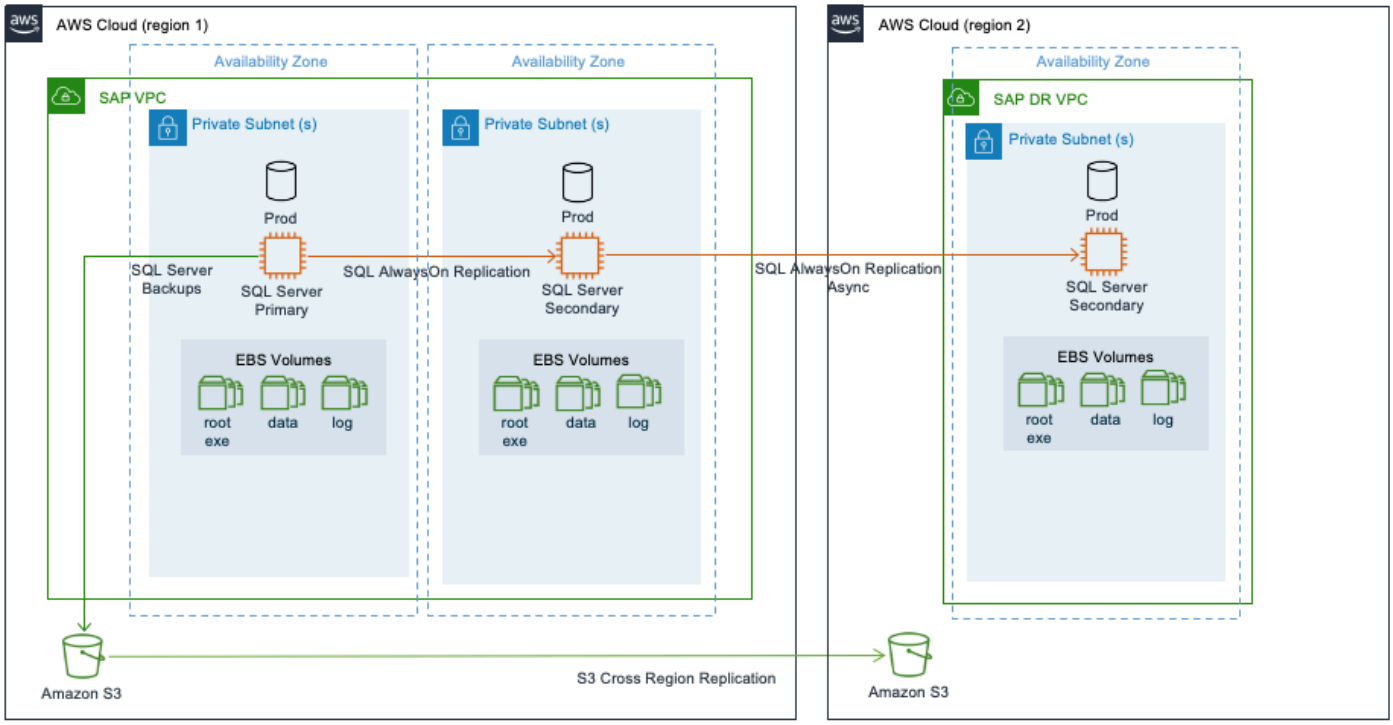
除了模式 3 的架构外，这种模式还在主区域的 SQL Server 和辅助区域的其中一个可用区中的相同第三个实例之间 AlwaysOn 设置 SQL。由于延迟增加，我们建议在 AWS 区域之间复制 AlwaysOn 时对 SQL 使用异步（异步）模式。

如果主区域出现故障，生产工作负载将手动故障转移到辅助区域。这种模式可确保您的 SAP 系统具有高可用性和容灾能力。这种模式通过连续的数据复制提供了更快的故障转移和业务运营的连续性。

在辅助区域中为生产 SQL Server 部署所需的计算和存储以及区域之间的数据传输成本会增加。当您需要在主区域之外进行灾难恢复且恢复点和时间目标较低时，此模式非常适合。

这种模式既可以部署在多层复制配置中，也可以部署在多目标复制配置中。

下图显示了多层复制，其中以链式方式配置复制。

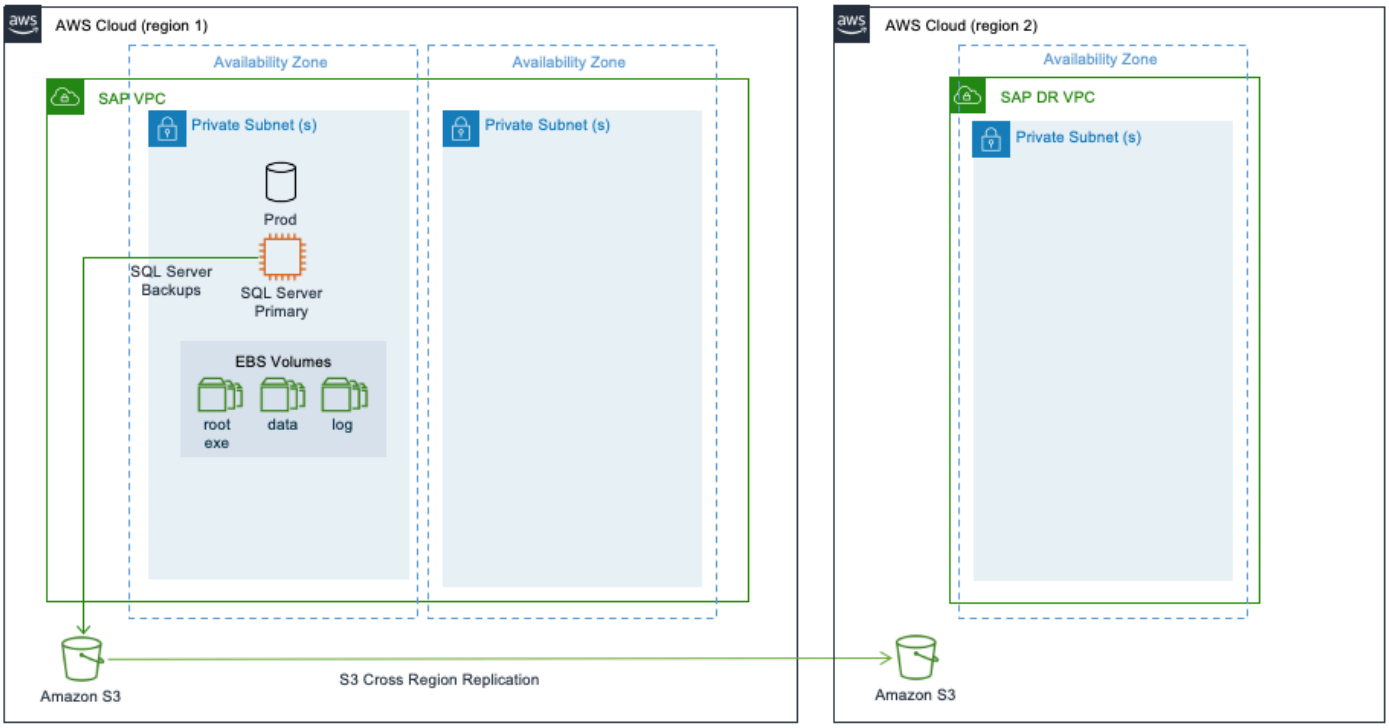


模式 5：主区域有一个用于生产的可用区和一个带有备份副本的辅助区域 AMIs

这种模式与模式 2 类似，在次要区域中进行额外的灾难恢复，该区域包含存储在 Amazon S3 中的 SQL Server 备份副本、Amazon EBS 快照和中的副本。 AMIs在这种模式下，SQL Server 作为独立安装部署在主区域的一个可用区中，没有目标 SQL 系统可以复制数据。

在这种模式下，您的 SQL 服务器可用性不高。如果区域完全失败，则需要使用 AMI 在辅助区域中构建生产 SQL 服务器。您可以使用 AWS CloudFormation 模板自动启动新 SQL Server。实例启动后，您可以从 Amazon S3 下载最后一组备份，将您的 SQL 服务器恢复到灾难事件发生 point-in-time前的状态。然后，您可以使用 DNS 将您的客户端流量重定向到辅助区域中的新实例。

对于主区域之外的灾难恢复，恢复点目标受您在 Amazon S3 存储桶中存储 SQL 备份文件的频率以及将 Amazon S3 存储桶复制到目标区域所花费时间的限制。您的恢复时间目标取决于在辅助区域中构建系统以及从备份文件恢复操作所需的时间。时间长短将根据数据库的大小而有所不同。这种模式适用于可以容忍恢复正常运行所需的停机时间的非生产或非关键生产系统。



模式 6：使用 Ela AWS stic 灾难恢复在区块级别复制的主区域，一个用于生产的可用区和一个辅助区域

AWS Elastic 灾难恢复通过在云上 AWS 启用基于云的灾难恢复，为组织提供了一种保护 Microsoft SQL Server 环境的现代方法。有关更多信息，请参阅什么是 Elastic 灾难恢复？

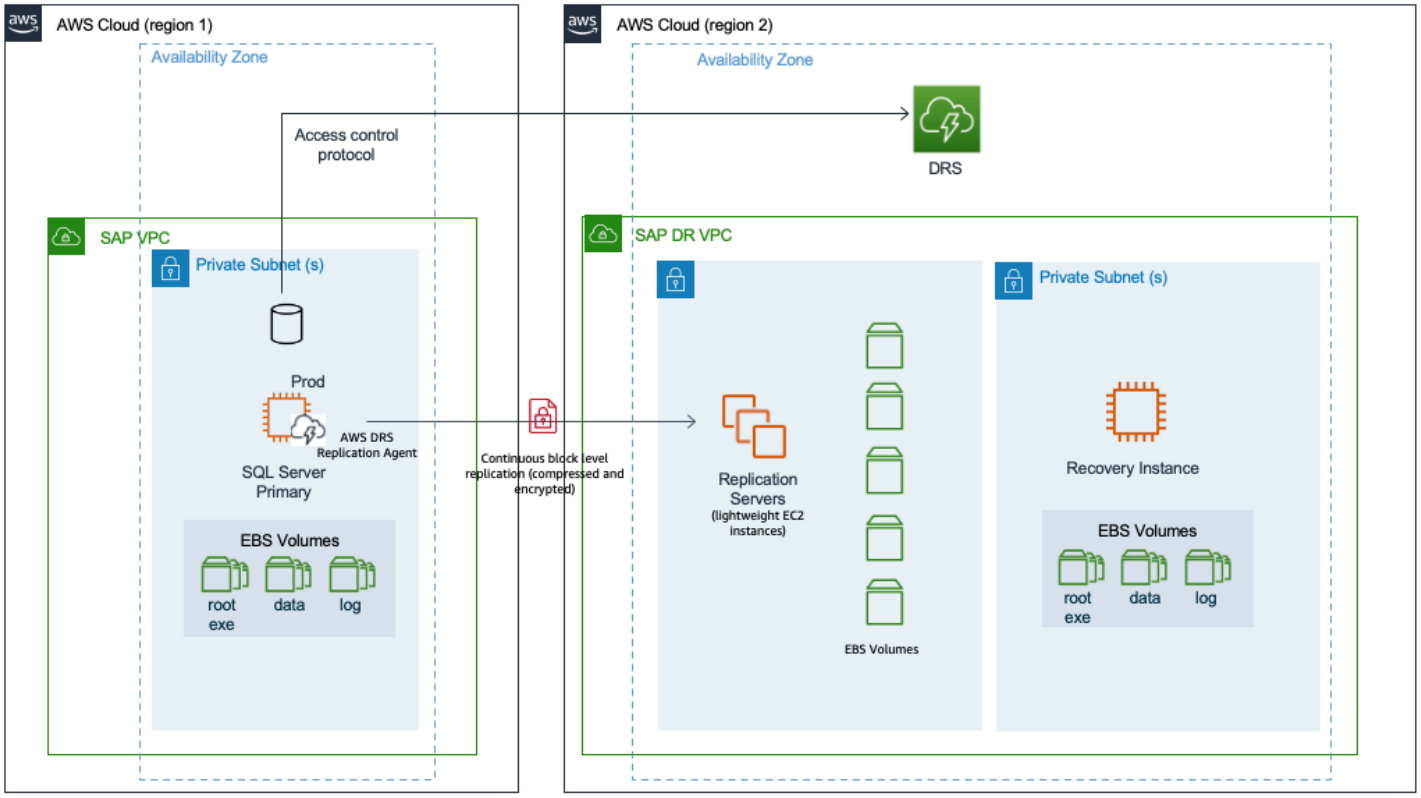
Elastic 灾难恢复使用块级复制，为支持的 Windows 和 Linux 操作系统版本复制操作系统、数据库、应用程序和系统文件。要了解更多信息，请参阅支持的操作系统。Elastic 灾难恢复需要在源系统上初始设置 AWS 复制代理，才能启动安全的数据复制。代理在内存中运行并识别对本地连接的磁盘的写入操作。这些写入操作会被捕获并异步复制到您 AWS 账户中的暂存区域。在此持续的复制过程中，Elastic Disaster Recovery 会维护同一源服务器中所有磁盘的写入顺序。复制的 Amazon EC2 实例可以在测试模式下运行，以便在隔离的环境中执行演练。

Elastic 灾难恢复允许您监控恢复实例的数据复制状态、查看恢复实例的详细信息、向 Elastic 灾难恢复添加恢复实例、编辑恢复实例故障恢复设置以及终止恢复实例。

借助 Elastic 灾难恢复，您可以通过在 AWS 云上启动恢复实例来执行故障转移。启动恢复实例后，必须将流量从主站点重定向到恢复站点。

AWS Elastic 灾难恢复使用 Amazon EBS point-in-time 快照拍摄暂存区域内保存的数据的快照。要了解更多信息，请参阅 Amazon EBS 快照。然后，它提供了崩溃一致的 point-in-time恢复选项，可以在

发生灾难或演习时使用。弹性灾难恢复可以保护 SQL Server Always On 可用性组的各个节点。在灾难恢复期间，该组将作为单个 SQL Server 实例启动 AWS。此解决方案适用于任何支持的 SQL Server 版本的 SQL Server 标准版和 SQL Server 企业版。



AWS 使用 AWS 弹性灾难恢复对 SAP 工作负载进行灾难恢复

自然事件（地震、飓风或洪水）、应用程序故障、技术故障或人为行为造成的灾难会导致应用程序停机和潜在的数据丢失，从而影响收入。为了缓解此类情况，您可以制定以灾难恢复为关键要素的业务连续性计划。设计、实施和维护灾难恢复计划对于运行任务关键型应用程序（例如 SAP）的组织至关重要。有关更多信息，请参阅业务连续性计划 (BCP)。

AWS Elastic 灾难恢复使组织能够快速轻松地实施新的灾难恢复计划或将现有的灾难恢复计划迁移到 AWS。源服务器可以托管在 AWS现有的物理或虚拟数据中心、私有云或其他云提供商上。我们建议使用 Elastic 灾难恢复为您的 SAP 工作负载实施灾难恢复计划，灾难恢复环境在 AWS 哪里，源环境可能处于开启状态，也可能未启用 AWS。您可以从 Elastic 灾难恢复控制台访问 Elastic 灾难恢复。

Elastic 灾难恢复需要在源系统上初始设置 AWS 复制代理，才能启动安全的数据复制。您的数据将使用安全协议直接通过互联网或通过加密和/或专用网络连接复制到 Elastic 灾难恢复支持的任何 AWS 区域。通过将源系统复制到暂存区的复制服务器，通过使用经济实惠的存储、共享服务器和最少的计算资源来维护持续的复制，从而优化灾难恢复的成本。

您可以执行无中断测试（称为演练），以确认您的 Elastic 灾难恢复实施已为灾难恢复场景做好准备。当您启动用于演练或恢复的实例 AWS 时，Elastic Dasaster Recovery 会自动将您的服务器转换为启动并在本地运行。该服务还会在服务器复制时自动创建服务器状态的时间点 (PIT) 快照。如果您需要恢复应用程序，则可以使用最新的快照或较早的 PIT 快照在几分钟 AWS 内启动恢复实例。应用程序运行后 AWS，您可以选择将其保留在原处，或者在问题解决后启动数据复制回主站点。您可以使用 Elastic 灾难恢复工具（例如 Failback Client）回切到主站点。

有关更多信息，请参阅什么是 Elastic 灾难恢复？

主题

- 场景
- 参考信息
- 服务级别协议和 SAP 许可证
- 网络、存储和计算
- 灾难恢复场景
- 共享存储弹性
- 在 AWS 云上为 SAP 工作负载实施灾难恢复

场景

本文档涵盖以下灾难恢复方案。

- 区域内 — 源工作负载在 AWS 云上运行，灾难恢复实施使用同一 AWS 区域中的第二个可用区。
- 跨区域 — 源工作负载在 AWS 云上运行，灾难恢复实施使用不同的 AWS 区域。选择其他地区可能是出于合规原因。
- 外部 AWS — 源工作负载在外部 AWS（本地、公共云或私有云）运行，并使用实现灾难恢复 AWS。

参考信息

本文档未提供设置和使用 AWS Elastic 灾难恢复的详细步骤。有关更多信息，请参阅什么是 DRSlong;？ 在《 AWS 弹性灾难恢复用户指南》中。

了解指导灾难恢复解决方案设计和实施的关键业务要求非常重要，包括恢复点目标、恢复时间目标以及灾难恢复计划和灾难恢复演习。请查看以下资源，了解与灾难恢复实施相关的概念 AWS。

- AWS 弹性灾难恢复核心概念
- AWS Well-Architected 框架：最佳实践 10.1
- SAP 上可用性和可靠性的架构指南 AWS

如果您不熟悉 AWS，请参阅以下文档。

- 入门 AWS
- 什么是亚马逊 EC2？
- Amazon VPC 是什么？
- Amazon Elastic Block Store（Amazon EBS）

要有效地使用此处提供的这些信息，您必须具有安装、迁移和操作 SAP 环境和系统的经验 AWS，以及高可用性和灾难恢复解决方案的实施经验。

服务级别协议和 SAP 许可证

对于灾难恢复实施，服务级别协议 (SLA) 用于定义系统在避免数据丢失和减少因灾难事件导致工作负载不可用时的停机时间方面的弹性。

SAP 系统灾难恢复方法需要复制应用程序层、数据库层和任何文件共享，例如 NFS 装载。以下是实施灾难恢复时需要考虑的一些因素。

主题

- 恢复时间目标（RTO）
- 恢复点目标 (RPO)
- 恢复一致性目标 (RCO)
- SAP 许可证

恢复时间目标（RTO）

恢复时间目标 (RTO) 是指应用程序在中断后能够以多快的速度恢复。在发生灾难时，Elastic Daser Recovery 使您能够在几分钟内将复制的服务器启动到目标区域的完全配置状态并继续运行。这种自动化方法支持低 RTO。它可能比手动方法更快、更有效。

考虑

由于通常根据对业务流程的影响来评估 RTO，因此其他因素，例如域名系统 (DNS) 传播、环境因素，包括灾难恢复团队的反应时间、目标环境的存储架构、操作系统启动和应用程序启动时间，都会影响该目标值。

恢复点目标 (RPO)

Elastic Disaster Recovery 会持续将区块级别的磁盘更改异步复制到目标站点。Elastic 灾难恢复的 RPO 通常在亚秒范围内。RPO 可能受到外部因素的影响，例如源系统将更改发送到暂存区域所花费的时间。源系统上的交易量进一步影响了这一点。其他因素包括网络吞吐量和延迟、源服务器和复制服务器性能等。应衡量这些因素，以计算灾难恢复事件期间可能丢失的数据量。

考虑

由于 Elastic 灾难恢复管理某些场景的方式，SAP 工作负载可能不时观察到的数据丢失量可能比亚秒的 RPO 更长。

如果发生硬重启、磁盘更改和崩溃，Elastic 灾难恢复会触发磁盘的重新扫描。在重新扫描期间，复制代理不会将源服务器的更改复制到目标服务器。这会在两台服务器之间造成延迟。如果主系统在这段时间内出现故障，客户遭受的数据丢失量（以 RPO 衡量）可能会比预期的要长。

重新扫描的时间取决于多个因素，如果不进行测试就无法预测。重新启动源服务器后，可能会进行重新扫描。重新扫描的时间将根据源磁盘的大小而有所不同。时间取决于磁盘的性能（线性读取）、暂存区

磁盘性能以及源服务器上的写入操作速率（与重新扫描并行发送）。只要向前移动，重新扫描就会正常运行，并且没有 “卡住”。

SAP 数据库的磁盘大小可能很大，更改率也很高。我们建议进行测试，以确保在此类事件中满足您的 SLA 要求。此外，您必须确保主数据库和目标数据库在高峰活动周期内保持同步。

恢复一致性目标 (RCO)

许多灾难恢复解决方案在弹性方面只考虑 RTO 和 RPO SLAs 。您还必须考虑 SAP 工作负载的恢复一致性目标 (RCO)。RCO 是衡量相互关联系统中分布式业务数据一致性的指标。在典型的客户环境中，SAP 系统紧密集成，这些系统之间经常交换数据，例如 SAP ECC 或 SAP S/4HANA、SAP BW 或 SAP BW/4HANA、SAP CRM、SAP SRM、SAP GTS 等。这组紧密集成的系统称为系统组。在灾难恢复故障转移的情况下，系统组内的 RCO 要求可能为零。这意味着，在灾难恢复故障转移的情况下，必须将 SAP 系统组中的所有数据库恢复到相同的状态 point-in-time。

考虑

Elastic 灾难恢复并不能保证多个源实例之间的一致性。如果您的 RCO 要求为零，则可以使用数据库本机复制技术进行 point-in-time恢复，也可以使用回溯技术进行二次时空旅行。

有关更多信息，请参阅 SAP Note 434647——在 SAP 系统组中 Point-in-time恢复（需要 SAP 门户访问权限）。

SAP 许可证

SAP 系统由使用硬件密钥的许可证保护。开启 AWS，硬件密钥基于您的 Amazon EC2 实例 ID。必须先启动您的 Amazon EC2 实例，然后才能生成 SAP 许可证。当您在灾难恢复站点中恢复 SAP 系统时，SAP 许可证将失效，因为灾难恢复站点是新的 Amazon EC2 实例。硬件密钥将不再匹配。启动恢复实例时会创建临时的 SAP 许可证，有效期为 28 天。您无需创建新的 SAP 许可证。如果您需要灾难恢复实例在 28 天后继续运行，则可以申请带有恢复 Amazon EC2 实例 ID 的新 SAP 许可证。

网络、存储和计算

本节提供有关为暂存环境和目标环境配置网络、存储和计算的信息，以便通过 Elastic 灾难恢复实现 SAP 工作负载 AWS 的灾难恢复目标。

主题

- 网络

- 存储
- 计算

网络

用于灾难恢复的网络架构和配置可以在支持有效的 RTO 和 RPO SLA 方面发挥重要作用。触发灾难恢复时，必须考虑网络设计和将流量重定向到恢复实例。

以下是设计用于灾难恢复的网络的四个步骤。

- 连接源网络和目标网络
- 定义暂存子网和恢复子网
- 配置网络安全设置
- SAP 最终用户和集成流量

连接源网络和目标网络

第一步是选择和配置从源网络到复制服务器的网络连接方法。您可以选择私有或公开。有关更多信息，请参阅数据路由和限制。

无论采用哪种方法，传输的数据在传输过程中始终是加密的。默认方法是 public，即数据通过 Internet 路由到复制服务器上的公共网络接口。在私有方法中，数据通过私有网络进行复制。专用网络的选择取决于所使用的灾难恢复方案。

- AWS 区域内灾难恢复 — 私有网络通常介于两者之间 VPCs，使用 Amazon VPC 对等互连或 Tr AWS ansit Gateway 进行连接。我们建议使用不同的 AWS 账户和单独的 Amazon VPC 进行灾难恢复。有关更多信息，请参阅什么是 Amazon VPC 对等互连？ 以及什么是公交网关？ 。
- AWS 跨区域灾难恢复 — 我们建议使用将不同 AWS 区域连接在一起的完全冗余的 AWS 网络主干。Amazon VPC 对等互连和 AWS Transit Gateway 支持区域间的连接。有关更多详细信息，请参阅上的《网络转型简介》 AWS。
- AWS 灾难恢复之外 — 在这种情况下，您的源网络与不同的电信或互联网服务提供商 (ISP) 之间的物理网络 AWS 由不同的电信或互联网服务提供商 (ISP) 提供。 AWS 上提供了以下解决方案 AWS。
  - AWS Direct Connect
  - AWS Site-to-Site VPN
  - 软件定义广域网已上市AWS

AWS SAP 通常对 AWS 客户使用 Direct Connect。与基于 VPN 或 SD-WAN 的解决方案相比，它针对基于服务级别协议 (SLA) 的目标（例如吞吐量、抖动和延迟）提供了更可预测的性能。您可以与 AWS Direct Connect 交付合作伙伴合作，获取有关哪些选项最适合您的环境的指导。

定义暂存子网和恢复子网

建议使用一个子网来托管复制服务器，称为暂存区域子网。其他子网（称为恢复子网）是灾难恢复操作的目标所必需的。对于源网络处于开启状态的场景 AWS，请考虑如何根据所选的 AWS 账户策略和 landing zone 分配子网。通常，这可能意味着暂存区域子网应与您的源服务器位于不同的 Amazon VPC 中。为了简化环境，这可能只是在同一 Amazon VPC 中使用不同的子网。这意味着减少生产和非生产灾难恢复环境之间的隔离。欲了解更多信息，请参阅 Well-Architec AWS ted Framework：最佳实践 5.3。

归根结底，这些子网的数量和设计应遵循与源环境相似的概念。有关更多信息，请参阅网络图。

对于AWS 区域内灾难恢复场景，我们建议将暂存区域子网托管在与恢复子网不同的可用区中。这种设计为灾难恢复提供了额外的冗余。启动的恢复实例受单独可用区中的暂存区的保护。这遵循了使用多个可用区来保持弹性的设计原则。

配置网络安全设置

确保配置了所需的网络安全设置。这包括允许通过本地防火墙、网络安全设备、安全组或网络访问控制列表（网络 ACL）中的多个端口进行访问，可能还包括其他任务，具体取决于您的源环境的位置。有关更多信息，请参阅复制网络要求。

SAP 最终用户和集成流量

以下是影响最终用户和集成相关网络流量如何影响您的 RTO 和 RPO 的一些因素。

- 客户端识别并解析到新 IP 的 DNS 传播时间
- 用于重新路由流量的网络组件（如有）的延迟，例如全局或本地负载均衡器，包括 AWS 应用程序负载均衡器、 AWS 全球加速器或 Amazon Route 53 公共数据平面

有关更多信息，请参阅云中的灾难恢复选项。

存储

AWS Elastic 灾难恢复旨在根据源服务器性能为您的暂存环境评估和定义最佳 Amazon EBS 卷设置。演练和恢复服务器使用默认性能设置。这些卷的大小可以满足源系统的容量需求。您必须根据 SAP 工

作负载的特定要求查看这些设置。这确保了高效且符合灾难恢复 SLA 的环境。这些不同的服务器类型具有不同的要求和管理存储的方法。

主题

- 复制服务器
- 演练和恢复实例
- 时间点恢复

复制服务器

暂存区需要存储空间来支持源计算机的持续复制。这些 Amazon EBS 卷通常是低成本的硬盘 (HDD) 类型的存储卷。但是，如果复制的磁盘写入吞吐量很高，则默认的复制服务器设置会动态更改为性能更高的固态硬盘 (SSD) 存储类型。SAP 工作负载的推荐设置是默认 Amazon EBS 卷类型设置（复制服务器的自动卷类型选择）。它会根据您的工作负载要求自动选择高性能、经济高效的 Amazon EBS 卷。

您可以通过选择固态驱动器 (SSD) 来提高暂存区域的性能。这可以帮助 SAP 工作负载，例如突发或持续高事务速率的数据库，这些数据库的创建、更新和/或删除操作速率很高，必须应用于其存储。对于此类工作负载，我们建议您监控 Amazon CloudWatch 指标，并检查是否存在持续或不断增加的延迟。您可以将以下 CloudWatch 指标用于 Elastic 灾难恢复。

- LagDuration— 最新一致性快照的使用年限，以秒为单位
- 待办事项列表 — 尚未同步的数据量，以字节为单位

如果复制服务器上的 Amazon EBS 指标也表明存在性能问题，则可以更改 Amazon EBS 卷类型。要了解更多信息，请参阅以下资源。

- Linux 实例上的 Amazon EBS 卷性能
- 卷
- 磁盘设置

演练和恢复实例

对于 90% 或更多的用例，包括 SAP 应用程序和数据库（SAP HANA 和任何其他），SAP 工作负载至少需要gp3卷类型。如果您的每卷 IOPS 要求更高，超过 16,000 IOPS，或者每个卷的吞吐量要求大于 1,000 MiB/s，请考虑或卷。`io2` `io2 Block Express`

当您启动演练或恢复实例时，Elastic 灾难恢复会根据启动模板中定义的类型创建 Amazon EBS 存储卷。有关更多信息，请参阅 Amazon EC2 启动模板。启动模板由 Elastic Daser Recovery 自动生成，具有存储性能的默认值，使用通用型 SSD（卷大小与源系统容量要求相匹配）。查看启动模板，确认启动模板的默认分配满足了工作负载的存储需求。

您可以根据不同的卷类型或性能设置修改启动模板。修改之前，请确认您的目标 Amazon EC2 实例类型是否支持更高的存储空间。有关更多详细信息，请参阅支持的实例类型。有关 SAP HANA 数据库，请参阅存储配置。将更改应用于模板后，将修改后的版本定义为服务器的默认启动模板。在使用 Elastic 灾难恢复时，我们不建议在模板中添加或移除 Amazon EBS 卷。

对于需要在激活数据之前加载大量数据的服务器（例如数据库服务器），您可以在启动模板中配置更高的性能设置和存储类型。例如，如果您的服务器配置了gp3存储，那么为您的存储定义更多的预配置吞吐量和 IOPS，和/或使用性能更高的扩展存储，例如`io2 Block Express`（支持的 Amazon EC2 实例类型），可以缩短演练或恢复实例处理预期工作负载所需的时间。演练或恢复实例完全联机后，您可以更改恢复存储设置。有关更多信息，请参阅 Amazon EBS 弹性卷。您可以增加卷大小、更改卷类型或调整 Amazon EBS 卷的性能，而无需分离卷或重新启动实例。

时间点恢复

AWS Elastic 灾难恢复使用 Amazon EBS 快照来提供可在演练或恢复期间使用的时间点 (PiT) 恢复选项。Amazon EBS 的暂存快照是连续拍摄卷，以提供最新（亚秒级 RPO）的恢复点，第一个小时以 10 分钟为增量，以 1 小时为增量，持续 24 小时。每日 PiT 将在您的时间点 (PiT) 政策中指定的天数内保留。您可以指定 1 到 365 天之间，默认值为 7 天。有关更多信息，请参阅了解时间点状态。

计算

您必须为复制服务器和恢复服务器选择 Amazon EC2 实例类型。

主题

- 复制服务器
- 演练和恢复实例
- 源服务器

复制服务器

复制服务器通常比源系统小。`t3.small`是默认的实例类型，它最多可以复制 15 个卷。您可以在 SAP 应用程序服务器或其他更改率较低的服务器之间使用共享复制服务器。

如果您的工作负载处于突发状态，或者数据库的事务速率一直很高，并且必须对其存储进行大量创建、更新和/或删除操作，则可能需要对暂存区域进行不同的配置。如果您发现工作负载的复制出现延迟，请将默认复制服务器更改为其他实例系列。例如，通用型 Amazon EC2 实例系列或使用专用的复制服务器。这种变化可能会影响成本。有关更多信息，请参阅复制服务器配置。

演练和恢复实例

对于恢复实例，请配置 Amazon EC2 启动模板设置，使 AWS 目标实例与源实例相匹配。有关 SAP 认证实例的列表，请参阅以下资源。

- SAP NetWeaver 认证实例
- SAP HANA 认证实例

以下是影响灾难恢复解决方案的 RTO 的一些与计算相关的因素。

- 服务器启动时间
- SAP 在微软 Windows Server 操作系统上运行
- 需要超过 10 分钟才能启动的大型 SAP HANA 数据库
- 服务器上安装的 SAP 应用程序及其启动时间
- 源服务器和目标服务器以及存储配置不匹配 — 在目标端配置较低的计算能力或存储性能会增加 RTO

您必须将应用程序启动时间视为恢复的一个因素。我们建议选择能够提供有效启动时间的 Amazon EC2 实例类型和存储配置。这有助于您优化灾难恢复解决方案的 RTO。此外，通过执行灾难恢复测试或演练，您可以根据自己的操作系统和数据库来衡量 RTO。

SAP 系统可以在各种操作系统、基础架构平台和处理器指令集上运行。如果您的源服务器位于本地或其他云提供商，则它必须与 Amazon EC2 和 Elastic 灾难恢复兼容。源服务器必须具有专为 x86 系统架构构建的基于 64 位的操作系统。源服务器上 CPUs AWS有各种基于 x86 的版本，尤其是在服务器是旧型号的情况下。建议使用基于 SAP 大小的方法将源系统映射到 Amazon EC2 实例类型。要了解更多信息，请参阅 SAP 的规模信息。

源服务器

虽然对复制代理的系统要求相对较低，但请考虑源服务器上的 CPU、内存、网络、存储和其他资源限制，这些限制可能会影响灾难恢复解决方案的性能。根据这些因素调整源服务器的大小。有关更多信息，请参阅源服务器要求。

灾难恢复场景

以下是三种灾难恢复方案。

主题

- AWS 区域内灾难恢复
- AWS 跨区域灾难恢复
- 除了 AWS 灾 AWS 难恢复

AWS 区域内灾难恢复

在 AWS 云中，可用区之间有一段有意义的距离，在 100 千米以内（彼此相距 60 英里）。这种距离可以隔离可能影响数据中心的最常见灾难，例如洪水、火灾、暴风雨、地震等。如今，许多 AWS 客户都使用它来支持他们对 SAP 工作负载的弹性需求。根据您的业务连续性需求，区域内灾难恢复可能适合您。有关更多信息，请参阅单区域架构模式。

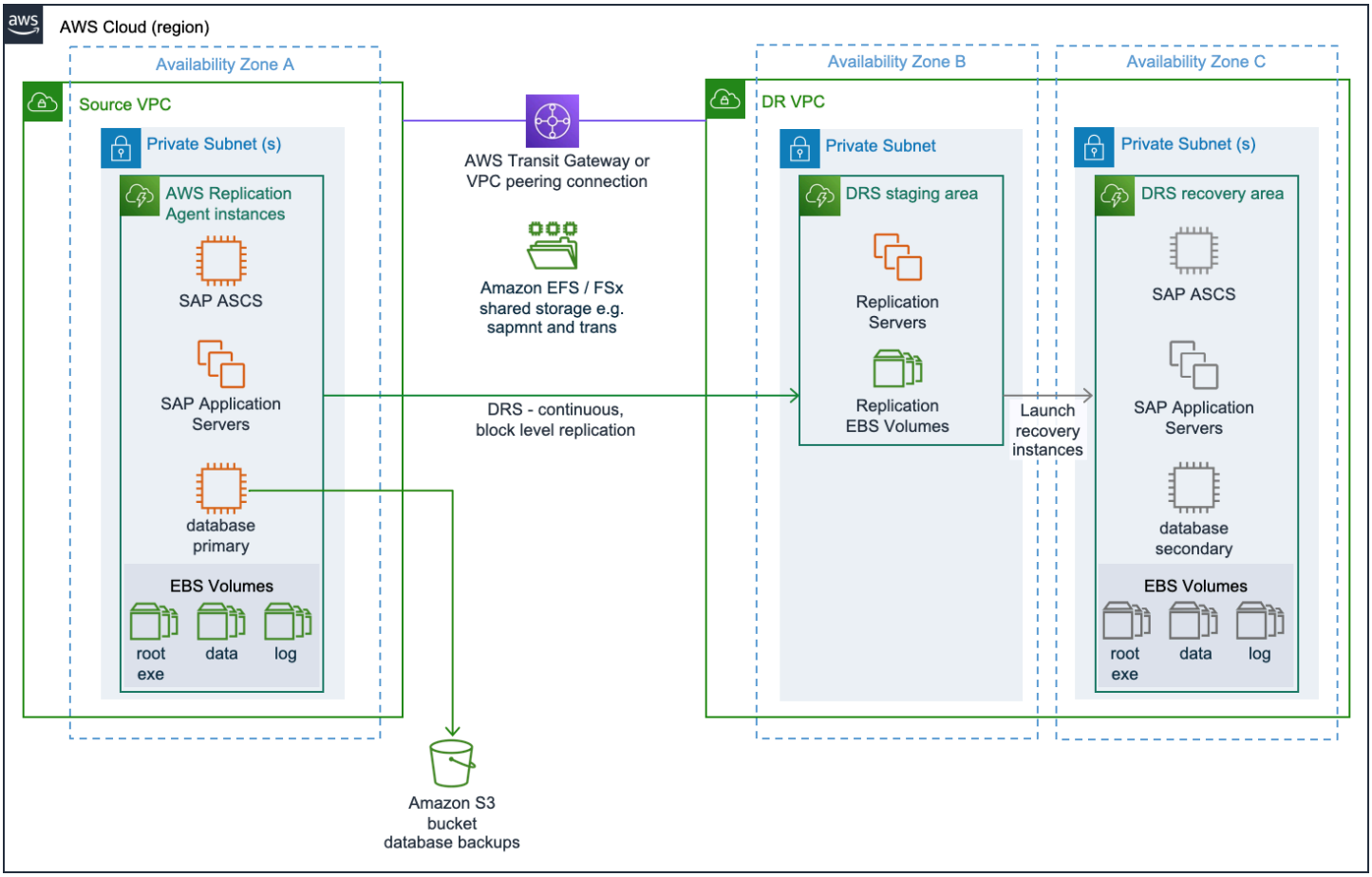
最佳实践

- 将同一地区的来源和恢复区域分开 Amazon VPCs
- 将源区和恢复区分开 AWS 账户
- AWS Transit Gateway 或 Amazon VPC 对等互连用于支持复制流量和最终用户连接

  有关更多信息，请参阅网络。
- 多可用区 Amazon S3 存储桶的弹性和 Amazon EFS 用于数据保护
- 将源区域、暂存区和恢复区分为不同的可用区

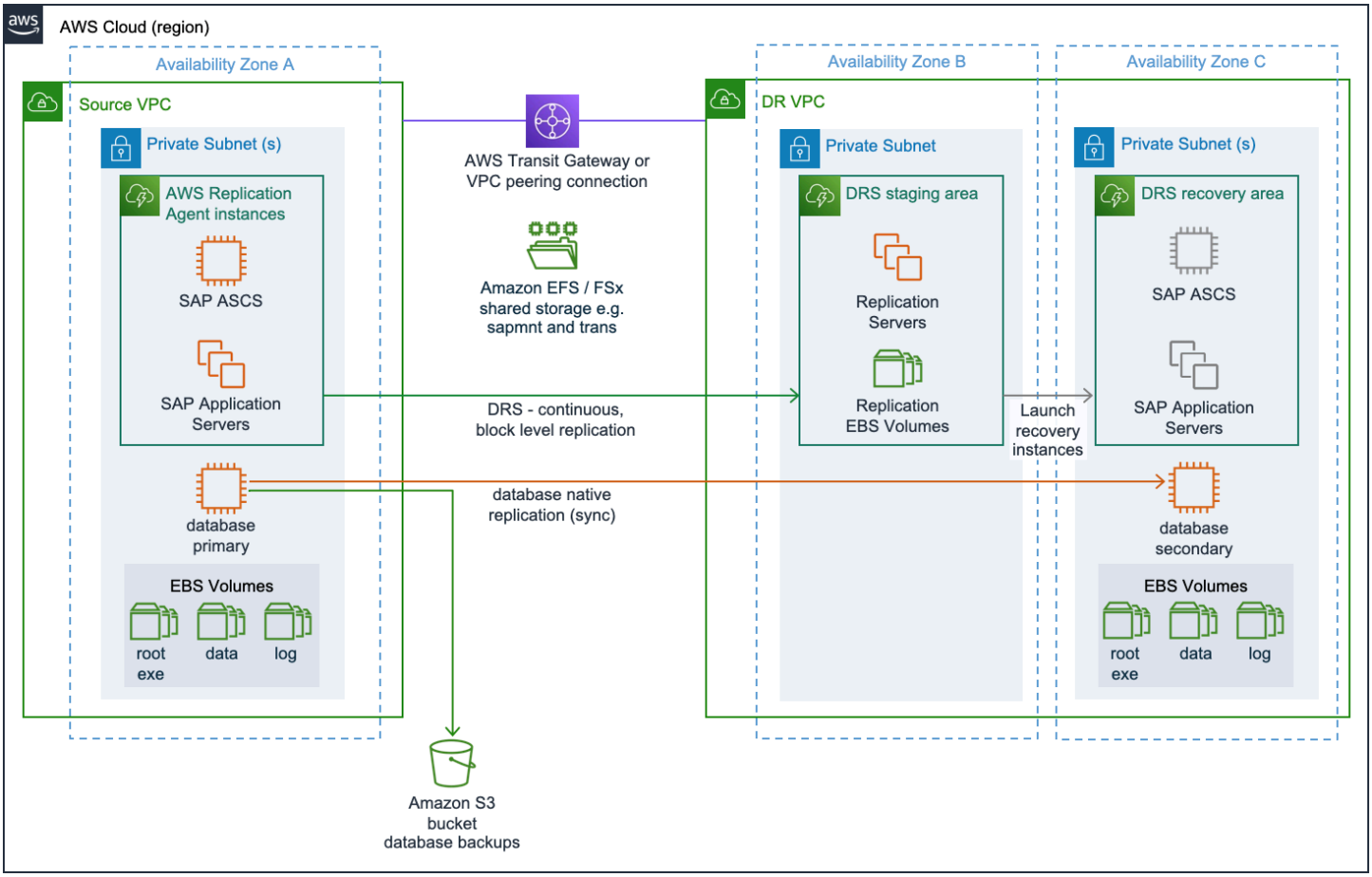
以下两节介绍此场景的参考架构。

全面实施区域内灾难恢复



在完整的区域内灾难恢复实施中，使用 Elastic 灾难恢复复制运行 SAP 应用程序组件的源服务器，例如中央服务实例 (A) SCS)、主应用程序服务器 (PAS)、其他应用程序服务器 (AAS) 和数据库。

混合区域内灾难恢复实施



在混合区域内灾难恢复实施中，使用 Elastic 灾难恢复复制运行 SAP 应用程序组件的源服务器，例如中央服务实例 [(A) SCS]、主应用程序服务器 (PAS) 和其他应用程序服务器 (AAS)。使用数据库本机复制方法复制数据库。

AWS 跨区域灾难恢复

具有多个 AWS 区域的灾难恢复场景可将数据存储在两个不同的地理位置，从而实现业务连续性。有关更多信息，请参阅多区域架构模式。

最佳实践

- 将同一地区的来源和恢复区域分开 Amazon VPCs
- 源区和恢复区的共享 AWS 账户
- AWS Transit Gateway 或 Amazon VPC 对等互连用于支持复制流量和最终用户连接

  有关更多信息，请参阅网络。
- 通过 Amazon EFS 或其他文件系统进行复制，以保护区域间的共享存储

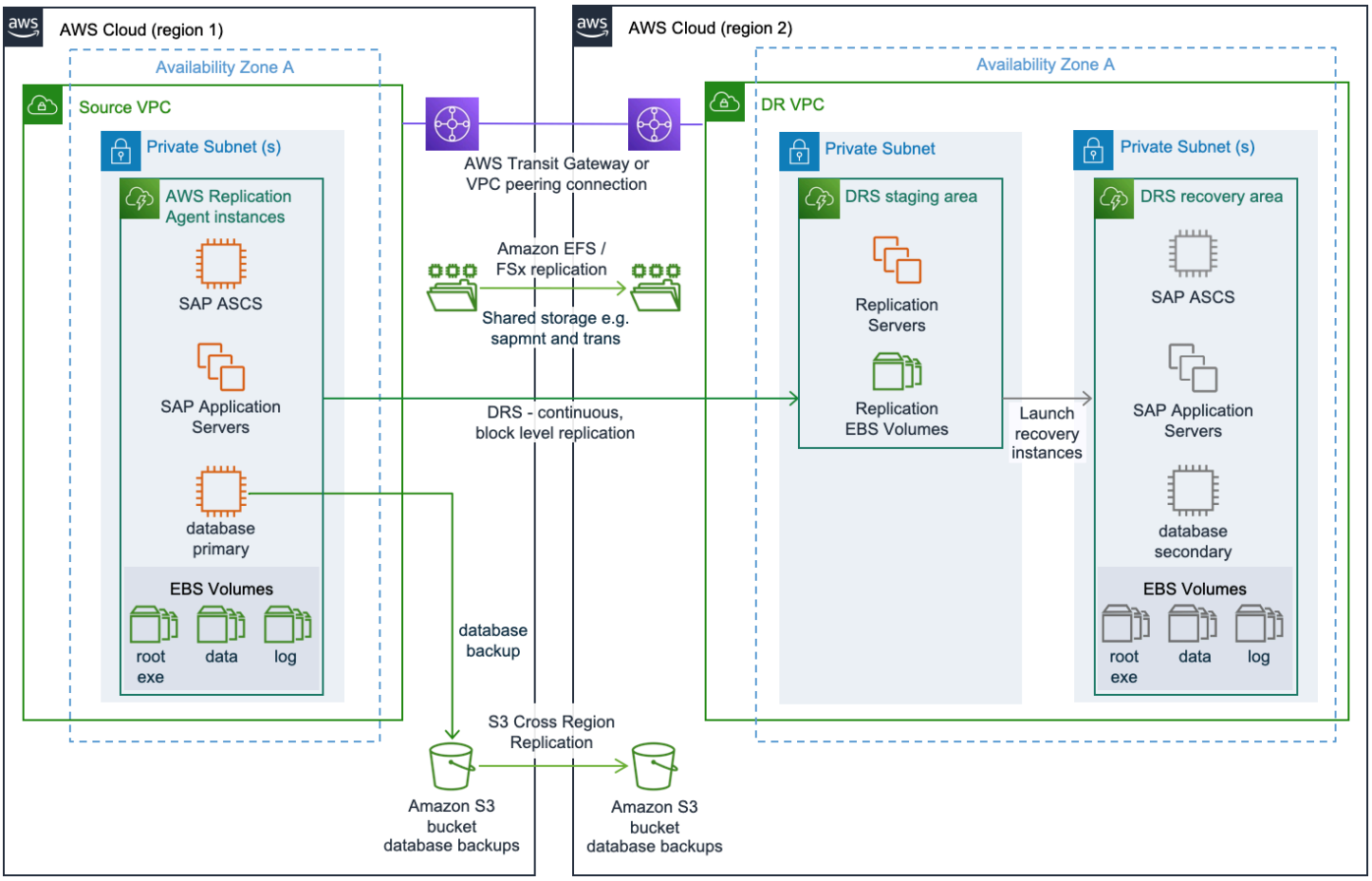
有关更多信息，请参阅AWS 跨区域灾难恢复。

> **Note**
>
> 您只能在 Amazon EFS 的同一个 AWS 账户中进行复制。

- Amazon S3 跨区域复制，为灾难恢复提供数据库备份和其他 Amazon S3 存储桶数据的副本 Amazon VPC
- 将源区、暂存区和恢复区分为不同的子网

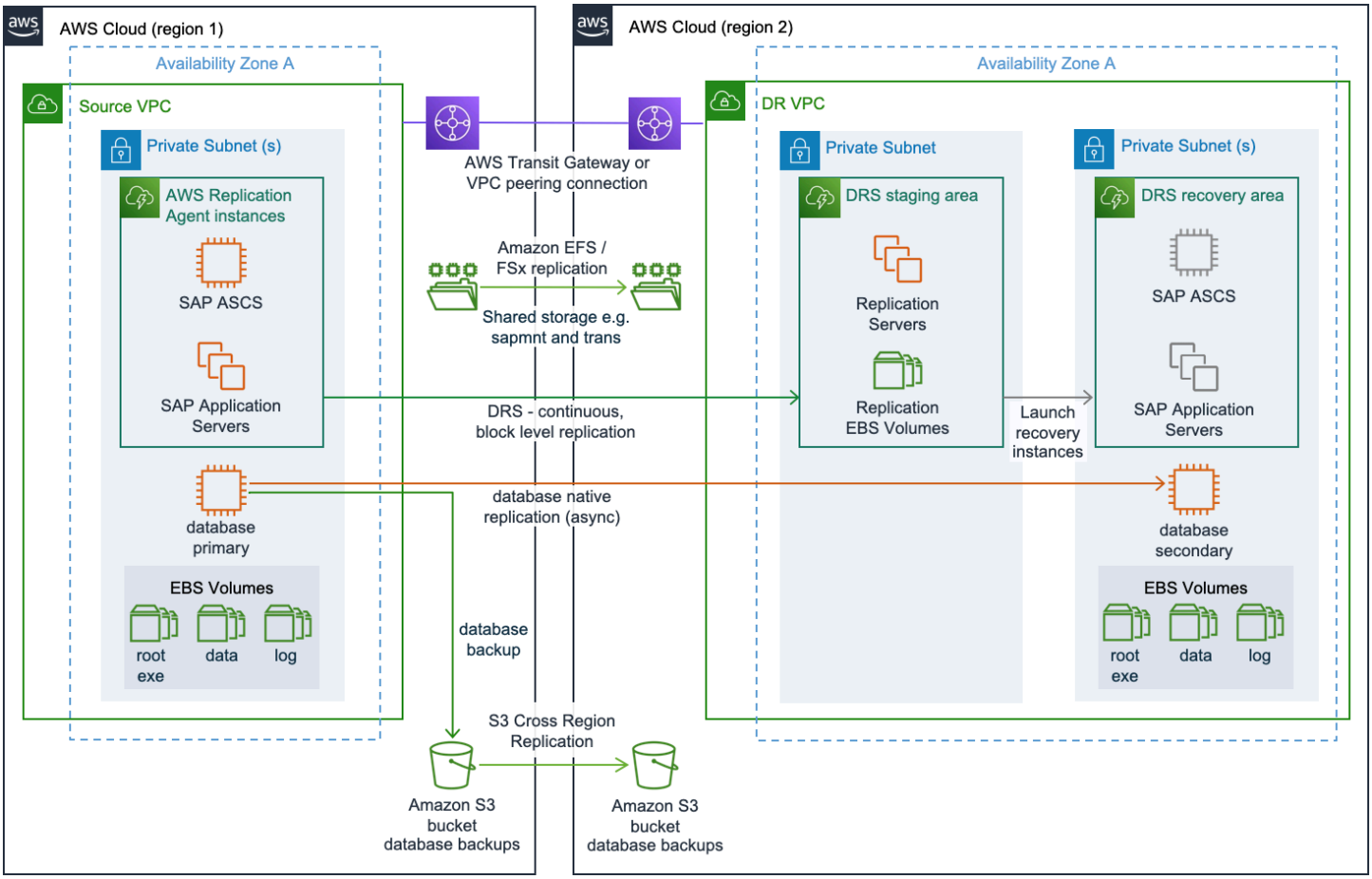
以下两节介绍此场景的参考架构。

全面实施跨区域灾难恢复



在完整的跨区域灾难恢复实施中，使用 Elastic 灾难恢复复制运行 SAP 应用程序组件的源服务器，例如中央服务实例 (A) SCS)、主应用程序服务器 (PAS)、其他应用程序服务器 (AAS) 和数据库。

混合跨区域灾难恢复实施



在混合跨区域灾难恢复实施中，使用 Elastic 灾难恢复复制运行 SAP 应用程序组件的源服务器，例如中央服务实例 [(A) SCS]、主应用程序服务器 (PAS) 和其他应用程序服务器 (AAS)。使用数据库本机复制方法复制数据库。

除了 AWS 灾 AWS 难恢复

在这种情况下，源系统在非AWS 环境中运行。可以实施这样的混合灾难恢复解决方案，以便在其他平台上快速增加现有生产环境的弹性。

最佳实践

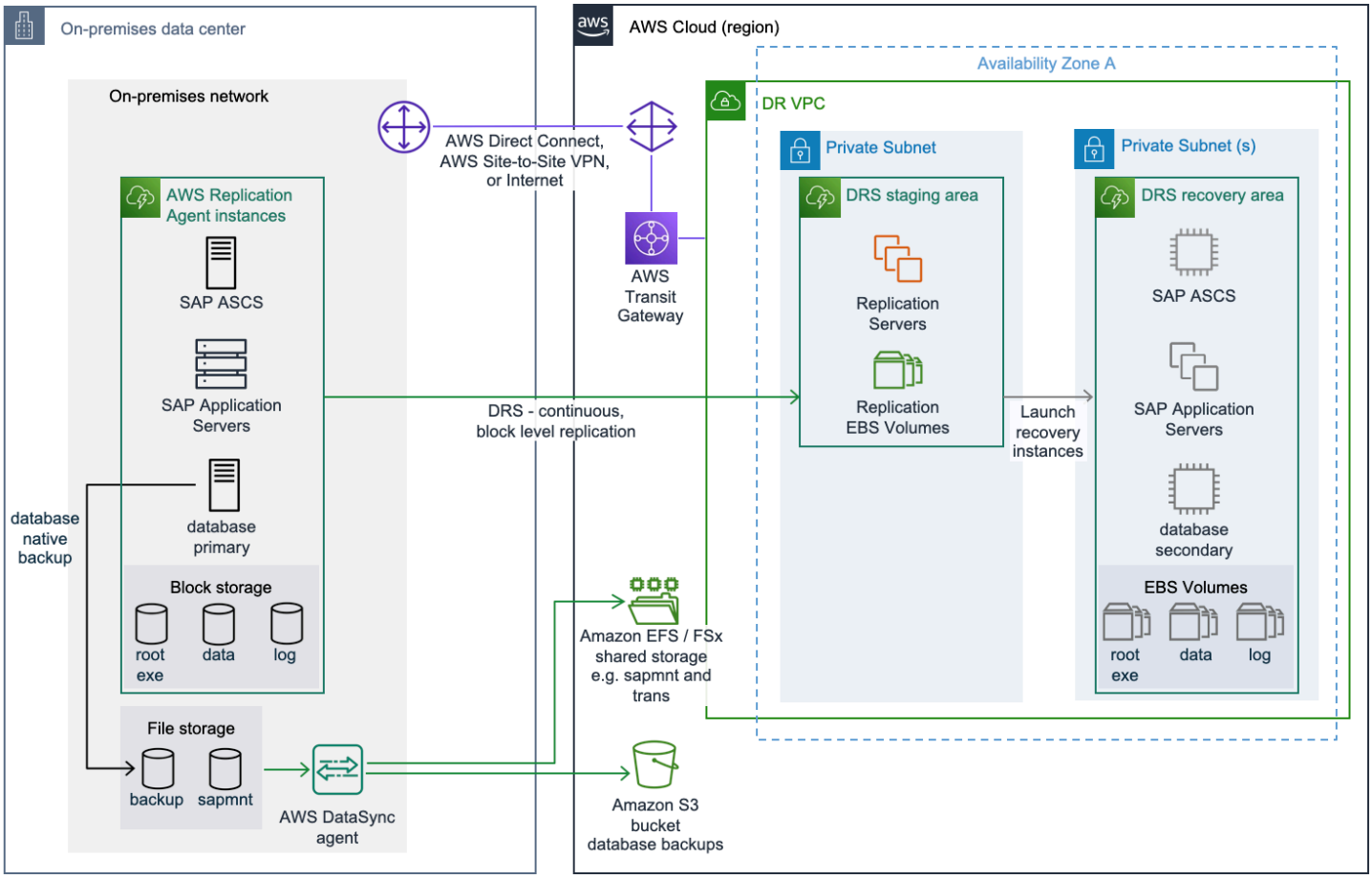
- AWS Direct Connect 用于支持复制流量和最终用户连接

  有关更多信息，请参阅网络。
- AWS DataSync 保护共享存储

  有关更多信息，请参阅AWS 灾 AWS 难恢复之外。
- 暂存区和恢复区的子网分开

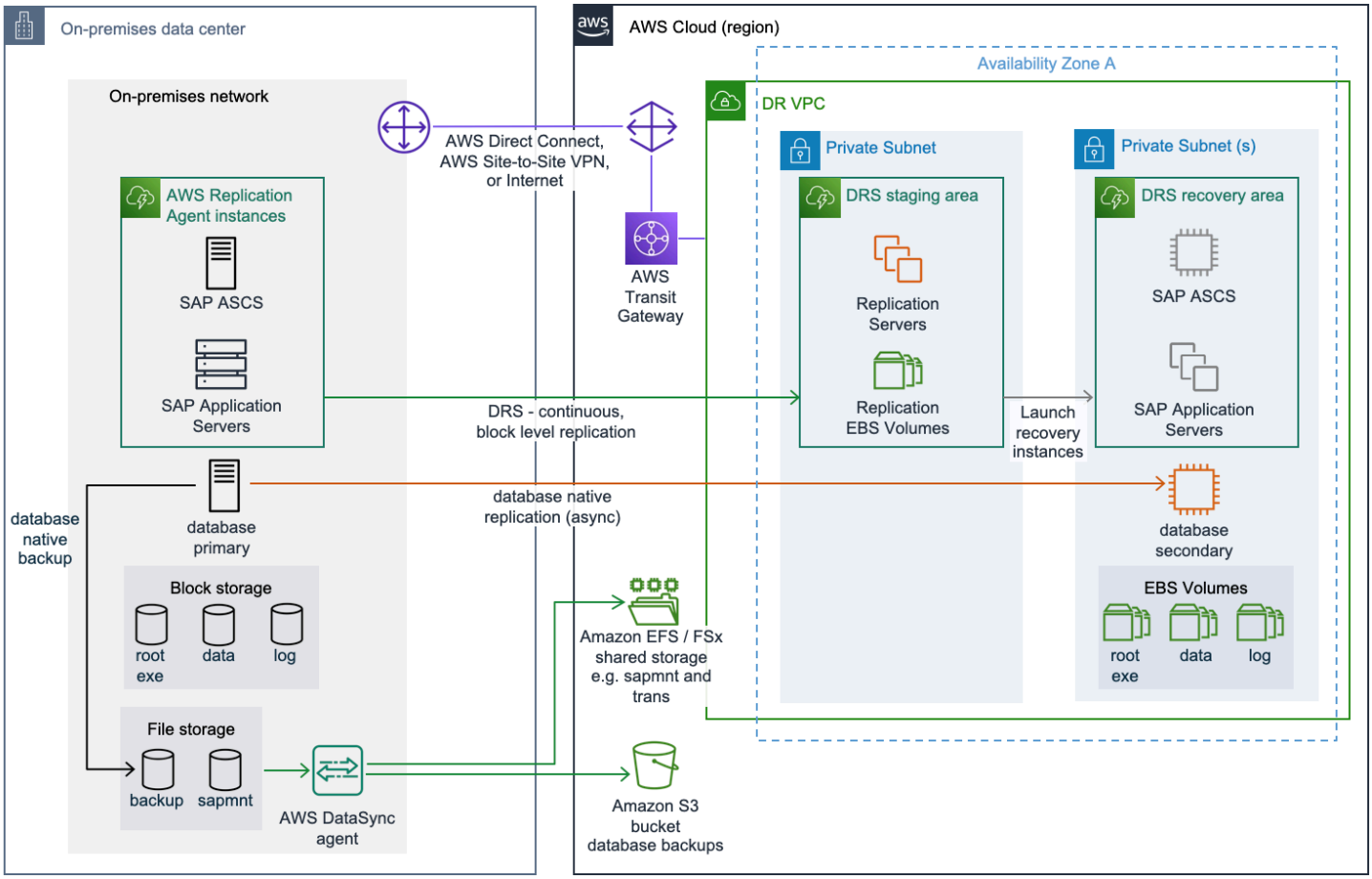
以下两节介绍此场景的参考架构。

全面实施非 AWS 灾AWS 难恢复



在全面的非AWS AWS 灾难恢复实施中，使用 Elastic 灾难恢复复制运行 SAP 应用程序组件的源服务器，例如中央服务实例 (A) SCS)、主应用程序服务器 (PAS)、其他应用程序服务器 (AAS) 和数据库。

混合非 AWS 灾AWS 难恢复实施



在非 AWS 灾难恢复混合实施中，使用 Elastic 灾难恢复复制运行 SAP 应用程序组件的源服务器，例如中央服务实例 [(A) SCS]、主应用程序服务器 (PAS) 和其他应用程序服务器 (AAS)。AWS 使用数据库本机复制方法复制数据库。

如需更多灾难恢复选项和信息，您可以联系 Su AWS pp ort。

共享存储弹性

SAP 服务器上的文件系统可以在块类型存储上创建，例如在本地连接的磁盘或企业存储区域网络 (SAN) 设备上，也可以基于共享文件系统，例如来自服务器或网络连接存储 (NAS) 设备的 SMB 或 NFS 共享卷。

由于 Elastic Disaster Recovery 是一项块级复制服务，因此只有在磁盘表示为块存储设备时，它才会复制磁盘。必须使用其他工具和流程为共享文件系统提供弹性。为了满足这些要求，我们建议使用完全托管的共享存储服务 AWS ，这些服务既简单又经济实惠，可以在云中启动、运行和扩展功能丰富、高性能和弹性的文件系统。文件系统的选择取决于灾难恢复场景的操作系统。

- Linux — 亚马逊 Elastic File Sy stem（亚马逊 EFS）

- 微软 Windows Server — 亚马逊 FSx Windows 文件服务器（亚马逊 FSx）
- 混合版 — FSx 适用于 Windows 文件服务器的亚马逊或适用于 ONTAP FSx 的亚马逊（FSx 适用于 NetApp ONTAP）

以下各节根据您的灾难恢复场景提供有关文件系统的指导。

主题

- AWS 区域内灾难恢复
- AWS 跨区域灾难恢复
- 除了 AWS 灾 AWS 难恢复

AWS 区域内灾难恢复

在使用 Amazon EFS、 FSx ONTAP 或 FSx Windows 文件服务器等托管服务托管您的共享文件系统时，其多可用区域设计提供的内置弹性意味着您的共享存储已经可以进行灾难恢复。为了进一步提高弹性，请确保定期备份您的共享存储，以防潜在的数据损坏。

如果您使用 NFS 或 SMB 协议直接从其中一个 Amazon EC2 实例共享文件系统，则如果该文件系统位于 Amazon EBS 上并通过复制代理连接到服务器，则可能不需要执行其他步骤。这样可以确保通过 Elastic 灾难恢复进行复制。如果共享文件系统与其他不属于您的 SAP 工作负载的内容一起托管在另一个 Amazon EC2 实例上，请使用操作系统原生工具（例如`rsync`管理此文件系统到恢复区的复制）。

您也可以使用 AWS DataSync 来提供选择性复制。可以将其安排为至少每小时运行一次，然后将这些文件复制到恢复区的目标存储器中。您必须在可以访问文件系统的 Amazon EC2 实例上安装额外的代理。有关更多信息，请参阅AWS DataSync 工作原理。

AWS 跨区域灾难恢复

要支持跨区域灾难恢复，第二个区域中必须有另一个共享文件系统可用。来自主共享文件系统的数据必须复制到第二个区域的共享文件系统上。根据您选择的 AWS 服务，您的实施方式会有所不同。

- Amazon Elastic File System — Amazon EFS 原生复制可以支持在单个 AWS 账户内进行跨区域复制。
- Amazon FSx for Windows 文件服务器 — 您还可以使用 AWS DataSync 在主共享存储和辅助共享存储之间复制数据。有关更多信息，请参阅AWS DataSync 工作原理。

- Amazon FSx for NetApp ONTAP — 您可以使用 NetApp SnapMirror 在源实例和目标实例上的 ONTAP 文件系统之间 FSx 复制文件，频率为每 5 分钟一次，以维护共享文件系统的当前副本。有关更多信息，请参阅使用计划复制 NetApp SnapMirror。

除了 AWS 灾 AWS 难恢复

根据共享存储的源区域设计，您必须考虑在中的 AWS灾难恢复实例上复制这些文件。我们建议使用 AWS DataSync。它可以在服务（例如 NFS 和 SMB 共享）以及使用 Amazon EFS、Windows 文件服务器和 FSx ON FSx TAP 的文件系统之间复制数据。

在某些情况下，您可以考虑使用其他选项来保护您的源区域 SAP 共享文件系统，例如，如果在源环境中使用以下选项。

- FSx 对于 ONTAP — 您可以使用 NetApp SnapMirror 在源实例和目标实例上的 ONTAP 文件系统之间 FSx 复制文件，频率为每 5 分钟一次，以维护共享文件系统的当前副本。有关更多信息，请参阅使用计划复制 NetApp SnapMirror。
- 本地存储 — 如果可以在托管本地存储的源服务器上配置 Replication Agent AWS，Elastic 灾难恢复会将其复制到您的灾难恢复环境中。

在 AWS 云上为 SAP 工作负载实施灾难恢复

使用 Elastic 灾难恢复为 SAP 工作负载实施灾难恢复解决方案，需要考虑典型 SAP 工作负载的不同部分（例如 S/4HANA 部署）的不同注意事项。 AWS 以下各节提供了有关在应用程序和数据库层中使用 Elastic 灾难恢复时如何设计、实施和管理 Elastic 灾难恢复的差异的指导。

主题

- SAP 应用程序层
- SAP 数据库层

SAP 应用程序层

我们建议使用 AWS 弹性灾难恢复来保护您的 SAP 应用程序服务器，例如 SAP ASCS/SCS、PAS、AAS 等。Elastic 灾难恢复支持基于 SAP 的 SAP 应用程序层 NetWeaver、ABAP 基础以及 TREX、内容服务器等独立应用程序。您可以对 Amazon EBS 支持的存储使用弹性灾难恢复，例如 SAP 实例二进制文件、存储在 Amazon EBS 卷上的本地文件。

应用程序层还包含共享文件系统，例如 SAP 装载、传输和接口目录。这些文件系统通常需要单独管理。有关更多信息，请参阅共享存储弹性。

要进行设置，请在应用程序服务器上安装 Elastic 灾难恢复代理。创建具有所需权限的 IAM 用户。向 Elastic 灾难恢复代理提供用户信息，以便与 Elastic 灾难恢复建立连接 APIs。配置代理后，它将使用 TLS 1.3 加密的 Elastic Daser Recovery API 端点进行身份验证握手。该服务在暂存区域子网中为每个复制的源卷生成大小相同的 Amazon EBS 卷，用于数据同步。可以在复制服务器设置中配置 Amazon EBS 卷的类型。复制将在生成暂存区域子网资源并安装代理后开始。通过加密将数据从源服务器直接传输到复制服务器。该服务自动管理暂存区域的子网资源，根据源服务器和磁盘的并行复制情况向上或向下扩展这些资源。

SAP 数据库层

AWS Elastic 灾难恢复完全支持作为灾难恢复解决方案，适用于在任何数据库上运行的 SAP 应用程序，也适用于在纵向扩展配置下在 SAP HANA 数据库上运行的 SAP 应用程序。不支持复制多节点 SAP 数据库，例如 SAP HANA 横向扩展群集。

SAP 系统中的数据存储在数据库中。这些数据包括主数据、交易数据和 ABAP 工件。在评估灾难恢复解决方案的 Elastic 灾难恢复时，您必须考虑您的业务 RPO 和 RTO 要求。该服务不具备应用程序感知能力，而是通过将连接的存储复制到目标暂存环境来在操作系统层运行。根据您的 RTO 和 RPO 要求，您可以选择弹性灾难恢复或数据库原生复制方法，例如适用于 SAP HANA 的 SAP HANA 系统复制 (HSR)。

以下是选择数据库复制方法的重要注意事项。

主题

- 网络带宽
- RPO
- 变化率
- RTO
- 成本
- RCO
- 存储限制

网络带宽

AWS Elastic 灾难恢复在操作系统层运行，对连接的存储设备进行块级复制。根据源位置的更改率，您可能需要更高的网络带宽来保持复制的最新状态。像 SAP HSR 这样的数据库感知技术需要更少的网络带宽，从而可以更快地复制变化率高的系统。

RPO

弹性灾难恢复支持亚秒级的 RPO。对于 SAP 工作负载，请确保您的网络能够支持峰值变化率。如果您的 RPO 非常小，我们建议您同时测试数据库本机复制方法以及 Elastic 灾难恢复。

导致数据库数据发生重大变化的操作会导致暂存区域的数据复制延迟。它可以包括将备份部分或全部恢复到源服务器上数据库的受保护卷中。对存储卷所做的更改远高于源服务器上通常的更改率。从备份中恢复到源服务器上受保护卷的数据被视为已更改的数据块，并由 Elastic 灾难恢复进行复制。复制服务器需要更多时间才能从源系统接收和写入如此大量的更改数据。这可能会影响您的业务 RPO。

建议在工作负载不太重要的时候管理操作，例如从备份中恢复。这样，较长的 RPO 值就不会影响您的工作负载。您可以使用 Elastic 灾难恢复跟踪仍在等待复制的更改数据量。有关更多信息，请参阅 “恢复” 控制面板。

变化率

对于更改率较高的数据库，您可以通过性能充足的网络以及复制服务器的存储和计算配置来满足性能要求。如果这些更改不足以满足业务性能要求，则可以选择数据库本机复制方法来优化 RPO。

RTO

使用 Elastic 灾难恢复，一旦触发灾难恢复事件，就会配置目标灾难恢复环境。总时间取决于数据库的大小和所选的 Point-in-Time (PiT)。在生产环境中实施灾难恢复场景之前，必须先测试灾难恢复方案。

成本

由于 Elastic 灾难恢复不使用热备用或热备用方法，因此与许多其他灾难恢复选项相比，您的灾难恢复环境的计算成本可以降至最低。有关更多信息，请参阅 AWS Elastic 灾难恢复定价。使用数据库本机复制方法，成本可能会随着灾难恢复区域的计算资源而增加。

RCO

如果您有多个紧密耦合的系统，则需要使用数据库本机复制方法。

存储限制

在大多数情况下，可用的 Amazon EBS 卷类型足以满足任何存储容量和性能需求。根据源环境架构，在某些情况下，恢复实例上的存储量会超过单个 Amazon EBS 卷的容量和/或性能限制。这可能发生在非AWS AWS 灾难恢复实施中，`data`并且`log`卷连接到高负载数据库服务器。有关更多信息，请参阅 Amazon EBS 卷类型。

将服务器迁移到时 AWS，必须将此类存储卷重构为新的存储架构，例如，创建条带卷集。条带卷集是使用恢复实例操作系统中的逻辑卷管理器工具定义和维护的。有关更多信息，请参阅 Linux 上的 RAID 配置。这些卷集将跨越两个或更多 Amazon EBS 卷，最多可达到满足所需卷大小和性能所需的总量。然后将存储卷数据复制到新的条带卷集。虽然可以通过 Elastic 灾难恢复启动后脚本或通过 Amazon 事件规则触发代码的警报 EventBridge 事件自动执行此过程，但额外的步骤可能会导致更长的恢复时间。

在这些情况下，实施混合灾难恢复解决方案是合适的。大多数服务器由 Elastic 灾难恢复管理，部分服务器（出于存储性能考虑）使用其他灾难恢复方法，例如本机数据库复制技术。存储架构重构是在初始灾难恢复环境实施期间设置备用复制服务器时完成的。由于复制现在是在应用程序级别进行的，因此灾难恢复服务器能够写入与源服务器上不同的存储架构。

借助 SAP 在 AWS 云端崛起

RISE with S/4HANA Cloud，私有版是 SAP 推出的云 ERP 产品。除ERP外，它还包括业务流程情报、业务平台和分析以及业务网络。SAP 负责为RISE提供整体服务等级协议、云运营和技术支持。您可以在 RISE 中使用 SAP 选择自己的云服务提供商。

SAP S/4 HANA Cloud，私有版是一种单租户设置，其中不同的客户环境通过 AWS 账户和专用的虚拟私有云 (VPC) 隔离。

> **Important**
>
> SAP 拥有并管理部署 RISE with SAP 的 AWS 账户，并负责为你的 SAP 环境提供 AWS 服务的服务 AWS。

在 RISE 中，SAP 与 SAP 一起负责云端的安全。有关更多信息，请参阅《AWS 云安全-责任共担模型》和《SAP 和超大规模企业：阐明云中的安全》。除了 SAP 提供的安全性外，您还可以为 SAP 环境实施额外的安全保护。有关更多详细信息，请参阅 “安全” 部分。

在 SAP 管理的 AWS 账户中，SAP 管理运行 SAP 环境所需的 AWS 服务 AWS。您仍然可以在自己的、不由 SAP 管理的 AWS 账户中利用 AWS 服务通过 SAP 扩展 RISE。例如，您可以使用 Amazon AppFlow 或 AWS Glue 创建数据湖。有关更多详细信息，请参阅 “扩展” 部分。

> **Note**
>
> 您必须创建一个单独的 AWS 账户或使用不受 SAP 管理的现有 AWS 账户来创建带有 AWS 服务的扩展。

SAP 为由 SAP 管理的 AWS 账户提供 Support。您无需为由 SAP 管理的 AWS 账户建立额外的 Support。

本文档重点介绍使用 SAP S/4HANA Cloud、私人版和 SAP S/4HANA Cloud（私人版、量身定制的选项）的 RISE。本文档涵盖以下主题。

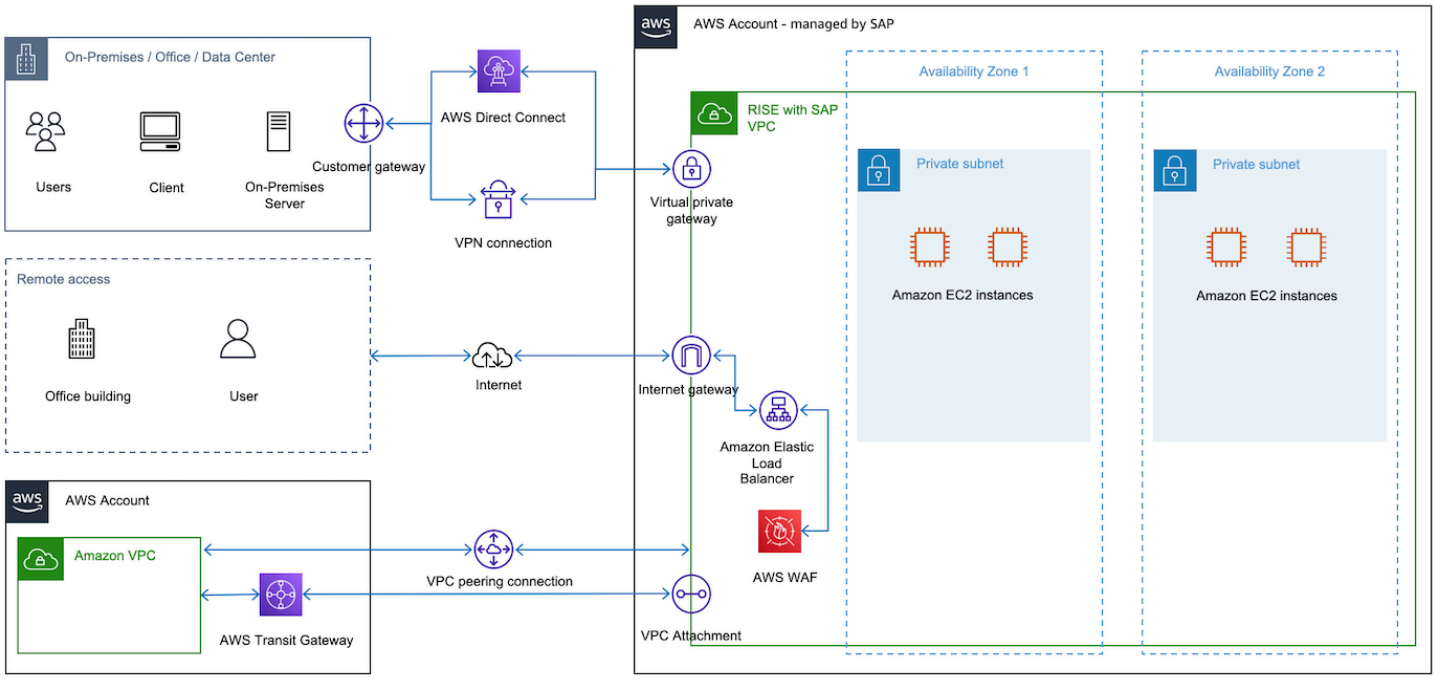
主题

- 连接

- 安全性
- 可靠性
- 扩展

连接

您必须在运行 RISE with SAP 解决方案的 AWS 云和本地数据中心之间建立连接。您还需要连接以实现直接数据传输（以避免通过本地位置路由数据），以及在 SAP 系统和 AWS 云上运行的应用程序之间进行通信。下图提供了使用 SAP VPC 与 RISE 连接的示例概述。



有关更多详细信息，请参阅以下主题：

主题

- 建立与 RISE 的连接的角色和责任
- 从本地网络连接到 RISE
- 从您的 AWS 账户连接到 RISE
- 通过最近的 Di AWS rect Connect POP（包括 AWS 本地区域）连接到 RISE
- 连接到 RISE 的决策树
- 其他考虑因素

建立与 RISE 的连接的角色和责任

在 RISE with SAP 的领导下，SAP 企业云服务 (ECS) 团队管理 SAP S/4HANA 私有云环境。SAP 提供的补充条款和条件中有一个关于排除任务的部分。您负责运行此类任务。您也可以使用第三方服务提供商为您管理排除的任务。有关更多详细信息，请参阅 SAP 产品政策。

使用 SAP 部署 RISE 所需的主要任务是在开启 SAP VPC 的情况下建立与 RISE 的网络连接 AWS。根据RISE与SAP的协议，你负责建立与RISE的连接。

我们建议您花点时间了解有关如何在开启 SAP VPC 的情况下将您的本地网络 and/or 现有 AWS 账户连接到 RISE 的可用选项 AWS。请查看后续章节以了解更多信息。

从本地网络连接到 RISE

使用 AWS VPN 或 Di AWS rect Connect 或两者的组合支持在开启 SAP 的情况下 AWS 从本地连接到 RISE。

主题

- 使用 VP AWS N 通过 SAP VPC 连接到 RISE
- 使用 Di AWS rect Connect 通过 SAP VPC 连接到 RISE
- 使用 SD-WAN 通过 SAP VPC 连接到 RISE
- RISE 与您的本地网络之间连接的实施步骤

使用 VP AWS N 通过 SAP VPC 连接到 RISE

允许使用 VP AWS Site-to-Site N 通过 SAP VPC 从 RISE 访问您的远程网络。 AWS 云端和您的本地位置之间的流量通过 Internet 协议安全性 (IPsec) 进行加密，并通过互联网上的安全隧道进行传输。与 Di AWS rect Connect 相比，此选项效率高，实施速度更快。有关更多信息，请参阅使用 AWS 虚拟专用网络将您的 VPC 连接到远程网络。

每个 VPN 隧道可以获得高达 1.25 Gbps 的最大带宽。有关更多信息，请参阅 Site-to-Site VPN 配额。

要超越单个 VPN 隧道吞吐量 1.25 Gbps 的默认最大限制，请参阅如何使用与传输网关关联的多个 Site-to-Site VPN 隧道实现 ECMP 路由？

使用此选项时，SAP 需要以下详细信息：

- BGP ASN

- 您的设备的 IP 地址

您可以从本地 AWS VPN 设备获取这些详细信息。

使用 AWS 站点到站点 AWS VPN 将远程网络直接连接到 RISE 时， AWS VPN 连接的费用和数据传输费用包含在 RISE 订阅中。

有关更多信息，请参阅：AWS 站点到站点 AWS VPN 定价。

注意：由于与 “客户网关设备”（ Site-to-Site AWS VPN 连接端的物理设备或软件应用程序）的生命周期和运行相关的成本各不相同，因此本文档不考虑这一点。

使用 Di AWS rect Connect 通过 SAP VPC 连接到 RISE

如果您需要比基于互联网的连接更高的吞吐量或更稳定的网络体验，请使用 Di AWS rect Connect。AWS Direct Connect 通过标准的以太网光纤电缆将您的内部网络连接到 AWS Direct Connect 位置。您可以创建不同类型的虚拟接口 (VIFs) 来连接各种 AWS 服务。例如，您可以创建一个公有 VIF 来与 Amazon S3 等公共服务或私有资源（如 Amazon Private/Transit VPC）的 VIF 进行通信，同时绕过网络路径中的互联网服务提供商。有关更多信息，请参阅 AWS Direct Connect 连接。

您可以从 1 Gbps、10 Gbps、100 或 400 Gbps 的专用连接中进行选择，也可以选择 Direc AWS t Connect 合作伙伴的托管连接，其中合作伙伴已与云建立了网络链接。 AWS 托管连接的可用速率为 50 Mbps。100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、10 Gbps 和 25 Gbps。您可以从获准支持此模式的 AWS Direct Connect 交付合作伙伴处订购托管连接。有关更多信息，请参阅 AWS Direct Connect 交付合作伙伴。

要进行连接，请使用由 SAP 管理的 AWS 账户中的虚拟专用网关，或者在您的账户中使用与 SAP 管理的 AWS 账户中的虚拟专用网关关联的 Direct Connect 网关。 AWS 有关更多信息，请参阅 Direct Connect 网关。Direct Connect 网关也可以连接到 T AWS ransit Gateway。有关更多信息，请参阅使用您的单一 AWS 账户连接到 RISE。

要在 SAP 管理的 AWS 账户中设置 Di AWS rect Connect 专用连接，您必须获得 SAP 的授权书。

使用 AWS Direct Connect 将远程网络直接连接到 RISE 时，数据传出（出口）的费用包含在 RISE 订阅中。RISE 订阅中不包括与容量（通过网络连接传输数据的最大速率）和端口时间（配置端口供您使用 AWS 或 Di AWS rect Connect 交付合作伙伴的时间）相关的费用。 AWS Direct Connect不收取安装费，您可以随时取消，但是，您的 AWS Direct Connect交付合作伙伴或其他本地服务提供商提供的服务可能有其他适用的条款和条件。

有关更多信息，请参阅：AWS Direct Connect 定价

使用 SD-WAN 通过 SAP VPC 连接到 RISE

什么是 SD-WAN

软件定义广域网 (SD-WAN) 是一种网络技术，它使用软件来管理和路由不同网络上的流量，例如多路径标签交换 (MPLS)、公共互联网或 AWS 主干网络，重点是改善连接和应用程序性能。SD-WAN 主要在网络 OSI 模型的第 3 层（网络层）运行，提供集中控制、路由、路径选择、基于 IP 的策略，并能够确定特定任务关键型应用程序（例如 SAP）的优先级，因此非常适合基于云的 RISE 和 SAP 环境。

尽管 SD-WAN 主要在第 3 层运行，但它使用宽带互联网等重叠网络，但它可以利用第 2 层（数据链路）技术，例如 Direc AWS t Connect 作为传输的底层网络，以及 VPN 等第 3 层（网络）技术。AWS Site-to-Site

在 SD-WAN 架构中，SD-WAN 前端充当集线器或集中式网络组件，而 SD-WAN 边缘设备部署在分支机构、远程站点或数据中心，充当 WAN 流量的入口和出口点。

您可以在上的 “实施 SD-WAN 解决方案的参考架构” 中参考更多详细信息。 AWS

场景 A：本地部署的 SD-WAN 设备（边缘 and/or 前端/集线器）

AWS T@@ ransit Gateway Connect 允许您将 SD-WAN 网络扩展到 AWS 使用 GRE（通用路由封装）隧道，而无需额外的基础架构。 AWS 通过 Tr ansit Gateway Connect Peer，你可以在 AWS 账户中的传输网关和本地 SD-WAN 设备之间建立 GRE 隧道，后者通过 Direc AWS t Connect 连接作为底层传输进行连接。

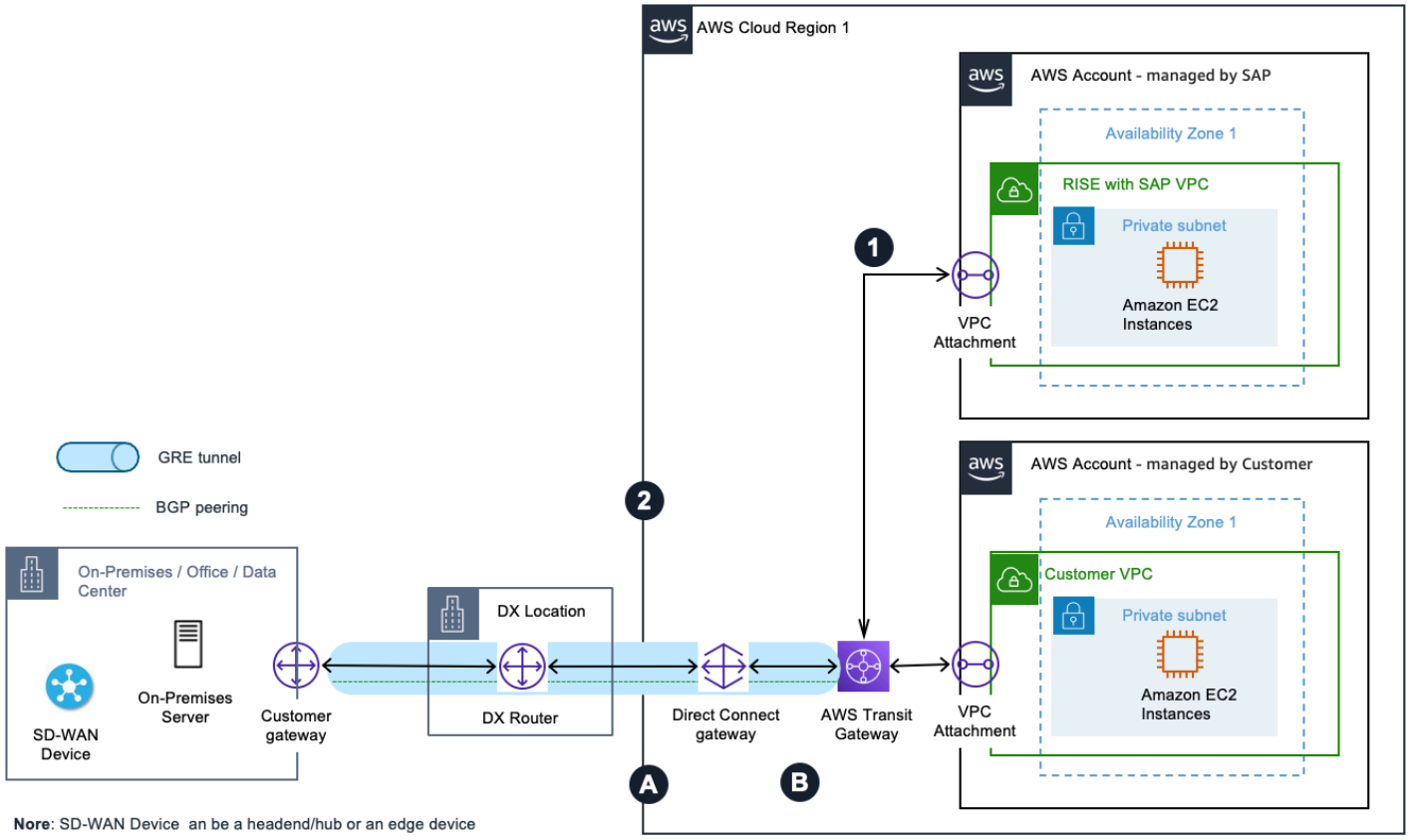
必须将设备配置为使用 C onnect 附件通过 GRE 隧道发送和接收往返传输网关的流量。必须将设备配置为使用 BGP（边界网关协议）进行动态路由更新和运行状况检查。

每个连接都可以配置自己的路由表和 BGP 对等体，从而使您能够通过虚拟路由和转发 (VRF) 将本地网络分段扩展到 aws。带有 SAP VPC 的 RISE 已连接到 Tr AWS ansit Gateway。

此设置提供了一种简化的方法，可以 AWS 使用 Direct Connect 将软件定义广域网环境与 RISE 与 SAP AWS 连接起来，在简化整体架构的同时保持网络分离。

在这种情况下，重叠网络是 SD-WAN（使用 GRE 隧道）， headend/hub 或边缘设备部署在本地，底层传输为 Direct Connect AWS

模式 A-1：SD-WAN 设备与 Transit Gateway 集成，Direc AWS t Connect 与你的着 AWS 陆区集成 AWS



上图说明了如何在 AWS 不添加额外基础设施的情况下扩展和分段软件定义广域网流量的模式。您可以使用 Di AWS rect Connect 连接作为 AWS 账户中的底层传输来创建 Transit Gateway 连接附件。

使用 SAP VPC 从 RISE 出站：

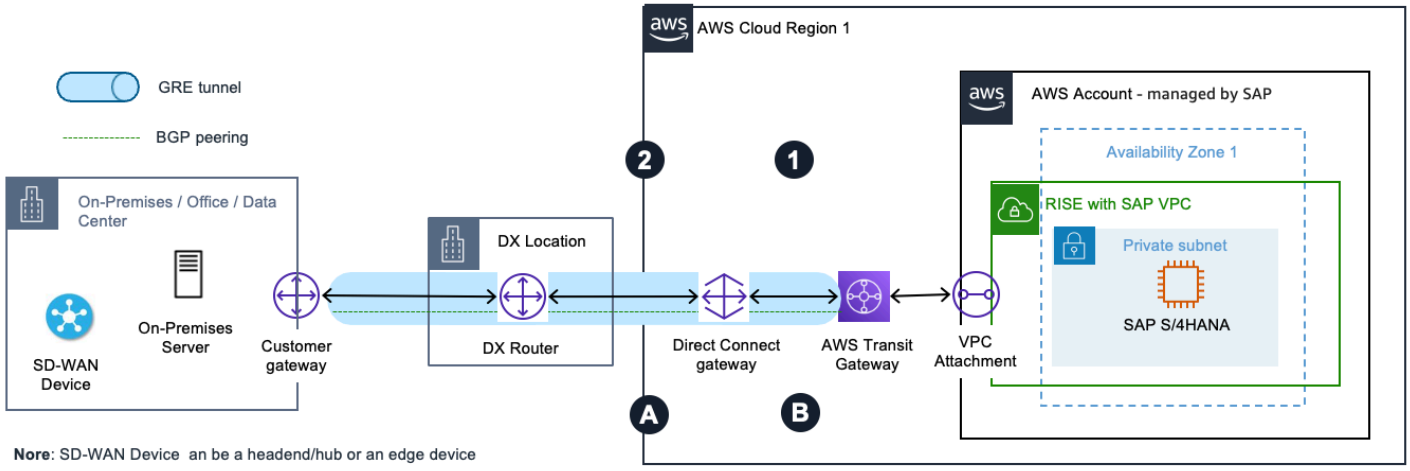
1. 从 RISE VPC 发起到企业数据中心的流量将路由到 Transit Gateway。
2. Transit Gateway 连接连接使用 Direct Connect 连接作为底层传输，并通过 GRE 隧道和 BGP 将 Transit Gateway 连接到企业数据中心 SD-WAN 设备。

使用 SAP VPC 入站到 RISE：

A. 从企业数据中心 SD-WAN 设备到 RISE VPC 的流量通过 Transit Gateway 连接的 GRE 隧道通过 Direct Connect 链路转发到 Transit Gateway。

B. Transit Gateway 使用 SAP VPC 将流量转发到目标 RISE。

模式 A-2：SD-WAN 设备与 Transit Gateway 和 Direc AWS t Connect 集成，没有着 AWS 陆区 AWS



上图说明了如何在 AWS 不添加额外基础设施的情况下扩展和分段软件定义广域网流量的模式。在 RISE with SAP 中，你可以请求 SAP 使用 Direct Connect 连接作为底层传输来创建 Transit Gateway 连接附件。如果需要，客户可以利用 SAP 管理的 Direc t Connect 网关 (DXGW)。

使用 SAP VPC 从 RISE 出站：

1. 从 RISE VPC 发起到企业数据中心的流量将路由到 Transit Gateway。
2. Transit Gateway 连接连接使用 Direct Connect 连接作为传输，并使用 GRE 隧道和 BGP 将 Transit Gateway 连接到企业数据中心 SD-WAN 设备。

使用 SAP VPC 入站到 RISE：

A. 从企业数据中心 SD-WAN 设备到 RISE VPC 的流量通过 Transit Gateway 连接的 GRE 隧道通过 Direct Connect 链路转发到 Transit Gateway。

B. Transit Gateway 使用 SAP VPC 将流量转发到目标 RISE。

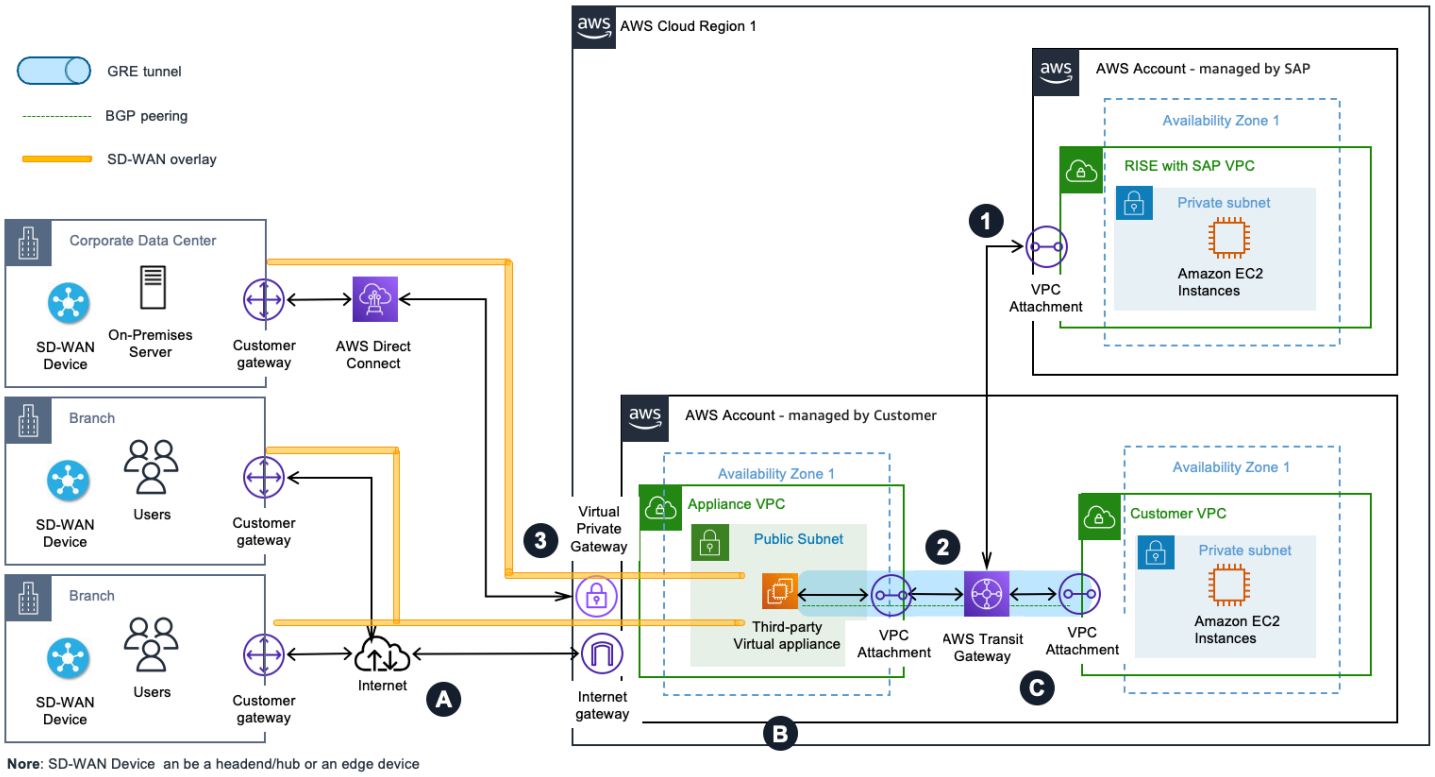
场景 B：中的 SD-WAN 设备（边缘 and/or 前端/集线器设备） AWS

在这种情况下，SD-WAN 网络的虚拟设备部署在 aws 内的 VPC 中。然后，您可以使用 VPC 附件作为 SD-WAN 虚拟设备与 AWS 账户中的 Transit Gateway 之间的 Transit Gateway 连接附件的底层传输。与场景 A 类似，Transit Gateway 连接附件支持 GRE，与 VPN 连接相比，带宽性能更高。它支持 BGP 进行动态路由，无需配置静态路由。此外，它与 T ransit Gateway Network Manager 的集成可通过全球网络拓扑、连接级别性能指标和遥测数据提供高级可见性。

在本地和之间 AWS，重叠网络是带有 GRE 的 SD-WAN 或内部 headend/hub 部署的 IPSec 隧道，底层传输可以是 Internet AWS、MLPS 或 Direct Connect。以下是此场景下的架构模式：

注意：以下各节中介绍的网络模式仅适用于您在 aws 上设置的现有或新的 landing zone。有关 SD-WAN 设备部署和直接与 AWS 账户连接（由 SAP 管理），请参阅模式 A-2。

模式 B-1：SD-WAN 设备与 Transit Gate AWS way Connect AWS 集成到您的着陆区 AWS



上图说明了一种使用连接附件将软件定义广域网网络与 Transit Gateway 集成的模式，并将软件定义广域网网络的（第三方）虚拟设备放置在 aws 内的设备 VPC 中。通常在分支机构和本地数据中心部署 SD-WAN 边缘设备以创建全网状拓扑。

使用 SAP 从 RISE 出站：

1. 从 RISE VPC 发起到企业数据中心的流量将路由到 Transit Gateway。
2. Transit Gateway 连接使用 VPC 附件作为传输，并使用 GRE 隧道和 BGP 将 Transit Gateway 连接到设备 VPC 中的第三方设备。
3. 第三方虚拟设备封装了流量，该流量使用 Direct Connect 链路之上的 SD-WAN 叠加层到达公司数据中心。

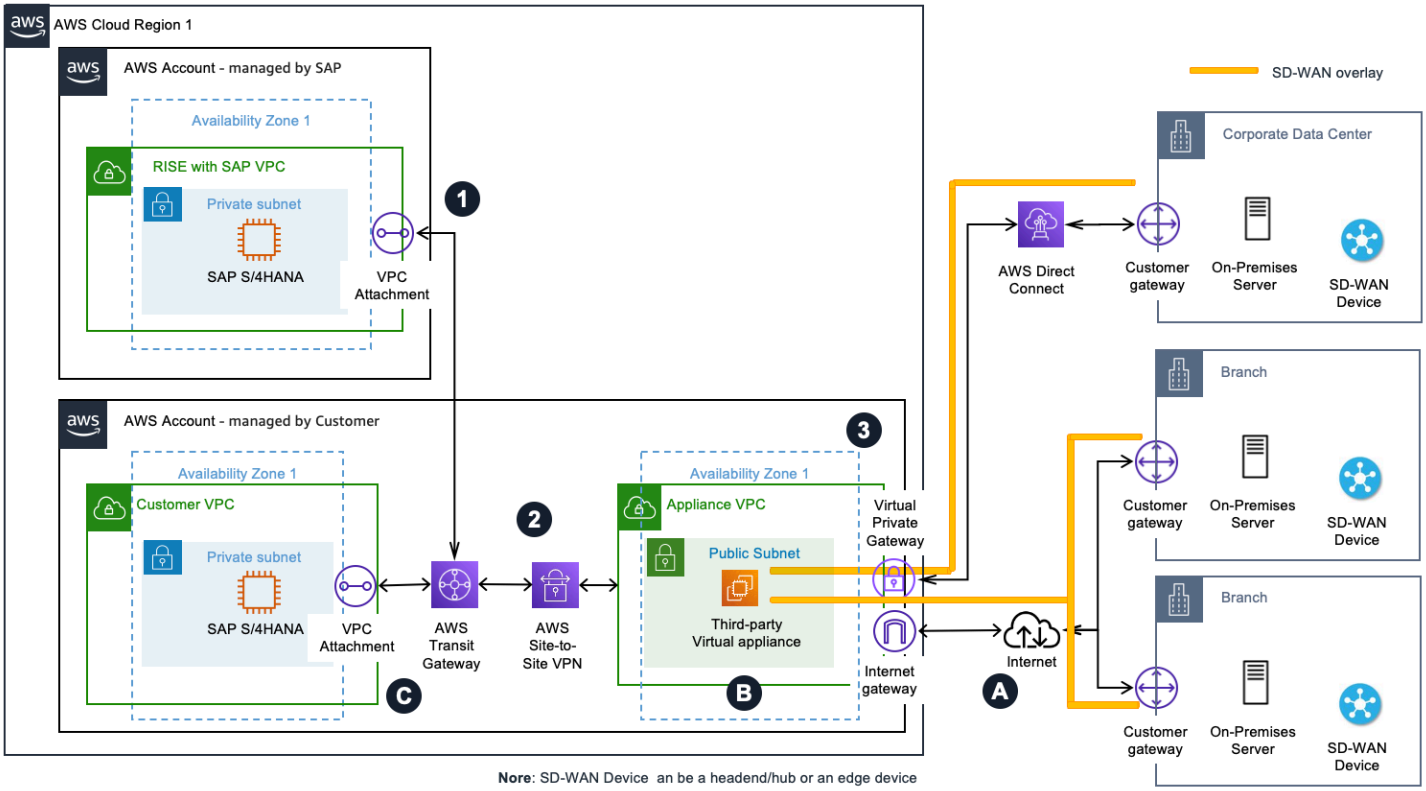
借助 SAP 实现入站提升：

A. 从外部分支机构 AWS 到 RISE VPC 的流量通过互联网通过 SD-WAN 覆盖到达设备 VPC 的互联网网关。同样，从公司数据中心到 RISE VPC 的流量通过 Direct Connect 链路通过 SD-WAN 叠加层到达设备 VPC 的虚拟专用网关。

B. 设备 VPC 中的第三方虚拟设备通过连接附件将流量转发到 Transit Gateway。

C. Transit Gateway 将流量转发到目标 RISE VPC。

模式 B-2：与 VPN 集成的 SD-WAN 设备 AWS AWS Site-to-Site



上图说明了一种模式，即使用 AWS 站点-站点 VPN 连接将软件定义广域网网络与 Transit Gateway 集成，并将软件定义广域网网络的（第三方）虚拟设备放置在 aws 内的设备 VPC 中。当您的第三方虚拟设备不支持 GRE 时，您可以使用此选项。通常在分支机构和本地数据中心部署 SD-WAN 边缘设备以创建全网状拓扑。

使用 SAP 从 RISE 出站：

1. 从 RISE VPC 发起到企业数据中心的流量将路由到 Transit Gateway 弹性网络接口 (TGW ENI)。
2. 流量使用 Site-to-Site VPN 连接在 Transit Gateway 和第三方虚拟设备之间路由。
3. 第三方虚拟设备封装了流量，该流量使用 Direct Connect 链路之上的 SD-WAN 叠加层到达公司数据中心。

借助 SAP，入境量将上升：

A. 从外部分支机构 AWS 到 RISE VPC 的流量通过互联网通过 SD-WAN 覆盖到达设备 VPC 的互联网网关。同样，从公司数据中心到 RISE VPC 的流量通过 Direct C AWS onnect 链路通过 SD-WAN 叠加层到达设备 VPC 的虚拟专用网关。

B. 设备 VPC 中的第三方虚拟设备通过 VP Site-to-Site N 连接将流量转发到 Transit Gateway。

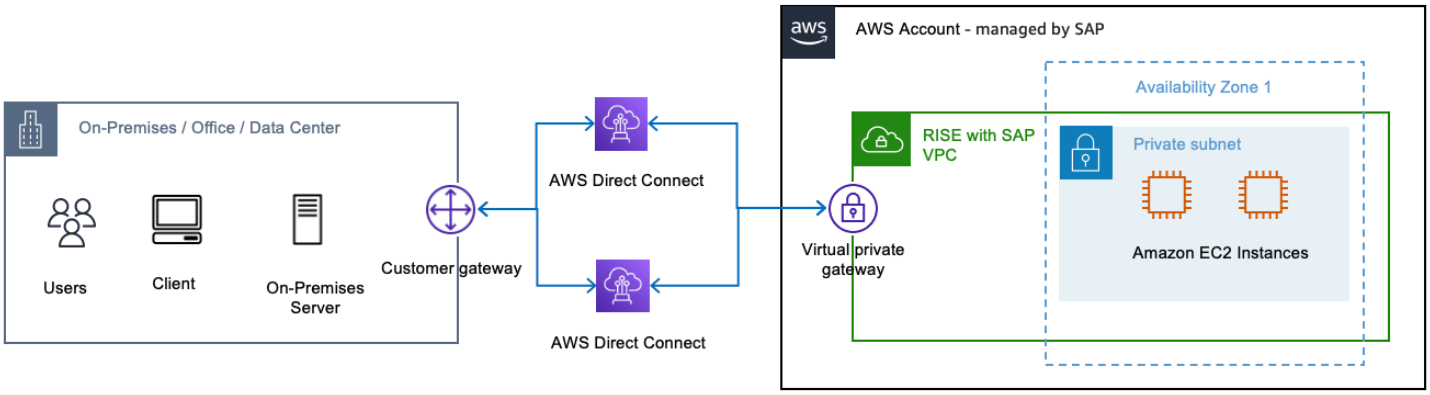
C. Transit Gateway 将流量转发到目标 RISE VPC 的 TGW ENI。

RISE 与您的本地网络之间连接的实施步骤

本节将更深入地探讨RISE与SAP与您的本地环境（不使用任何客户托管 AWS 帐户）之间的连接的实施步骤。我们将介绍的两个选项是：第一，为关键工作负载创建高弹性的部署；第二，为非关键工作负载创建具有成本效益的替代方案。

对于每个选项，我们将明确说明 SAP 需要的细节，以及你将在本地环境中采取的步骤。

选项 1：关键工作负载的弹性部署



AWS Direct Connect (DX) 有两种连接类型，即专用连接和托管。专用 DX 是与单个客户关联的物理以太网连接，位于客户的专用网络和 aws 之间。托管 DX 是 Di AWS rect Connect 合作伙伴代表客户配置的物理以太网连接。了解 AWS Direct Connect 以熟悉该服务。

要为你的 RISE 和 SAP 部署设置弹性的 Direct Connect 解决方案，请按照以下实施步骤操作：

先决条件

在配置 Direct Connect 连接之前，请确保您的本地网络已准备就绪。这包括：

- 有关路由器配置的详细指导，请查看有关使用 AWS Direct Connect 的 BGP 的 AWS 文档。

- 使用 MD5 身份验证在路由器上配置边界网关协议 (BGP)。BGP 是使用 Direct Connect 的必备条件。
- 验证您的网络是否可以支持多个 BGP 连接以实现冗余。

启动安装过程

首先联系你的 SAP ECS（企业云服务）代表，申请 RISE with SAP on Di AWS rect Connect 设置的“AWS 连接问卷”。本调查问卷将帮助收集必要的信息，以提供 Direct Connect 连接。

我们建议您为计划建立的每个 Direct Connect 连接填写调查问卷，设置冗余连接以实现高可用性。查看 Direct Connect 弹性建议，了解最佳实践。

填写 SAP 问卷

填写 AWS 连接调查问卷时，请指定要设置弹性的 Di AWS rect Connect 配置。

在调查问卷中，提供有关您的 Direct Connect 连接的以下详细信息：

- 无论是新的还是专用 Direct Connect 连接
- 你将使用的 Direct Connect 提供商或合作伙伴
- 具体的 Direct Connect 区域/位置
- 所需的 Direct Connect 链路的最小数量
- 主 Direct Connect 链路和辅助 Direct Connect 链路的子网 CIDR 块（采用 /30 CIDR 格式）
- VLAN ID
- 本地路由器的自治系统号 (ASN)
- 本地网络的 IP 地址范围（以便正确配置防火墙）此外，还应包括有关您的本地路由器的信息，例如品牌、型号和接口详细信息。

将填好的问卷提交给您的 SAP ECS 代表。然后，SAP 将使用这些信息在 aws 上的 RISE with SAP 环境中配置必要的 Direct Connect 资源。

SAP 的责任

在您提交填写好的调查问卷后，SAP 将处理以下任务（以下列表仅供参考）：

- 创建虚拟接口（取决于您的 DX 类型：托管还是专用）

- 创建直连 Connect 网关
- 如果你需要 SAP 在 RISE VPC 中配置 Transit Gateway，
  - 设置 Transit Gateway（包括您提供的 ASN）
  - 为您的 VPC 创建 Transit Gateway 附件
  - 更新路由表以允许 Transit Gateway 通过 SAP 网络 VPC 与 RISE 通信
  - 将 Transit Gateway 与 Direct Connect Gateway 关联，包括 RISE 的 CIDR 与 SAP 网络，该网络将通告到你的网络

完成安装过程

收到来自 SAP 的必要信息（例如 VLAN ID、BGP 对 IPs等体和可选的 BGP 身份验证密钥）后，请相应地配置本地路由器。这包括为 Direct Connect 连接设置 VLAN 接口和 BGP。有关详细说明，请参阅有关 Di rect Connect 路由器配置的 AWS 文档。

配置 active/active 拓扑：实施路由策略以平衡冗余的 Direct Connect 连接上的流量，利用 BGP 社区或更具体的子网通告来影响从本地网络 AWS 到您的本地网络的路径选择。

建立和测试连接

与 SAP 协调，为两个 Direct Connect 连接启用 BGP 会话。通过模拟一个连接的故障来验证 BGP 路径并测试故障转移方案，以确保流量正确故障转移到另一个连接。

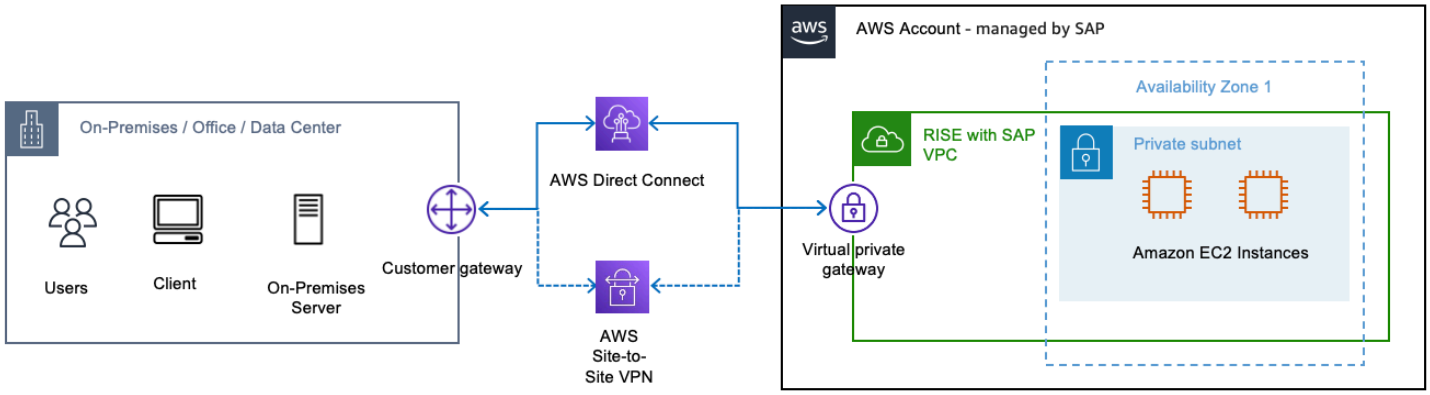
确认两条路径都与 SAP 的 end-to-end连接。您还可以利用 Di AWS rect Connect Resiliency Toolk it 执行定期故障转移测试，验证连接的弹性，并验证连接的弹性。

保持连接

根据需要定期检查和更新 Direct Connect 配置。与 SAP 协调所有变更。监控两个连接的性能和可用性，有关最佳实践，请参阅有关监控 Direct Connect 的 AWS 文档。

通过执行这些步骤，您可以建立弹性的 Di AWS rect Connect 解决方案，在开启 SAP 环境的情况下将您的本地基础设施与 RISE 安全地连接 AWS，从而确保高可用性和可靠的网络性能。

选项 2：非关键工作负载的经济高效替代方案



一些 AWS 客户更喜欢将一个或多个 Di AWS rect Connect 连接作为其主要连接 AWS，再加上成本较低的备份解决方案。此外，他们可能想要一种灵活且适应性强的连接，这种连接可以在全球网络位置之间快速建立或停用。为了实现这些目标，他们可以通过 AWS Site-to-Site VPN 备份实现 AWS Direct Connect 连接。

Site-to-SiteVPN 连接由三个关键组件组成：

1. 虚拟专用网关 (VGW)-旁边的路由器 AWS
2. 客户网关 (CGW)-客户端的路由器
3. 在 active/passive 配置中通过两 IPSec 条安全隧道将 VGW 和 CGW 绑定在一起的 S2S VPN 连接有关建立 AWS Site-to-Site VPN 连接的详细文档，您可以参考.html 上的文档。 AWS https://docs.aws.amazon.com/vpn/ latest/s2svpn/SetUpVPNConnections

先决条件

此方法建立在前面的选项 1 中概述的设置弹性 AWS 直接连接解决方案的步骤之上。完成这些 Direct Connect 实施步骤后，您可以添加 Site-to-Site VPN 连接作为故障转移选项。

在配置 Direct Connect 连接时，您可以开始为 VPN 设置准备本地基础架构：* 查看 Site-to-Site VPN AWS 文档，了解要求和最佳实践。* 确保您的防火墙允许 VPN 隧道所需的流量。* 确认您有两台客户网关设备或一台能够管理多个 VPN 隧道的设备。

添加 Site-to-Site VPN 连接可为您的主要 Direct Connect 链路提供更快、更灵活的备份。这与设置 Direct Connect 的过程类似，但有一些主要区别。

启动安装过程

首先，再次联系您的 SAP ECS 代表，并申请 “AWS 连接问卷”，以便在 AWS 设置时将 AWS Site-to-Site VPN 连接添加到 RISE。告知 SAP 你打算将 VPN 作为故障转移到你的 Direct Connect 链路。

填写 SAP 问卷

这次填写 AWS 连接调查问卷时，请指定除了 Direct Connect 连接之外还要设置 AWS Site-to-Site VPN。

在 AWS 连接调查问卷中，除了为 DX 填写的详细信息外，您还需要提供有关 VPN 连接的以下信息：

- 客户 VPN 网关详细信息，例如您的客户网关设备的品牌和型号
- 客户 VPN 网关面向互联网的公有 IP 地址
- 路由类型（静态/动态）
- 用于动态路由的 BGP ASN（BGP 的客户网关 ASN）。 仅支持 16 位 ASN。 ）
- BGP 会话 AWS 一侧的 ASN（16 位或 32 位 ASN）
- 客户端 BGP 对等 IP 地址（如果与提供的 VPN 对等 IP 不同）
- 第二个公有 IP 地址（可选：仅当使用主动-主动模式时）
- 客户本地网络 IP 范围将填写好的调查表提交给 SAP。然后，他们将创建 VPN 连接并为您提供配置详细信息。

SAP 的责任

在您提交填写好的调查问卷后，SAP 将处理以下任务（以下列表仅供参考）：* 创建客户网关（使用您提供的信息，例如 BGP ASN、IP 地址和可选的私有证书）* 创建 AWS Site-to-Site VPN 并通过 SAP Transit Gateway 和您的客户网关将其附加到 RISE * 提供 VPN 配置文件供您在本地路由器上设置 * 如果你需要 SAP 在 RISE VPC 中配置 Transit Gateway，SAP 将向 Transit 添加必要的路由网关路由表并更新安全组

使用从 SAP 收到的信息，在本地路由器上配置 VPN 隧道。实施路由策略，优先选择 Direct Connect 连接而不是 VPN 作为主路径。

有关必要设置的指导，请参阅有关 Di rect Connect 路由器配置的 AWS 文档。

测试和验证连接

与 SAP 协调以启用 VPN 连接并验证 end-to-end连通性。通过模拟 Direct Connect 故障来测试故障转移场景，并确保流量正确故障转移到 VPN。

向 SAP 确认 Direct Connect 和 VPN 路径的故障转移是否按预期运行。

保持连接

定期检查和更新 Direct Connect 和 VPN 连接的配置。与 SAP 协调所有变更。

监控两个连接的性能和可用性，有关最佳实践，请参阅有关监控 Direct Connect 和 VPN 的 AWS文档。

通过实施这款 Direct Connect with Site-to-Site VPN 故障转移解决方案，您可以在开启 SAP 部署的情况下为 RISE 实现高度弹性的连接设置 AWS，从而确保无缝故障转移和可靠的网络性能。

从您的 AWS 账户连接到 RISE

您可以通过以下方式从您的 AWS 账户连接到 RISE。

主题

- Amazon VPC 对等连接
- AWS Transit Gate
- AWS 直连 Connect 网关
- 使用您的单一 AWS 账户连接到 RISE
- 使用共享 AWS 着陆区连接到 RISE

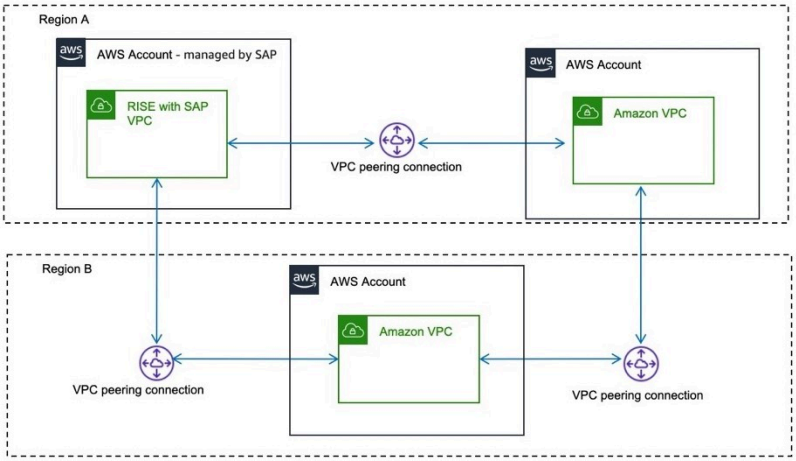
Amazon VPC 对等连接

VPC 对等互连 AWS VPCs 使用私 IPv4 有 IPv6 地址实现两者之间的网络连接。实例可以通过同一个网络进行通信。有关更多信息，请参阅什么是 VPC 对等连接？

在设置 VPC 对等连接之前，您需要创建申请，以获得 SAP 的批准。要成功实现 VPC 对等互连，定义的 IPv4 无类域间路由 (CIDR) 块不得重叠。请向 SAP 查询，了解可以在 RISE 和 SAP VPC 中使用的 CIDR 范围。

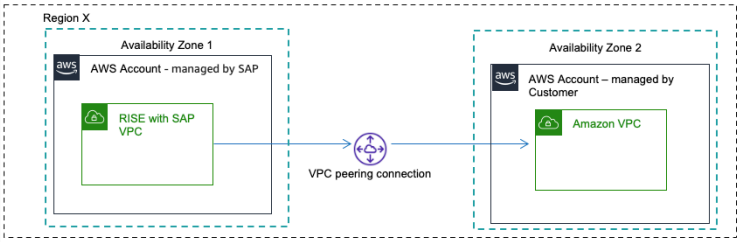
VPC 对等互 one-on-one连是相互之间的连接 VPCs，不是可传递的。流量无法通过中间 VPC 从一个 VPC 传输到另一个 VPC。您必须设置多个对等连接才能在 RISE 与 SAP VPC 和多个 VPCs对等连接之间建立直接通信。

VPC 对等互连可以跨 AWS 区域使用。所有区域间流量都经过加密，没有单点故障或带宽瓶颈。流量保持 AWS 在全球网络上，永远不会穿越公共互联网，从而减少了常见漏洞利用和 DDo S 攻击的威胁。



可用区内的 VPC 对等互连的数据传输是免费的，跨可用区的 “数据输入” 和 “数据输出” 按每 GB 收费。跨区域 VPC 对等互连的数据传输按每 GB 的 “输出” 收费。有关更多信息，请参阅 Amazon EC2 定价。在您的 AWS 账户中，使用 SAP 管理的 AWS 账户的可用区 ID 以避免跨可用区数据传输费用。您可以向 SAP 索要可用区 ID。有关更多信息，请参阅您的 IDs AWS 资源的可用区。

定价示例-跨可用区域的 VPC 对等



从 AWS 账户发送的 100GB 数据（由 SAP 通过 VPC Peering 管理）到该 AWS 账户的数据由客户管理，包括： AZs

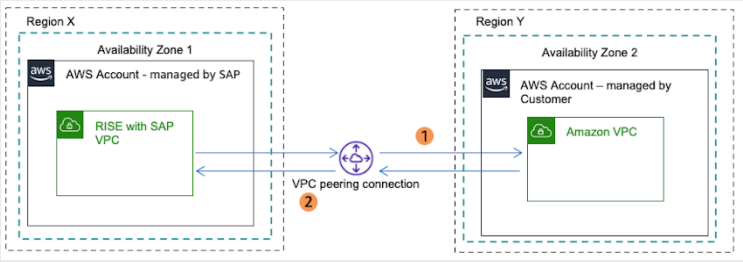
100GB * 每 GB 0.01 美元 = 1 美元（出账——计入 AWS 账户 — 由 SAP 管理）和 100GB * 每GB 0.01美元 = 1 美元（输入——账单到账户 — 由客户管理） AWS

由于数据传输费用已包含在RISE订阅中，因此由客户管理的 AWS 账户将仅产生流量费用，例如每GB0.01美元。

[注意：当发件人是 AWS 账户——由客户管理而收款人是账户——由 SAP 管理时，费用示例也适用] AWS

定价示例-跨区域 VPC 对等

[注意：不同 AWS 地区的费用各不相同。有关更多信息，请参阅：Amazon EC2 定价 [数据传输]



1)。从 AWS 账户发送的 100GB 数据（由 SAP 通过 VPC Peering 与 AWS 账户对等互连管理）由跨区域的客户管理。

100GB *（每GB 0.01-0.138美元）= 1-13.8美元（出账——账单到账——由 SAP 管理） AWS

由于数据传输费用已包含在RISE订阅中，因此本示例中由客户管理的 AWS 账户不会产生费用。

2)。从 AWS 账户发送的 100GB 数据（由客户通过 VPC Peering 向 AWS 账户管理）由 SAP 跨区域管理。

100GB *（每 GB 0.01-0.138 美元）= 1-13.8 美元（已出账——账单到账户 — 由客户管理） AWS

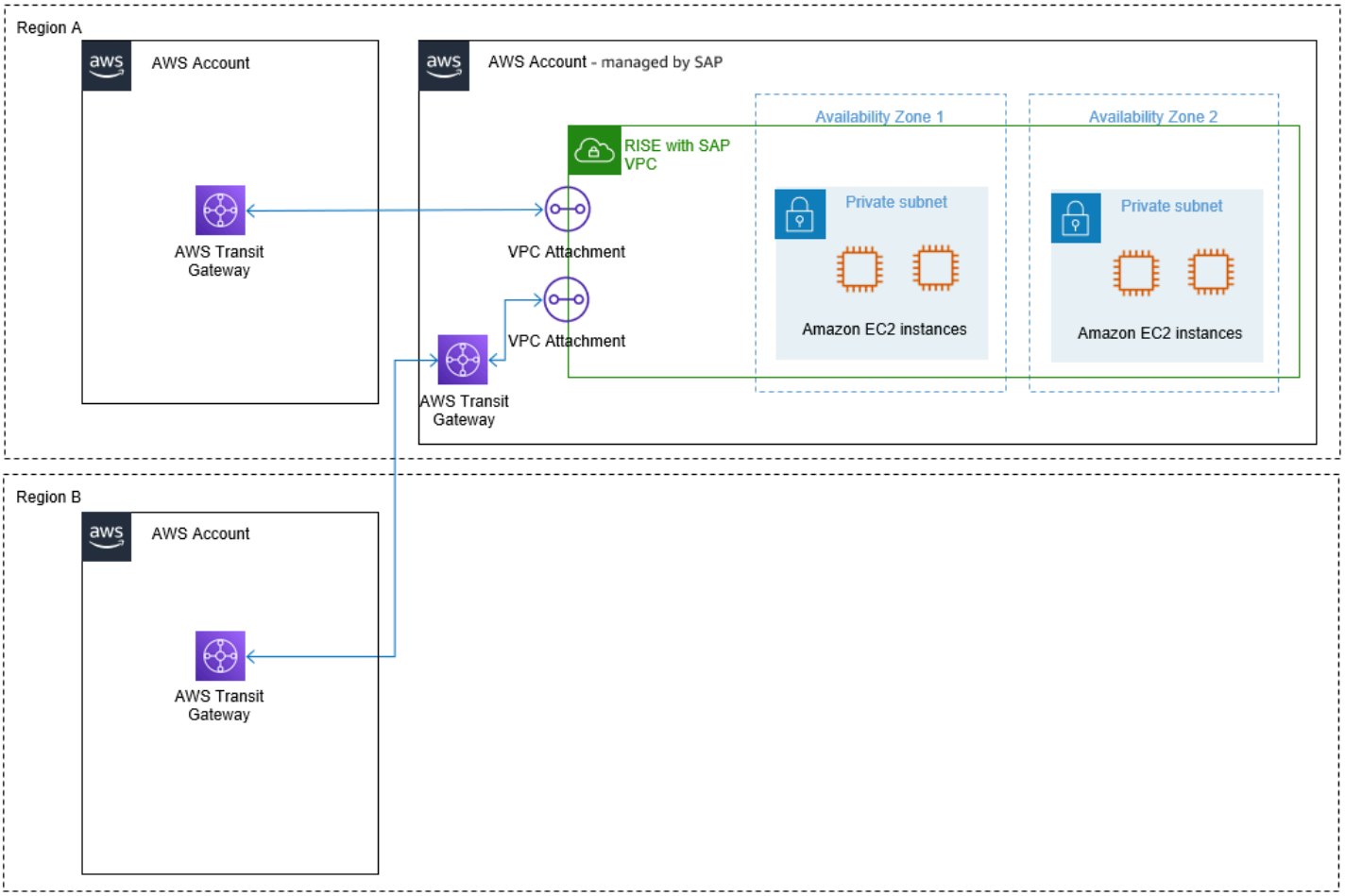
由于数据传输的成本是针对 “数据输出” 计算的，因此本示例将由客户管理的 AWS 账户承担费用。

AWS Transit Gate

AWS Transit Gateway 是连接亚马逊 VPCs的网络交通枢纽。它充当云路由器，通过充当中央通信中心来解决复杂的对等互连设置问题。您只需与 SAP 管理的 AWS 账户建立一次此连接。

你自己的 AWS 账户中的 Transit Gateway

要与 SAP 管理的 AWS 账户建立连接，请在 AWS 账户中通过 AWS 资源访问管理器 (RAM) 创建和共享 Tr AWS ansit Gateway。然后，SAP 会创建一个附件，使流量能够流经路由表中的条目。由于 AWS Transit Gateway 位于您的 AWS 账户中，因此您可以保留对流量路由的控制权。有关更多信息，请参阅 T ransit 网关对等连接附件。



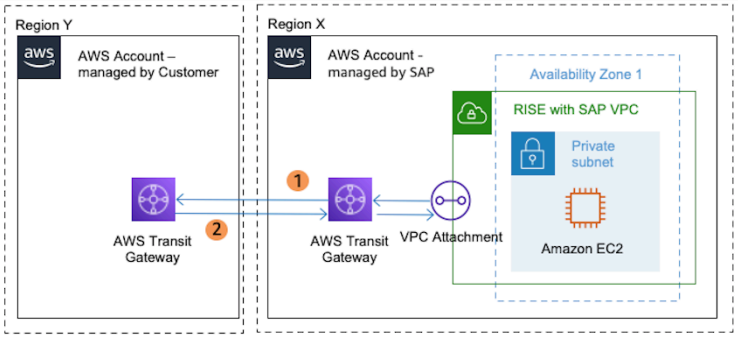
SAP 管理的 AWS 账户中的 Transit Gateway

当你已经在另一个 AWS 地区拥有 Transit Gateway，并且无法在该地区创建另一个拥有 RISE with SAP AWS 账户的 Transit Gateway 账户时，SAP 可以为 RISE 中的 Transit Gateway 提供将由 SAP 管理的 SAP 账户。你可以通过 Transit Gateway Peering 在 Transit Gateway 和 SAP 托管的 Transit Gateway 您无法将 RISE 环境之 VPCs 外的 VPC 附件连接到 SAP 管理的 Transit Gateway。

对于对等连接附件，每位 Transit Gateway 所有者每小时按小时收取与其他 Transit Gateway 的对等连接费用，因此，由 SAP 管理的 SAP 账户中 Transit Gateway 的对等连接的每小时费用是 RISE 订阅的一部分。但是，客户账户 — 客户管理的 Transit Gateway 对等连接的每小时费用由客户收取。有关更多信息，请参阅：T ransit Gateway 定价

定价示例-跨不同地区的 Transit VPCs Gateway

[注意：不同 AWS 地区的费用各不相同。有关更多信息，请参阅：Amazon EC2 定价 [数据传输]



1)。从账户中 X 区域的 VPC 发送的 100GB 数据（由 SAP 通过位于 AWS 账户中的 Transit Gateway 进行管理），由 SAP 管理，发送到位于另一个区域 Y 的对等公交网关，该网关位于该账户中，由客户管理，结尾为 AWS 账户中的 VPC，由客户管理，由客户管理： AWS AWS

100GB * 每 GB 0.02 美元 = 2 美元（Transit Gateway 数据处理）+ 100GB *（每 GB 0.01-0.138 美元）= 1-13.8 美元（区域外）= 3-15.8 美元（总计-计入账户 — 由 SAP 管理） AWS

数据处理费用由发送流量到 Transit Gateway 的 VPC 所有者承担。由于发送方的 VPC 位于由 SAP 管理的 AWS 账户中，并且数据传输费用包含在 RISE 订阅中，因此客户管理的 AWS 账户不会为此示例产生数据传输费用。由于从对等互连附件发送到 Transit Gateway 的数据不收取数据处理费，而且入站区域间数据传输费用不收取，因此该 AWS 账户无需支付额外的数据传输费用，由客户管理。由客户管理的 AWS 账户仅按每小时每个 Transit Gateway 对等连接的费用进行计费。从可用区传出的数据将始终通过该可用区的 Transit Gateway 终端节点到达其他 VPC，因此不会产生跨可用区数据传输费用。

2)。从账户中 Y 区域的 VPC 发送的 100GB 数据（由客户通过位于 AWS 账户中的 Transit Gateway 进行管理），由客户管理，发送到位于不同区域 X 的对等公交网关（由 SAP 管理，结尾为账户中的 VPC），由 SAP 管理，由 SAP 管理，结尾为 AWS 账户中的 VPC，由 SAP 管理： AWS AWS

100GB * 每 GB 0.02 美元 = 2 美元（Transit Gateway 数据处理）+ 100GB *（每 GB 0.01-0.138 美元）= 1-13.8 美元（区域外）= 3-15.8 美元（总计-账入账户 — 由客户管理） AWS

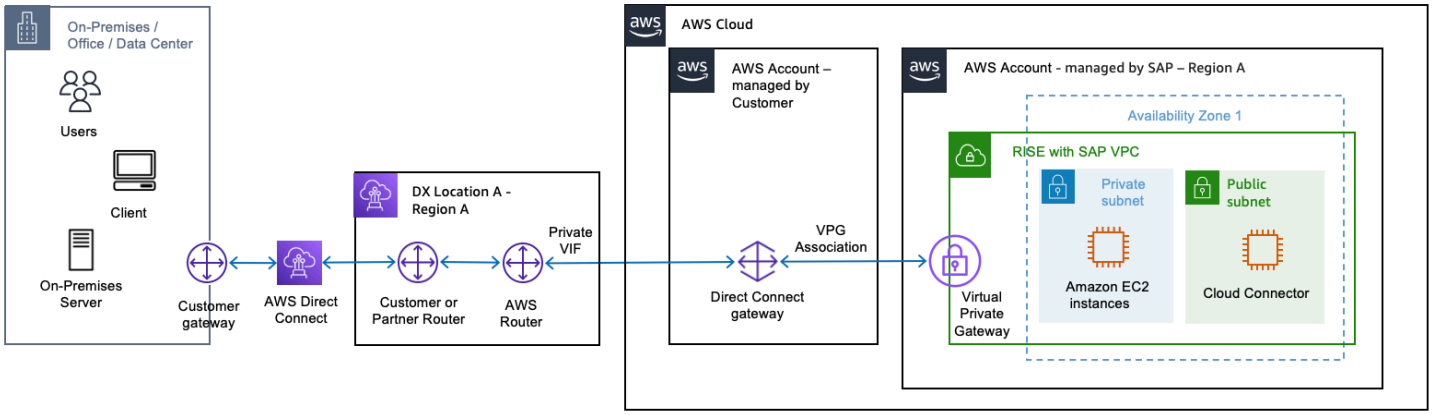
数据处理费用由发送流量到 Transit Gateway 的 VPC 所有者承担。由于发送方的 VPC 位于 AWS 账户中（由客户管理），因此本示例的所有数据传输费用均由客户管理的 AWS 账户计费。此外，由客户管理的 AWS 账户将按每小时 Transit Gateway 对等连接的费用进行计费。

AWS 直连 Connect 网关

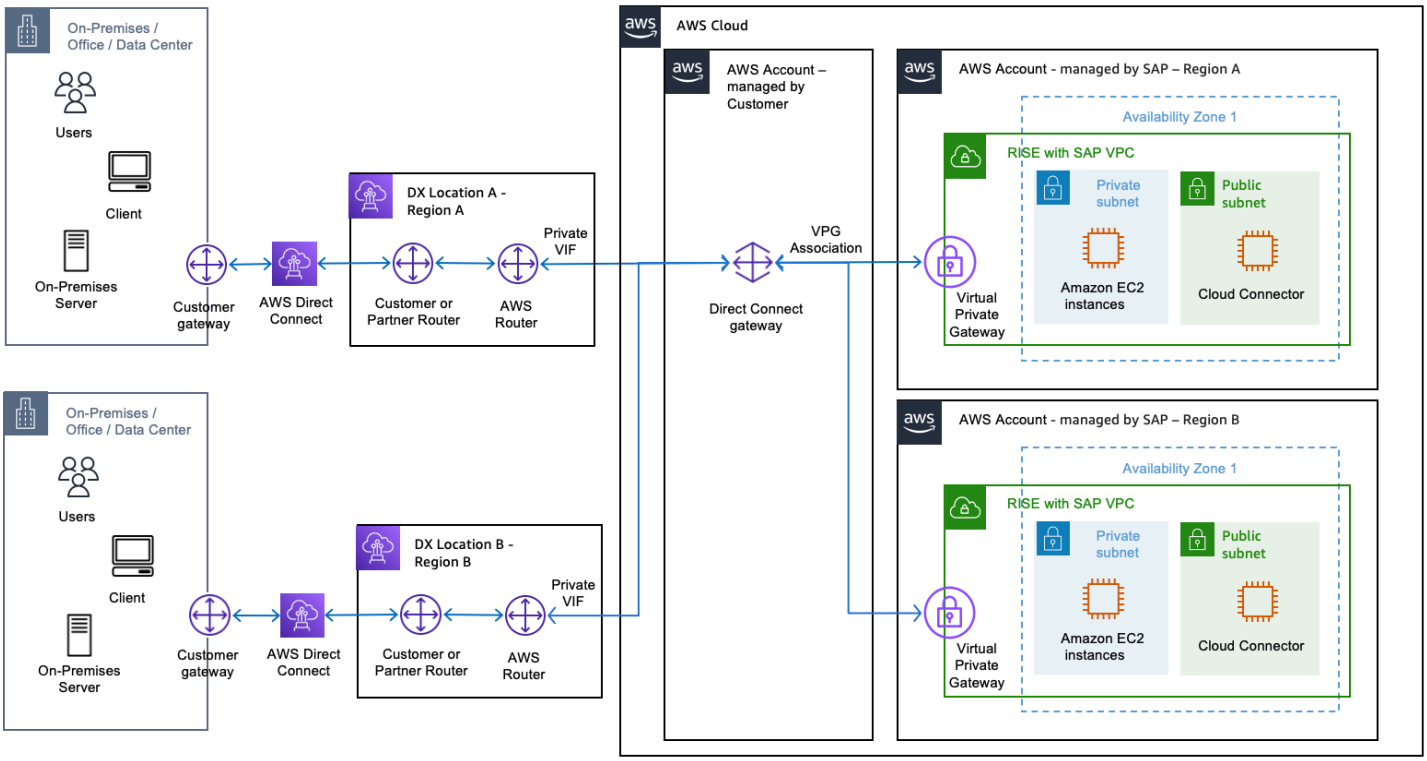
AWS Di@@ rect Connect 网关是一项全球服务，可让您在本地网络与不同 AWS 地区的多个 Amazon VPCs 之间建立私有连接。这个集中式连接中心允许您整合网络架构，降低复杂性，维护安全的高带宽连接，同时避免为任务关键型工作负载使用公共互联网。

AWS 您自己的 AWS 账户中的 Direct Connect 网关

要与 SAP 管理的 AWS 账户建立连接，请创建将流量从私有 VIF 路由到 VPC 私有网关的 Di AWS rect Connect 网关。由于 AWS Direct Connect 网关位于您的 AWS 账户中，因此您可以保留对流量路由的控制权。

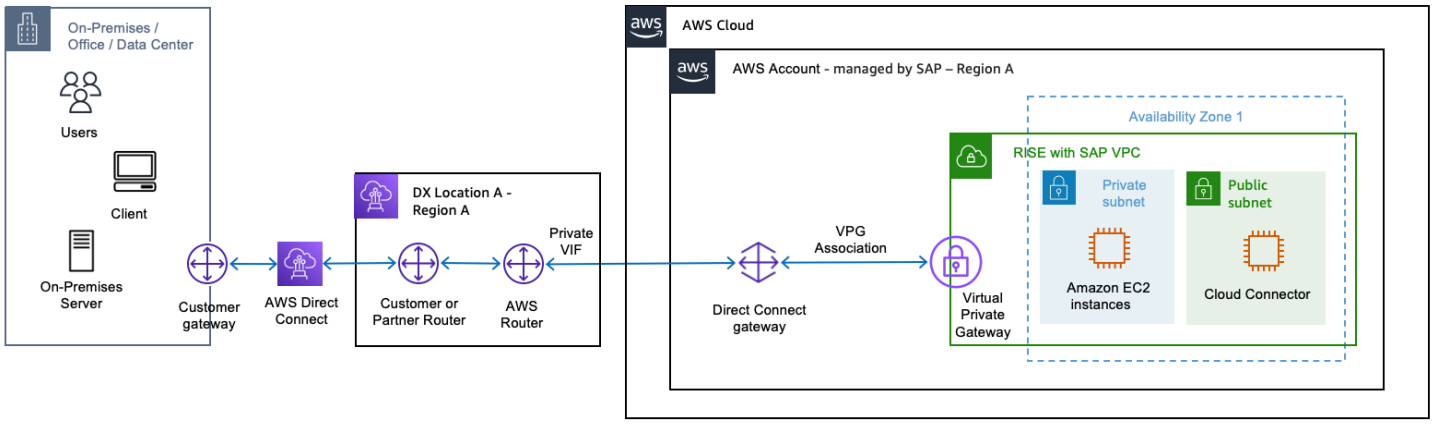


当你需要从多个本地站点进行连接时，将多个 AWS 区域用于带有 SAP and/or 的 RISE（即远程灾难恢复），则可以使用 Direct Connect Gateway 来简化连接



AWS SAP 管理的 AWS 账户中的 Direct Connect 网关

如果您不需要拥有和管理 AWS 账户，则可以请求 SAP 提供 Di AWS rect Connect 网关，该网关属于由 SAP 管理的 AWS 账户的一部分。



Di AWS rect Connect 网关本身不收取额外费用。你可以从 Di AWS rect Connect 中了解更多信息 FAQs。

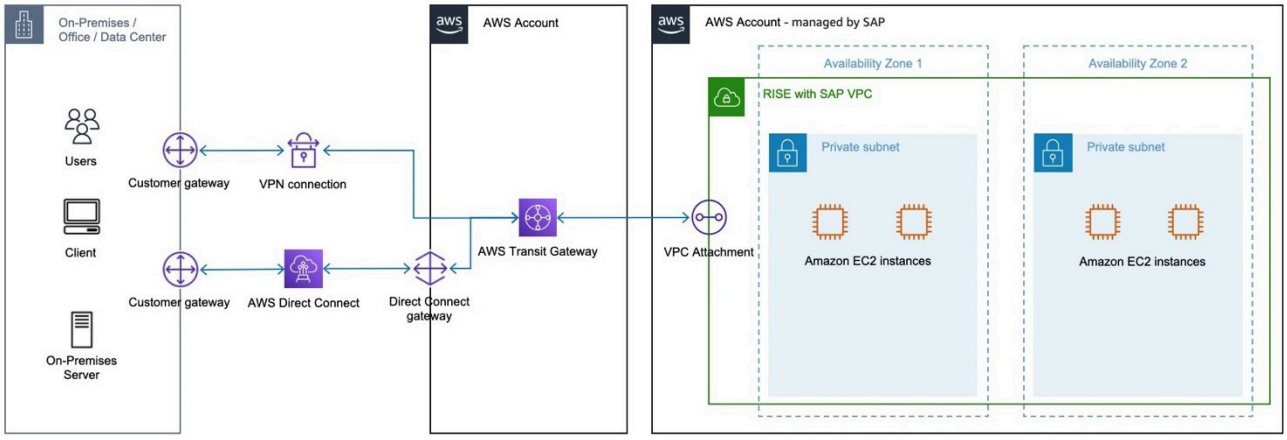
使用您的单一 AWS 账户连接到 RISE

您可以使用您的 AWS 账户在本地和 RISE 之间通过 SAP VPC 建立连接。此方法为您提供更多控制权，但也需要在您的 AWS 账户中管理 AWS 服务。您可以使用以下任一选项。

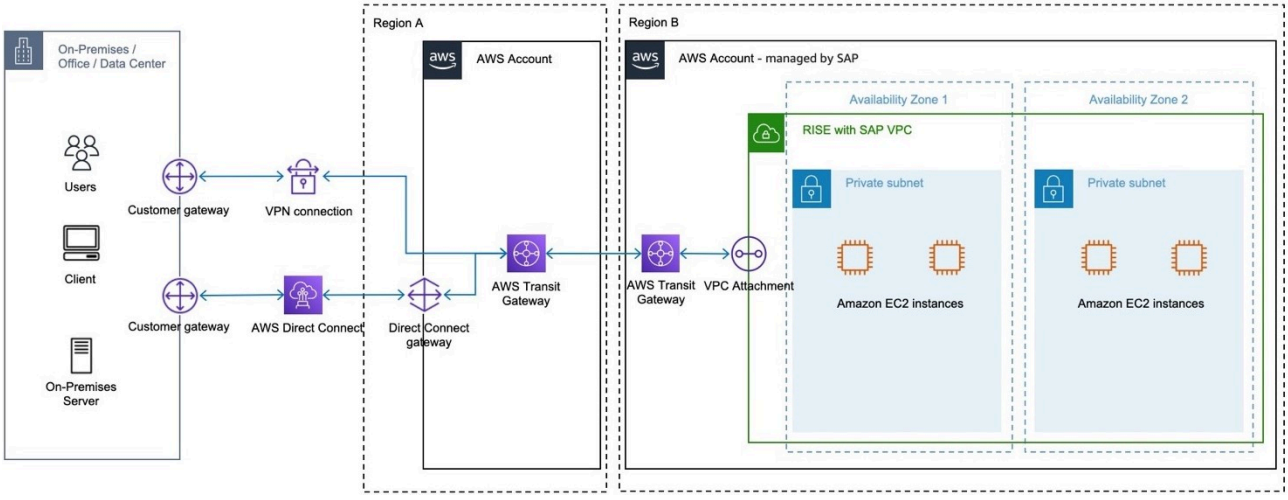
- AWS Transit Gateway — 与 AWS SAP 管理的账户共享您 AWS 账户中的 T AWS ransit Gateway 资源。
- AWS 使用 T AWS ransit Gateway 的 IPsec VPN — 通过互联网在远程网络和传输网关之间创建 VPN 连接。有关更多信息，请参阅 AWS Site-to-Site VPN 的工作原理和传输网关 VPN 附件。
- Direct Connect 网关 — 创建带有传输虚拟接口的 Direct Connect 网关。有关更多信息，请参阅连接到 Di rect Connect 网关的公交网关。

  要增强安全性，请参阅如何通过 Di AWS rect Connect 连接建立 AWS VPN？

下图显示了相同 AWS 区域内的此选项。



下图显示了不同 AWS 区域的此选项。



当您选择 AWS Site-to-Site VPN 和/或 AWS Direct Connect 使用账户中的 Transit Gateway 在本地和带有 SAP VPC 的 RISE 之间建立连接时，使用 AWS 账户中的 Transit Gateway（由客户管理），与使用 SAP VPC 的 RISE 位于同一 AWS AWS 区域或不同的区域，则适用以下条件。

每小时费用：

由于 AWS Site-to-Site VPN 驻留在 AWS 账户中（由客户管理），并与 AWS 账户中的 Transit Gateway 挂钩（由客户管理），因此 VPN 连接费用和 Transit Gateway 连接费用将 AWS 记入账户，由客户管理

由于 Direct Connect 和 Direct Connect Gateway 驻留在 AWS 账户中（由客户管理），并连接到 AWS 账户中的公交网关（由客户管理），因此 Di AWS rect Connect 端口工时费用和 Transit Gateway 连接费用将 AWS 记入账户，由客户管理。

对于对等连接附件，每位 Transit Gateway 所有者按小时计费与其他 Transit Gateway 的对等连接费用。

数据处理费用：

从 VPC、Direct Connect 或 VPN to/via （Transit Gateway）发送的每千兆字节收取数据处理费。

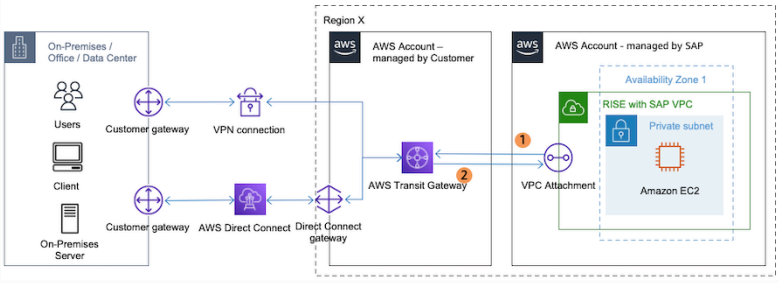
根据来源和目的地，数据处理费用各不相同，将计入由客户管理的 AWS 账户，或者已经包含在RISE 订阅中（有关成本估算示例：见下文）

有关更多信息，请参阅：

- AWS Site-to-Site VPN 定价
- AWS 直连 Connect 定价
- Transit Gatewa

定价示例 — 通过 VPN 或 Direct Connect VPCs 在同一地区的 Transit Gateway

[注意：不同 AWS 地区的费用各不相同。有关更多信息，请参阅：Amazon EC2 定价 [数据传输]



1)。从账户中的 VPC 发送的 200GB 数据（由 SAP 通过位于 AWS 账户中的 Transit Gateway 进行管理），由客户通过 VPN 或 AWS 账户中的 Direct Connect 管理，由 SAP 管理到本 AWS 地：

200GB * 每 GB 0.02 美元 = 4 美元（Transit Gateway 数据处理）+ 100 GB * 每 GB 0.09 美元 = 9 美元（VPN 数据传出，前 100 GB 免费，然后每 GB 0.09 美元）= 13 美元（向账户计费的数据传输总额 — 由 SAP 管理） AWS

或

200GB * 每 GB 0.02 美元 = 4 美元（Transit Gateway 数据处理）+ 200GB *（每 GB 0.02-0.19 美元）= 4-38 美元（Direct Connect 数据传出）= 8-42 美元（向账户计费的数据传输总额 — 由 SAP 管理） AWS

数据处理费用由发送流量到 Transit Gateway 的 VPC 所有者承担。由于发送方的 VPC 位于由 SAP 管理的 AWS 账户中，并且数据传输费用包含在 RISE 订阅中，因此在本示例中，由客户管理的 AWS 账户不会产生数据传输费用。

2)。通过账户中的 VPN 或 Direct Connect 从本地发送的 200GB 数据 — 由客户通过位于 AWS 账户中的 Transit Gateway 进行管理 — 由客户管理到 AWS 账户中的 VPC — 由 SAP 管理： AWS

200GB * 每GB 0.00美元 = 0 美元（VPN 数据传入）+ 200GB * 每 GB 0.02 美元 = 4 美元（Transit Gateway 数据处理）+ 0 美元（VPN 数据传入）= 4 美元（向账户计费的数据传输总额 — 由客户管理） AWS

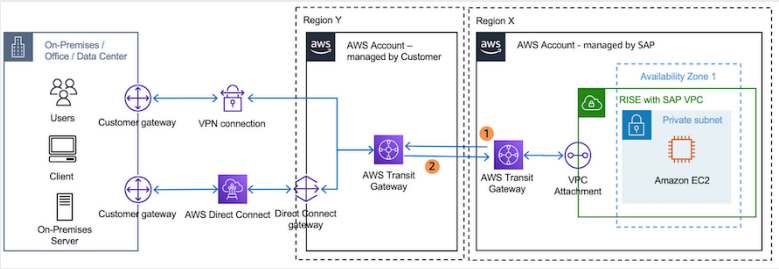
或

200GB * 每 GB 0.000 美元 = 0 美元（Direct Connect 数据传入）+ 200GB * 每 GB 0.02 美元 = 4 美元（Transit Gateway 数据处理）= 4 美元（计入账户的数据传输总额 — 由客户管理） AWS

数据传输 AWS 是免费的，这也适用于VPN和Direct Connect，因此唯一的数据处理费用是Transit Gateway的数据处理。由于 Transit Gateway 驻留在 AWS 账户中（由客户管理），因此数据传输费用由 AWS 账户收取，由客户管理

定价示例 — 通过 VPN 或 Direct Connect VPCs 在不同地区的 Transit Gateway

[注意：不同 AWS 地区的费用各不相同。有关更多信息，请参阅：Amazon EC2 定价 [数据传输]



1)。从账户中的 VPC 发送的 200GB 数据 — 由 SAP 通过 AWS 账户内的 Transit Gateway 进行管理 — 由 SAP 管理，与 AWS 账户中不同区域的 Transit Gateway 对等 — 由客户通过 VPN 或 AWS 账户中的 Direct Connect 进行管理 — 由客户管理到本 AWS 地：

200GB * 每 GB 0.02 美元 = 4 美元（Transit Gateway 数据处理）+ 200GB *（每 GB 0.01-0.138 美元）= 2-27.6 美元（区域外）+ 100GB * 每 GB 0.09 美元 = 9 美元（VPN 数据传输出去，前 100 GB 是免费的，然后是每 GB 0.09 美元）= 15-40.6 美元（向账户计费的数据总额 — 由 SAP 管理）AWS

或

200GB * 每 GB 0.02 美元 = 4 美元（Transit Gateway 数据处理）+ 200GB *（每 GB 0.01-0.138 美元）= 2-27.6 美元（区域外）+ 200GB *（每 GB 0.02-0.19 美元）= 4-38 美元（Direct Connect 数据传出）= 10-69.6 美元（计入账户的数据传输总额 — 由 SAP 管理） AWS

数据处理费用由发送流量到 Transit Gateway 的 VPC 所有者承担。由于发送方的 VPC 位于由 SAP 管理的 AWS 账户中，并且数据传输费用包含在 RISE 订阅中，因此在本示例中，由客户管理的 AWS 账户不会产生数据传输费用。

2)。通过账户中的 VPN 或 Direct Connect 从本地发送的 200GB 数据 — 由客户通过 AWS 账户内的 Transit Gateway 进行管理 — 由客户通过 AWS 账户中不同区域的对等 Transit Gateway 进行管理 — 由 SAP 向 AWS 账户中的 VPC 管理 — 由 SAP 管理： AWS

200GB * 每 GB 0.02 美元 = 4 美元（Transit Gateway 数据处理）+ 200GB * 每 GB 0.000 美元 = 0 美元（VPN 数据传入）+ 200GB *（每 GB 0.01-0.138 美元）= 2-27.6 美元（向账户计费的数据传输总额 — 由客户管理） AWS

或

200GB * 每 GB 0.02 美元 = 4 美元（Transit Gateway 数据处理）+ 200GB * 每 GB 0.000 美元 = 0 美元（Direct Connect 数据传入）+ 200GB *（每GB 0.01-0.138 美元）= 2-27.6 美元（向账户计费的数据传输总额 — 由客户管理） AWS

数据传输到输入 AWS 是免费的，这也适用于 VPN 和 Direct Connect，因此数据处理费用是 Transit Gateway 的数据处理费用和区域间数据传输费用。由于 Transit Gateway 位于由客户管理的 AWS 账户中，因此数据传输费用由客户管理的 AWS 账户收费。

使用共享 AWS 着陆区连接到 RISE

现代 SAP 环境有多种连接要求。可以通过本地和 AWS 云端以及各种 SaaS 解决方案和其他云服务提供商访问服务。

创建 AWS 着陆区有助于 RISE 与 SAP 的安全且可扩展的连接。它具有以下好处：

- 控制网络配置
- 能够在更广泛的 AWS 解决方案中重复使用 AWS Direct Connect 连接
- 减少了与其他 SaaS 解决方案和云服务提供商连接的网络跳跃和延迟，因为它们不是通过本地进行路由
- 能够通过使用 AWS 服务进行额外的管理和控制

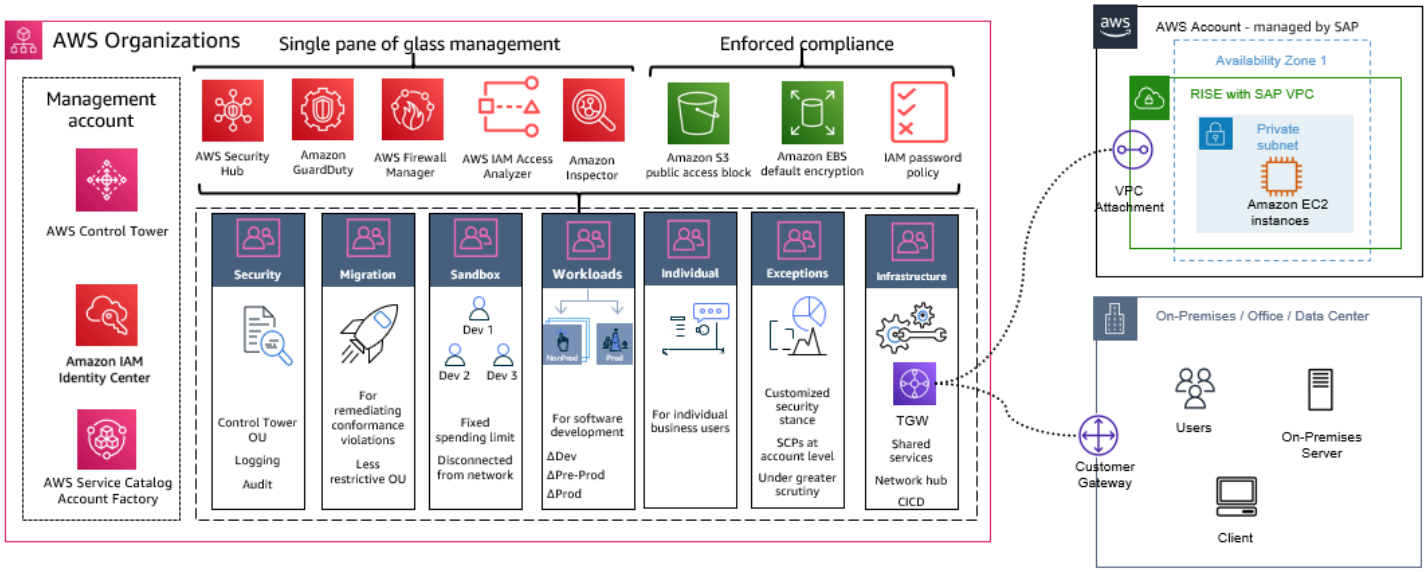
着陆区旨在通过自动设置遵循W AWS ell Architected 框架的 AWS 环境来帮助组织实现其云计划。它提供了可扩展性，可以满足所有场景，从最简单的连接（只需要通过SAP连接到本地环境的RISE）到连接多个SaaS解决方案 CSPs 、多个本地连接的复杂需求。

着陆区的关键组成部分和优势包括：

- 多账户结构 — 它使用组织单位 (OU) 结构为不同的工作负载设置多个 AWS 账户的基准环境。例如，生产、开发、共享服务等。
- AWS I@@ dentity and Ac cess Management — 它配置AWS 身份和访问管理 (IAM) 角色和策略，以实现安全访问和权限管理。
- 联网 — 它遵循网络隔离和安全的最佳实践，建立包含子网、路由表和安全组的 Amazon Virt ual Private Cloud（Amazon VPC）。
- 日志和监控 — 它配置诸如 AWS Config、AWS CloudTrail、Amazon 之类的 AWS 服务，GuardDuty用于集中记录、监控和审核资源变更和安全事件。

- 安全 — 它实施 AWS 安全最佳实践，例如启用 AWS Config 规则、设置 AWS CloudTrail 跟踪和创建 Sec AWS urity Hub 标准。
- 自动化 — 它使用AWS CloudFormation模板和 S AWS ervice Catalog 来自动部署和管理着陆区环境。
- 自定义 — 它允许根据特定的组织要求进行自定义和扩展，例如添加其他 AWS 服务或与现有本地基础设施集成。

我们建议使用带有 SAP 连接的 RISE AWS 着陆区。



建造着 AWS 陆区

你可以使用 Cont AWS rol Tower 实现 AWS 着陆区。它提供了建造着陆区的自动化流程，包括管理和治理服务。

在一个简单的场景中，着陆区包含的占地面积最小，侧重于连接，而连接通常以Tr AWS ansit Gateway为中心。有关更多信息，请参阅着陆区。

以下是该过程的总体概述：

1. 定义需求 — 了解您组织的安全、合规和运营需求。这将有助于确定着陆区中应包含的适当护栏、控制装置和服务。
2. 设计架构 — 规划整体架构，包括账户数量（管理、共享服务、工作负载账户）、网络设计（VPCs、子网、路由）、共享服务（记录、监控、身份管理）和安全控制（IAM、服务控制策略、护栏）。

3. 设置 C AWS on tro AWS l Tower — Control Tower 可根据最佳实践帮助设置和管理多账户 AWS 环境。它允许您创建和配置新 AWS 帐户，并在这些账户中部署基本安全配置。
4. 配置 AWS 组织 — O rganizations 使您能够集中管理和管理您的 AWS 帐户。通过创建必要的组织单位 (OUs) 和服务 AWS 控制策略 (SCPs) 在 Control Tower 中配置组织。
5. 部署核心账户和服务-创建和配置核心账户，例如管理账户、共享服务账户（用于日志记录、安全工具）以及任何其他必需的共享账户。部署共享服务，例如 CloudTrail Config 和 Security Hub。
6. 部署网络架构-设置网络架构，包括子网 VPCs、路由表和任何必要的网络设备或服务（例如， hub-and-spoke模型的 Transit Gateway）。
7. 配置 IAM — 建立 IAM 角色、策略和群组，以控制跨着陆区域账户的访问和权限。
8. 实施安全控制 — 部署安全服务和护栏，例如 Security Hub、Firewall Manager、 AWS WAF 和 Confi AWS g 规则，以强制执行安全最佳实践和合规要求。
9. 配置日志和监控-设置集中式日志和监控解决方案，例如 CloudWatch CloudTrail、和 Config，以捕获和分析着陆区账户中的日志和事件。
10. 部署工作负载帐户-使用您的着陆区部署工作负载帐户。你可以创建一个 AWS 账户，通过 SAP VPC 连接到 RISE。我们建议使用 Transit Gateway 进行转机，这样既灵活又便于管理。
11. 自动化和维护 — 使用 AWS CloudFormation 模板或其他基础设施即代码工具自动部署和维护着陆区资源。建立持续维护、更新和合规性检查的流程。

AWS 专业服务或AWS 合作伙伴通过SAP为RISE建立和维护着陆区（Landing zone）提供帮助。

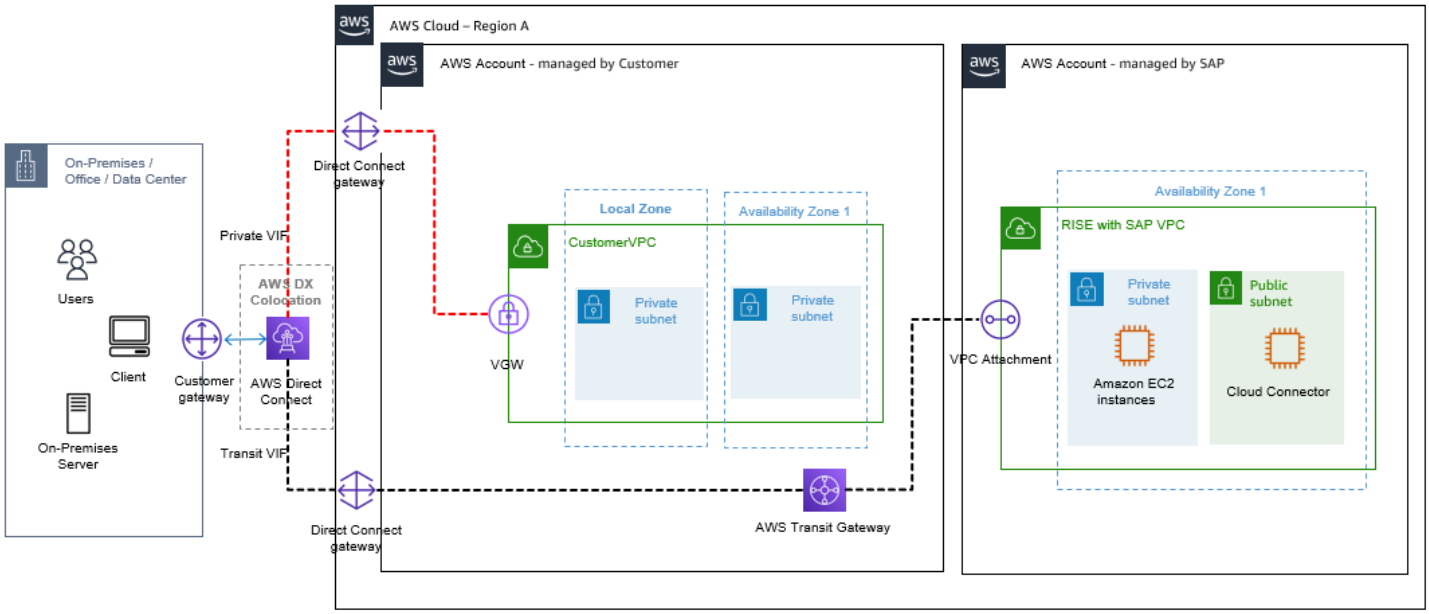
与客户管理的 AWS 着陆区相关的费用因所使用的 AWS 服务而异。本段所述的 AWS 服务有自己的定价模式。有关价格的更多信息，请参阅所列 AWS 服务的专用定价页面。

通过最近的 Di AWS rect Connect POP（包括 AWS 本地区域）连接到 RISE

AWS Direct Connect point-of-presence (POP) 是一种物理交叉连接，允许用户建立从其场所到 AWS 区域或 AWS 本地区域的网络连接。您可以使用最近的 Direct Connect POP（例如在 AWS 本地区域中），从更低的设置和运行成本中受益，网络延迟与在父 AWS 区域上运行的 SAP VPC 的 RISE 相同或更低。有关更多信息，请参阅 AWS Direct Connect 流量与 AWS 本地区域。

以下是一个示例场景-您居住在菲律宾，并且您想在 AWS 新加坡地区部署带有 SAP 的 RISE。你可以在马尼拉使用 Direct Connect POP 从本地数据中心或办公室设置 Direct Connect。与直接连接到新加坡 AWS 地区相比，该策略提供了更低的网络延迟。

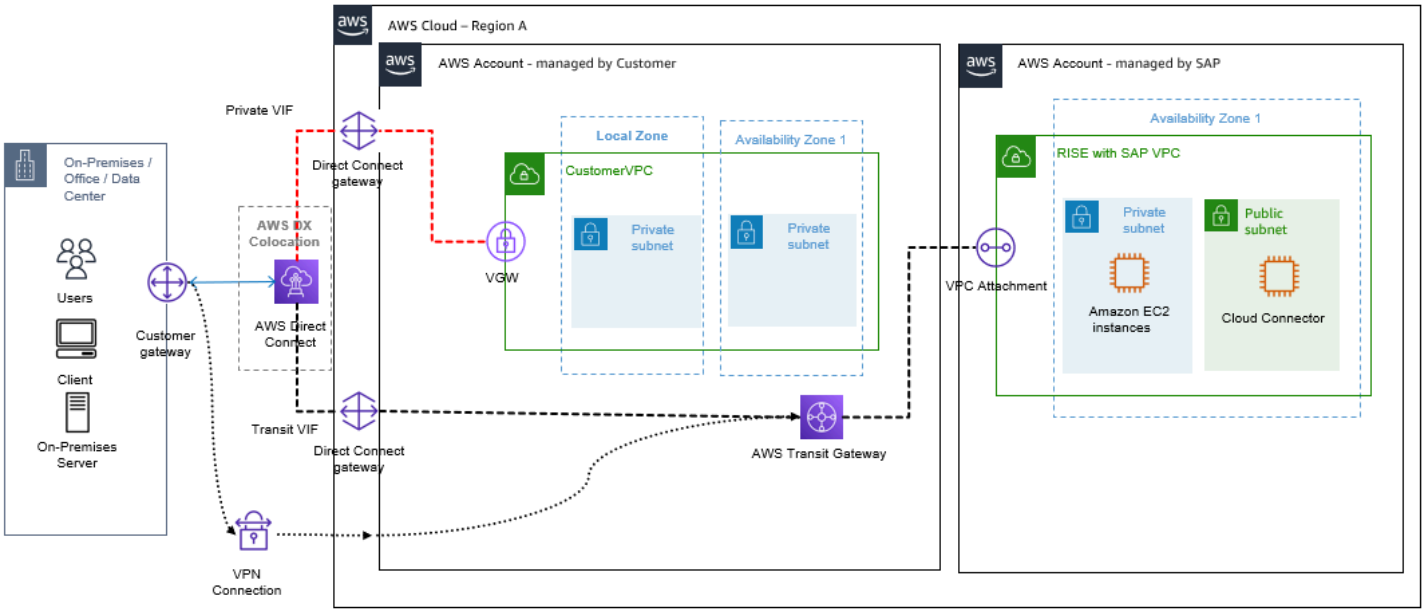
下图显示了通过最近的 Di AWS rect Connect POP 进行的 RISE 连接。



以下是使用 Di AWS rect Connect POP 时的一些注意事项：

- VPCs 对基于区域（使用 SAP VPC 的 RISE）和基于本地区域的非 SAP 工作负载单独使用
- 在直接连接 POP 和专用 VIF 连接中使用 AWS Direct Connect 网关
- 在 Direct Connect POP 中使用 Direct Connect Gateway，在区域 VPCs （使用 SAP VPC 的 RISE）中使用 Transit VIF 连接。之所以这样做，是因为 AWS 直接连接 POP 中不存在直接 AWS 连接网关，而且 Tr AWS ansit Gateway 仅存在于区域中 AWS 。

如果弹性至关重要，请使用 SAP VPC 设置与运行 RISE 的 AWS 区域的辅助直接连接，或者使用 AWS Site-to-Site VPN 到 AWS 区域连接选项。这些服务在父 AWS 区域内运行，可作为故障转移连接选项，确保在出现中断或故障时不间断连接。



在同一 AWS 区域内的本地区域和可用区之间传输数据，在本地区域中 “进入” 和 “传出” Amazon EC2 的费用各不相同。有关更多信息，请参阅：EC2 -按需定价-同一 AWS 区域内的数据传输

连接到 RISE 的决策树

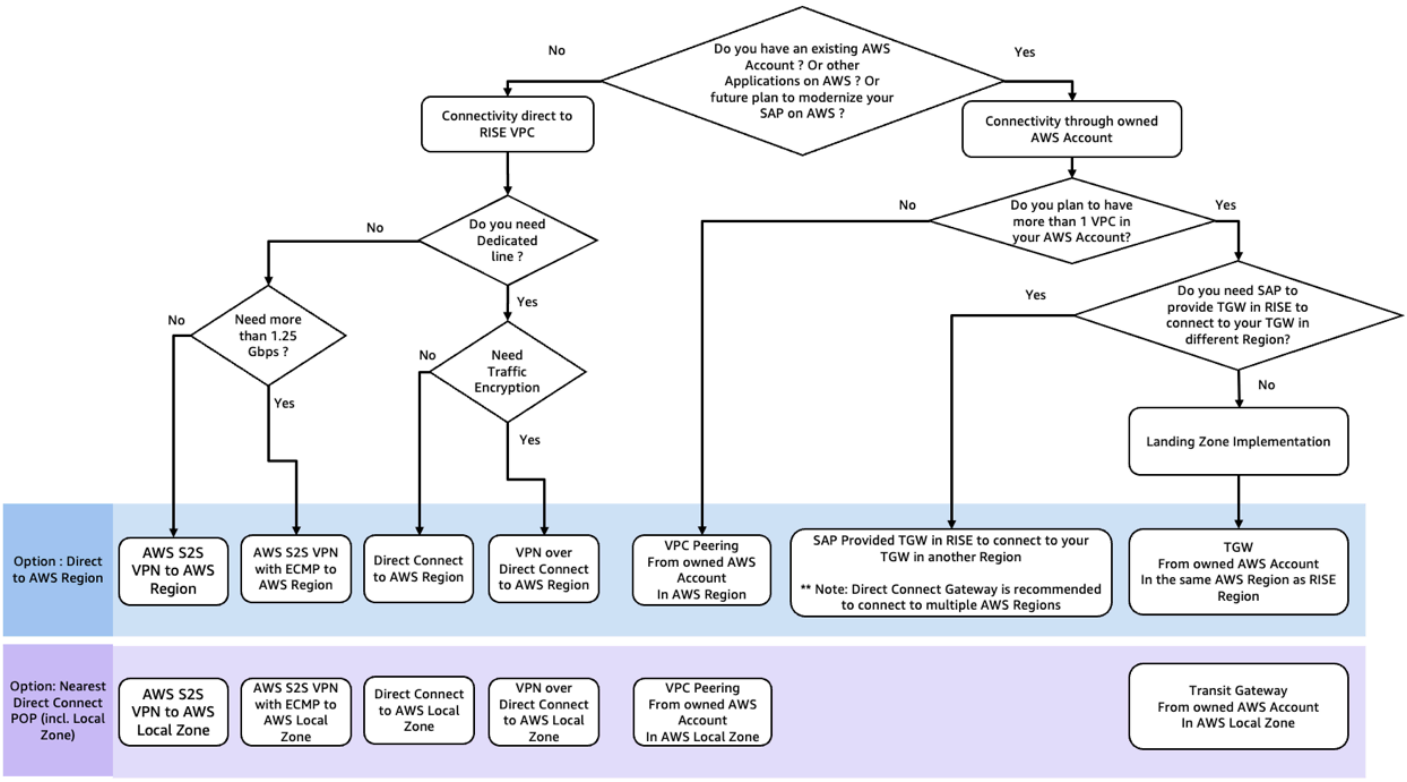
您必须建立所需的连接才能在 SAP 开启的情况下继续 RISE AWS。以下是前几节中描述的几种连接模式：

- 直接连接到 RISE VPC，支持 Site-to-Site VPN
- 直接连接到 RISE VPC，支持 Direct Connect
- 通过 VPC 对等互连通过您的 AWS 账户进行连接
- 通过 Transit Gateway 进行连接，支持多账户部署
- 通过 SAP 管理的 Transit Gateway 进行连接，支持多账户部署

您还必须考虑是否要连接：

- 直接部署到要部署 RISE with SAP VPC 的 AWS 区域
- 或通过 AWS 本地区域（最近的 Di AWS rect Connect POP），以更低的设置和运行成本受益，使用 SAP VPC 连接到您的 RISE 的网络延迟相同或更低

下图中显示的决策树可帮助您根据自己的需求（例如未来计划中的额外账户 AWS 或 RISE 帐户、专线（安全、性能）和带宽需求，来决定哪种连接是合适的。



注意：

1. ECMP 需要 Transit Gateway 才能使用 S2S VPN。
2. 建议使用 Direct Connect 网关连接到多个 AWS 区域。这简化了连接设置，避免了区域之间的 TGW 对等互连。 AWS

其他考虑因素

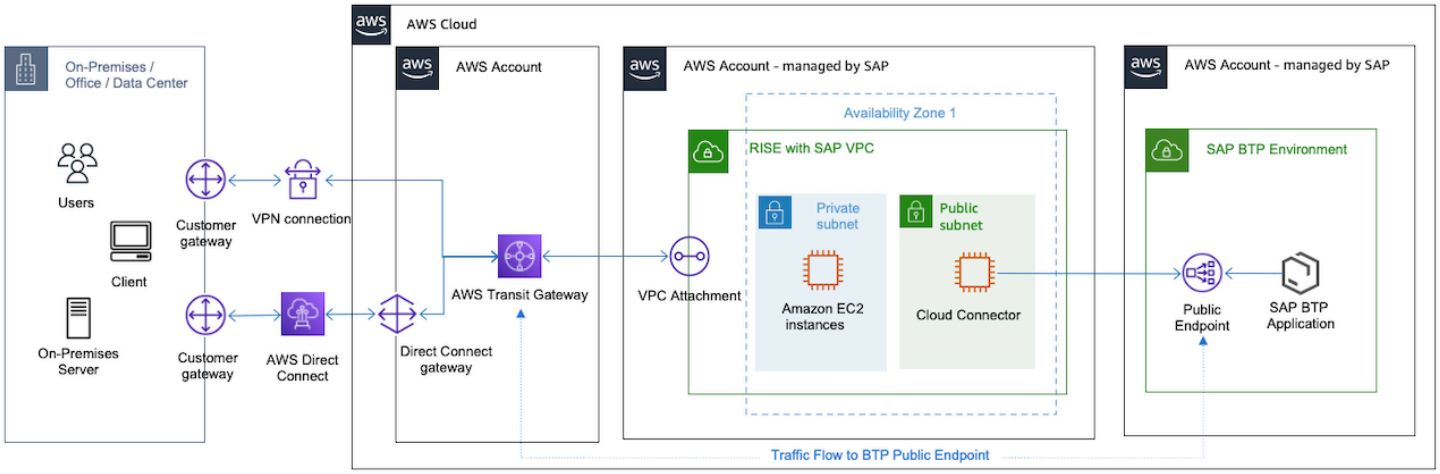
本节提供有关连接到 RISE 时其他注意事项的信息。

主题

- 开启 RISE 的 SAP 商业技术平台 (BTP) AWS
- 从 RISE 连接到云解决方案或 SaaS
- 多云到 RISE 的连接模式
- 如何实现与 RISE 的连接的退款功能
- 将域名系统集成到 RISE 和 Route 53 的注意事项

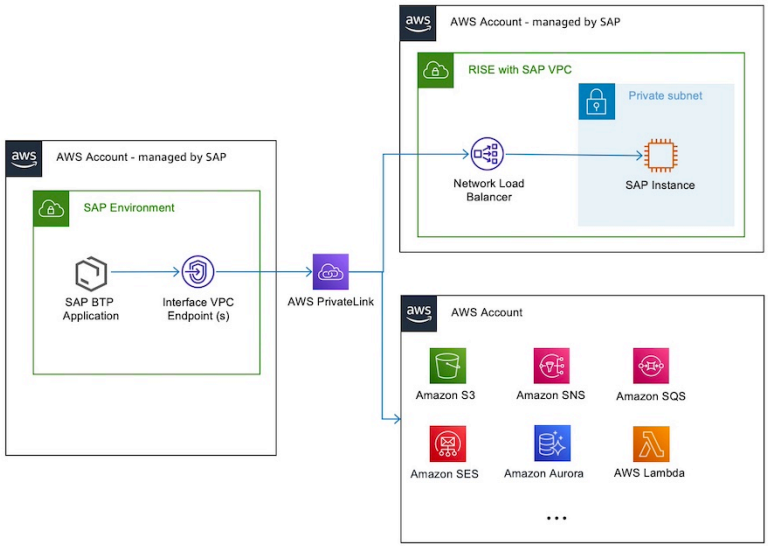
开启 RISE 的 SAP 商业技术平台 (BTP) AWS

你可以使用 SAP Business Technology Platf AWS orm BTP 服务，通过 SAP 扩展 RISE 的功能。SAP 建议 SAP Cloud Connector 通过互联网将 RISE 与 SAP VPC 与 SAP BTP 连接 当 RISE with SAP 和 SAP BTP 同时运行 AWS （在同一 AWS 区域或不同 AWS 区域）时，网络流量将被加密并包含 AWS 在全球网络中，而无需通过互联网（见下图）。这为RISE与SAP和SAP BTP之间的任何集成用例提供了更好的安全性和性能。有关更多信息，请参阅 Amazon VPC FAQs -当两个实例使用公有 IP 地址通信或实例与公共 AWS 服务终端节点通信时，流量是否会通过 Internet 传输？ 。



如上图所示，您可以将 Transit Gateway 配置为同时处理 RISE 和 BTP 网络流量。有关更多信息，请参阅如何通过 Amazon VPC 从本地路由互联网流量？

SAP 还提供适用于 SAP BTP 的 SAP 专用链接服务。 AWS SAP Private Link 通过安全连接连接 SAP BTP，无需 IPs 在你的 AWS 账户中使用公共连接。 AWS

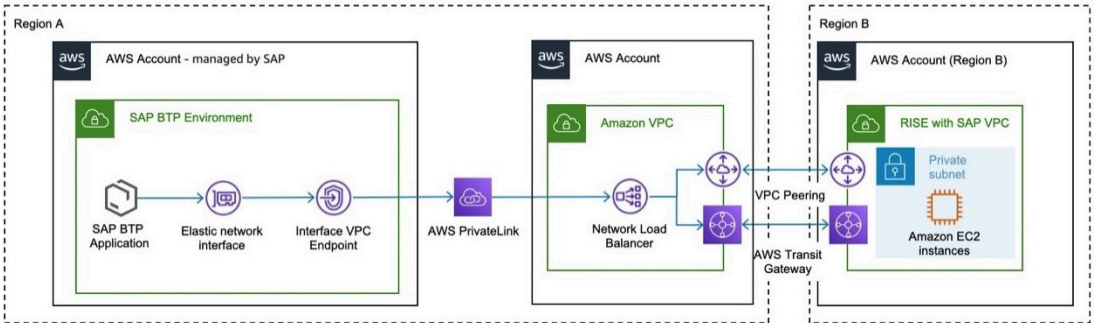


您可以从 Cloud Foundry 上运行的 SAP BTP 应用程序连接到 AWS 终端节点服务。通过建立此连接，您可以直接连接到 AWS 服务，或者例如，连接到 S/4HANA 系统。有关支持 AWS 服务的完整列表，请参阅在 SA P BTP 中使用亚马逊 Web 服务。

您可以使用 SAP 私有链接服务在 SAP BTP 和 AWS 服务之间建立安全和私密的通信。通过使用私有 IP 地址范围 (RFC 1918)，可以减少应用程序的攻击面。该连接不需要互联网网关。如果你不需要这种额外的安全层，你仍然可以在没有 SAP Private Link 的情况下通过 SAP BTP APIs 的公共网络进行连接，并从 AWS 全球网络中受益。有关更多信息，请参阅 Amazon VPC FAQs。

SAP Private Link AWS 目前支持从 SAP BTP Cloud Foundry 发起的 AWS连接

对于跨 AWS 区域的 AWS 服务，你可以在与 SAP BTP Cloud Foundry 运行时相同的 AWS 区域中创建 VPC，然后 VPCs 通过 VPC 对等互连或 Tr AWS ansit Gateway 进行连接。有关支持的区域列表，请参阅可用于 Cloud Foundry 环境的地区和 API 终端节点。



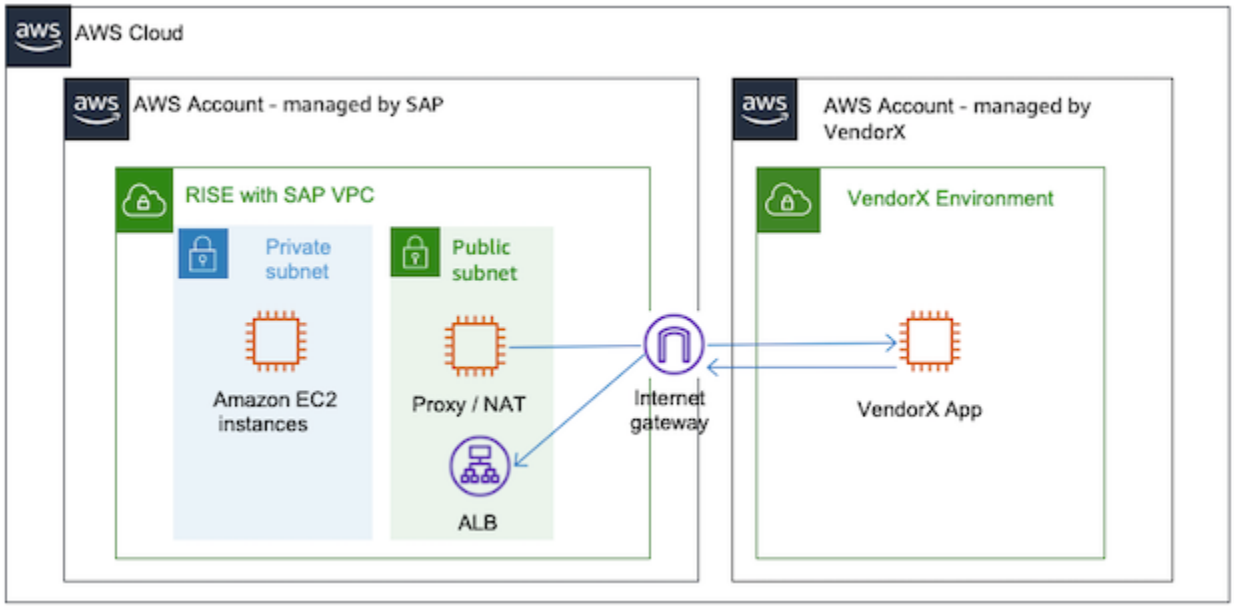
SAP 私有链接服务是 SAP 在 SAP BTP 上提供的付费服务。有关更多信息，请参阅：SAP 探索中心 — 服务 — SAP 私有链接服务。

与 AWS 账户中的 AWS 服务（例如 AWS 网络负载均衡器或 Transit Gateway）相关的费用各不相同，这些服务由客户管理，以促进跨区域连接。有关价格的更多信息，请参阅所列 AWS 服务的专用定价页面。

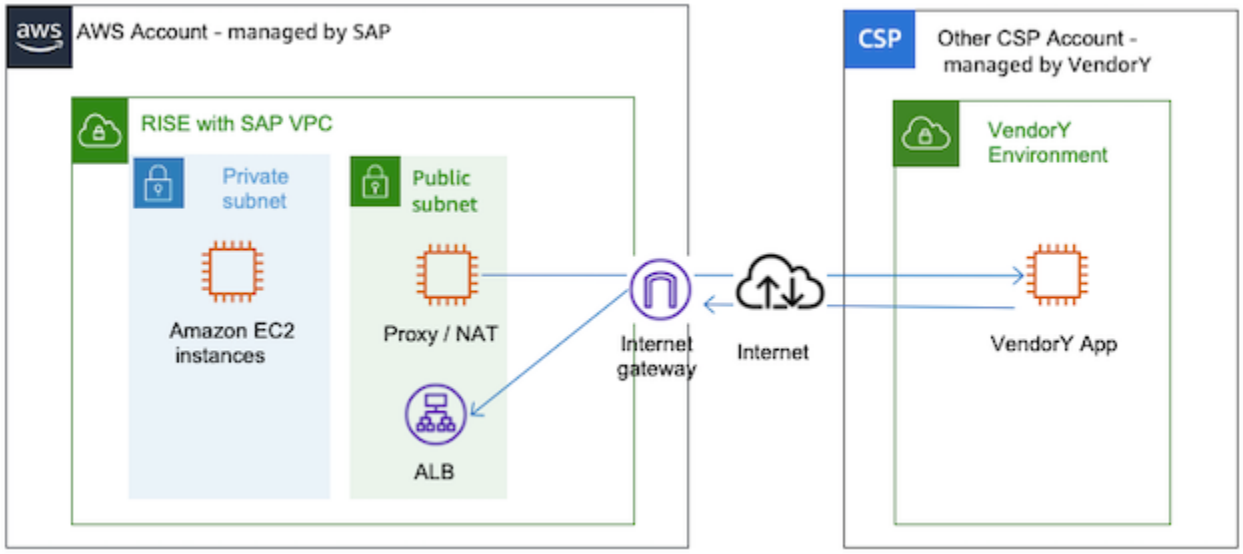
从 RISE 连接到云解决方案或 SaaS

在对 SAP 环境进行现代化改造时，你可以订阅独立软件供应商提供的多个 SAP 云解决方案或 SaaS，将 RISE 与 SAP 解决方案相辅相成。

当云解决方案运行时 AWS （在同一 AWS 区域或不同 AWS 区域），RISE与SAP的连接将保持 AWS 在全球网络中，而无需互联网连接。连接是通过 RISE 中提供的 squid 代理服务器与 SAP VPC 保持的。有关更多信息，请参阅 Amazon VPC FAQs -当两个实例使用公有 IP 地址通信或实例与公共服务终端节点通信时，流量是否会通过互联网传输？ AWS 。



如果您的云在其他数据中心或其他云服务提供商上运行，则需要互联网连接。



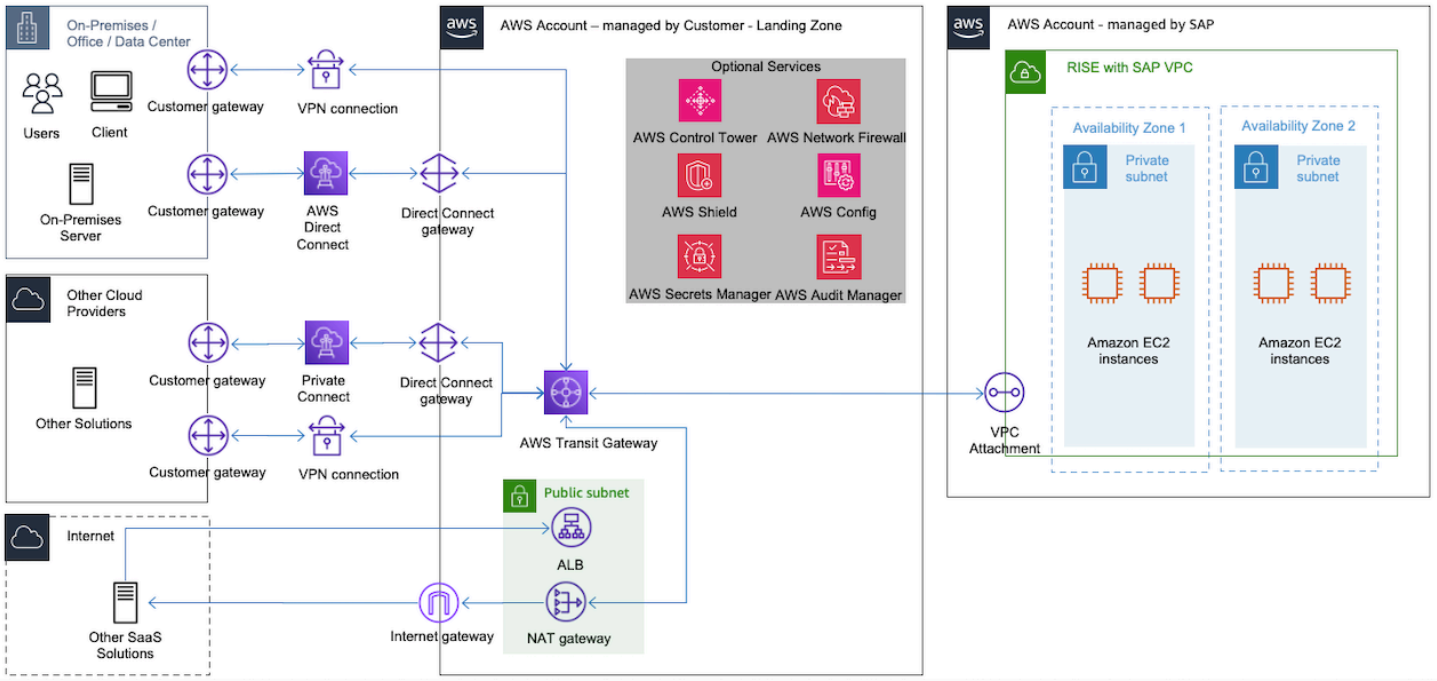
SaaS 云解决方案不提供通过 VPN、Direct Connect 或任何其他私有连接方式的连接。您可以实施集中式互联网出口架构来管理这种连接。有关更多信息，请参阅集中式互联网出口。

多云到 RISE 的连接模式

在复杂的连接场景中，您可能需要将 AWS RISE 与 SAP 设置与本地、托管系统、各种 SaaS 解决方案和其他云服务提供商集成。

直接从 AWS 环境中管理连接，使依赖关系与本地网络基础设施脱钩，从而提高整体环境的可用性和弹性。

您可以使用公共或私有连接将多云与 RISE 连接起来。



公共连接

连接通过公共互联网路由。这种模式通常用于从带有 SAP 的 RISE 到跨多个云运行的 SaaS 解决方案的连接。建立通过公共互联网路由的连接时，请考虑以下几点：

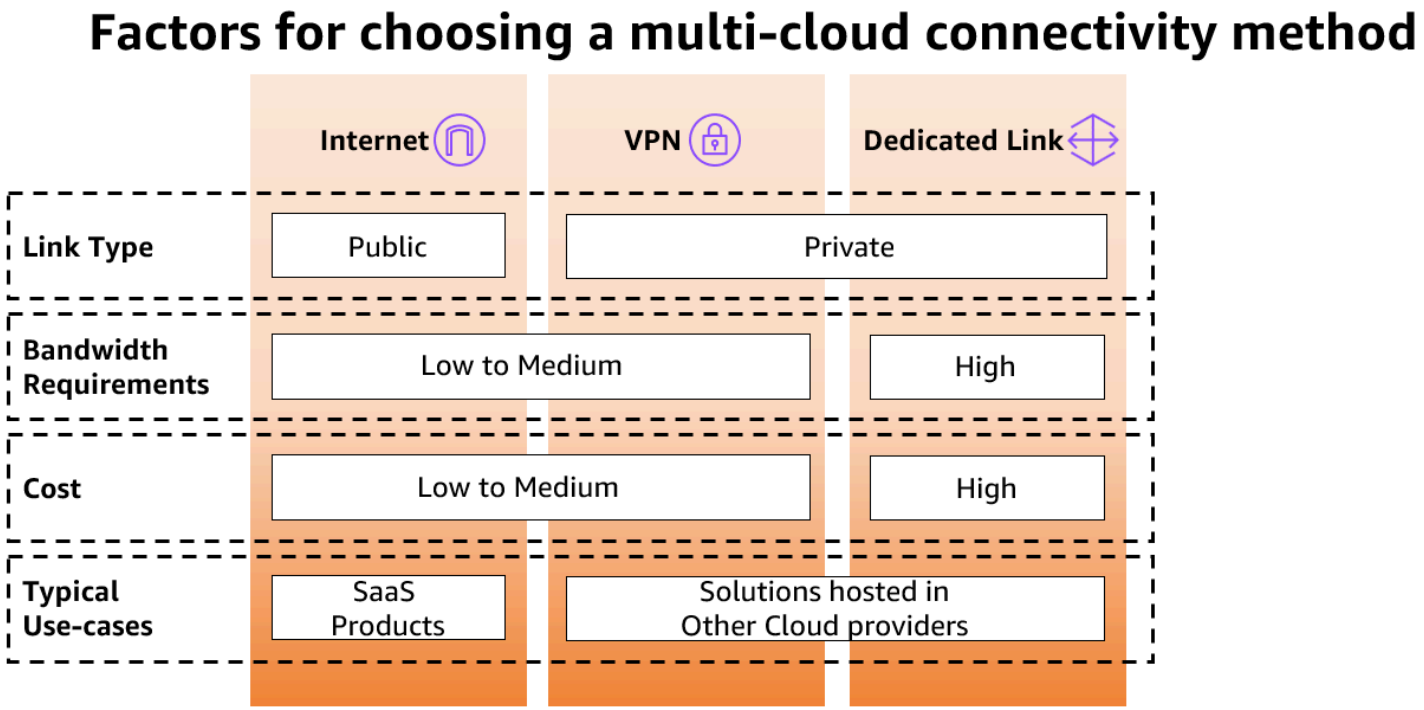
- 确保所有通信都已加密
- 使用弹性负载均衡器和 Shield 等 AWS 服务保护端点 AWS
- 使用 Amazon 监控终端节点 CloudWatch
- 确保托管的两个公有 IP 地址之间的流量通过网络路由 AWS AWS

私有连接

以下三种是在不同云服务提供商之间建立私有连接的选项：

- Site-to-site 通过公共互联网路由的 VPN 加密隧道
- 在托管基础架构中使用 AWS Direct Connect 进行私有互连（使用 ExpressRoute 适用于 Azure 的 Azure 和谷歌云平台的谷歌专用互连）
- 在与多云连接提供商的设施中使用 AWS Direct Connect 进行私有互连

下图描述了选择多云连接方法的因素。

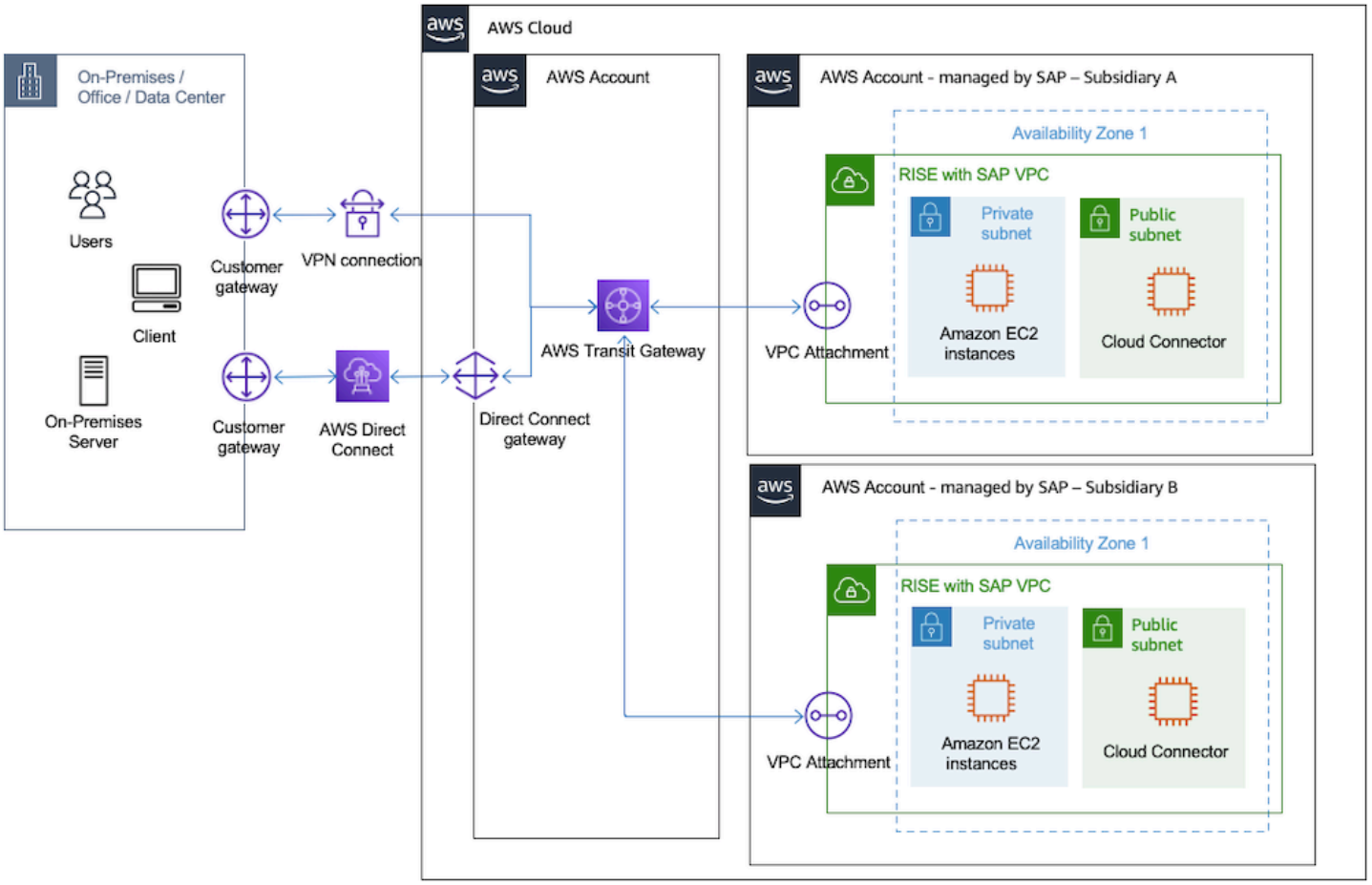


有关更多信息，请参阅设计与 Microsoft Azure AWS 之间的私有网络连接。

如何实现与 RISE 的连接的退款功能

如果您是一家拥有子公司的公司，则可能有不同的RISE合同，因此需要在不同的 AWS 账户中进行部署，同时需要互连的网络连接。在这种情况下，您必须在着陆区（多账户）设置中部署 Transit Gateway 连接。它可以扩展你的 RISE 部署，并通过 SAP 与多个 RISE 集成 VPCs。

Transit Gateway 流量日志可实现有效的成本管理。Transit Gateway Flow Logs 可以与成本和使用量报告 (CUR) 集成，后者可以归因于业务部门的退款。有关更多信息，请参阅使用 Transit Gateway 流日志记录网络流量。



上图显示了如何使用 Transit Gateway 将多个 RISE 与 SAP 连接起来， VPCs 并通过流日志提供退款功能。

有关更多信息，请参阅以下博客：

- 使用 Tr AWS ansit Gateway Flow Logs 对多账户环境中的数据处理成本进行计费
- 共享服务退款操作方法：Transit Gateway 示例 AWS

使用以下步骤启用此设置：

1. 启用 Transit Gateway 流日志 有关更多信息，请参阅创建发布到 Amazon S3 的流日志。
2. 设置成本和使用情况报告并设置 Athena 以使用该报告。有关更多信息，请参阅使用 Amazon Athena 创建成本和使用量报告和查询成本和使用量报告。
3. 获取每个账户的 Transit Gateway 数据处理费用。
   a. 确定成本分配策略——将成本平均分配给所有账户或按比例分配给所有账户。
   b. 使用 Tr AWS ansit G ateway 查询计算每个账户的总网络流量和分配百分比。

c. 通过从收集网络输入（上传）和 NetworkOut（下载） CloudWatch 的账户中收款，估算每个账户的费用。

   i. NetworkIn（上传）+ NetworkOut（下载）每个使用账户/在网络账户中处理的数据总数

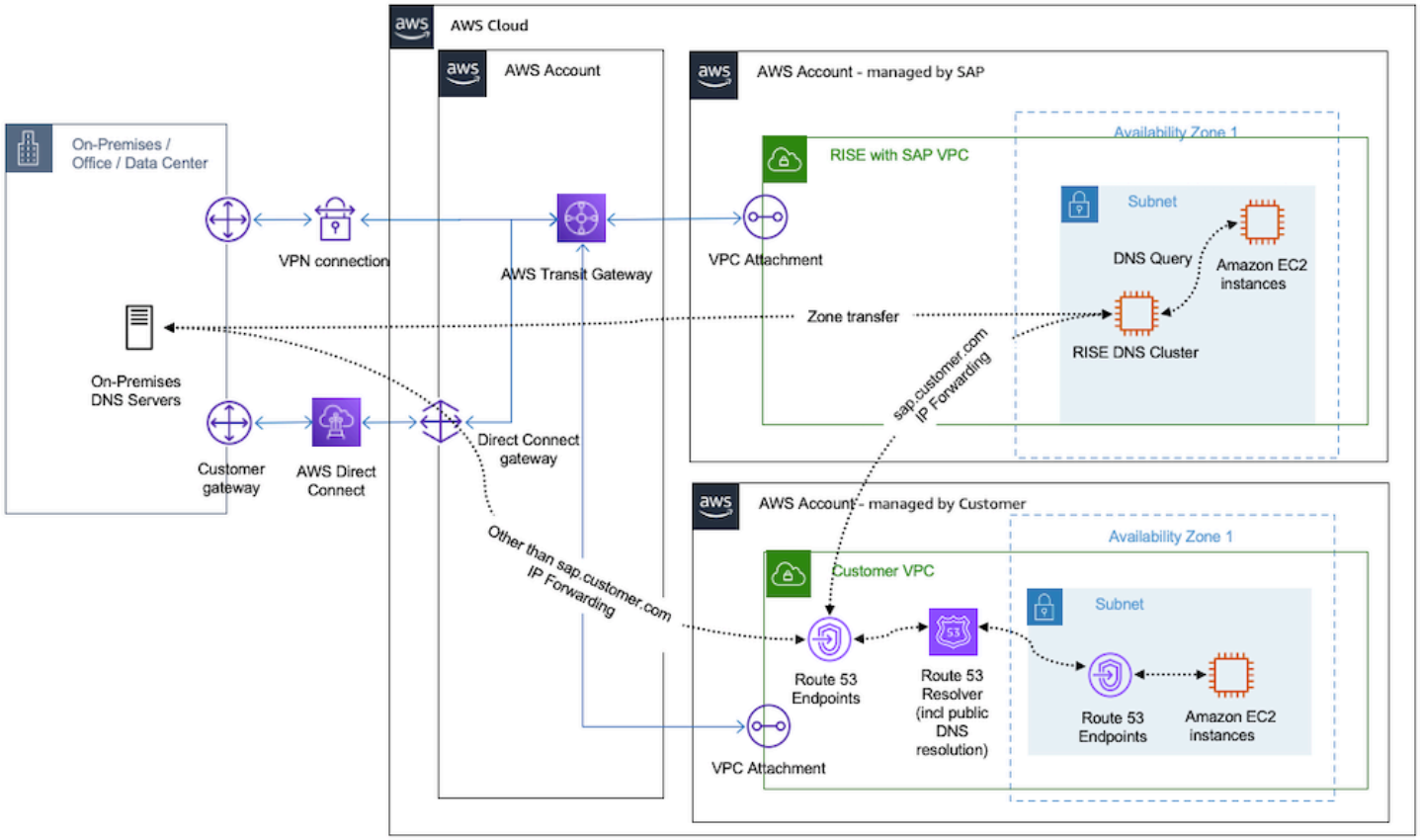
   ii. 使用百分比 x 总成本 = 每个使用账户的退款成本

将域名系统集成到 RISE 和 Route 53 的注意事项

域名系统 (DNS) 以两种方式翻译域名和 IP 地址，例如（www.amazon.com 为 1.2.3.4 in IPv4 或 1200:ab 00:1024:1:: b410:e6b1 in）。 IPv6有两种方法可以将 DNS 集成到 RISE：

- DNS 区域传输：此方法在一组 DNS 服务器之间复制 DNS 数据库。它可以提供更高的可用性、冗余性和更高的 SLA。在典型的 RISE 环境中，您可以将子域（例如*.sap.customer.com）委托给 RISE DNS 服务器。如果一台服务器不可用，其他服务器可以不间断地继续提供 DNS 服务。如果客户使用不支持区域传输的 Route 53，则客户需要将 Route 53 入站解析器与 Route 53 私有托管区域一起设置，并将解析器提供 IPs 给 SAP 进行路由，您可以在 DNS 条件转发中找到更多信息，如下所示。
- DNS 条件转发（也称为 IP 转发）：DNS 服务器仅转发对不属于其自身命名空间的特定域名的查询。（示例：亚马逊 Route 53 将*.sap.customer.com 的 DNS 查询转发给 RISE DNS 服务器）。这样可以更精确地控制 DNS 查询的处理方式，尤其是在复杂的网络环境中。Amazon Route 53 Resolver 支持公有和私有 DNS 解析，简化了混合云的设置，并增强了 AWS 资源和本地网络的可用性、性能和安全性。

以下是有关如何将 Amazon Route 53 与 RISE 集成的参考架构。



有关更多详细信息，请参阅以下 AWS 文档：

- 将出站 DNS 查询转发到您的网络
- 将入站 DNS 查询转发给您的 VPCs
- 在单账户 AWS 环境中为混合网络设置 DNS 解析
- 在多账户 AWS 环境中为混合网络设置 DNS 解析
- 什么是 Amazon Route 53 Resolver？

安全性

SAP 负责管理 SAP 管理的 AWS 账户的安全性。您可以在自己的 AWS 账户中实施其他安全机制。

主题

- 单点登录 — SAP 云身份服务和 AWS IAM 身份中心
- 单点登录 — SAP 云身份服务和微软 Entra（以前是 Azure AD）
- 单点登录 — SAPGUI 前端

- 使用 SAP 的 RISE AWS 服务实现高级安全性
- 将 SAP 密钥管理服务 (SAP KMS) 与 AWS 密钥管理服务 (AWS KMS) 集成
- AWS Nitro 如何通过 SAP 帮助保护 RISE？
- Amazon WorkSpaces 是 RISE 与 SAP 合作的远程访问解决方案

单点登录 — SAP 云身份服务和 AWS IAM 身份中心

RISE with SAP 的安全最佳实践之一是通过与企业身份提供商 (IdP) 集成来集中用户访问控制。这使您可以更轻松地配置、取消配置和管理整个公司的用户访问权限，包括 RISE with SAP、 AWS 服务等。

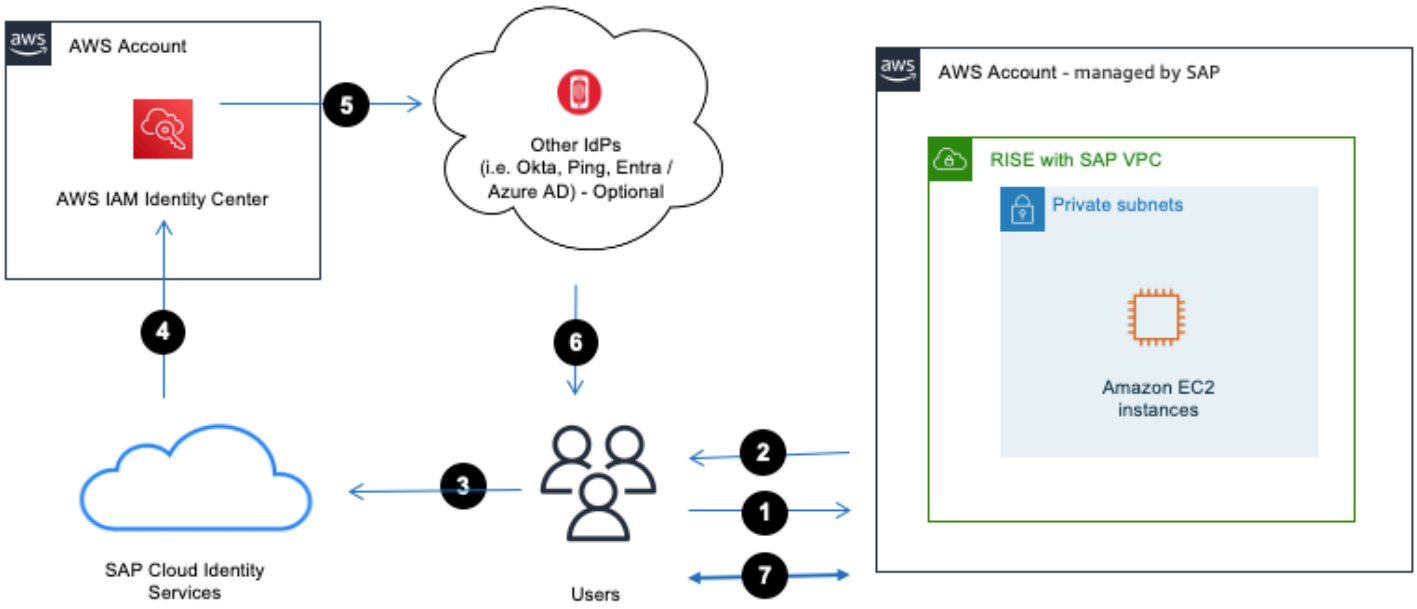
AWS IAM 身份中心是您可以与 RISE 集成的 IdP 之一。IAM Identity Center 为用户提供了一个集中式接入点，使他们能够在 AWS 组织内一致地管理 AWS 账户和应用程序（例如在多账户设置中）。

如果你已经有现有的身份源，例如 Okta、Ping、微软 Windows Active Directory、Microsoft Entra（以前称为 Azure Active Directory）或其他身份源，则可以通过安全断言标记语言 (SAML) 和跨域身份管理系统 (SCIM) 协议将身份源集成到 IAM 身份中心。

有关更多信息，您可以参考以下参考资料：

- 什么是 IAM Identity Center？
- IAM Identity Center 与其他身份源的集成，请参阅入门教程。
- SAP 云身份服务-身份认证。

下图显示了在 RISE with SAP 的背景下，来自 SAP BTP 的身份验证和 AWS IAM Identity Center 之间的集成



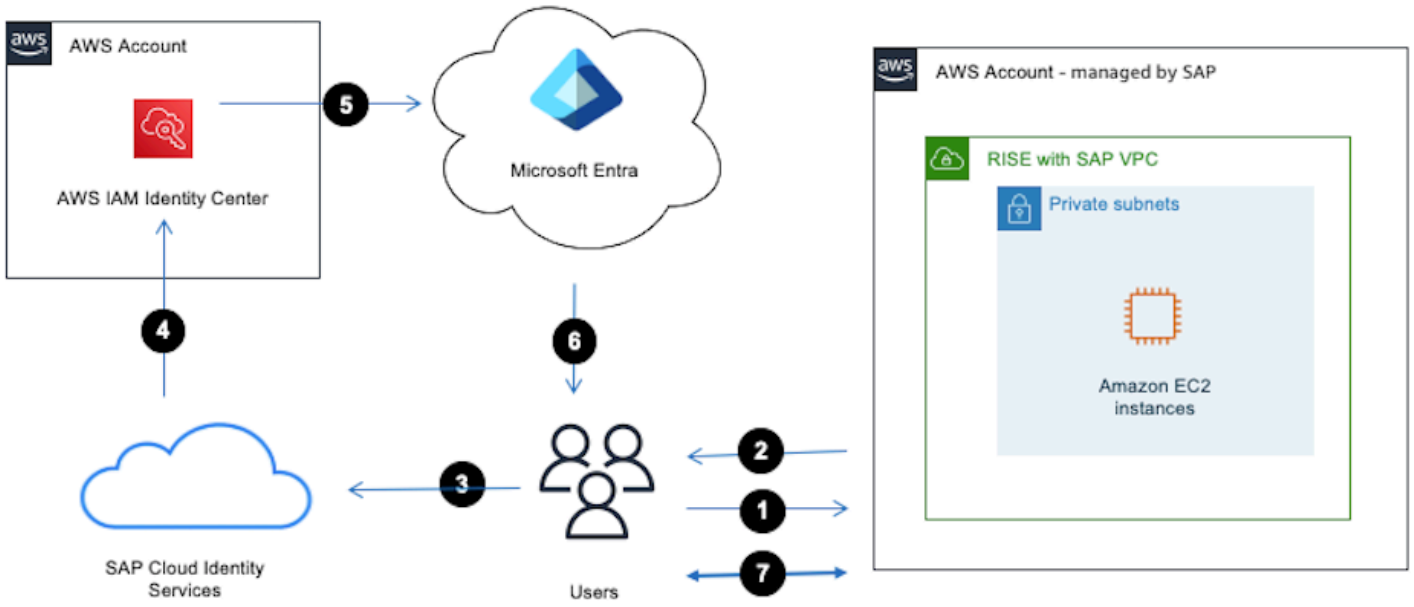
身份验证流程

1. 用户通过互联网浏览器访问 SAP Fiori。
2. SAP Fiori 会将 SAML 请求重定向回互联网浏览器。
3. 互联网浏览器将 SAML 请求中继到 SAP 云身份服务。
4. SAP 云身份服务将身份验证请求委托给 IAM 身份中心。
5. 如果 IAM Identity Center 与 Okta、Ping、Entra 等现有身份源集成，那么 IdP 将对用户进行身份验证。
6. 用户通过 IdP 进行身份验证，并向互联网浏览器提供带有用户身份信息的 SAML 响应。
7. 用户可以通过 SAP 系统访问 RISE。

有关如何执行此操作的更多信息，您可以参阅 SA [P Cloud Platform Cloud Foundry 的 IA AWS M 身份中心（ AWS SSO 的继任者）集成指南](#)。

单点登录 — SAP 云身份服务和微软 Entra（以前是 Azure AD）

微软 Entra（以前是 Azure AD）或其他 IdPs 可以直接集成到 SAP 云身份服务中。当你不需要 AWS IAM Identity Center（即不需要运行利用 Organiz AWS ations 的多账户策略）时，这支持直接身份验证。



身份验证流程

1. 用户通过互联网浏览器访问 SAP Fiori。
2. SAP Fiori 会将 SAML 请求重定向回互联网浏览器。
3. 互联网浏览器将 SAML 请求中继到 SAP 云身份服务。
4. SAP 云身份服务将身份验证请求委托给 IdPs。
5. 用户通过 IdP 进行身份验证，并向互联网浏览器提供带有用户身份信息的 SAML 响应。
6. 用户可以通过 SAP VPC 访问 RISE 中的 SAP S/4HANA。

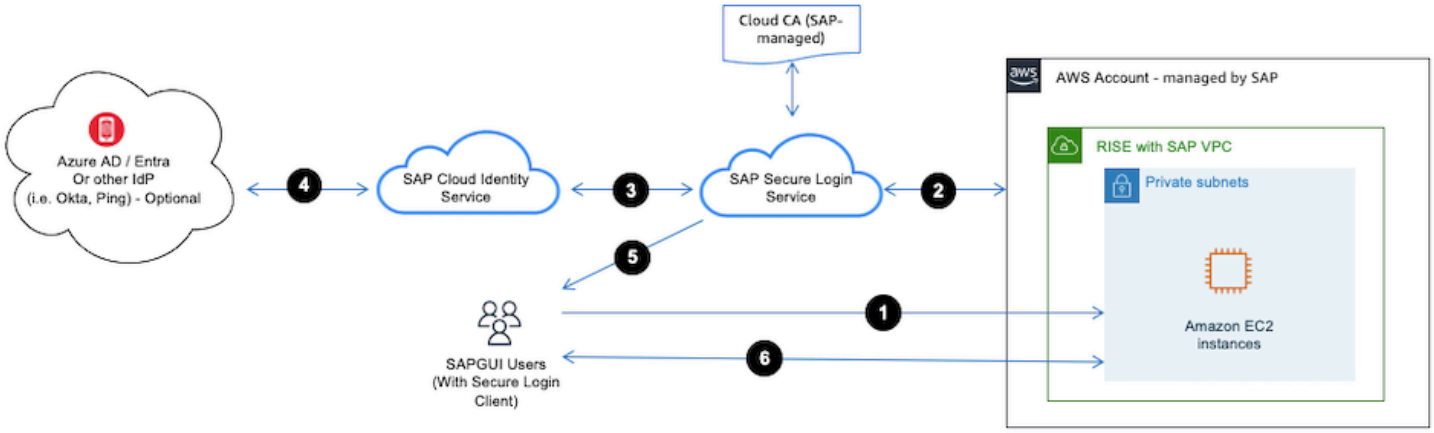
有关如何执行此操作的更多信息，你可以参考使用身份认证服务在 Azure AD 和 SAP 云平台之间启用 SSO。

单点登录 — SAPGUI 前端

SAPGUI 是 SAP ERP 数据库、应用程序服务器和客户端三层架构中的图形用户界面客户端。它需要安装在运行在 Windows、macOS 或 Linux 上的本地桌面上。

为了使用 SAP 在 RISE 中实现 Single-Sign-On SAPGUI，我们必须使用 Kerberos 或 X.509 方法。不建议使用 Kerberos AWS，因为它要求用户始终连接到公司网络并根据 Microsoft Active Directory 进行身份验证，这会降低他们的移动性。因此，建议使用 X509。

Single-Sign-On带有 X509 的 SAPGUI 可以通过 BTP 上的 SAP 安全登录服务实现，下图描述了集成的工作原理。



身份验证流程

1. 用户在其桌面上访问 SAPGUI。
2. SAP S/4HANA 会将身份验证请求重定向到 SAP 安全登录服务。
3. SAP 安全登录服务会将身份验证委托给 SAP 云身份服务。
4. 当 SAP 云身份服务集成到 IdP（即 Azure AD、Okta、Ping 等）时，IdP 将对用户进行身份验证。
5. 用户通过 IdP 进行身份验证，X509 由 SAP 安全登录服务提供给 SAPGUI。
6. 用户可以通过 SAP VPC 访问 RISE 中的 SAP S/4HANA。

有关如何执行此操作的更多信息，请参阅使用 SAP 安全登录服务保护 SAP GUI。

使用 SAP 的 RISE AWS 服务实现高级安全性

AWS 提供一套全面的安全服务，在开启 SAP 部署的情况下，这些服务可以充当围绕 RISE 的多层安全信封。 AWS这些服务充当额外的安全屏障，在潜在威胁到达RISE账户之前将其拦截和缓解，提供强大的保护并帮助遵守行业标准的安全最佳实践。

AWS 网络防火墙

AWS Network Firewall 是一项托管防火墙服务，可为亚马逊虚拟私有云 (VPC) 环境提供基本的网络保护。 AWS Network Firewall 充当第一道防线，它过滤和检查所有进出 RISE 资源的网络流量，从而有效地在 RISE 环境周围创建保护边界。

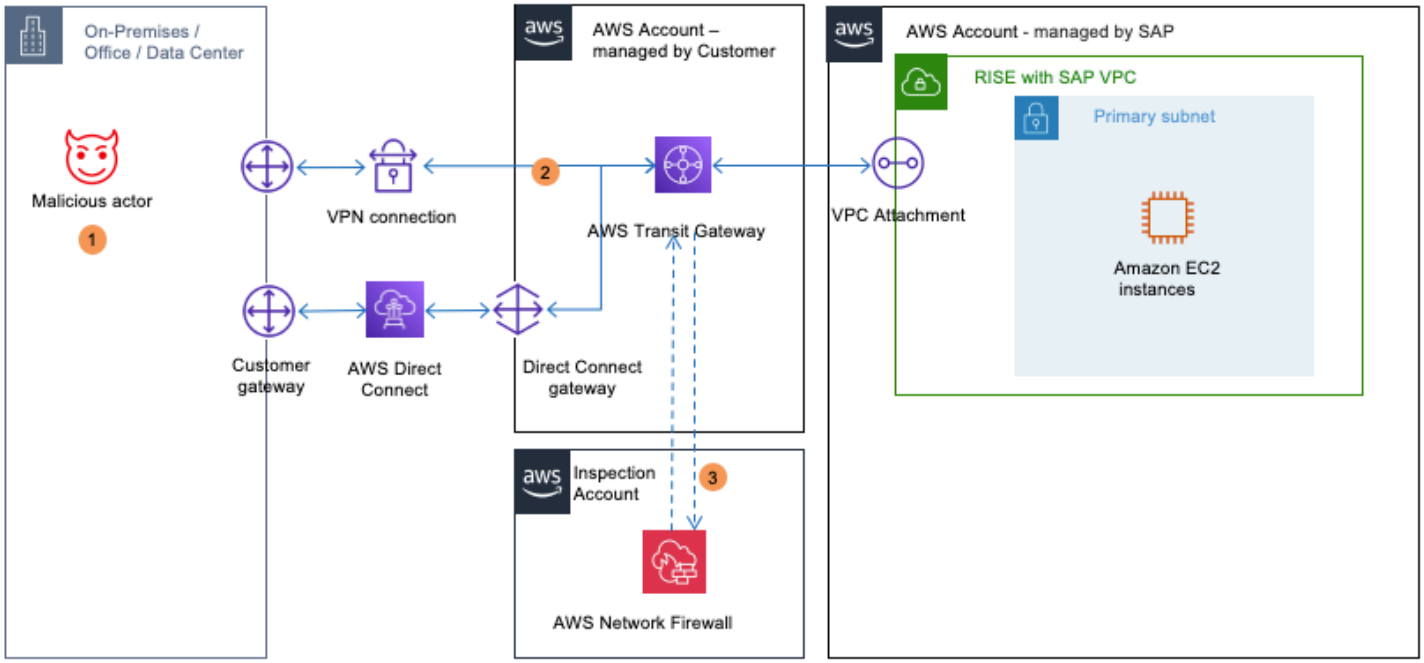
Network Fire AWS wall 的主要功能包括：

- 状态防火墙功能。 AWS Network Firewall 提供高级状态防火墙功能，用于监控和控制网络流量。它可以检查网络连接的完整上下文，包括来源、目的地、端口和协议，以检测和阻止恶意或未经授权的流量。
- 威胁签名匹配。 AWS Network Firewall 预装了一套全面的威胁检测规则和签名，这些规则和签名会持续更新 AWS，以识别和缓解针对 RISE 部署的已知威胁、恶意软件和其他恶意活动。
- 自定义规则定义。除了预定义的威胁签名外，客户还可以创建和部署自定义的防火墙规则，以满足在RISE环境中访问SAP系统的连接所特有的特定安全要求或策略。
- 集中式策略管理。 AWS Network Firewall 允许集中定义和管理防火墙策略，然后可以轻松地在 VPCs 包括非 SAP 在内的多个防火墙策略中进行部署， VPCs 并 VPCs 与 SAP 管理的 RISE VPC 相关联，从而确保一致的安全执行。
- 可扩展性和高可用性。作为一项完全托管的服务， AWS Network Firewall 可自动扩展以应对网络流量和模式的变化，从而确保无需复杂的基础架构管理即可保护RISE环境。

在 RISE with SAP 的背景下，可以利用 AWS Network Firewall 实现以下目的：

- 集中式防火墙管理。 AWS Network Firewall 提供集中式托管防火墙服务，用于控制和监控进出由 SAP 管理的 RISE VPC 的网络流量。
- 状态数据包检查。 AWS Network Firewall 执行状态数据包检查，使其能够通过分析 RISE VPC 中的 to/from SAP 系统的网络连接环境来检测和缓解高级威胁。
- 监管合规。 AWS Network Firewall 通过强制执行安全策略和为 RISE with SAP 环境提供 logging/auditing 功能，帮助组织满足合规性要求。

以下是 Network Fire AWS wall 的架构示例，该架构在 SAP 网络流量到达 RISE 之前对其进行检查



在上图中

1. 恶意行为者利用网络配置错误来访问 RISE 上的 SAP 系统。
2. 流量首先通过 Tr AWS ansit Gateway 路由。
3. Network Fire AWS wall 的数据包检查可以捕获异常的连接尝试...

值得注意的是，想要使用通过Direct Connect首先 AWS 连接到Tran AWS sit Gateway托管的SAP BTP服务的客户也可以使用Network Fi AWS rewall，这样他们就可以 end-to-end继续使用 AWS 主干 AWS 网络。

有关配置 AWS 网络防火墙的说明，请参阅AWS 网络防火墙入门。

Amazon Macie

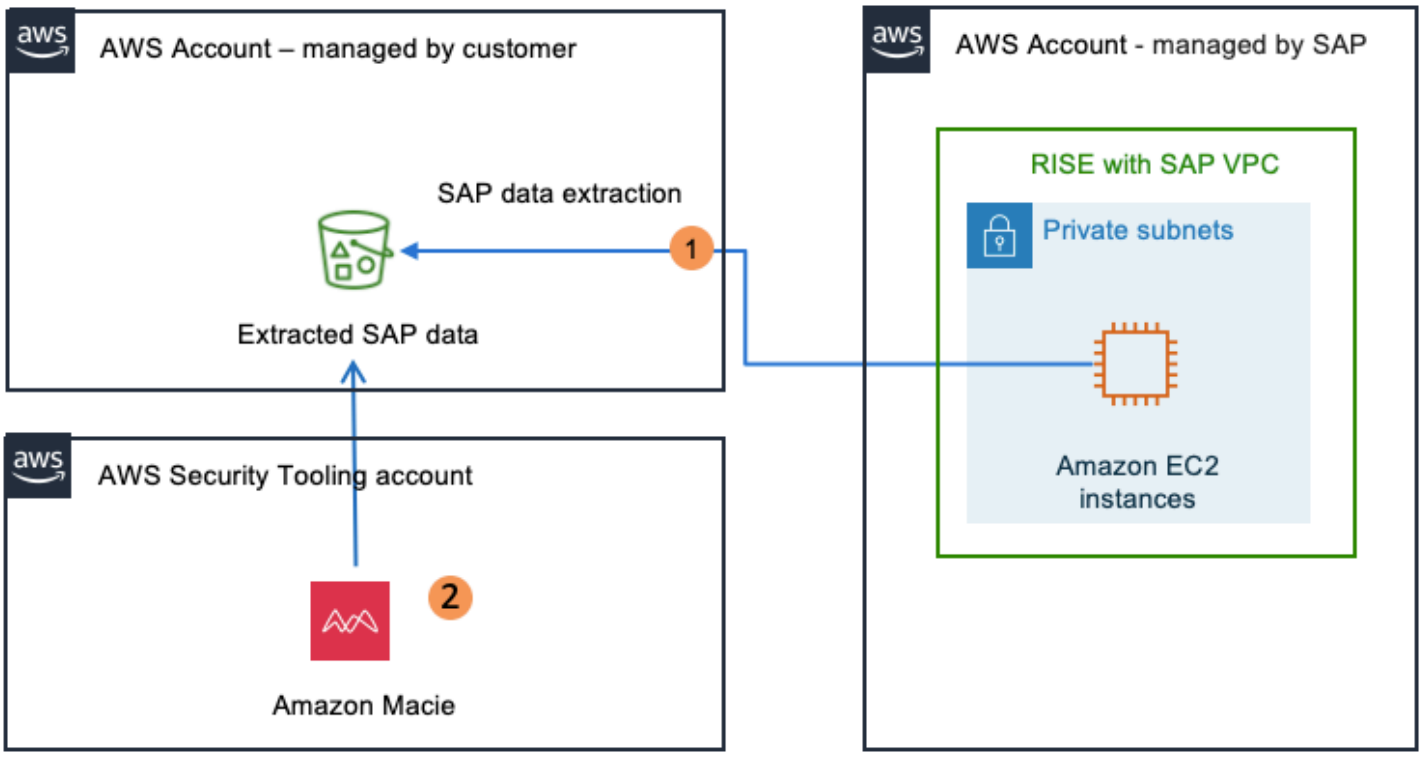
Amazon Macie 是一项数据安全服务，通过持续监控潜在的数据风险和未经授权的访问尝试并发出警报，帮助客户发现、分类和保护存储在 Amazon S3 存储桶中的敏感数据。

在 RISE with SAP 的背景下，Amazon Macie 可以保护客户管理的 AWS 账户中的 Amazon S3 存储桶，这些存储桶由 RISE with SAP 环境提供，例如：

- 作为 RISE 客户，可以将备份从 SAP 管理的 AWS 账户复制到客户管理的环境和 S3 存储桶。

- 可以将SAP数据从或RISE环境（参见使用服务提取 SAP数据的架构选项）提取到客户管理的S3存储桶，以便使用其他 AWSAWS 服务（例如Amazon Athena、G AWS lue和Amazon Sagemaker）实现高级分析、机器学习和商业智能；
- 某些行业和法规，例如 GDPR、HIPAA 或 PCI-DSS，可能需要长期存储和保存敏感数据。将这些数据导出到客户管理的 S3 有助于满足这些合规性要求，因为 S3 提供了强大的安全性和耐久性功能。
- 集中式策略管理。 AWS Network Firewall 允许集中定义和管理防火墙策略，然后可以轻松地在 VPCs 包括非 SAP 在内的多个防火墙策略中进行部署， VPCs 并 VPCs 与 SAP 管理的 RISE VPC 相关联，从而确保一致的安全执行。
- 客户还可以从 RISE 环境中使用安全事件日志，因此请将其载入自己的 S3 存储桶或 SIEM 系统中。

以下是 Amazon Macie 持续扫描 S3 存储桶的架构示例，其中包含从 RISE 中提取的 SAP 数据



在上图中

1. 数据被写入 S3 存储桶以用于数据 lake/compliance 报告。
2. Amazon Macie 会持续分析存储桶，以检测可私密识别的信息。

有关配置亚马逊 Macie 的说明，请参阅什么是 Macie？ 。

Amazon GuardDuty

Amazon GuardDuty 是一项威胁检测服务，可持续监控 AWS 环境中的恶意活动和未经授权的行为。它结合了机器学习、异常检测和集成威胁情报，可识别潜在威胁，并通过 SAP 环境、工作负载和数据保护与 RISE 关联的 AWS 账户。

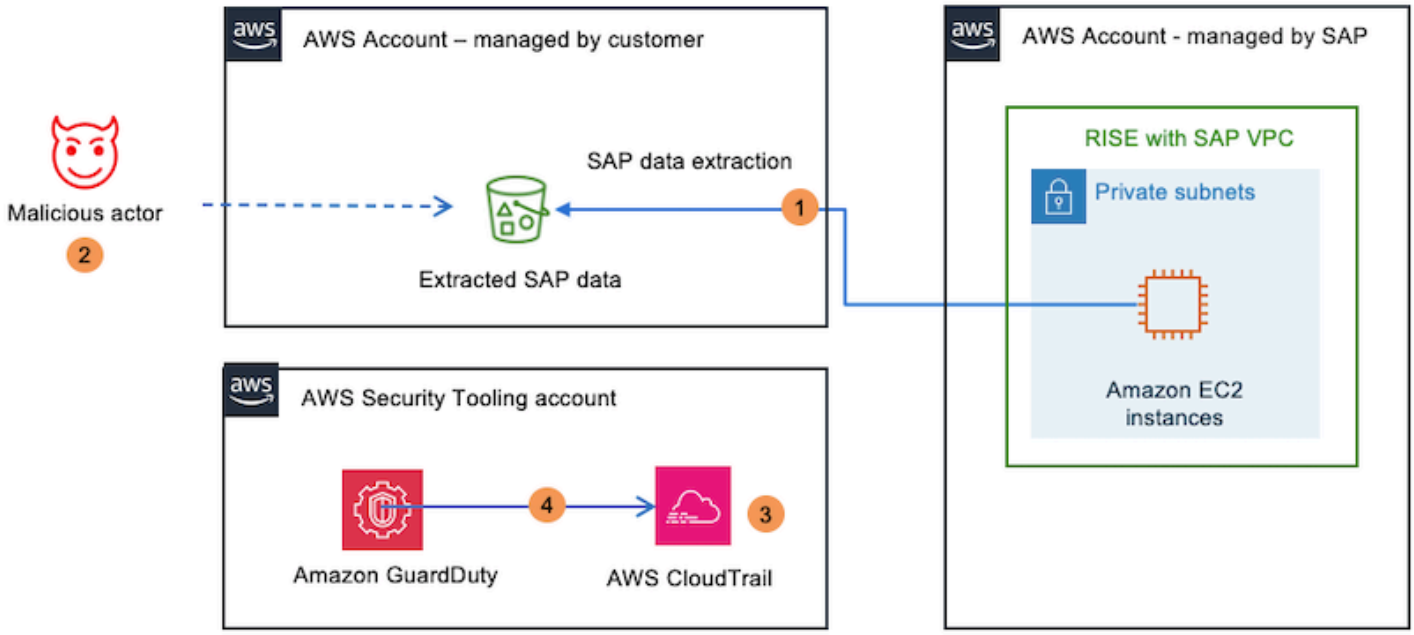
Amazon GuardDuty 监控以下内容：

- AWS CloudTrail 日志：Amazon GuardDuty 监控 AWS 账户中的 API 活动，以检测可疑 API 调用、未经授权的部署和未经授权的资源访问尝试。Amazon 会 GuardDuty 识别从未经授权的 IP 地址或区域访问 AWS 服务的企图。亚马逊在身份和访问管理 (IAM) Access Management 用户、角色和策略中 GuardDuty 检测到异常行为，例如权限提升。
- VPC 流日志。Amazon 会 GuardDuty 分析虚拟私有云 (VPC) Virtual Cloud (VPC) 内的网络流量，以检测意外流量模式、数据泄露企图或未经授权的访问，同时识别资源与已知的恶意 IP 地址或域名 AWS 之间的通信。在开启 SAP 的情况下进行 RISE 的背景下 AWS，检查在 RISE SAP 管理的账户前面的 VPC 上进行；
- DNS 日志。Amazon 会 GuardDuty 监控 AWS 资源进行的 DNS 查询，以检测试图连接恶意域名或异常的 DNS 请求模式。Amazon GuardDuty 还检测到使用域生成算法 (DGA) 生成与命令和控制服务器关联的域名的情况。

在 RISE with SAP 的背景下， GuardDuty 可以利用 Amazon 实现以下目的：

- 入侵检测： GuardDuty 通过识别恶意活动（例如未经授权的 API 调用、网络侦测和来自已知恶意 IP 地址的访问尝试），及早检测到客户管理的 AWS 账户所面对的 RISE 环境的入侵企图；
- 合规性验证：对于具有严格合规要求的组织， GuardDuty 可以持续监控违反策略和未经授权的访问尝试，提供详细的日志和报告以供审计，从而帮助确保合规性。当从客户管理的 AWS 账户访问 SAP RISE 环境时，就可以实现这一点。有关更多详细信息，请参阅合规性验证
- 自动事件响应。 GuardDuty 可以与 AWS Lambda 和 Sec AWS urity Hub 集成，以自动执行事件响应工作流程。检测到威胁后，这些服务可以触发自动补救措施，例如隔离受感染的资源或通知安全团队。

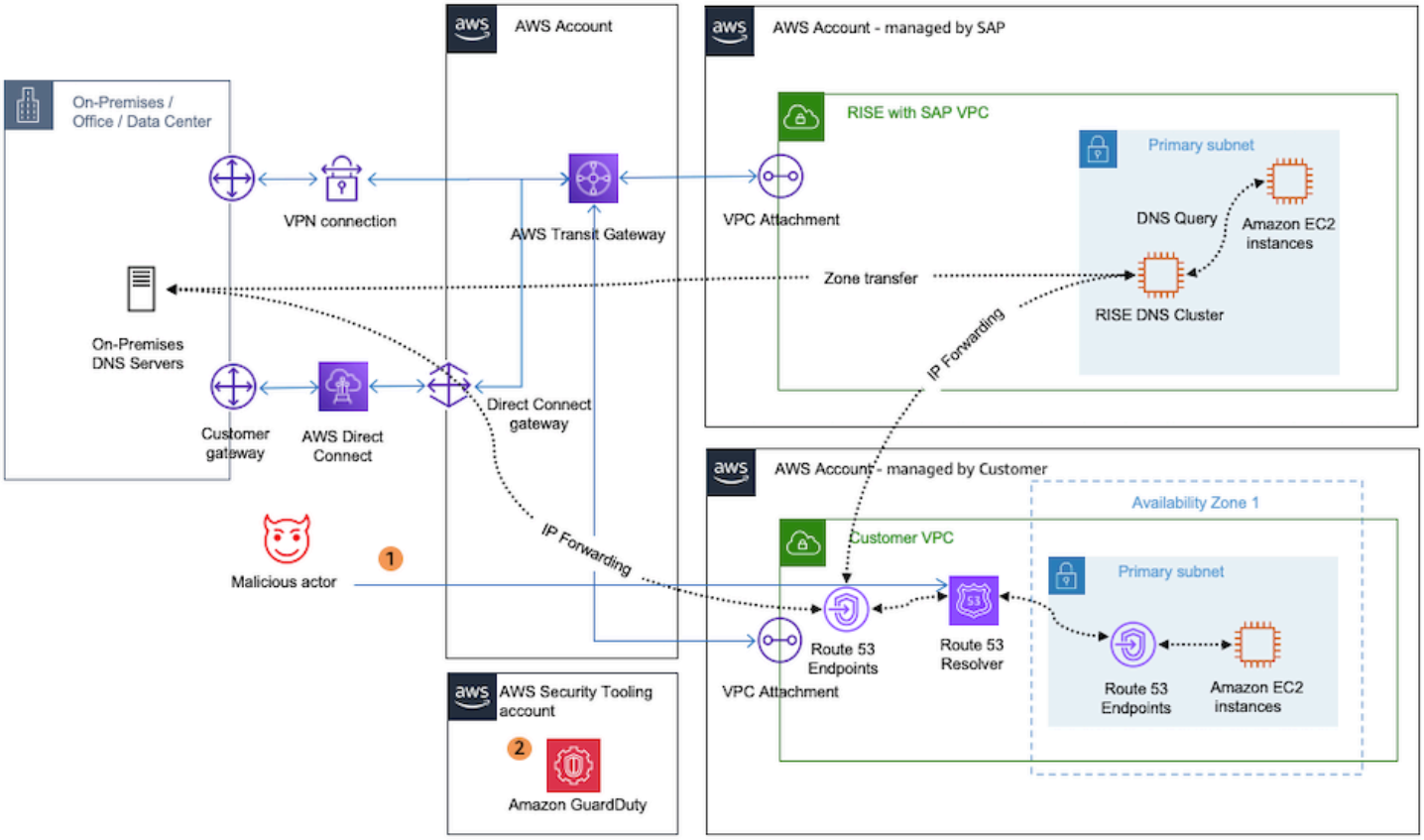
以下是在 SAP 部署状态下 GuardDuty 监控 RISE CloudTrail 跟踪的示例架构 AWS



在上图中

1. 数据被写入 S3 存储桶以用于数据 lake/compliance 报告。
2. 恶意行为者更改 S3 存储桶上的 IAM 规则和 IAM 权限以获取访问权限。
3. IAM 更改会被 AWS CloudTrail拦截。
4. GuardDuty 检测可疑活动并提醒管理员。

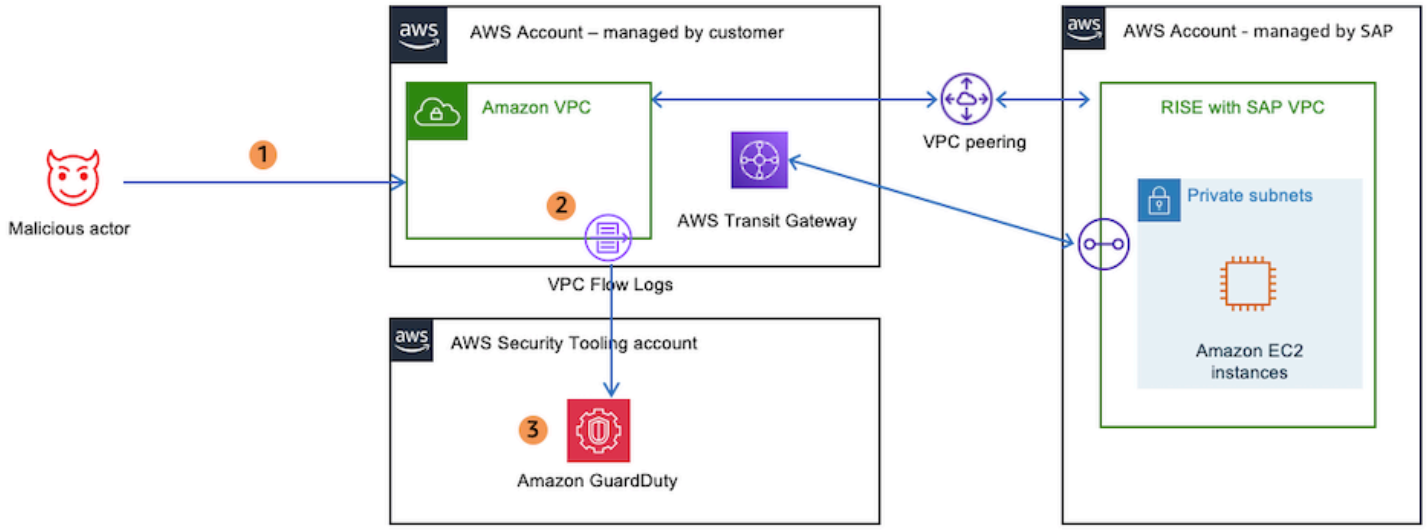
以下是在 SAP 部署开 GuardDuty 启的情况下监控 RISE 的 DNS 日志的示例架构 AWS



在上图中

1. 恶意行为者引入了流氓 DNS，将用户重定向到临时的 SAP 系统。
2. 恶意 DNS 条目由管理员检测 GuardDuty 并报告给管理员。

以下是使用 SAP VPC GuardDuty 监控 RISE 的 VPC 流日志的示例架构



在上图中

1. 恶意行为者试图从客户管理的 VPC 访问 SAP 系统，该虚拟私有网络与 RISE VPC 对等或扫描端口。
2. 从 VPC 流日志中登录的恶意行为者 IP 发起的连接尝试。
3. Amazon 检测到可疑的连接尝试 GuardDuty 并报告给管理员。

有关配置 Amazon 的说明 GuardDuty，请参阅入门。

在 Security Hub、Amazon Detective、Audit M AWS anager 和亚马逊上使用 AWS 安全服务 EventBridge

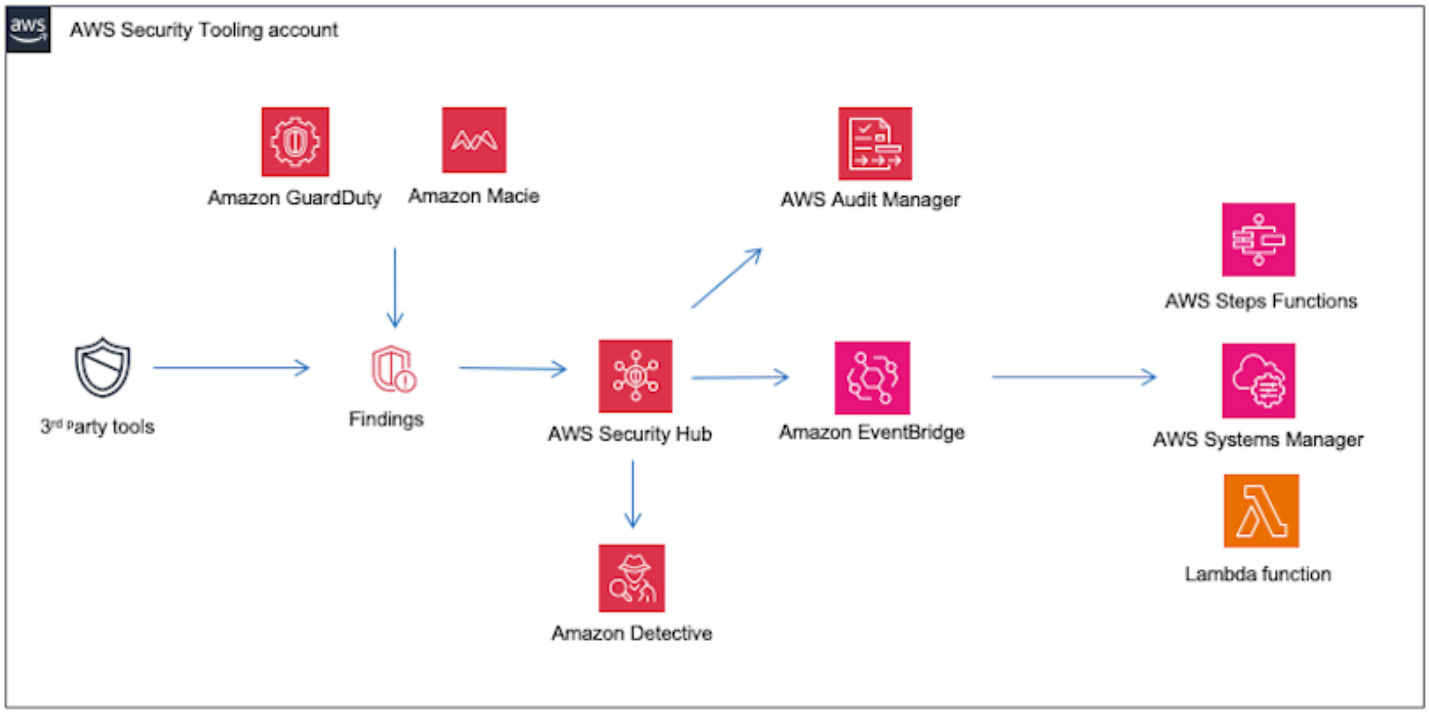
在 Amazon Macie 的 GuardDuty 实施基础上，Sec AWS urity Hub 充当中心枢纽，整合安全调查结果 AWS 安全服务并确定其优先级。 AWS Security Hub 提供了围绕 SAP 部署的 RISE 服务的安全态势的统一视图，从而可以更快地识别和解决任何安全问题。

为了进一步提高调查和事件响应能力，Amazon Detective 通过从 AWS 资源中收集和处理相关日志数据来分析安全事件。该服务有助于快速确定问题的根本原因，从而能够采取适当的措施来减轻影响。

保持合规性也是保护 RISE with SAP 环境的一个关键方面。 AWS Audit Manager 可根据行业标准和法规自动评估 AWS 资源，帮助证明合规性并降低不合规风险。

最后，Amazon 通过触发自定义自动工作流程和补救措施， EventBridge 实现对安全事件的实时响应。该服务允许快速高效地处理安全事件，最大限度地减少部署SAP对RISE的潜在影响

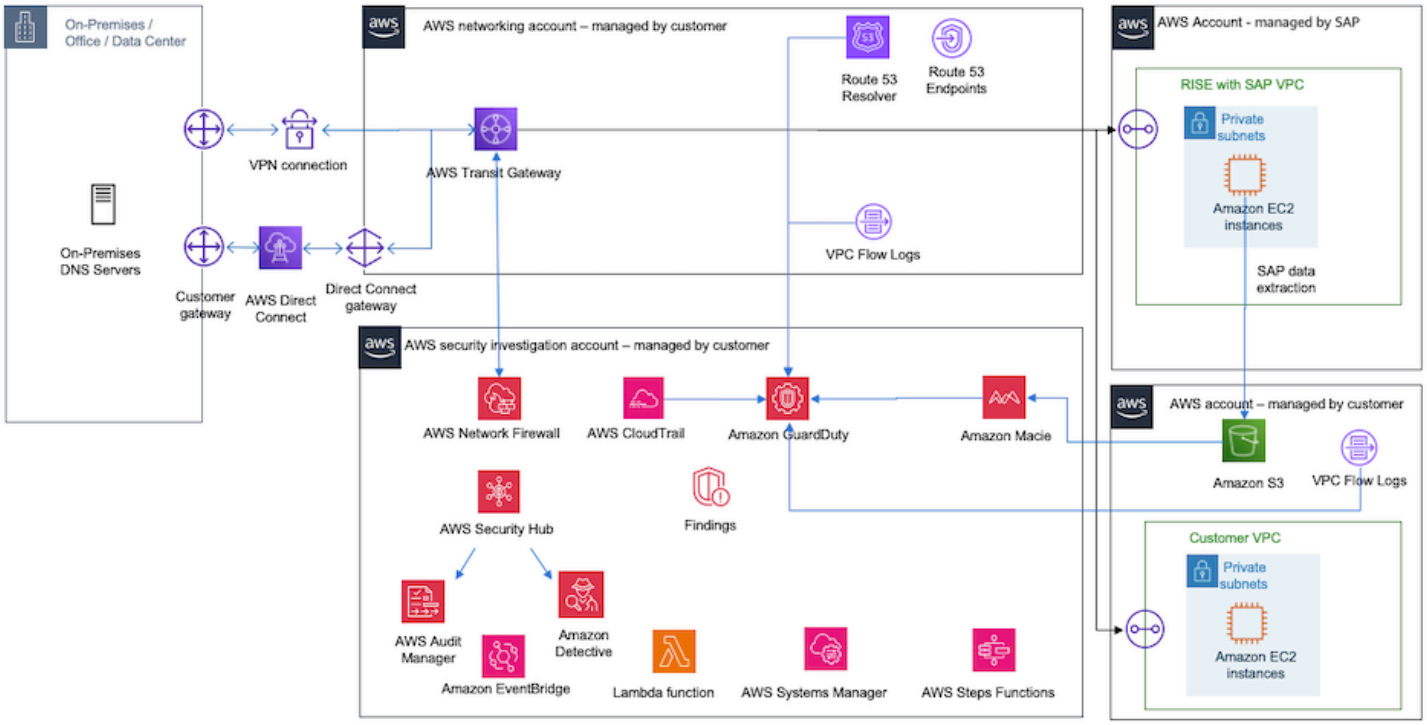
以下是 Sec AWS urity Hub、Amazon Detective、Audit AWS Manager 和亚马逊 EventBridge 与 RISE 与 SAP 配对的架构示例



使用所有 AWS 安全服务

将上述所有服务结合在一起，允许架构在 AWS 部署时监控 RISE 的多个区域：网络流量、DNS 日志、 CloudTrail API 活动、提取的 SAP 数据的敏感信息。Amazon GuardDuty 和 Sec AWS urity Hub 由多种服务提供，并使用 AIML 情报来检测恶意活动和异常情况。调查结果将传递给 Amazon Detective 以进行更深入的 RCA 分析，或者发送给亚马逊 EventBridge 进行自定义报告和提醒。

以下是 Network Fire AWS wall GuardDuty、Amazon Macie、Sec AWS urity Hub 和 Amazon Detective 组合在一起的架构示例，通过部署 SAP 来改善 RISE 的安全状况 AWS



将 SAP 密钥管理服务 (SAP KMS) 与 AWS 密钥管理服务 (AWS KMS) 集成

SAP KMS 是一款多云 SaaS 应用程序，可帮助组织保持云端数据的可见性、控制和加密。它由两项主要服务组成：

- 透明度与控制服务，提供数据治理功能，包括数据沿袭、审计和合规监控。
- 密钥管理服务，它为存储在各种云服务中的数据启用客户管理的加密密钥，包括 AWS. 请注意，SAP KMS 与 AWS KMS 不同。

SAP KMS 通常由 SAP 客户用于以下用途：

- 数据治理与合规。SAP KMS 通过提供对数据存储和处理的可视性、控制和审计，帮助组织遵守全球数据保护法规，例如 GDPR 和 CCPA。
- 数据透明度。SAP KMS 提供实时见解、数据沿袭跟踪和审计功能，用于监控云环境中的数据使用情况和合规性状态。
- 安全和访问控制。SAP KMS 实施了高级安全措施，包括加密、访问控制和异常检测，以保护敏感数据免遭未经授权的访问。
- 自动化和策略管理。SAP KMS 可自动执行数据策略，并允许根据特定业务需求和监管要求量身定制自定义策略。

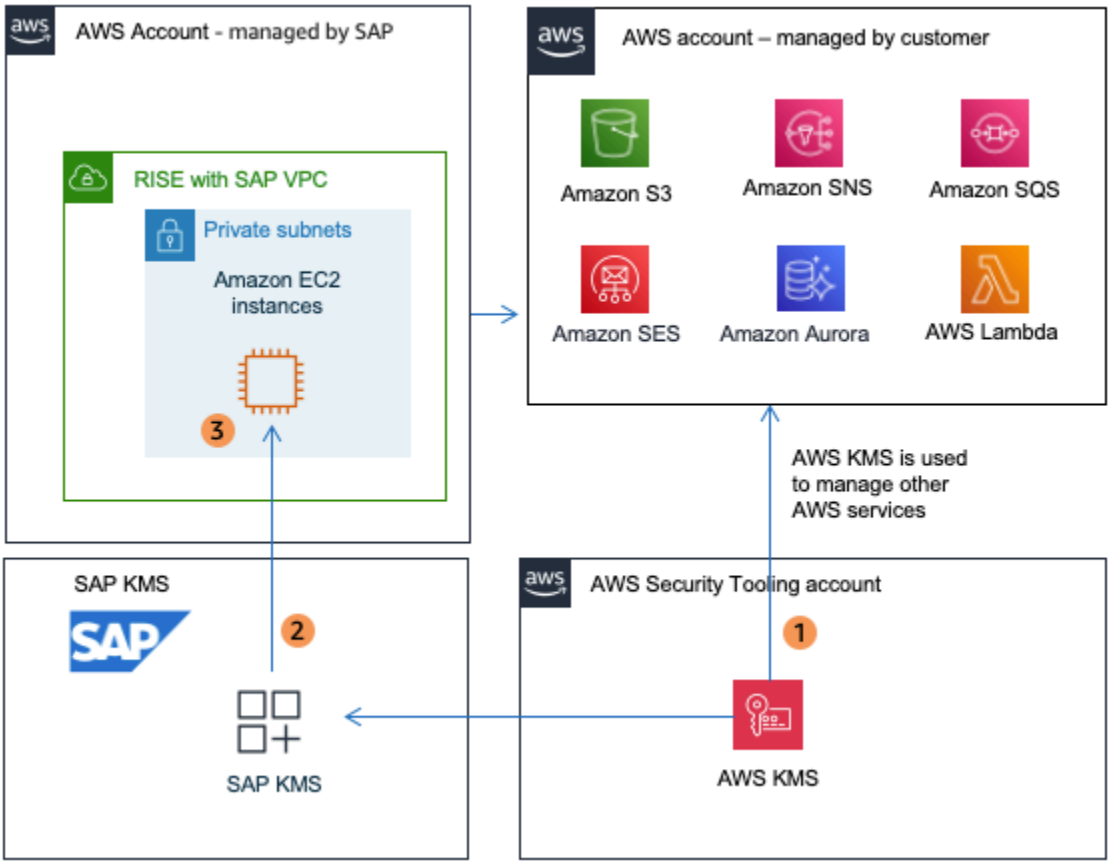
作为使用 SAP KMS 自己的密钥管理服务的替代方案，SAP KMS 可以与 KM AWS S 集成。使用 AWS KMS 作为 SAP KMS 的密钥库可以提供一致的集中式密钥管理方法，尤其是在已将 AWS KMS 用于其他 AWS 工作负载的情况下，可实现无缝集成，简化密钥生命周期管理，并通过 AWS 强大的加密和访问控制机制增强安全性。

这种集成使客户能够管理和控制用于保护其敏感数据的加密密钥，从而确保更高的安全性和合规性。SAP KMS 可以在 BYOK（自带 AWS 密钥）或 HYOK（自带密钥）场景中与 KMS 接口：

区域图	AWS KMS（BYOK 场景）	AWS KMS（HYOK 场景）
支持的密钥类型	AES，RSA	RSA
支持的密钥大小	3072、4096	3072、4096
密钥管理	密钥在 AWS KMS 密钥库中创建并导入到 SAP KMS 提供的租户中	密钥已创建并存储在 AWS KMS 密钥库中
密钥撤销	可以随时禁用或删除密钥	可以随时禁用或取消注册密钥

请注意，SAP 建议在与使用的 SAP 服务和 SAP KMS 租户相同的 AWS 区域中启用密钥库（请参阅 AWS BYOK 场景）。根据密钥库区域的可用性，SAP KMS 仅支持单区域密钥。

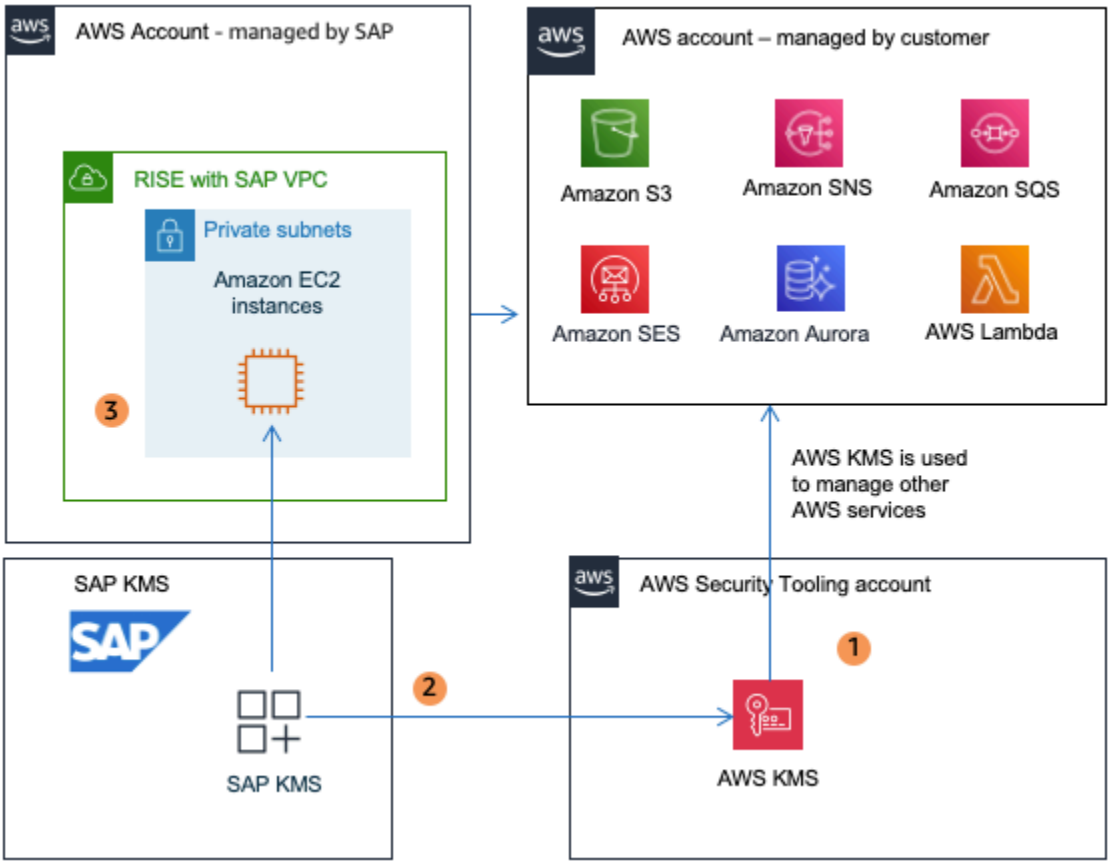
以下是 SAP KMS 与 KM AWS S 的集成-BYOK



在上图中：

- 密钥是在 AWS KMS 密钥库中创建的
- 密钥已导入 SAP KMS 租户中
- SAP KMS 在应用程序级别对 SAP 数据进行加密

以下是 SAP KMS 与 KM AWS S 的集成-HYOK



在上图中：

- 密钥是在 AWS KMS 密钥库中创建的
- 密钥存储在 AWS KMS 中，需要时由 SAP KMS 检索
- SAP KMS 在应用程序级别对 SAP 数据进行加密

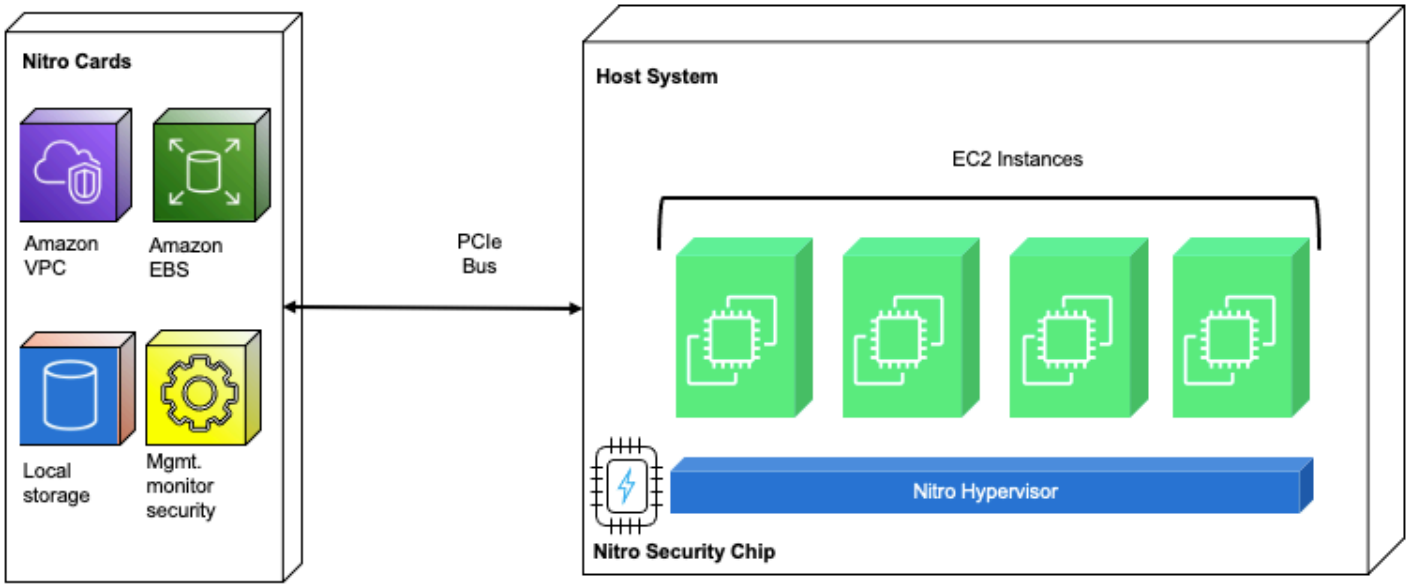
AWS Nitro 如何通过 SAP 帮助保护 RISE？

AWS Nitro System 是使用 SAP 的 RISE 中用于亚马逊弹性计算云 (Amazon EC2) 实例的底层技术。AWS Nitro System 提供了一组独特的功能，可支持多租户、超大规模云环境中最敏感的工作负载。

传统的虚拟化架构包括 “虚拟机管理程序” 或 “虚拟机监视器 (VMM)” 以及 Xen 项目中通常被称为 “Dom0” 或 Hyper-V 中的 “父分区”。 有关传统虚拟化架构的更多详细信息可在此处获得。

在 Nitro System 虚拟化架构中，管理或控制域组件（具有对硬件和设备驱动程序的特权访问权限）被分成独立的专用服务处理器单元（SoC-片上系统），这些单元被称为 Nitro 卡。尽管 “虚拟机管理程序” 层仍然存在，但设计已最小化，仅包括其任务所必需的服务和功能。此外，还推出了 “Nitro Security Chip”，以增强安全性，同时确保没有性能开销。

以下是 Nitro 高级架构



由此产生的 Nitro 系统已分为以下组件：

硝基卡

Nitro Controller-这是物理服务器与 Amazon EBS 和 EC2 Amazon VPC 的控制平面之间唯一的朝外的管理接口。它以被动 API 端点的形式实现，其中记录每个操作，所有调用 API 的尝试都使用细粒度的访问控制模型进行加密身份验证和授权。Nitro Controller 还为整个系统提供硬件信任根，并负责管理服务器系统的所有其他组件，包括系统中加载的固件。系统的固件存储在直接连接到 Nitro 控制器的加密固态硬盘上。固态硬盘的加密密钥旨在通过可信平台模块 (TPM) 和 SOC.nitro 卡的安全启动功能的组合进行保护。Nitro 卡专为特定功能而构建 Nitro Cards 专为特定功能而构建 Nitro 卡：

联网-适用于 VPC 的新一代 Nitro 卡可透明地加密所有 VPC 流量，这些流量在还配备了加密兼容的 Nitro 卡的主机上运行的其他 EC2 实例。它使用关联数据的身份验证加密 (AEAD) 算法和 256 位加密。在 RISE with SAP 中，根据客户的要求，选择不同的计算实例系列。虽然在所有类型的 EC2 实例之间 AWS 提供安全的私有连接，但传输中流量加密仅在下一代实例之间可用。请在此处检查您的 RISE with SAP 实例是否支持此功能。

EBS (SSD) 存储——适用于 EBS 的 Nitro Card 可对远程 EBS 卷进行加密，而不会对其性能产生任何实际影响。

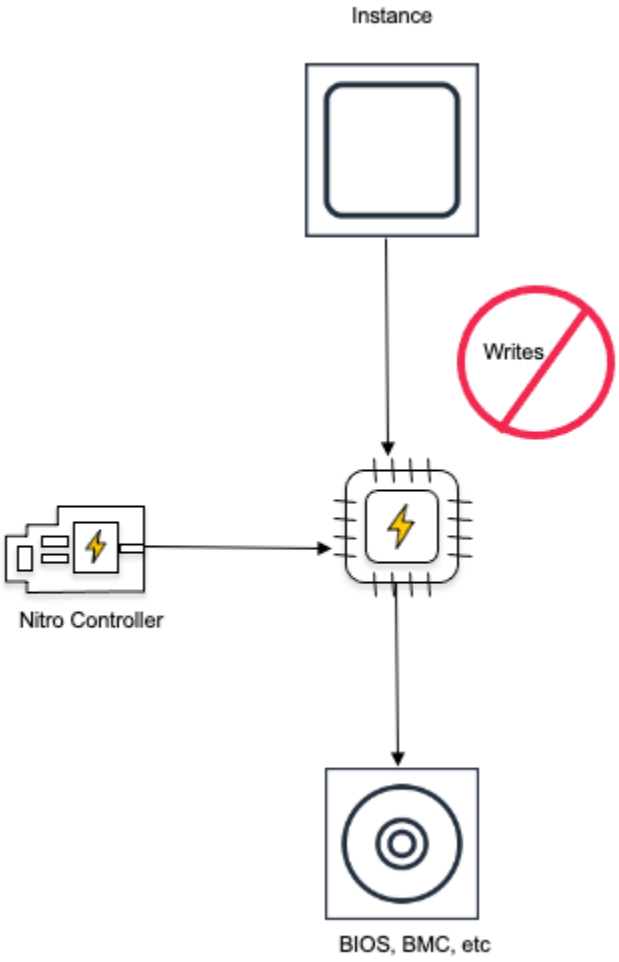
本地实例存储（短暂存储）— 与适用于 EBS 的 Nitro Card 类似，用于实例存储的 Nitro Card 为本地实例存储提供加密。所有 EC2 实例都没有本地实例存储，这将取决于为带有 SAP 工作负载的 RISE 选择的实例类型。详情可以在这里找到。

用于 VPC、EBS 和实例存储的加密密钥只能以纯文本形式存在于 Nitro Card 的受保护内存中。

Nitro Security Chip

当 Nitro Controller 和其他 Nitro 卡作为一个域运行时，运行 SAP 工作负载的系统主板构成了第二个域。虽然 Nitro Controller 及其安全启动过程在 Nitro System 组件之间提供了硬件信任根，但 Nitro Security 芯片用于将这种信任和控制扩展到系统主板。Nitro Security Chip 是这两个域之间的纽带，它将 Nitro 控制器的控制扩展到系统主板，使其成为系统的从属组件，从而扩展了 Nitro Controller 的信任链以涵盖它。为了维护信任根，硬件中会阻止对非易失性存储器的所有写入访问。

以下是 Nitro 阻止对非易失性存储器的写入访问的时间



Nitro Hypervisor

与传统虚拟机管理程序不同，Nitro Hypervisor 不是通用系统，也没有外壳，也没有任何类型的交互式访问模式。Nitro Hypervisor 中增强其安全状况的一些关键排除项包括网络堆栈、通用文件系统实现、外围设备驱动程序支持、ssh 服务器、shell 等。Nitro Hypervisor 的主要功能仅限于：

1. 接收从 Nitro Controller 发送的虚拟机管理命令（启动、停止等）
2. 利用服务器处理器的硬件虚拟化功能对内存和 CPU 资源进行分区
3. 将 Nitro 硬件接口提供的 SR-IOV 虚拟功能（用于 EBS 和实例存储的NVMe 块存储、用于网络的弹性网络适配器 [ENA] 等）分配给相应的虚拟机 PCIe

与传统的虚拟机管理程序相比，Nitro Hypervisor 的这种简单性具有显著的安全优势。

AWS 硝基系统的主要优点

- Nitro 芯片将虚拟化任务从主芯片中卸载 CPUs，从而减少了攻击面并提高了整体系统的安全性。
- AWS 人员无权在 AWS Nitro System EC2 实例上访问您的内容。没有技术手段或 AWS 人员 APIs 可以访问您在 Nitro System EC2 实例或连接到 AWS Nitro System 实例的加密 EBS 卷上的内容。AWS EC2 对 AWS Nitro Syste APIs m EC2 实例的访问始终会被记录下来，该实例允许 AWS 人员在不访问您的内容的情况下操作系统，并且需要身份验证和授权。请在此处查找更多信息。
- 租户保护和侧信道攻击防护-Nitro Hypervisor 由 Nitro 控制器指示，为实例分配全部物理内核和内存。这些硬件资源被 “固定” 到该特定实例。CPU 内核不用于运行其他客户工作负载，也不会以任何方式在实例之间共享任何实例内存页面。不共享 CPU 内核意味着实例永远不会共享特定于 CPU 核心的资源，包括 1 级或 2 级缓存，从而可以强有力地缓解侧信道攻击。请在此处查找更多信息。
- Nitro 架构允许安全启动和运行时完整性验证，确保 AWS 基础架构在可信和经过验证的状态下运行。
- Nitro Card 固件和虚拟机管理程序均设计为可实时更新（客户实例的停机时间为零）。这消除了围绕更新进行仔细权衡的必要性，从而改善了安全状况。请在此处查找更多信息。
- 使用集成在 SoC 中的安全密钥存储的硬件卸载引擎对静态和传输中的数据进行数据加密。

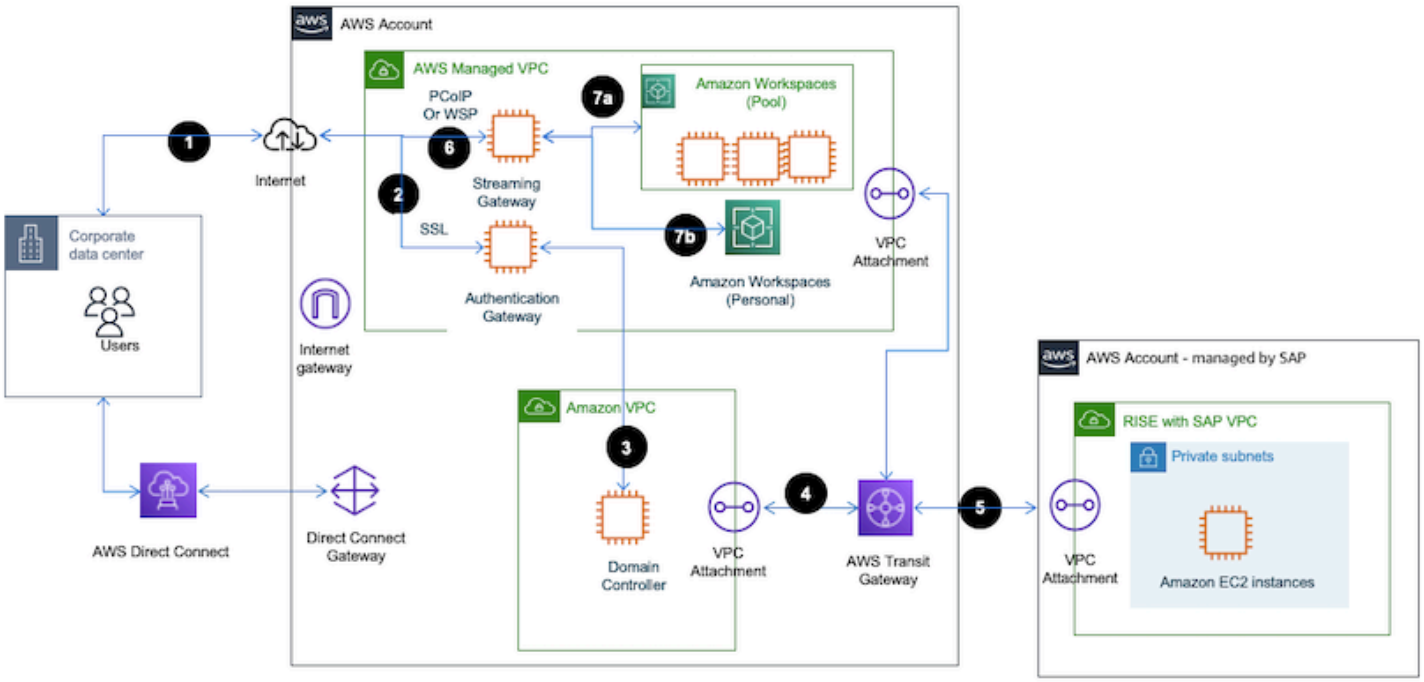
Amazon WorkSpaces 是 RISE 与 SAP 合作的远程访问解决方案

使用 Amazon WorkSpaces 可以为访问 SAP 系统提供安全、可扩展和托管的虚拟桌面环境。该虚拟桌面可用作 SAP最终用户软件（例如SAPGUI）的集中管理托管平台，并通过SAP连接到RISE中的SAP S/4HANA环境。

Amazon Personal 提供永久虚拟桌面，专为需要配置高度个性化的桌面供其专用（类似于分配给 WorkSpaces 个人的物理台式机）的用户量身定制。

Amazon P WorkSpaces ool 提供非永久虚拟桌面，专为需要访问临时基础设施上托管的精心策划的桌面环境的用户量身定制。

下图显示了如何使用亚马逊 WorkSpaces 作为带有 SAP 的 RISE 的远程访问解决方案。



交通流

1. 用户通过 Web 浏览器或WorkSpaces 客户端启动与 AWS WorkSpaces URL 的连接。
2. 用户通过 AWS 托管 VPC 内的身份验证网关进行身份验证。当最终用户登录时，Authentication Gateway会根据目录服务对用户进行验证，一旦用户通过身份验证，网关就会为用户建立安全会话以访问其虚拟桌面。这种会话管理可确保用户在活动会话期间 WorkSpaces 保持可访问状态，并有助于维护会话的完整性和安全性。这部分架构在端口 443 上使用带有 TCP 协议的安全套接字层 (SSL)。
3. 连接通过另一个 VPC 附件进行路由，到达单独的 Amazon VPC 中的域控制器。域控制器管理用户的权限和访问控制策略。它可确保用户根据其角色和群组成员资格，拥有对资源的适当访问权限。这通常通过集成来完成（例如 AWS 托管 Microsoft AD 或通过 AWS Directory Service 连接的本地 AD）
4. Transit Gateway 管理 Direct Connect 或 VPN 之间的 VPCs 路由。 AWS Direct Connect 或 VPN 提供 AWS 与 SAP RISE 环境的安全连接。
5. 在用户的设备和 SAP 托管的 RISE VPC 之间建立安全会话。
6. AWS 托管 VPC 内的流媒体服务网关开始将虚拟桌面环境流式传输到用户的设备。这种直播在 AWS 基础架构内受到保护和管理。流媒体网关通过互联网将桌面流安全地传输到用户的设备。现在，用户的设备可以通过诸如SAPGUI之类的SAP最终用户软件访问托管在RISE环境中的SAP S/4之类的SAP应用程序。

7. 根据您的组织和用户需求，Amazon WorkSpaces 允许您访问以下 2 种类型的 WorkSpaces

   WorkSpaces 在@@ 池化配置中，池 WorkSpaces 是动态分配给共享池中的用户的。当用户登录时，他们可能并不总是连接到同一台计算机，而且，诸如已安装的应用程序或用户配置之类的更改通常不会在会话之间持续存在

   WorkSpaces 个人，在此配置中，为每个用户分配了自己的专用虚拟桌面，他们可以在其中安装应用程序、保存文件以及在会话之间保留其设置和数据。

为亚马逊设置 SAP WorkSpaces RISE Access

1. 要使用或设置 Amazon 连接 WorkSpaces 到 SAP RISE，请按照 “入门” 进行操作 WorkSpaces。
2. 有关将亚马逊 WorkSpaces 与 SAP 集成的更多信息 Single-sign-on，请参阅如何将亚马逊 WorkSpaces 与 SAP 单点登录集成
3. WorkSpaces 从 SAP 软件下载中安装你的 SAPGUI
4. WorkSpaces 使用你@@ 的 SAP 系统详细信息通过 SAPGUI 客户端连接到 SAP 系统

Amazon Workspaces 运营最佳实践

1. 监控：AWS CloudWatch 用于监控您的性能和运行状况 WorkSpaces。
2. Backup and Recovery：确保您的 WorkSpaces 关键数据已备份，并制定了恢复计划。
3. 更新和维护：定期更新您的软件和系统 WorkSpaces ，以确保安全性和合规性。默认情况下，Windows WorkSpaces 将每周自动更新一次。
4. 优化 性能

   扩展和性能调整：您可以根据用户需求在标准、功耗、性能和计算类型 WorkSpaces 之间切换。
5. 成本管理

   WorkSpaces 捆绑包：考虑购买包含最终用户软件需求的虚拟桌面套装。通常，对于简单的 SAPGUI 访问，“价值” 用户可以节省成本。更多详情请参阅AWS WorkSpaces 定价页面

   监控使用情况：使用 C AWS ost Explorer 和预算来有效地监控和管理成本。

   对于非持久、安全的桌面访问，可以考虑将 P WorkSpaces ools 视为极具成本效益的选择。

通过执行这些步骤，您可以将 Amazon WorkSpaces 设置为使用 SAP 系统的 RISE 的有效远程访问解决方案，从而确保安全、可扩展和高效的运营。

WorkSpaces RISE 的好处

在部署SAP的RISE中使用Amazon WorkSpaces 作为远程访问解决方案可以带来多项好处，尤其是在安全、访问控制和运营效率方面。以下是这种方法的主要优点：

1. 增强安全性和受控访问

   隔离环境： WorkSpaces 提供一个隔离的环境，在该环境中，可以严格控制对 RISE 部署中的 SAP 系统的访问。这有助于防止未经授权的直接访问关键系统

   不直接暴露互联网：通过 WorkSpaces 用作远程访问解决方案，您可以限制对 SAP 环境的互联网访问。外部用户或管理员必须首先连接到安全的 WorkSpaces、限制对 SAP 系统的暴露。

   安全协议 (PCoIP/WSP)： WorkSpaces 使用 PCo IP 或 WSP 等安全流媒体协议，确保在传输过程中对数据进行加密。

   减少攻击面：通过 WorkSpaces 将其用作 SAP 系统的唯一访问点，您可以将 SAP 环境与通过互联网或公司网络的直接访问隔离开来，从而减少攻击面。

   VPC 集成： WorkSpaces 可以部署在亚马逊虚拟私有云 (VPC) 的私有子网中，确保使用 SAP 基础设施安全直接地连接到 RISE。

   AWS Direct Connect 或 VPN：您可以使用 AWS Direct Connect 或 VPN 连接在 WorkSpaces 和 SAP 环境之间提供安全的网络路径，从而进一步增强安全性。

2. 集中管理

   统一接入点：Amazon WorkSpaces 充当使用 SAP 环境管理和运营 RISE 的单一访问点，从而简化了监控和控制。

   审计和记录： AWS CloudTrail 和 Amazon 等 AWS 服务 CloudWatch 可以记录用户操作并监控用户在上的活动 WorkSpaces。这有助于安全审计和跟踪 SAP 系统的访问权限。

   与 AWS IAM 集成：通过 AWS 身份和访问管理 (IAM) 进行基于角色的访问控制 (RBAC)，可确保对 SAP 资源的精细访问。 WorkSpaces 这样可以最大限度地降低未经授权访问的风险并支持合规性要求。

3. 提高运营效率：

   按需扩展性： WorkSpaces 可以快速配置并按需扩展，因此无需漫长的设置过程即可轻松为需要访问 SAP 环境的管理员或开发人员提供访问权限。

最少的维护：Amazon WorkSpaces 完全托管，这减少了维护物理服务器或传统远程桌面基础设施的开销。更新和补丁由处理 AWS，从而腾出时间进行更关键的操作。

成本效益： WorkSpaces 可以配置为仅在使用时收费（按小时定价），这使其成为临时或不经常访问的经济实惠的解决方案，尤其是在非连续运行时。

远程访问：通过远程访问 WorkSpaces，管理员和用户可以从任何有互联网连接的位置安全地访问 SAP 环境。这对于支持 SAP 环境的分散团队或远程员工特别有用。

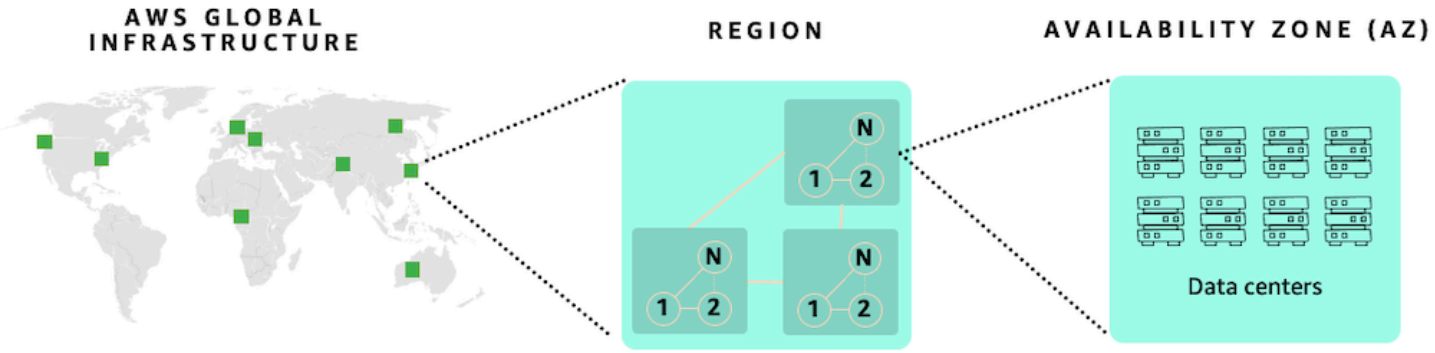
弹性和可用性： WorkSpaces 可以与 AWS 备份解决方案集成并分布在多个 AWS 可用区 (AZs)，从而确保冗余和高可用性。

快速恢复：在 SAP 环境出现故障或灾难时， WorkSpaces 提供一种快速且可扩展的方式来重新连接到备用环境或备份系统。

可靠性

可靠性是 SAP Lens——Well-Architecte AWS d Framework 的六大支柱之一。有关更多信息，请参阅可靠性。

AWS 云在一个区域内有多个可用区， AWS 可提供可靠性。这使您的 SAP 应用程序 AWS 能够更具弹性。每个区域与其他区域进一步隔离，从而提供尽可能高的容错能力和稳定性。在每个 AWS 区域内，至少有三个隔离、物理上独立的可用区。有关更多信息，请参阅区域和可用区。

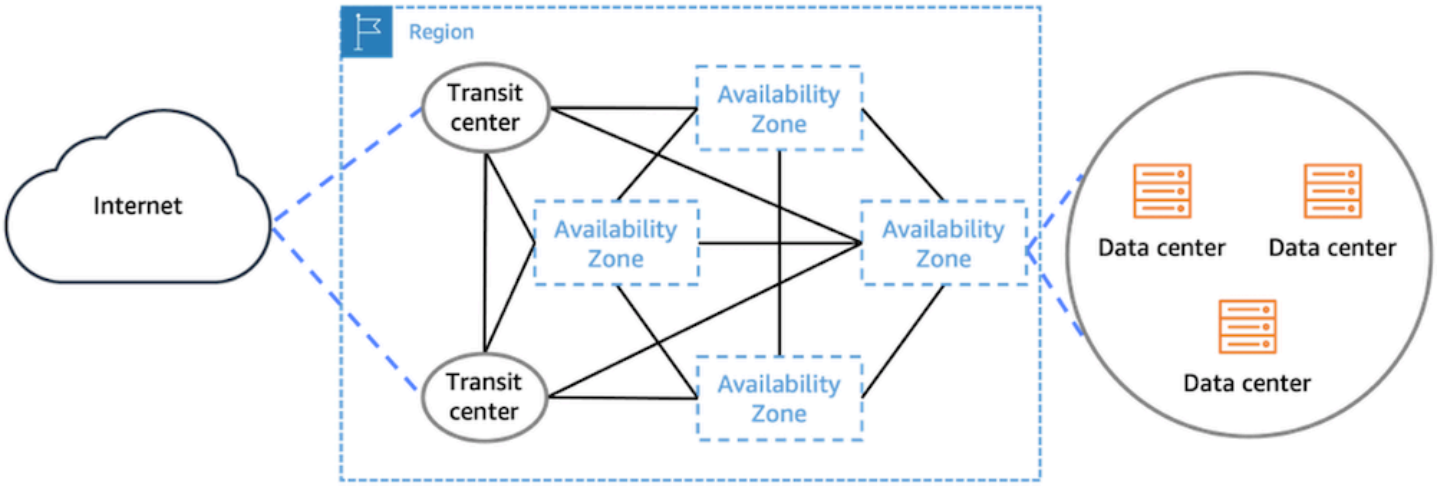


可用区使您能够操作生产应用程序和数据库，这些应用程序和数据库的可用性要高于单个数据中心所能达到的可用性。将您的应用程序分布在多个可用区中，使您能够在面对大多数故障模式（包括自然灾害或系统故障）时保持弹性。

每个可用区可以是多个数据中心。全面而言，它可以包含数十万台服务器。它们是 AWS 全球基础设施的完全隔离的分区。可用区在物理上与任何其他区域隔开，拥有自己的独立电源和网络资源。有几千米

的距离，尽管所有距离都在100千米以内（彼此相距60英里）。这种距离可以隔离可能影响数据中心的最常见灾难，例如洪水、火灾、暴风雨、地震等。

一个区域内的所有可用区域都通过完全冗余的专用城域光纤与高带宽和低延迟网络互连。这可确保可用区域之间的高吞吐量、低延迟联网。网络性能足以完成同步复制。



可用区使您能够以高度可用的方式运行应用程序，在可用区之间进行同步数据复制和自动故障转移。RISE with SAP 可以为你在每个 AWS 地区的工作负载提供如此高的可用性设计。

弹性和成本注意事项

SAP 为 RISE 提供了多种选项，以满足不同的弹性要求。RISE的以下关键要求可通过SAP提供的选项包进行调整。

- 服务级别协议 (SLA)-描述解决方案的目标可用性。
- 恢复时间目标 (RTO)-描述从灾难事件中完成恢复的目标持续时间。
- 恢复点目标 (RPO)-描述灾难事件恢复期间可能发生的目标数据丢失级别。

有关更多详细信息，请参阅 SAP 在 RISE 协议中提供的定义，了解违规时的具体定义、条款、影响和处罚。

中断对您的组织的影响和数据丢失可能导致生产力下降和收入损失，并可能损害声誉。权衡成本和弹性之间的权衡有助于评估组织面临的风险。

弹性和性能注意事项

当您选择 RISE 中的短距离灾难恢复选项时，SAP 应用程序服务器和数据库服务器将安装在多个可用区中。此架构支持针对您的 SAP 工作负载的高可用性设计。

在主动-主动配置中使用多个可用区域中的应用程序服务器时，它可以提高弹性。同时，引入了从应用程序服务器到数据库服务器的跨可用区域更高的延迟。您可以参阅 SAP Note 3496343（开启网络延迟 AWS），其中详细介绍了在多可用区部署中由于应用程序服务器和数据库服务器之间的距离而增加的延迟。这将在下一节中详细讨论。

- 根据 SAP Note 1100926，SAP 应用程序服务器和数据库服务器之间的网络延迟应小于 0.7 毫秒
- 使用同步数据复制（实现零数据丢失所必需的）的 HANA 系统复制的网络延迟小于 1 毫秒

您可以使用 AWS Network Manager-基础设施性能工具自动测量可用区间、可用区内和区域间网络延迟。或者，你可以按照 SAP N ote 2986631 的规定使用 SAP 的 NIPING 工具。

当 SAP 应用程序服务器和数据库服务器分布在多个可用区 (AZs) 时，它可以显著增强系统的可靠性和可用性，抵消网络延迟增加的影响。

跨可用区域流量可能会增加执行频繁调用数据库的某些事务或批处理作业所需的时间。如果影响很大，我们建议使用 SAP 登录组、RFC 服务器组和 Batc h Server Groups ulink> 将此流量保持在同一个可用区内。这样可以确保受影响的事务或批处理作业仅使用与数据库服务器位于同一可用区的应用程序服务器。

为了在与数据库服务器位于同一可用区的应用程序服务器上自动化和优化此类性能关键型批处理作业和事务的运行， AWS 提供了客户可以在其 S AP 系统中测试和实施的 ABAP 代码示例。

你可以参阅 re AWS : Post 文章 SAP 的可用区间延迟来降低网络延迟，从而通过 C-State 参数实现进一步的优化。

当无法在多个可用区的主动-主动模式下运行应用程序服务器时，您可以使用 ABAPSetServerInactive (SAP Note 3075829) 在主动-被动模式下运行

在极少数情况下，当您在一个可用区域内观察到延迟导致的性能影响时，您可以使用集群置放群组来实现尽可能低的延迟。您可以从中参阅《放置策略指南》 AWS。

总而言之，以下是多可用区部署中的架构模式：

中的应用程序服务器 AZ1	中的应用程序服务器 AZ2	故障转移机制从 AZ1 到 AZ2
活动	活动	自动脚本（即起搏器）
活动	活动	手动调整登录组、RFC 和 Batch 服务器组

中的应用程序服务器 AZ1	中的应用程序服务器 AZ2	故障转移机制从 AZ1 到 AZ2
活动	活动	用于调整登录组、RFC 和 Batch 服务器组的自动脚本
活动	Passive	手动激活被动应用程序服务器
活动	Passive	用于激活被动应用程序服务器的自动脚本

为了实现 SAP 工作负载的高可靠性，我们建议执行以下任务：

1. 与 SAP 讨论 RISE 部署的可用性 SLA 要求。这将推动将部署在多个可用区的组件（即数据库和应用程序服务器），以最大限度地提高 RISE 的可靠性和可用性。
2. 如果您的业务场景涉及频繁调用数据库服务器的批处理作业 and/or ，可能会受到可用区间网络延迟的不利影响，则可以考虑使用 SAP 的工作负载分配机制（SAP 登录组、RFC 服务器组和 Batch Server 组）来确保这些作业和事务在与数据库服务器位于同一可用区的应用程序服务器上运行
3. 你可以通过参阅 re AWS : Post 文章 SAP 的可用区间延迟来进一步优化网络延迟。
4. 当主动-主动模式不可行时，您可以使用 ABAPSetServerInactive （SAP Note 3075829）在应用程序服务器的主动-被动模式下运行。
5. 您可以考虑将 RISE 之外的其他工作负载放在同一个可用区内，以实现更好的网络延迟和更低的数据传输成本。

灾难恢复选项

您可以通过将数据复制到第二个 AWS 区域来实施灾难恢复解决方案。您的 SAP 工作负载将受到保护，以防发生罕见的本地或区域故障。

搭载 SAP S/4HANA Cloud 的 RISE 私有版提供以下两个选项。

- 短距离灾难恢复或城域灾难恢复 — RISE with SAP 在一个 AWS 区域中使用多个可用区。具有三个或更多可用区的独特 AWS 区域提供了在每个 AWS 区域进行短距离灾难恢复的选项。
- 远距离灾难恢复或区域灾难恢复 — RISE with SAP 使用辅助 AWS 区域作为故障转移系统的备用区域。由于两个区域之间的物理距离，因此数据是在两个 AWS 区域之间异步复制的。 AWS

有关更多详细信息，请参阅 SAP 文档 SAP 服务描述：灾难恢复和客户调用的故障转移。

扩展

您可以使用 AWS 服务来提高性能、安全性、敏捷性并降低成本，从而通过 SAP 扩展 RISE。下表根据用例提供了推荐的 AWS 服务。

类别	应用场景	AWS 服务
性能	具有主动可观察性的 SAP Fiori 和 SAP GUI 访问权限	亚马逊 CloudFront、加速 Site-to-Site VPN、AWS 互联网监控器
数据集成	数据提取和数据联合	亚马逊 Appflow 、适用于 SAP 的 AWS Glue OData、AWS 适用于 SAP的 SDK ABAP、亚马逊 Athena
数据分析	数据湖和数据仓库	AWS Lake Formation、亚马逊 S3、亚马逊 QuickSight、亚马逊 Redshift
应用程序集成	应用程序集成	AWS Lambda 和 A mazon API Gateway
存档和文档管理	存档和文档管理	亚马逊 S3、AWS S3 文件网关、亚马逊 EFS
开发和扩展	开发、兼容包和替代方案	AWS 适用@@ 于 SAP ABAP 的 SDK，AWS Mar ket
安全扩展	单点登录，零信任访问	通过 Amazon ALB 进行 mTLS 身份AWS验证，SAP 已验证访问权限
人工智能	生成式人工智能	Amazon Q for Busines s、Amazon Q in QuickSigh t、Amazon Bedrock

性能

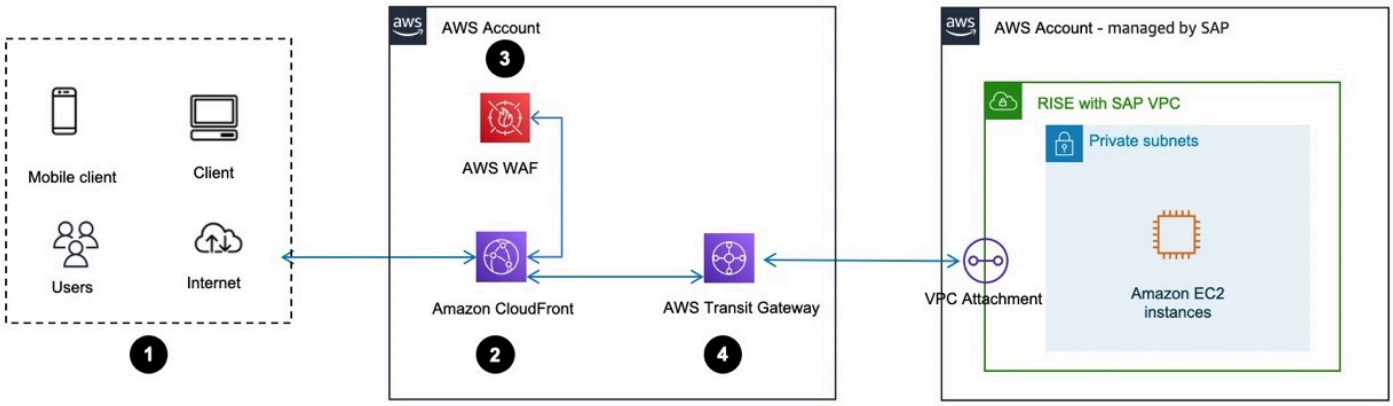
借助亚马逊提高 SAP Fiori 的绩效 CloudFront

亚马逊 CloudFront是一项内容分发网络服务，旨在通过SAP提高RISE中SAP Fiori启动板的性能并减少延迟。 CloudFront 为静态内容创建缓存，并通过边缘计算加速动态内容。

来自多个地理区域的用户访问的全球 SAP 系统可以使用 A mazon CloudFront VPC（虚拟私有云）Origins 来减少网络延迟并改善 SAP 最终用户体验。

CloudFront VPC Origins 是一项功能，可增强安全性并简化托管在 Amazon VPC 私有子网中的 SAP Fiori 等网络应用程序的操作。这种架构 CloudFront 允许作为 SAP Fiori 的单一入口点，从而无需将 SAP 服务器公之于众。

CloudFront VPC Origins 部署在客户管理的 AWS 账户中，将 SAP 用户引导到内部的 Appl CloudFront ication Loa d Balancer (ALB)。AWS ALB 通过 T AWS ransit Gateway 将 Fiori 流量直接路由到 SAP RISE AWS 账户中托管的 SAP 系统。 AWS Web 应用程序防火墙 (WAF) 是可选的，但建议使用它来改善安全状况。



数据流

1. 用户通过互联网浏览器或移动设备访问 SAP Fiori 启动板
2. 请求会被路由到 Amazon CloudFront ，到达用户所在位置最近的边缘计算
3. 或者， AWS Web 应用程序防火墙 (WAF) 会根据客户配置的规则评估请求，以阻止恶意流量。此外，AWS Shield St andard 还提供分布式拒绝服务 (DDOS) 保护，当您与 WAF CloudFront 一起 AWS 使用时，该保护将自动包含在内，无需支付额外费用
4. 然后，请求被解析到 ALB， AWS ALB 会将流量转发到 SAP 托管 RISE 账户中托管的 SAP 系统。

这通过以下方式改善了 SAP 系统的安全状况：

- 消除 SAP 服务器直接暴露在公共互联网上
- 缩小攻击面，因为攻击面 CloudFront 成为唯一的入口点
- 通过集中控制来简化安全管理 CloudFront
- 可轻松与 AWS WAF 和 AWS Shield 标准集成，提供额外保护

将 CloudFront VPC Origins 与 SAP 集成可以提高性能：

- 全球用户受益于 CloudFront全球边缘站点
- 使用AWS 全球网络骨干对流量进行优化。 CloudFront 流量一直保持在高吞吐量的 AWS 全球网络主干上，一直延伸到你的 SAP 服务器，从而提供优化的性能和低延迟
- 静态 SAP Fiori 内容缓存在边 CloudFront 缘位置，动态的 SAP Fiori 内容通过其全球边缘网络进行 CloudFront加速

要为 SAP 实施 CloudFront VPC 起源，请执行以下操作：

1. 默认情况下，RISE with SAP 中的应用程序托管在私有 VPC 子网中， AWS 账户由 SAP 管理
2. 在客户管理的 AWS 账户中，在 RISE 账户中创建一个指向 SAP 系统的 AWS ALB
3. 创建一个 VPC 起源指向 AWS ALB 的 CloudFront 分配
4. 更新您的 VPC 私有源（在本例中为AWS ALB）的安全组，以明确允许 CloudFront 托管前缀列表。这限制了进入 VPC 来源的流量
5. 确保 ALB 和 SAP 使用相同的完全限定域名 CloudFront
6. 配置 CloudFront 为处理来自 SAP 系统的静态和动态内容
7. （可选）实施 AWS WAF 以提高边缘的安全性

有关更多信息，请参阅 AWS 文档限制使用 VPC 源进行访问。

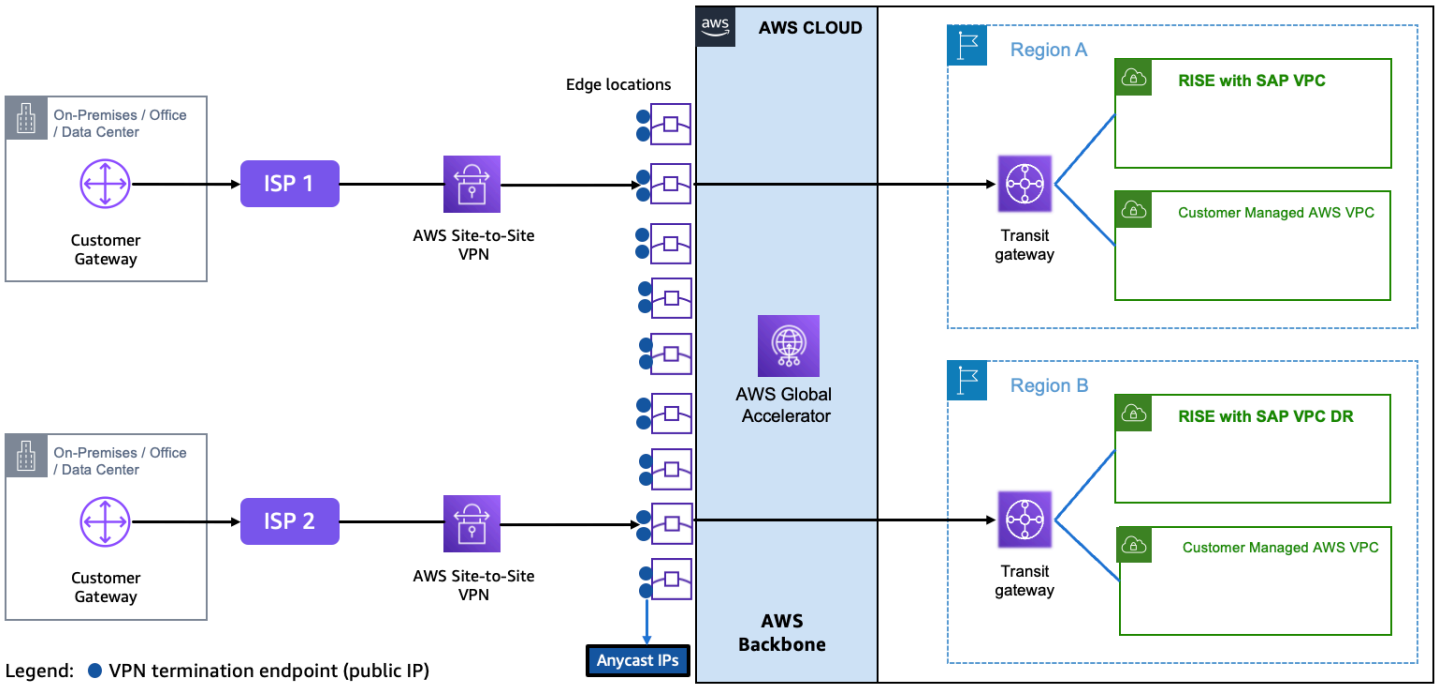
通过加速 Site-to-Site VPN 连接优化性能

当你在开启 SAP 的情况下部署 RISE AWS 进行全球推广时，你可以利用基于AWS 全球加速器的加速 Site-to-Site VPN 来减少网络延迟。该服务是对基础Transit Gateway和Direct Connect的补充，可解决地理位置分散的用户的性能挑战，同时确保通过SAP高效、安全地访问任务关键型RISE。它同时支持 SAP Fiori（HTTPs 基于）流量和 SAP GUI（基于 TCP）的流量。

AWS Global Accelerator 是一项创建加速器以提高本地和全球用户应用程序性能的服务。它作为第 4 层 TCP/UDP 代理运行，优化了通过全球网络基础设施 AWS的流量路由。它终止 AWS 边缘位置的客

户端 TCP 连接，并通过私有主干与后端端点建立新 AWS的 TCP 连接。因此，通过绕过公共互联网跳线来减少延迟（高达75%，因地点而异），并确保全球分布的用户无拥塞路由。

加速 Site-to-Site VPN 连接将传统 AWS Site-to-Site VPN 与 AWS 全球加速器相结合，以优化流量路由。它利用 AWS 主干将流量从本地网络路由到离客户网关设备最近的 AWS 边缘位置。与标准相比，这将使延迟减少多达30%-60%。 VPNs



使用 SAP 使用 AWS 互联网监视器增强 RISE 的可观察性

AWS Intern et Monitor 持续分析最终用户和 AWS托管应用程序之间的互联网流量，检测可能影响 RISE 和 SAP 性能的网络异常。它提供了对延迟增加、数据包丢失或区域连接中断等问题的见解，使组织能够在潜在的中断影响 SAP 工作负载之前主动解决这些问题。

RISE with SAP 依赖于稳定且可预测的网络性能， AWS Internet Monitor 可通过以下方式

- 识别影响 SAP 响应时间的 ISP 或区域网络中断。
- 提供早期预警和可行的建议，以缓解与网络相关的服务降级。
- 区分 AWS 基础设施问题和外部互联网中断，简化故障排除。
- 提高 Internet 路由的可观察性，该路由是动态的，缺乏可预测的服务级别协议 () SLAs。
- 主动管理外部 ISPs 和传输提供商，这可能会带来不可预测的延迟、数据包丢失和拥塞问题。

要实现该功能，您可以参阅 Internet Monitor 入门。

数据集成

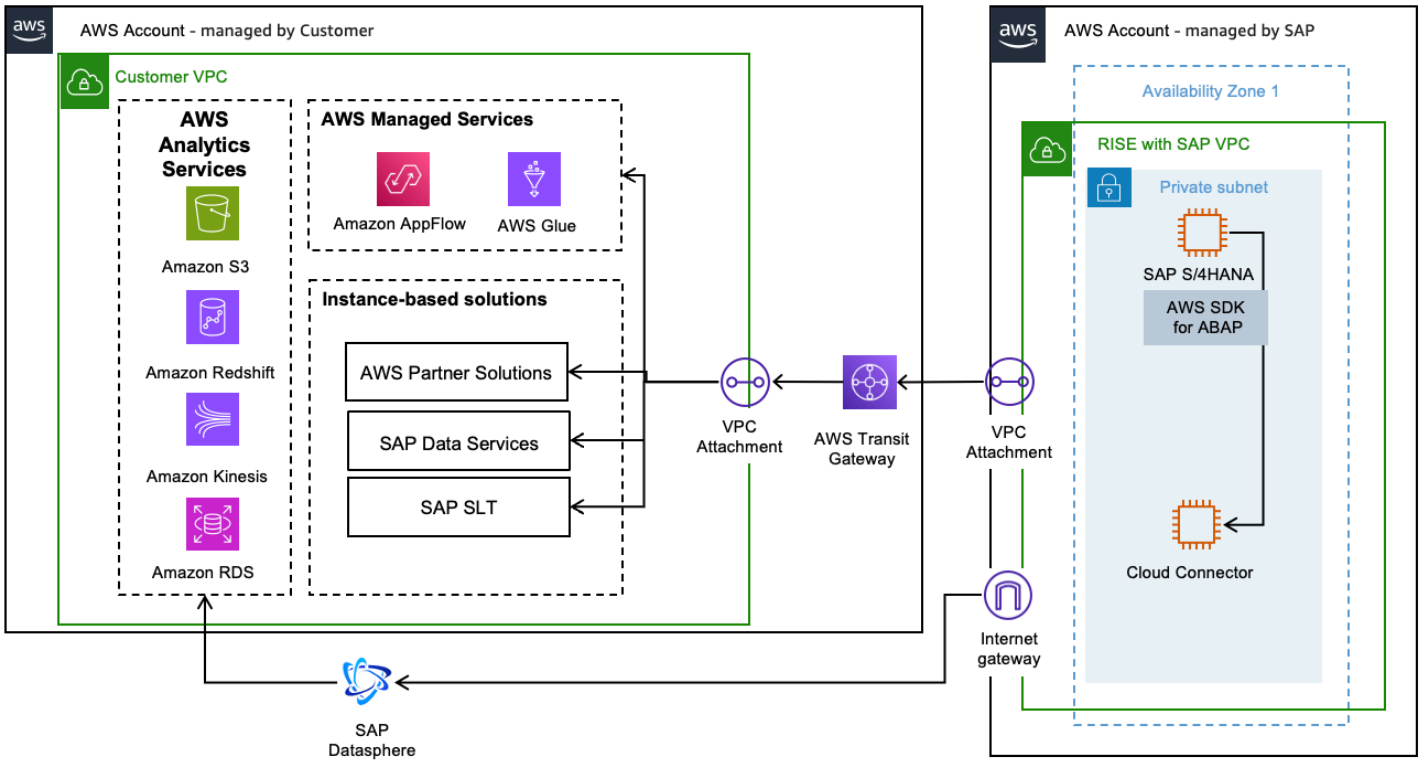
RISE with SAP 数据集成可扩展性 AWS 是一个技术框架，可在 SAP 系统、 AWS 服务和第三方解决方案之间实现数据流动。这种集成架构提供了标准化 APIs、连接器和协议，用于建立安全的通信渠道，满足了现代云环境中企业数据无缝集成的关键需求

RISE with SAP 数据集成可扩展性概述了两种主要的数据处理和集成机制：

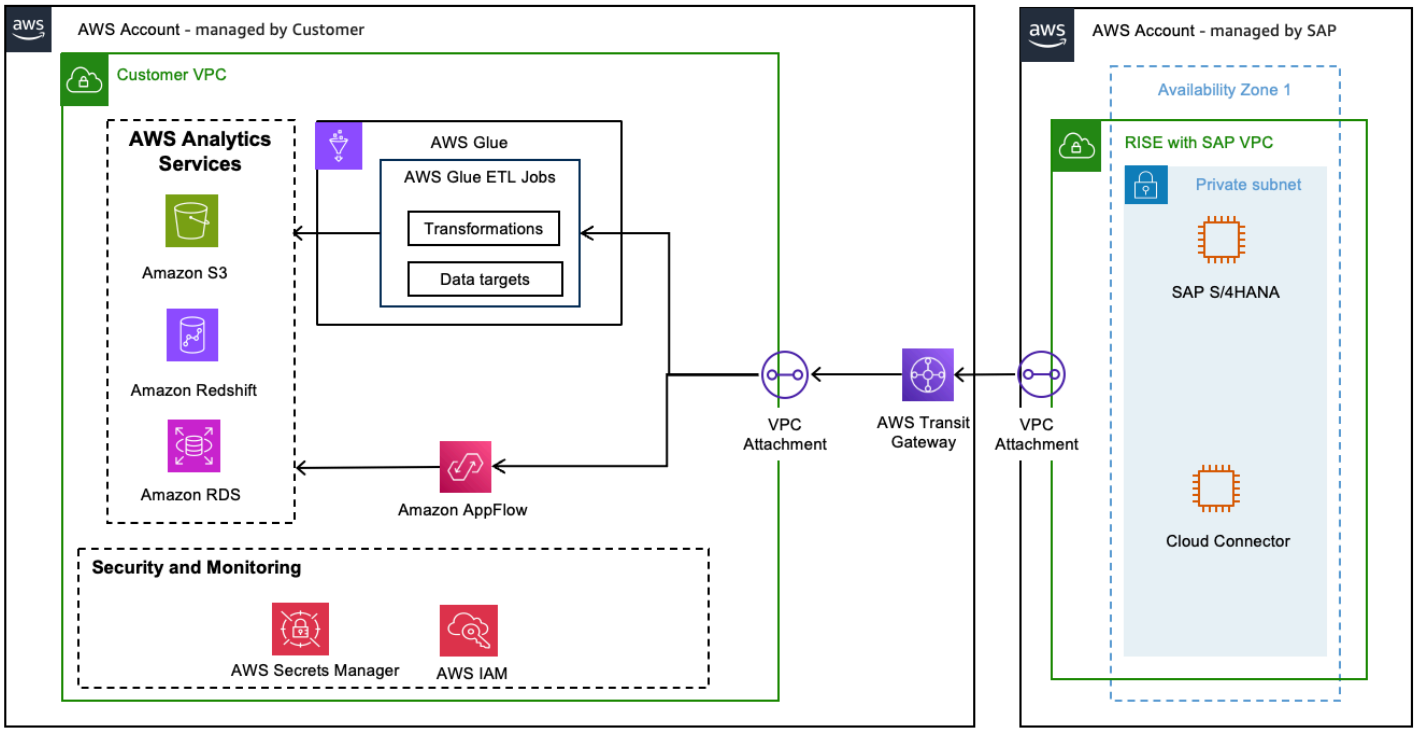
1. 数据提取
2. 数据联合

数据提取

从 SAP 提取数据是使数据可用于报告、分析和与其他系统集成的关键步骤。



使用 AWS Managed Services 从 SAP 提取数据



Amazon AppFlow

AppFlowA mazon SAP OData 连接器提供了通过获取、创建和更新 SAP S/4HANA 和 SAP 本地系统公开的记录的功能。 OData APIs当您将 Amazon 连接 AppFlow 到 ODP 提供商时，您可以创建运行完整数据传输或增量更新的流程。ODP 数据的增量更新非常有效，因为它们只传输自上一次流程运行以来更改过的记录。

适用于 Amazon 的 SAP OData 连接器 AppFlow用户指南提供了详细的设置说明 AppFlow，涵盖了从建立连接到从 SAP 传输数据的所有内容。

AWS Glue

AWS G lue 是一项无服务器数据集成服务，可让分析用户轻松发现、准备、移动和整合来自多个来源的数据。借 AWS 助 Glue，您可以在集中式数据目录中使用 OData 和管理您的数据，发现并连接到 SAP。您可以直观地创建、运行和监控提取、转换和加载 (ETL) 管道，将 SAP 数据加载到数据湖和数据仓库中。

OData 使用 Glue 连接到 SAP 用户指南提供了有关设置 Glue ETL 作业、配置 SAP OData 连接和从 SAP 读取数据（包括处理增量传输）的全面说明。注意：Amazon AppFlow 与 SAP 版 AWS Glue 的主要区别 OData

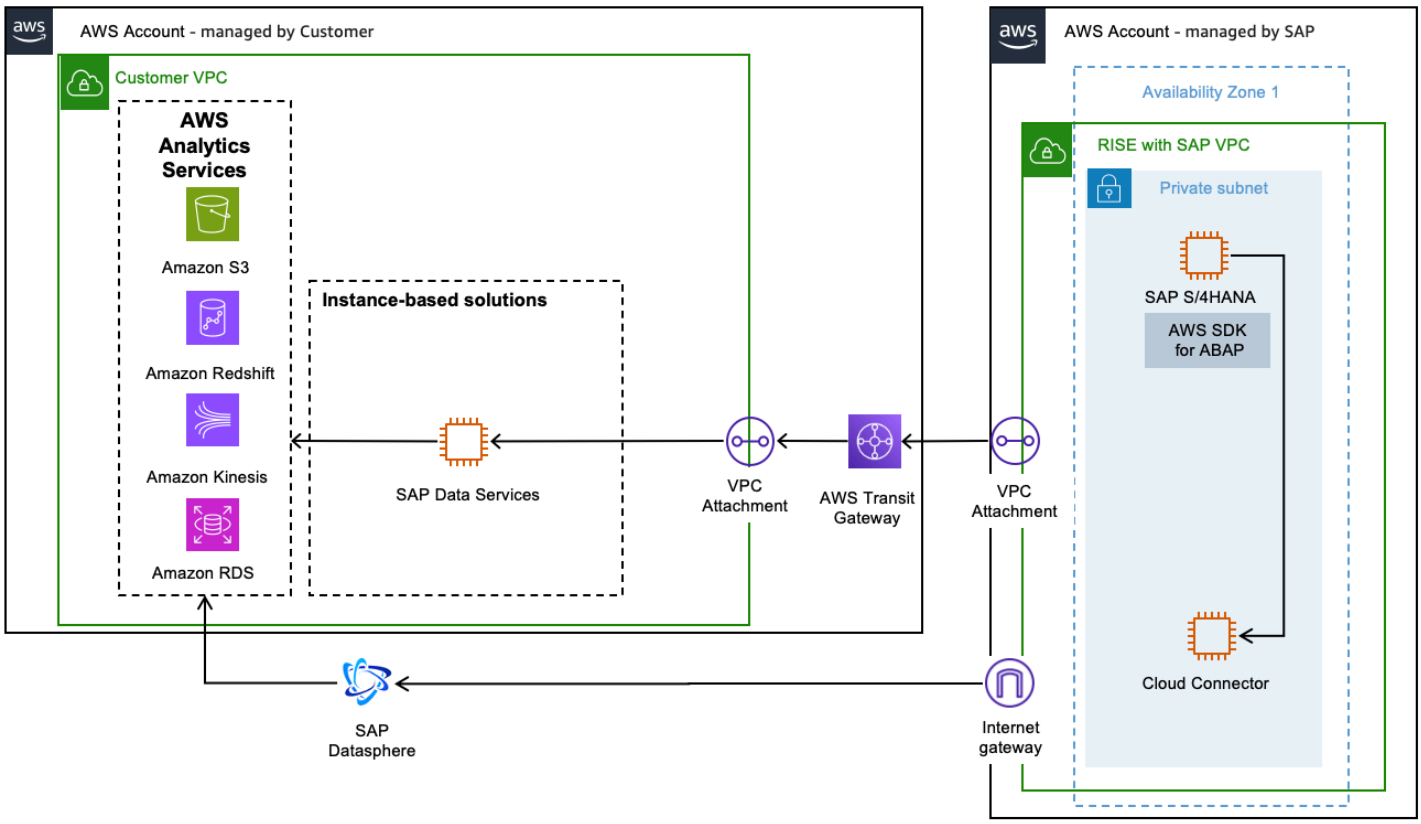
Amazon AppFlow AWS 和 Glue 在数据集成中扮演着不同的角色，每种角色都为不同的用例提供了独特的优势。而 AWS Glue 在复杂的 ETL 操作、数据发现、准备和提取方面表现出色，尤其适用于基于 SAP ODP 的提取等特殊场景。 AppFlow 旨在为基于 API 的数据传输提供更简化的无代码解决方案。

AWS Glue 需要更多的动手管理，包括代码部署和维护，但它为数据转换过程提供了更大的灵活性和控制力。相比之下， AppFlow 它提供了一个用户友好的 point-and-click界面，其中包含适用于常用 SaaS 应用程序的预建连接器，无需复杂的 API 实现即可实现双向数据传输。

AWS 适用于 ABAP 的 SDK

AWS 适用于 ABAP 的 SDK 通过与 ABAP 开发人员一致且熟悉的模块的客户端库简化了 AWS 服务与 SAP 应用程序的使用。凭借其通过 ABAP 代码使用 AWS 服务的功能，它允许您构建 ETL 数据管道，并从 SAP ABAP Stack 复制到 S3 存储桶、Redshifts 等 AWS 目的地。

使用 SAP Datasphere 和 SAP 数据服务等 SAP 服务从 SAP 提取数据



SAP 数据圈

SAP Datasphere 提供各种连接类型，例如 SAP ABAP 连接、SAP ECC 连接、支持 RFC 和 ODP 协议的 SAP S/4HANA 云连接。请参阅 SAP Datasphere 文档，选择最合适的连接来提取 SAP 数据。使

用 [亚马逊简单存储连接 (Amazon S3)] 的高级出站集成，配置 SAP Datasphere 复制流程以将数据提取到亚马逊 S3。

SAP 数据服务

SAP 数据服务提供各种连接，用于从 SAP ECC 数据中提取数据。请参阅 S AP 数据服务文档，选择最合适的连接。SAP 数据服务提供亚马逊 Redshift Datastore 和 Amazon S3 数据存储以接收数据。AWS它还提供了 Amazon S3 文件定位协议的选项，例如加密类型、压缩类型、批处理大小、线程数、Amazon S3 存储类别等。

使用 AWS 合作伙伴解决方案从 SAP 提取数据

AWS Partner Solutions 提供具有增强功能的即用型解决方案，例如预先构建的连接器、专门的数据管道和高级优化技术，可降低复杂性并提高部署速度。

要查找和部署符合你特定需求的解决方案，你可以浏览Partner S olutions Finder 或浏览 AWS Marketplace，在那里你可以搜索并快速部署针对你的独特 SAP 用例量身定制的合作伙伴解决方案。AWS

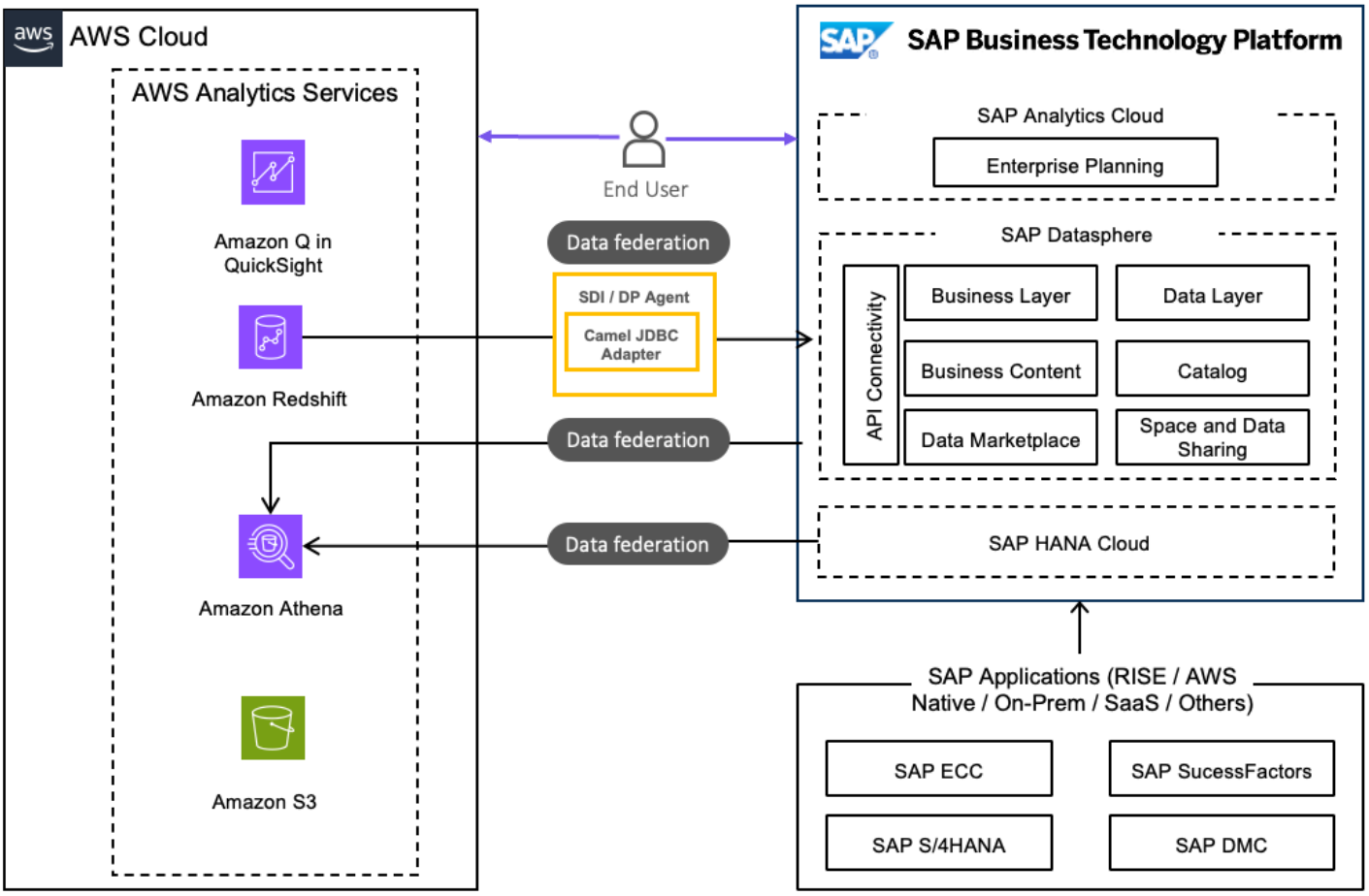
更多资源

《SAP 数据集成与管理指南》 AWS为构建数据和分析解决方案提供了基本的数据基础。它展示了如何使用 AWS 服务、SAP 产品和 AWS 合作伙伴解决方案， AWS 以实时或批处理模式将来自 SAP ERP 源系统的数据与变更数据捕获进行集成。本指南包括一个概述的参考架构，展示了如何将 SAP 系统引入，此外还有五种详细的架构模式，这些模式使用上面重点介绍的 AWS 服务 OData、SAP 产品和合作伙伴解决方案来补充 SAP 支持的机制（例如 ODP、SLT 和 BTP）。 AWS AWS

数据联合

数据联合是一种数据管理策略，可实现来自不同数据源的数据的无缝集成和有效利用。当业务需要整合数据用于交易、分析、机器学习时，最好从源头访问数据，而不是复制数据，以避免延迟、不一致和额外的存储成本。

在 SAP 和 AWS 服务的背景下，它允许组织无缝访问、合并和分析来自 SAP 系统和 AWS 云服务的数据。



使用 Managed Services AWS 进行数据联合

Amazon Athena

Amazon Athena 是一项无服务器、可扩展且灵活的交互式查询服务 AWS ，允许直接在 Amazon S3 中分析数据。可以使用 Amazon Athena 将存储在 Amazon S3 中的多个来源的数据进一步转换为表和视图，并进行查询，以结构化方式提取有意义的信息。

Athena 中的数据可以通过来自 SAP Datasphere 连接的数据联合从 SAP Datasphere 中访问。用户还可以使用 Athena 联合查询查询 SAP HANA，从 Athena 访问 SAP Datasphere 表和视图。

也可以使用智能数据访问 — Athena 适配器将 Athena 配置为远程源，从而将数据联合到 SAP HANA 云。Athena Federated Query 连接还可用于从独立的 SAP HANA 云环境中读取数据。

Amazon Redshift

Amazon Redshift 是一项完全托管的、千万亿字节规模的数据仓库服务。 AWS客户已经建立了自己的数据仓库并建立了用于分析和报告的数据模型。

使用 SAP HANA 智能@@ 数据集成 (SDI) 或 SAP 数据配置代理，可以将数据从 Amazon Redshift 到 SAP Datasphere 进行数据联合。Amazon Redshift 数据也可以通过 Athena 联合查询数据源连接器进行联合。

更多资源

SAP 之间的数据联合指南 AWS 概述了 SAP 和 AWS 云分析服务之间联合数据的过程，使您能够建立数据网格架构。通过在 SAP 和 AWS. 之间联合数据，你可以轻松地以可扩展、安全且经济实惠的方式转换和可视化数据，从而为决策提供依据。

数据分析

SAP 客户需要实时的业务见解，以应对业务变化并利用尚未开发的商机。这需要通过现代的云原生解决方案来实现，才能从隔夜数据处理转向实时分析。利用 AWS 和 SAP 解决方案来构建分析解决方案，客户可以利用专为目的构建的分析服务在各自的行业中获得竞争优势。

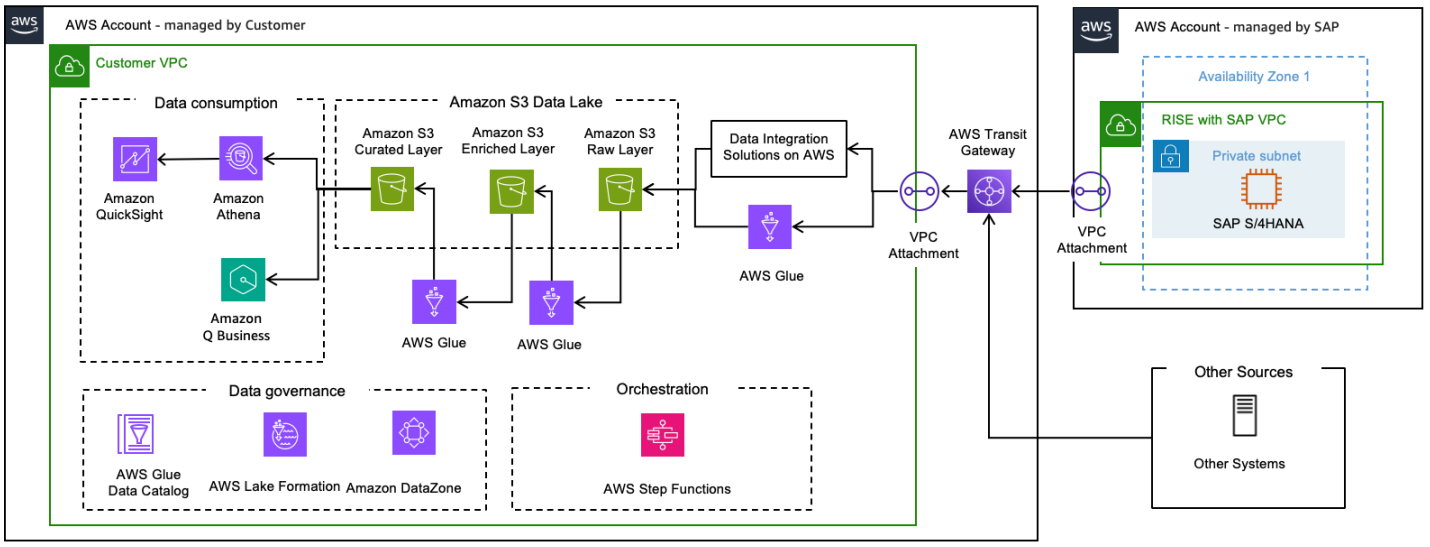
数据湖和数据仓库等现代数据架构提供了模式和服务的组合，使组织能够处理大量结构化和非结构化数据以进行分析和报告，也为人工智能 (AI) 和Machine Learning (ML) 应用程序（包括生成式人工智能）提供了坚实的基础。这些架构提供了可以独立实现的构建块，也可以根据需求和偏好相互补充。

数据湖架构

数据湖架构提供了构建块，用于演示如何使用分析和机器学习服务，合并和整合来自不同来源的 SAP 和非 SAP 数据。 AWS

数据湖使客户能够处理结构化和非结构化数据。它们是基于 “schema-on-read” 方法设计的，这意味着数据可以以原始形式存储，并且仅在使用时应用架构或结构（即：创建财务报告）。结构是在从源读取数据时定义的，当时定义了数据类型和长度。因此，存储和计算是分离的，利用低成本存储，与传统数据库相比，这种存储可以扩展到PB级大小，而成本却很小。

数据湖使组织能够执行各种分析任务，例如创建交互式仪表板、生成可视化见解、处理大规模数据、进行实时分析以及跨不同数据源实施机器学习算法。



Data Lake 参考架构提供了三个不同的层，可将原始数据转化为有价值的见解：

原始图层

原始层是基于 Amazon S3 构建的数据湖中的初始层，数据直接从源系统以原始格式到达，无需进行任何转换。该层中的数据用于确定要在下一层中合并的更改和数据，因为它将包含相同数据的多个版本（更改、满载等）。

从 SAP 提取的数据（通过 SAP ODP OData 或其他机制）需要做好进一步处理的准备。提取的数据将被打包成多个文件（由提取工具中的包或页面大小定义），因此可以为给定的提取运行生成多个文件。

丰富图层

丰富层基于 Amazon S3 构建，它包含源 SAP 系统中数据的真实表示以及逻辑删除内容，并以 Iceberg 格式存储。Iceberg Table 文件格式允许在 Glue 数据目录中创建 G lue 或 Athena 表，支持插入、更新和删除等数据库类型操作，Iceberg 文件格式处理文件操作（删除记录等）。冰山表还支持时空旅行的概念，该概念允许查询特定时间点的数据。

来自原始图层的数据将根据表键以正确的顺序插入或更新到富集图层中，并以其原始格式保存（不进行转换或更改）。每条记录都需要添加某些属性，例如提取时间和记录编号，这可以通过Glue 作业AWS 来实现。

精选图层

策划层是存储数据以供数据使用的图层。在源上删除的记录会被物理删除。任何计算（平均值、日期间隔时间等）或数据操作（格式更改、从另一个表中查找）都可以存储在此层中，随时可以使用。使

用 AWS Glue 作业更新此层中的数据。Amazon Athena 视图是在这些表的基础上创建的，供下游通过 QuickSight 亚马逊或类似工具使用。

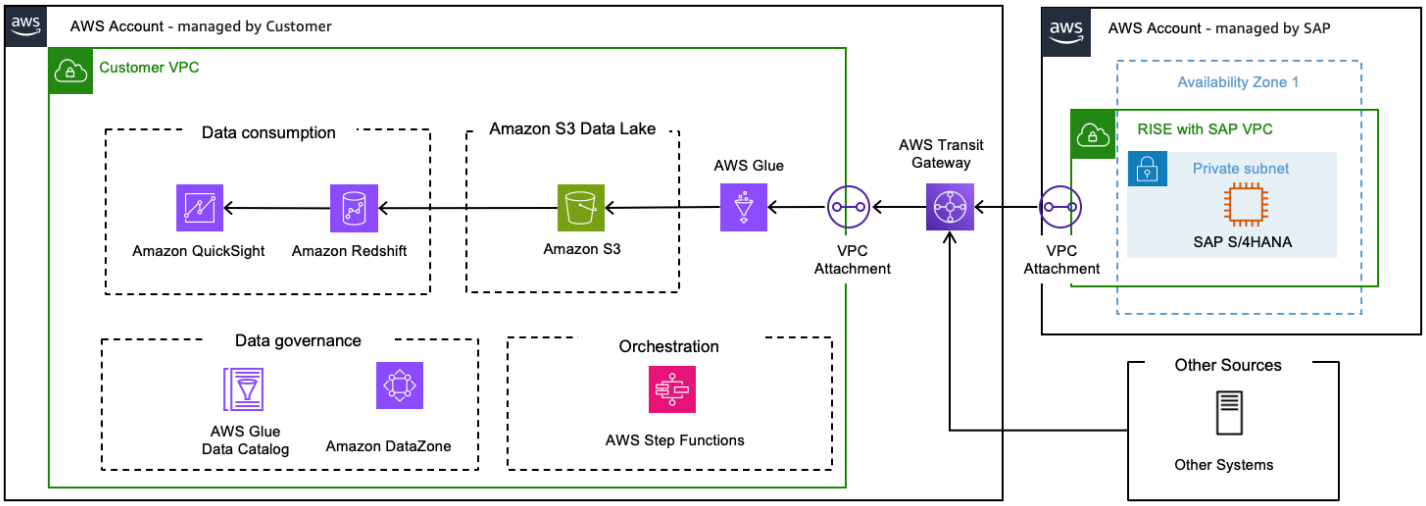
《包含 SAP 和非 SAP 数据的数据湖 AWS 解决方案指南》提供了详细的架构、实施步骤以及用于快速跟踪 SAP 和非 SAP 数据数据湖实施的加速器。在前面的 “数据集成” 一节中，您可以参考将数据从 SAP 提取到数据湖的不同可用选项。

数据仓库架构

数据仓库是基于 “schema-on-write” 方法的集中式存储库，它汇总来自多个来源（SAP 和非 SAP）的结构化历史数据，以实现高级分析、报告和商业智能 (BI)。它使组织能够使用经过优化的架构来处理复杂的查询，而不是事务处理，从而分析大量的集成数据，从而做出明智的决策。

业务分析师、数据工程师、数据科学家和决策者利用商业智能 (BI) 工具、SQL 客户端和其他分析应用程序访问数据仓库。该架构包括多个层：用于呈现结果的前端客户端、用于数据访问和分析的分析引擎以及用于数据加载和存储的数据库服务器。

数据存储在数据库中的表和列中，按架构组织。数据仓库整合来自多个来源的数据，支持历史数据分析并确保数据质量、一致性和准确性。将分析处理与事务数据库分开可以增强两个系统的性能，通过高效存储数据来支持报告、仪表板和分析工具，从而最大限度地减少 I/O 查询结果并将其快速提供给大量并发用户。



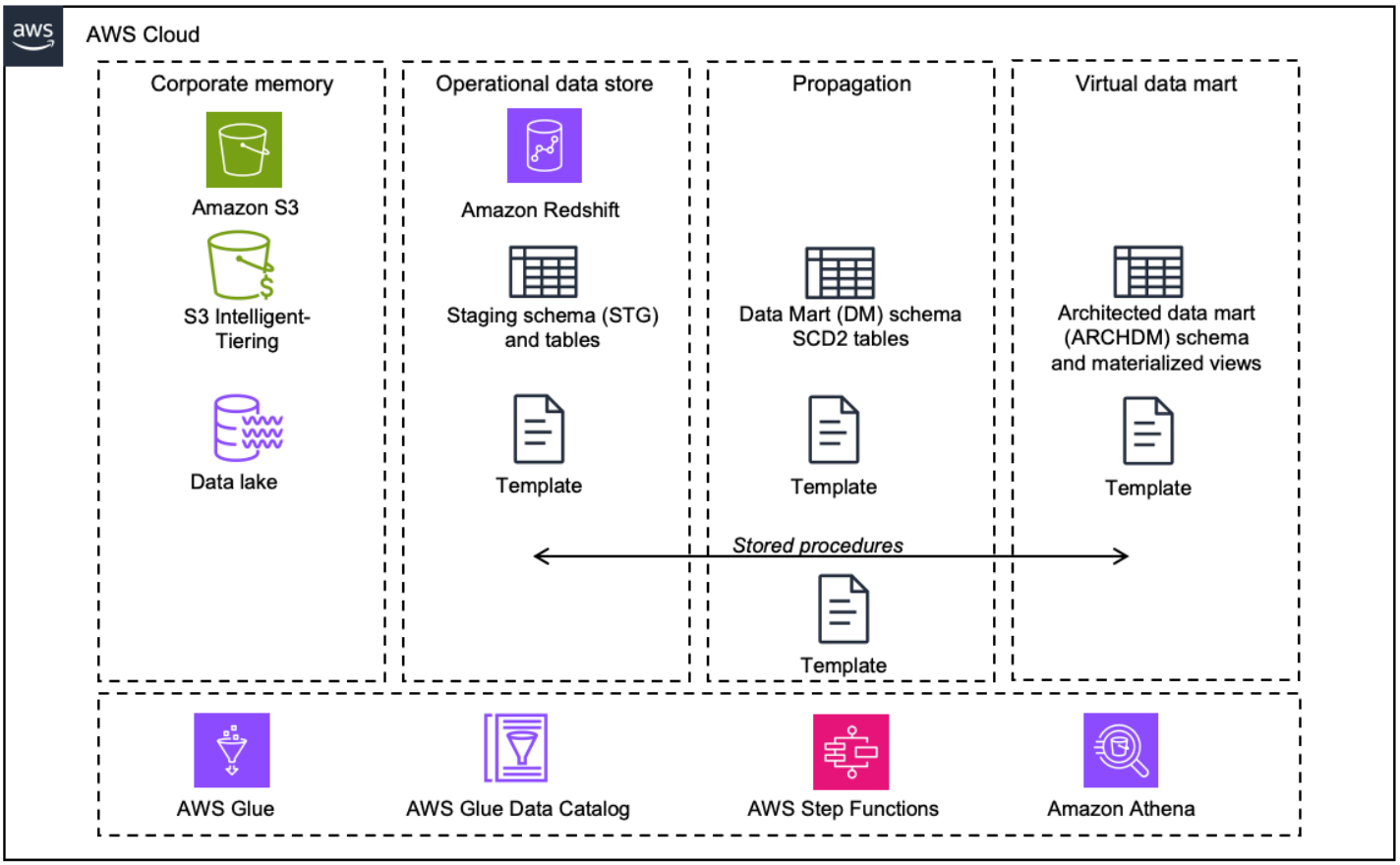
主要特征

- 集成：将来自不同来源（例如 CRM、ERP）的数据整合到一个统一的架构中，解决格式或命名惯例中的不一致问题。
- 时变：跟踪历史数据，允许对数月或数年的趋势进行分析。
- 以主题为导向：围绕销售或库存等业务领域而不是运营流程进行组织。

- 非易失性：数据存储后保持静态；更新是通过预定的提取、转换、加载 (ETL) 过程进行的，而不是通过实时更改进行的。

架构组件

- ETL 工具：自动从源中提取数据、进行转换（清理和标准化）以及加载到仓库。
- 存储层：
  - 结构化数据的关系数据库
  - 用于多维分析的 OLAP（在线分析处理）立方体
- 元数据：描述数据来源、转换和关系。
- 访问工具：SQL 客户端、BI 平台和机器学习接口。



数据仓库利用分层架构来组织不同粒度级别的数据，这有助于确保一致性和灵活性。最常见的数据仓库架构层是源层、暂存层、仓库层和消费层。SAP 系统还采用基于层的数据仓库架构。在构建 SAP 云数据仓库的背景下 AWS。该架构涉及用于数据采集、存储、转换和消费的几个关键层和组件。

企业记忆

Amazon S3 Intelligent-Tiering 是一种存储类，它根据不断变化的访问模式在访问层之间移动数据，从而自动优化存储成本。这样可以确保经常访问的数据随时可用，而访问频率较低或 “较冷” 的数据则存储在较低的成本层。

操作数据存储层

Amazon Redshift 用于运营数据存储、传播和数据集市功能。提供了用于创建架构和部署数据定义语言 (DDL) 的脚本，其中包含加载 SAP 源数据所需的结构。 DDLs 可以对其进行自定义，使其包含特定于 SAP 的字段。

数据传播层

通过 Glue/flows 加载到 S3 中的增 AppFlow 量数据用于生成缓慢变化的维度类型 2 (SCD2) 表，这些表保留了完整的更改历史记录。

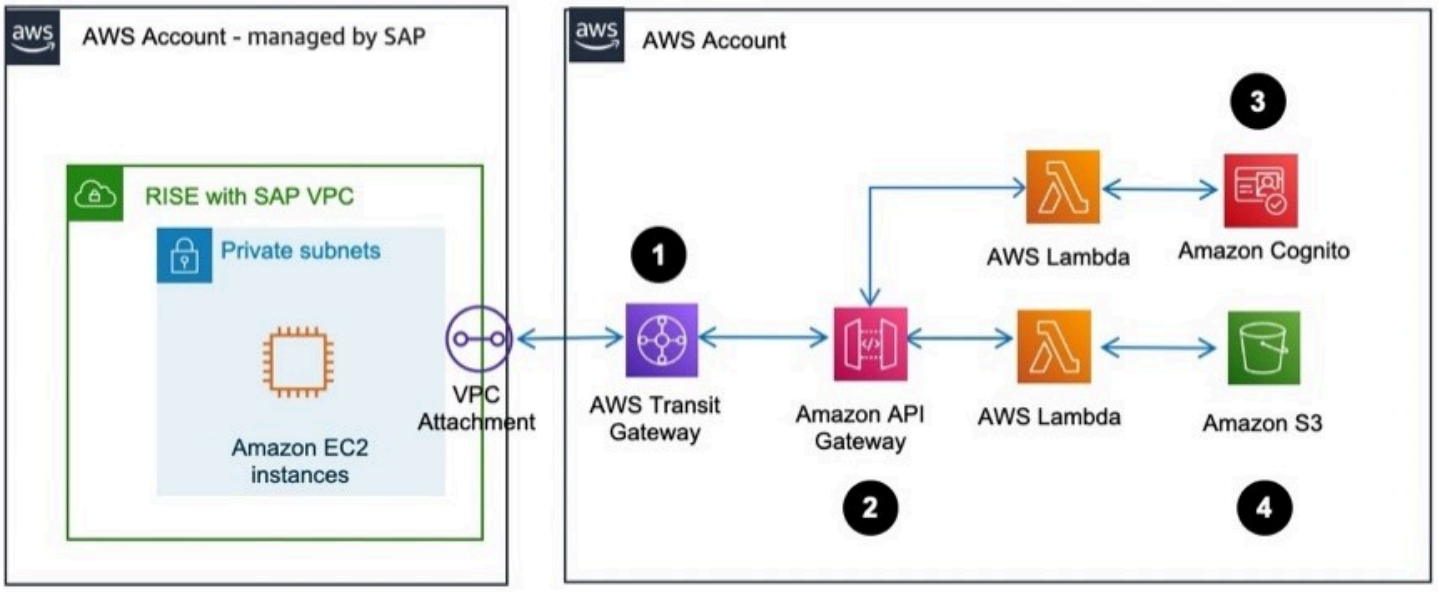
数据集市层

架构数据集市模型是使用 Redshift 中的物化视图创建的。交易数据中充斥着主数据（属性和文本），从而构建可供数据使用的数据模型。

《在 AWS 解决方案基础上构建 SAP 数据仓库指南》提供了详细的架构、实施步骤以及快速跟踪 SAP 数据仓库实施的加速措施。

应用程序集成

部署 Amazon API Gatew ay，通过 HTTP API 从 SAP S/4HANA 中提取数据。API Gateway 可以使用来自 IDOC、BAPI 和 RFC 的数据。这些需要转换为 Web 服务调用。有关更多信息，请参阅AWS 博客。下图显示了这种情况。



数据流

1. 带有 SAP VPC 的 RISE 通过 Tr AWS ansit Gateway 连接到你不由 SAP 管理的 AWS 账户。
2. Amazon API Gateway 配置为将身份验证路由到 AWS Lambda 和 Amazon Cognito
3. Amazon Cognito 会对会话进行身份验证。
4. 经过身份验证后，Amazon API Gateway 会将包裹路由到 AWS Lambda。
5. AWS Lambda 将数据存储在亚马逊 S3 存储桶中。

存档和文档管理

无论是在与 SAP 一起迁移到 RISE 之前还是之后，SAP 数据存档和文档管理系统 (DMS) 都起着至关重要的作用。它可以帮助企业有效地管理数据库增长并优化总体成本。在迁移到 S/4HANA 之前，归档可以减少迁移费用，最大限度地减少停机时间，并通过减少数据量来降低风险。迁移到 S/4HANA 后，它有助于控制运营成本并确保最佳系统性能。此外，企业可以停用传统的 SAP ECC 系统，从而消除不必要的开支，同时保留对历史数据的访问权限

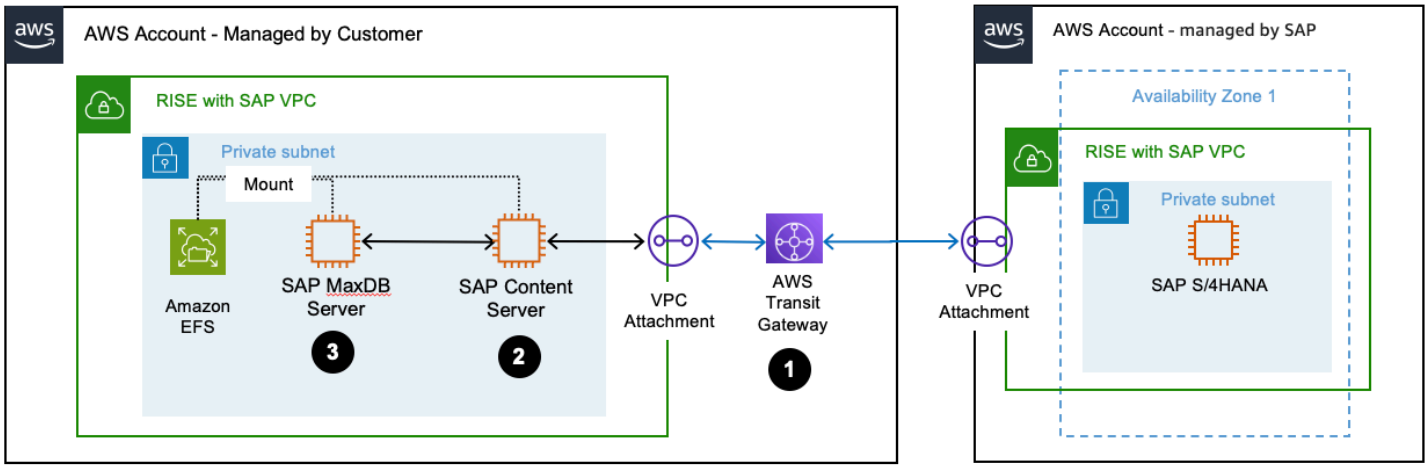
结构化数据的数据存档。数据存档是指将已完成的业务交易数据从实时 SAP 系统移动到离线或辅助存储。数据存档的关键方面是制定流程和策略，以减少手动工作，同时确保遵守法律数据保留要求。

非结构化数据的文档管理。数据存档和文档存档的区别在于您要存档的数据类型。文档存档涉及非结构化数据，例如发票、销售订单、交货单等，这些数据通常采用 pdf、words、excels 等格式。这种存档是实时进行的，可以存储在任何内容服务器上并链接到相关的 SAP 事务。

我们将讨论您在 SAP 中的数据存档和文档管理系统的可用选项。

选项 1：在 MaxDB 上运行的 SAP 内容服务器

许多通过 SAP 迁移到 RISE 的客户选择在过渡到 SAP BTP 文档管理系统或OpenText 存档解决方案 AWS之前保持其 SAP 内容服务器开启状态。SAP Content Server 是一个独立组件，旨在存储大量不同格式的电子文档。这些文档可以安全地保存在一个或多个 SAP MaxDB 实例中或文件系统中。存储在 SAP Content Server 中的常见文档示例包括销售发票、采购订单、工资单、电子邮件、协议等。这种方法可确保将文档管理无缝集成到 SAP 业务流程中，同时保持可访问性和合规性。

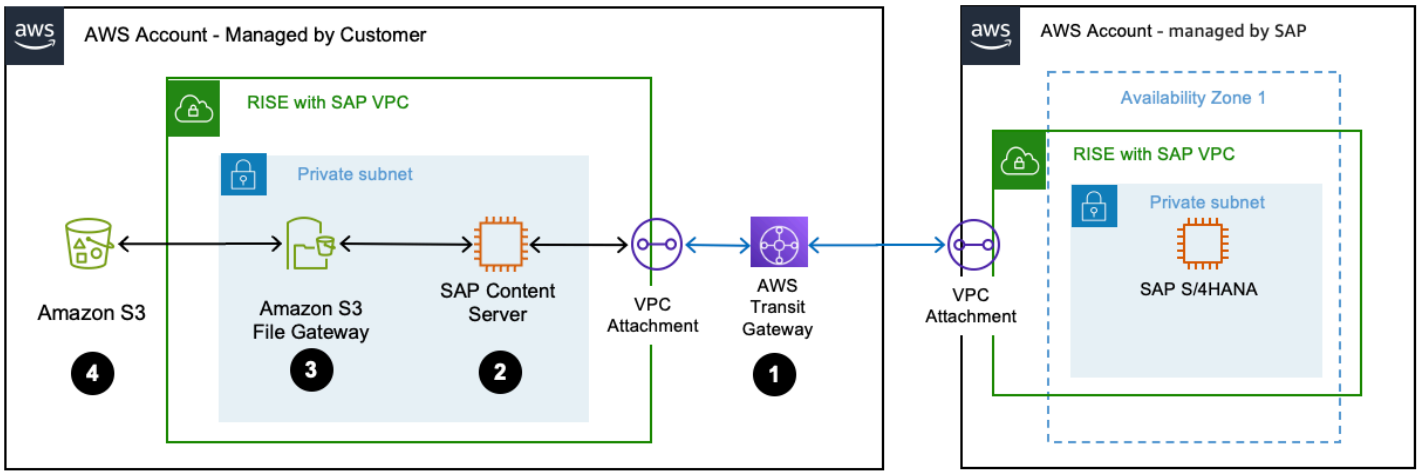


架构描述

1. 带有 SAP VPC 的 RISE 与你通过 AWS Transit Gateway 管理的 AWS 账户相关联。
2. SAP Content Server 已在您的 AWS 帐户中设置，并配置为用作数据存档的目的地。
3. SAP MaxDB 已在您的 AWS 账户中设置并配置为在 AWS EC2 实例上运行。
4. 使用 Amazon EFS 的 SA@@ P 内容服务器实现高可用性。对于不经常访问的文档，可以考虑使用 EFS 不频繁访问。

选项 2：Amazon S3 上的 S AP 内容服务器 SAP 内容服务器和 A mazon S3 都可以通过为存档数据提供可扩展且安全的存储来满足 SAP 数据存档需求。它们提供版本控制、访问控制、不可变性以及与 SAP 系统的集成等功能。本节适用于正在经历 SAP 数据库增长、寻求性能改进、旨在降低存储成本或需要满足在 SAP 环境中长期保留数据的合规性要求的客户。

下图显示了与 Amazon S3 集成的 SAP 内容服务器。



架构描述

1. 带有 SAP VPC 的 RISE 与你通过 AWS Transit Gateway 管理的 AWS 账户相关联。
2. SAP Content Server 已在您的 AWS 帐户中设置，并配置为用作数据存档的目的地。
3. SAP 内容服务器与 A mazon S3 文件网关集成，后者充当存储网关，便于基于文件的存储。S3 文件网关允许将 Amazon S3 安装为网络文件系统 (NFS)。
4. Amazon S3 存储桶用于存储必要的存档文件。您可以使用 S3 生命周期配置来管理对象的生命周期。为了增强数据保护或监管合规性，您可以使用 S3 Object Lock 实施保留策略。您可以使用自动生命周期管理将文件移动到不同的 S3 存储类别。有关更多信息，请参阅使用 Amazon S3 存储类别。

SAP 内容服务器与 Amazon S3 配合使用，提供了一种将存档数据传输到长期 S3 存储（例如 Amazon S3 Glacier）的机制。然后，可以使用 SAP 的标准存档读取程序访问这些存档数据。

但是，如果您需要与 SAP 进行更广泛的集成，可以使用 Synta x 等第三方解决方案 CxLink 或OpenText提供其他库。它们增强了集成能力，为直接在 SAP 环境中管理和访问存档数据提供了更高级的功能。对于采用 SAP 信息生命周期管理 (ILM) 来管理数据保留和治理的组织，请参阅 Sy ntax Cxlink for ILM 如何通过使用 Amazon S3 作为 SAP ILM 的辅助存储解决方案来增强您的 ILM 战略。这种方法利用了云存储的可扩展性和成本效益，同时保持了 SAP ILM 强大的数据管理功能。

选项 3：RISE 中的 SAP OpenText 存档

SAP OpenText 存档正在为 RISE 和 SAP 提供安全的文档存储、合规性和经济高效的数据管理。SAP A OpenText rchiving 是一种基于云的文档管理和存档解决方案，它与 SAP 集成，用于存储、检索和管理非结构化内容（例如发票、合同、采购订单）。它可确保遵守监管要求，减少数据库占用空间，并优化 SAP S/4HANA 性能。在 RISE 和 SAP 中 OpenText ，作为可选组件包含在 RISE BOM 中。

选项 4：RISE 的 OpenText InfoArchive

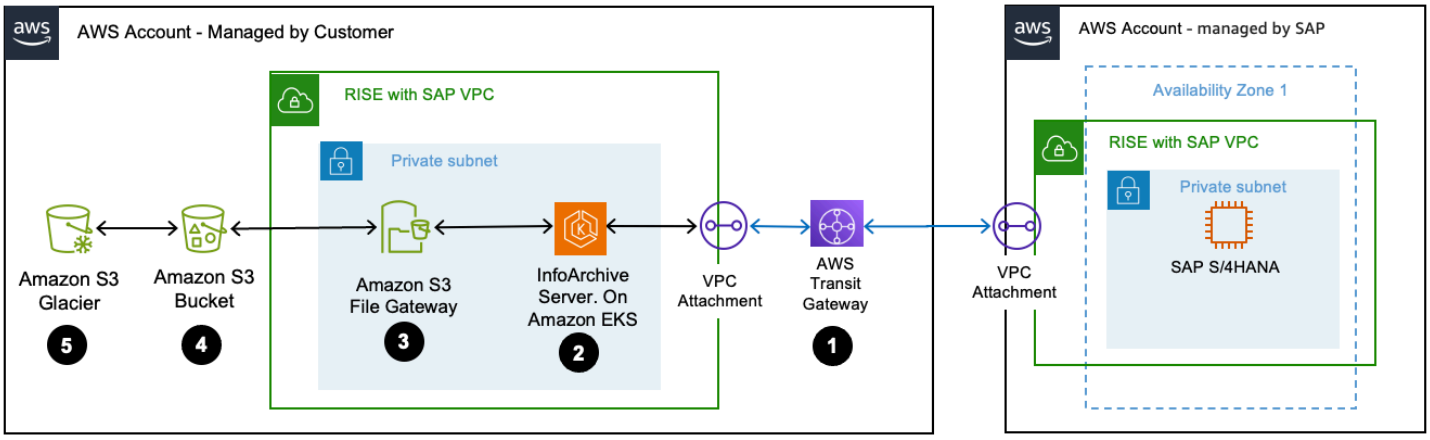
OpenText InfoArchive 是一种现代存档解决方案和基于云的服务，用于对结构化和非结构化信息进行合规存档，具有高度可访问性、可扩展性和经济性。它是一个集中式平台，可为非结构化内容提供灵活的存储选项，包括亚马逊简单存储服务 (Amazon S3) 上的存储。InfoArchive 上 AWS 的 Cloud Edition 以客户部署的形式提供，也可以在上 OpenText AWS运行作为托管解决方案提供。

OpenText InfoArchive 是一个通用存档平台，旨在淘汰传统的 SAP 应用程序并存储来自多个系统的结构化和非结构化数据。除此之外，它还支持 SAP ECC、CRM、HR 和特定行业的系统（医疗保健、银行等）OpenText InfoArchive 可用于归档非活动数据和停用已停用的 SAP 传统应用程序。它附带了预先构建的 SAP 视图。

主要功能

1. 应用程序停用-停用旧版应用程序，同时保持数据可访问性。
2. 结构化和非结构化数据存档-存储文档、电子邮件、记录和数据库。
3. MultiSystem Support — 可与 SAP、Oracle、Salesforce、微软和定制应用程序配合使用。
4. 高级搜索和分析- AI/ML 用于深入了解存档数据。
5. 监管合规 — HIPAA、GDPR、SEC 17a-4 等

您可以部署与 Amazon S3 集成的 OpenText InfoArchive 服务器，用于停用 SAP 数据。下图显示了这种使用 AWS 服务的场景。 OpenText InfoArchive on 部署在 AWS 亚马逊 Elastic Kubernetes Service (EKS) 上用于托管其 Web 应用程序、用于身份验证和授权的 Directory Ser v OpenText ice 以及服务器。 InfoArchive 客户也可以通过AWS 市场购买。



架构描述

1. 带有 SAP VPC 的 RISE 通过 Tr AWS ansit Gateway 连接到你的 AWS 账户。

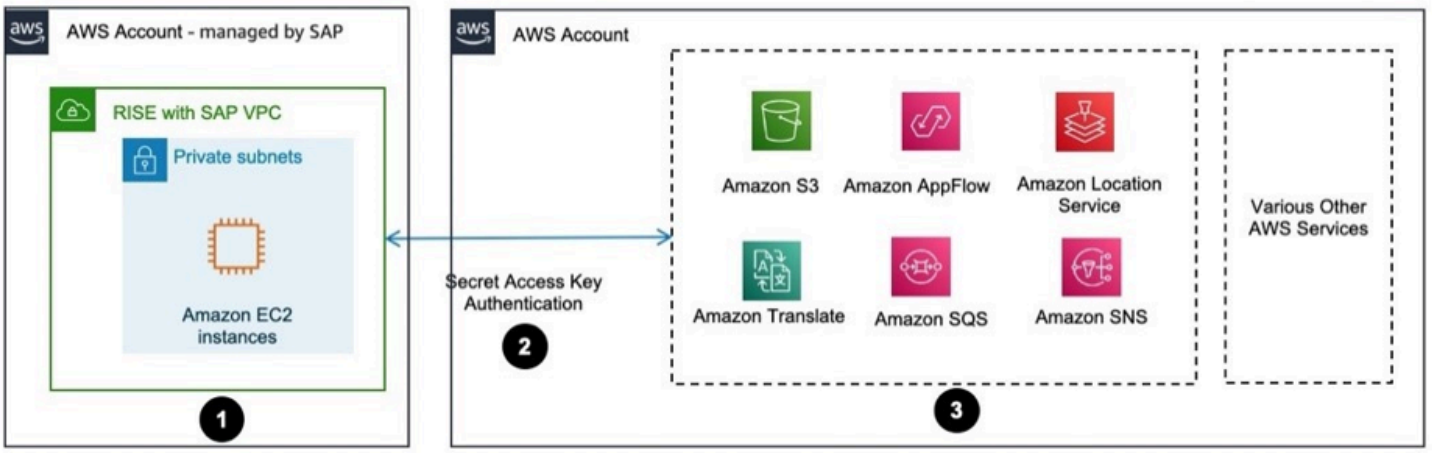
2. OpenText InfoArchive on 部署在 AWS 您的账户 AWS中的亚马逊 Elastic Kubernetes Service (Amazon EKS) 上，并配置为用作数据存档的目的地。
3. OpenText InfoArchive 与 Amazon S3 文件网关集成，后者充当存储网关，便于基于文件的存储。S3 文件网关允许将 Amazon S3 安装为网络文件系统 (NFS)。
4. Amazon S3 存储桶用于存储必要的存档文件。您可以使用 S3 生命周期配置来管理对象的生命周期。为了增强数据保护或监管合规性，您可以使用 S3 Object Lock 实施保留策略。
5. 可以将较旧的文档移至 Amazon S3 Glacier 进行长期存档。
6. 您可以使用自动生命周期管理将文件移动到不同的 Amazon S3 存储类别。有关更多信息，请参阅使用 Amazon S3 存储类别。

开发和扩展

AWS 适用于 SAP 的 SDK ABA

使用 SAP VPC 在 RISE 上部署 AWS 适用于 SAP ABAP 的 SDK，以便使用 ABAP 语言使用 AWS 服务。有关更多信息，请参阅什么是 AWS 适用于 SAP ABAP 的 SDK？

您可以使用 IAM 访问密钥对 AWS 适用于 SAP ABAP 的软件开发工具包进行身份验证。下图显示了这种情况。



数据流

1. AWS 适用于 SAP ABAP 的 SDK 是通过 SAP VPC 的 RISE 中的 SAP S/4HANA 中的一组传输安装的。
2. SAP S/4HANA 配置了 IAM 访问密钥，用于对服务访问进行身份验证。 AWS 有关更多信息，请参阅管理 IAM 用户的访问密钥。

3. 已经建立了使用适用于 SAP ABAP 的 S AWS DK 访问 AWS 服务的权限。

兼容包和替代品

兼容包 (CP) 是 2016 年创建的 S/4HANA 中经典功能的临时使用权。它是 SAP S/4HANA 每份合同的一部分，无论是本地部署还是私有云。这是为了让 SAP 的客户实现平稳过渡，并争取时间完成新的简化应用程序架构。

在从SAP Business Suite过渡到S/4HANA的过程中，业务职能在此过程中经历了这些路径。你可以从迈克尔·戴勒（SAP）和罗兰·哈姆（SAP）的演讲中了解更多信息。

在 SAP Note 2269324 中，SAP 定义了类别，以帮助组织规划其兼容包策略。这些类别指导从SAP商务套件过渡到SAP S/4HANA的决策。

- 存在替代方案
- 路线图中存在替代方案-存在提供核心功能的替代方案；路线图上有全面的覆盖范围
- 备选计划——开发范围和时间表的规划正在进行中
- 没有替代计划——没有意图或计划在 2025 年之后提供替代方案
- 澄清-正在澄清战略

如何 AWS 帮助客户寻找替代品？

Organizations 应评估其当前的 SAP 格局，并考虑到 SAP 兼容包的到期日期和可用的替代方案，规划过渡策略。当兼容包缺少替代方案时，你可以利用组合服务 AWS 和 SAP 服务。这种方法与AWS 重构和重新架构迁移策略一致，后者侧重于重新构想应用程序和流程。以下是细节

- SAP 和 AWS 联合参考架构的开发旨在解决共同客户和合作伙伴提出的关于如何将 SAP BTP 和/或 AWS 服务用于不同业务解决方案场景的常见问题。有关更多详细信息，另请参阅此博客。
- 适用@@ 于 SAP ABAP 的 S AWS DK 通过与 ABAP 开发人员一致且熟悉的模块的客户端库简化了 200 多种 AWS 服务以及 SAP 应用程序的使用。
- M AWS arketplace 上的 SAP 产品和 AWS 合作伙伴解决方案
- 如有必要，您可以联系我们的 SAP AWS 专家团队为您提供指导。

在 SAP Note 2269324（参见 S4HANA CompScope — Way Forward — Info — 06032025.xlsx）中，“SAP 税收分类和报告” 被标记为 “没有替代方案”，在这种情况下，你可以在 Marketplace 上探索汤森路透间接 ONESource 税确定等替代方案。 AWS

安全扩展

mTLS 身份验证

相互传输层安全 (mTLS) 身份验证在客户端和服务器之间建立安全的双向加密连接。与只有服务器提供证书的标准 TLS 不同，mTLS 要求双方出示数字证书。

mTLS身份验证过程分为四个步骤:. 客户端请求与服务器建立连接。服务器出示其证书。客户端验证服务器的证书。客户端出示其证书以进行服务器验证和身份验证

为什么 SAP 需要使用 mTLS 身份验证

对 SAP 系统实施双向 TLS (mTLS) 身份验证将增强安全性、改善用户体验并减少运营开销。它将对用户身份验证基础架构进行现代化改造，以支持数字化转型，同时确保符合安全标准。mTLS 可满足 SAP 环境中的以下安全要求：

1. 增强的安全性：mTLS 提供双向身份验证，确保客户端和服务器都验证彼此的身份。这大大降低了未经授权的访问和 man-in-the-middle攻击的风险。
2. 通过单点登录 (SSO) 实现无缝用户体验：mTLS 可以与 SSO 解决方案集成，使用户无需重复输入凭据即可访问多个 SAP 应用程序和服务。这为整个 SAP 生态系统创造了更流畅、更高效的用户体验。
3. 自动证书轮换：mTLS 允许自动轮换证书，无需人工干预即可定期更新身份验证凭据，从而增强安全性。这降低了使用过期或已泄露证书的风险，并最大限度地减少了管理开销。
4. 接口的主体传播：mTLS 支持在不同的 SAP 接口和系统之间进行安全的主体传播。这样就无需使用通用帐户和特权帐户（例如具有 SAP_ALL 授权的 SAP 用户）进行 system-to-system通信，从而显著提高了安全性和可审计性。
5. 可扩展性和性能：可以在网络层面实现 mTLS，将身份验证过程从应用程序服务器上卸载。这可以提高 SAP 系统的性能和可扩展性。
6. 对零信任架构的支持：mTLS 与零信任安全模型非常吻合，在零信任安全模型中，从不假设信任，并且始终经过验证。

使用 Application Load Balancer 进行客户端身份验证

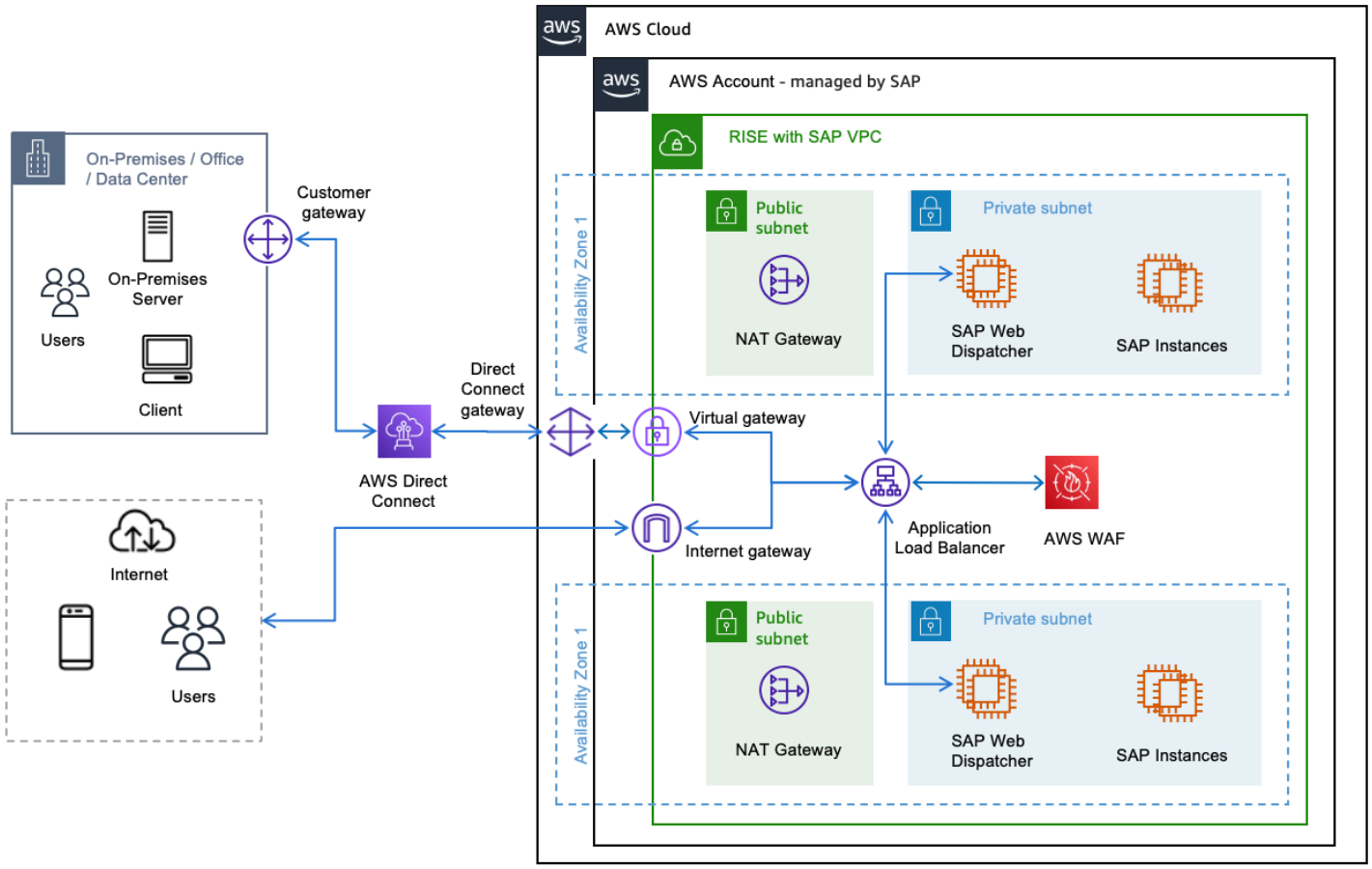
Application Load Balancer (ALB) 支持 mTLS 身份验证。它提供两种模式：验证和直通模式。

先决条件

为了确保无缝通信，在基础架构中使用的所有 SSL（安全套接字层）或 TLS 证书，包括 ALB、SAP Web Dispatcher 和 S/4HANA 系统的证书，都应来自一个可信的根证书颁发机构，以简化这些证书的实施和维护。

mTLS 架构图

下图描述了一个基本的 SAP AWS 架构，该架构经过调整以与 RISE 和 SAP SKU 产品保持一致。



mTLS 验证模式

要启用 mTLS 验证模式，请创建包含 CA 证书捆绑包的信任存储。这可以通过使用 Certif AWS icate Manager (ACM)、 AWS 私有 CA 或通过导入自己的证书来完成。使用存储在 Amazon S3 中并链接到信任存储库的证书吊销列表 (CRLs) 管理已吊销的证书。

ALB 根据信任存储库处理客户端证书验证，从而有效地阻止未经授权的请求。这种方法将mTLS处理从后端目标上卸载，从而提高了系统的整体效率。ALB CRLs 从 S3 导入并执行检查，无需重复提取 S3，从而最大限度地减少了延迟。

除了客户端身份验证之外，ALB 还通过 HTTP 标头（例如 X-Amzn-Mtls-Clientcert-Leaf）将客户端证书元数据通过 HTTP 标头传输到后端 SAP Web Dispatcher。这允许根据证书详细信息在后端目标上实现额外的逻辑，以满足 SAP 服务器保留原始 “主机标头” 信息的要求。

这使服务器能够一致地处理客户端证书元数据，即使这些元数据来自非 SAP 来源，例如终止 SSL 连接的 AWS 负载平衡器。如果您通过 ALB（SAP Web Dispatcher — SAP 服务器）实施 end-to-end加密，则必须配置 SAP Web Dispatcher 配置文件参数，例如 _certific icm/HTTPS/clientate_header_name，有关更多详细信息，请参阅此链接。

mTLS 直通模式

在 mTLS 直通模式下，ALB 会将客户端的整个证书链转发到后端目标。这是通过名为的 HTTP 标头完成 X-Amzn-Mtls-Clientcert的。链条（包括树叶证书）以 URL 编码的 PEM 格式发送，+、= 和/作为安全字符。以下是使用 mTLS 直通模式时的注意事项：

- 如果缺少客户端证书，ALB 不会添加任何标头；后端必须处理这个问题。
- 后端目标负责客户端身份验证和错误处理。
- 对于 HTTPS 侦听器，ALB 会终止客户端 ALB TLS，并使用目标安装的证书启动新的 ALB 后端 TLS。
- ALB 的 TLS 终止允许使用任何 ALB 路由算法进行负载平衡。

NLB 直通

如果您有严格的安全合规规则要求服务器端终止客户端 TLS 连接，则可以使用 N etwork Load Balancer (NLB)。

需要注意的要点：

1. NLB 在传输层（OSI 模型的第 4 层）运行。
2. 它为 TCP/UDP 连接提供低延迟的负载平衡。
3. NLB 允许后端服务器处理 TLS 终止，这对于某些安全合规性场景可能至关重要。

这种方法可确保敏感的解密过程发生在您受控的服务器环境中，从而有可能满足特定的安全要求，同时保持高效的流量分配。

mTLS 验证模式与 mTLS 直通模式与 NLB 直通模式的比较。

注意事项	带有 mTLS 的 ALB 验证模式	带有 mTLS 直通模式的 ALB	NLB
OSI 层	第 7 层（应用程序）	第 7 层（应用程序）	第 4 层（传输）
与 AWS WAF 集成	支持	支持	不支持
客户端身份验证	由 ALB 完成（AWS 托管）	由后端完成（客户管理）	由后端完成（客户管理）
SSL/TLS 终止客户端	在 ALB（AWS 托管）	在 ALB（AWS 托管）	在后端目标（由客户管理）
基于标题的路由	支持	支持	不支持
信任商店	ALB 的必填项	ALB 不要求这样做	NLB 不需要
证书撤销清单	在 ALB 管理	由后端管理（如果需要）	由后端管理（如果需要）
后端处理负载	小于	小于	更高
错误处理	由 ALB 管理	由后端管理	由后端管理

注意：开启 SAP 的 RISE AWS 支持带有 mTLS 验证模式的 ALB。

零信任访问

AWS Verified Access 是一种零信任安全解决方案，它取代了传统的 VPNs 企业应用程序安全解决方案。它通过检查用户身份、设备运行状况和位置来验证每个访问请求。该服务与 Okta、Azure Active Directory 和 IAM 身份中心集成，同时提供详细的访问记录和监控。有关更多信息，请参阅AWS 已验证的访问权限。

SAP AWS 验证访问权限的主要特点和优势

该解决方案通过零信任安全保护 SAP 环境，通过统一框架管理 SAPGUI 和基于 Web (HTTPs) 的访问。它对 SAPGUI TCP 连接和 Fiori 应用程序的 HTTPs 访问进行加密，在保持安全标准的同时消除了传统 VPN。

用户可以更快地通过 SAP 系统访问 RISE（在设置 VPN 连接之前）。它允许您向无法通过 VPN 访问您的公司网络的远程用户和外部顾问授予安全访问权限

1. 以身份为中心的安全验证访问权限与现有身份提供者 (IdP) 集成，例如微软 Azure AD (Entra)、Okta、Ping 等。它提供支持 SAML 2.0 和 AWS IAM 身份中心的实时用户身份验证和授权
2. 情境访问控制 Verified Access 能够实施设备安全态势评估、基于位置的访问策略、基于角色的访问管理和动态策略评估。
3. 增强的性能验证访问提供了直接、优化的连接路径到 SAP 系统，从而减少了网络延迟，提高了性能，为 SAP 系统提供了更一致的用户体验。
4. 简化管理 Verified Access 通过 AWS Cedar 策略语言和授权引擎提供集中式策略管理。它提供自动合规报告、实时访问监控和减少基础设施维护

实施指南

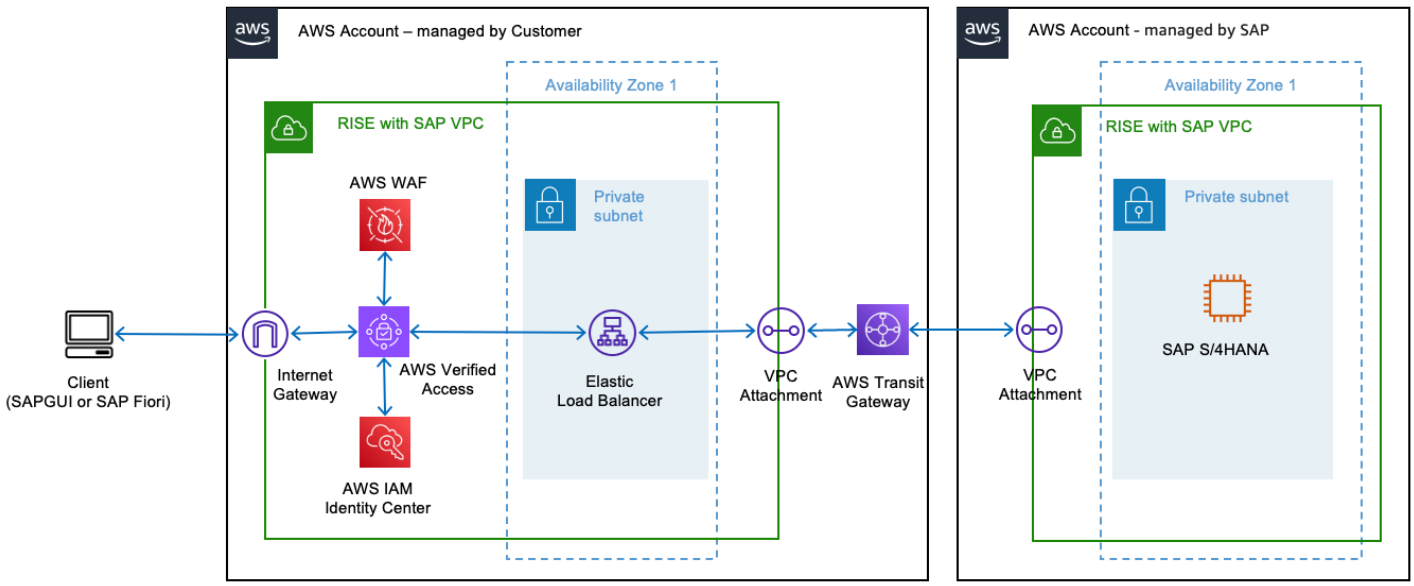
先决条件

- AWS IAM 身份中心已在您首选的 AWS 区域启用。有关更多信息，请参阅启用 AWS IAM 身份中心。
- 允许通过网络访问 SAP 应用程序的安全组。
- 在内部 AWS Elastic Load Balancer 后面运行的 SAP 应用程序。将您的安全组与负载均衡器关联。（你可以使用 Network Load Balancer 进行 SAP GUI 和 SAP Fiori 访问，或者只能使用 Application Load Balancer 访问 SAP Fiori）。
- 为基于 HTTP 的访问（即 SAP Fiori）配置 AWS 已验证访问权限时，Certifice Manager 中的公共 TLS AWS 证书。使用密钥长度为 1024 或 2048 的 RSA 证书。
- 公共托管域以及更新该域的 DNS 记录所需的权限。（示例：亚马逊 Route 53）
- 具有创建 AWS 已验证访问权限实例所需权限的 IAM 策略。有关更多信息，请参阅创建已验证访问权限实例的策略。
- 按照 SAP 注释 1346768 设置系统环境变量 S AP_ IPV6 _ACTIVE=1（需要 SAP S-user ID 才能访问），使用 SAP GUI 中的已验证访问端点访问 SAP 应用程序时需要这样做。

如何为 SAP 实施 AWS 经过验证的访问权限

1. 创建经过验证的访问信任提供商。在您的 AWS 账户上启用 IAM Identity Center 后，您可以使用以下步骤将 IAM Identity Center 设置为经过验证的访问的信任提供商。

2. 创建已验证访问实例。您可以使用 Verified Access 实例组织信任提供商和 Verified Access 组。使用以下过程创建已验证访问实例，然后将信任提供者与已验证访问权限关联或分离。
3. 创建 Verified Access 组。您可以使用已验证访问权限组根据端点的安全要求组织端点。创建已验证访问终端节点时，将该终端节点与组关联。使用以下步骤创建 “已验证访问权限” 组
4. 为已验证的访问权限创建负载平衡器端点。已验证的访问端点代表一个应用程序。每个端点都与已验证的访问权限组相关联，并继承该组的访问策略。使用以下过程为 SAP 应用程序的已验证访问权限创建负载平衡器端点。
5. 为已验证访问终端节点配置 DNS。在此步骤中，您需要将 SAP 应用程序的域名（例如 www.myapp.example.com ）映射到您的已验证访问终端节点的域名。要完成 DNS 映射，请在您的 DNS 提供商处创建规范名称记录（CNAME）。
6. 添加已验证访问权限组级别的访问策略。 AWS 验证访问策略允许您定义访问托管在中的 SAP 应用程序的规则 AWS。请参阅以下示例语句，根据您的要求为您的应用程序派生一个语句。
7. 测试与应用程序的连接。现在，您可以通过在 Web 浏览器中输入 SAP 应用程序的域名来测试与应用程序的连接，以进行基于 HTTP (S) 的访问，例如 SAP Fiori。



上图描述了如何部署 AWS 经过验证的 Access 并将其与 RISE 与 SAP 集成

人工智能

适用于 SAP 的生成式人工智能 AWS

生成式人工智能是指能够根据训练过的数据创建文本、图像、音频或代码等新内容的智能系统。这些系统使用机器学习技术，尤其是深度学习和神经网络，来识别训练数据中的模式和关系，然后生成与所学信息相似的新输出。

随着组织为员工和客户采用生成式人工智能，网络安全从业人员必须快速评估与这种不断发展的技术相关的风险、治理和控制措施。作为与 Amazon Web Services (AWS) 规模最大、最复杂的客户合作的安全领导者，我们经常就趋势、最佳实践、生成人工智能的快速演变格局以及相关的安全和隐私影响征求我们的意见。生成式 AI 解决方案涵盖影响您的安全范围的多个用例。要更好地了解范围和相应的关键安全学科，请参阅 AWS 博客文章《保护生成式 AI：生成式 AI 安全范围矩阵简介》。

SAP和 AWS Have共同创新的服务，帮助客户将SAP的人工智能创新和企业专业知识与亚马逊尖端的人工智能能力和技术解决方案相结合，从而开启业务增强的巨大机会。RISE客户可以通过生成式人工智能中心等 SAP商业技术平台（BTP）人工智能服务，以及包括Amazon B edrock 在内的 AWS 企业GenAI服务，以及支持安全、可扩展的人工智能解决方案的A mazon Q，加速其采用人工智能。

开启的 SAP 数据集成和管理 AWS

数据是任何生成式人工智能解决方案成功的基石。数据的质量、数量和多样性是直接影响 AI 模型性能和效率的关键因素。我们建议您查看我们的《SAP 数据集成与管理指南》 AWS，该指南为授权客户构建 AI 解决方案提供了基本的数据基础。它展示了如何使用 AWS 服务、SAP 产品和 AWS 合作伙伴解决方案， AWS 以实时或批处理模式将来自 SAP ERP 源系统的数据与变更数据捕获进行集成。这包括一个概述参考架构，展示了如何将 SAP 系统引入，此外还有详细的架构模式，这些模式使用 AWS 服务、SAP 产品和 AWS 合作伙伴解决方案来补充 SAP 支持的机制。 AWS

在 RISE 上实施生成式 AI 解决方案的方法 AWS

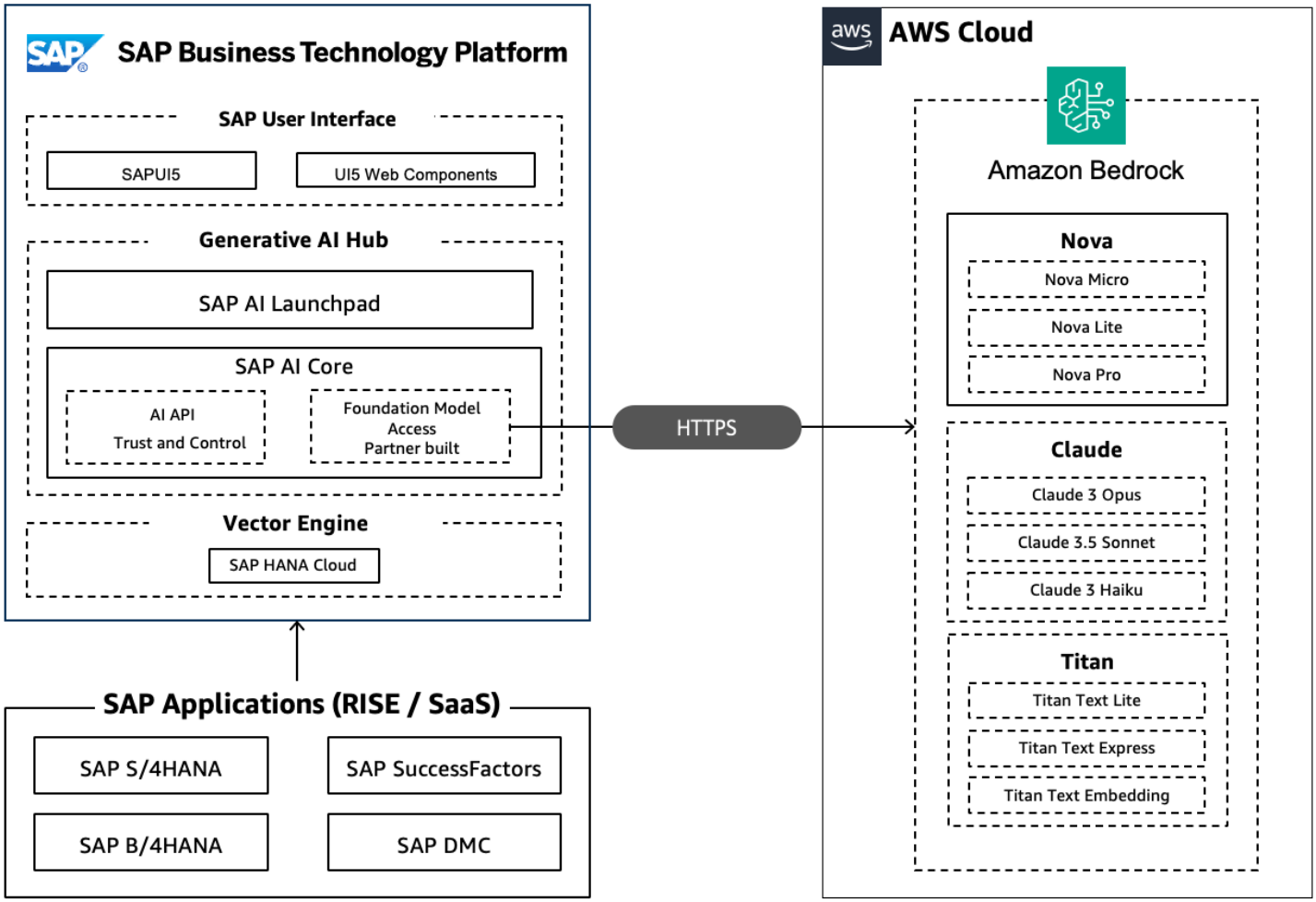
本架构指南可帮助您构建高级 AI 解决方案。它向您展示了如何有效地将RISE与SAP、SAP商业技术平台（BTP）和 AWS的人工智能服务相结合，以创建强大而创新的系统。

SAP 生成式人工智能中心

SAP Generation AI Hub 可帮助企业客户在安全可控的环境中无缝访问一系列商业和开源的大型语言模型 (LLMs)。SAP 的生成人工智能中心进一步简化了在 RISE 上运行的组织访问和实施由 Amazon 托管的复杂人工智能模型的流程。有关SAP通过Bedrock支持的生成式人工智能中心模型的更多详细信息，请参阅 SAP Note 343 7766。

这些模型现已通过 Generation AI Hub 推出，开发人员可以有效地利用它们与 SAP BTP 的强大功能相结合，构建和扩展与 SAP 应用程序无缝集成的人工智能驱动解决方案。

RISE客户可以通过SAP BTP服务利用Bedrock LLM模型来创建量身定制的人工智能解决方案，包括增强的SAP人工智能副驾驶焦耳功能。这种集成支持自动化工作流程和优化的企业数据处理，确保RISE客户在云转型之旅中实现精确、可操作的业务成果。



该图说明了在 BTP 上创建和实现的生成式 AI 解决方案或 S/4 HANA 扩展的设计框架。该设计说明了与运行的RISE和SAP解决方案的流畅集成 AWS。利用连接服务，并通过生成人工智能中心利用Bedrock LLM模型。

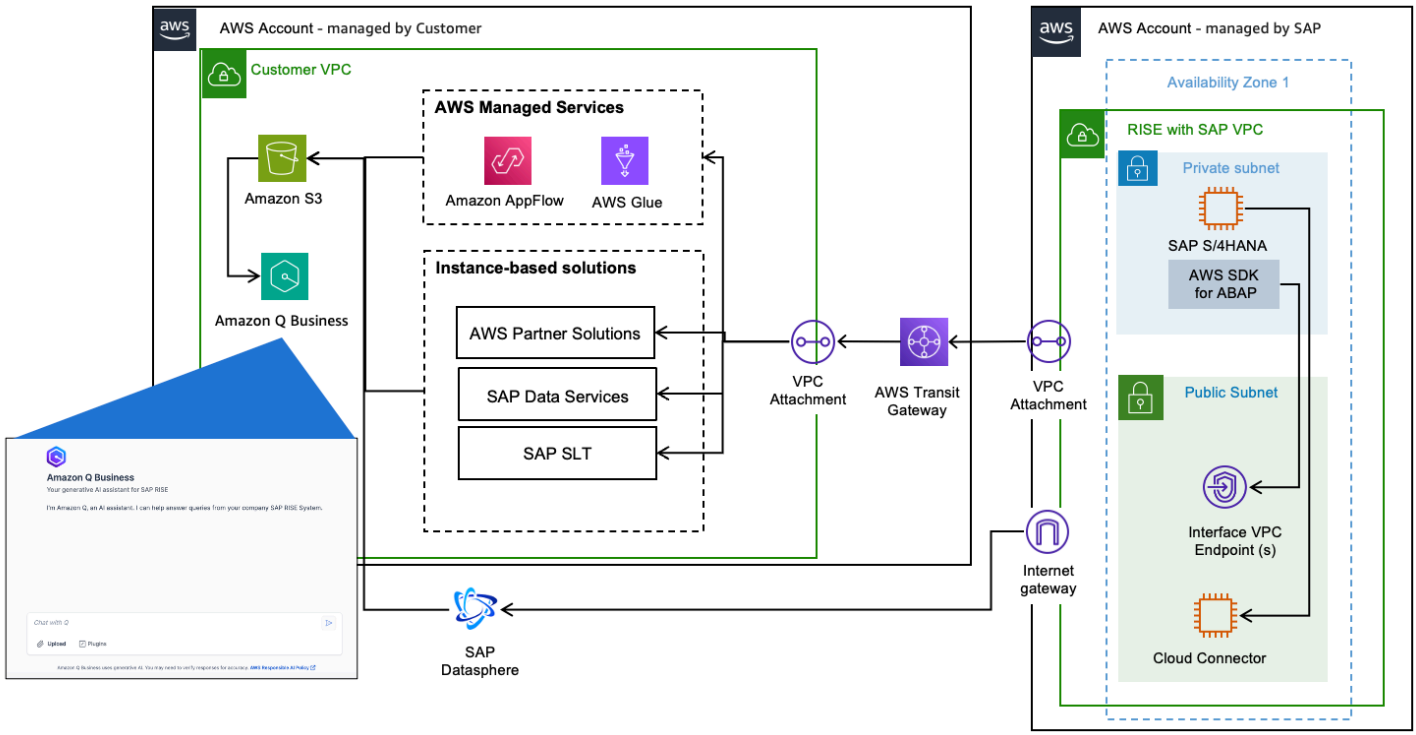
面向企业的 Amazon Q

RISE 客户可以利用 Amazon Q Bus iness 来回答问题、提供摘要、生成内容并根据企业数据完成任务。最终用户会立即收到来自企业数据源的带有引文的权限感知响应。Q Business 是一款完全托管的 Generative-AI 助手，具有 40 多个预先构建的连接器，可连接各种企业应用程序和数据源。

选择通过创建数据仓库或数据湖解决方案来打破数据孤岛的客户可以使用 SAP 和其他企业数据作为 Q Business 的来源，以便：

- 创建跨系统和数据的统一搜索体验，从而提取关键见解

- 创建和共享轻量级应用程序以选择用户或将其添加到组织的应用程序库中
- 跨常用业务应用程序和平台执行操作
- 创建和自动化复杂的业务工作流程



上图说明了基于Q Business的RISE客户搜索的设计框架。它说明了如何利用 AWS 服务提取 SAP 数据，以及如何使用 Q Business 组织的预建连接器来创建统一的搜索体验。

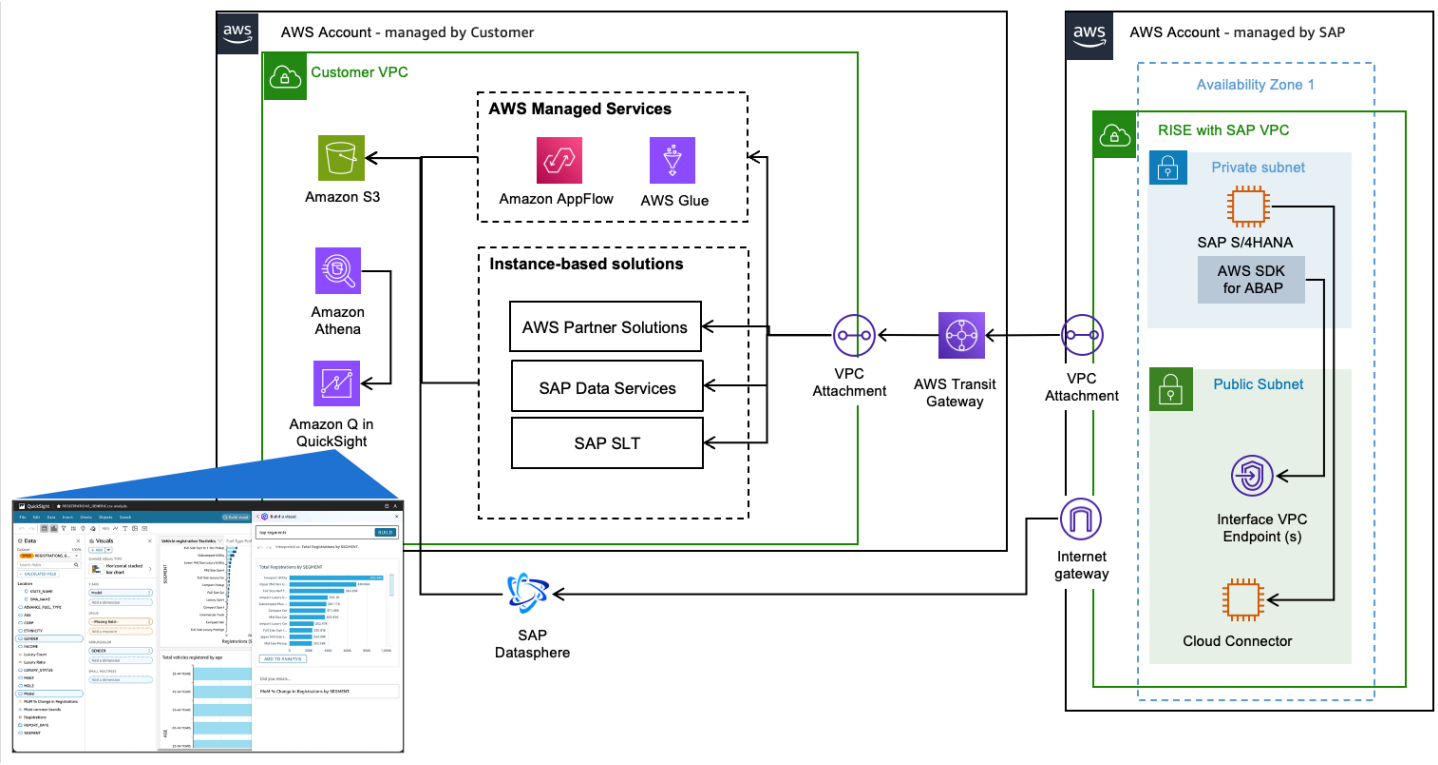
解决方案流程：

1. 通过为 SAP 创建 Glue 连接，建立 AWS 与 RISE 环境的连接 OData
2. 通过创建 ETL 作业来摄取相关的 SAP 数据
3. 利用各种数据源和应用程序的预建连接器与 Q Business 连接。在继承现有身份、角色和权限的同时摄取相关内容。
4. 最终用户可以用自然语言进行交互，从多个应用程序的数据中得出业务见解

亚马逊 Q in QuickSight

A@@ mazon Q in 通过其先进的 “生成商业智能” 功能 QuickSight彻底改变了 SAP 数据分析，为企业用户提供了直观的自助报告工具。使用自然语言提示，RISE客户可以毫不费力地创建复杂的可视化仪表板和数据叙述，而无需SQL或编程专业知识。

这种数据分析的民主化将报告生成时间从几天缩短到几小时，从而消除了对专业的 ABAP 开发人员 and/or 分析团队的依赖。该系统的人工智能驱动的自动化可以智能地生成情境标题、有条理的章节、连贯的故事流程以及带有具体建议的可操作见解。对于RISE客户来说，这可以加快决策流程，从他们的企业数据中获得更深入、更容易获得的见解。



该图说明了带有 SAP 数据的 Quicksight 中的 Amazon Q 框架。

解决方案流程：

1. SAP 报告用于处理业务逻辑并将数据上传到 Amazon S3。
2. 使用适用于 SAP ABAP 的 S AWS DK，它将创建一个与 S3 上的 SAP 报告数据关联的 Amazon Athena 查询。
3. 基于 Athena 查询创建 QuickSight 数据集和主题。
4. 现在，在 Quicksight 中使用 Q，你可以使用自然语言与 SAP 报告生成的数据进行交互，获得数据见解，从而构建仪表板和生成故事。

Amazon 基岩代理商

Amazon Bedrock Agen ts 能够在您的应用程序中构建和配置自主代理。代理可帮助最终用户根据组织数据和用户输入完成操作。代理协调基础模型 (FMs)、数据源、软件应用程序和用户对话之间的交互。此外，代理会自动调用 APIs 以采取行动，并调用 Amazon Bedrock 知识库来补充有关这些操作的信息。通过集成 Bedrock Agents，您可以加快开发工作以交付生成式人工智能（生成式 AI）应用程序。

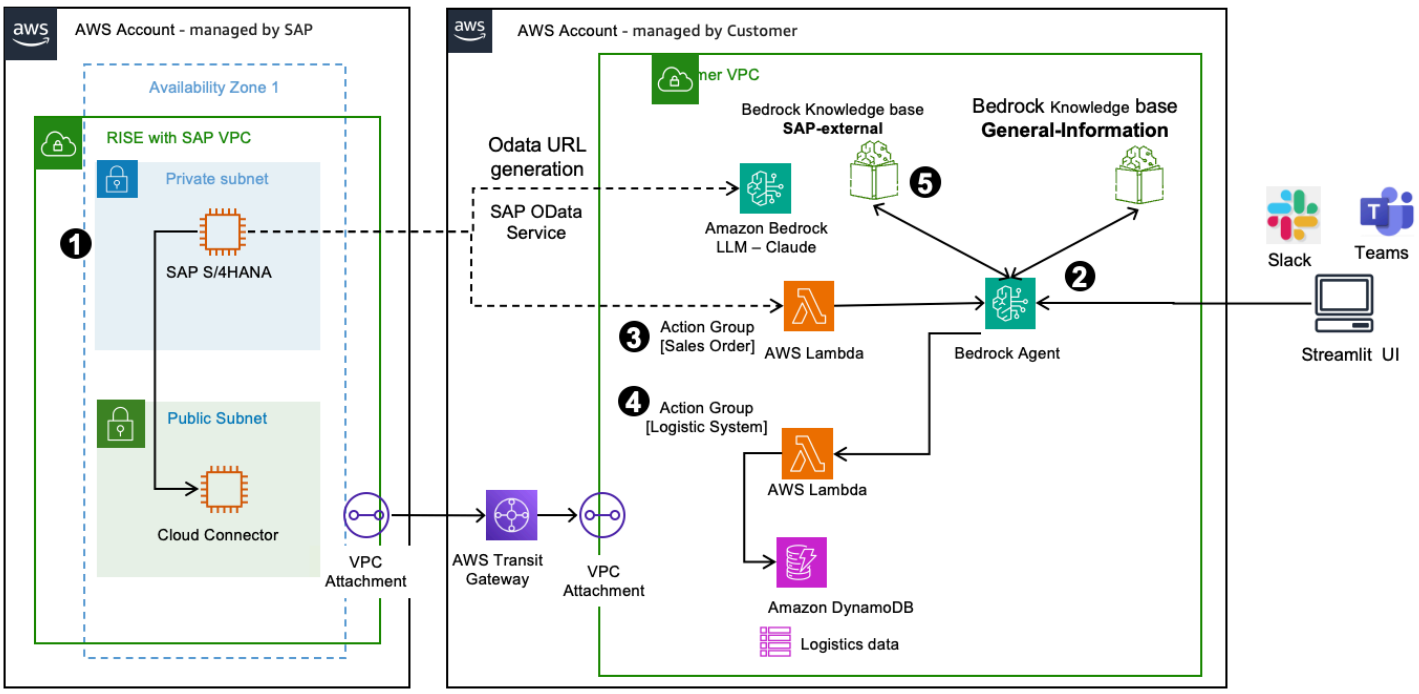
座席可以执行以下任务：

- 扩展基础模型来了解用户请求，并将座席必须执行的任务分解为更小的步骤。
- 通过自然对话从用户那里收集其他信息。
- 通过向贵公司的系统发出 API 调用，采取措施来满足客户的请求。
- 通过查询数据来源来提高性能和准确性。

RISE 客户可以通过利用 Bedrock Agents 来显著优化其业务流程。这些代理可与 SAP 系统、其他企业系统和组织的企业知识库无缝集成，从而实现自然语言交互，从而实现复杂的业务流程和工作流程的自动化。

通过将 SAP 和其他企业数据与 AWS其高级 AI 功能相结合，客户可以创建定制、安全和全面的解决方案，从而简化运营、改善决策并推动创新。

Bedrock Agents 可以根据特定的业务需求进行定制，使组织能够自动执行日常任务，从 SAP 和其他企业数据中提取宝贵的见解，并在整个企业中高效地扩展其 AI 实施。这种集成使RISE客户能够加快其数字化转型，同时维护其SAP生态系统内的数据安全性和合规性。



上图说明了一种生成式 AI 架构，该架构可以自动执行客户的任务，并回答他们的 SAP 和其他企业环境中的问题。

解决方案流程：

1. 用户通过轻量级应用程序（例如 Streamlit 用户界面、Slack 或 Microsoft Teams）访问该应用程序。
2. 根据用户输入，Bedrock Agent 协调不同应用程序、数据源或知识库之间的交互。
3. 如果用户查询与 SAP 销售订单相关，则 Bedrock Agent 会调用 SAP API 的销售订单操作组来获取相关详细信息。
4. 如果用户查询与 SAP 发货信息相关，则 Bedrock Agent 会调用非 SAP Logistic System 操作组。
5. 如果用户从组织的企业数据中查询一般信息，Bedrock Agent 会调用一般信息知识库。
6. 如果用户查询需要来自多个系统的数据，Bedrock Agent 会从不同的工具中获取数据，并在响应中进行整理。

拥有自主ERP系统的愿景可能会成为现实，即使用Bedrock Agents实现工作流程的自动化，从而减少手动工作，提高用户执行更重要的业务任务和流程的工作效率。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。