SAP 指南

常规 SAP 指南

常规 SAP 指南: SAP 指南

Table of Contents

主页 1
概述 2
关于本指南 2
AWS 概览 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 Note 12
AWS 架构上的 SAP 12
选择 AWS 区域和可用区 14
网络和连接 15
遵循安全最佳实践 6
用于 SAP 的 EC2 实例类型 17
操作系统 18
数据库 20
SAP 安装媒体 21
SAProuter 和 SAP 解决方案经理 22
文档修订 22
Amazon EC2 实例类型 24
实例类型可用性 24
SAP NetWeaver 支持的实例 24
SAP 的当前一代实例 NetWeaver 25
上一代 SAP 实例 NetWeaver 52
SAP HANA 的已认证和未认证实例 54
最新一代认证实例 55
上一代认证实例 65
未认证实例 66

SAP Business One 认证实例，适用于 SAP HANA 的版本 68
文档历史记录 69
AWS 数据提供商 71
简介 71
定价 72
技术要求 73
Amazon VPC 网络拓扑 73
Amazon VPC 端点 74
IAM 角色 75
DataProvider 4.3 77
正在安装 DataProvider 4.3 78
正在更新到 DataProvider 4.3 96
卸载旧版本 100
问题排查 101
在 Linux 上进行故障排除 101
Windows 上的问题排查 105
自定义 DataProvider 109
配置文件的语法规则 110
用户可配置的 EC2 实例类型 110
用户可配置的 EBS 卷类型 112
监测的验证 113
使用 SAP Operating System Collector（SAPOSCOL）检查指标 113
使用 SAP CCMS 事务检查指标 114
收集的指标示例 117
版本历史记录 122
成本估算 127
AWS 区域 127
计算 127
仓储服务 128
Amazon EBS 128
Amazon EFS 129
FSx 适用于 Windows 文件服务器的亚马逊 129
FSx 适用于 NetApp ONTAP 的亚马逊 129
Amazon S3 130
Network 130
Amazon VPC 130

AWS Site-to-Site VPN 131
AWS 直接连接 131
Elastic Load Balancing 132
数据传输定价 132
自动化 134
备份、还原和恢复 134
AWS 适用于 SAP HANA 的 Backint Agent 134
AWS 弹性灾难恢复 134
Amazon EBS 快照 135
迁移 135
Migration Hub Orchestrator 135
AWS DataSync 135
监控 135
AWS 数据提供商 136
CloudWatch 适用于 SAP HANA 的 Amazon 应用程序见解 136
Amazon CloudWatch 136
AWS CloudTrail 136
VPC 流日志 136
操作系统许可证 137
Red Hat 137
SUSE 137
Windows 138
Oracle Enterprise Linux 138
AWS Marketp 138
AWS Support 139
架构指南 140
概述 140
先决条件 140
专业知识 140
推荐阅读内容 141
简介 141
SAP NetWeaver 架构单点故障 141
高可用性和灾难恢复 142
本地部署模式与云部署模式 143
架构指南和决策 145
区域和可用区 145

AWS账户 147
计算 148
Networking 150
仓储服务 153
监控和审计 156
架构模式 156
故障场景 156
图案 157
Summary 175
Microsoft SQL 177
模式 177
比较表 177
单区域模式 178
多区域模式 180
使用弹性灾难恢复服务进行灾难恢复 186
场景 187
参考信息 187
SLAs 和许可证 187
恢复时间目标（RTO） 188
恢复点目标 (RPO) 188
恢复一致性目标（RCO） 189
SAP 许可证 189
网络、存储和计算 189
网络 190
存储 191
计算 193
场景 195
AWS 区域内灾难恢复 195
AWS 跨区域灾难恢复 197
AWS 外部向 AWS 的灾难恢复 199
共享存储韧性 201
AWS 区域内灾难恢复 202
AWS 跨区域灾难恢复 202
AWS 外部向 AWS 的灾难恢复 203
实施 203
SAP 应用程序层 203

SAP 数据库层 204
RISE with SAP 207
连接 208
建立连接的角色与责任 210
从本地网络连接到 RISE 210
从您的 AWS 账户连接到 RISE 222
连接到最近的 Direct Connect POP（包括本地区域） 241
RISE 连接方案决策树 242
其他考虑因素 244
安全性 258
SSO — SAP 云身份服务和 AWS IAM 身份中心 259
SSO – SAP Cloud Identity Services 与 Microsoft Entra 260
SSO - SAPGUI 前端 261
使用 AWS 服务实现高级安全性 262
将 SAP 数据托管人 KMS 与 AWS KMS 集成 271
AWS Nitro 如何通过 SAP 帮助保护 RISE？ 272
Amazon WorkSpaces 作为远程访问解决方案 276
可靠性 280
可观测性 284
责任共担 284
可观测性选项 284
变更管理 297
RISE with SAP 的变更管理 298
AWS 服务变更管理 298
使用 Partner Solutions 进行变更管理 300
数据集成与分析 301
数据集成 301
数据分析 307
代理式人工智能 311
Amazon Bedrock 代理 312
Amazon Bedrock Agentcore 313
Strands Agent 314
用于管理 ERP 异常的代理式人工智能 316
AWS 还有 SAP JRA 317
将数据转化为价值 318
人工智能 321

集成 324
自定义应用程序 326
运营可靠性 330
物联网 333
扩展程序 337
性能 338
应用程序集成 341
归档和文档管理 342
开发和扩展 345
安全扩展 347
人工智能 353
..... ccclvii

常规 SAP 指南

此部分包含以下指南。

- 概述：
- Amazon EC2 实例类型
- 估算
- AWS 数据提供程序
- 架构指南
- 使用 AWS 弹性灾难恢复服务进行灾难恢复
- RISE with SAP on AWS Cloud

其他 SAP on AWS 文档

- SAP HANA on AWS
- SAP NetWeaver on AWS
- AWS 上适用于 SAP 应用程序的数据库
- AWS Launch Wizard for SAP
- AWS Systems Manager for SAP
- 适用于 SAP ABAP 的 AWS SDK
- SAP BusinessObjects on AWS
- AWSMigration Hub Orchestrator

SAP 谈 AWS 概述和规划

SAP 专家，Amazon Web Services

上次更新时间：2023 年 1 月

本指南面向考虑在 Amazon Web Services 云端实施 SAP 环境或系统或者向云端进行迁移的 SAP 客户和合作伙伴，提供概述和规划信息。

本指南适用于之前已有在传统本地基础设施上安装、迁移和操作 SAP 环境及系统经验的用户。指南分为三个主要部分：

- 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。
- 技术注意事项，帮助您在 AWS云端规划并充分利用 SAP 环境。

> **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。有关详情，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 SAP AWS 文档。

AWS 概览

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。以下列表简要介绍了每种服务及其在 SAP 系统中的用途。要查看各项服务的功能、定价和文档，请点击说明后面的详细信息链接。

区域图	服务	说明	SAP 应用
计算	Amazon Elastic Compute Cloud（Amazon EC2）	云中大小可调且安全的计算容量。（详细信息）	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 实例的持久块存储卷。（详细信息）	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，提供高度持久、高度可用且可无限扩展的数据存储基础设施。（详细信息）	用于文件备份、数据库备份、归档数据、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	完全托管式、高度持久且原生可用的 Microsoft Windows 文件系统。（详细信息）	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	SAP 应用程序服务器的共享文件系统（例如 `/sapmnt`）。

区域图	服务	说明	SAP 应用
		扩展、高性能的文件存储（详细信息）	
联网	Amazon Virtual Private Cloud（Amazon 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）	用于 SAP 资源的网络。您可以控制 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	让您可以安全地将本地网络或分支机构站点连接到您的 VPC。（详细信息）	本地 systems/users 和 SAP 系统之间的网络连接已开启 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 systems/users 与 SAP 系统或环境之间的私有网络连接 AWS。
	Amazon Route 53	高度可用和可扩展的云域名系统（DNS）Web 服务。（详细信息）	AWS云端运行的 SAP 系统的名称和地址解析。
	Amazon Time Sync	高度准确和可靠的时间参考，可从 EC2 实例原生访问。（Linux | Windows）	用于 EC2 实例上 SAP 系统的时间同步。
管理和运营工具	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。

区域图	服务	说明	SAP 应用
	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。
	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	记录您账户上的活动，并将日志文件传输到 S3 存储桶。（详细信息）	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 Amazon S3 以及从中恢复 SAP HANA 数据库。（详细信息）	用于将 SAP HANA 数据库备份存储到 Amazon S3 的备份解决方案。

区域图	服务	说明	SAP 应用
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 资源启动、停止和启动 EC2 实例而不终止它们。

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。每个可用区包含一个或多个数据中心，这些数据中心通过延迟低、吞吐量高且高冗余的网络连接在一起。这些可用区提供了更加简单且高效的方式，供您设计和操作应用程序及数据库，与传统的单个或多个数据中心基础设施相比，可以实现更高的可用性、容错能力和可扩展性。

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。云安全性与本地数据中心的安全性有着相似之处，只不过无需承担维护设施和硬件所产生的费用。在云中，您无需管理物理服务器或存储设备。而是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，您可以像在内部数据中心那样，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。

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 符合要求的部分保障计划清单：

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

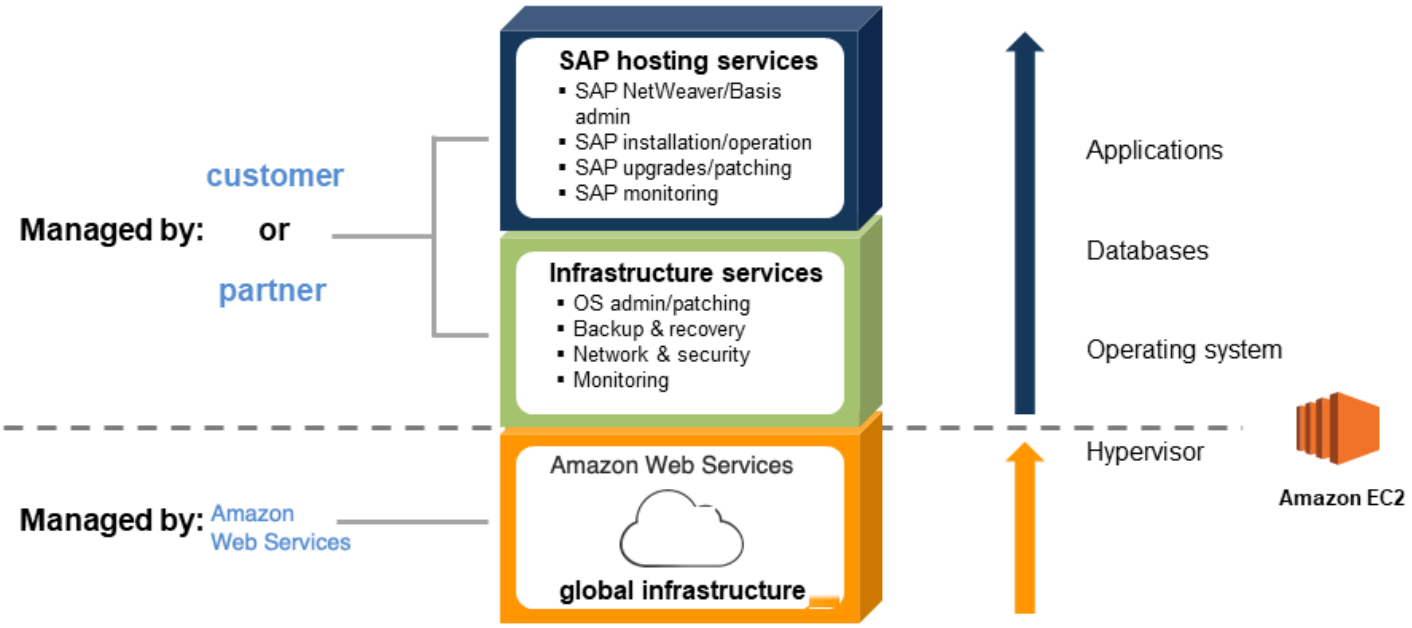
有关更多信息，请参阅 AWS 合规性计划。

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。有关可用于预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 显示了由 SAP 管理的 AWS 服务和由客户或合作伙伴管理的服务。

图 1：SAP on AWS 的托管式服务



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

此部分介绍 AWS云端可用的 SAP 软件和许可证的选项。

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。如果您是 SAP 的现有客户，则在运行 SAP on AWS时，可以使用现有的 SAP 许可证。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 试用版和开发人员版许可证

SAP Cloud Appliance Library 提供对最新预配置 SAP 解决方案的在线存储库的访问。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 Cloud Appliance Library 中提供的一些解决方案附带免费试用版或开发人员版许可证。

SAP 硬件密钥生成

在 EC2 实例上生成 SAP 硬件密钥使用一个特定的流程，该流程依赖于 SAP 内核补丁级别。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，使得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 Note（需要 SAP One Support Launchpad 访问权限）：

- 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 Amazon 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

SAP on AWS全面支持大多数在传统本地基础设施上运行的 SAP 解决方案。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：

- CloudWatch在每个 EC2 实例上启用 Amazon 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，请参阅亚马逊 CloudWatch。
- 在各个 EC2 实例上安装、配置和运行适用于 SAP 的AWS 数据提供程序。 AWS 数据提供商从各种来源（包括 Amazon 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

上支持的大多数 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。

预构建映像

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预置新的 SAP 系统，而不必像传统手动 SAP 安装那样需要耗费大量的时间和精力。

预构建的 SAP 系统映像可从以下来源获得：

- AWS Marketp
- SAP Cloud Appliance Library

SAP 解决方案	部署选项
SAP Business Suite（ERP、CRM 等）	手动 | SAP CAL
SAP NetWeaver	手动 | AWS Launch Wizard for SAP | SAP CAL
SAP S/4HANA	手册 | SAP AWS 版 Launch Wizard | SAP CAL
SAP BW/4HANA	手动 | SAP CAL
SAP HANA	手册 | SAP AWS 版 Launch Wizard | SAP CAL
SAP BusinessObjects BI	手动 | AWS Marketplace | SAP CAL
SAP Commerce（Hybris）	手动
SAP Business One，适用于 SAP HANA 的版本	手动 | SAP CAL
SAP Business One，适用于 Microsoft SQL Server 的版本	手动

获取 APN 合作伙伴的帮助

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，帮助您最大限度地发挥在 AWS云端运行 SAP 解决方案的好处。

适用于 SAP 的合作伙伴服务和解决方案的类型 AWS

- 云评测服务：咨询服务，帮助您为云采用旅程制定高效、有效的计划。典型的服务包括 financial/TCO （总拥有成本）、技术、安全与合规以及许可。
- Proof-of-concept 服务 — 帮助你测试 SAP 的服务 AWS；例如：SAP ERP/ECC 迁移到 SAP HANA 或 SAP S/4HANA，SAP Business Warehouse (BW) 迁移到 SAP HANA 或 SAP BW/4HANA，SAP OS/DB 迁移，实施新的 SAP 解决方案。
- 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此部分提供指导，

介绍在 AWS上运行 SAP 解决方案时，如何实现最佳的性能、可用性和可靠性以及降低总拥有成本（TCO）。

SAP Note

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。首先阅读 SAP Note 1656099 来获取一般信息，然后点击其他相关 SAP Note 的链接（需要 SAP One Support Launchpad 访问权限）。

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。

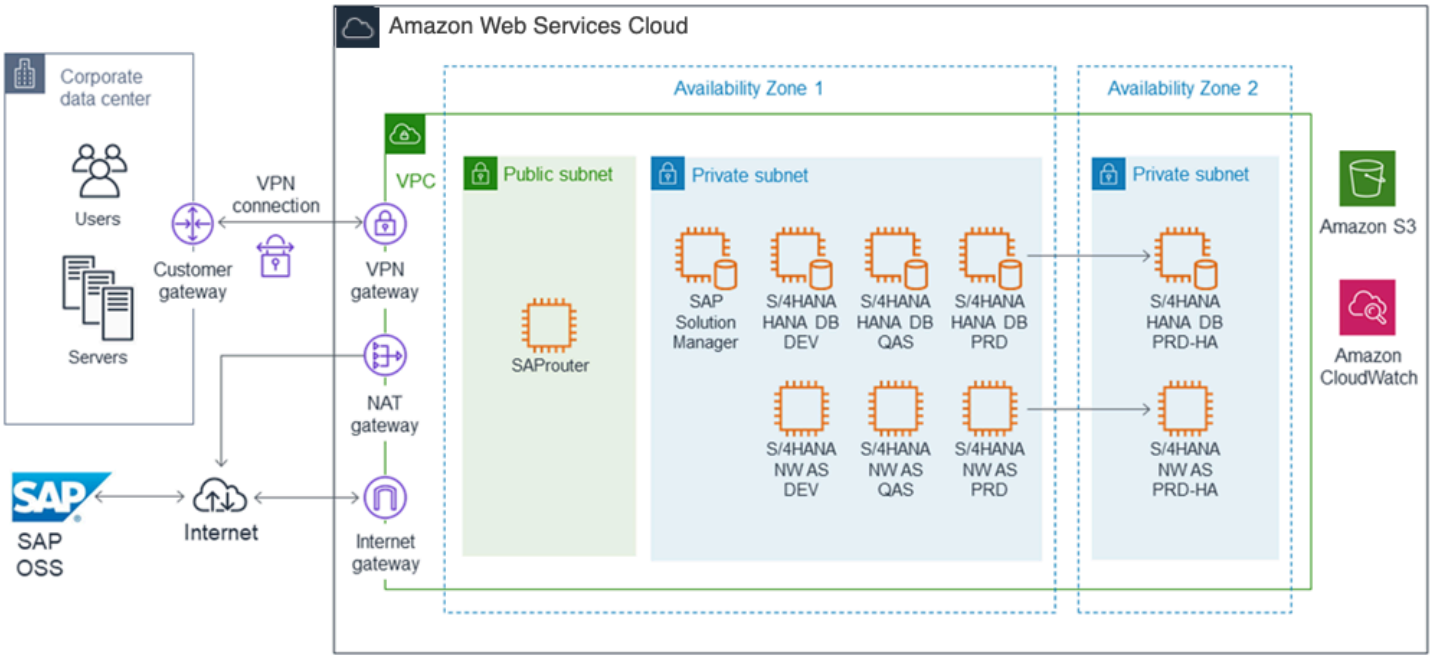
全能架构AWS

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



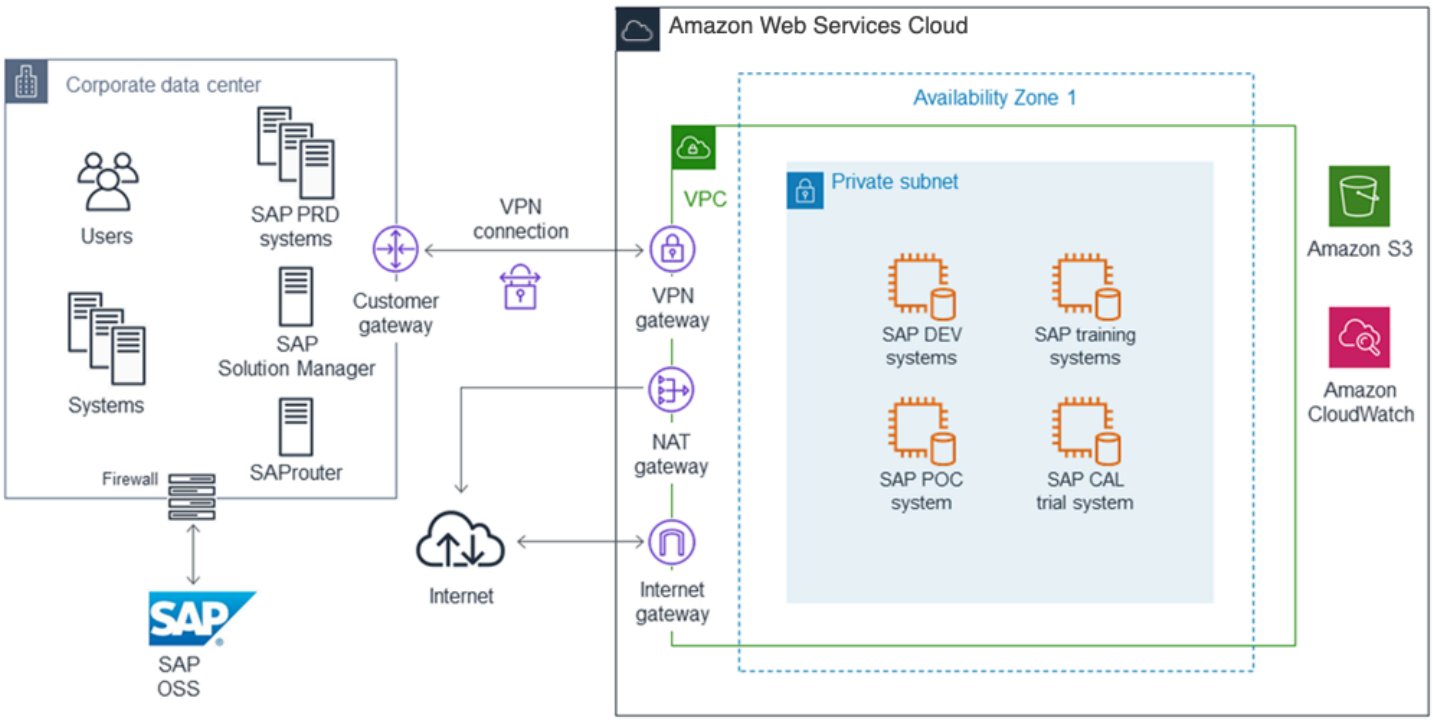
混合 AWS 架构

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，尽可能减少网络延迟。
- 数据驻留和监管合规性要求。
- 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。
- 您计划在区域中使用的 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 SA P 的 Amazon EC2 实例类型网页。

选择可用区

在为部署在 AWS云端的 SAP 选择可用区时，没有特别的注意事项。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）应部

署在同一个可用区中。如果具有高可用性（HA）要求，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。

专用网络连接

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。相比基于互联网的连接，在很多情况下，这样可以降低网络成本，增加带宽吞吐量，并提供更一致的网络体验。有关更多信息，请参阅 AWS Direct Connect 用户指南。

使用案例：建议相比硬件 VPN 提出了更高带宽和更低延迟要求的客户使用。

有关更多信息，请参阅 Amazon Virtual Private Cloud 连接选项。

直接互联网连接

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：仅带有公有子网的 VPC。

使用案例：非常适合不包含敏感数据的 SAP 演示、培训和测试类型的系统。

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 VPC 添加硬件虚拟专用网关。

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。

使用案例：为您的远程员工和业务合作伙伴提供简单快速的连接。

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 提供了安全详细信息，您必须完成这些设置才能够为资源正确地设置访问和限制措施。Amazon VPC 提供三种功能，供您用来增强和监控 VPC 的安全性：

- 安全组用作关联 EC2 实例的防火墙，在实例级别控制入站和出站的流量。

- 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。
- 路由表包含一组称为“路由”的规则，用于确定将网络流量发送到何处。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。
- 流日志可捕获有关在 VPC 中传入和传出网络接口的 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》的安全性部分。

用于 SAP 的 EC2 实例类型

Amazon EC2 提供各种不同的实例类型，这些实例类型经过优化，适合不同的使用案例。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。此部分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 EC2 实例类型的特定子集上运行，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

运行在 SAP HANA 数据库上的 SAP HANA 平台和 SAP 解决方案 [例如 HANA、SAP S/4HANA 上的 SAP Suite；HANA、SAP S/4HANA 上的 SAP Business Warehouse（BW）] 需要已通过 SAP HANA 认证的特定 EC2 实例类型。有关更多信息，请参阅适用于 SAP on AWS的 Amazon EC2 实例类型。

SAP Business One，适用于 SAP HANA 的版本

有关已通过 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 Intel 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
- Oracle Enterprise Linux

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

SLES for SAP 和 RHEL for SAP

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

- SAP 的配置和优化
- 扩展版本支持
- 适用于 SAP 的高可用性扩展
- 专属支持渠道

> **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

要了解有关 SUSE 和 Red Hat 适用于 SAP 的操作系统版本的更多信息，请参阅 SLES 和 Red Hat 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

- 适用于 SAP 解决方案的红帽企业 Linux
- Red Hat Cloud Access
- How to Locate Red Hat Cloud Access Gold Images on Amazon EC2
- What is the Difference between Red Hat Cloud Access and Red Hat Enterprise Linux On-Demand Subscriptions in the public cloud?

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亚马逊机器映像（AMI）中。操作系统许可证的费用包含在按需型实例的小时费用或该实例类型的预留实例费用中。
- 自带 License/Subscription (BYOL) — 将您现有的操作系统许可证或订阅带到 AWS 云端。
- 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，请点击表中的链接。

操作系统	许可/订阅选项
SLES	按需 | BYOL
适用于 SAP 的 SLES	AWS 市场 | BYOL
RHEL	按需 | BYOL
RHEL for SAP，带 HA 和 US	AWS 市场 | BYOL
Windows	按需 | BYOL
Oracle Linux	BYOL

数据库

支持的数据库

SAP 在本地基础设施上支持的所有数据块平台和版本，在 SAP on AWS上同样受支持。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

Amazon EC2 上的客户托管数据库

大多数 SAP 解决方案在 Amazon EC2 上使用客户托管模式。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 上使用自行管理数据库模式：

- 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 Business One

Amazon RDS

Amazon Relational Database Service（Amazon RDS）是一项托管式服务，让您能够在云中更轻松地设置、操作和扩展关系数据库。此服务在管理耗时的数据库管理任务的同时，提供经济实用的可调节容量，使您能够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 Commerce（以前称为 SAP Hybris Commerce）

Amazon Aurora

Amazon Aurora（Aurora）是一种专为云构建的 MySQL 和 PostgreSQL 兼容关系数据库。此数据库既具有传统企业数据库的性能和可用性，又具有开源数据库的简单性和成本效益。以下 SAP 解决方案目前支持 Aurora MySQL：

- SAP Commerce（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亚马逊机器映像（AMI）中。数据库许可证的费用包含在按需型实例的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 Adaptive Server Enterprise（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 Microsoft 软件保障或 Amazon EC2 专属主机才能将这些许可证自带到 AWS云端。有关更多信息，请参阅：
- SAP Note 2139358 - Effect of changes in licensing terms of SQL Server
- 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。有两个主要选项可用于将 SAP 安装媒体复制到 AWS云端：

- 从 SAP Software Download Center 下载到 Amazon EC2。从您的 EC2 实例，连接到 SAP Software Download Center 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，并创建多个卷，可以用来并行连接到多个实例。
- 从您的网络复制到 Amazon EC2。如果您已经将所需的 SAP 安装媒体下载到自己网络上的某个位置，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。
- 对于互联网连接，请使用安全网络通信（SNC）。有关更多信息，请参阅 SAP Remote Support 和连接。

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

日期	更改	位置
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) 提供多种经过优化的实例类型，以适应不同的用例。利用 CPU、内存、存储和网络容量的不同组合，您可以灵活地为应用程序选择资源。您可以选择满足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 的已认证和未认证实例
- SAP Business One 认证实例，适用于 SAP HANA 的版本
- 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 Amazon 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。在进行规划时，您应确认目标可用区中提供了 SAP 工作负载所需的实例类型。

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
m8a.large	2	8	4,820	最多 12.5	最高 10,000	最多 40,000
m8a.xlarge	4	16	9,640	最多 12.5	最高 10,000	最多 40,000
m8a.2xlarge	8	32	19,280	最多 15	最高 10,000	最多 40,000
m8a.4xlarge	16	64	38,560	最多 15	最高 10,000	最多 40,000
m8a.8xlarge	32	128	77,120	15	10000	40000
m8a.12xlarge	48	192	115,680	22.5	15000	60000
m8a.16xlarge	64	256	154,240	30	20000	80,000

实例类型	vCPU	内存（GiB）	SAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
m8a.24xlarge	96	384	231,360	40	30000	120,000
m8a.48xlarge	192	768	462,800	75	60000	240,000
m8i.large	2	8	4,278	最多 12.5	最高 10,000	最多 40,000
m8i.xlarge	4	16	8,556	最多 12.5	最高 10,000	最多 40,000
m8i.2xlarge	8	32	17,112	最多 15	最高 10,000	最多 40,000
m8i.4xlarge	16	64	34,224	最多 15	最高 10,000	最多 40,000
m8i.8xlarge	32	128	68,448	15	10000	40000
m8i.12xlarge	48	192	102,672	22.5	15000	60000
m8i.16xlarge	64	256	136,896	30	20000	80,000
m8i.24xlarge	96	384	205,334	40	30000	120,000
m8i.32xlarge	128	512	273,792	50	40000	160000
m8i.48xlarge	192	768	410,730	75	60000	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
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

实例类型	vCPU	内存（GiB）	SAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
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
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

实例类型	vCPU	内存（GiB）	SAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
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
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

实例类型	vCPU	内存（GiB）	SAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
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
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	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r5.large	2	16	2,891	不适用	最多 10	最多 4,750	18,750
r5.xlarge	4	32	5,782	不适用	最多 10	最多 4,750	18,750
r5.2xlarge	8	64	11,564	不适用	最多 10	最多 4,750	18,750

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r5.4xlarge	16	128	23,128	不适用	最多 10	4750	18,750
r5.8xlarge	32	256	46,257	不适用	10	6800	30000
r5.12xlarge	48	384	69,385	不适用	10	9500	40000
r5.16xlarge	64	512	92,513	不适用	20	13600	60000
r5.24xlarge	96	768	138,770	不适用	25	19000	80,000
r5.metal	96	768	143,230	不适用	25	19000	80,000
r5b.large	2	16	2,891	不适用	最多 10	最高 10,000	43333
r5b.xlarge	4	32	5,782	不适用	最多 10	最高 10,000	43333
r5b.2xlarge	8	64	11,564	不适用	最多 10	最高 10,000	43333
r5b.4xlarge	16	128	23,128	不适用	最多 10	10000	43333
r5b.8xlarge	32	256	46,257	不适用	25	20000	86667
r5b.12xlarge	48	384	69,385	不适用	50	30000	130,000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r5b.16xlarge	64	512	92,513	不适用	75	40000	173333
r5b.24xlarge	96	768	138,770	不适用	100	60000	260000
r5b.metal	96	768	143,230	不适用	100	60000	260000
r5n.large	2	16	2,891	不适用	最多 25	最多 4,750	18,750
r5n.xlarge	4	32	5,782	不适用	最多 25	最多 4,750	18,750
r5n.2xlarge	8	64	11,564	不适用	最多 25	最多 4,750	18,750
r5n.4xlarge	16	128	23,128	不适用	最多 25	4750	18,750
r5n.8xlarge	32	256	46,257	不适用	25	6800	30000
r5n.12xlarge	48	384	69,385	不适用	50	9500	40000
r5n.16xlarge	64	512	92,513	不适用	75	13600	60000
r5n.24xlarge	96	768	138,770	不适用	100	19000	80,000
r5n.metal	96	768	143,230	不适用	100	19000	80,000
r6a.large	2	16	2,984	不适用	最多 12.5	最高 10,000	40000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r6a.xlarge	4	32	5,968	不适用	最多 12.5	最高 10,000	40000
r6g.2xlarge	8	64	11,935	不适用	最多 12.5	最高 10,000	40000
r6a.4xlarge	16	128	23,871	不适用	最多 12.5	最高 10,000	40000
r6a.8xlarge	32	256	47,742	不适用	12.5	10000	40000
r6a.12xlarge	48	384	71,613	不适用	18.75	15000	60000
r6a.16xlarge	64	512	95,483	不适用	25	20000	80,000
r6a.32xlarge	128	1024	190,967	不适用	50	40000	160000
r6a.24xlarge	96	768	143,225	不适用	37.5	30000	120,000
r6a.48xlarge	192	1,536	286,450	不适用	50	40000	240,000
r6i.large	2	16	3,063	不适用	最多 12.5	最高 10,000	40000
r6i.xlarge	4	32	6,127	不适用	最多 12.5	最高 10,000	40000
r6i.2xlarge	8	64	12,253	不适用	最多 12.5	最高 10,000	40000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r6i.4xlarge	16	128	24,506	不适用	最多 12.5	最高 10,000	40000
r6i.8xlarge	32	256	49,013	不适用	12.5	10000	40000
r6i.12xlarge	48	384	73,519	不适用	18.75	15000	60000
r6i.16xlarge	64	512	98,025	不适用	25	20000	80,000
r6i.24xlarge	96	768	147,038	不适用	37.5	30000	120,000
r6i.32xlarge	128	1024	196,050	不适用	50	40000	160000
r6i.metal	128	1024	203,600	不适用	50	40000	160000
r6id.large	2	16	3,063	不适用	最多 12.5	最高 10,000	40000
r6id.xlarge	4	32	6,127	不适用	最多 12.5	最高 10,000	40000
r6gd.2xlarge	8	64	12,253	不适用	最多 12.5	最高 10,000	40000
r6id.4xlarge	16	128	24,506	不适用	最多 12.5	最高 10,000	40000
r6id.8xlarge	32	256	49,013	不适用	12.5	10000	40000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r6id.12xlarge	48	384	73,519	不适用	18.75	15000	60000
r6id.16xlarge	64	512	98,025	不适用	25	20000	80,000
r6id.24xlarge	96	768	147,038	不适用	37.5	30000	120,000
r6id.32xlarge	128	1024	196,050	不适用	50	40000	160000
r6idn.large	2	16	3,063	不适用	最多 25	最多 25,000	100000
r6idn.xlarge	4	32	6,127	不适用	最多 30	最多 25,000	100000
r6idn.2xlarge	8	64	12,253	不适用	最多 40	最多 25,000	100000
r6idn.4xlarge	16	128	24,506	不适用	最多 50	最多 25,000	100000
r6idn.8xlarge	32	256	49,013	不适用	50	25000	100000
r6idn.12xlarge	48	384	73,519	不适用	75	37,500	15万
r6idn.16xlarge	64	512	98,025	不适用	100	50000	200,000
r6idn.24xlarge	96	768	147,038	不适用	150	75000	300,000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r6idn.32xlarge	128	1024	196,050	不适用	200	100000	400,000
r6id.metal	128	1024	203,600	不适用	50	40000	160000
r6in.large	2	16	3,063	不适用	最多 25	最多 25,000	100000
r6in.xlarge	4	32	6,127	不适用	最多 25	最多 25,000	100000
r6in.2xlarge	8	64	12,253	不适用	最多 25	最多 25,000	100000
r6in.4xlarge	16	128	24,506	不适用	最多 25	最多 25,000	100000
r6in.8xlarge	32	256	49,013	不适用	12.5	25000	100000
r6in.12xlarge	48	384	73,519	不适用	18.75	37,500	15万
r6in.16xlarge	64	512	98,025	不适用	25	50000	200,000
r6in.24xlarge	96	768	147,038	不适用	37.5	75000	300,000
r6in.32xlarge	128	1024	196,050	不适用	200	100000	400,000
r7a.medium	1	8	2,255	不适用	最多 12.5	最高 10,000	最多 40,000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r7a.large	2	16	4,510	不适用	最多 12.5	最高 10,000	最多 40,000
r7a.xlarge	4	32	9,020	不适用	最多 12.5	最高 10,000	最多 40,000
r7a.2xlarge	8	64	18,040	不适用	最多 12.5	最高 10,000	最多 40,000
r7a.4xlarge	16	128	36,080	不适用	最多 12.5	最高 10,000	最多 40,000
r7a.8xlarge	32	256	72,160	不适用	12.5	10000	40000
r7a.12xlarge	48	384	108,240	不适用	18.75	15000	60000
r7a.16xlarge	64	512	144,320	不适用	25	20000	80,000
r7a.24xlarge	96	768	216,480	不适用	37.5	30000	120,000
r7a.32xlarge	128	1024	288,640	不适用	50	40000	160000
r7a.48xlarge	192	1536	432,980	不适用	50	40000	240,000
r7i.large	2	16	4,155	不适用	最多 12.5	最高 10,000	40000
r7i.xlarge	4	32	8,310	不适用	最多 12.5	最高 10,000	40000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r7i.2xlarge	8	64	16,620	不适用	最多 12.5	最高 10,000	40000
r7i.4xlarge	16	128	33,240	不适用	最多 12.5	最高 10,000	40000
r7i.8xlarge	32	256	66,480	不适用	12.5	10000	40000
r7i.12xlarge	48	384	99,720	不适用	18.75	15000	60000
r7i.16xlarge	64	512	105,500	不适用	25	20000	80,000
r7i.24xlarge	96	768	158,250	不适用	37.5	30000	120,000
r7i.48xlarge*	192	1536	296,200	不适用	50	40000	240,000
r8a.large	2	16	6,646	不适用	最多 12.5	最高 10,000	最多 40,000
r8a.xlarge	4	32	13,292	不适用	最多 12.5	最高 10,000	最多 40,000
r8a.2xlarge	8	64	26,584	不适用	最多 15	最高 10,000	最多 40,000
r8a.4xlarge	16	128	53,168	不适用	最多 15	最高 10,000	最多 40,000
r8a.8xlarge	32	256	106,366	不适用	15	10000	40000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r8a.12xlarge	48	384	159,504	不适用	22.5	15000	60000
r8a.16xlarge	64	512	212,672	不适用	30	20000	80,000
r8a.24xlarge	96	768	318,980	不适用	40	30000	120,000
r8a.48xlarge	192	1536	596,370	不适用	75	60000	240,000
r8i.large	2	16	4,802	740	最多 12.5	最高 10,000	40000
r8i.xlarge	4	32	9,604	1,480	最多 12.5	最高 10,000	40000
r8i.2xlarge	8	64	19,208	2,960	最多 15	最高 10,000	40000
r8i.4xlarge	16	128	38,416	5,921	最多 15	最高 10,000	40000
r8i.8xlarge	32	256	76,832	11,842	15	10000	40000
r8i.12xlarge	48	384	115,270	17,763	22.5	15000	60000
r8i.16xlarge	64	512	145,280	23,683	30	20000	80,000
r8i.24xlarge	96	768	217,920	35,525	40	30000	120,000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
r8i.32xlarge	128	1024	290,620	47,367	50	40000	160000
r8i.48xlarge	192	1536	416,520	71,050	75	60000	240,000
r8i.96xlarge	384	3072	740,050	142,100	100	80,000	480,000
u-3tb1.56xlarge	224	3,072	237,750	不适用	50	19000	80,000
u-6tb1.56xlarge	224	6,144	380770	不适用	100	38,000	160000
u-6tb1.112xlarge	448	6,144	475,500	不适用	100	38,000	160000
u-6tb1.metal	448	6,144	480,600	不适用	100	38,000	160000
u-9tb1.112xlarge	448	9,216	475,500	不适用	100	38,000	160000
u-9tb1.metal	448	9,216	480,600	不适用	100	38,000	160000
u-12tb1.112xlarge	448	12,288	475,500	不适用	100	38,000	160000
u-12tb1.metal	448	12,288	480,600	不适用	100	38,000	160000
u-18tb1.112xlarge	448	18432	520,330	不适用	100	38,000	160000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
u-18tb1.metal	448	18432	534,130	不适用	100	38,000	160000
u-24tb1.112xlarge	448	24576	508,720	不适用	100	38,000	160000
u-24tb1.metal	448	24576	517,480	不适用	100	38,000	160000
u7i-6tb.112xlarge	448	6,144	670,265	不适用	100	60000	420,000
u7i-8tb.112xlarge	448	8192	674,950	不适用	100	60000	420,000
u7i-12tb.224xlarge	896	12,288	1,254,030	不适用	100	60000	420,000
u7in-16tb.224xlarge	896	16,384	1,281,620	不适用	200	100000	420,000
u7in-24tb.224xlarge	896	24576	1,225,250	不适用	200	100000	420,000
u7inh-32tb.480xlarge	1,920	32,768	不适用	不适用	200	160000	840,000
x1.16xlarge	64	976	65,750	不适用	10	7,000	40000
x1.32xlarge	128	1,952	131,500	不适用	25	14,000	80,000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
x1e.xlarge	4	122	4,109	不适用	最多 10	500	3,700
x1e.2xlarge	8	244	8,219	不适用	最多 10	1000	7,400
x1e.4xlarge	16	488	16,437	不适用	最多 10	1,750	10000
x1e.8xlarge	32	976	32,875	不适用	最多 10	3,500	20000
x1e.16xlarge	64	1,952	65,750	不适用	10	7,000	40000
x1e.32xlarge	128	3,904	131,500	不适用	25	14,000	80,000
x2idn.16xlarge	64	1024	98,025	不适用	50	40000	15万
x2idn.24xlarge	96	1,536	147,038	不适用	75	60000	200,000
x2idn.32xlarge	128	2,048	196,050	不适用	100	80,000	300,000
x2iedn.xlarge	4	128	5,906	不适用	最多 25	最多 20,000	12,500
x2iedn.2xlarge	8	256	11,813	不适用	最多 25	最多 20,000	25000
x2iedn.4xlarge	16	512	23,625	不适用	最多 25	最多 20,000	50000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
x2iedn.8xlarge	32	1024	47,250	不适用	25	20000	75000
x2iedn.16xlarge	64	2,048	94,500	不适用	50	40000	15万
x2iedn.24xlarge	96	3,072	141,750	不适用	75	60000	200,000
x2iedn.32xlarge	128	4,096	189,000	不适用	100	80,000	300,000
x2iezn.2xlarge	8	256	14,170	不适用	最多 25	3,170	13,333
x2iezn.4xlarge	16	512	28,340	不适用	最多 25	4,175	20000
x2iezn.6xlarge	24	768	42,510	不适用	50	9500	40000
x2iezn.8xlarge	32	1024	56,680	不适用	75	12000	55,000
x2iezn.12xlarge	48	1,536	85,020	不适用	100	19000	80,000
x8i.large	2	32	5,016	748	最多 12.5	最高 10,000	40000
x8i.xlarge	4	64	10,032	1,496	最多 12.5	最高 10,000	40000
x8i.2xlarge	8	128	20,064	2,992	最多 15	最高 10,000	40000

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
x8i.4xlarge	16	256	40,128	5,983	最多 15	最高 10,000	40000
x8i.8xlarge	32	512	80,250	11,967	15	10000	40000
x8i.12xlarge	48	768	116,280	17,950	22.5	15000	60000
x8i.16xlarge	64	1024	147,370	23,933	30	20000	80,000
x8i.24xlarge	96	1536	217,824	35,900	40	30000	120,000
x8i.32xlarge	128	2048	290,420	47,867	50	40000	160000
x8i.48xlarge	192	3172	413,376	71,800	75	60000	240,000
x8i.64xlarge	256	4096	551,220	95,733	80	70,000	320,000
x8i.96xlarge	384	6144	733,800	143,600	100	80,000	480,000

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

实例类型	vCPU	内存（GiB）	SAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
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
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

实例类型	vCPU	内存（GiB）	SAPS	网络（Gbps）	存储空间（Mbps）	最大 IOPS
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

*advanced SAP Application Performance Standard（aSAPS）是一个独立于硬件的衡量单位，用于描述系统配置在 SAP 环境中的性能。它源自 SAP Quote-to-cash 标准应用程序基准 (Q2C)

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
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

实例类型	vCPU	内存（GiB）	SAPS
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

实例类型	vCPU	内存（GiB）	SAPS
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 的已认证和未认证实例

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。有关更多信息，请参阅 SAP Note 2271345。

内容

- 最新一代认证实例
  - SAP HANA OLTP 和 OLAP 纵向扩展
  - SAP HANA OLTP 和 OLAP 横向扩展
- 上一代认证实例
  - SAP HANA OLTP 和 OLAP 纵向扩展
  - SAP HANA OLTP 和 OLAP 横向扩展
- 未认证实例

最新一代认证实例

SAP HANA OLTP 和 OLAP 纵向扩展

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps	存储空间（Mbps）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	FSx 适用于 ONTAP
r5.8xlarge	32	256	46,257	不适用	10	6800	✓	标准	✓	标准	✗
r5.12xlarge	48	384	69,385	不适用	10	9500	✓	标准	✓	标准	✗
r5.16xlarge	64	512	92,513	不适用	20	13600	✓	标准	✓	标准	✗
r5.24xlarge	96	768	138,77	不适用	25	19000	✓	标准	✓	标准	✗
r5.metal	96	768	143,23	不适用	25	19000	✓	标准	✓	标准	✗
r5b.8xlarge	32	256	46,257	不适用	25	20000	✓	标准	✓	标准	✗
r5b.12xlarge	48	384	69,385	不适用	50	30000	✓	标准	✓	标准	✗
r5b.16xlarge	64	512	92,513	不适用	75	40000	✓	标准	✓	标准	✗
r5b.24xlarge	96	768	138,77	不适用	100	60000	✓	标准	✓	标准	✗
r5b.metal	96	768	143,23	不适用	100	60000	✓	标准	✓	标准	✗

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps	存储空间（Mbps）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	FSx 适用于 ONTAP
r6i.8xlarge	32	256	49,013	不适用	12.5	10000	✓	标准	✗	不适用	✗
r6i.12xlarge	48	384	73,519	不适用	18.75	15000	✓	标准	✓	标准	✓
r6i.16xlarge	64	512	98,025	不适用	25	20000	✓	标准	✓	标准	✓
r6i.24xlarge	96	768	147,03	不适用	37.5	30000	✓	标准	✓	标准	✓
r6i.32xlarge	128	1024	196,05	不适用	50	40000	✓	标准	✓	标准	✓
r7i.8xlarge	32	256	66,480	不适用	12.5	10000	✓	标准	✓	标准	✓
r7i.12xlarge	48	384	99,720	不适用	18.75	15000	✓	标准	✓	标准	✓
r7i.16xlarge	64	512	105,50	不适用	25	20000	✓	标准	✓	标准	✓
r7i.24xlarge	96	768	158,25	不适用	37.5	30000	✓	标准	✓	标准	✓
r7i.48xlarge	192	1536	296,20	不适用	50	40000	✓	标准	✓	标准	✓
r8i.12xlarge	48	384	115,27	17,763	22.5	15000	✓	标准	✓	标准	✓

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps	存储空间（Mbps）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	FSx 适用于 ONTAP
r8i.16xlarge	64	512	138,84	23,683	30	20000	✓	标准	✓	标准	✓
r8i.24xlarge	96	768	208,26	35,525	40	30000	✓	标准	✓	标准	✓
r8i.32xlarge	128	1024	277,68	47,367	50	40000	✓	标准	✓	标准	✓
r8i.48xlarge	192	1536	416,52	71,050	75	60000	✓	标准	✓	标准	✓
r8i.96xlarge	384	3072	740,05	142,10	100	80,000	✓	标准	✓	标准	✓
u-3tb1.xlarge	224	3,072	237,75	不适用	50	19000	✓	标准	✓	工作负载	✓
u-6tb1.xlarge	224	6,144	380770	不适用	100	38,000	✓	标准	✓	工作负载	✓
u-6tb1.2xlarge	448	6,144	475,50	不适用	100	38,000	✓	标准	✓	标准	✓
u-6tb1.tal	448	6,144	480,60	不适用	100	38,000	✓	标准	✓	标准	✗
u-9tb1.2xlarge	448	9,216	475,50	不适用	100	38,000	✓	标准	✓	工作负载	✓
u-9tb1.tal	448	9,216	480,60	不适用	100	38,000	✓	标准	✓	工作负载	✗

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps	存储空间（Mbps）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	FSx 适用于 ONTAP
u-12tb1 12xlarg	448	12,288	475,50	不适用	100	38,000	✓	标准	✓	工作负载	✓
u-12tb1 etal	448	12,288	480,60	不适用	100	38,000	✓	标准	✓	工作负载	✗
u-18tb1 12xlarg	448	18432	520,33	不适用	100	38,000	✓	工作负载	✓	工作负载	✓
u-18tb1 etal	448	18432	534,13	不适用	100	38,000	✓	工作负载	✓	工作负载	✗
u-24tb1 12xlarg	448	24576	508,72	不适用	100	38,000	✓	工作负载	✗	不适用	✓
u-24tb1 etal	448	24576	517,48	不适用	100	38,000	✓	工作负载	✗	不适用	✗
u7i-6tb 12xlarg	448	6,144	670,26	不适用	100	60000	✓	标准	✓	标准	✓
u7i-8tb 12xlarg	448	8192	674,95	不适用	100	60000	✓	标准	✓	标准	✓
u7i-12t 224xlar	896	12,288	1,254,0	不适用	100	60000	✓	标准	✓	标准	✓
u7in-16 .224xla e	896	16,384	1,281,6	不适用	200	100000	✓	标准	✓	标准	✓

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps	存储空间（Mbps）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	FSx 适用于 ONTAP
u7in-24.224xlarge	896	24576	1,225,1	不适用	200	100000	✓	工作负载	✓	工作负载	✓
u7inh-3b.480xlarge	1,920	32,768	不适用	不适用	200	160000	✓	标准	✓	标准	✓
x1.16xlarge	64	976	65,750	不适用	10	7,000	✓	标准	✓	标准	✗
x1.32xlarge	128	1,952	131,50	不适用	25	14,000	✓	标准	✓	标准	✗
x1e.32xlarge	128	3,904	131,50	不适用	25	14,000	✓	标准	✓	工作负载	✗
x2idn.16large	64	1024	98,025	不适用	50	40000	✓	标准	✓	工作负载	✓
x2idn.24large	96	1,536	147,03	不适用	75	60000	✓	标准	✓	工作负载	✓
x2idn.32large	128	2,048	196,05	不适用	100	80,000	✓	标准	✓	标准	✓
x2iedn.xlarge	96	3,072	141,75	不适用	75	60000	✓	标准	✓	工作负载	✓
x2iedn.xlarge	128	4,096	189,00	不适用	100	80,000	✓	标准	✓	工作负载	✓

实例类型	vCPU	内存（GiB）	SAPS	aSAPS	网络（Gbps	存储空间（Mbps）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	FSx 适用于 ONTAP
x8i.12xrge	48	768	116,28	17,950	22.5	15000	✓	标准	✓	标准	✓
x8i.16xrge	64	1024	147,37	23,933	30	20000	✓	标准	✓	标准	✓
x8i.24xrge	96	1536	217,82	35,900	40	30000	✓	标准	✓	标准	✓
x8i.32xrge	128	2048	290,42	47,867	50	40000	✓	标准	✓	标准	✓
x8i.48xrge	192	3172	413,37	71,800	75	60000	✓	标准	✓	标准	✓
x8i.64xrge	256	4096	551,22	95,733	80	70,000	✓	标准	✓	标准	✓
x8i.96xrge	384	6144	733,80	143,60	100	80,000	✓	标准	✓	标准	✓

SAP HANA OLTP 和 OLAP 横向扩展

实例类型	vCPU	内存（GiB	SAPS	aSAP	网络（Gbp	存储空间（Mbp）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	OLTP 最大节点数	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	OLAP 最大节点数	FSx 适用于 ONTAP
r5.24x ge	96	768	138,7	不适用	25	19000	✗	不适用	不适用	✓	标准	16	✗
r6i.24 rge	96	768	147,0	不适用	37.5	30000	✗	不适用	不适用	✓	标准	16	✓
r6i.32 rge	128	1024	196,0	不适用	50	40000	✗	不适用	不适用	✓	标准	16	✓
u-6tb1 xlarge	224	6,144	38077	不适用	100	38,00	✓	标准	4	✓	工作负载	16	✓
u-6tb1 2xlarg	448	6,144	475,5	不适用	100	38,00	✓	标准	4	✓	标准	16	✓
u-6tb1 tal	448	6,144	480,6	不适用	100	38,00	✓	标准	4	✓	标准	16	✗
u-9tb1 2xlarg	448	9,216	475,5	不适用	100	38,00	✓	标准	4	✓	工作	16	✓

实例类型	vCPU	内存（GiB	SAPS	aSAP	网络（Gbp	存储空间（Mbp）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	OLTP 最大节点数	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	OLAP 最大节点数	FSx 适用于 ONTAP
											负载		
u-12tb 12xlar	448	12,28	475,5	不适用	100	38,00	✓	标准	4	✓	工作负载	16	✓
u-12tb etal	448	12,28	480,6	不适用	100	38,00	✓	标准	4	✗	不适用	不适用	✗
u7i-6t 12xlar	448	6,144	670,2	不适用	100	60000	✗	不适用	不适用	✓	标准	16	✗
u7i-8t 12xlar	448	8192	674,9	不适用	100	60000	✗	不适用	不适用	✓	标准	16	✗
u7in-1 .224xl e	896	12,28	1,254	不适用	100	60000	✓	标准	4	✓	标准	8	✓
u7in-1 .224xl e	896	16,38	1,281	不适用	200	10000	✓	标准	4	✓	标准	8	✓

实例类型	vCPU	内存（GiB	SAPS	aSAP	网络（Gbp	存储空间（Mbp）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	OLTP 最大节点数	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	OLAP 最大节点数	FSx 适用于 ONTAP
u7in-2 .224xl e	896	24576	1,225	不适用	200	10000	✓	工作负载	4	✓	工作负载	8	✓
u7inh- b.480 ge	1,920	32,76	不适用	不适用	200	16000	✓	标准	4	✓	工作负载	8	✗
x1.16 ge	64	976	65,75	不适用	10	7,000	✗	不适用	不适用	✓	标准	7	✗
x1.32 ge	128	1,952	131,5	不适用	25	14,00	✗	不适用	不适用	✓	标准	25	✗
x1e.3 rge	128	3,904	131,5	不适用	25	14,00	✗	不适用	不适用	✓	工作负载	25	✗
x2idn. large	64	1024	98,02	不适用	50	40000	✗	不适用	不适用	✓	标准	16	✓

实例类型	vCPU	内存（GiB	SAPS	aSAP	网络（Gbp	存储空间（Mbp）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	OLTP 最大节点数	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	OLAP 最大节点数	FSx 适用于 ONTAP
x2idn.large	96	1,536	147,0	不适用	75	60000	✗	不适用	不适用	✓	工作负载	16	✓
x2idn.large	128	2,048	196,0	不适用	100	80,00	✗	不适用	不适用	✓	工作负载	16	✓
x2iedn xlarge	96	3,072	141,7	不适用	75	60000	✗	不适用	不适用	✓	工作负载	16	✓
x2iedn xlarge	128	4,096	189,0	不适用	100	80,00	✗	不适用	不适用	✓	工作负载	16	✓
x8i.16rge	64	1024	147,3	23,93	30	20000	✗	不适用	不适用	✓	标准	16	✓
x8i.24rge	96	1,536	217,8	35,90	40	30000	✗	不适用	不适用	✓	标准	16	✓

实例类型	vCPU	内存（GiB	SAPS	aSAP	网络（Gbp	存储空间（Mbp）	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	OLTP 最大节点数	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整	OLAP 最大节点数	FSx 适用于 ONTAP
x8i.32rge	128	2,048	290,4	47,86	50	40000	✗	不适用	不适用	✓	标准	16	✓
x8i.48rge	192	3,172	413,3	71,80	75	60000	✗	不适用	不适用	✓	标准	16	✓
x8i.64rge	256	4,096	551,2	95,73	80	70,00	✗	不适用	不适用	✓	标准	16	✓
x8i.96rge	384	6,144	733,8	143,6	100	80,00	✗	不适用	不适用	✓	标准	16	✓

上一代认证实例

SAP HANA OLTP 和 OLAP 纵向扩展

实例类型	vCPU	内存（GiB）	SAPS	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整
r3.2xlarge	8	61	7,980	✗	标准	✗	标准

实例类型	vCPU	内存（GiB）	SAPS	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整
r3.4xlarge	16	122	15,960	✗	标准	✗	标准
r3.8xlarge	32	244	31,920	✓	标准	✓	标准
r4.8xlarge	32	244	38,200	10	7,000	✓	标准
r4.16xlarge	64	488	76,400	25	14,000	✓	标准

SAP HANA OLTP 和 OLAP 横向扩展

实例类型	vCPU	内存（GiB）	SAPS	SAP HANA OLTP 生产	SAP HANA OLTP 大小调整	SAP HANA OLAP 生产	SAP HANA OLAP 大小调整
r3.8xlarge	32	244	31,920	✗	不适用	✓	标准

未认证实例

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 – Cost-Optimized SAP HANA Hardware for Non-Production Usage（需要 SAP 门户访问权限）。

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	✗
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	最高 20000	✗
x2iedn.4xlarge	16	512	23,625	最多 25	最多 20,000	✗

实例类型	vCPU	内存（GiB）	SAPS	网络（Gbps）	存储空间（Mbps）	FSx 适用于 ONTAP
x2iedn.8xlarge	32	1024	47,250	25	20000	✗
x2iedn.16xlarge	64	2,048	94,500	50	40000	✗

SAP Business One 认证实例，适用于 SAP HANA 的版本

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
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

实例类型	vCPU	内存（GiB）	SAPS	最大并发用户数
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
在 SAP 中添加了 m8a 和 r8a NetWeaver	2026 年 1 月
在 SAP NetWeaver 和 SAP HANA 中添加了 x8i	2026 年 1 月
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

更改	日期
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
将 X2idn 和 R6i 添加到 SAP HANA OLAP 横向扩展	2022 年 6 月
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。通过此工具，这些数据可供 SAP 应用程序使用，来帮助监控并改善业务事务的性能。SAP 要求客户按照 SAP Note 1656250 中的说明安装代理（需要登录凭证）。

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。

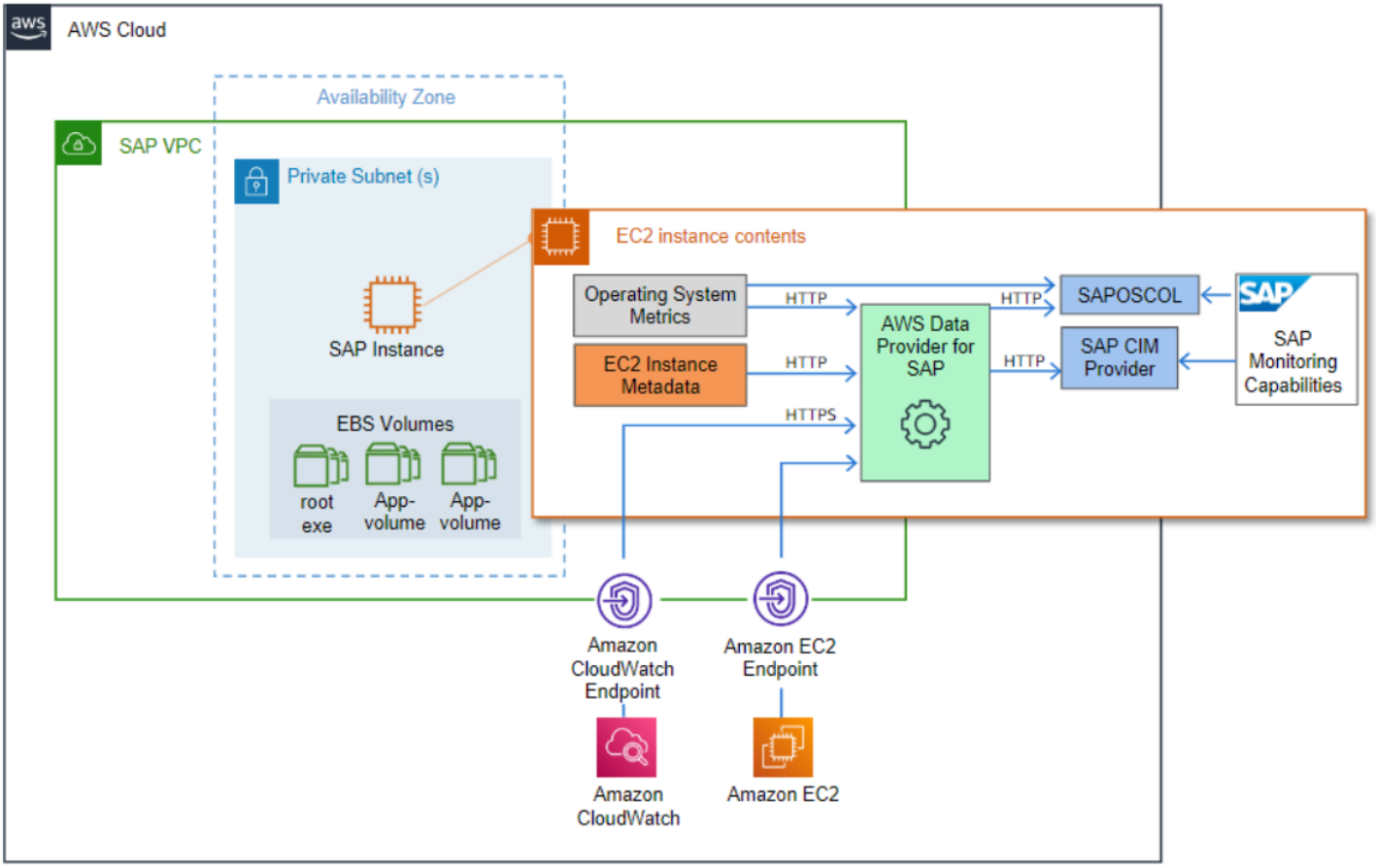
简介

许多不同规模的企业选择在 Amazon Web Services 云端托管关键 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。这样，企业就可以将更多的资源（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，对企业运营至关重要。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。这些数据是从您的 AWS 云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 SAP 基础设施相关的操作系统、网络和存储信息。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。
- 排查安装问题。

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相关的间接成本。这会导致频繁GetMetric调用 Amazon CloudWatch 和 Amazon EC2 API 来检索指标数据。 DataProvider 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，根据连接到 Amazon EC2 实例的磁盘数量会有所不同。

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 端点（监控、Amazon EC2）的费用约为每处理 1 GB 数据 14.00 美元 + 0.01 美元。

> **Note**
>
> 这些端点只需创建一次，由整个环境共享。如果您已在使用这些端点，则无需重新创建。

每个系统：

- 预计每个实例每天大约有 70000 个 API 调用（连接 6 个磁盘）。按每 1000 次调用 0.01 美元计算，约为每月 21.00 美元。根据所连接的磁盘数量，API 调用次数会增加或减少。

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

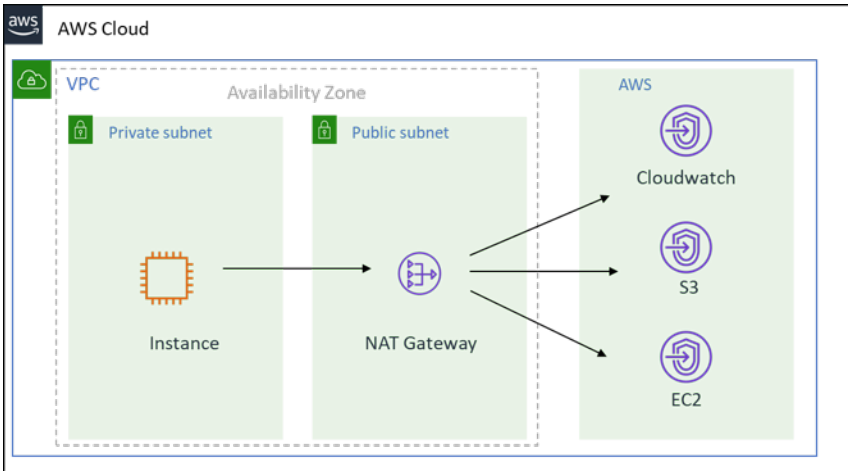
- Amazon VPC 网络拓扑
- Amazon VPC 端点
- IAM 角色

Amazon 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互联网中端点的路由：

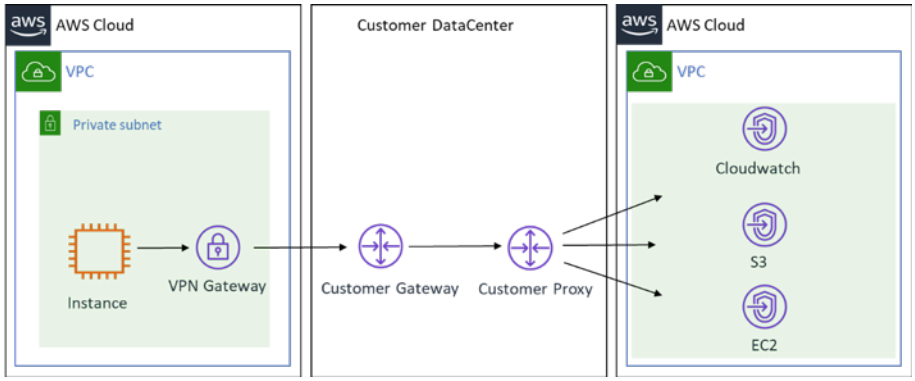
- 第一个拓扑结构配置通过 Amazon VPC 内的 NAT 网关直接进入 AWS 云的路由和流量。有关互联网网关的更多信息，请参阅 AWS 文档。

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到 Amazon 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，导航到端点，然后选择创建端点。
2. 在下一个屏幕上，搜索服务名称，选择相应的 VPC 和路由表，然后选择创建端点。
3. 创建完所有三个端点后，您应该会在端点列表中看到它们，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 和 Amazon EC2 服务的只读访问权限，这样您才能使用它们。 APIs为此，您可以为您的 Amazon EC2 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，向您的 Amazon EC2 实例授予权限：

1. 登录 AWS 管理控制台，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 作为使用案例，然后选择下一步：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，然后选择查看策略。

> **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 控制台发送类似于下文的消息来确认新策略。
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如有需要可添加任意标签，否则请选择下一步：查看。
12提供角色的名称，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。

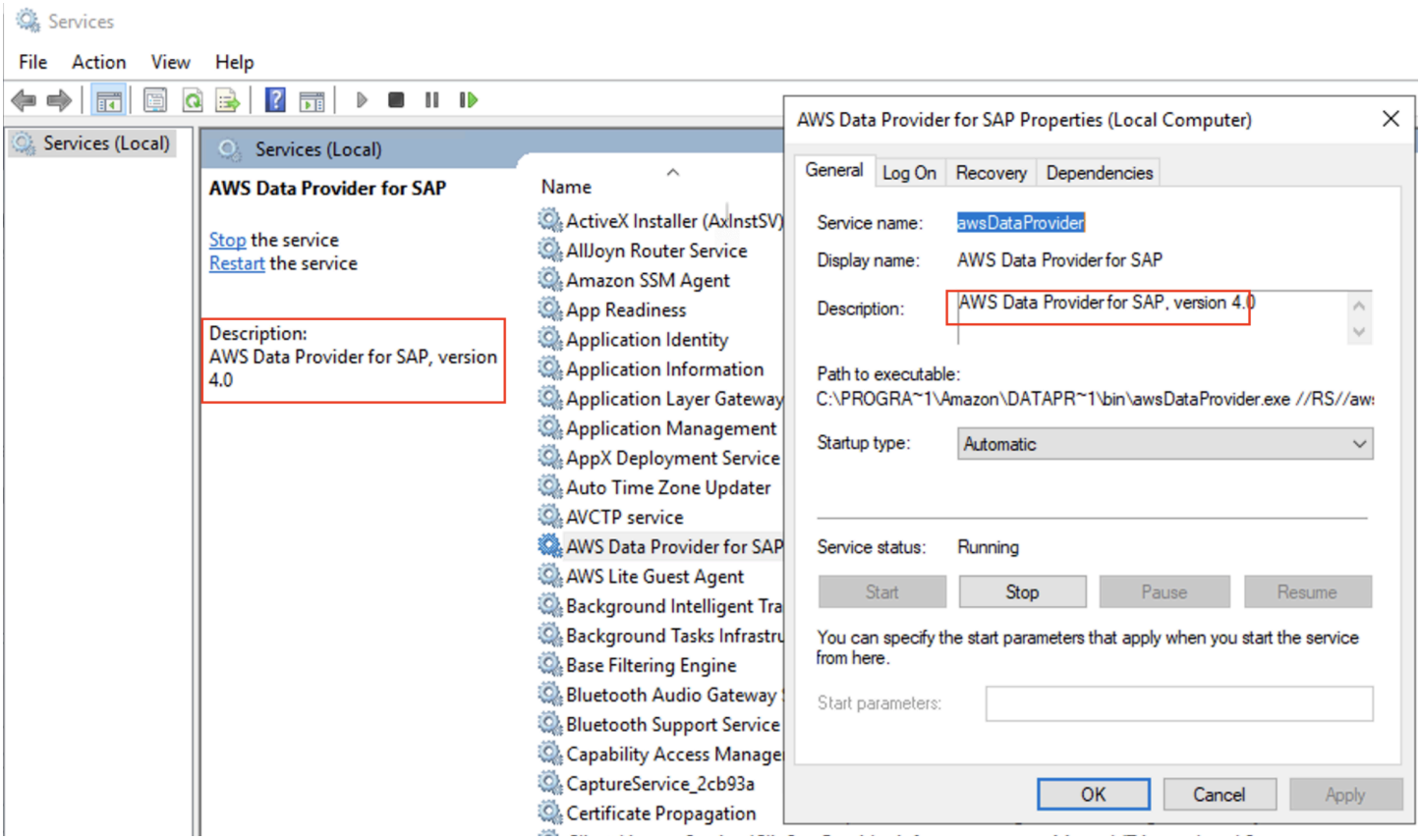
如果您的系统上安装了旧版本，请参阅卸载旧版本。

> **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。指标来自各种提供程序，这些提供程序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。对于无法访问的指标，提供程序会返回空白值。

例如，如果您的 Amazon EC2 实例没有与其关联的 IAM 角色来授予对 Amazon CloudWatch GetMetricStatisticsAPI 的显式访问权限，则 CloudWatch 提供商将无法在 Amazon EC2 实例上执行操作，并将返回空值。GetMetricStatistics

每个 SAP 生产系统上都需要安装该提供程序，才有资格获得 SAP 支持。一个系统上一次只能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 发行商安装 — 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 Red Hat Enterprise Linux 实例上手动安装 SSM Agent
- SUSE：在 SUSE Linux Enterprise Server 实例上手动安装 SSM Agent
- Oracle：在 Oracle Linux 实例上手动安装 SSM Agent
- Windows：在适用于 Windows Server 的 EC2 实例上手动安装载 SSM Agent

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，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：

- Amazon Corretto 8 或 OpenJDK 8
- Amazon Corretto 11 或 OpenJDK 11
- Amazon Corretto 17 或 OpenJDK 17

有关如何在 Amazon EC2 实例上下载和安装 JDK 的详细信息，请参阅 Amazon Corretto 文档。

在终端上，运行以下命令来验证安装。

```
java -version
```

例如，Coretto-8.252.09.1 的预期输出应为：

```
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 URL：GPG 密钥
- 登录到 SUSE 实例并运行以下命令来导入密钥：

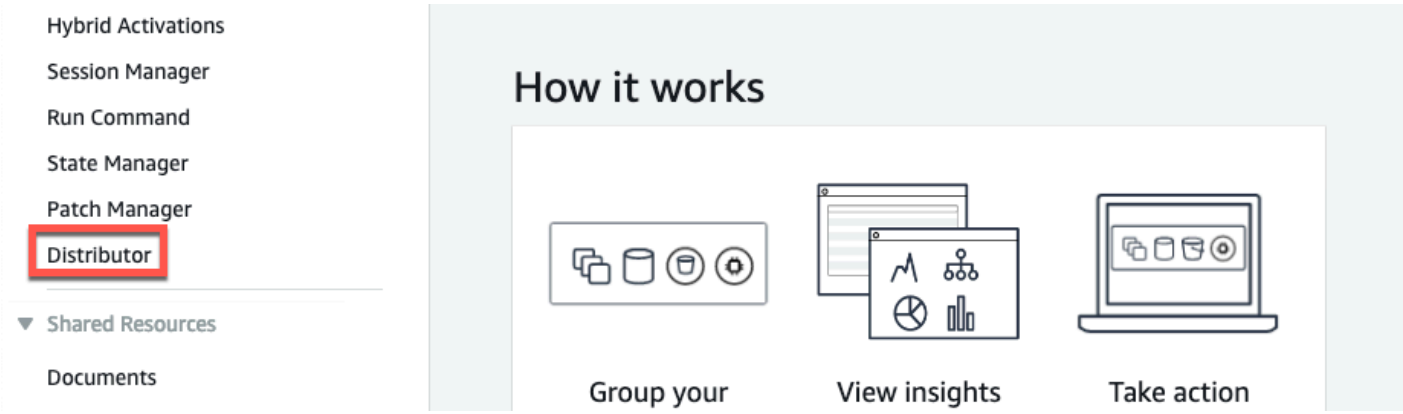
```
wget https//<url to GPG key>
```

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

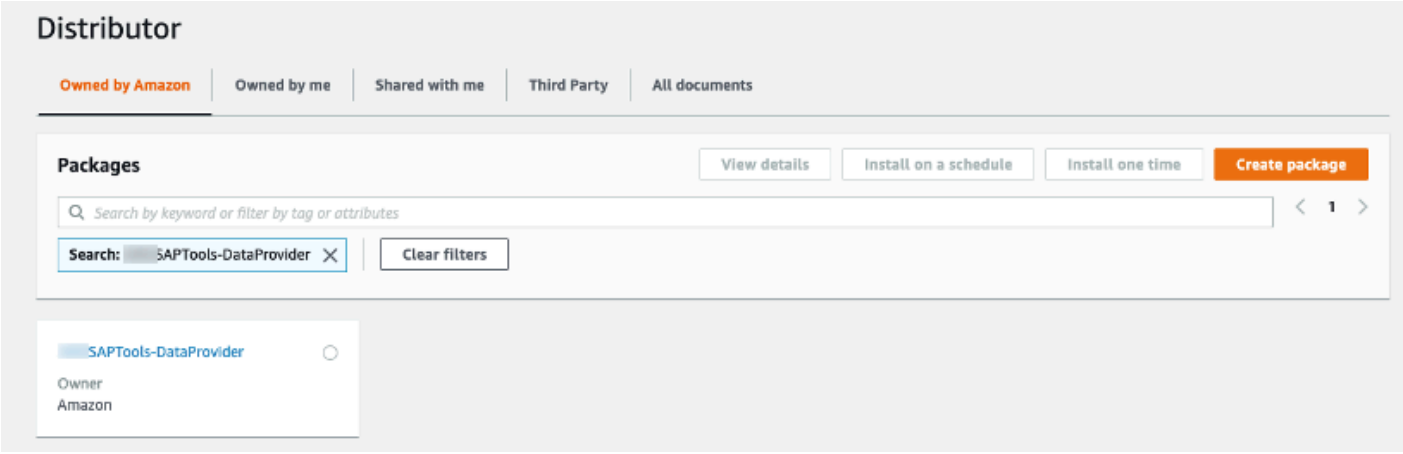
使用 SSM 分发服务器安装 DataProvider 代理

使用以下步骤安装 DataProvider 4.3。

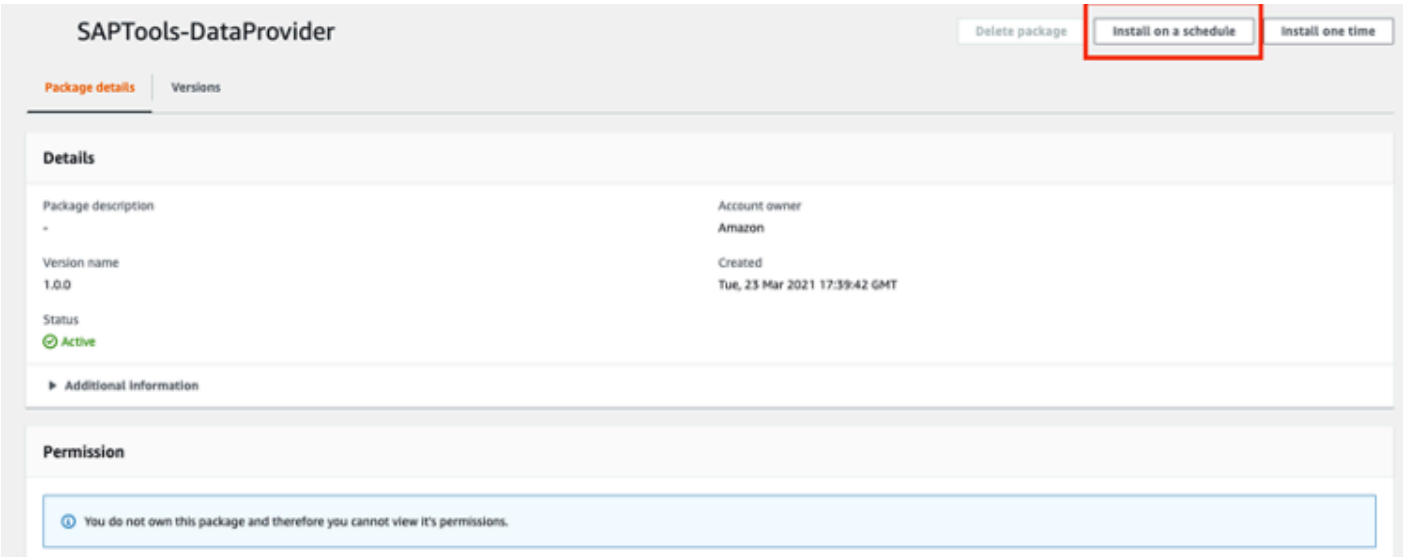
1. 打开 Systems Manager 控制台。
2. 在左侧导航窗格中的“节点管理”部分下，选择分发服务器。



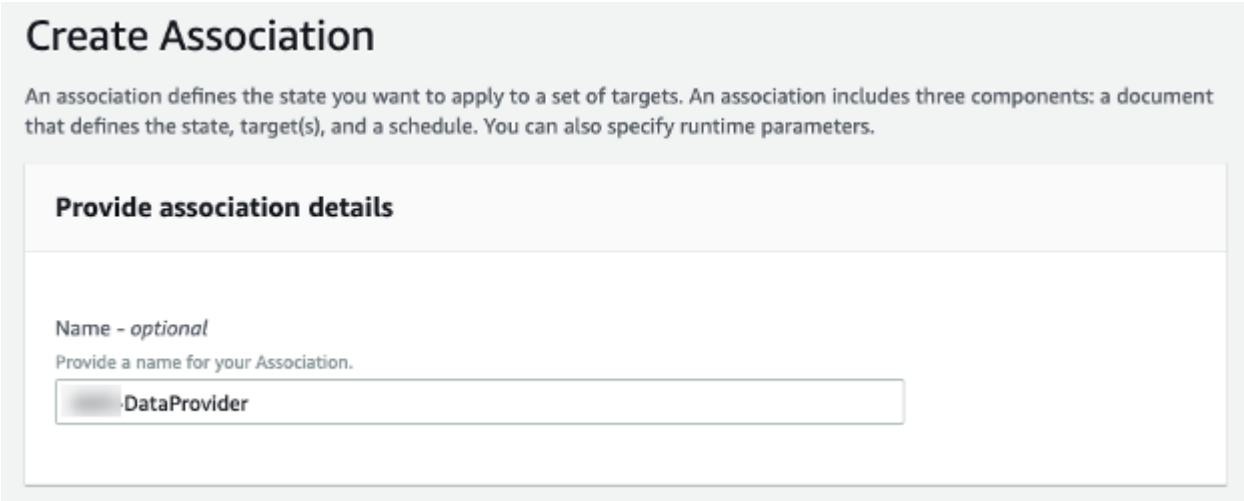
3. 在搜索栏中 AWSSAPTools-DataProvider，键入并选择软件包。



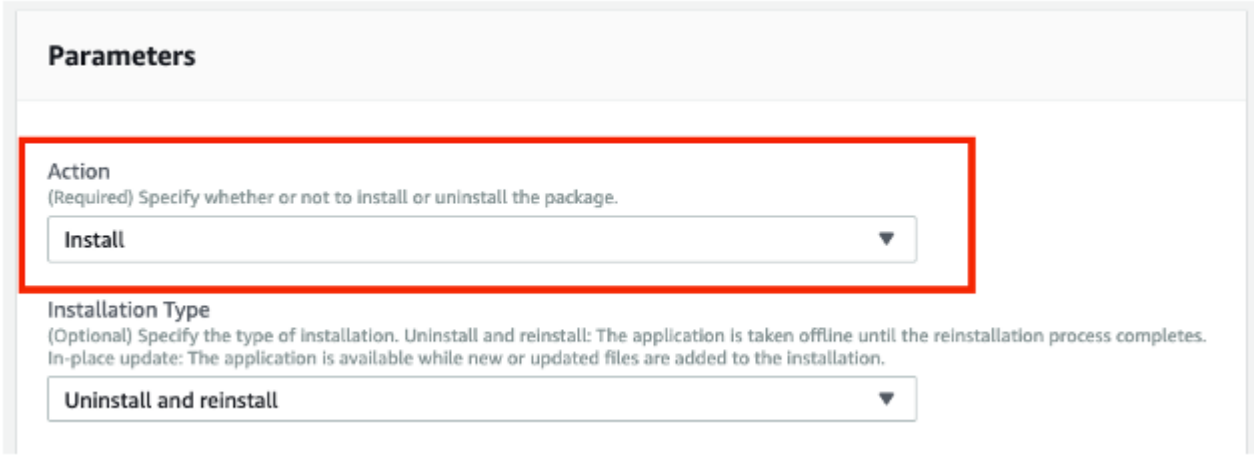
4. 要在新版本发布 DataProvider 时接收自动更新，请选择 “按计划安装”。



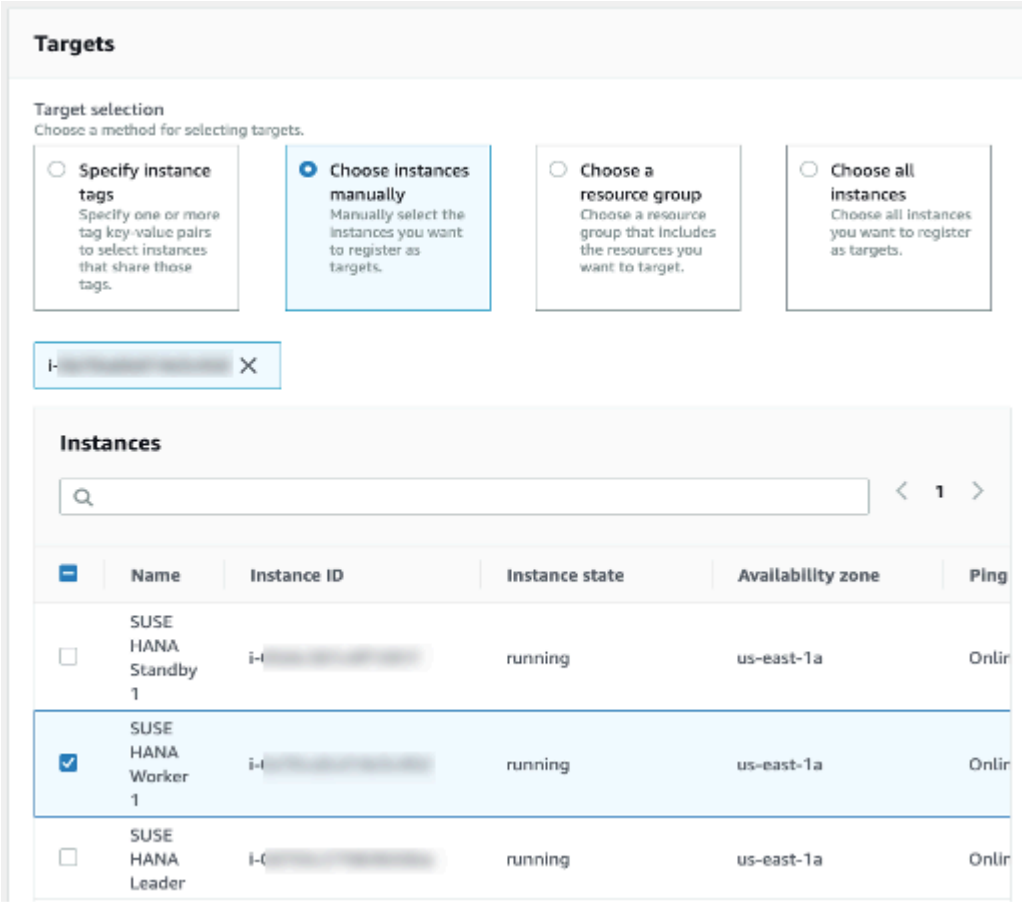
5. 在创建关联页面上，键入关联的名称。



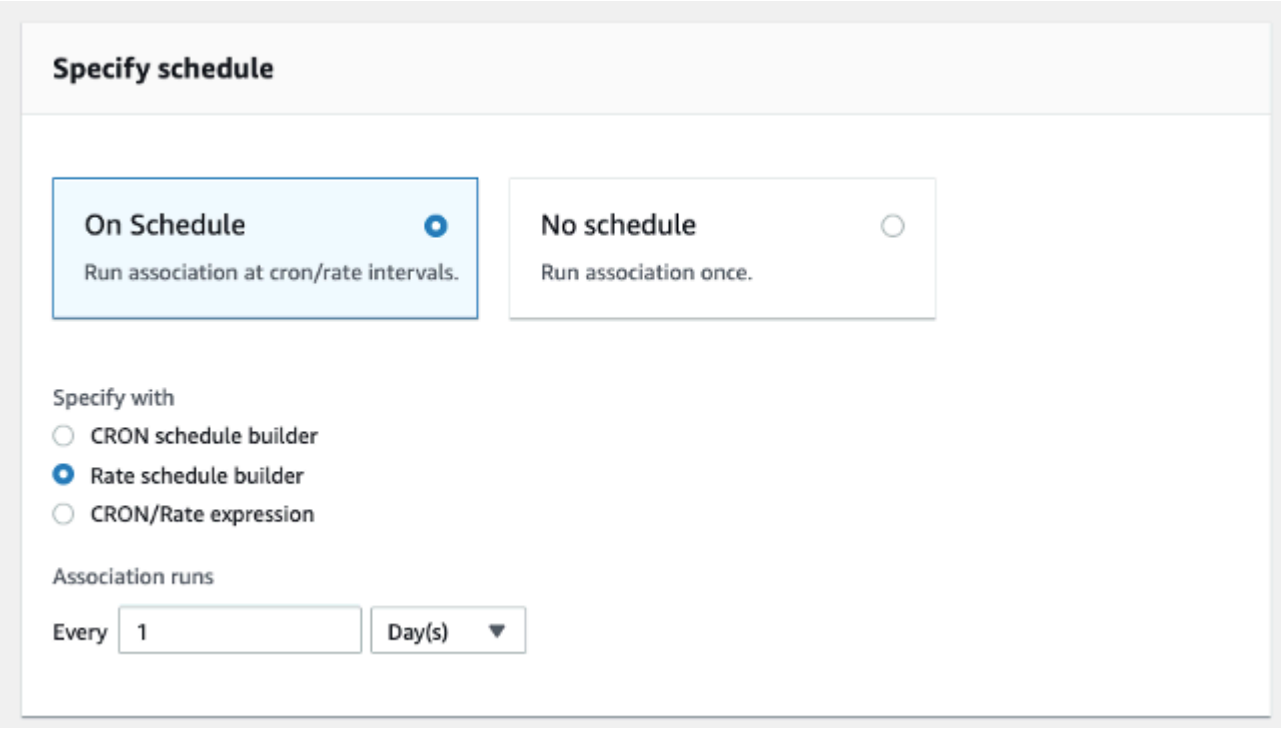
6. 在参数部分，对于操作选择安装。



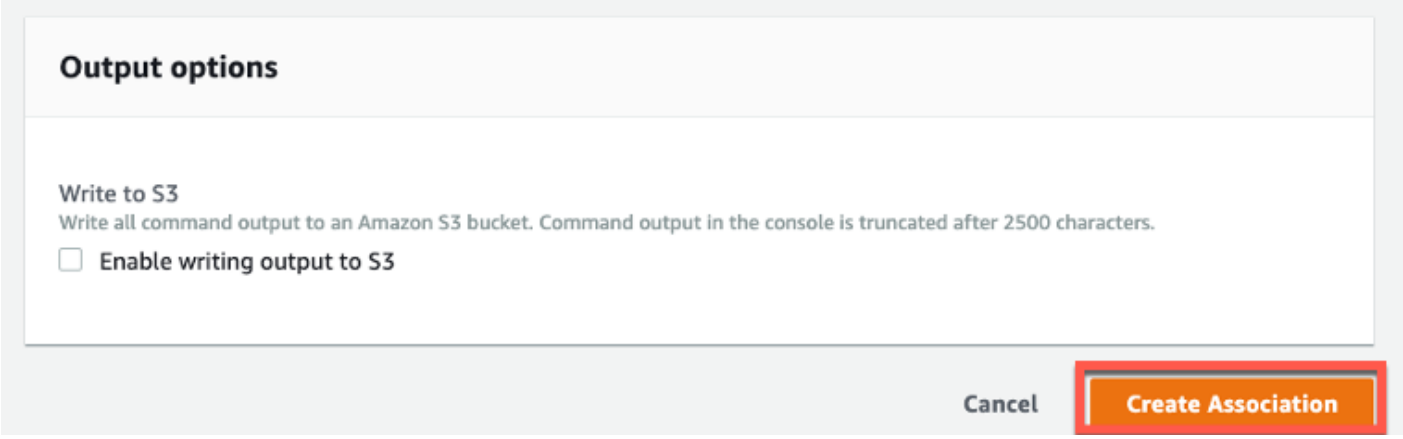
7. 在目标部分，对于目标选择，选择手动选择实例。然后，选择要安装的实例 DataProvider。



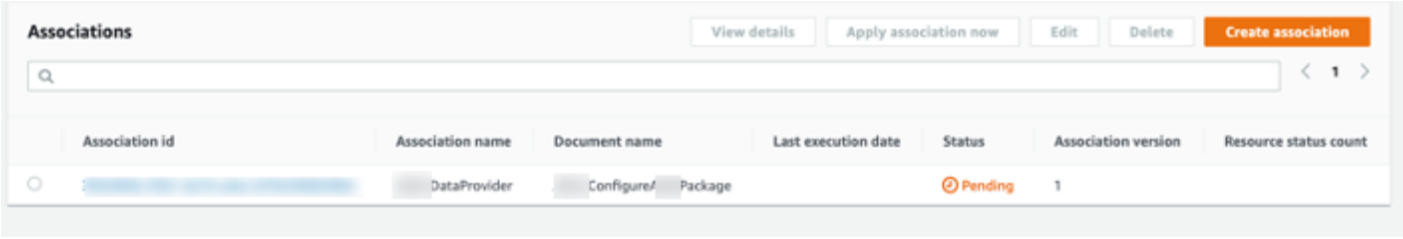
8. 在指定计划部分中，进行以下选择：
   - 选择按计划。
   - 对于指定方式，选择 Rate 计划生成器。
   - 对于助理跑步，请选择 30 天。（AWS 建议 30 天）



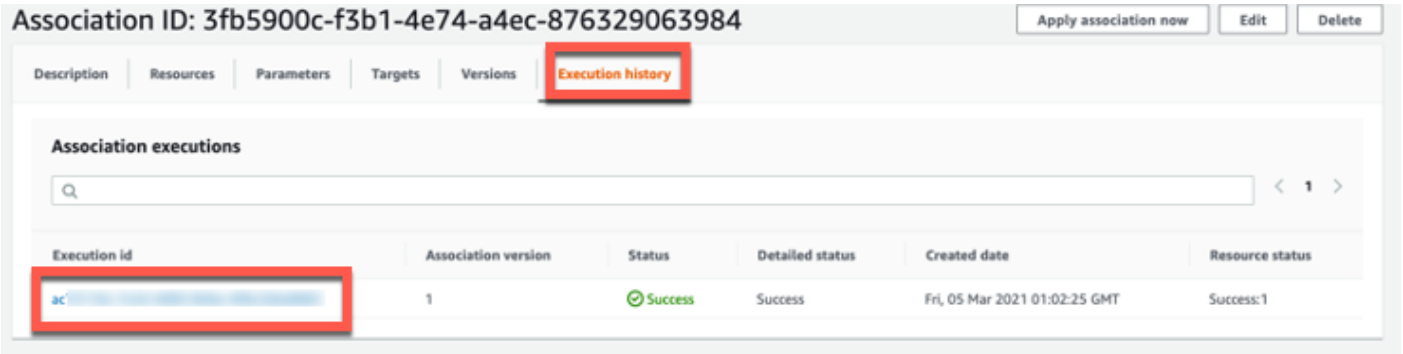
9. 在输出选项部分，选择创建关联。



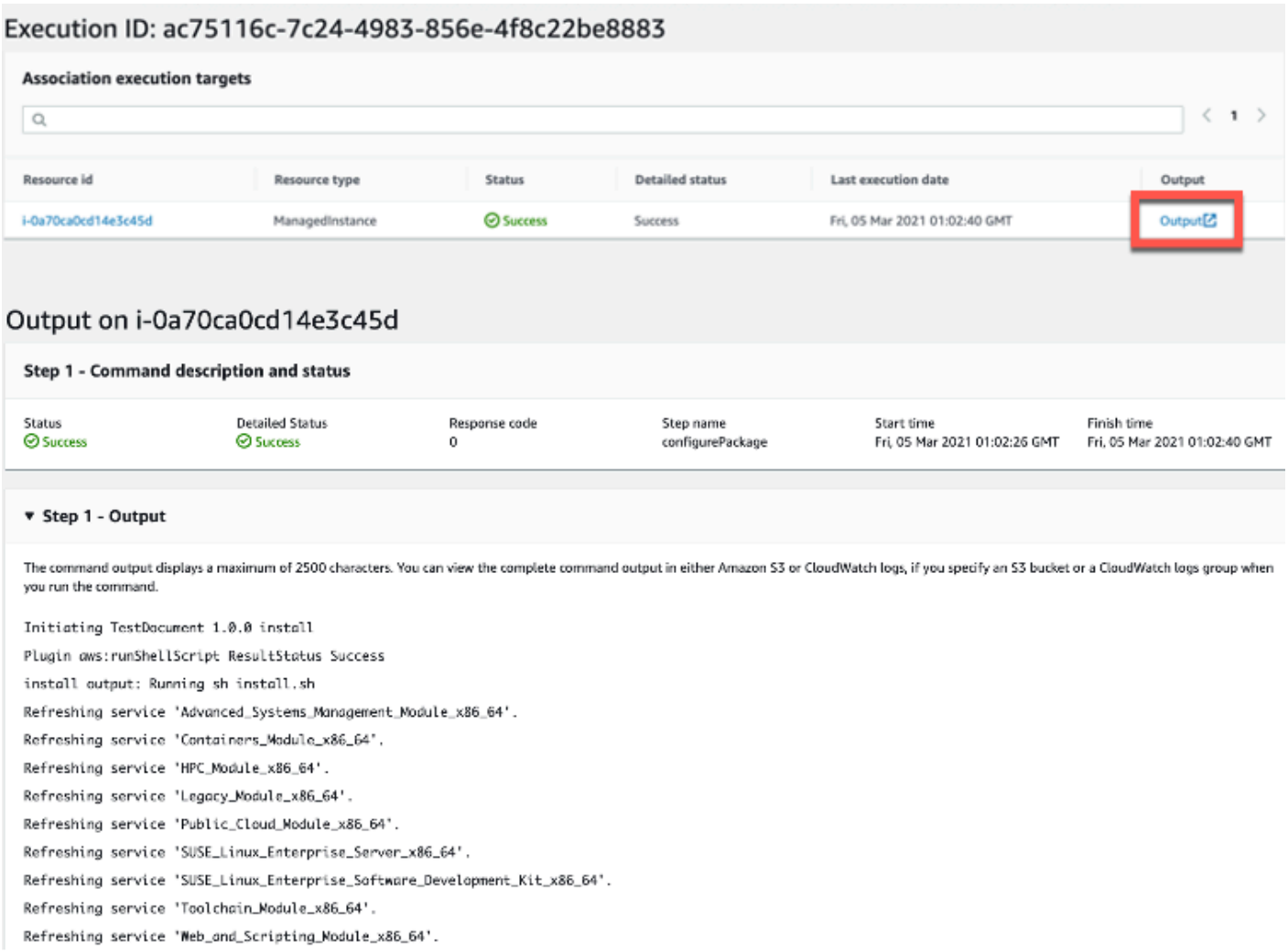
10.创建关联后，选择关联 ID。



11选择执行历史记录选项卡。然后，选择“执行 ID”。



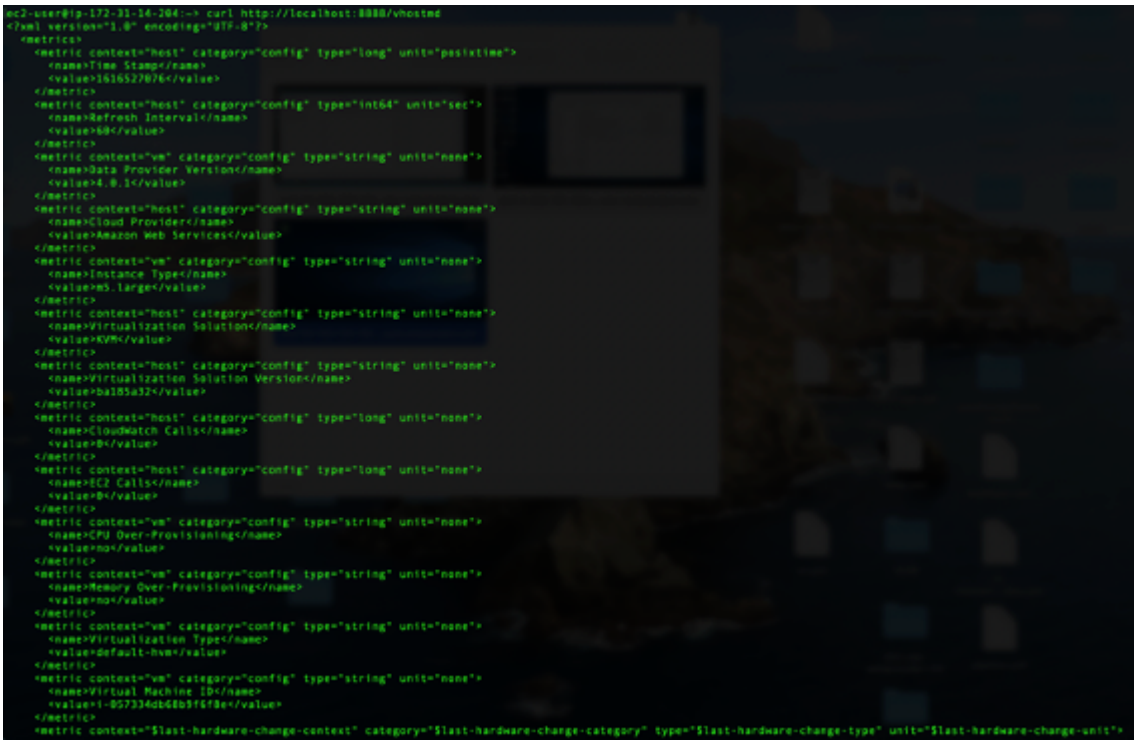
12.在执行 ID 页面上，选择输出以查看安装结果。



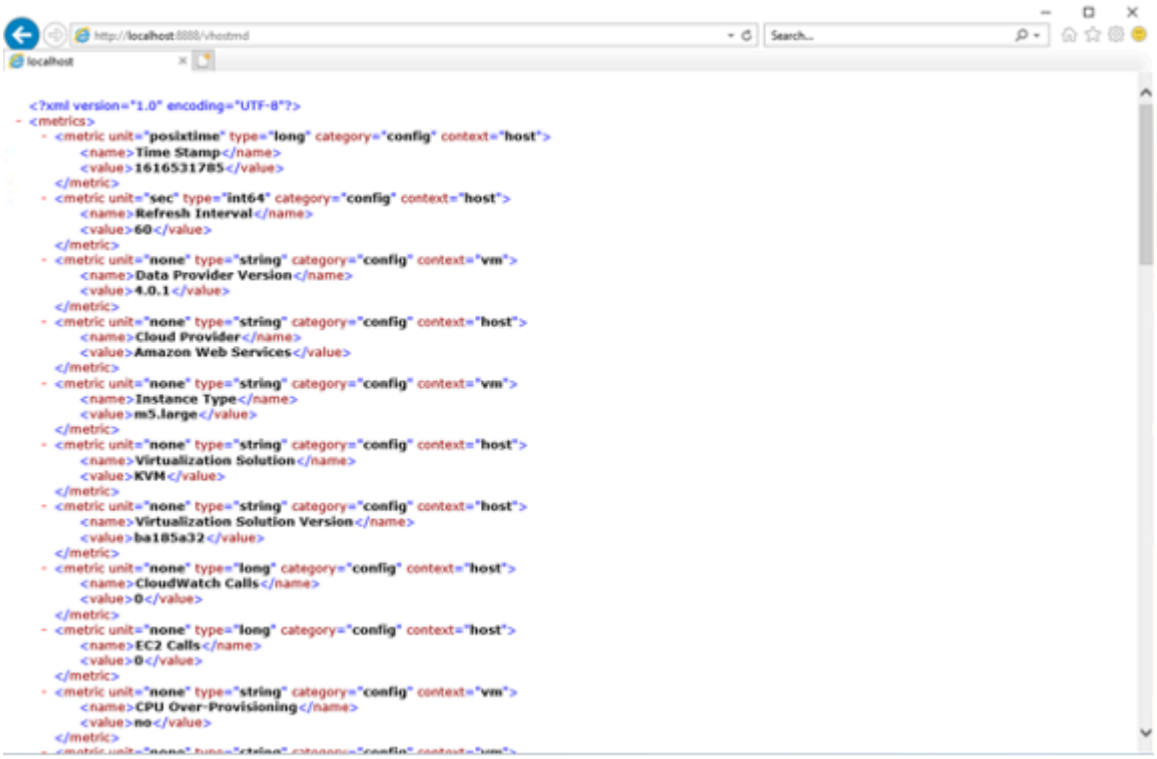

```
The following NEW package is going to be installed:
aws-sap-dataprovider-standalone

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。您不需要安装 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，如果您要将文件下载到其他区域，请在下载之前更改默认区域。

- 红帽 https://aws-sap-dataprovider-us-east-1.s3.us-east-1.amazonaws.com/v4/installers/linux/RHEL/aws-sap-dataprovider-rhel-standalone.x86_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 Lin 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 软件包的形式提供。

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。

要安装数据提供程序，请运行以下命令：

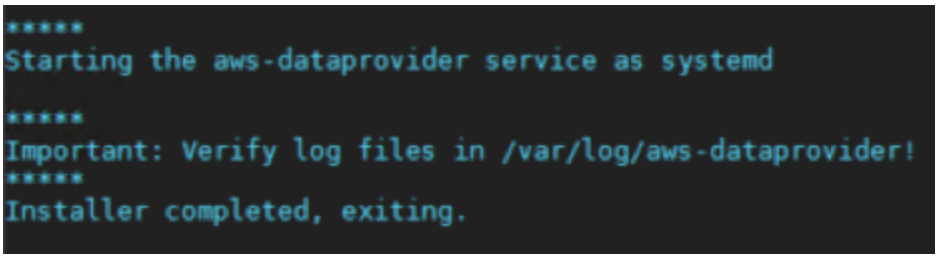
```
wget https://<url to rpm package>
wget https://<url to GPG key>
rpm --import RPM-GPG-KEY-AWS
zypper install -y <rpm package>
```

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
```

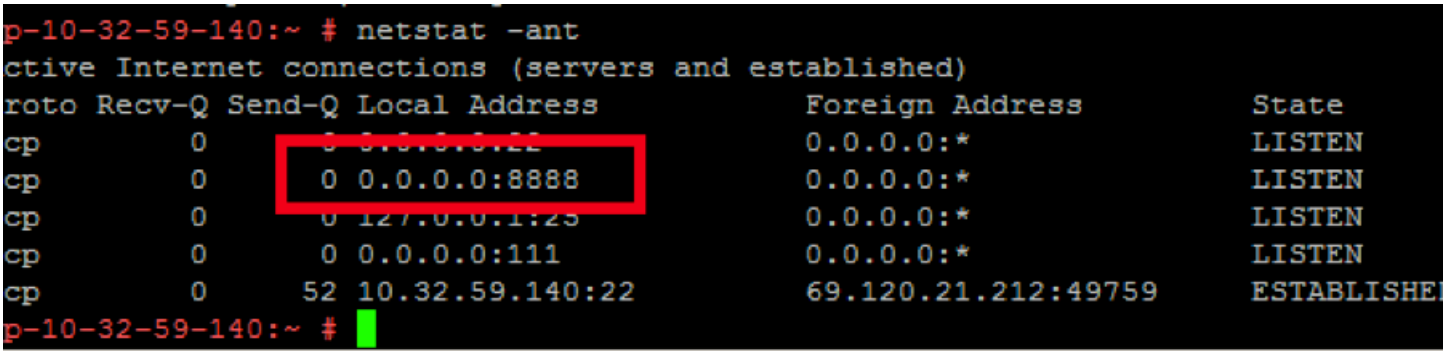
安装 RPM 软件包后，代理会作为进程守护程序启动，如下图所示。

RPM 软件包安装



调用 `netstat -ant` 以确定侦听器是否在本地主机端口 8888 上运行，来验证服务是否正在运行。

在 Linux 上验证安装情况



您还应该查看位于 `/var/log/aws-dataprovider/messages.0` 的日志文件，确保进程守护程序具有访问所需指标的相应连接和授权。

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，监控代理会运行三组诊断功能：

- 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，请参阅本指南前文中的 IAM 角色。
- 第三组诊断功能测试是否获得了访问 Amazon EC2 的授权，这同样需要将 IAM 角色关联到 Amazon EC2 实例。

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。您可以在文件中查看返回的指标，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 Red Hat Linux 6：

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

- SLES 12、SLES 15、Oracle Linux 7、Oracle Linux 8、Red Hat Linux 7 和 Red Hat Linux 8。

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

如果您无法透明地 HTTP/HTTPS 访问互联网，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 /usr/local/ec2/aws-dataprovider/proxy.properties 的文件中输入代理信息（如下所示）。

```
#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 Red Hat 和 Oracle Enterprise Linux 上进行安装

对于 Red Hat 和 Oracle Enterprise Linux，安装步骤与上述 SLES 的安装步骤相同，但 RPM 文件以及用于安装 RPM 软件包的命令有所不同。

- Red Hat

  默认值：aws-sap-dataprovider-rhel.x 86_64.rpm
- Oracle Enterprise Linux

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

要安装数据提供程序，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 Scriptable Install System，Nullsoft 可脚本化安装系统）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，验证服务是否在运行。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. 如果您无法透明地 HTTP/HTTPS 访问互联网，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 `C:\Program Files\Amazon\DataProvider\proxy.properties` 的文件中输入代理信息（如下所示）。

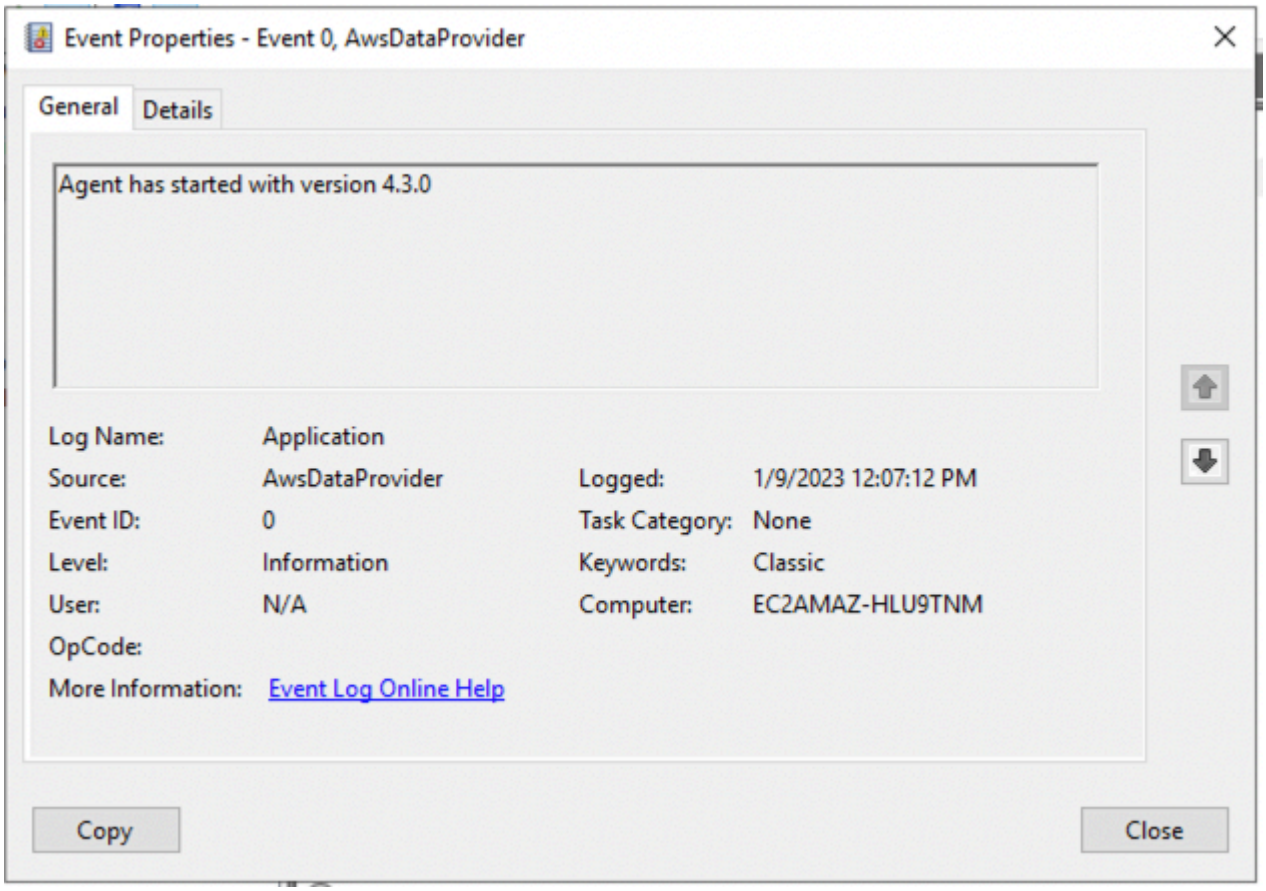
   ```
   #proxy.properties
   #used to set web proxy settings for the {aws} Data Provider for SAP
   #Https is the only supported proxy method
   #Blank values for everything means no proxy set

   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 上检查诊断信息

启动时，监控代理会运行三组诊断功能：

- 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，请参阅本指南前文中的 IAM 角色。
- 第三组诊断功能测试是否获得了访问 Amazon EC2 的授权，这同样需要将 IAM 角色关联到 Amazon EC2 实例。

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 会返回空白值。

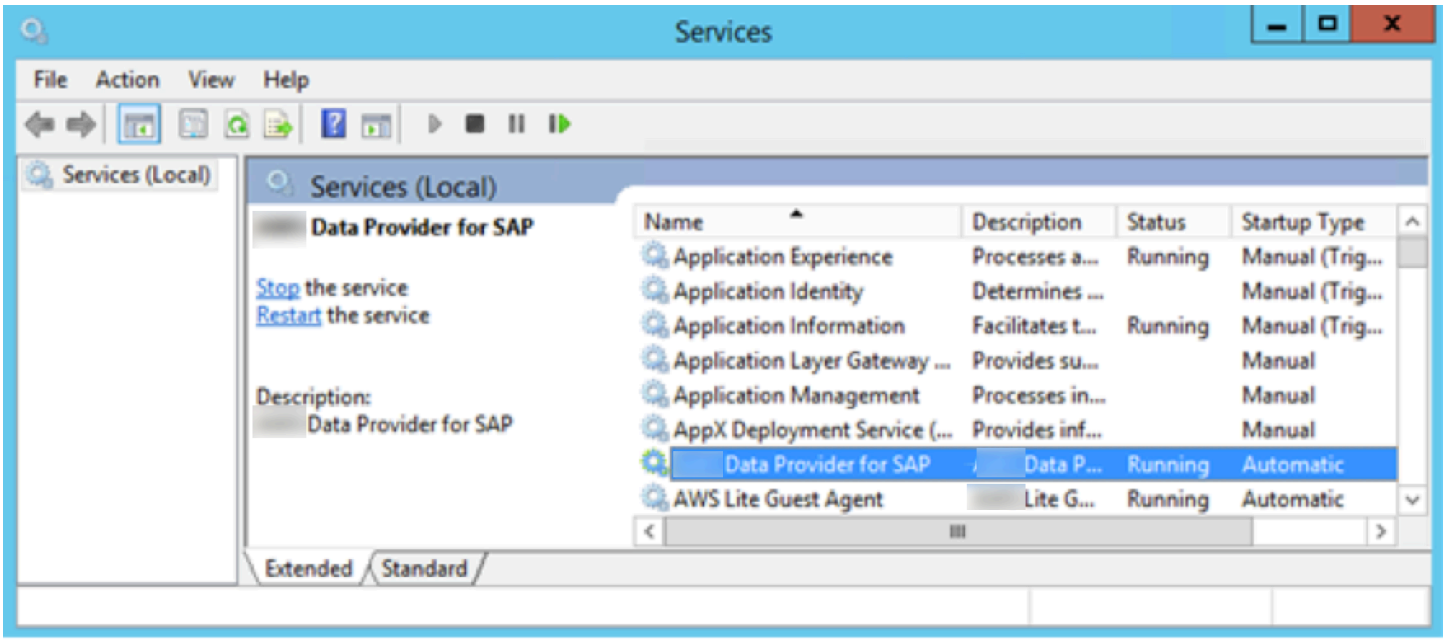
您也可以直接从 Web 浏览器调用 SAP AWS 数据提供程序来查看指标，如图所示。

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，您可以将自定义 `proxy.properties` 文件放在 Windows 的临时目录中，该目录通过 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. 确保您位于美国东部（弗吉尼亚州北部）（us-east-1）区域。
3. 在左侧导航窗格中，依次选择订阅 > 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。

Region	进行筛选
默认	`arn:aws:sns:us-east-1:804845276281:AWS-DataProvider-SAP-Update`

Region	进行筛选
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）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 SMS。
   - 电子邮件：在端点字段中，输入您想要用于接收通知的电子邮件地址。

     > **Note**
     >
     > 要启用电子邮件通知，您必须按照在所提供的电子邮件地址中收到的说明，确认您的电子邮件订阅。

   - SMS：在端点字段中，输入您想要用于接收通知的手机号码。
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，请使用以下步骤。

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. 从订阅列表中选择该订阅，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 分发包更新到 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。

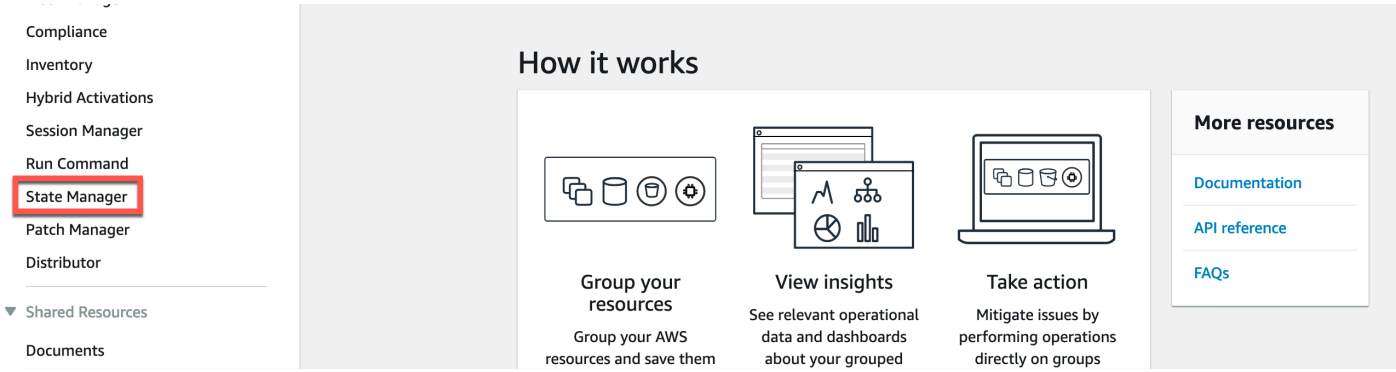
要手动更新 DataProvider 4.3，必须先卸载正在运行的版本，然后安装更新的版本。

DataProvider 4.3 不支持以下操作：

- 如果是使用 SSM 发行版安装的 DataProvider ，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。

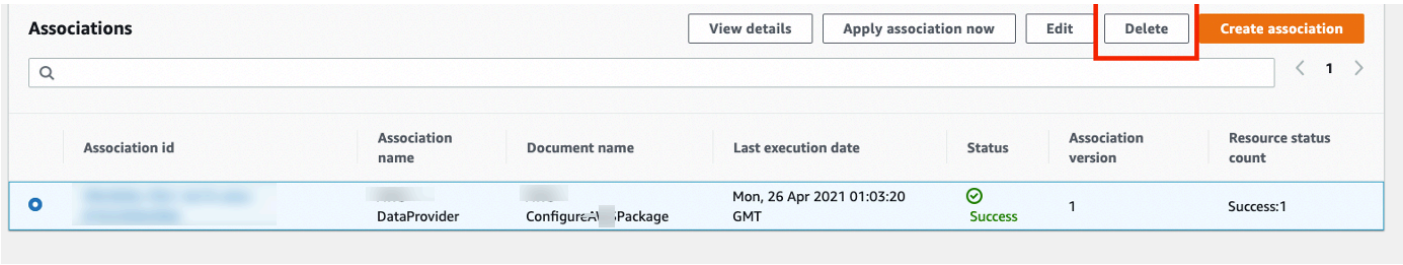
使用 SSM 发行版卸载 DataProvider 4.3

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

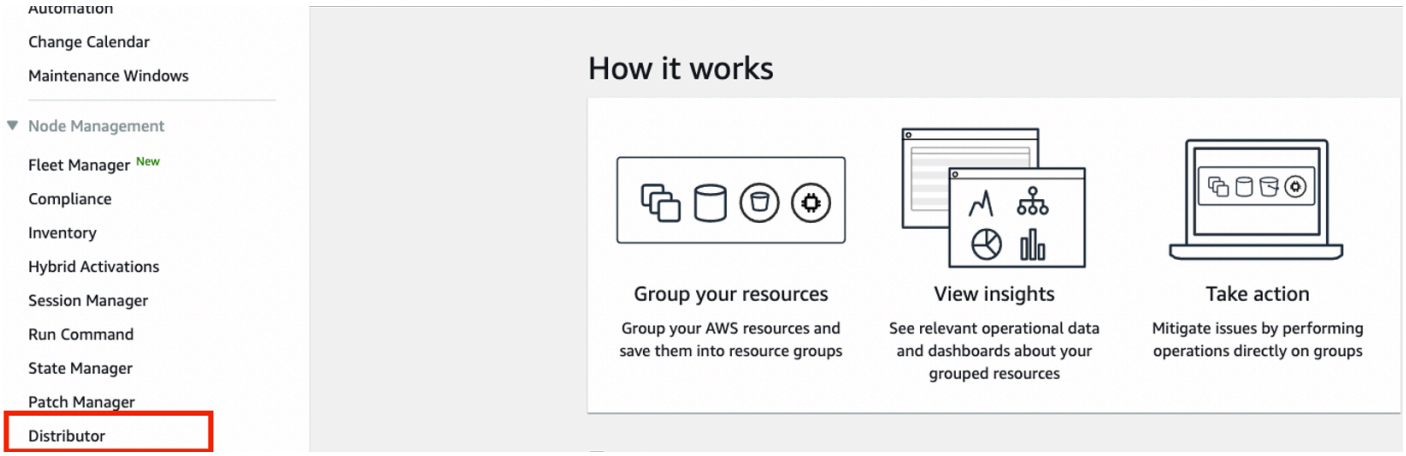


2. 在关联页面上，选择关联 ID。然后选择 Delete(删除)。

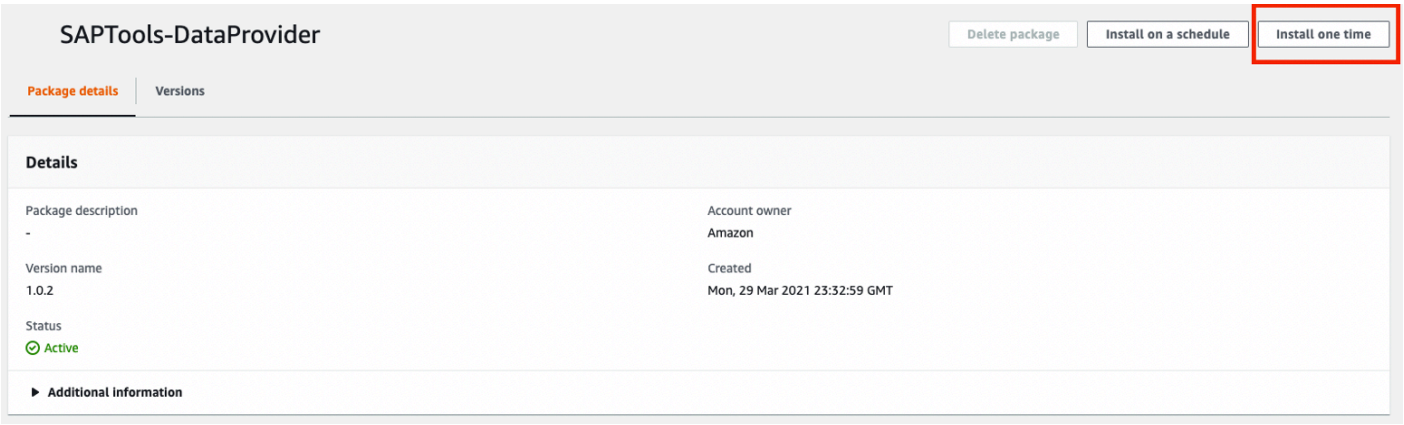
   成功完成删除后，自动更新将停止。



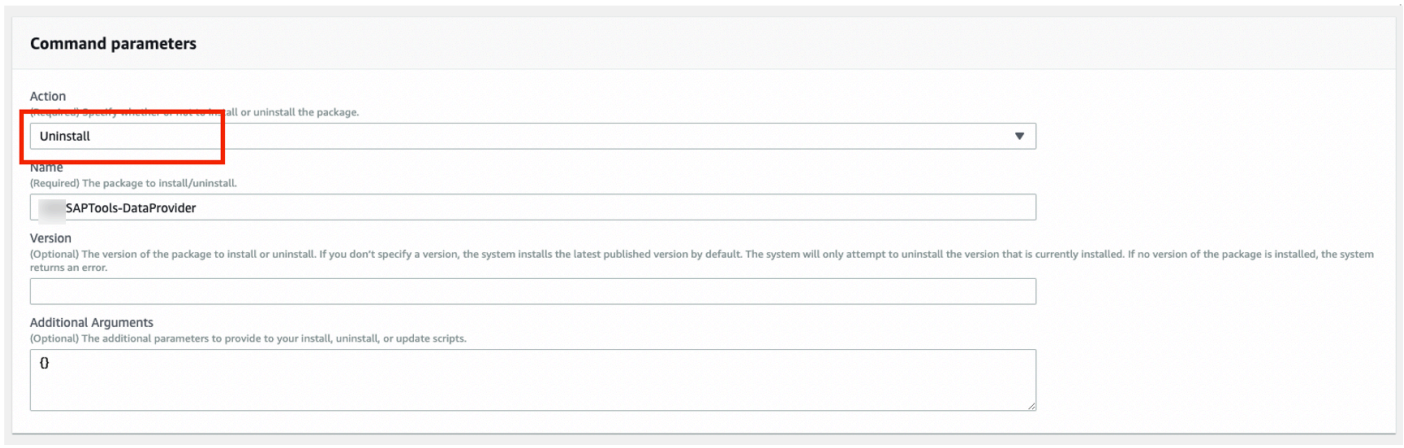
3. 在主页面上的左侧导航页面中，选择分发服务器。



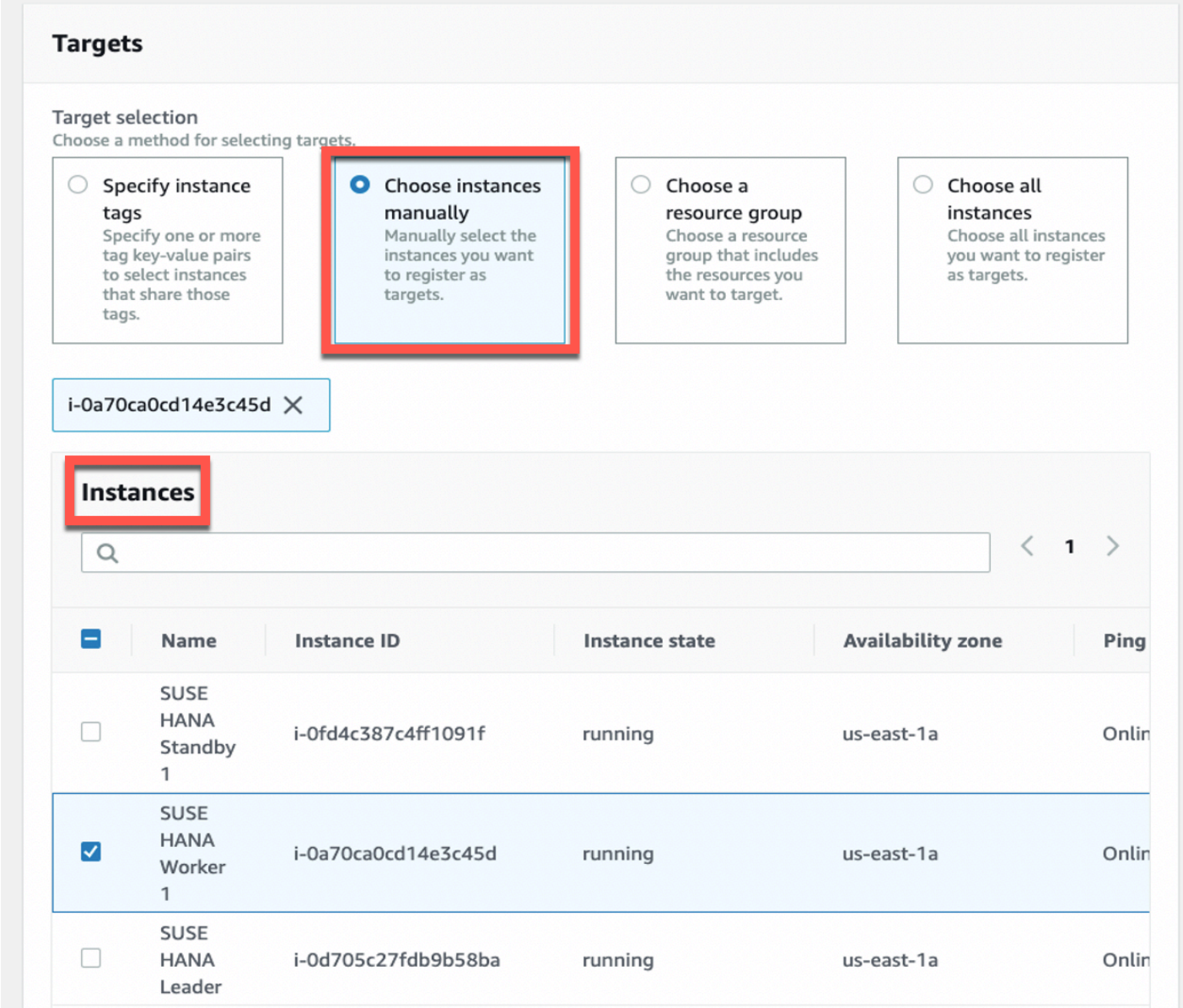
4. 选择分AWSSAPTools-DataProvider销商软件包，然后选择一次安装。



5. 在命令参数部分，选择卸载。



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



7. 选择运行以开始卸载。

手动卸载 DataProvider 4.3

RedHat

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

SUSE

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

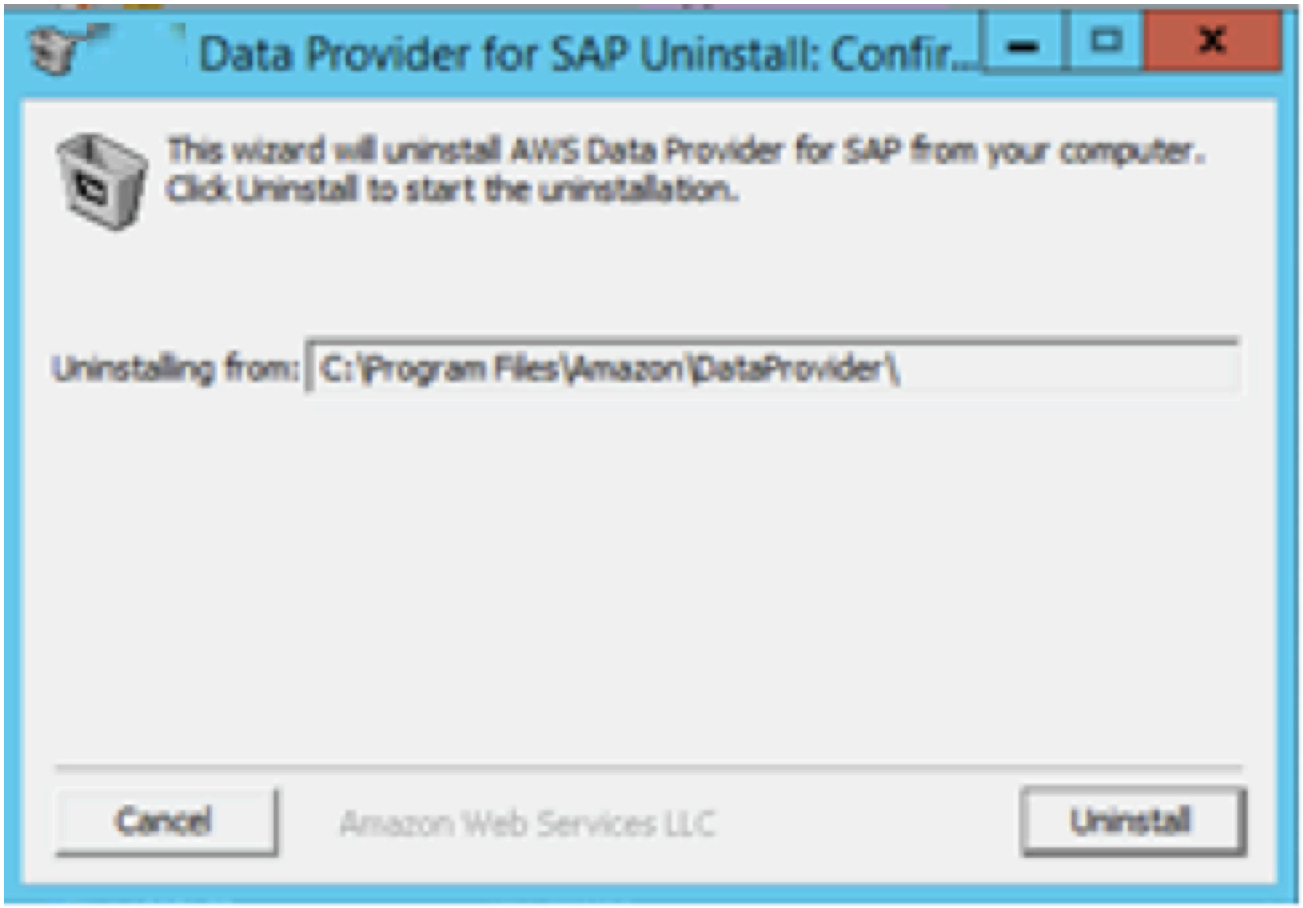
Windows

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



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“
```

问题排查

此部分提供用于分析安装问题的帮助。

在 Linux 上进行故障排除

问题：安装失败，我不确定文件是否处于一致的状态。

使用以下命令停止并删除数据提供程序。

SLES：

```
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 /var/log/aws-dataprovider 中的日志文件，获取哪些地方没有正常运行的提示。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，当您运行服务 aws-dataprovider-start 或 systemctl start aws-dataprovider 时，会收到大量调试输出，这些输出可以帮助您诊断造成问题的根本原因。

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：我在查看日志时，注意到安装的所有诊断均未通过。

Linux 上出现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，则表明您与互联网的出站连接存在问题。您可以通过 ping 一个知名的互联网位置（例如 www.amazon.com）来确认是否出现了这种情况。路由问题的最常见原因在于 VPC 网络配置，它需要有互联网网关，或者需要连接到数据中心并具有互联网路由的 VPN 连接。有关详细信息，请参阅本指南前文中的 Amazon VPC 网络拓扑。

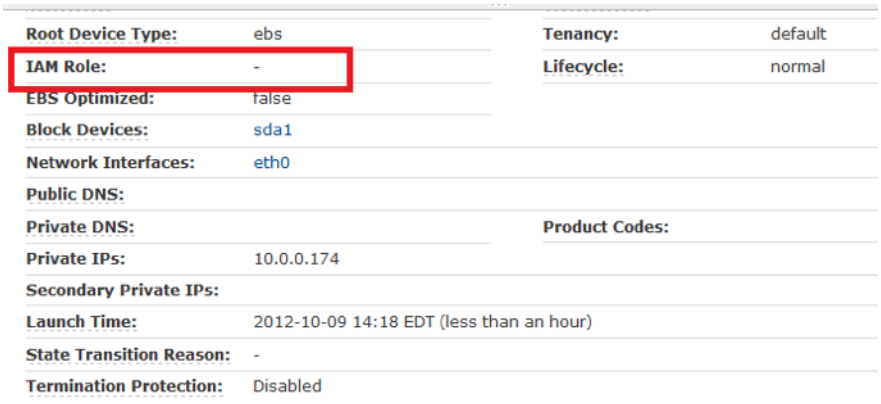
问题：当我查看日志时，我注意到我无法访问 Amazon EC2，但我确实通过了第一次 AWS 连接诊断。 CloudWatch

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 EC2 时遇到了授权问题。此问题的常见原因是您的实例没有关联已附加 IAM 策略的 IAM 角色，如本指南前文中的 IAM 角色所述。您可以在 Amazon EC2 控制台中查看相关的 Amazon EC2 实例并验证 IAM 角色，即可快速诊断此问题。

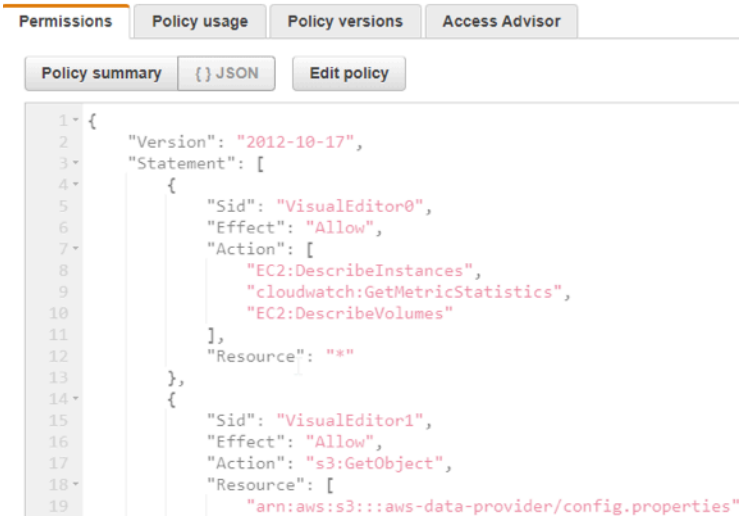
验证 EC2 实例的 IAM 角色



如果 IAM 角色不存在，则按照本指南前文“IAM 角色”中所述，创建该角色。

如果您确实为实例分配了 IAM 角色，请转到 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文 IAM 角色中指定的必需策略。

验证 IAM 角色的策略



问题：我想找数据 configure/update **JAVA_HOME**提供商。

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程序。

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

Windows 上的问题排查

问题：安装失败，我不确定文件是否处于一致的状态。

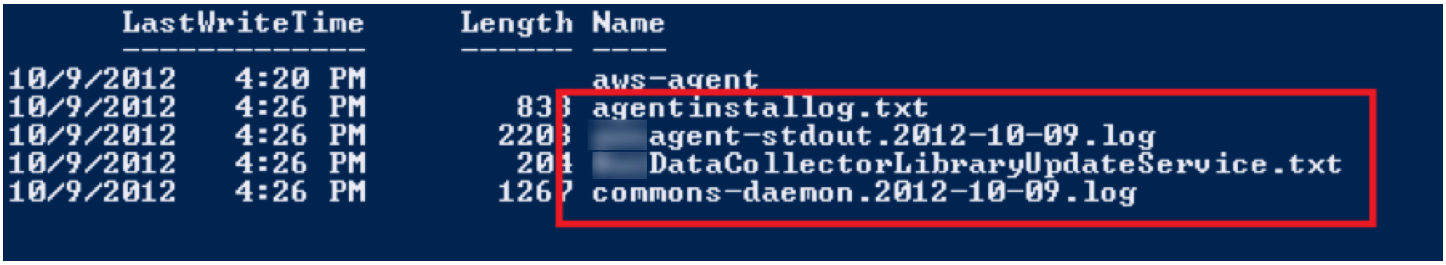
根据系统的 DataProvider 版本，按照更新到 DataProvider 4.3 或卸载旧版本中的步骤进行操作。

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。

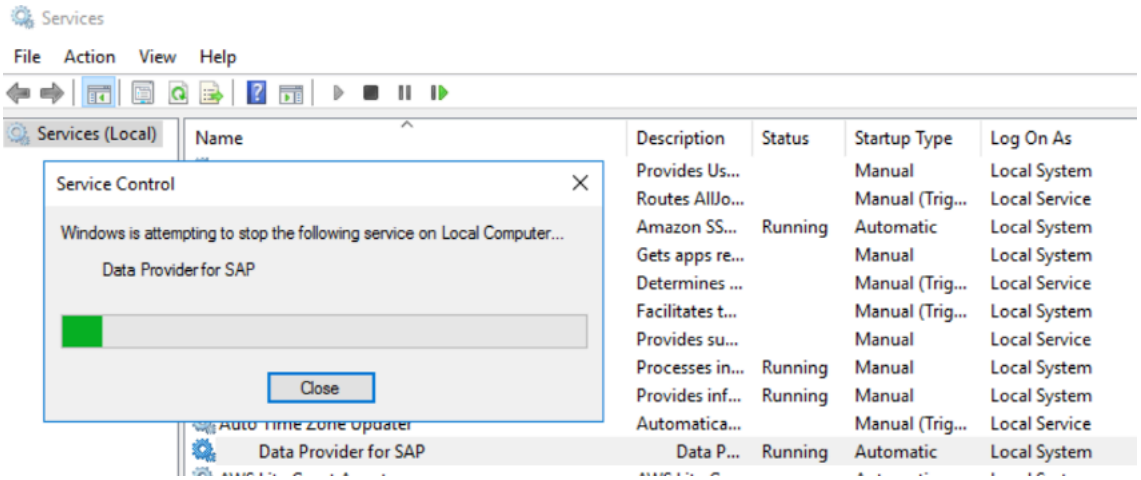
Windows 上的日志文件



问题：我想从数据提供程序中获得更详细的日志信息。

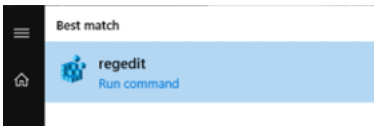
首先停止数据提供程序服务。

在 Windows 上停止服务



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

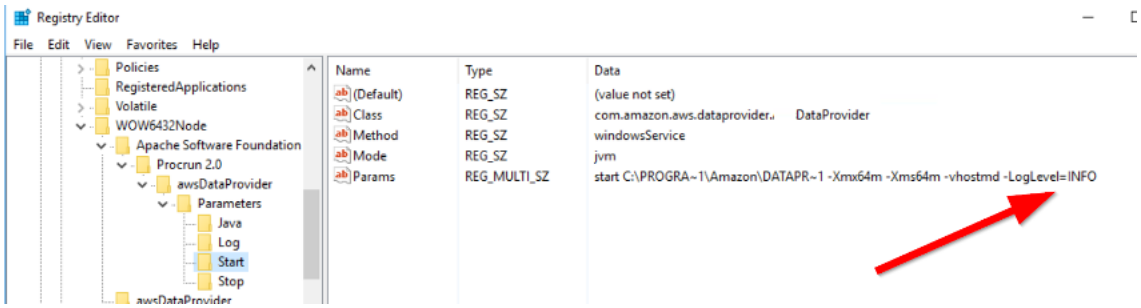
Start **`regedit`**



在注册表中，导航到键：

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

日志记录设置



数据提供程序接受两个日志级别：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，以避免日志不必要地占用磁盘空间。

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：我在查看日志时，注意到安装的所有诊断均未通过。

Windows 上出现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 : [redacted] 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，则表明您与互联网的出站连接存在问题。您可以通过 ping 一个知名的互联网位置（例如 www.amazon.com）来确认是否出现了这种情况。路由问题的最常见原因在于 VPC 网络配置，它需要有互联网网关，或者需要连接到数据中心并具有互联网路由的 VPN 连接。

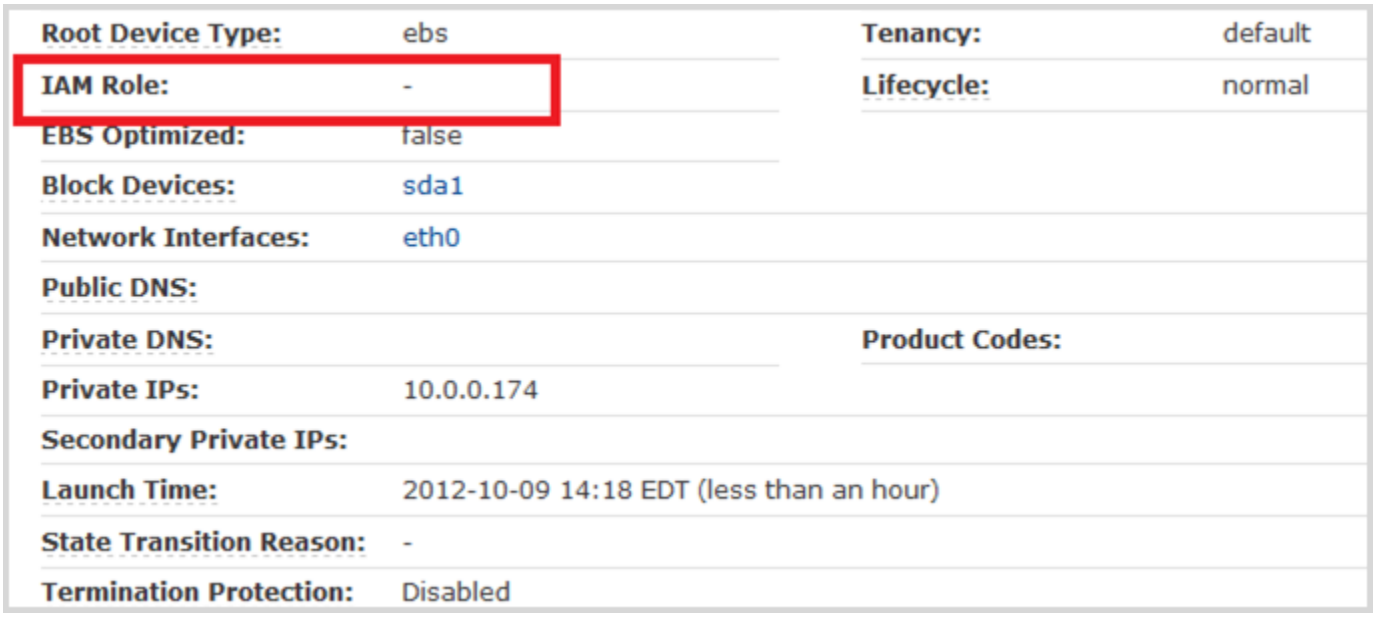
问题：当我查看日志时，我注意到我无法访问 Amazon EC2，但我确实通过了第一次 AWS 连接诊断。 CloudWatch

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 EC2时遇到了授权问题。此问题的常见原因是您的实例没有关联已附加 IAM 策略的 IAM 角色，如本指南前文中的 IAM 角色所述。您可以在 Amazon EC2 控制台中查看具体的 Amazon EC2 实例并验证 IAM 角色，即可快速诊断此问题。

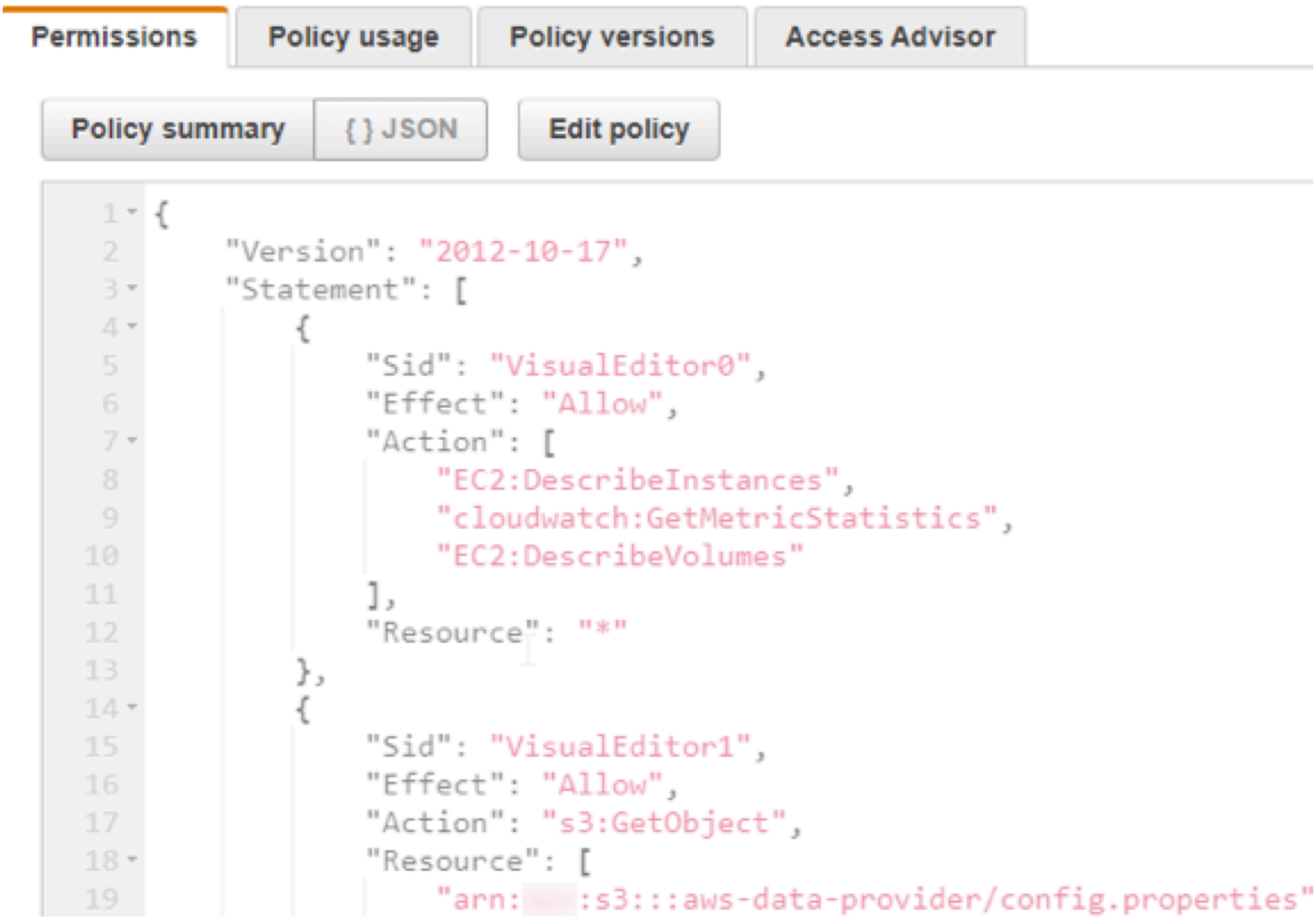
验证 EC2 实例的 IAM 角色



如果 IAM 角色不存在，则按照本指南前文“IAM 角色”中所述，创建该角色。

如果您确实为实例分配了 IAM 角色，请转到 IAM 控制台，选择 IAM 角色名称，然后选择显示。验证您是否拥有 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：

- 数据提供程序应用程序的 JAR（Java 存档）文件。
- 安装目录。只有在需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。将 <region> 替换为区域的区域代码（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添加逗号。
- 系统不忽略字符串中的空格。逗号之间的整个字符串（包括任何空格）都被接受作为值。
- 如果有多行具有相同实例类型，则将覆盖该类型的现有值。
- 字符串区分大小写。

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 的所有相关的 Amazon EC2 实例类型的数据库。

EC2 实例类型的条目必须是以逗号分隔的列表，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,
```

以下说明适用：

字段名称	内容	示例	Type	说明
关键字	ec2type	—	字符串	一个令牌，用于标识包含 EC2 实例描述的记录
i-type（实例类型）	参见列表	r3.8xlarge	字符串	实例类型，必须与 EC2 实例元数据字符串匹配
中央处理器 (CPUs)	1 | 2	2	整数	插槽的数量

字段名称	内容	示例	Type	说明
core（核心数）	integer	16	整数	处理器核心总数
threads（每个核心的线程数）	1 | 2	2	整数	每核心线程数
t-ecu（总 ECU 值）	integer	32	双精度	对于具有 ECU 评级的上一代实例类型，为 ECU 值；对于 ECU 之后的实例类型，为核心数
ecu（每内核 ECU）	双	1	双精度	对于 ECU 之后的所有实例类型为 1；对于具有 ECU 评级的上一代实例类型为总 ECU 值除以核心数
hthread（超线程）	线程 | 核心	线程	字符串	对于超线程实例类型，为线程；对于非超线程实例类型为核心
l-map（Linux NIC 映射）	eth0	eth0	字符串	网络接口的 Linux 映射
w-map（Windows NIC 映射）	eth0	lan2	字符串	网络接口的 Windows 映射
speed（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

字段名称	内容	示例	Type	说明
p-ecu（ECU 之后）	true | false	true	布尔值	对于没有 ECU 评级的现代化实例为 true

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 卷类型的条目必须是以逗号分隔的列表，如下所示：

voltype,ebs-type,sample-time,

例如：

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

以下说明适用：

字段名称	内容	示例	Type	说明
关键字	voltype	—	字符串	一个令牌，用于标识包含 EBS 卷描述的记录
ebs-type（EBS 类型）	io1 | gp2 | sc1 | st1	Io1	字符串	EBS 类型，必须与 EBS 卷元数据字符串匹配
sample-time	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 指标时，需要抽样时间。采样时间发生变化会导致 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。

此部分说明哪些指标会向 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 Operating System Collector（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。以下示例演示在 Windows 中如何进行查看。Linux 下的查看方式非常相似。

1. 打开 Windows 命令 shell 并将 shell 指向目录 `C:\Program Files\SAP\hostctrl\exe`。使用 `-d` 选项启动 `saposcol.exe`。

   Starting 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，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：

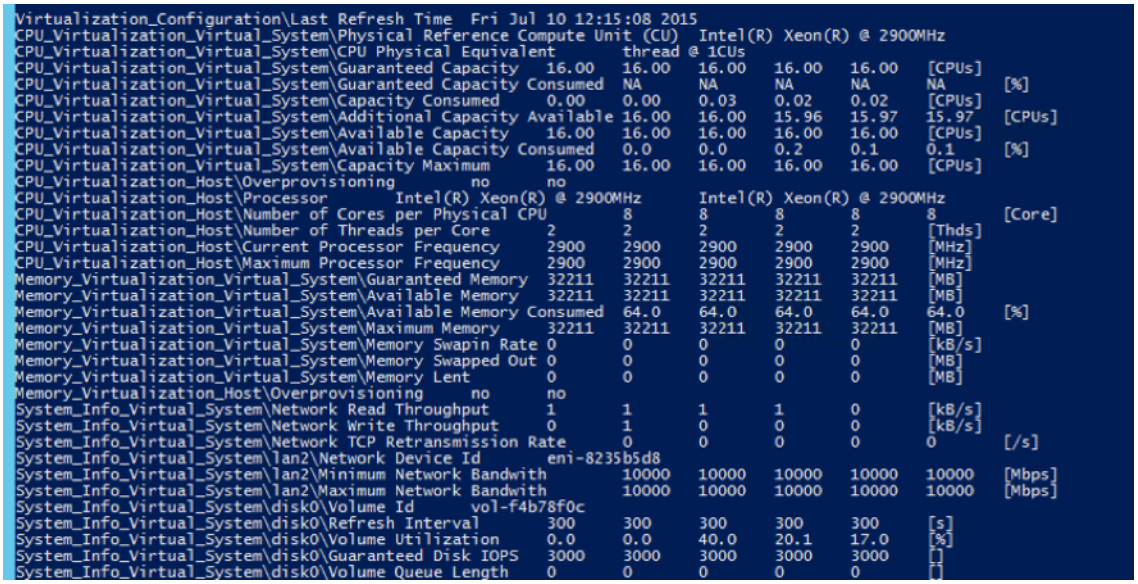
- Enhanced Monitoring Access TRUE
- Enhanced Monitoring Details ACTIVE

AWS特定指标以以下字符串开头：

+

- 虚拟化_配置
- CPU_Virtualization_Virtual_System
- Memory_Virtualization_Virtual_System
- System_Info_Virtualization_System

特定于 AWS的指标



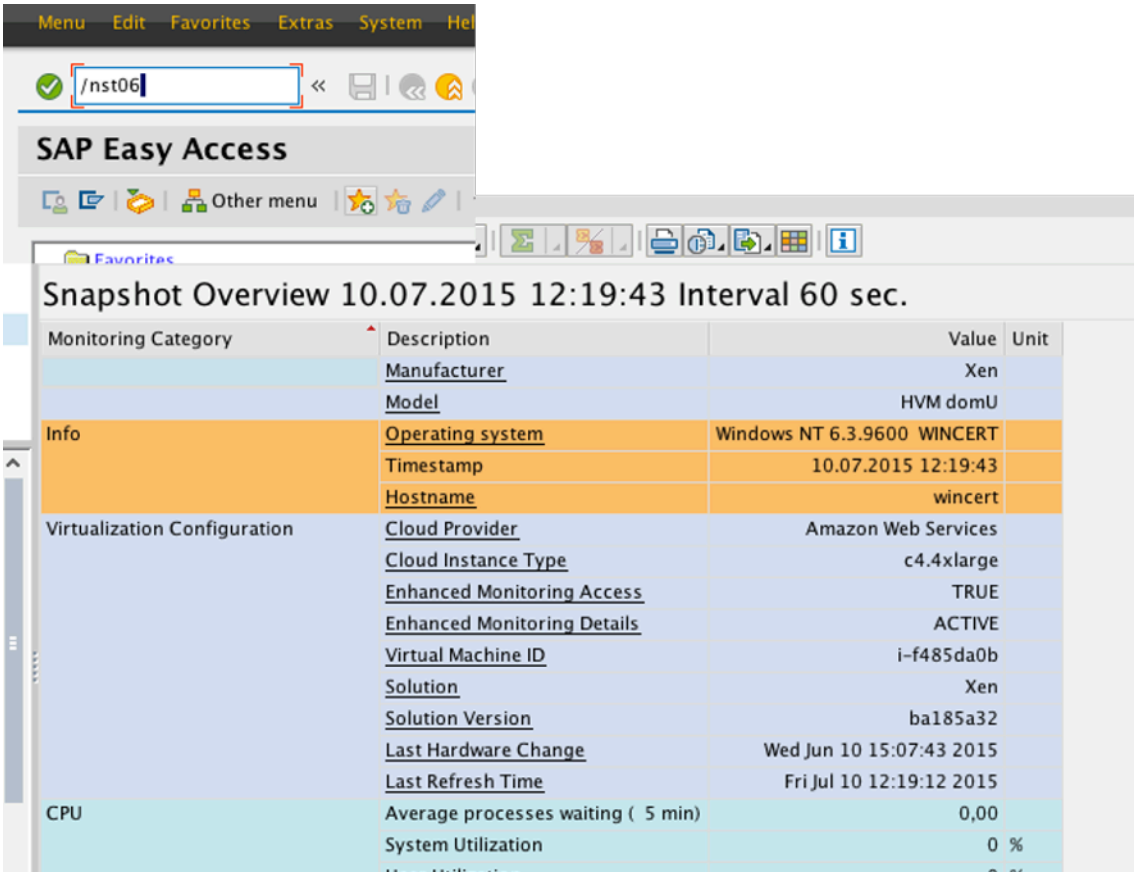
```
Virtualization_Configuration\Last Refresh Time  Fri Jul 10 12:15:08 2015
CPU_Virtualization_Virtual_System\Physical Reference Compute Unit (CU)  Intel(R) Xeon(R) @ 2900MHz
CPU_Virtualization_Virtual_System\CPU Physical Equivalent       thread @ 1CUs
CPU_Virtualization_Virtual_System\Guaranteed Capacity   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 事务检查指标

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），来快速访问数据。

> **Note**
>
> 您需要获得相应的授权才能查看此信息。

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（必须为 ACTIVE）
- 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。系统会显示全面的列表。其中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

它还会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。

内存和联网统计数据（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。

收集的指标示例

以下显示了示例指标。您的系统指标可能会略有不同。

```
<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：数据提供程序现已进行设置，可成功安装 SAP JVM。

版本 4.3（2023 年 1 月）

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

版本 4.2（2022 年 11 月）

- 增加了对 Oracle 和 Linux 的支持
- 增加了与 Linux `logrotate` 功能的集成
- 对 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：针对 Log4j2 问题（CVE-2021-44228）的安全更新。

版本 4.0（2021 年 4 月）

- 版本 4.0 初始发布。
- 支持 SSM 软件包安装。
- Support fo IMDSv2 r.

版本 3.0（2020 年 4 月）

- 版本 3.0 初始发布。

- 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。
- 增加了 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）。
- 改进了接入点确定功能。
- 支持 X1E 实例系列。

版本 2.8（2017 年 3 月 1 日）

- SLES 12、Red Hat 7 和 Oracle Linux 7 现在使用 SYSTEMD 来管理进程守护程序。
- 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。
- 日志记录文本发生了一些小更改。
- 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）

- 支持加拿大（中部）、美国东部（俄亥俄州）和欧洲地区（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：安装脚本会检查是否存在 wget。
- 支持 Oracle Linux。

版本 2.5（2016 年 5 月 2 日）

- 错误修复：版本 2.2-2.4 中的安全性和稳定性修复。

- 新增：支持新 Amazon EBS 卷类型：
  - 吞吐量优化型 HDD（st1）
  - 冷 HDD（sc1）
- 新增：支持 Amazon EC2 X1 实例系列。

版本 2.1（2016 年 1 月 20 日）

- 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 VM 的使用量现在限制为 64 MB 的最大堆大小。

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。已安装 1.3 代理的用户在迁移实例时，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。
- 安全修复：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。
- 新增内容： CloudWatch 以及 Amazon EC2 指标接入点：
  - 增加了对欧洲地区（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：可以使用用户可配置的 EC2 实例类型。

- 新增：针对未来的 EC2 实例类型增加了 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：针对新 EBS 卷类型的用户可配置采样时间现已可用。
- 新增：SAP AWS 的数据提供商现在报告 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 卷现在为卷类型报告正确的属性类型（“string”）。

版本 1.2（2014 年 9 月 16 日）

- 新增：支持 T2、R3 和 C3 实例系列。
- 新增：支持 ECU 之后（EC2 计算单位）实例类型：
  - 新实例类型不再具有 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 一分钟卷统计数据报告。
  - 现在，EBS 卷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：在 Linux 上增加了对 JRE 8 的支持。

SAP 谈 AWS 成本估算

上次更新时间：2023 年 5 月

AWS 提供 pay-as-you-go定价。您只需为所使用的服务按照所使用的时长付费。无需签署长期合同，也没有复杂的许可要求。有关更多信息，请参阅 AWS Pricing 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
- 仓储服务
- Network
- 自动化
- 备份、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。您必须先选择要在其中部署 SAP 系统的区域，然后才能开始进行估算。有关更多信息，请参阅区域和可用区。

计算

Amazon Elastic Compute Cloud（Amazon EC2）提供广泛的实例类型供选择，这些实例具有不同的 CPU、内存、存储、I/O 和联网功能组合。每个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。

仓储服务

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 Amazon EC2 实例提供持久的块级存储卷。运行 SAP 环境的每个 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，您只需按实际预置量付费。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，这意味着只会对存储的发生更改的块收取费用。存档层中的 Amazon EBS 快照是您的块数据的完整副本，这意味着您需要为存储的所有块付费，而不仅仅是发生更改的块。

您也可以启用回收站功能来防止意外删除。回收站中的 Amazon EBS 快照具有相同费率。

Amazon EBS 快照的另一个功能也非常适合 SAP 工作负载，这个功能是快速快照还原（FSR）。通过此功能，您能够从快照中快速恢复完全预置的 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

Amazon Elastic File System（Amazon EFS）提供无服务器文件存储。您可以共享文件数据，而无需预置或管理存储容量和性能。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。您可以方便快速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，使其具备高可用性。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。

通过 Amazon EFS，您只需为文件系统使用的存储付费，无最低费用或设置费用。有关更多信息，请参阅 Amazon EFS 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。此服务支持 Windows 文件系统功能和业界标准的服务器消息块（SMB）协议，以便通过网络访问文件存储。

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

您使用文件系统的费用按以下类别计费：

- 固态硬盘存储容量（GB/月）
- 您预置的固态硬盘 IOPS 超过三个 IOPS/GB （每月 IOPS）
- 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）是一种对象存储服务，提供行业领先的可扩展性、数据可用性、安全性和性能。您可以使用 Amazon S3 来暂存媒体、存储备份和归档数据。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。

Network

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。此虚拟网络与您在数据中心内运行的传统网络极其相似，并会为您带来使用 AWS的可扩展基础设施的优势。

使用 Amazon VPC 无需额外付费。有些组件（如 NAT 网关、IP 地址管理器、流量镜像、Reachability Analyzer 和网络访问分析器）需要付费。有关更多信息，请参阅 Amazon VPC pricing。

使用以下选项可在本地网络与 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）网络进行通信。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。

您需要为从 Amazon EC2 传出到互联网的数据付费。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 Global Accelerator 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

弹性负载均衡在一个或多个可用区中的多个目标（如 Amazon EC2 实例、容器和 IP 地址）之间自动分配传入的流量。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使用案例而异。它仅占SAP工作负载总成本的一小部分 AWS，即1-5%。

下表总结了适用于 SAP 环境的常见数据传输场景。

场景	架构	数据传输费用	定价指导	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	定价指导	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	
传输到本地网络或公司网络	AWS VPN	是	数据传输的每 GB 费用，请参阅 Amazon EC2 定价	AWS VPN 和 AWS Transit Gatewa
传输到本地网络或公司网络	AWS 直接连接	是	数据传出的每 GB 费用，根据位置和提供商而定，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，您可以使用备份功能在 Amazon 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。

备份、还原和恢复

借助这些服务，您可以快速高效地备份、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，适用于在云端亚马逊 EC2 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 弹性灾难恢复定价。

Amazon EBS 快照

请参阅 Amazon 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、安全地在 AWS 存储服务之间移动文件或对象数据。

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

使用以下服务，您可以监控运行在 AWS云端的 SAP 工作负载。

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
- 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。通过此工具，这些数据可供 SAP 应用程序使用，来帮助监控并改善业务事务的性能。

有关费用的信息，请参阅适用于 SAP 的AWS 数据提供程序定价。

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 Amazon 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。这些功能将根据亚马逊的 CloudWatch 定价从您的 AWS 账户中扣除。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。您可以收集并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。

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

您可以为所选操作系统自带许可证，也可以从 AWS Marketplace 购买许可证。

主题

- Red Hat
- SUSE
- Windows
- Oracle Enterprise Linux

Red Hat

Red Hat 提供两个 Linux 发行版来运行 SAP 工作负载。有关更多详细信息，请参阅红帽文档中的适用于 SAP 解决方案的红帽企业 Linux 简介。

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 Red Hat Cloud Access 计划。对于 RHEL 8，在生产环境中运行 SAP 应用程序需要 RHEL for SAP 解决方案或 RHEL for 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。RHEL for SAP 解决方案专为运行 SAP 工作负载而设计。此解决方案提供更长的生命周期支持及扩展更新支持（E4S），并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 的集群所需的全部必要软件包，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 的额外费用包含在 Amazon 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 Enterprise Server（SLES）和 SUSE Linux Enterprise Server for SAP Applications（SLES for SAP）

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，对 Amazon EC2 的支持取决于您的 SUSE 购买协议。

适用于 Amazon EC2 的 SLES 按小时费率或按年度承诺用量提供。RHEL for SAP 解决方案专为运行 SAP 工作负载而设计。此解决方案提供更长的生命周期支持及扩展更新支持（E4S），并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 的集群所需的全部必要软件包，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 Amazon EC2 实例成本中，基于 Amazon EC2 实例的 vCPU 数量。SLES for SAP 专为运行 SAP 工作负载而设计。此服务提供更长的生命周期支持，以及总共提供 4.5 年支持的扩展服务包叠加支持。SLES for SAP 还提供软件组件和服务方案，例如 SAP HANA 高可用性资源代理和集群连接器。

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

Windows

Amazon EC2 上的 Windows 服务器可以按固定的小时费率使用，无使用量承诺（按需型），也可以一次性付款使用（节省计划或预留实例）。在 Windows 操作系统上，这两种选项的成本没有区别。您也可以自带许可证。有关更多信息，请参阅上的 Microsoft 许可 AWS。

Oracle Enterprise Linux

SAP 要求您订阅 Oracle Linux Premier Support 才能使用 Oracle Enterprise Linux 操作系统。有关更多信息，请查看 Oracle 和 SAP 提供的以下资源。

- Oracle Store
- SAP Note 2069760 - Oracle Linux 7.x SAP Installation and Upgrade（需要 SAP 门户访问权限）

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 AWS Support 计划定价。

在 AWS云端运行 SAP 工作负载时，SAP 要求您至少获得 Business 级别的支持。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

本指南是一个内容系列的一部分，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”。

概述

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。

本指南中将介绍：

- SAP 高可用性和可靠性简介
- 架构指南和决策考虑事项
- 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 需求的业务要求 and/or 以及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

推荐阅读内容

在阅读本文档之前，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，为了保护本地部署中的 SAP 工作负载，SAP 客户采用了两种常见模式：高可用性和灾难恢复。云计算的出现带来了全新的机遇，促使客户开始思考使用现代化架构和技术来重塑 SAP 的 HADR 功能。

我们先回顾一下 SAP 的系统设计，以及在 SAP 的 n 层架构中包含的单点故障。

SAP NetWeaver 架构单点故障

图 1：SAP 单点故障

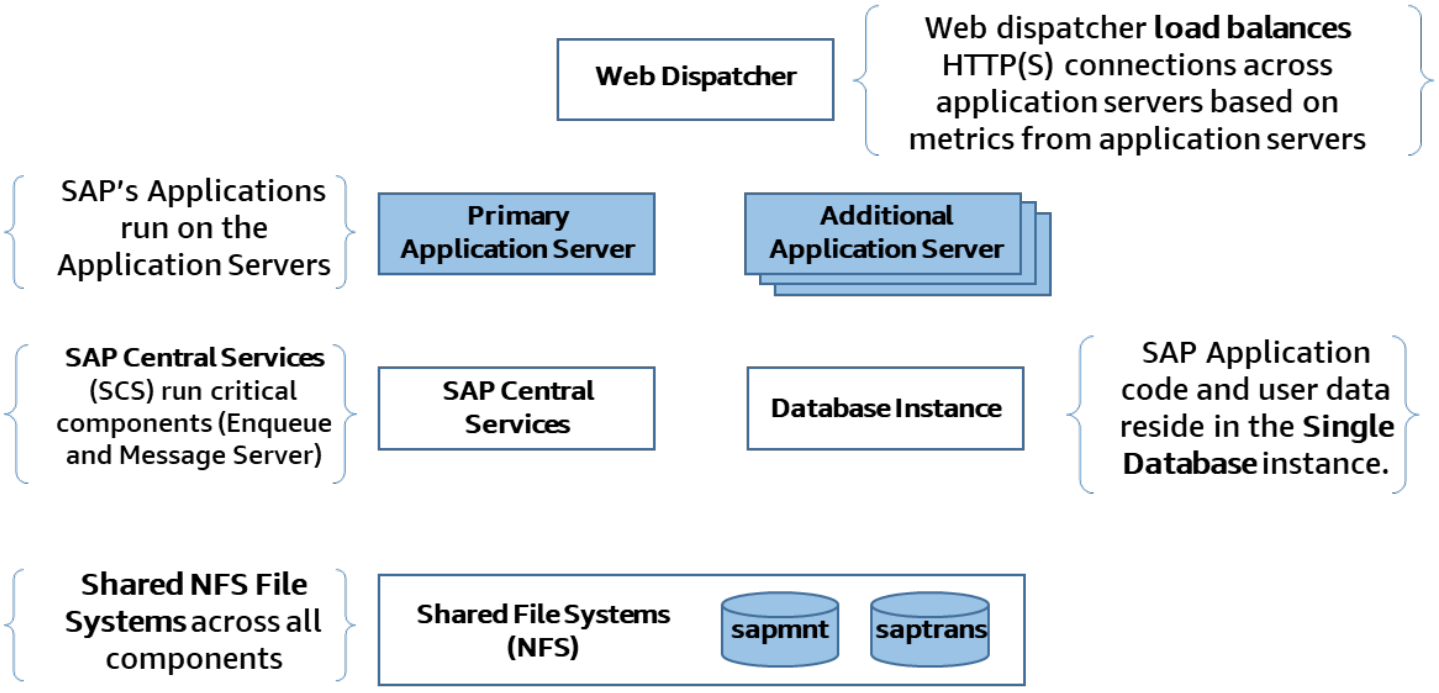


图 1 显示了典型的 SAP NetWeaver 架构，它有几个单点故障，如下所示：

- SAP 中央服务（消息服务器和入队流程）

- SAP 应用程序服务器
- NFS（共享存储）
- 数据库
- SAP Web Dispatcher

对于 SAP 中央服务和数据库，可以通过部署更多的主机来增加保护。例如，添加另一台主机来运行 SAP 复制入队，可以防止应用程序级锁（入队锁）丢失，而添加另一台主机来运行辅助数据库实例可以防止数据丢失。

但是，这些设计中存在固有的单点故障，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。此服务有助于防御 SAP 单点故障之一。

高可用性和灾难恢复

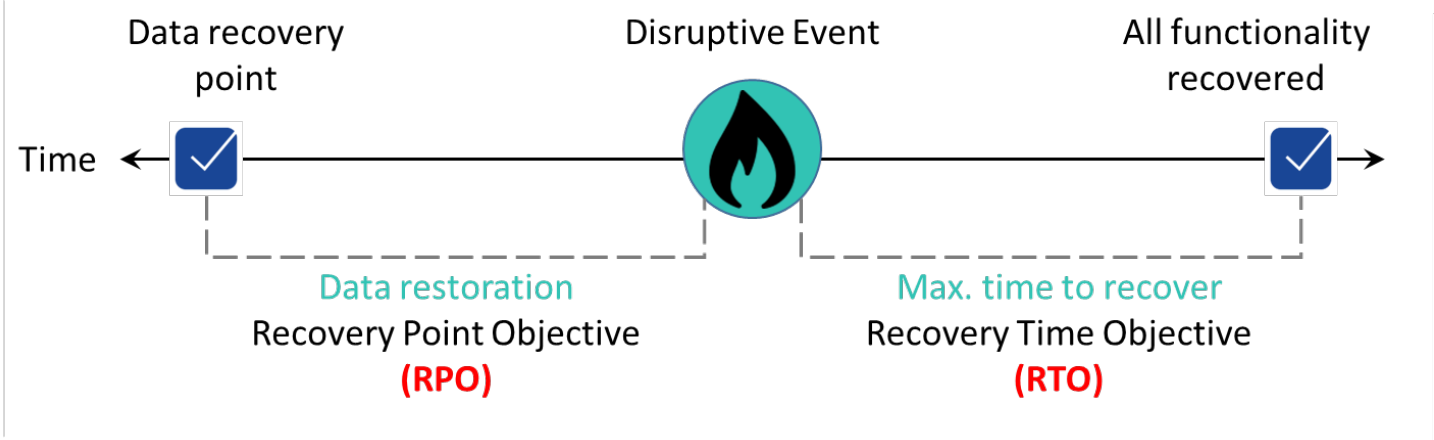
高可用性（HA）是系统的属性，用于在定义的时间段内以可接受或商定的水平提供服务，并让最终用户不会察觉到计划外中断。此功能通常通过使用集群服务器来实现。这些服务器提供自动化的故障检测和恢复，或者提供具有高韧性的硬件、可靠测试以及问题和变更管理。

灾难恢复 (DR) 通过在不同的硬件 and/or 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。这种问题通常采用单独的解决方案来解决，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失效转移到另一个设施。

从有记录和可衡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）是系统或服务出现停机、解决方案进行恢复，然后服务重新可供使用的可以接受的最大总时间长度。
- 恢复点目标（RPO）是指企业能够接受的数据丢失量，用时间表示。这是出现故障的时间与恢复点之间的最长时间间隔。

图 1：SAP 单点故障



≈

本地部署模式与云部署模式

传统上，如果客户具有高可用性要求，就会将其主要计算容量部署在单个数据中心或托管设施中，通常是在数据中心的两个独立的计算机室或机房中，这些位置具有不同的冷却和电源系统并具备高速网络连接。一些客户会运行两个近距离的托管设施，这些设施具备独立的计算容量，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场所故障风险更高），许多客户会扩展其架构，在备用位置存储数据副本，并提供额外的闲置计算容量。主位置与备用位置之间的距离通常会导致需要异步传输数据，这会影响恢复点目标。对于运行 SAP 的许多行业和公司而言，这是用于实现高可用性和灾难恢复的标准且普遍接受的架构模式。

图 3：本地部署灾难恢复

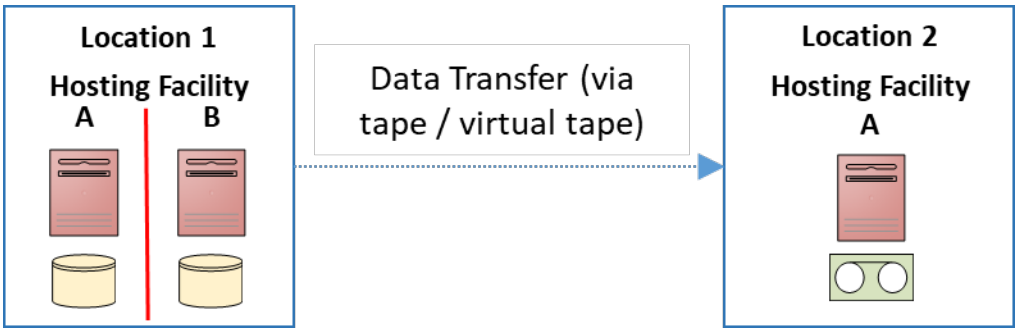
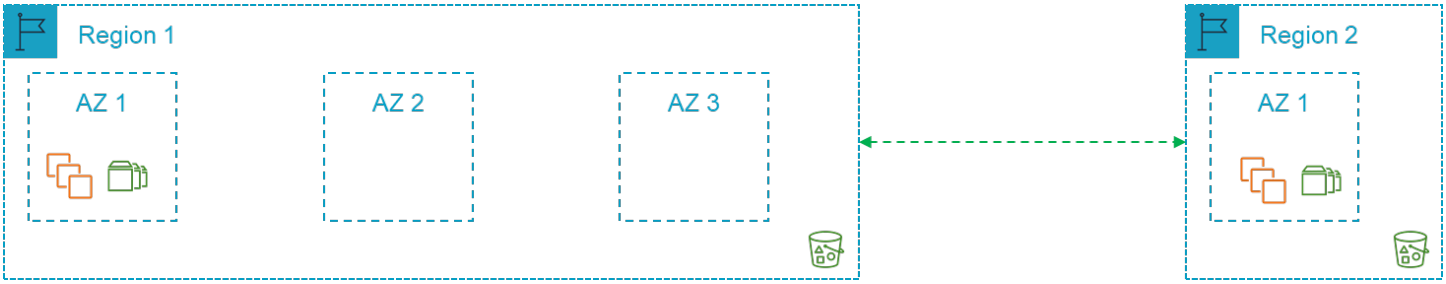


图 3 举例说明了客户在本地部署中通常采用的方法。在地点 1 中，客户有两个托管设施，通常分隔在相同数据中心内的不同计算机室或机房内，客户在其中为 SAP 单点故障部署高可用性架构。地点 2 是用于灾难恢复的地点，在地点 1 的两个托管设施都出现严重故障时，SAP 系统将在其中恢复。

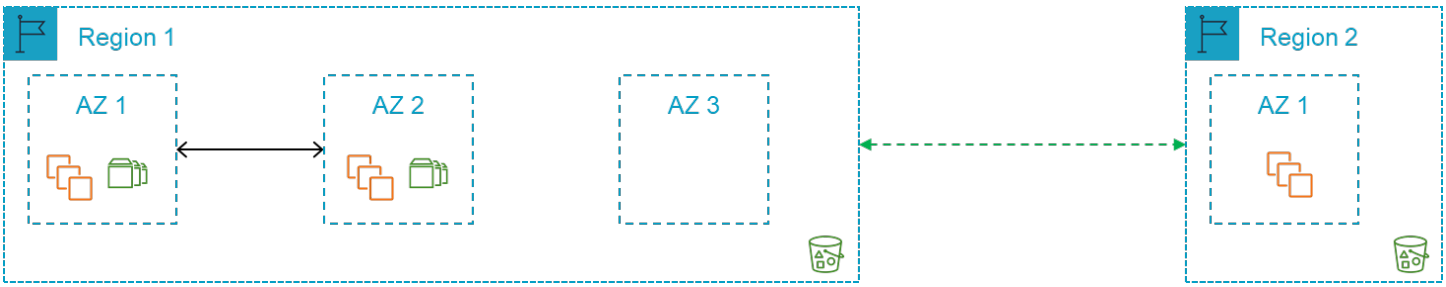
将 SAP 工作负载迁移到云提供商的客户仍会恢复到该架构，并将其映射到AWS区域和可用区 (AZs)，如图 4 所示。虽然这种架构可以用于您的环境，但没有遵循 AWS Well-Architected Framework，该框架可帮助云架构师为应用程序构建安全、高性能、高韧性和高效的基础设施。

图 4：本地到AWS区域的映射方法



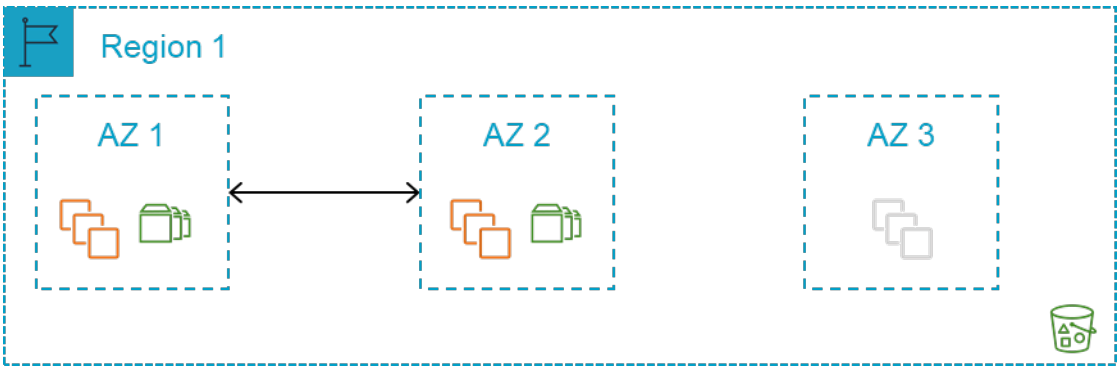
AWS在区域和可用区中按地理位置隔离设施。对于主计算容量，多可用区方法在确保间隔一定距离的同时维护性能。这种方法（图 5）大幅降低了某个地点出现故障的风险。

图 5：本地与AWS区域映射的替代方法



在显著降低了主计算容量的地点故障风险后，可以根据业务需求评估是否需要第二个区域。您可以使用在相同或不同的区域快速部署所需的容量AWS。不会再出现空闲硬件的问题。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。这种架构可以实现简化并且现成可用（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所导致的业务数据丢失。

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。出现这种情况时，需要有相关决策来从正常的本地副本恢复业务数据。为此需要制定决策，确定数据的存储位置，以及发生逻辑灾难恢复事件时如何使用数据。

本指南的下文中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。

架构指南和决策

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。

Regions

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。每个区域都是隔离的，独立于其他区域。有关区域名称和代码的列表，请参阅区域端点。

区域提供容错能力、稳定性和韧性。通过区域，您可以创建冗余资源，即使在遇到极少出现的中断情况时，这些资源仍保持可用且不受影响。

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。可用区由位于分离设施中的独立数据中心组成，具有冗余电源、联网和连接。

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。通过将应用程序分布在多个可用区中，您在面对大多数故障模式（包括自然灾害或系统故障）时能够保持韧性。

每个可用区可包含多个数据中心。在完全扩展的情况下，单个可用区可容纳数十万台服务器。它们是AWS全球基础架构中完全隔离的分区。所有可用区在物理上是彼此分开的，自身具有强大的基础设施。可用区之间有距离间隔，不过都在 100 公里以内（彼此相距 60 英里）。此距离能够隔离可能会影响数据中心的最常见灾害（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。这确保了可用区间的高吞吐量、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以完全相同的数据并行运行，这样在发生灾难时，就能以最少的停机时间进行无缝失效转移。

Services

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，交流您对本地区服务交付的兴趣，索取服务路线图信息，或者深入了解服务的相互依赖关系（需签署 NDA）。

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，您需要在某个区域内指定所需的可用区域。

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，尽可能减少网络延迟。
- 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 Region Table。
- 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 AWS定价和优化》指南。

多区域注意事项

跨多个区域进行部署时，一个重要的考虑因素是在每个区域中，所需核心服务（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辅助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 架构时需要用到这些方法。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 and/or Amazon S3 复制）相关的成本以及次要区域的存储。

第 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、 and/or 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。这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。利用该服务，您可以更好地满足业务的预算、安全性和合规性需求。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环境用于运行安全且可扩展的工作负载，同时在创建核心账户和资源时实施初始安全基准，来节省时间。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 基于与成千上万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。您可以通过预配置的护栏，以交互方式监管账户。

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地使用实例（应用程序层）。根据计算、内存、存储吞吐量和许可证合规要求，您还需要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出现故障时无法灵活进行更改的层，请考虑在运行实例的区域和所需可用区中，通过预留实例或按需容量预留来实现容量预留。这种方法称为静态稳定性。有关详细信息，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。要想享受到折扣优惠，这些按需型实例必须与特定属性（例如实例类型和区域）匹配。

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。除了相比按需型实例定价可以实现节省之外，区域预留实例还可在指定可用区内提供容量预留。这可以确保您可以随时使用所需的容量。

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。这使您能够独立地创建和管理容量预留，并享受到节省计划或区域预留实例带来的账单折扣。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，建议您取消容量预留来停止产生费用。

跨可用区的实例系列可用性

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提供该类型。

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 中央服务），则应考虑使用跨两个可用区的集群来帮助确保高可用性。

内存增强型裸机专属主机

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属主机恢复。如果在专属主机上检测到故障，主机恢复自动在新的替换主机上重新启动实例。主机恢复可减少人工干预的需求，并降低了意外发生专属主机故障时的运营负担。

我们建议您在所选区域的不同可用区中使用第二个内存增强型实例，以防出现可用区故障。

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。维护事件分为两种类型：

- 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，将保留您的实例的所有配置设置。

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，一些更新需要短暂的重启。这样的重启应该很少发生，但对于应用升级来增强安全性、可靠性和操作性能是必要的。

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：

- 实例重启是对虚拟实例进行重启，相当于操作系统重启。
- 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。

如果您不执行任何操作，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，实例将完成重启，大多数情况下需要几分钟。

或者，您可以通过对实例执行停止和启动操作，将实例迁移到新主机。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。

Networking

Amazon 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 的主网段。

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。您在同一个可用区内可以有多个子网，但单个子网不能跨多个可用区。

为了确保以后的灵活性，建议您的子网和连接设计支持您的账户在该区域中的所有可用区，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。在同一区域中，不同可用区之间资源的延迟为几毫秒。

为了实现高可用性，我们建议跨多个可用区部署生产 SAP 工作负载，包括 SAP 应用程序服务器层。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运行在合适的应用程序服务器上。

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 Direct Connect 的连接，通过 Direct Connect 网关可以连接到多个区域。

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。

AWS Direct Connect 韧性工具包提供了具有多种韧性模式的连接向导。这些模式可帮助您订购专用连接来实现 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 Amazon 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。

跨区域对等连接

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。区域间对等连接会产生数据传输费用。

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

弹性负载均衡支持以下类型的负载均衡器：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 Dispatchers SA and/or P Central Services 的高可用性。有关详细信息，请参阅使用网络负载均衡器的覆盖 IP 路由。

负载均衡器充当客户端的单一接触点。负载均衡器将传入流量分配到多个目标，例如 Amazon EC2 实例。

侦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，然后将请求转发给目标组。

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，网络负载均衡器基于协议、源 IP 地址、源端口、目标 IP 地址、目标端口和 TCP 序列号，使用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。Route 53 提供 100% 的 SLA。

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。

仓储服务

对象存储

Amazon Simple Storage Service（Amazon S3）是一种对象存储服务，提供行业领先的可扩展性、数据可用性、安全性和性能。Amazon S3 是一项区域性服务，覆盖一个区域中的所有可用区，设计为可实现 99.999999999%（11 个 9）的持久性以及 99.9% 的 SLA。

为了防止数据丢失，您可以将备份（例如数据库备份或文件备份）存储到 Amazon S3 中。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 复制支持自动跨 Amazon S3 存储桶以异步方式复制对象。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。

Amazon 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，您还可以对跨区域复制启用 Amazon S3 Replication Time Control。Amazon S3 Replication Time Control（Amazon S3 RTC）可以帮助您满足数据复制的合规性要求或业务要求，并提供对 Amazon S3 复制时间的可见性。Amazon S3 RTC 会在几秒钟内复制您上传到 Amazon S3 的大多数对象，并在 15 分钟内复制 99.99% 的对象。

除了以上列出的跨区域复制费用外，Amazon S3 RTC 还会产生下列费用：

- Amazon S3 RTC 管理功能：按每 GB 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。您可以在这些卷上创建文件系统，或者以使用块设备（如硬盘）的任何方式使用这些卷。您可以动态更改附加到实例的卷的配置。

Amazon EBS 卷放在一个特定的可用区内，并在其中自动复制，以保护您免受单一组件发生故障而造成的影响。所有 Amazon EBS 卷类型都提供持久快照功能，旨在通过多可用区配置实现每个卷的 99.999% 可用性和 99.99% 的服务可用性。您需要使用数据库复制功能、块级复制解决方案或 Amazon EBS 快照，才能为存储在 Amazon EBS 上跨多个可用区的 SAP 数据确保持久性。

Amazon EBS 卷的年故障率（AFR）设计为 0.1% 到 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 卷的可靠程度比普通商用磁盘高 20 倍，后者通常出现故障的 AFR 约为 4%。例如，如果 1000 个 Amazon EBS 卷运行 1 年，则可能会有一两个卷出现故障。

Amazon EBS 提供多种不同的卷类型。此服务必须用于与 SAP 数据库相关的数据，且必须使用通用型 SSD（gp2）或预调配 IOPS SSD（io1）。吞吐量和 IOPS 要求将决定需要使用 gp2 还是 io1。

通过 Amazon EBS 多重挂载，您可以将单个预调配 IOPS SSD（io1）卷连接到位于同一可用区中的最多 16 个基于AWS 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。启用多重连接的卷不支持 I/O 屏蔽。 I/O 屏蔽协议控制共享存储环境中的写入访问权限以保持数据一致性。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。每个快照都包含将数据（拍摄快照时存在的数据）还原到新 Amazon EBS 卷所需的所有信息。

可以将 Amazon EBS 快照复制（复制）到与不同AWS账户 and/or 共享的不同区域。

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

从现有 Amazon EBS 快照创建的新卷在后台延迟加载。也就是说，通过快照创建卷之后，无需等待所有数据从 Amazon S3 传输到 Amazon EBS 卷，附加的实例即可开始访问该卷及其所有数据。

此初步操作需要时间，并且会大大增加 I/O 操作的延迟。如果您的实例访问尚未加载的数据，卷会立即从 Amazon S3 下载请求的数据，然后在后台继续加载卷数据的剩余部分。

快速快照还原

Amazon EBS 快速快照还原使您能够从快照创建在创建时已完全初始化的卷。这消除了首次访问区块时对其进行 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。Amazon EFS 提供 99.99% 的 SLA。

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 Backup 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。您可以随时进行额外的备份。

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，它们的设计目的是，即使在某个可用区不可用时也能连续提供数据供使用。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。写入文件系统中磁盘的任何更改都会跨可用区同步复制到备用区。

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。该事件历史记录简化了安全分析、资源变更跟踪和故障排除工作。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

在此部分中，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 系统选择合适的模式。

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 and/or 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。
- 多个 Amazon Elastic Block Store（Amazon EBS）卷出现卷状态检查错误，卷因而失败。

Amazon Elastic Block Store 故障

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，您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。

为了防范逻辑数据丢失，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。

图案

在此部分中，我们将探讨可用于处理上述故障场景的架构模式。

在选择能够满足企业特定业务需求的模式时，需要考虑两个关键参数：

- 针对 SAP 单点故障的计算容量可用性
- Amazon EBS 上保存的 SAP 数据的可用性

这些参数决定从故障场景中恢复所需的时间，即 SAP 系统恢复服务需要花费的时间。

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）。

   或者

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具备高可用性。部署多区域模式时，您可以获益于自动化方法（例如集群解决方案）的使用，这样可以自动在可用区之间进行失效转移，从而最大限度地减少总停机时间并消除人为干预的需求。多区域模式不仅提供了高可用性，还可以实现灾难恢复，从而降低总体成本。

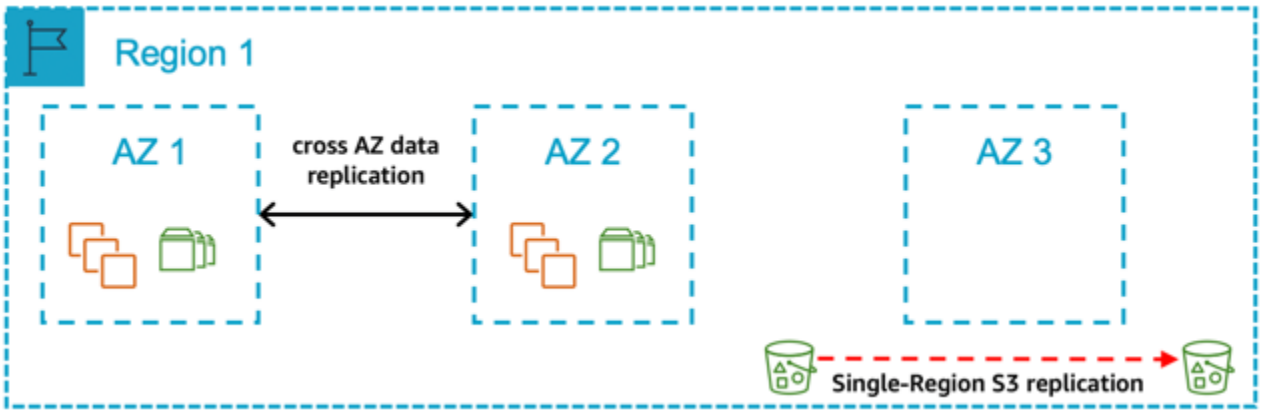
单区域架构模式

在以下情况下，选择单区域模式：

- 您要求数据始终仅位于特定的地理AWS区域（区域）
- 您希望避免多区域方法中可能出现的潜在网络延迟因素
- 您希望避免多区域方法带来的成本影响或差异，包括：
  - AWS不同AWS地区的服务定价
  - 跨区域数据传输费用

模式 1：单个区域，有两个 AZs 用于生产

图 7：单个区域，具有两个可用区用于生产环境



在这种模式下，您可以跨两个可用区部署所有生产系统。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容量大小相同，在一个可用区出现故障时，可自动进行失效转移。SAP 应用程序层所需的计算容量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可用区中。

如需满足以下要求，请选择此模式：

- 您需要规定完成生产环境恢复的时间长度，并需要确保在另一个可用区中，提供用于生产 SAP 数据库和中央服务层的计算容量。
- 对于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容量，您可以接受由此产生的额外成本。
- 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。
- 您可以接受在可用区之间实现自动失效转移需要第三方集群解决方案。
- 您可以接受在某个可用区出现故障时，将应用程序层恢复到 100% 容量所需的时间长度不确定（包括在剩余可用区中提供所需计算容量会出现的任何延迟）。

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，用于生产应用程序层（主动/主动）。在某个可用区出现故障时，需要扩展应用程序层，在剩余的可用区中恢复 100% 的容量。
- 使用数据库复制功能或块级复制解决方案，将 SAP 数据库保存在两个可用区中的 Amazon EBS 上。
- 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 数据库定期备份到 Amazon S3。
- 配置 Amazon S3 单区域复制来防范逻辑数据丢失。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照。

优点

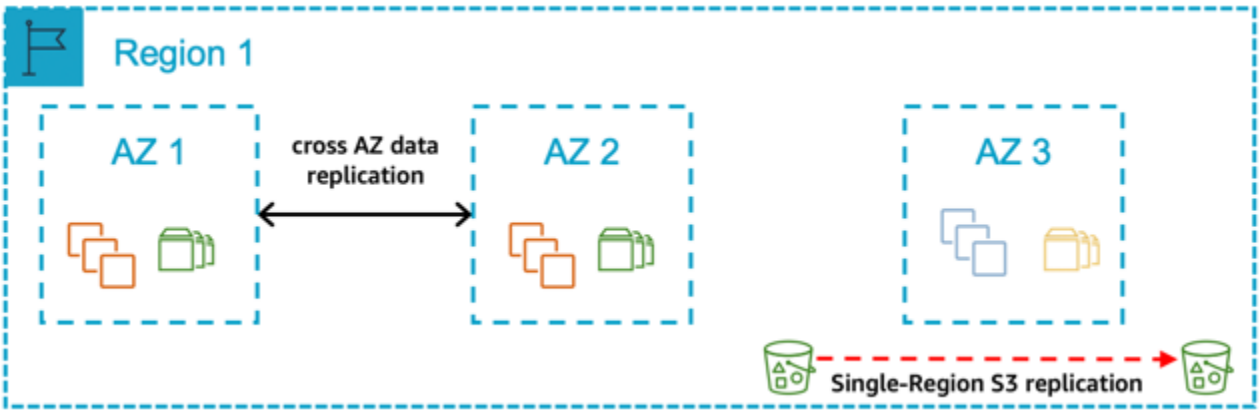
- 低平均恢复时间（MTTR）
- 可预测的恢复服务（RTS）
- 能够将数据库和中央服务层失效转移到可用区 2，防止性能严重降级或可用区的整体故障
- 可用区或 Amazon EBS 出现故障时，不要求从 Amazon S3 恢复数据

注意事项

- 对于可用区之间的自动失效转移，需要有明确记录在案且经过测试的流程。
- 对于维护自动化失效转移解决方案，需要有明确记录在案且经过测试的流程。
- 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：单个区域，具有两个可用区用于生产环境，与生产环境相同大小的非生产环境位于第三个可用区中



在这种模式下，您可以跨两个可用区部署所有生产系统。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容量大小相同，在一个可用区出现故障时，可自动进行失效转移。SAP 应用程序层所需的计算容量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生产系统相等，部署在第三个可用区中。如果部署生产系统的某一个可用区出现故障，则会重新分配非生产容量，以便将生产环境恢复到多可用区模式。

如需满足以下要求，请选择此模式：

- 在该区域内的某个可用区出现故障时，您需要能够继续保持用于生产环境的多可用区配置。
- 您需要规定完成生产环境恢复的时间长度，并需要确保在另一个可用区中，提供用于生产 SAP 数据库和中央服务层的计算容量。
- 对于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容量，您可以接受由此产生的额外成本。
- 您可以接受跨可用区的数据复制（需要数据库复制功能或块级复制解决方案）和相关成本。
- 您可以接受在可用区之间实现自动失效转移需要第三方集群解决方案。
- 您可以接受在某个可用区出现故障时，将应用程序层恢复到 100% 容量所需的时间长度不确定（包括在剩余可用区中提供所需计算容量会出现的任何延迟）。

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% 的生产计算容量（数据库和中央服务）部署在第三个可用区，供非生产环境用于正常操作。
- 计算容量部署在可用区 1 和可用区 2 中，用于生产应用程序层（主动/主动）。在某个可用区出现故障时，需要扩展应用程序层，在剩余的可用区中恢复 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 数据库保存在两个可用区中的 Amazon EBS 上。
- Amazon EFS 用于 SAP 全球文件系统。
- SAP 数据库定期备份到 Amazon S3。
- 配置 Amazon S3 单区域复制来防范逻辑数据丢失。
- 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）
- 能够将数据库和中央服务层失效转移到可用区 2，防止性能严重降级或可用区的整体故障
- 可用区出现故障或 Amazon EBS 出现故障时，不要求从 Amazon S3 恢复数据
- 将数据保存在三个不同可用区中的 Amazon EBS 上的选项，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整个可用区出现故障，则使用非生产计算容量，在两个可用区上恢复生产

注意事项

- 对于可用区之间的自动失效转移，需要有明确记录在案且经过测试的流程。
- 对于维护自动化失效转移解决方案，需要有明确记录在案且经过测试的流程。
- 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。
- 在某个可用区出现故障影响生产时，对于从非生产环境重新分配计算容量来在两个可用区中回复生产环境的运行，需要有明确记录在案且经过测试的流程。

模式 3：单个区域，一个可用区用于生产环境，另一个可用区用于非生产环境

图 9：单个区域，一个可用区用于生产环境，另一个可用区用于非生产环境

在这种模式下，您将所有生产系统部署在一个可用区中，并将所有非生产系统部署在另一个可用区中。您的非生产系统的大小与生产系统相等。

如需满足以下要求，请选择此模式：

- 您需要规定完成生产环境恢复的时间长度，并需要确保另一个可用区中，用于 SAP 数据库和中央服务层的计算容量的可用性。
- 您可以接受在恢复生产的总时间长度中，包括将计算容量从非生产环境重新分配到生产环境所需的额外时间。
- 您可以接受在恢复生产的总时间长度中，包括将数据从另一个可用区中的 Amazon S3 恢复到 Amazon EBS 所需的时间。
- 您可以接受在某个可用区出现故障后，将应用程序层恢复到 100% 容量所需的时间长度不确定（包括在剩余可用区中提供所需计算容量会出现的任何延迟）。
- 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，供非生产环境用于正常操作。
- 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，不复制到其他可用区。

- Amazon EFS 用于 SAP 全球文件系统。
- SAP 数据库的数据定期备份到 Amazon S3。
- 配置 Amazon S3 单区域复制来防范逻辑数据丢失。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照。

优点

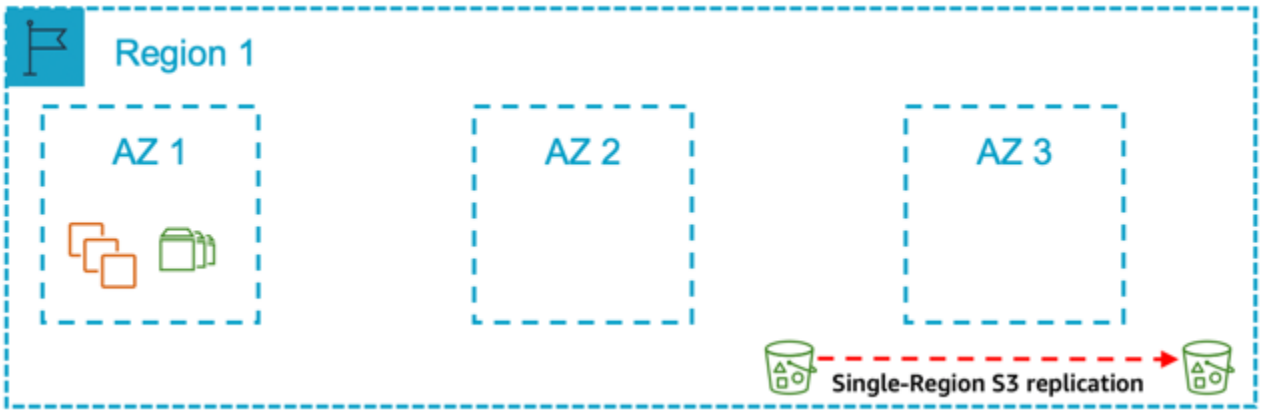
- 在生产环境可用区出现故障时，使用非生产容量来优化成本
- 所需的计算容量部署在两个可用区中，从而实现更可预测的恢复时间

注意事项

- 对于将所需的计算容量从非生产环境部署到生产环境并在不同的可用区中恢复数据，需要有明确记录在案且经过测试的流程来确保可恢复性。
- 如果某个可用区故障影响到生产环境，则非生产环境可能会丢失。
- 由于采用两个可用区缺乏高可用性，因此在计算容量或可用区出现故障时，恢复生产所需的时间会增加。

模式 4：单个区域，具有单个可用区用于生产环境

图 10：单个区域，具有单个可用区用于生产环境



在这种模式下，您将所有生产系统部署在一个可用区中，并将所有非生产系统部署在同一个或另一个可用区中。您的非生产系统的大小与生产系统不相等。**

如需满足以下要求，请选择此模式：

- 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。
- 您希望避免多可用区方法带来的成本影响，并可以接受生产 SAP 系统停机时间的相关风险。

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，不到为生产 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，不复制到其他可用区。
- Amazon EFS 用于 SAP 全球文件系统。
- SAP 数据库定期备份到 Amazon S3。
- 配置 Amazon S3 单区域复制来防范逻辑数据丢失。
- 所有服务器的 Amazon Machine Image/Amazon EBS 快照都是定期拍摄的。

优点

- 最低的成本
- 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

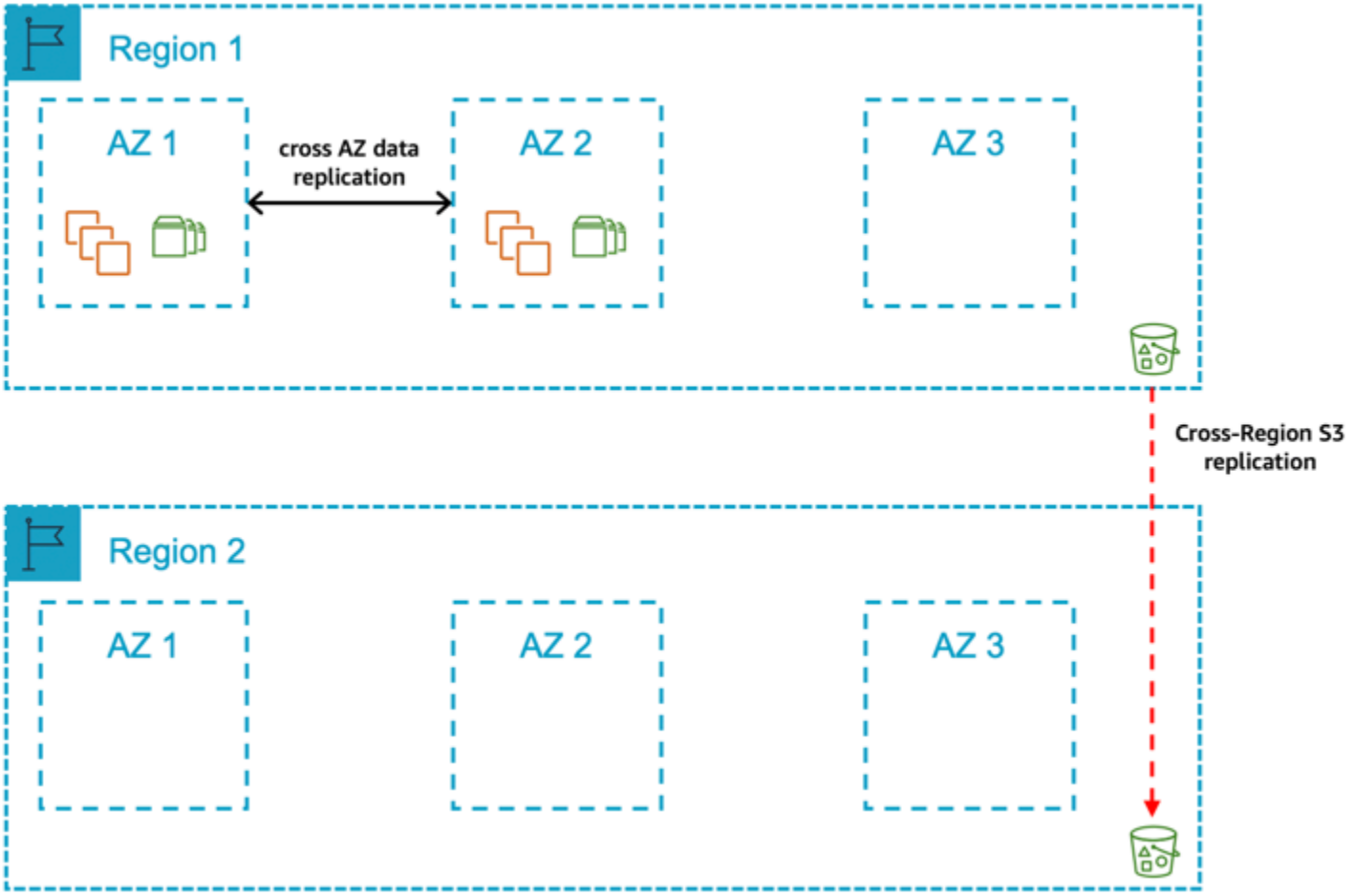
如果您有以下要求，则应选择多区域架构：

- 您要求数据始终位于两个特定的地理AWS区域。
- 您可以接受多可用区方法带来的潜在网络延迟因素。
- 您可以接受多区域方法带来的复杂性增加。

- 您可以接受多区域方法带来的成本影响/差异，包括：
  - AWS不同AWS地区的@@ 服务定价（例如 Amazon EC2）
  - 跨区域数据传输费用
- 第二个区域的额外计算 and/or 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，您跨主区域中的两个可用区部署生产系统。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容量大小相同，在一个可用区出现故障时，可自动进行失效转移。SAP 应用程序层所需的计算容量在两个可用区之间以 50/50 的比例分配。此外，存储在 Amazon S3 中的生产数据库备份、Amazon EBS 快照和亚马逊机器映像会复制到辅助区域。如果整个区域出现故障，生产系统将在辅助区域中从最新一组备份恢复。

如需满足以下要求，请选择此模式：

- 您需要规定完成生产环境恢复的时间长度，并需要确保在主区域的另一个可用区中，提供用于生产 SAP 数据库和中央服务层的计算容量。
- 对于跨主区域中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容量，您可以接受由此产生的额外成本。
- 您可以接受数据复制时与跨可用区相关的数据传输费用。
- 您可以接受在可用区之间实现自动失效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的数据复制（需要数据库复制功能或块级复制解决方案）。
- 您可以接受将应用程序层恢复到 100% 容量所需的时间长度不确定（包括在剩余可用区中提供所需计算容量会出现的任何延迟）。
- 您可以接受在区域出现故障时，完成生产环境的恢复所需的时间长度不确定。
- 您可以接受多区域方法带来的复杂性和成本增加。
- 您可以接受需要手动操作才能在辅助区域恢复生产。

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。
- 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。
- Amazon EFS 用于 SAP 全球文件系统，并在辅助区域上复制。
- SAP 数据库的数据定期备份到 Amazon S3。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照
- replicated/copied 为了保护逻辑数据丢失，Amazon S3 数据（数据库备份）、Amazon EBS 快照和亚马逊计算机映像存储到辅助区域。

优点

- Amazon EC2 或可用区出现故障时的平均恢复时间 (MTTR) 较低

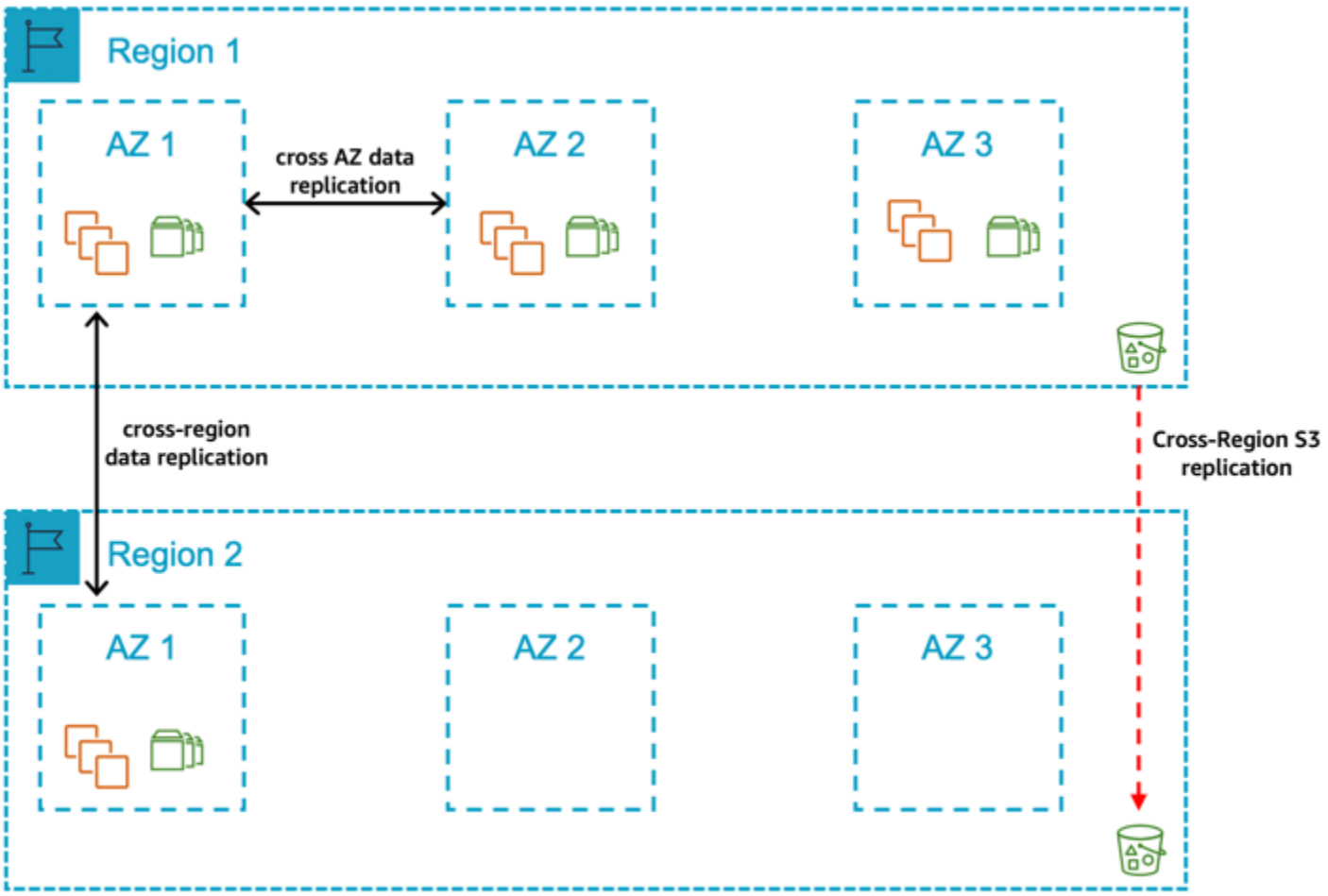
- Amazon EC2 或可用区出现故障时可预测的恢复服务 (RTS)
- 通过数据库复制功能或块级复制解决方案，将与数据库相关的数据保存在两个可用区的不同 Amazon EBS 卷集上
- 在主区域的两个可用区部署所需的计算容量
- 主区域中的某个可用区出现故障时，不必依赖于从 Amazon S3 恢复数据
- 能够将数据库和中央服务层失效转移到可用区 2，防止性能严重降级或可用区的整体故障
- 能够通过失效转移到辅助区域来防范性能严重降级或整个区域故障

注意事项

- 对于可用区之间的自动失效转移，需要有明确记录在案且经过测试的流程。
- 对于维护自动化失效转移解决方案，需要有明确记录在案且经过测试的流程。
- 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 12：一个主区域，具有两个可用区用于生产环境，辅助区域中在单个可用区内部署了计算和存储容量



在这种模式下，您跨主区域中的两个可用区部署所有生产系统。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容量大小相同，在一个可用区出现故障时，可自动进行失效转移。SAP 应用程序层所需的计算容量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 中的生产数据库备份、Amazon EBS 快照和亚马逊机器映像会复制到辅助区域。在整个区域出现故障时，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新一组备份，在辅助区域中恢复生产系统。

如需满足以下要求，请选择此模式：

- 您需要规定完成生产环境恢复的时间长度，并需要确保在主区域的另一个可用区中，提供用于生产 SAP 数据库和中央服务层的计算容量。

- 对于跨主区域中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容量，您可以接受由此产生的额外成本。
- 对于跨主区域中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容量，您可以接受由此造成的成本上升。
- 您可以接受数据复制时与跨可用区相关的数据传输费用。
- 您可以接受在可用区之间实现自动失效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的复制与数据库相关的数据（需要数据库复制功能或块级复制解决方案）。
- 您可以接受将应用程序层恢复到 100% 容量所需的时间长度不确定（包括在剩余可用区中提供所需计算容量会出现的任何延迟）。
- 您需要规定在出现区域故障时恢复生产所需的时间长度。
- 您可以接受多区域方法带来的复杂性和成本增加。
- 您需要在辅助区域的单个可用区中，确保为生产 SAP 数据库和中央服务层提供计算容量。
- 对于在辅助区域中的单个可用区为生产 SAP 数据库和中央服务层部署所需的计算和存储容量，您可以接受由此造成的成本上升。
- 您可以接受需要手动操作才能在区域之间进行失效转移。

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。
- 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 EBS 上与 SAP 数据库相关的数据。
- Amazon EFS 用于 SAP 全球文件系统，并复制到辅助区域。
- SAP 数据库的数据定期备份到 Amazon S3。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照

- replicated/copied 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存储到辅助区域。

优点

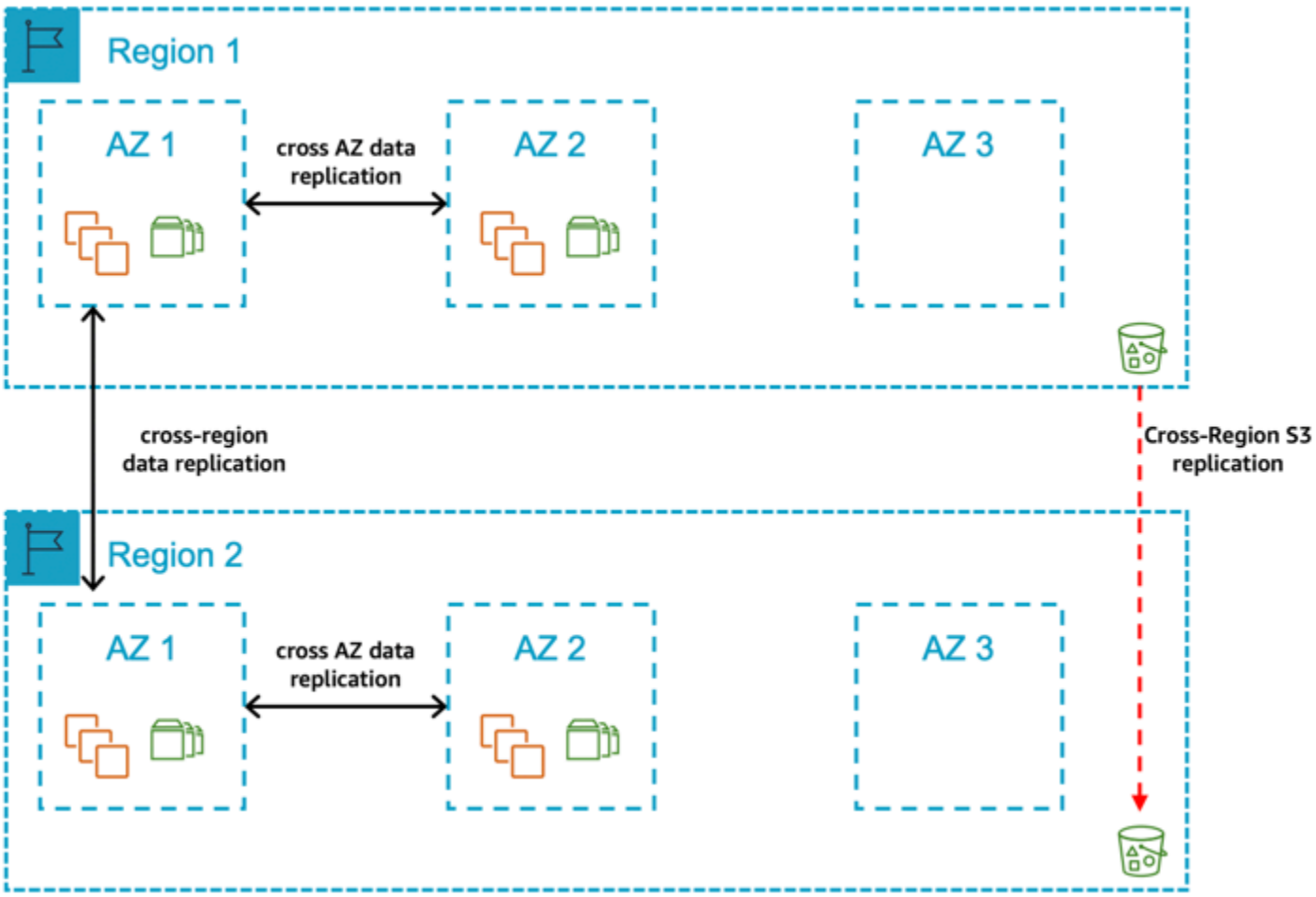
- Amazon EC2、可用区或区域出现故障时的平均恢复时间 (MTTR) 较低
- 可预测的恢复服务（RTS）
- 通过数据库复制功能或块级复制解决方案，将与数据库相关的数据保存在主区域中两个可用区的不同 Amazon EBS 卷集上，此外还保存到辅助数据库中一个可用区的卷集上
- 在主区域的两个可用区以及辅助区域的一个可用区上部署所需的计算容量
- 某个可用区或区域出现故障时，不必依赖于从 Amazon S3 恢复数据
- 能够将数据库和中央服务层失效转移到可用区 2，防止性能严重降级或可用区的整体故障
- 能够通过失效转移到辅助区域来防范性能严重降级或整个区域故障

注意事项

- 对于可用区之间的自动失效转移，需要有明确记录在案且经过测试的流程。
- 对于维护自动化失效转移解决方案，需要有明确记录在案且经过测试的流程。
- 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。
- 对于将生产环境转移到辅助区域，需要有明确记录在案且经过测试的流程。
- 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。
- 在两个不同的区域中维护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 13：一个主区域，具有两个可用区用于生产环境，在辅助区域中部署了计算和存储容量，在两个可用区之间复制数据



在这种模式下，您跨主区域中的两个可用区部署所有生产系统。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容量大小相同，在一个可用区出现故障时，可自动进行失效转移。SAP 应用程序层所需的计算容量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 中的生产数据库备份、Amazon EBS 快照和亚马逊机器映像会复制到辅助区域。在整个区域出现故障时，生产系统将手动移动到辅助区域。

如需满足以下要求，请选择此模式：

- 您需要规定完成生产环境恢复的时间长度，并需要确保在主区域的另一个可用区中，提供用于生产 SAP 数据库和中央服务层的计算容量。
- 对于跨主区域中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容量，您可以接受由此产生的额外成本。
- 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的复制与数据库相关的数据（需要数据库复制功能或块级复制解决方案）。
- 您可以接受数据复制时与跨可用区相关的数据传输费用。
- 您可以接受在可用区之间实现自动失效转移需要第三方集群解决方案。
- 您可以接受将应用程序层恢复到 100% 容量所需的时间长度不确定（包括在剩余可用区中提供所需计算容量会出现的任何延迟）。
- 您需要规定在出现区域故障时恢复生产所需的时间长度。
- 您需要在辅助区域的两个可用区中，确保为生产 SAP 数据库和中央服务层提供计算容量。
- 对于跨辅助区域中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容量，您可以接受由此产生的额外成本。
- 您可以接受多区域方法带来的复杂性和成本增加。
- 您可以接受需要手动操作才能在区域之间进行失效转移。

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。
- 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 EBS 上与 SAP 数据库相关的数据。
- Amazon EFS 用于 SAP 全球文件系统，并在辅助区域上复制。
- SAP 数据库的数据定期备份到 Amazon S3。
- 所有服务器的 Amazon Machine Image/Amazon EBS 快照都是定期拍摄的。
- replicated/copied 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存储到辅助区域。

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

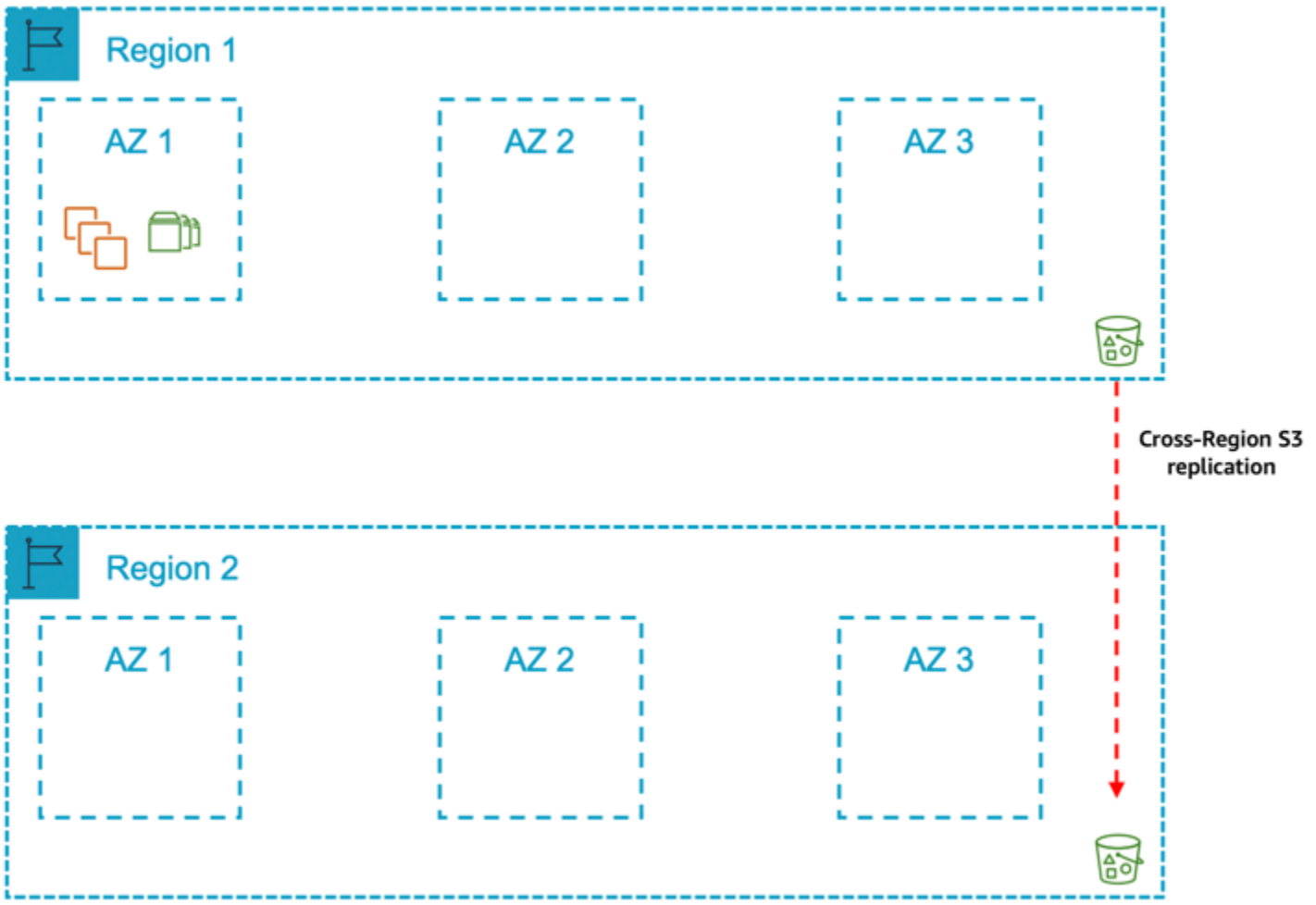
- 可预测的恢复服务（RTS）
- 通过数据库复制功能或块级复制解决方案，将与数据库相关的数据保存在主区域中两个可用区的不同 Amazon EBS 卷集上，此外还保存到辅助数据库中两个可用区的不同 Amazon EBS 卷集上
- 在主区域的两个可用区以及辅助区域的两个可用区上部署所需的计算容量
- 某个可用区或区域出现故障时，不必依赖于从 Amazon S3 恢复数据
- 能够将数据库和中央服务层失效转移到可用区 2，防止性能严重降级或可用区的整体故障
- 能够通过失效转移到辅助区域来防范性能严重降级或整个区域故障

注意事项

- 对于可用区之间的自动失效转移，需要有明确记录在案且经过测试的流程。
- 对于维护自动化失效转移解决方案，需要有明确记录在案且经过测试的流程。
- 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。
- 对于将生产环境转移到辅助区域，需要有明确记录在案且经过测试的流程。
- 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。
- 在两个不同的区域中维护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。您的非生产系统的大小与生产系统不相等，并且部署在该区域内的相同可用区或不同可用区中。

此外，存储在 Amazon S3 中的生产数据库备份、Amazon EBS 快照和亚马逊机器映像会复制到辅助区域。如果整个区域出现故障，生产系统将在辅助区域中从最新一组备份恢复。

如需满足以下要求，请选择此模式：

- 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。
- 您可以接受在区域出现故障时，完成生产环境的恢复所需的时间长度不确定的风险。
- 您希望避免多可用区方法带来的成本影响，并可以接受生产 SAP 系统停机时间的相关风险。
- 您可以接受多区域方法带来的复杂性和成本增加。
- 您可以接受需要手动操作才能在辅助区域恢复生产。

关键设计原则

- 100% 的计算容量部署在可用区 1 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，不到为生产 SAP 数据库和中央服务层部署的计算容量的 100%。
- 仅将 SAP 数据库保存在单个可用区中的 Amazon EBS 上，并且不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 数据库定期备份到 Amazon S3。
- 配置 Amazon S3 单区域复制来防范逻辑数据丢失。
- 定期为所有服务器拍摄 Amazon Machine Image/Amazon EBS 快照。
- replicated/copied 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存储到辅助区域。

优点

- 与多可用区相比，成本更低
- 能够通过失效转移到辅助区域来防范性能严重降级或整个区域故障

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。
- 由于采用两个可用区缺乏高可用性，因此在计算容量、可用区或区域出现故障时，恢复生产所需的时间会增加。

Summary

下表总结了这些模式及其主要特征。

#	单个区域	多区域	主区域单可用区	主区域多可用区	辅助区域单可用区	辅助区域多可用区	第 2 个可用区中的生产容量	非生产容量的使用	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：模式总结

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。您可以根据自己的 SAP 系统，选择最符合业务需求的模式。这可以让您免于根据最高要求进行选择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，这样就能降低总拥有成本。

如果您的需求随着时间推移发生变化，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，您可能不需要另一个可用区中的高可用性计算容量，但在产品上线之前的几周，您可能会在第二个可用区部署容量。

在AWS云端选择运行 SAP 系统的架构模式时，应考虑以下几点：

- 数据的驻留地理位置

- 生产 SAP 系统停机时间对企业的影响
- 恢复时间目标
- 恢复点目标
- 成本分析

适用于 Microsoft SQL Server 的 SAP on AWS 架构模式

本文档提供了有关在 AWS Cloud on Microsoft SQL Server 上部署 SAP 工作负载的架构模式的信息。这些模式提供高可用性和高韧性的实施选项，同时考虑到了恢复时间目标和恢复点目标。

从业务需求出发逆向思维，定义能够满足 SAP 系统和数据可用性目标的方法。对于每种故障场景，韧性要求、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相当。

您可以根据自己的具体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，以及防范问题的成本。

主题

- 模式
- 比较表
- Microsoft SQL Server 的单区域架构模式
- 适用于 Microsoft SQL Server 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

比较表

下表提供了所有架构模式的对比，这些内容将会进一步讨论。

模式	业务需求	解决方案特征	实施详情

	韧性类型	恢复点目标	恢复时间目标	成本	复杂度较高：	SQL AlwaysOn	Amazon S3 复制
模式 1	单区域灾难恢复	接近零*	低	中	中	2 层	不适用
模式 2		中	高	非常低	非常低	不适用	不适用
模式 3	多区域复制灾难恢复	中	高	中	中	2 层	跨区域
模式 4		接近零*	低	高	高	3 层	跨区域
模式 5		中	高	低	低	不适用	跨区域
模式 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 区域内设置采用同步数据提交模式的数据库复制。

Microsoft SQL Server 的单区域架构模式

单区域架构模式有助于避免网络延迟，因为 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。如需更多信息，请参阅 AWS 全球基础设施地图。

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

以下是两种单区域架构模式。

模式

- 模式 1：单个区域，具有两个可用区用于生产环境
- 模式 2：单个区域，具有一个可用区用于生产环境

模式 1：单个区域，具有两个可用区用于生产环境

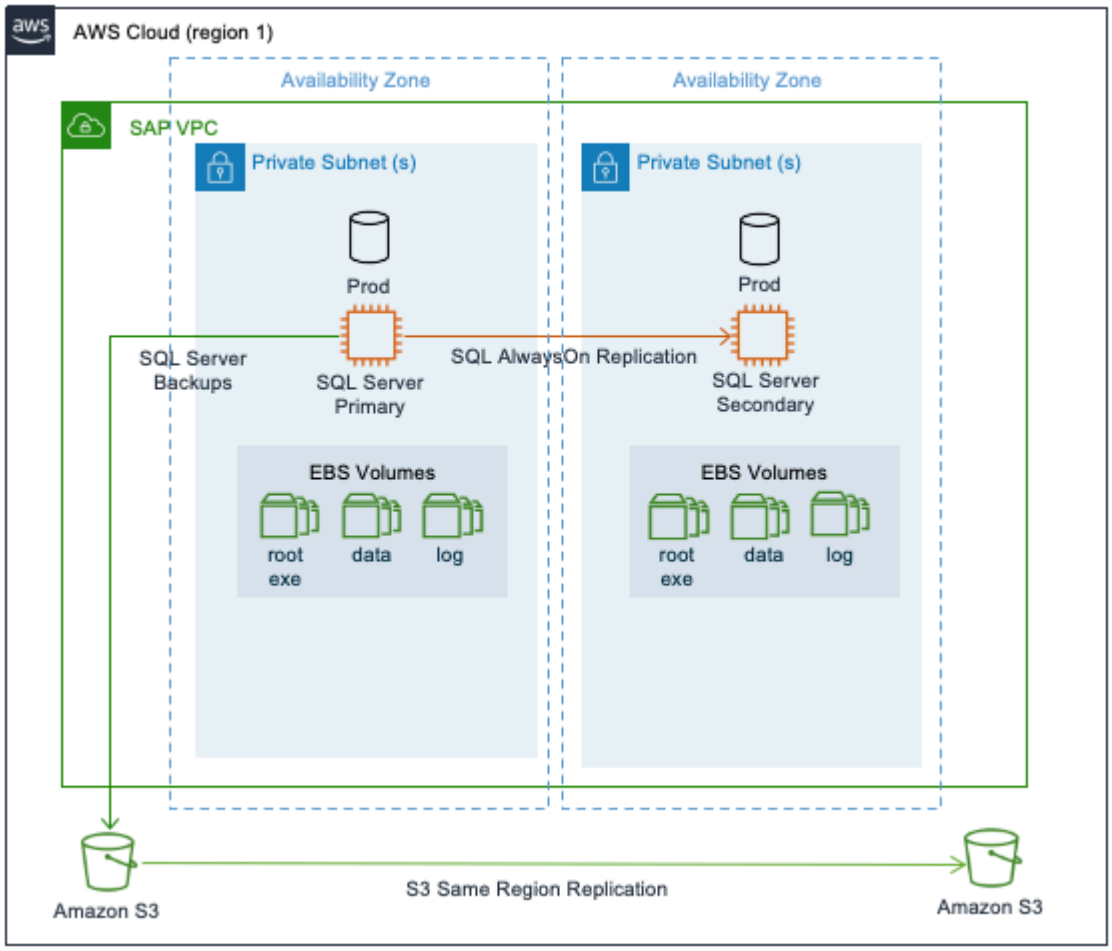
在这种模式下，您的 Microsoft SQL Server 部署在两个可用区域中，两个实例上都配置了 AlwaysOn。主实例和辅助实例的实例类型相同。辅助实例可以在主动/被动或主动/主动模式下部署。我们建议使用同步复制模式，在两个可用区之间实现低延迟连接。

如果您正在寻找用于自动失效转移的高可用性集群解决方案，以实现接近零的恢复点目标和恢复时间目标，则可以将此模式作为基础。为自动失效转移使用 SQL AlwaysOn with Windows 集群，可在出现故障时（包括罕见的可用区丢失）提供韧性。

您需要考虑 AlwaysOn 配置的额外许可成本。此外，预置与生产环境中相同的实例类型作为备用实例，会增加总拥有成本。

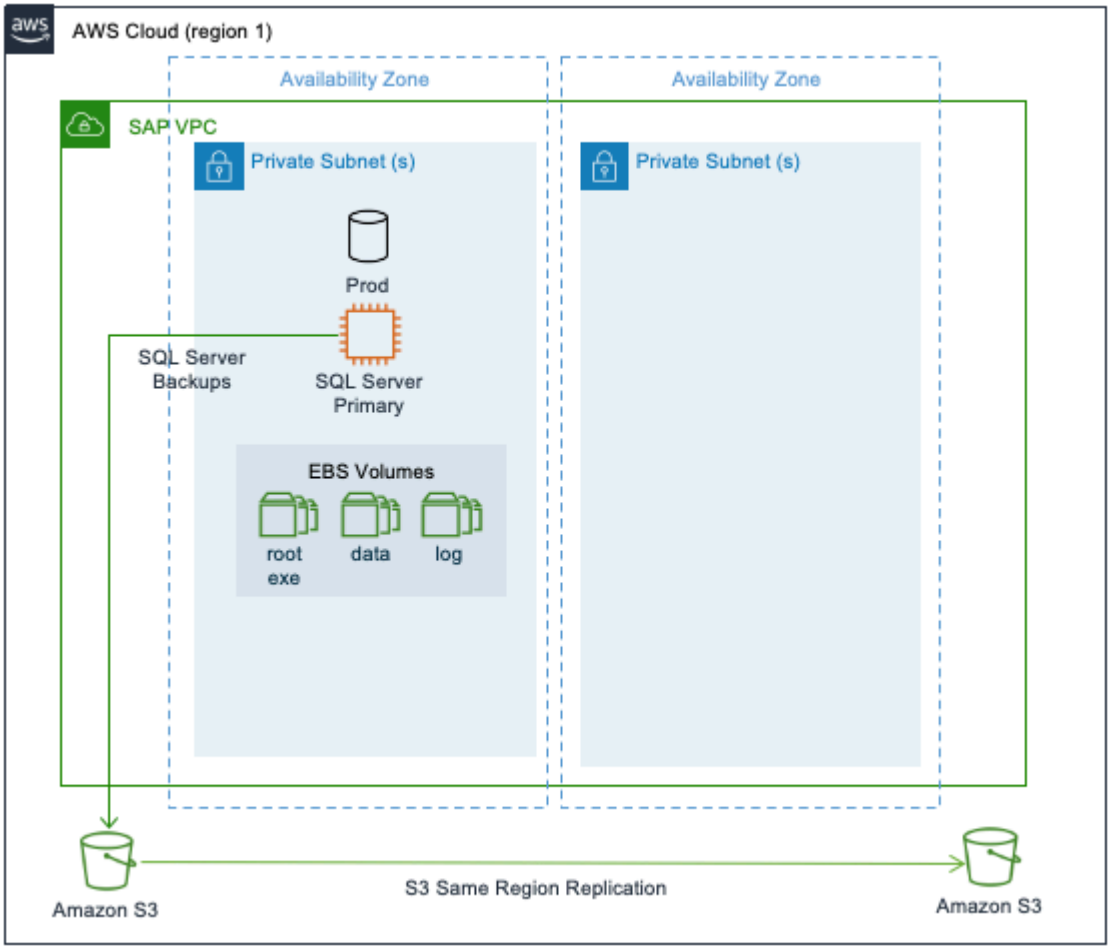
Microsoft SQL Server 备份可以存储在 Amazon S3 存储桶中。Amazon S3 对象会自动存储在单个区域中至少三个可用区的多个设备中。为了防范逻辑数据丢失，您可以使用 Amazon S3 的同区域复制功能。

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。此策略可确保不会因为恶意活动或人为错误导致所有数据副本丢失。要设置同区域复制，请参阅设置复制。



模式 2：单个区域，具有一个可用区用于生产环境

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。在故障场景中用于恢复业务运营的选项，出现实例故障时通过 Amazon EC2 自动恢复功能提供，出现影响可用区的重大问题时从最新的有效备份中还原和恢复。



适用于 Microsoft SQL Server 的多区域模式

AWS 全球基础设施覆盖全球众多区域，并且设施规模仍在不断增长。有关最新更新，请参阅 AWS 全球基础设施。如果您希望在任何时间点 SAP 数据都会存放在多个区域，以确保在出现故障时提高可用性并尽可能减少停机时间，则应选择多区域架构模式。

部署多区域模式时，您可以获益于自动化方法（例如集群解决方案）的使用，这样可以自动在可用区之间进行失效转移，从而最大限度地减少总停机时间并消除人为干预的需求。多区域模式不仅提供了高可用性，还可以实现灾难恢复，从而降低总体成本。所选区域之间的距离会直接影响延迟，因此在多区域模式的整体设计中必须考虑这一点。

跨区域复制或数据传输还会对成本产生额外的影响，在解决方案的总体定价中也需要考虑这些影响。不同区域的定价各不相同。

以下是四种多区域架构模式。

模式

- 模式 3：主区域具有两个可用区用于生产环境，辅助区域包含备份的副本/AMI
- 模式 4：主区域具有两个可用区用于生产环境，辅助区域中在单个可用区内部署了计算和存储容量
- 模式 5：主区域具有一个可用区用于生产环境，辅助区域包含备份的副本/AMI
- 模式 6：主区域具有一个可用区用于生产环境，辅助区域使用 AWS 弹性灾难恢复在块级进行复制

模式 3：主区域具有两个可用区用于生产环境，辅助区域包含备份的副本/AMI

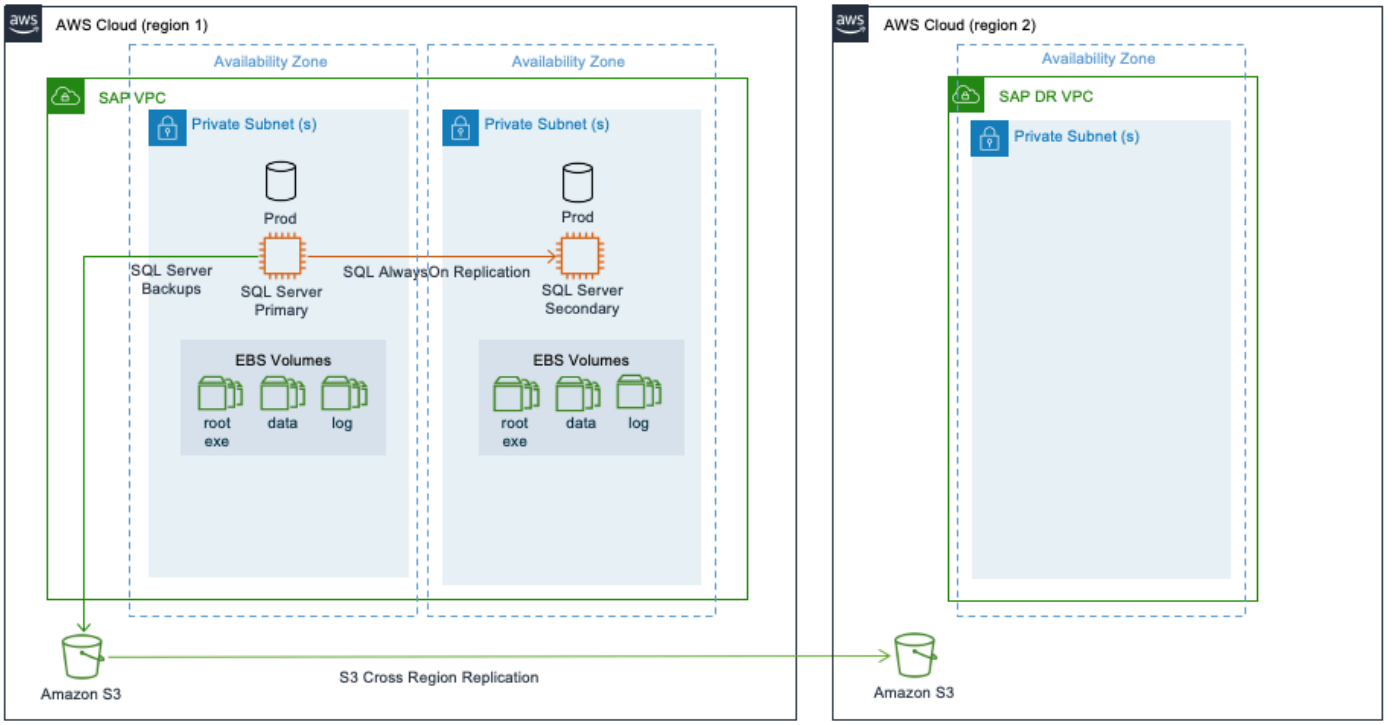
这种模式类似于模式 1，Microsoft SQL Server 实现了高可用性。您使用 AlwaysOn，跨主区域中的两个可用区部署生产实例。您可以使用存储在 Amazon S3 中的备份副本、Amazon EBS 和亚马逊机器映像（AMI），在辅助区域中恢复 SQL 数据库。

通过跨区域复制存储在 Amazon S3 中的文件，存储桶中存储的数据会自动（异步）复制到目标区域。Amazon EBS 快照可以在区域之间复制。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、AWS SDK 或 Amazon EC2 API，在区域内或跨区域复制 AMI。有关更多信息，请参阅复制 AMI。您还可以使用 AWS Backup 来调度和运行快照以及跨区域复制。

在整个区域出现故障时，需要使用 AMI 在辅助区域中构建生产 SQL Server。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 下载最新的一组备份，将您的 SQL Server 恢复到灾难事件发生之前的时间点。在辅助区域还原并恢复 SQL Server 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，能够在出现故障时立即进行失效转移。对于主区域之外的灾难恢复，恢复点目标受以下因素限制：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需的时间。您可以使用 Amazon S3 Replication Time Control 进行限定时间的复制。有关更多信息，请参阅启用 Amazon S3 Replication Time Control。

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。所需时间随数据库的大小而变。此外，在没有预留实例容量的情况下，恢复过程获得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目标和恢复点目标，而对于在主区域之外进行灾难恢复可以接受较高的恢复点目标和恢复时间目标时，这种模式非常适合。



模式 4：主区域具有两个可用区用于生产环境，辅助区域中在单个可用区内部署了计算和存储容量

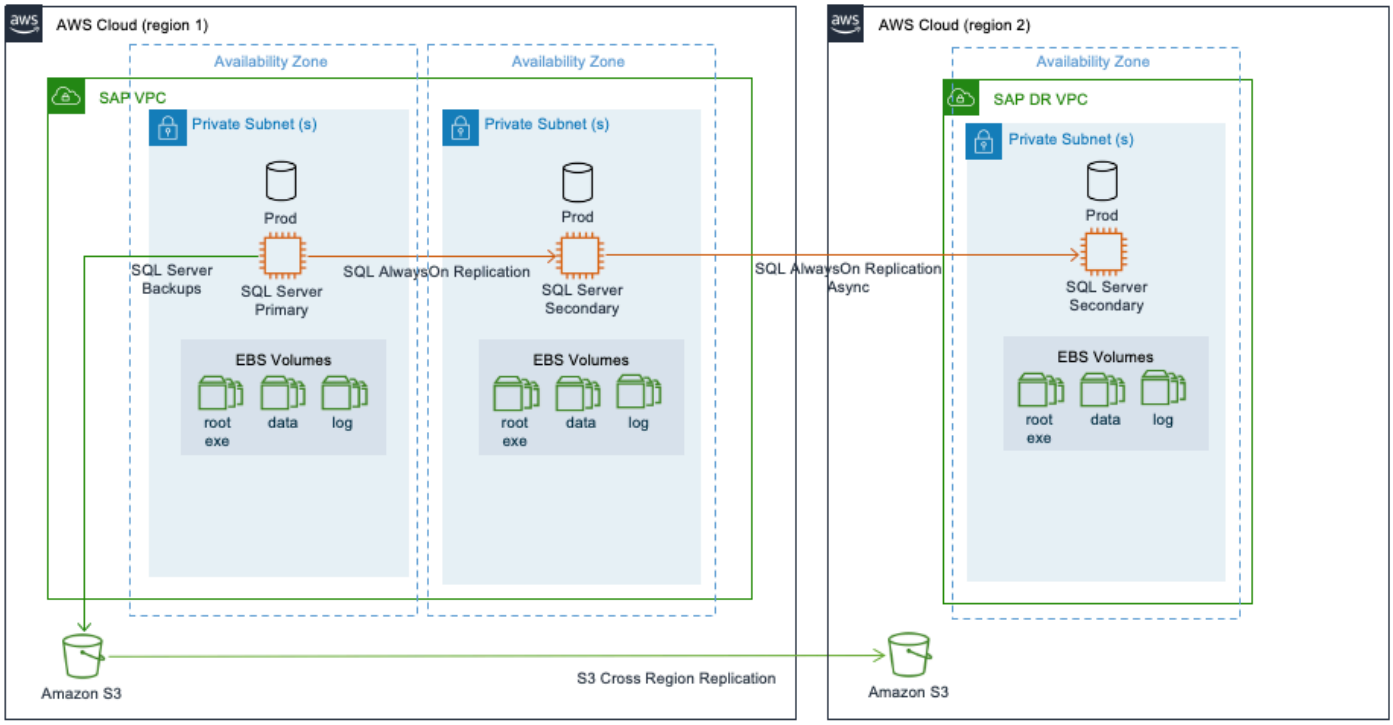
在模式 3 的架构之外，此模式还在主区域的 SQL Server 与辅助区域的一个可用区中相同的第三个实例之间设置了 SQL AlwaysOn。在 AWS 区域之间复制时，由于延迟增加，我们建议使用 SQL AlwaysOn 的异步模式。

主区域发生故障时，生产工作负载将手动失效转移到辅助区域。这种模式可确保 SAP 系统具有高可用性和容灾能力。这种模式通过连续数据复制，提供了更快的失效转移和业务运营连续性。

为辅助区域中的生产 SQL Server 部署所需的计算和存储容量，以及区域之间的数据传输，会导致成本增加。当您需要在主区域之外进行灾难恢复并需要较低的恢复点目标和时间目标时，这种模式非常适合。

这种模式可以部署在多层复制配置以及多目标复制配置中。

下图显示了以链式方式配置复制的多层复制。

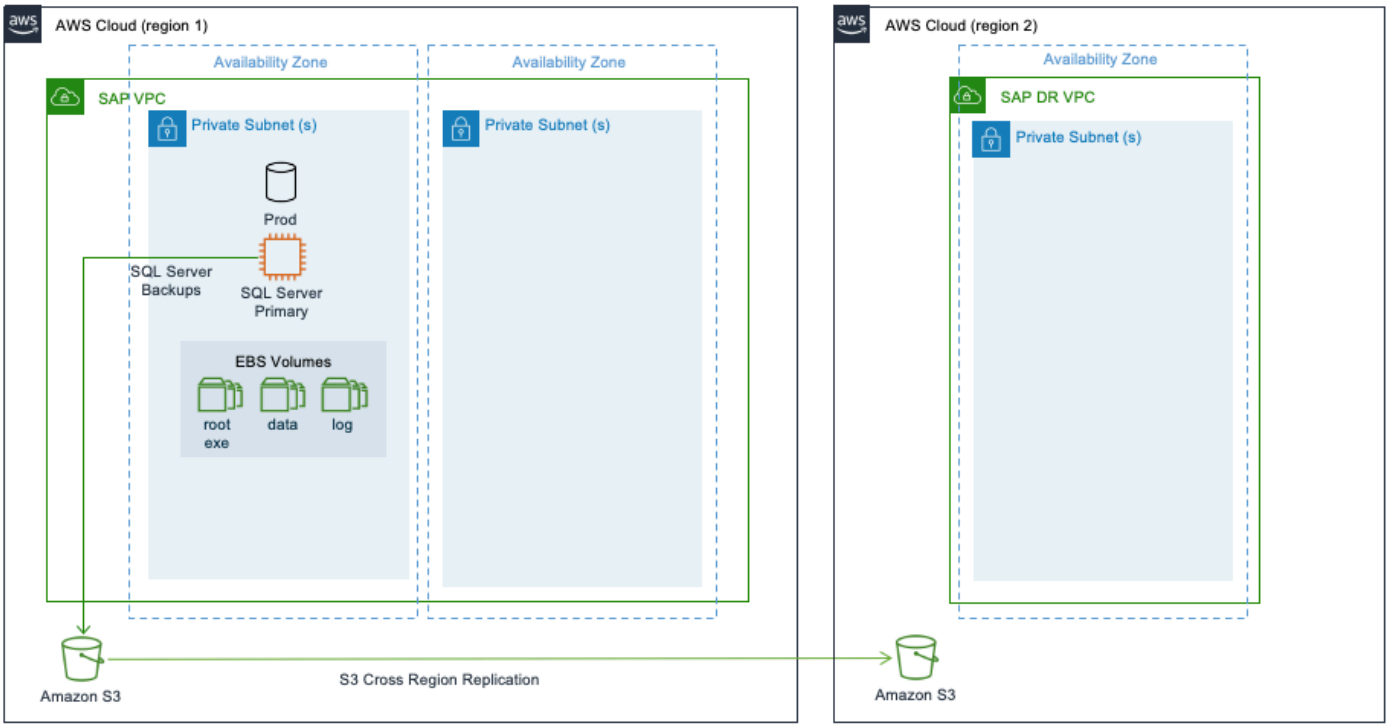


模式 5：主区域具有一个可用区用于生产环境，辅助区域包含备份的副本/AMI

这种模式与模式 2 类似，但辅助区域中包含存储在 Amazon S3 中的 SQL Server 备份副本、Amazon EBS 快照和 AMI，可以进行额外的灾难恢复。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，没有用于复制数据的目标 SQL 系统。

在这种模式下，您的 SQL Server 不具备高可用性。在整个区域出现故障时，需要使用 AMI 在辅助区域中构建生产 SQL Server。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 下载最新的一组备份，将您的 SQL Server 恢复到灾难事件发生之前的时间点。然后，您可以使用 DNS，将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，恢复点目标受以下因素限制：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需的时间。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。所需时间随数据库的大小而变。这种模式适用于可以容忍停机时间以恢复正常运行的非生产系统或非关键生产系统。



模式 6：主区域具有一个可用区用于生产环境，辅助区域使用 AWS 弹性灾难恢复在块级进行复制

AWS 弹性灾难恢复向企业提供了现代化的方法，通过在 AWS 云上启用云端灾难恢复来保护 Microsoft SQL Server 环境。有关更多信息，请参阅什么是弹性灾难恢复？

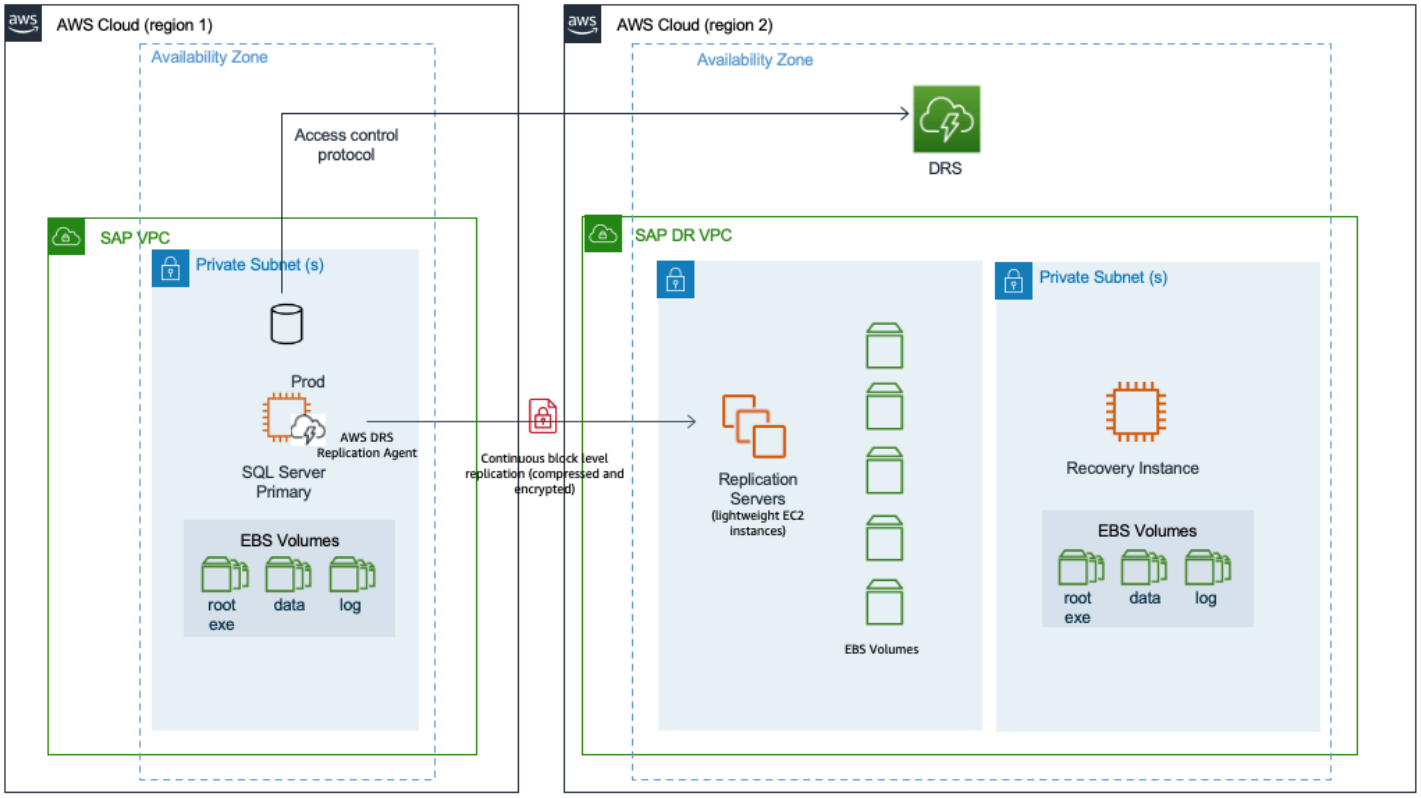
弹性灾难恢复使用块级复制，为支持的 Windows 和 Linux 操作系统版本复制操作系统、数据库、应用程序和系统文件。要了解更多信息，请参阅支持的操作系统。弹性灾难恢复需要在源系统上完成 AWS 复制代理的初始设置，才能启动安全的数据复制。代理在内存中运行，识别对本地连接的磁盘的写入操作。这些写入操作会被捕获并异步复制到 AWS 账户中的暂存区。在此持续复制过程中，弹性灾难恢复会维护同一源服务器中所有磁盘的写入顺序。复制的 Amazon EC2 实例可以在测试模式下运行，以便在分隔的环境中用于开展演习。

通过弹性灾难恢复，您可以监控恢复实例的数据复制状态、查看恢复实例的详细信息、向弹性灾难恢复添加恢复实例、编辑恢复实例的失效自动恢复设置以及终止恢复实例。

通过弹性灾难恢复，您可以在 AWS 云上启动恢复实例来执行失效转移。启动恢复实例后，您必须将流量从主站点重定向到恢复站点。

AWS 弹性灾难恢复使用 Amazon EBS 快照，拍摄暂存区内所保存数据的时间点快照。要了解更多信息，请参阅 Amazon EBS 快照。然后，此服务提供崩溃一致性时间点恢复选项，可在发生灾难或演习

时使用。弹性灾难恢复可以保护 SQL Server AlwaysOn 可用性组的各个节点。在灾难恢复期间，该组作为单个 SQL Server 实例在 AWS 上启动。此解决方案适用于任何支持的 SQL Server 版本的 SQL Server Standard 版和 SQL Server Enterprise 版。



使用 AWS 弹性灾难恢复服务对 AWS 上的 SAP 工作负载进行灾难恢复

自然事件（地震、飓风或洪水）导致的灾害、应用程序故障、技术故障或人为操作会导致应用程序出现停机时间，可能出现数据丢失，进而影响收入。为了防范此类情况，您可以制定业务连续性计划，将灾难恢复作为关键要素。对于运行任务关键型应用程序（例如 SAP）的企业而言，设计、实施和维护灾难恢复计划至关重要。有关更多信息，请参阅业务连续性计划（BCP）。

AWS 弹性灾难恢复使企业能够轻松快速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 云端，可以是现有的物理或虚拟数据中心，也可以托管在私有云或其他云提供商处。我们建议使用弹性灾难恢复为您的 SAP 工作负载实施灾难恢复计划，将 AWS 作为灾难恢复环境，源环境可以在 AWS 云端也可以不在。您可以从弹性灾难恢复控制台访问弹性灾难恢复服务。

弹性灾难恢复需要在源系统上完成 AWS 复制代理的初始设置，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，复制到弹性灾难恢复支持的任何 AWS 区域。将源系统复制到暂存区中的复制服务器，使用经济实惠的存储、共享服务器和尽可能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（称为演习），来确认您的弹性灾难恢复实施已为灾难恢复场景做好准备。当您启动用于演习或恢复的实例时，弹性灾难恢复会自动转换您的服务器以在 AWS 云端引导并原生运行。该服务还会在复制时，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，则使用最新的快照或较早的 PIT 快照，只需几分钟时间就可以在 AWS 云端启动恢复实例。应用程序运行在 AWS 云端之后，您可以选择将其保留在云端，也可以在问题解决后启动数据复制来恢复到主站点。您可以使用弹性灾难恢复工具（例如失效自动恢复客户端）切回到主站点。

有关更多信息，请参阅什么是弹性灾难恢复？

主题

- 场景
- 参考信息
- 服务水平协议和 SAP 许可证
- 网络、存储和计算
- 灾难恢复场景
- 共享存储韧性
- 在AWS云上为 SAP 工作负载实施灾难恢复

场景

本文档探讨了以下灾难恢复场景。

- 区域内：源工作负载在 AWS 云上运行，灾难恢复实施使用相同 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，灾难恢复实施使用另一个 AWS 区域。选择其他区域可能是出于合规原因。
- AWS 之外：源工作负载运行在 AWS 云之外（本地部署、公共云或私有云），使用 AWS 云实施灾难恢复。

参考信息

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

了解指导灾难恢复解决方案的设计和实施的关键业务要求非常重要，这包括恢复点目标、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 AWS 云端灾难恢复实施相关的概念。

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

如果您不熟悉 AWS，请参阅以下文档。

- 开始使用 AWS
- 什么是 Amazon EC2？
- Amazon VPC 是什么？
- Amazon Elastic Block Store（Amazon EBS）

要高效地利用此处提供的这些信息，您必须具有在 AWS 云端安装、迁移和操作 SAP 环境和系统的经验，以及实施高可用性和灾难恢复解决方案的经验。

服务水平协议和 SAP 许可证

对于灾难恢复实施，服务水平协议（SLA）用于定义在因灾难事件导致工作负载不可用时，系统在避免数据丢失和减少停机时间方面的韧性。

SAP 系统灾难恢复方法需要复制应用程序层、数据库层以及所有文件共享，例如 NFS 挂载。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以多快的速度恢复。在发生灾难时，弹性灾难恢复使您能够在几分钟内，在目标区域上启动复制的服务器，使其进入完全预置的状态，从而继续运行业务。这种自动化方法可以实现低 RTO，并且比手动方法更快、更高效。

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）的传播] 以及环境因素（包括灾难恢复团队的反应时间、目标环境的存储架构、操作系统的引导和应用程序启动时间），都会影响该目标值。

恢复点目标 (RPO)

弹性灾难恢复使用异步的块级复制，持续将更改复制到目标站点的磁盘。弹性灾难恢复的 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所花费的时间。源系统上的事务量会对此造成进一步的影响。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。在计算灾难恢复事件期间可能丢失的数据量时，这些因素都应考虑在内。

考虑

由于弹性灾难恢复管理某些场景的方式，可能会不时观察到 SAP 工作负载的数据丢失量超出了亚秒级 RPO 下的预期水平。

发生硬重新引导、磁盘更改和崩溃时，弹性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。这会造成两台服务器之间的延迟。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）可能会比预期的要多。

重新扫描时间取决于多个因素，不进行测试就无法预测。重新引导源服务器后，可能会进行重新扫描。重新扫描时间将根据源磁盘的大小而变。具体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）。只要重新扫描还在继续执行并且没有“卡住”，操作就在正常运行。

SAP 数据库的磁盘可能会很大，更改率也可能会很高。我们建议您进行测试，以确保出现此类事件时能够满足您的 SLA 要求。此外，您必须确保主数据库与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 系统紧密集成并且数据在这些系统之间频繁交换，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。对于灾难恢复失效转移，系统组内可能会要求 RCO 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

弹性灾难恢复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 系统通过使用硬件密钥的许可证进行保护。开启 AWS，硬件密钥基于您的 Amazon EC2 实例 ID。您必须启动 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 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 SAP 许可证。如果您需要灾难恢复实例在 28 天后继续运行，则可以使用恢复 Amazon EC2 实例 ID 申请新 SAP 许可证。

网络、存储和计算

此部分提供有关为暂存环境和目标环境配置网络、存储和计算，以便通过弹性灾难恢复实现 AWS 云端 SAP 工作负载的灾难恢复目标的信息。

主题

- 网络

- 存储
- 计算

网络

在支持高效达成 RTO 和 RPO SLA 方面，用于灾难恢复的网络架构和配置发挥着重要作用。您必须考虑触发灾难恢复时的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。您可以在私有网络和公有网络之间选择。有关更多信息，请参阅数据路由和节流。

无论采用何种方法，传输的数据在传输过程中始终加密。默认方法是公有网络，即数据通过互联网路由到复制服务器上的公共网络接口。在私有网络方法中，数据通过私有网络进行复制。私有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：私有网络通常是 VPC 之间的连接，使用 Amazon VPC 对等连接或 AWS Transit Gateway 进行连接。建议为灾难恢复使用不同的 AWS 账户和单独的 Amazon VPC。有关更多信息，请参阅什么是 Amazon VPC 对等？和什么是 Transit Gateway？
- AWS 跨区域灾难恢复：建议使用完全冗余的 AWS 网络主干，将不同 AWS 区域连接在一起。Amazon VPC 对等连接和 AWS Transit Gateway 支持区域间的连接。有关详细信息，请参阅 Introduction to Network Transformation on AWS。
- AWS 外部向 AWS 的灾难恢复：在此场景中，您的源网络与 AWS 之间的物理网络由不同电信提供商或互联网服务提供商（ISP）提供。AWS 上提供以下解决方案。
  - AWS Direct Connect
  - AWS Site-to-Site VPN
  - AWS Marketplace 上提供的 SD-WAN

SAP on AWS 客户通常使用 AWS Direct Connect。相比采用 VPN 或 SD-WAN 的解决方案，此服务为基于服务水平协议（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

建议使用称为暂存区子网的子网来托管复制服务器。称为“恢复子网”的其他子网是必需的灾难恢复操作目标。对于源网络位于 AWS 云端的场景，请考虑如何根据您选择的 AWS 账户策略和登录区来分配子网。通常，这可能意味着暂存区子网应与您的源服务器位于不同的 Amazon VPC 中。对于简化的环境，这可能只是在相同 Amazon VPC 中使用不同的子网。这意味着减少了生产与非生产灾难恢复环境之间的隔离。有关更多信息，请参阅 AWS Well-Architected Framework：最佳实践 5.3。

最终，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，请参阅网络示意图。

对于 AWS 区域内灾难恢复场景，我们建议将暂存区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。启动的恢复实例将由单独的可用区中的暂存区提供保护。这遵循了使用多个可用区来保持韧性的设计原则。

配置网络安全设置

确保配置了所需的网络安全设置。这包括在本地防火墙、网络安全设备、安全组或网络访问控制列表（网络 ACL）中允许通过多个端口进行访问，根据您的源环境位置，可能还需要完成其他任务。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

以下介绍了一些因素，会影响到与最终用户和集成相关的网络流量如何对您的 RTO 和 RPO 产生影响。

- 客户端识别并解析为新 IP 的 DNS 传播时间
- 用于重新路由流量的网络组件（如有）中的延迟，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 Global Accelerator 或 Amazon Route 53 公共数据面板

有关更多信息，请参阅云中的灾难恢复选项。

存储

AWS 弹性灾难恢复设计用于根据源服务器性能，为您的暂存环境评估和定义最佳 Amazon EBS 卷设置。演习和恢复服务器使用默认性能设置。这些卷可以调整大小来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。这可确保实现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
- 演习和恢复实例
- 时间点恢复

复制服务器

暂存区需要存储空间来支持从源计算机持续进行复制。这些 Amazon EBS 卷通常是低成本的硬盘驱动器（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进行更改，转为采用性能更高的固态硬盘（SSD）存储类型。对于复制服务器，Amazon EBS 卷类型的默认设置自动卷类型选择是推荐用于 SAP 工作负载的设置。它会根据工作负载的要求，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）来提高暂存区的性能。这对 SAP 工作负载有明显的好处，例如数据库在遇到突发或持续高事务速率时，具有高速率的创建、更新和/或删除操作需要应用到存储。对于此类工作负载，建议您监控 Amazon CloudWatch 指标，并检查是否存在任何持续或不断增加的延迟。您可以将以下 CloudWatch 指标用于弹性灾难恢复。

- LagDuration：最新的一致性快照的寿命，以秒为单位
- Backlog：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，您可以更改 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

演习和恢复实例

对于 90% 或更多的使用案例，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。如果您要求每个卷的 IOPS 超过 16000 IOPS，或者要求每个卷的吞吐量大于 1000 MiB/s，请考虑 `io2` 或 `io2 Block Express` 卷。

当您启动演习或恢复实例时，弹性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。启动模板由弹性灾难恢复自动生成，对于存储性能采用默认设置，使用通用型 SSD（卷大小与源系统容量要求相匹配）。检查启动模板，确认启动模板的默认分配满足了工作负载的存储需求。

您可以针对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。有关更多信息，请参阅支持的实例类型。对于 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。在将模板与弹性灾难恢复结合使用时，建议不要在模板中添加或移除 Amazon EBS 卷。

对于在使数据可供使用之前需要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，则可以为存储定义更多的预调配吞吐量和 IOPS，和/或使用 `io2 Block Express` 等（采用支持的 Amazon EC2 实例类型）性能更高的扩展存储，这样可以缩短演习或恢复实例处理预期工作负载数量所需的时间。演习或恢复实例完全上线后，您可以进行更改来恢复存储设置。有关更多信息，请参阅 Amazon EBS 弹性卷。您还可以在不分离卷或重启实例的情况下，增加卷大小、更改卷类型或者调节 Amazon EBS 卷的性能。

时间点恢复

AWS 弹性灾难恢复使用 Amazon EBS 快照来提供可在演习或恢复期间使用的时间点（PiT）恢复选项。Amazon EBS 的暂存快照连续拍摄卷，用来提供最新（亚秒级 RPO）的恢复点，第一个小时内以 10 分钟为增量，24 小时内以 1 小时为增量。每日 PiT 将保留在您的时间点（PiT）策略中指定的天数。您可以指定 1 到 365 天之间的值，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
- 演习和恢复实例
- 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，最多可以复制 15 个卷。您可以在 SAP 应用程序服务器之间或者其他更改率较低的服务器之间使用共享的复制服务器。

如果您遇到了突发工作负载或者数据库的事务速率一直很高，存在大量创建、更新和/或删除操作需要应用到存储，则可能需要对暂存区进行不同的配置。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复制服务器。这种更改可能会影响成本。有关更多信息，请参阅复制服务器配置。

演习和恢复实例

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

以下介绍了一些与计算相关的因素，可能会影响到灾难恢复解决方案的 RTO。

- 服务器启动时间
- SAP 运行在 Microsoft Windows Server 操作系统上
- 大型 SAP HANA 数据库，启动时间超过 10 分钟
- SAP 应用程序安装在服务器上，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，目标端配置的计算能力或存储性能较低会增加 RTO

您必须将应用程序启动时间作为恢复过程中的因素来考虑。我们建议选择能够提供快速启动时间的 Amazon EC2 实例类型和存储配置。这有助于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习，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、基础设施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的云端，则它必须与 Amazon EC2 和弹性灾难恢复兼容。源服务器必须采用针对 x86 系统架构构建的 64 位操作系统。AWS 提供了各种基于 x86 的 CPU 供源服务器使用，尤其是当服务器是旧型号的情况下。建议使用基于 SAP 调整大小的方法，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 Sizing 信息。

源服务器

虽然对复制代理的系统要求相对较低，但需要考虑源服务器上的 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场景。

主题

- AWS 区域内灾难恢复
- AWS 跨区域灾难恢复
- AWS 外部向 AWS 的灾难恢复

AWS 区域内灾难恢复

在 AWS 云中，可用区之间相隔合理的距离，并且不超过 100 公里（彼此之间相距不超过 60 英里）。此距离能够隔离可能会影响数据中心的最常见灾害，例如，洪水、火灾、暴风雨、地震等。如今，许多 AWS 客户都使用此方法来支持对 SAP 工作负载的韧性要求。根据您的业务连续性要求，可能适合使用区域内灾难恢复。有关更多信息，请参阅单区域架构模式。

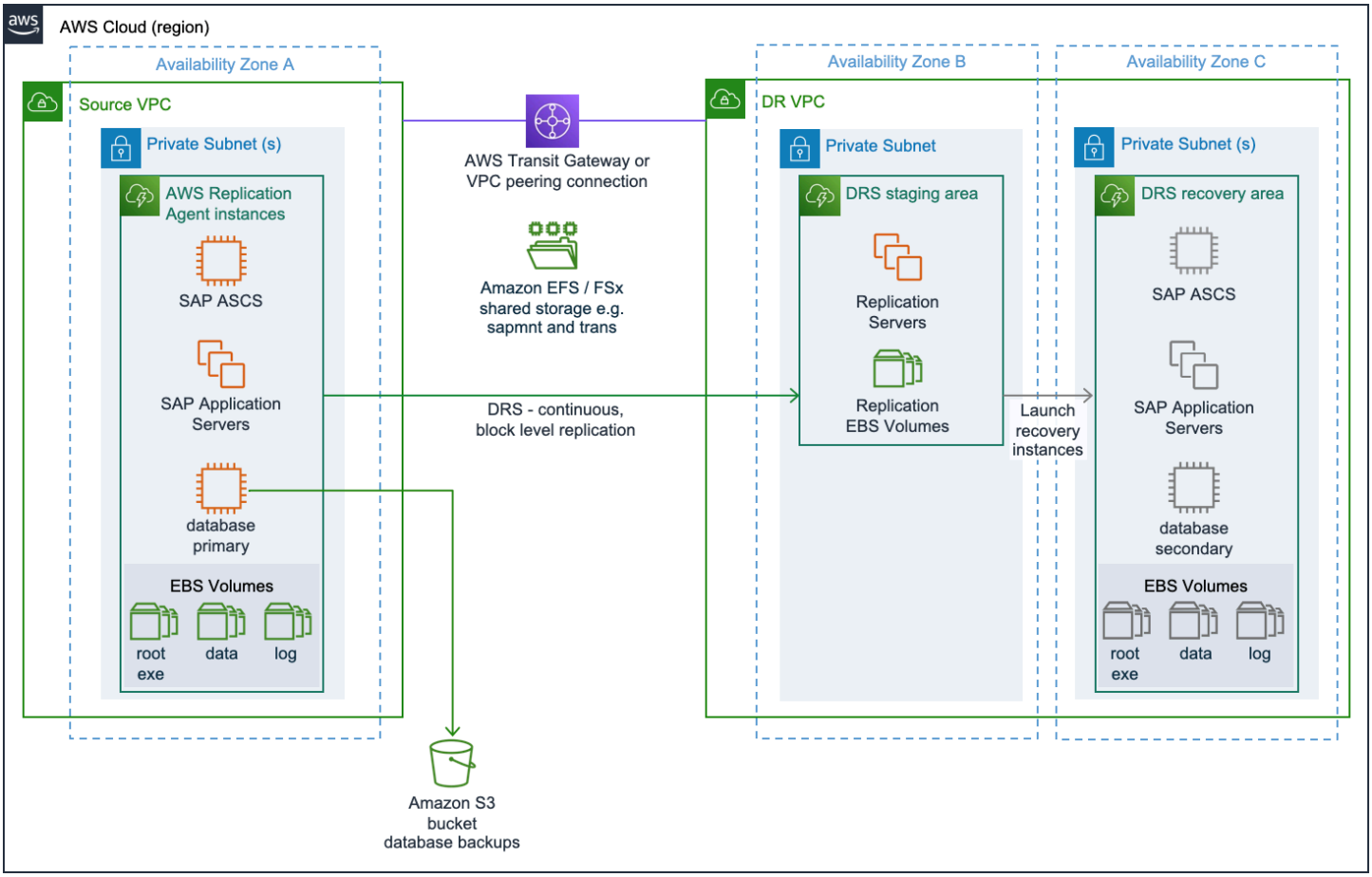
最佳实践

- 将源区和恢复区的 Amazon VPC 分开放在同一区域中
- 分隔源区和恢复区的 AWS 账户
- 使用 AWS Transit Gateway 或 Amazon VPC 对等连接来支持复制流量和最终用户连接

  有关更多信息，请参阅网络。
- 用于数据保护的 Amazon S3 存储桶和 Amazon EFS 采用多个可用区来获得韧性
- 将源区、暂存区和恢复区分隔在不同可用区中

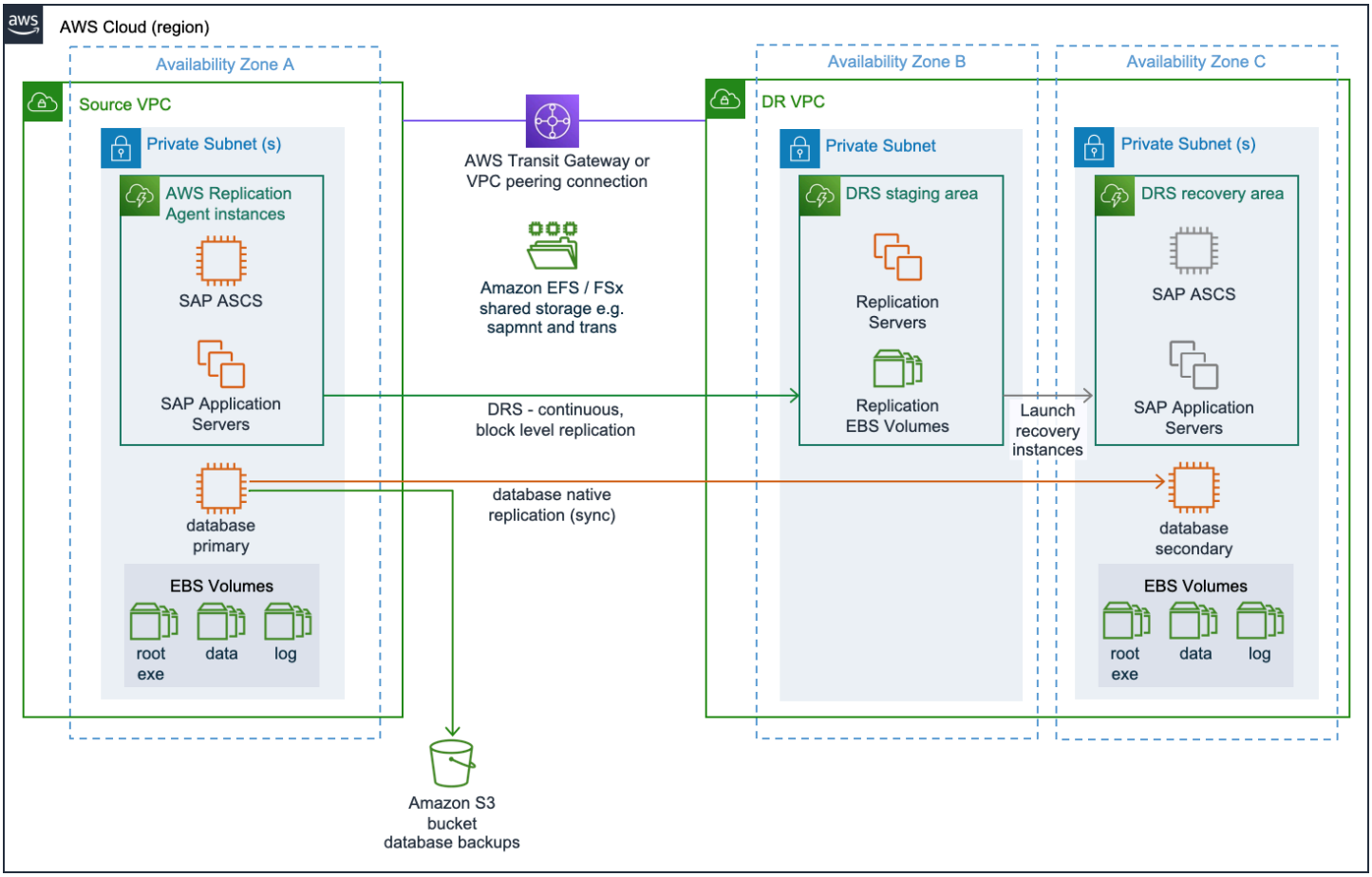
以下两个部分介绍此场景的参考架构。

完整区域内灾难恢复实施



在完整区域内灾难恢复实施中，使用弹性灾难恢复来复制运行 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，使用弹性灾难恢复来复制运行 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）。数据库则使用数据库原生复制方法进行复制。

AWS 跨区域灾难恢复

在具有多个 AWS 区域的灾难恢复场景中，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

- 将源区和恢复区的 Amazon VPC 分开放在不同区域中
- 源区和恢复区共享 AWS 账户
- 使用 AWS Transit Gateway 或 Amazon VPC 对等连接来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，来保护区域之间的共享存储

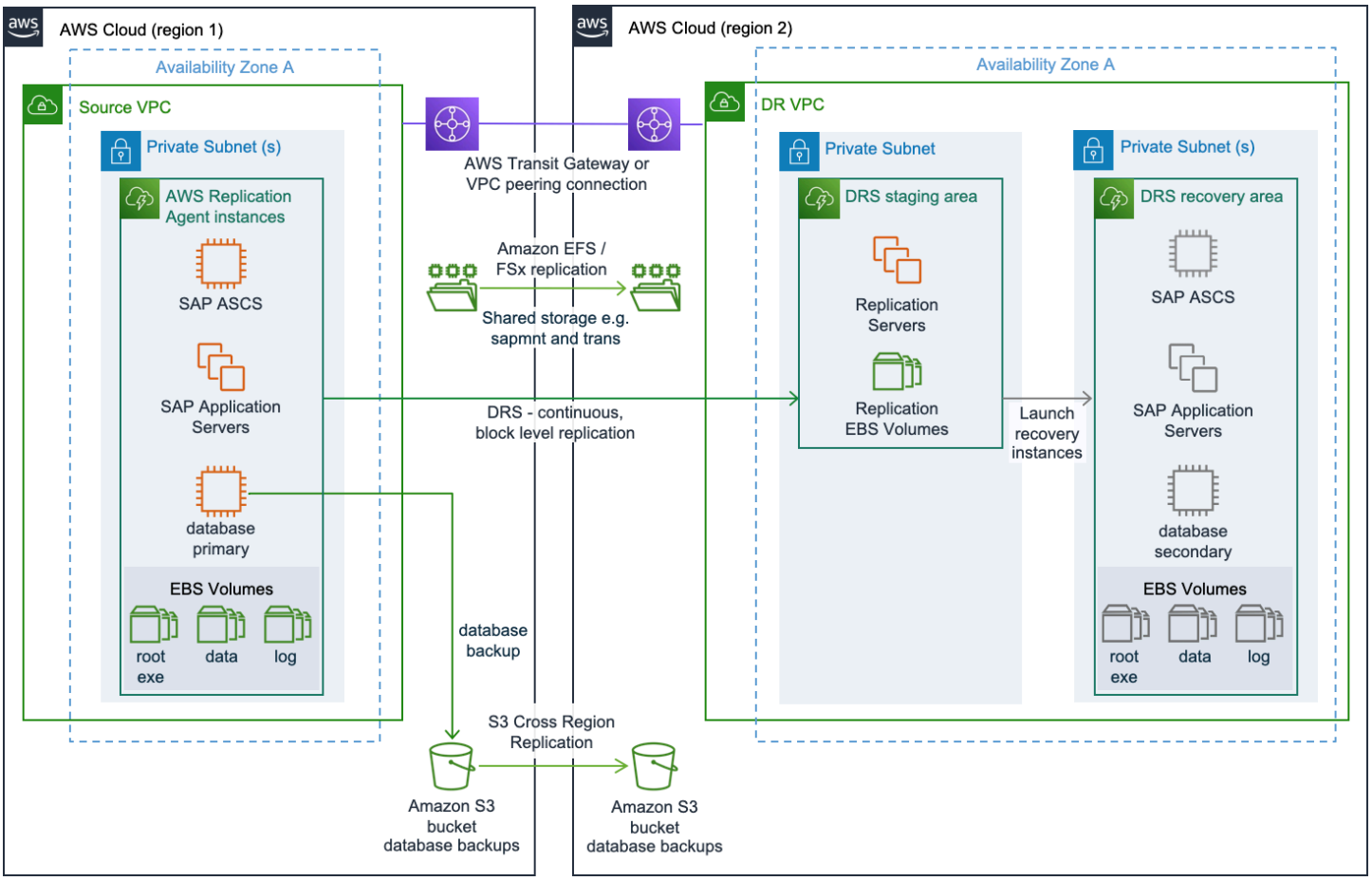
有关更多信息，请参阅 AWS 跨区域灾难恢复。

> **Note**
>
> 使用 Amazon EFS 时，您只能在同一个 AWS 账户中进行复制。

- Amazon S3 跨区域复制提供数据库备份以及其他 Amazon S3 存储桶数据的副本，用于 Amazon VPC 灾难恢复
- 为源区、暂存区和恢复区使用不同的子网

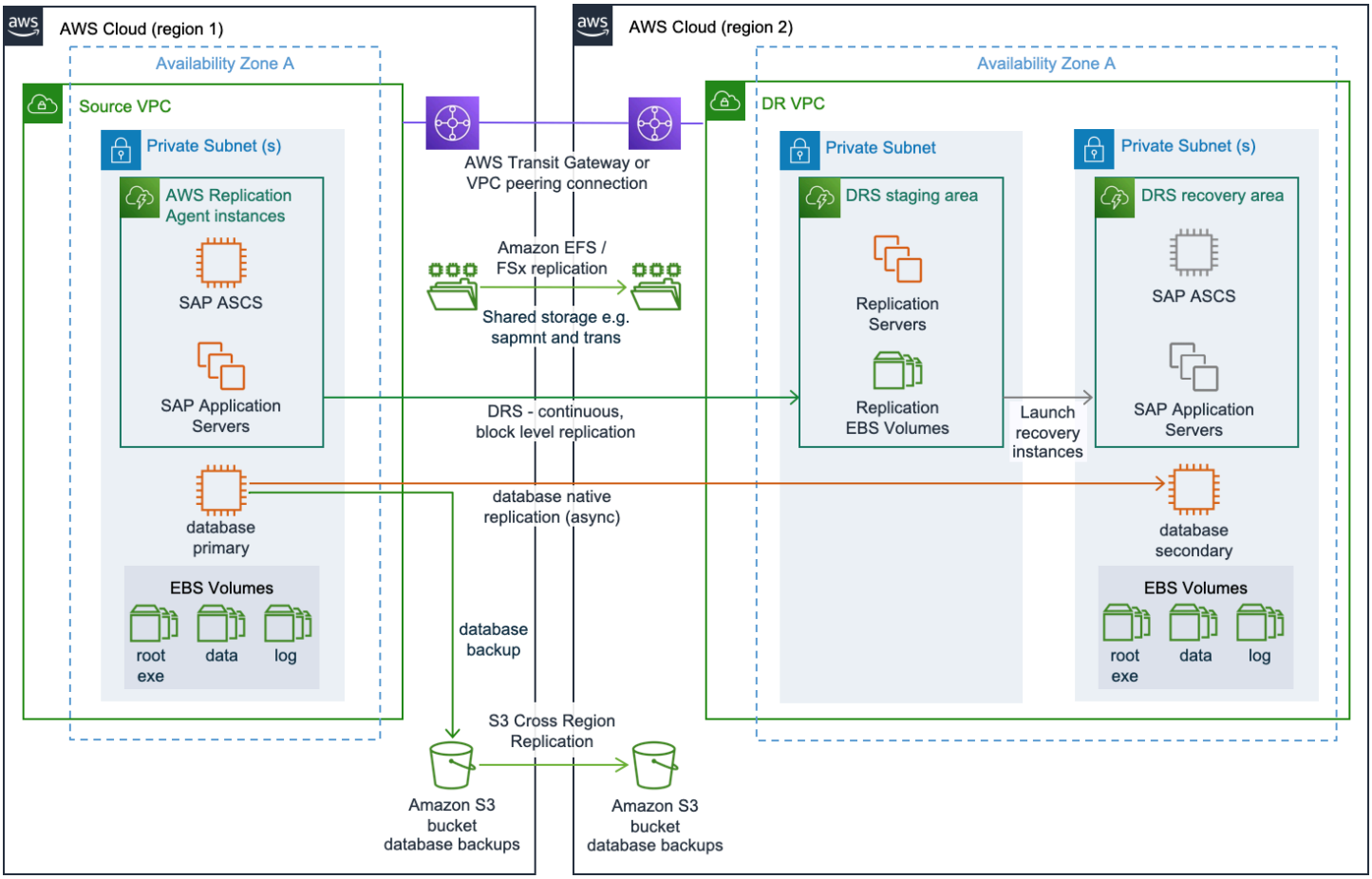
以下两个部分介绍此场景的参考架构。

完整跨区域灾难恢复实施



在完整跨区域灾难恢复实施中，使用弹性灾难恢复来复制运行 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，使用弹性灾难恢复来复制运行 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。数据库则使用数据库原生复制方法进行复制。

AWS 外部向 AWS 的灾难恢复

在此场景中，源系统运行在非 AWS 环境上。实施像这样的混合灾难恢复解决方案，可以为其他平台上的现有生产环境快速实现韧性。

最佳实践

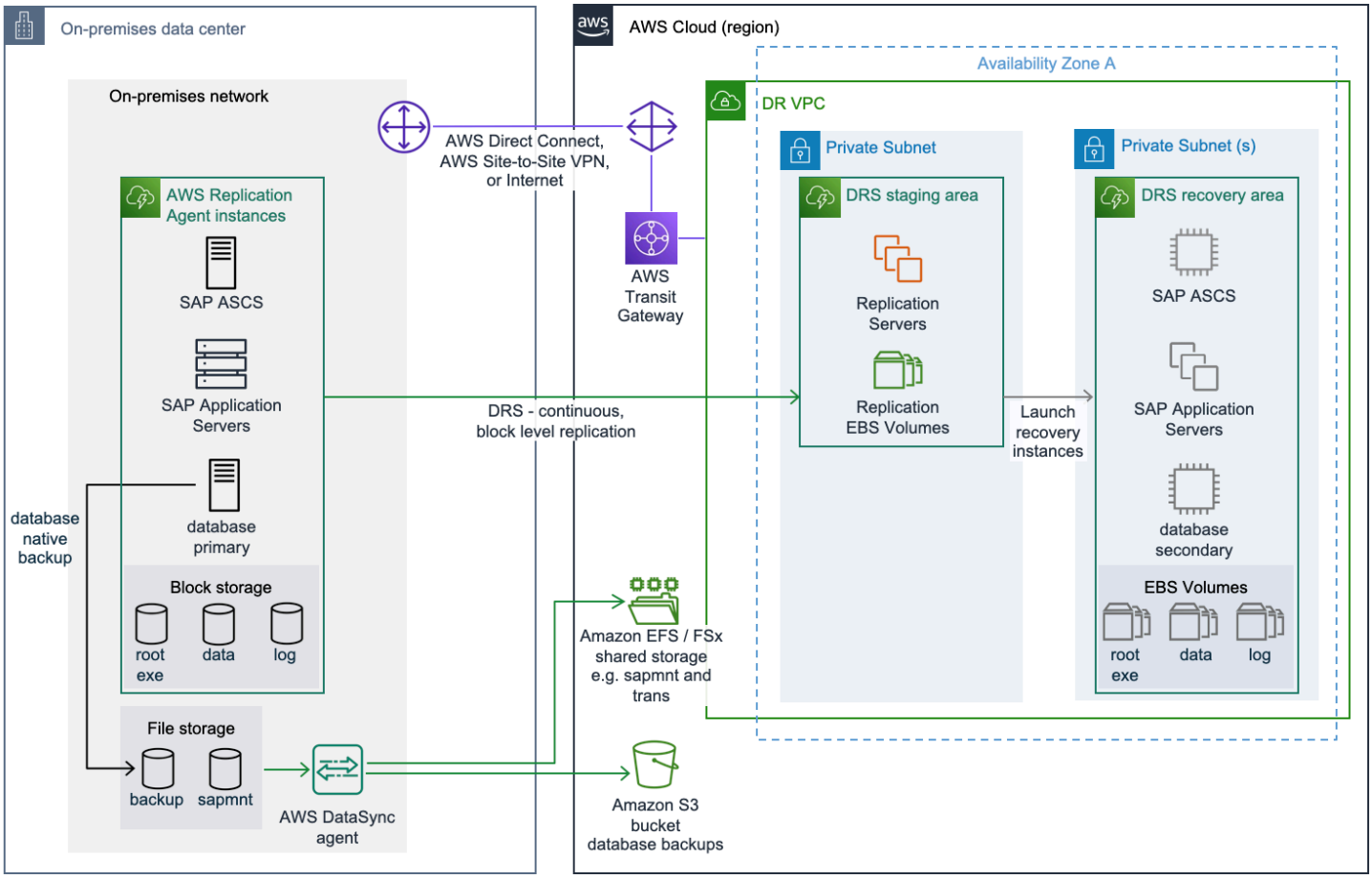
- 使用 AWS Direct Connect 来支持复制流量和最终用户连接

  有关更多信息，请参阅网络。
- 使用 AWS DataSync 保护共享存储

  有关更多信息，请参阅 AWS 外部向 AWS 的灾难恢复。
- 为暂存区和恢复区使用不同的子网

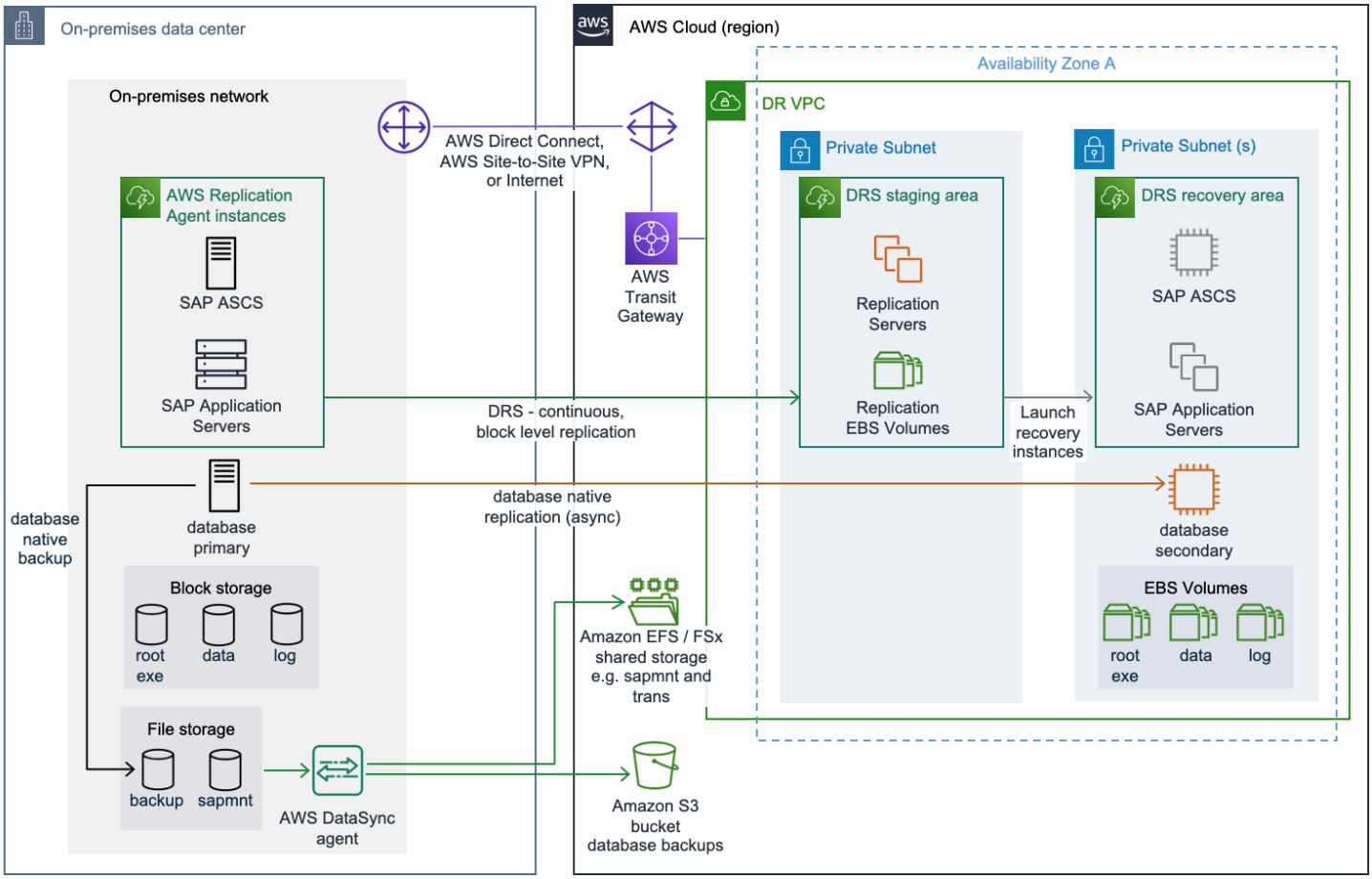
以下两个部分介绍此场景的参考架构。

完整非 AWS 向 AWS 的灾难恢复实施



在完整非 AWS 向 AWS 的灾难恢复实施中，使用弹性灾难恢复来复制运行 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 向 AWS 的灾难恢复实施



在混合非 AWS 向 AWS 的灾难恢复实施中，使用弹性灾难恢复来复制运行 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）。数据库则使用数据库原生复制方法进行复制。

有关更多灾难恢复选项和信息，请联系 AWS Support。

共享存储韧性

SAP 服务器上的文件系统可以在块类型存储上创建，例如本地连接的磁盘或 Enterprise Storage Area Network（SAN）设备，也可以基于共享文件系统，例如来自服务器或网络附属存储（NAS）设备的 SMB 或 NFS 共享卷。

由于弹性灾难恢复是一项块级复制服务，因此只有在将磁盘表示为块存储设备时，此服务才会复制磁盘。对于共享文件系统，必须使用其他工具和流程来提供韧性。为了满足这些要求，建议使用 AWS 的完全托管式共享存储服务，从而在云中轻松且经济高效地启动、运行和扩展功能丰富、高性能和高韧性的文件系统。文件系统的选择取决于灾难恢复场景的操作系统。

- Linux：Amazon Elastic File System（Amazon EFS）

- Microsoft Windows Server：适用于 Windows File Server 的 Amazon FSx（Amazon FSx）
- 混合：适用于 Windows File Server 的 Amazon FSx 或者适用于 NetApp ONTAP 的 Amazon FSx（FSx for ONTAP）

以下部分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
- AWS 外部向 AWS 的灾难恢复

AWS 区域内灾难恢复

当您使用托管服务（例如 Amazon EFS、适用于 ONTAP 的 FSx 或适用于 Windows File Server 的 FSx 等）来托管共享文件系统时，这些服务的多可用区设计提供的固有韧性意味着共享存储已经可以进行灾难恢复。为了进一步提高韧性，请确保定期备份您的共享存储，以防可能出现的数据损坏。

如果您使用 NFS 或 SMB 协议直接从 Amazon EC2 实例之一共享文件系统，当该文件系统位于 Amazon EBS 上并通过复制代理连接到服务器时，您不需要执行其他步骤。这样可以确保通过弹性灾难恢复进行复制。如果共享文件系统托管在另一个 Amazon EC2 实例上，其中还有不属于您的 SAP 工作负载的其他内容，请使用操作系统原生工具（例如 `rsync`）来管理此文件系统向恢复区的复制。

您也可以使用 AWS DataSync 来提供选择性复制。可以安排此服务至少每小时运行一次，将这些文件复制到目标存储的恢复区中。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 的工作原理。

AWS 跨区域灾难恢复

要支持跨区域灾难恢复，辅助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辅助区域的共享文件系统上。根据您选择的 AWS 服务，实施将有所不同。

- Amazon Elastic File System：Amazon EFS 原生复制可以支持单个 AWS 账户内的跨区域复制。
- 适用于 Windows File Server 的 Amazon FSx：您还可以使用 AWS DataSync，在主共享存储与辅助共享存储之间复制数据。有关更多信息，请参阅 AWS DataSync 的工作原理。
- 适用于 NetApp ONTAP 的 Amazon FSx：您可以使用 NetApp SnapMirror，在源实例和目标实例上的适用于 ONTAP 的 FSx 文件系统之间复制文件来维护共享文件系统的当前副本，频率最高为 5 分钟一次。有关更多信息，请参阅使用 NetApp SnapMirror 计划复制。

AWS 外部向 AWS 的灾难恢复

根据共享存储的源区设计，您必须考虑在 AWS 中的灾难恢复实例上复制这些文件。我们建议使用 AWS DataSync。此服务可以与多种服务来回复制数据，例如 NFS 和 SMB 共享，并与使用 Amazon EFS、适用于 Windows File Server 的 FSx 和适用于 ONTAP 的 FSx 的多种文件系统来回复制数据。

在某些情况下，您可以考虑使用其他选项来保护您的源区 SAP 共享文件系统，例如在源环境中使用以下选项时。

- 适用于 ONTAP 的 FSx：您可以使用 NetApp SnapMirror，在源实例和目标实例上的适用于 ONTAP 的 FSx 文件系统之间复制文件来维护共享文件系统的当前副本，频率最高为 5 分钟一次。有关更多信息，请参阅使用 NetApp SnapMirror 计划复制。
- 本地存储：如果可以在托管本地存储的源服务器上配置复制代理，弹性灾难恢复会将本地存储复制到 AWS 上的灾难恢复环境中。

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以下部分提供的指导介绍了在应用程序层和数据库层中使用弹性灾难恢复时，设计、实施和管理弹性灾难恢复方法上的不同。

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 Elastic 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 挂载、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，请参阅共享存储韧性。

要进行设置，请在应用程序服务器上安装弹性灾难恢复代理。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，此服务将与使用 TLS 1.3 加密的弹性灾难恢复 API 端点进行身份验证握手。此服务在暂存区子网中，为复制的

每个源卷生成大小相同的 Amazon EBS 卷用于数据同步。Amazon EBS 卷的类型可以在复制服务器设置中配置。复制将在生成暂存区子网资源并安装代理后开始。数据经过加密，从源服务器直接传输到复制服务器。此服务自动管理暂存区的子网资源，根据源服务器和磁盘的并行复制情况扩展或缩减这些资源。

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。此服务不支持复制多节点 SAP 数据库，例如 SAP HANA 横向扩展集群。

SAP 系统中的数据存储在数据库中。这些数据包括主数据、事务数据和 ABAP 构件。在评估将弹性灾难恢复用于灾难恢复解决方案时，您必须考虑业务的 RPO 和 RTO 要求。此服务不具备应用程序感知能力，而是在操作系统层运行，将连接的存储复制到目标暂存环境。根据 RTO 和 RPO 要求，您可以选择弹性灾难恢复或数据库原生的复制方法，例如适用于 SAP HANA 的 SAP HANA System Replication（HSR）。

以下是选择数据库复制方法时的重要注意事项。

主题

- 网络带宽
- RPO
- 更改率
- 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。根据来源的更改率，您可能需要更高的网络带宽来将复制保持在最新状态。像 SAP HSR 这样的数据库感知技术所需的网络带宽较少，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变化率的峰值。如果您的 RPO 非常小，建议您同时测试数据库原生复制方法以及弹性灾难恢复。

导致数据库的数据发生重大变化的操作，会在暂存区中造成数据复制延迟。这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更改过的数据块，由弹性灾难恢复进行复制。复制服务器需要更多时间才能从源系统接收如此大量的更改数据并写入。这会影响您的业务 RPO。

对于从备份中进行恢复之类的操作，建议在工作负载压力较低的时候进行。这样，较长的 RPO 值就不会影响您的工作负载。您可以跟踪仍在等待弹性灾难恢复服务进行复制的更改数据量。有关更多信息，请参阅恢复控制面板。

更改率

对于更改率较高的数据库，您可以通过具备足够性能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，您可以选择数据库原生复制方法来优化 RPO。

RTO

使用弹性灾难恢复，在触发灾难恢复事件时，就会预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之前，您必须先测试灾难恢复方案。

成本

由于弹性灾难恢复不使用温备用或热备用方法，因此相比许多其他灾难恢复选项，此方法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弹性灾难恢复定价。使用数据库原生复制方法，成本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，则需要使用数据库原生复制方法。

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，恢复实例上的存储卷会超过单个 Amazon EBS 卷的容量 and/or 性能限制。这可能发生在非AWSAWS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。有关详细信息，请参阅 Linux 上的 RAID 配置。这些卷集将跨越两个或更多 Amazon EBS 卷，直至达到满足所需卷大小和性能所需的总量。然后，存储卷数据被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，适合实施混合灾难恢复解决方案。大多数服务器由弹性灾难恢复管理，特定服务器（出于存储性能考虑）使用其他灾难恢复方法，例如原生数据库复制技术。存储架构重构是在初始灾难恢复环境实施期间，在设置备用复制服务器时完成。由于现在是在应用程序级别进行复制，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 SAP S/4HANA Cloud 私有版是 SAP 推出的一款云端 ERP 解决方案。除 ERP 外，此解决方案还集成了业务流程智能、业务平台与分析以及业务网络功能。SAP 负责面向 RISE 的整体服务水平协议、云运维和技术支持。您可以在 RISE with SAP 中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。

SAP 负责 RISE with SAP 中的云中安全性。有关更多信息，请参阅 AWS 云安全性 – 责任共担模式和 SAP and Hyperscalers: Clarifying Security in the Cloud。除了 SAP 提供的安全性外，您还可以为 SAP 场景实现额外的安全性。有关更多详细信息，请参阅安全性部分。

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 账户提供支持。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 RISE with SAP S/4HANA Cloud 私有版和 SAP S/4HANA Cloud 私有版（定制选项），并涵盖了以下主题。

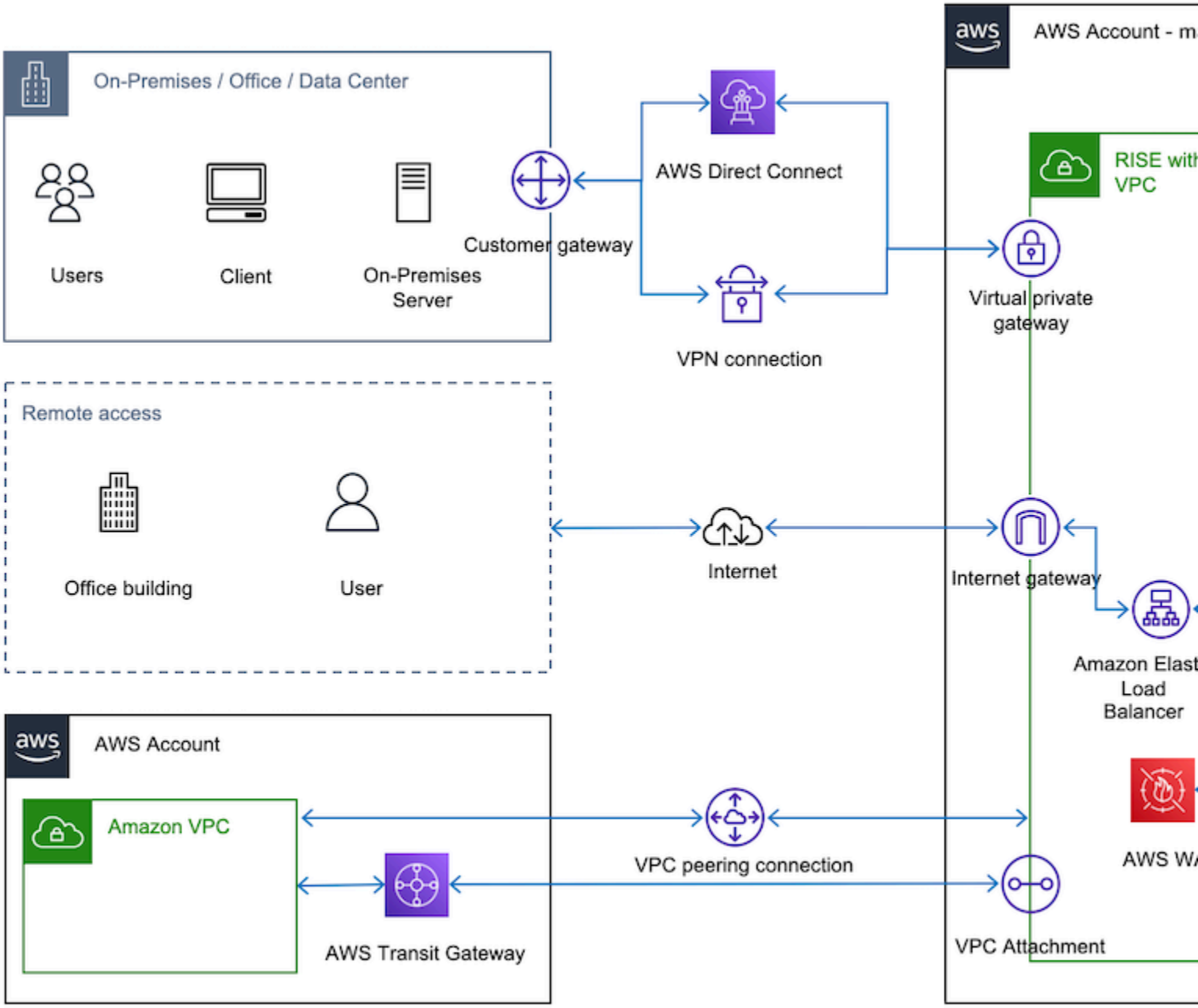
主题

- 连接
- 安全性

- 可靠性
- 可观测性
- 变更管理
- 数据集成与分析
- 代理式人工智能
- AWS 还有 SAP JRA
- 扩展程序

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。下图提供了与 RISE with SAP VPC 的连接示例概览。



有关更多详细信息，请参阅以下主题：

主题

- 建立连接的角色与责任
- 从本地网络连接到 RISE
- 从您的 AWS 账户连接到 RISE
- 连接到最近的 Direct Connect POP（包括本地区域）

- RISE 连接方案决策树
- 其他考虑因素

建立连接的角色与责任

在使用 RISE with SAP 时，SAP 企业云服务（ECS）团队负责管理 SAP S/4HANA 私有云环境。SAP 提供的《补充条款和条件》中包含“豁免任务”部分。此类任务由您负责执行。您也可以委托第三方服务提供商为您管理此类豁免任务。有关更多详细信息，请参阅 SAP Product Policies。

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 with SAP 协议，您负责建立与 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。有关更多信息，请查看后续部分。

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 AWS VPN 连接到 RISE
- 使用 Di AWS rect Connect 连接 RISE
- 使用 SD-WAN 连接到 RISE
- 连接的实施步骤

使用 AWS VPN 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。

每条 VPN 隧道的最大带宽可达 1.25 Gbps。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？

采用此方案时，SAP 需要以下详细信息：

- BGP ASN
- 您设备的 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 连接 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。

您可以选择 1 Gbps、10 Gbps、100 或 400 Gbps 的专用连接，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 托管连接的可用带宽为 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适用其他条款和条件。

有关更多信息，请参阅：AWS Direct Connect 定价。

使用 SD-WAN 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 主要运行于网络 OSI 模型的第 3 层（网络层），它提供了集中式控制、路由、路径选择、基于 IP 的策略，并且能够设定 SAP 等特定的关键业务应用的优先级，这使其非常适用于基于云的 RISE with 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 头端设备充当集线器或集中式网络组件，而部署在分支机构、远程站点或数据中心的 SD-WAN 边缘设备则作为 WAN 流量的入口和出口点。

有关更多详细信息，请参阅 Reference Architectures for Implementing SD-WAN Solutions on 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。

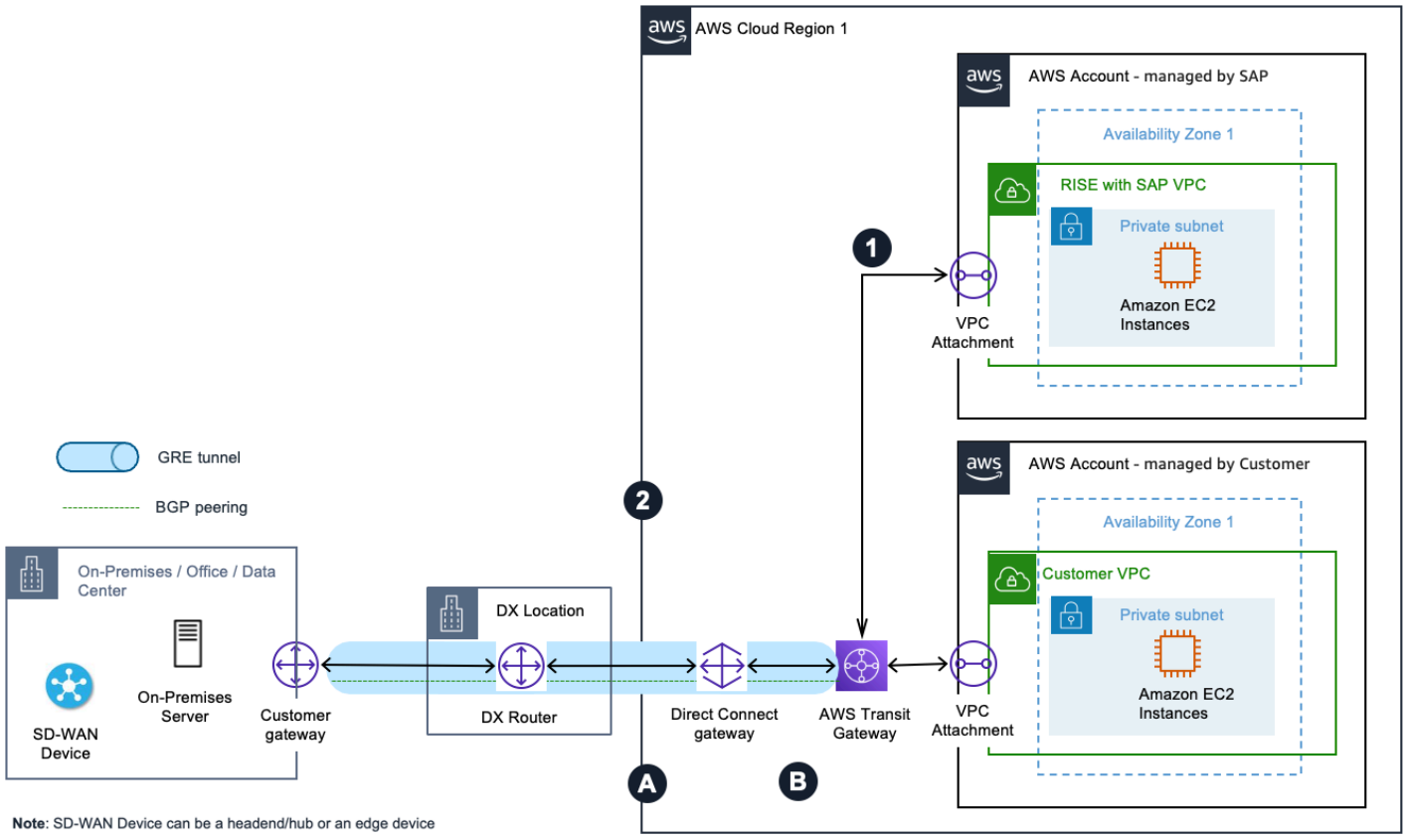
必须将该设备配置为使用 Connect 附件通过 GRE 隧道在中转网关之间发送和接收流量。必须将该设备配置为使用 BGP（边界网关协议）进行动态路由更新和运行状况检查。

每个连接均可配置独立的路由表和 BGP 对等，这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。

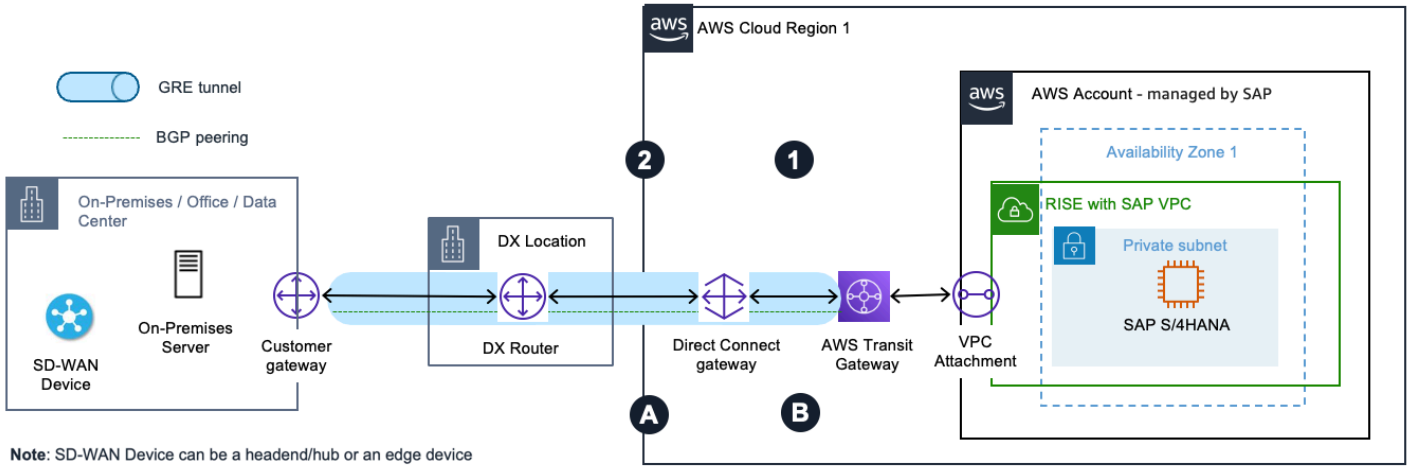
来自 RISE with SAP VPC 的出站流量：

1. 从 RISE VPC 流向企业数据中心的流量将被路由至 Transit Gateway。
2. Transit Gateway Connect 附件使用 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。

流至 RISE with SAP VPC 的入站流量：

A. 从企业数据中心 SD-WAN 设备流向 RISE VPC 的流量借助中转网关连接的 GRE 隧道，通过 Direct Connect 链路转发到 Transit Gateway。
B. Transit Gateway 将流量转发到目标 RISE with SAP VPC。

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，您可以请求 SAP 创建 Transit Gateway Connect 附件，并将 Direct Connect 连接用作底层传输载体。如果需要，客户可以利用由 SAP 管理的 Direct Connect 网关（DXGW）。

来自 RISE with SAP VPC 的出站流量：

1. 从 RISE VPC 流向企业数据中心的流量将被路由至 Transit Gateway。
2. Transit Gateway Connect 附件使用 Direct Connect 连接作为传输载体，并通过 GRE 隧道和 BGP 将 Transit Gateway 连接到企业数据中心 SD-WAN 设备。

流至 RISE with SAP VPC 的入站流量：

A. 从企业数据中心 SD-WAN 设备流向 RISE VPC 的流量借助中转网关连接的 GRE 隧道，通过 Direct Connect 链路转发到 Transit Gateway。

B. Transit Gateway 将流量转发到目标 RISE with SAP VPC。

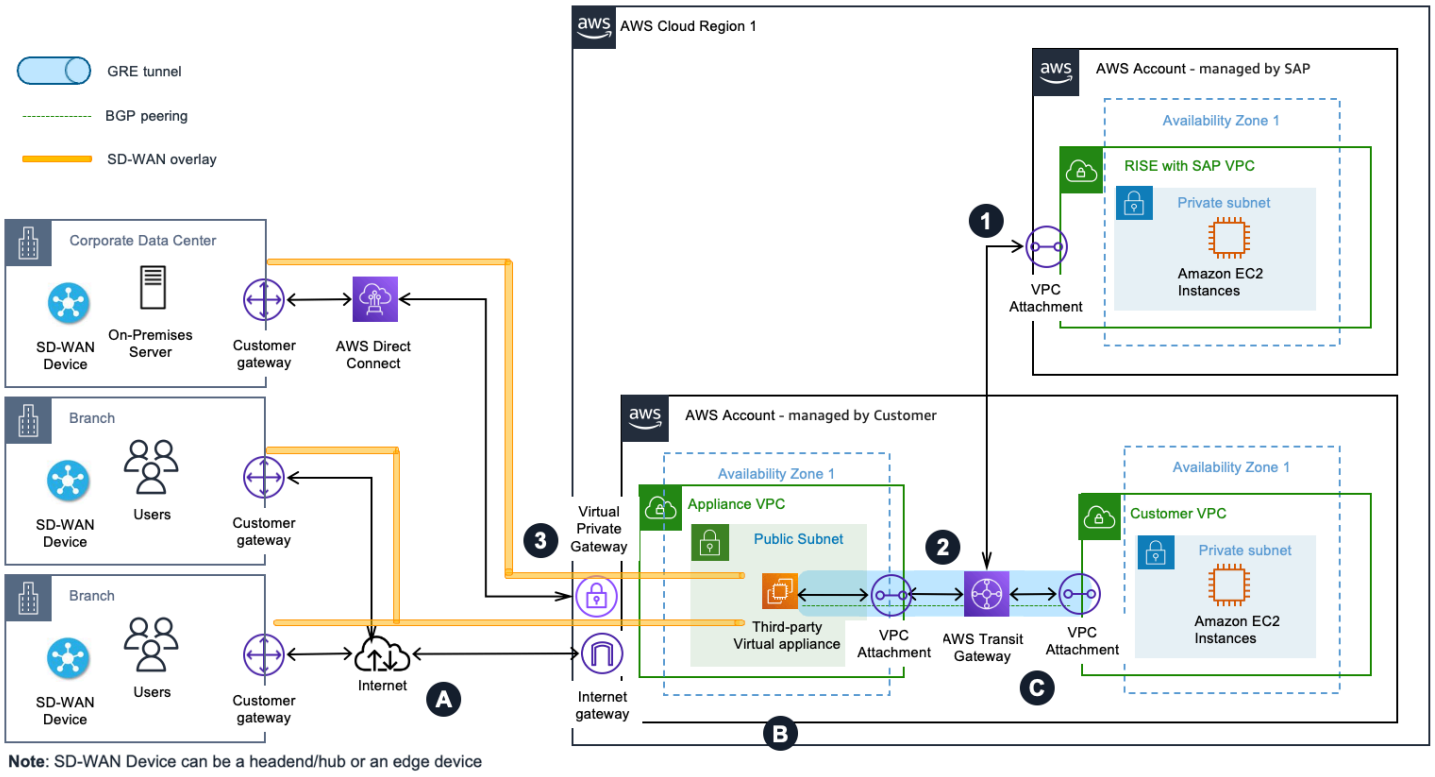
场景 B：中的 SD-WAN 设备（边缘 and/or 前端/集线器设备） AWS

在此场景中，SD-WAN 网络的虚拟设备部署在 AWS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 Connect 附件支持 GRE，与 VPN 连接相比，可提供更高的带宽性能。它支持 BGP 以实现动态路由，无需配置静态路由。此外，它与 Transit Gateway Network Manager 集成，可通过全局网络拓扑、附件级性能指标及遥测数据来实现高级可见性。

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：以下各部分中介绍的各种网络模式仅适用于 AWS上现有的或新的登录区设置。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



上图说明了一种模式，即借助连接附件将 SD-WAN 网络与 Transit Gateway 集成，并将 SD-WAN 网络的（第三方）虚拟设备置于 AWS的设备 VPC 中。通常会在分支机构和本地数据中心部署 SD-WAN 边缘设备，以构建全网状拓扑。

来自 RISE with SAP 的出站流量：

1. 从 RISE VPC 流向企业数据中心的流量将被路由至 Transit Gateway。
2. Transit Gateway Connect 连接使用 VPC 附件作为传输载体，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. 第三方虚拟设备会对流量进行封装处理，这些流量通过部署在 Direct Connect 链路上的 SD-WAN 重叠网络传输至企业数据中心。

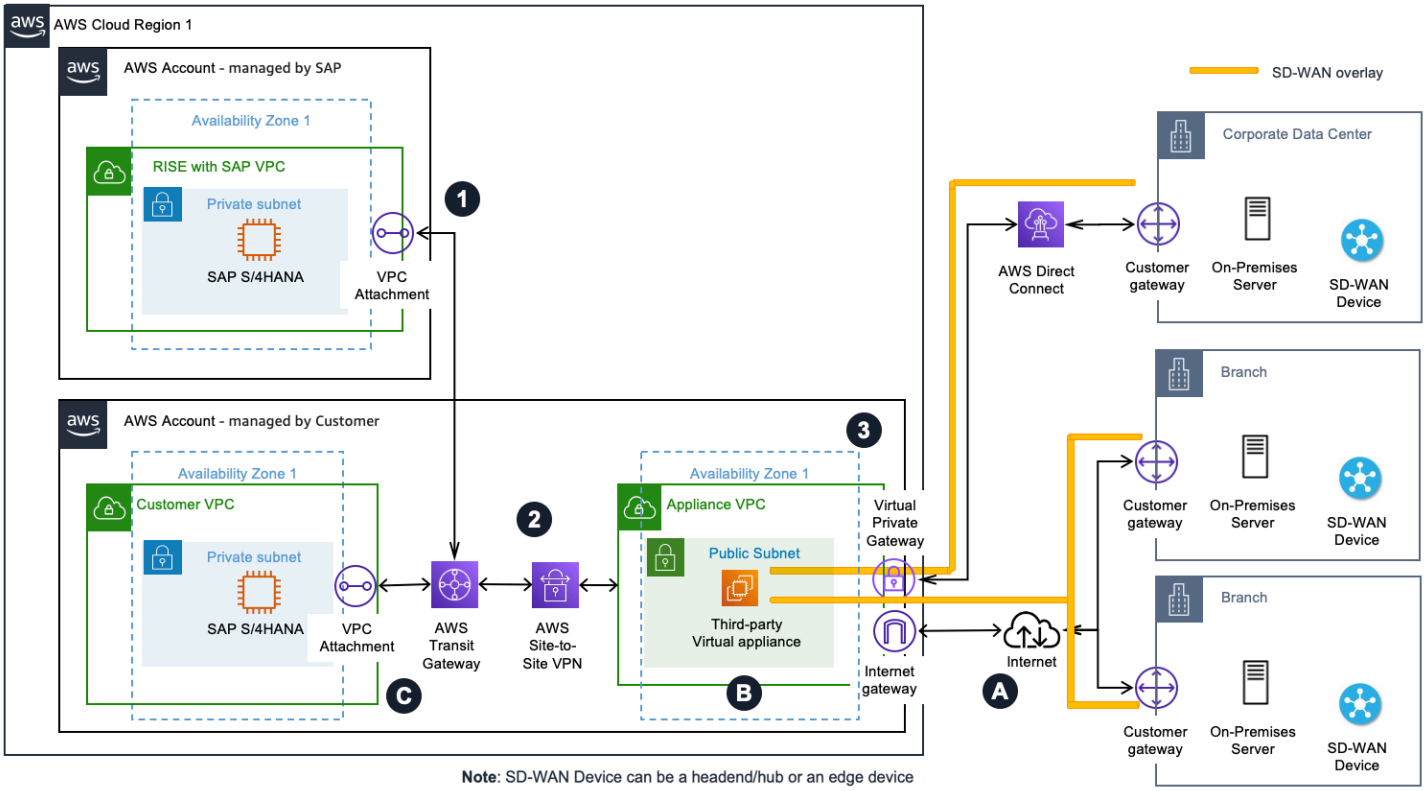
流至 RISE with SAP 的入站流量：

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，从企业数据中心流向 RISE VPC 的流量通过 Direct Connect 链路上的 SD-WAN 重叠网络到达设备 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



上图说明了一种使用 AWS 站点-站点 VPN 连接将您的 SD-WAN 网络与 Transit Gateway 集成，并将软件定义广域网网络的（第三方）虚拟设备置于其中的设备 VPC 中的模式。 AWS当您的第三方虚拟设备不支持 GRE 时，可以使用此方案。通常会在分支机构和本地数据中心部署 SD-WAN 边缘设备，以构建全网状拓扑。

来自 RISE with SAP 的出站流量：

1. 从 RISE VPC 流向企业数据中心的流量将被路由至 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. 第三方虚拟设备会对流量进行封装处理，这些流量通过部署在 Direct Connect 链路上的 SD-WAN 重叠网络传输至企业数据中心。

流至 RISE with SAP 的入站流量：

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。

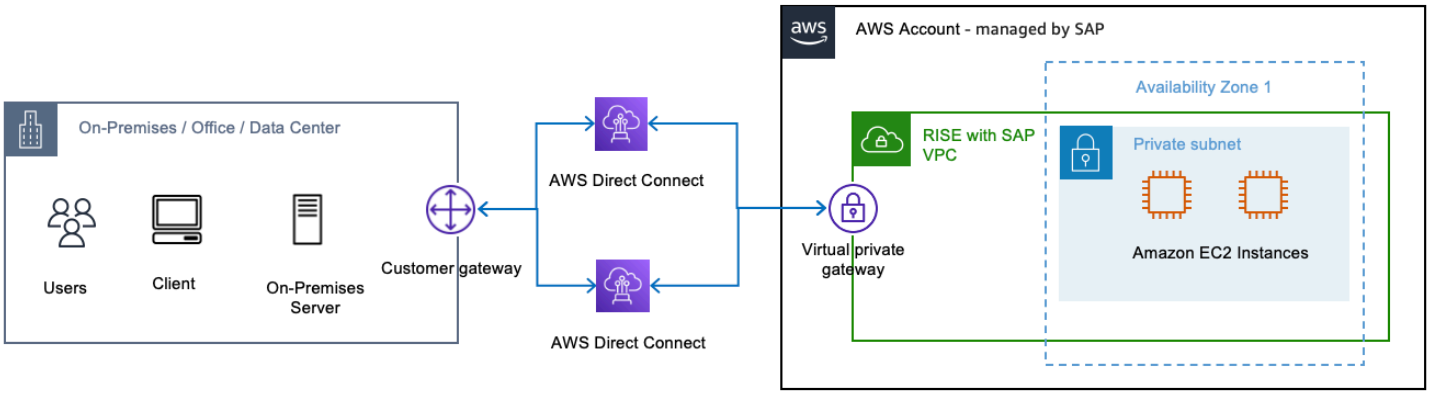
C. Transit Gateway 将流量转发到目标 RISE VPC 的 TGW ENI。

连接的实施步骤

本节更深入地探讨了RISE与SAP和您的本地环境之间的连接的实施步骤（不使用任何客户托管 AWS 帐户）。我们将详细介绍以下两种方案：第一种方案，为关键工作负载创建高弹性部署；第二种方案，为非关键工作负载创建经济高效的替代方案。

对于每种方案，我们将明确说明 SAP 所需的详细信息以及您需要在本地环境中执行的步骤。

方案 1：面向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 是在客户的私有网络与AWS之间建立的物理以太网连接，供单个客户专用。托管 DX 是由 AWS Direct Connect 合作伙伴代表客户预调配的物理以太网连接。参阅 AWS Direct Connect 自行熟悉该服务。

要为 RISE with SAP 部署设置弹性 Direct Connect 解决方案，请按照以下实施步骤操作：

先决条件

配置 Direct Connect 连接前，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。
- 验证您的网络是否能支持多个 BGP 连接以实现冗余。

启动设置过程

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预调配 Direct Connect 连接所需的必要信息。

我们建议您为计划建立的每个 Direct Connect 连接分别填写调查问卷来设置冗余连接，从而实现高可用性。查看 Direct Connect 弹性建议以了解最佳实践。

填写 SAP 调查问卷

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，提供以下有关您的 Direct Connect 连接的详细信息：

- 该连接是新连接还是专用 Direct Connect 连接
- 您将使用的 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
- 主要 Direct Connect 链路和次要 Direct Connect 链路的子网 CIDR 数据块（采用 /30 CIDR 格式）
- VLAN ID
- 本地路由器的自治系统编号（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。

将填写完的调查问卷提交给您的 SAP ECS 代表。然后，SAP 将使用这些信息在 AWS上的 RISE with SAP 环境中预调配必要的 Direct Connect 资源。

SAP 的责任

在您提交填写完的调查问卷后，SAP 将处理以下任务（以下列表为示例性说明，且仅适用于此场景）：

- 创建虚拟接口（取决于您的 DX 类型：托管还是专用）

- 创建 Direct Connect 网关
- 如果您需要 SAP 在 RISE VPC 中预调配 Transit Gateway，请执行以下操作：
  - 设置 Transit Gateway（包括您提供的 ASN）
  - 为 VPC 创建中转网关连接
  - 更新路由表以允许 Transit Gateway 与 RISE with SAP 网络 VPC 进行通信
  - 将 Transit Gateway 与 Direct Connect 网关关联，包括将告知您的网络的 RISE with SAP 网络的 CIDR

完成设置过程

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，同时为两个 Direct Connect 连接启用 BGP 会话。验证 BGP 路径，并通过模拟其中一个连接故障来测试失效转移场景，确保流量能正常失效转移至另一个连接。

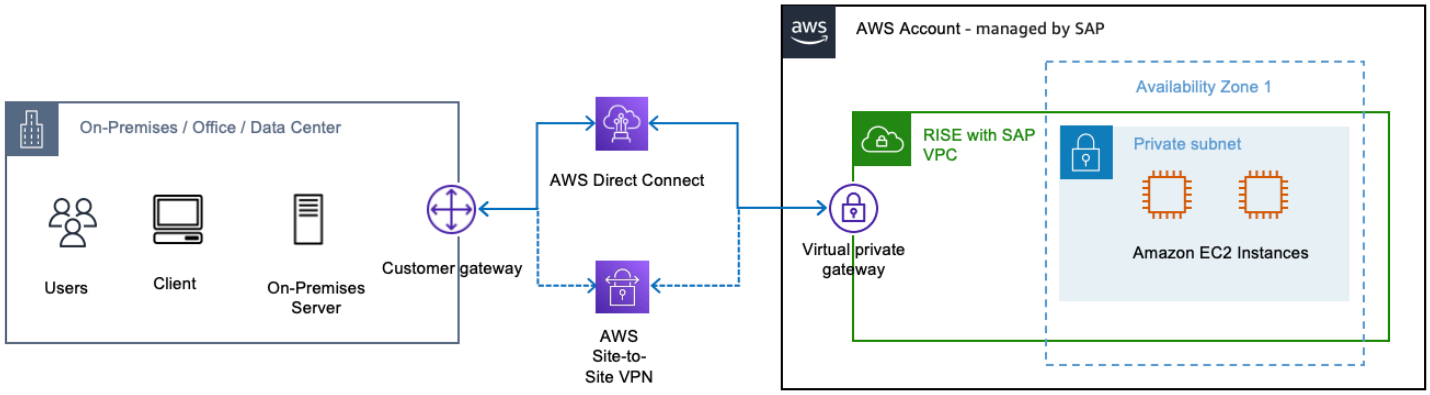
确认两条路径都与 SAP 的 end-to-end连接。您还可以利用 AWS Direct Connect Resiliency Toolkit 执行计划的失效转移测试以验证连接的弹性。

维护连接

定期检查并根据需要更新 Direct Connect 配置。与 SAP 协同实施所有变更。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。

方案 2：非关键工作负载的经济高效的替代方案



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，他们可能还需要一种灵活可变的连接，该连接可在全球各地的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. 在配置中通过两条安全隧道将 VGW 和 CGW 绑定在一起的 S2S VPN 连接 IPSec active/passive

有关建立 AWS Site-to-Site VPN 连接的深入文档，请参阅 AWS 文档中的 AWS Site-to-Site VPN 入门。

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：

- 查看有关 Site-to-Site VPN 的 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。虽然此过程与设置 Direct Connect 的过程类似，但存在几项主要差异。

启动设置过程

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，您打算将 VPN 作为 Direct Connect 链路的失效转移方案实施。

填写 SAP 调查问卷

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（用于 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：仅在使用主动-主动模式时）
- 客户本地网络 IP 范围

将填好的问卷提交给 SAP。随后，他们将创建 VPN 连接并为您提供配置详细信息。

SAP 的责任

在您提交填写完的调查问卷后，SAP 将处理以下任务（以下列表为示例性说明，且仅适用于此场景）：

- 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 并使用 SAP Transit Gateway 和你的客户网关将其连接到 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 会将必要的路由添加到 Transit Gateway 路由表并更新安全组

使用从 SAP 处收到的信息，在本地路由器上配置 VPN 隧道。实施路由策略，优先将 Direct Connect 连接而不是 VPN 作为主要路径。

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 故障来测试失效转移场景，确保流量能正常失效转移至 VPN。

与 SAP 确认，Direct Connect 和 VPN 路径的失效转移都按预期运行。

维护连接

定期检查并更新 Direct Connect 和 VPN 连接的配置。与 SAP 协同实施所有变更。

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
- AWS 云广域网
- 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

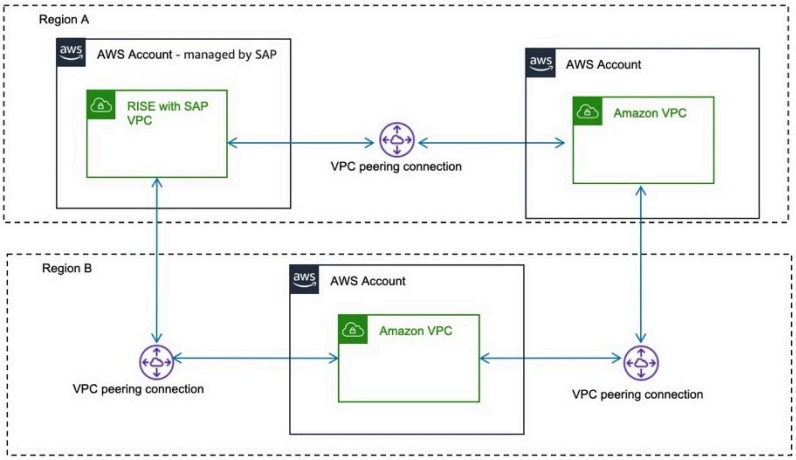
Amazon VPC 对等连接

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，您需要创建请求以供 SAP 审批。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。与 SAP 确认可在 RISE with SAP VPC 中使用的 CIDR 范围。

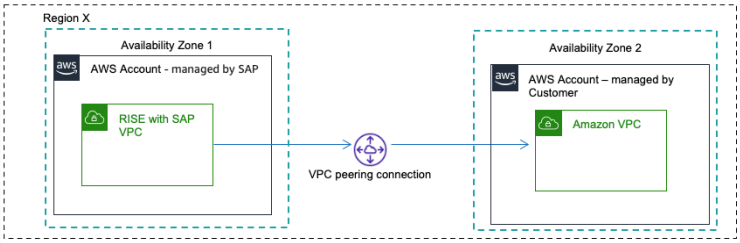
VPC 对等互 one-on-one连是相互之间的连接 VPCs，不是可传递的。流量无法通过中间 VPC 从一个 VPC 传输到另一个 VPC。您必须设置多个对等连接才能在 RISE 与 SAP VPC 和多个 VPCs对等连接之间建立直接通信。

VPC 对等互连跨 AWS 区域运行。所有区域间流量均经过加密，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。



同一可用区内的 VPC 对等连接的数据传输是免费的，跨可用区的数据传输按每 GB“传入数据”和“传出数据”收费。跨区域的 VPC 对等连接的数据传输按每 GB“传出数据”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 索要该可用区 ID。有关更多信息，请参阅您的 IDs AWS 资源的可用区。

定价示例 - 跨可用区的 VPC 对等连接



从 AWS 账户发送的 100GB 数据（由 SAP 通过 VPC Peering 与 AWS 账户对等互连进行管理）由客户管理： AZs

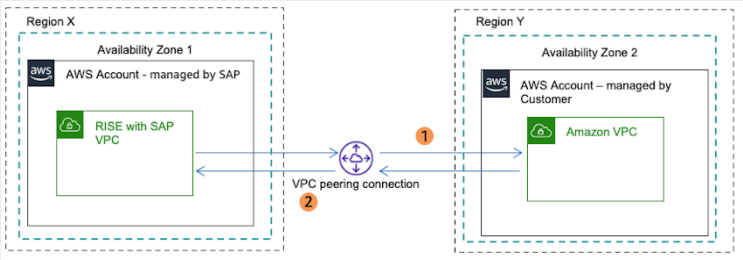
100GB * 每 GB 0.01 美元 = 1 美元（出账——计入 AWS 账户 — 由 SAP 管理）和 100GB * 每GB 0.01美元 = 1 美元（输入——账单到账户 — 由客户管理） AWS

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 - 跨区域的 VPC 对等连接

[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

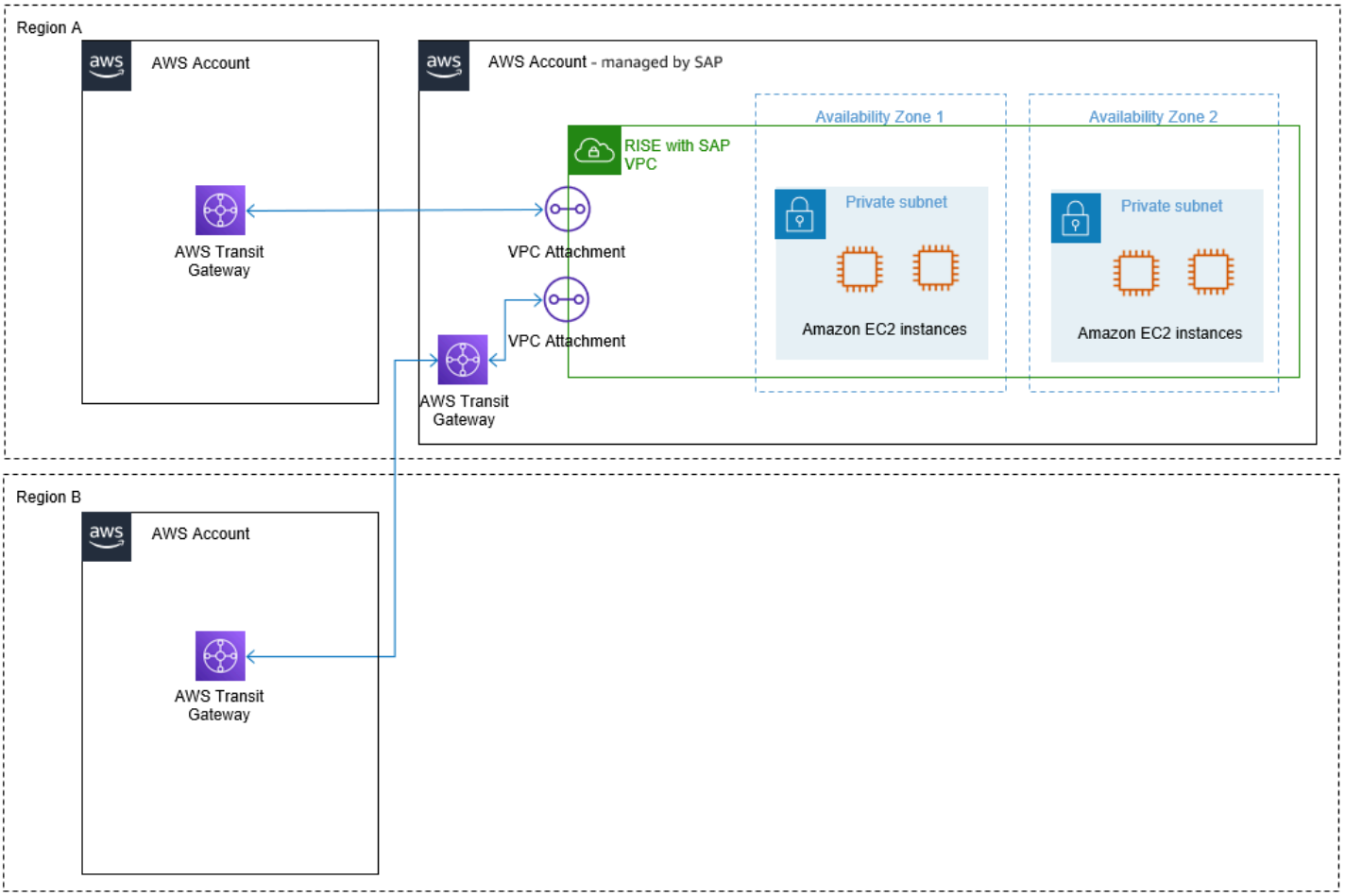
由于数据传输的成本是针对 “数据输出” 计算的，因此本示例将由客户管理的 AWS 账户承担费用。

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，通过作为中央通信中心来解决复杂的对等连接设置问题。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。随后，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，请参阅中转网关对等连接附件。



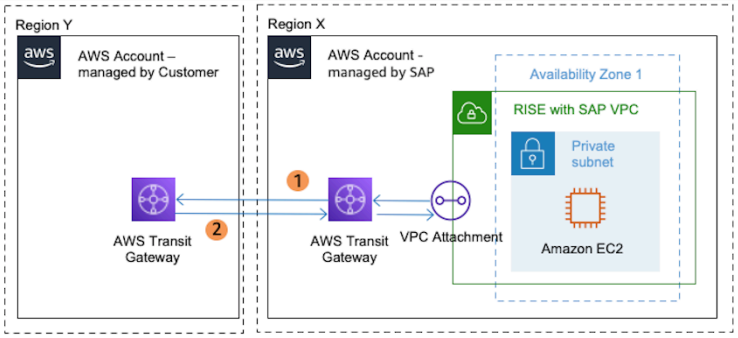
SAP 管理的 AWS 账户中的 Transit Gateway

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。您可以通过 Transit Gateway 对等连接实现 Transit Gateway 和由 SAP 管理的 Transit Gateway 之间的通信。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 拥有者需按小时支付与其他 Transit Gateway 的对等连接附件费用，因此，SAP 账户中由 SAP 管理的 Transit Gateway 的对等连接附件（用于区域间 Transit Gateway 对等连接）的每小时费用已包含在 RISE 订阅中。但是，客户账户中由客户管理的 Transit Gateway 对等连接附件的每小时费用由客户支付。有关更多信息，请参阅：Transit 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

数据处理费用由将流量发送到 Transit Gateway 的 VPC 所有者支付。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 端点送达其他 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

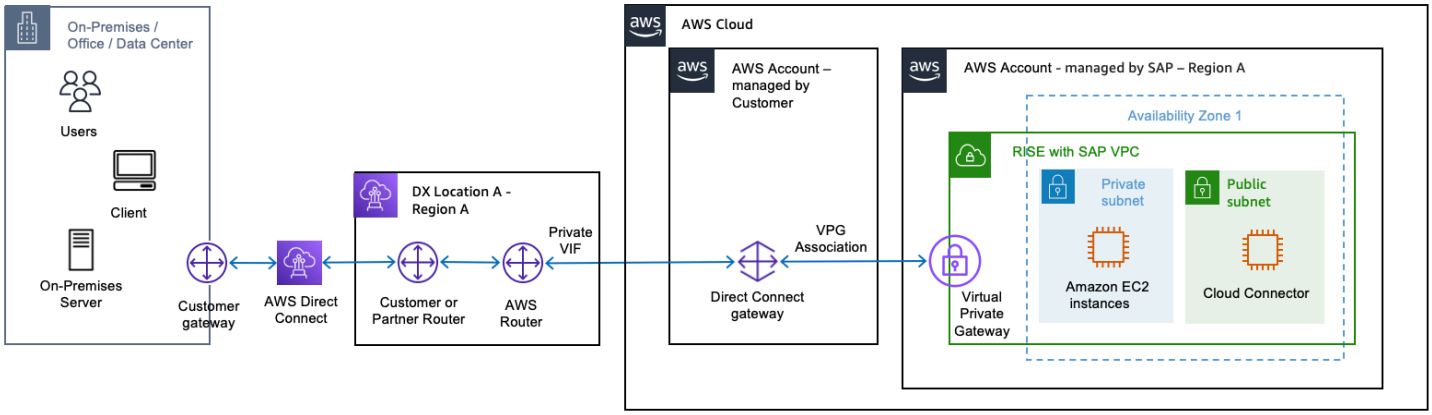
数据处理费用由将流量发送到 Transit Gateway 的 VPC 所有者支付。由于发送方的 VPC 位于 AWS 账户中（由客户管理），因此本示例的所有数据传输费用均由客户管理的 AWS 账户计费。此外，由客户管理的 AWS 账户将按每小时 Transit Gateway 对等连接的费用进行计费。

AWS 直连 Connect 网关

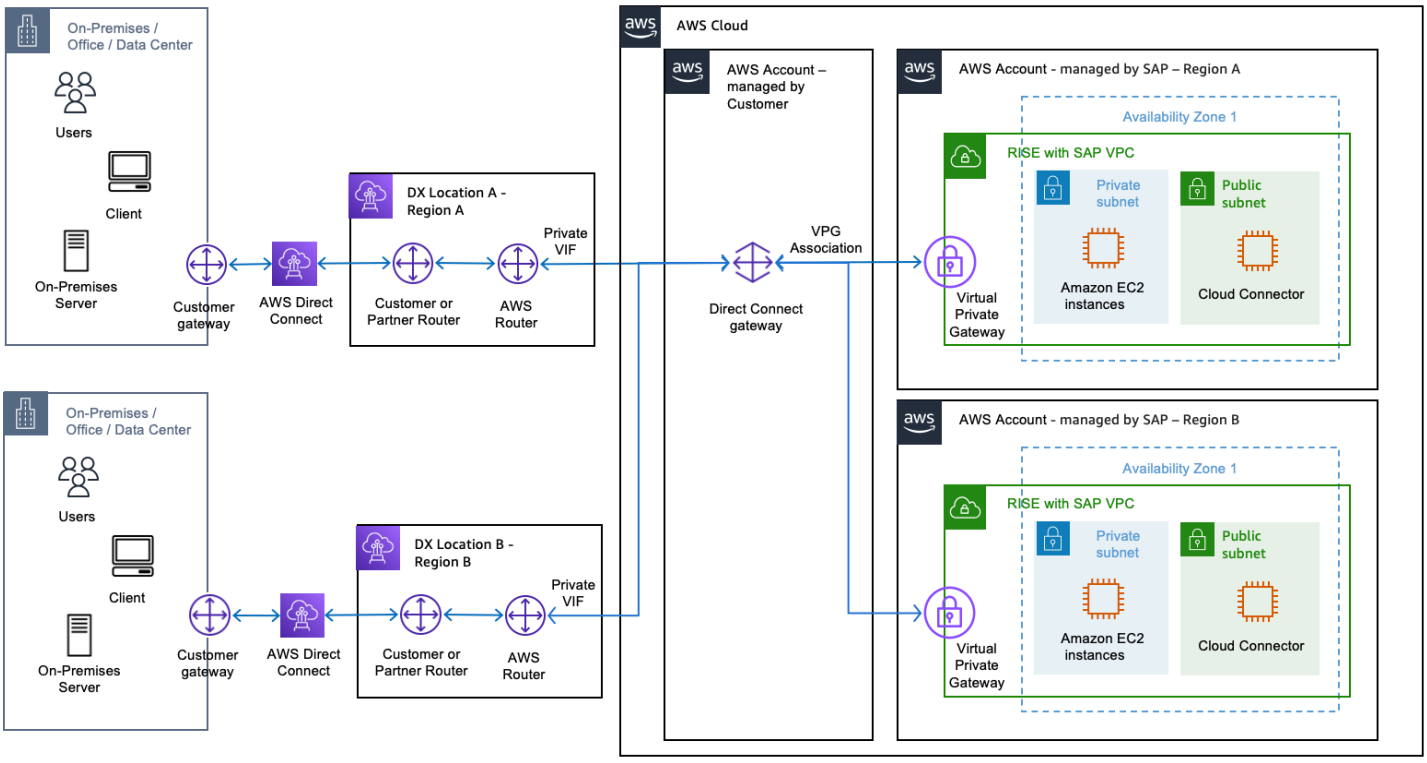
AWS Di@@ rect Connect 网关是一项全球服务，可让您在本地网络与不同 AWS 地区的多个 Amazon VPCs 之间建立私有连接。此集中式连接中心可让您整合网络架构、降低复杂度，并维持安全且高带宽的连接，同时避免在业务关键型工作负载中使用公共互联网。

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。

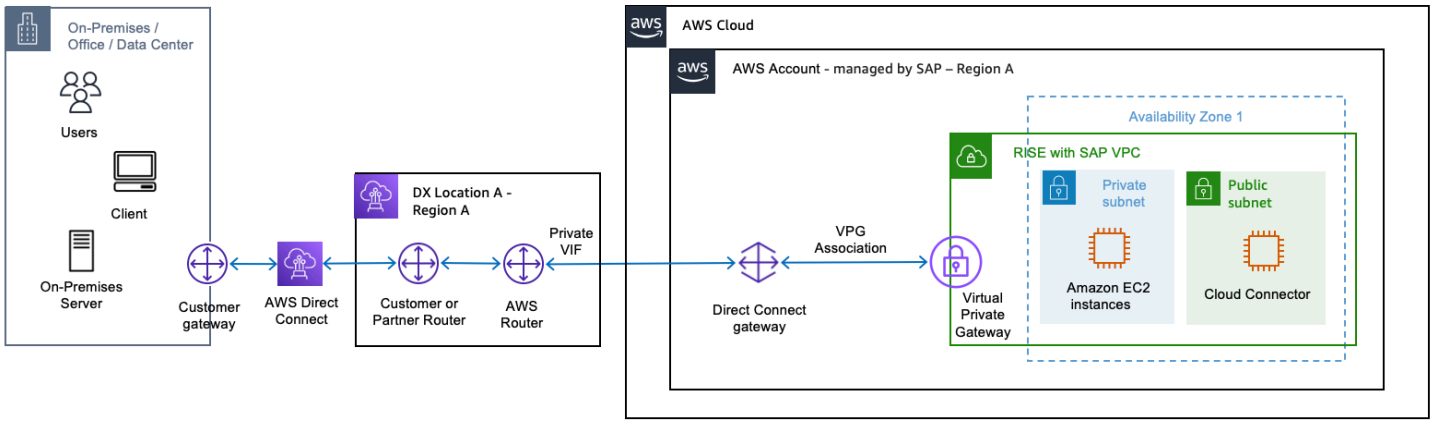


当您需要从多个本地站点 and/or 进行连接时，使用多个 AWS 区域进行 RISE 和 SAP（即远程灾难恢复），则可以使用 Direct Connect Gateway 来简化连接



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 网关本身不收取任何额外费用。你可以从 Di AWS rect Connect 中了解更多信息 FAQs。

AWS 云广域网

AWS Cloud WAN 是一项托管广域网 (WAN) 服务，旨在简化构建、管理和监控连接云和本地资源的统一全球网络的流程。它使组织能够使用集中控制面板和策略驱动的自动化，将数据中心、分支机构、远程站点和亚马逊虚拟私有云 (VPCs) 集中连接 AWS 全球主干网。有关更多信息，请参阅 AWS 云 WAN 文档。

在您的 AWS 账户中使用 AWS 云广域网从本地连接到 RISE

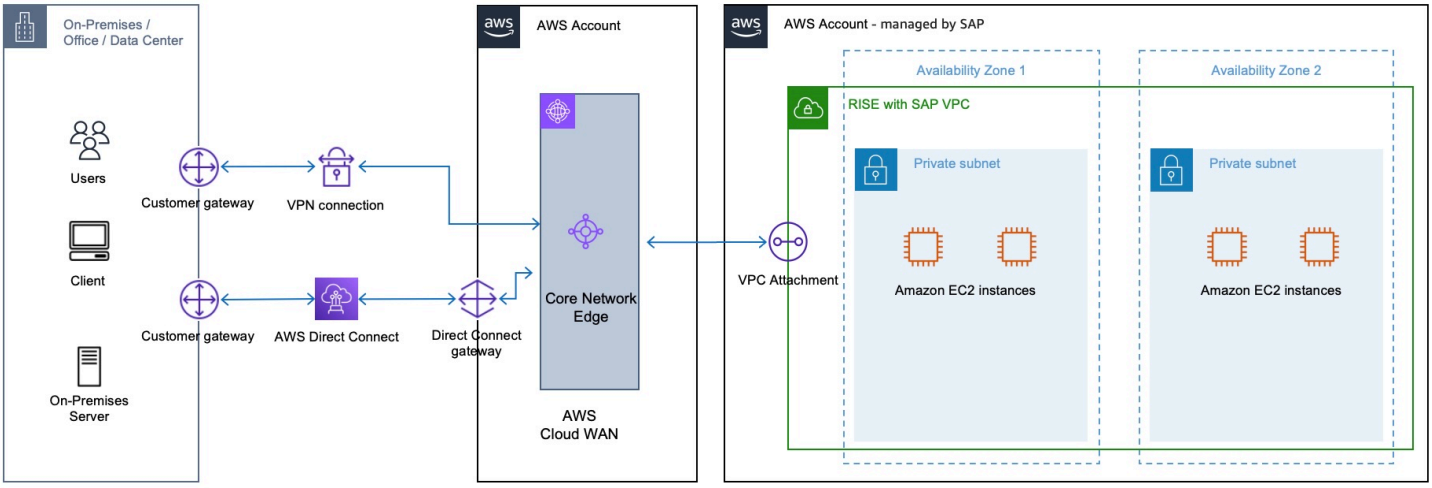
要与 RISE Environment（由 SAP 管理的AWS 账户）建立连接，请通过 AWS 账户中的 AWS 资源访问管理器 (RAM) 创建和共享 AWS Cloud WAN。随后，SAP 将接受共享的 Cloud WAN 并创建 VPC 附件，使流量能够流经路由表中的条目。由于 AWS Cloud WAN 位于您的 AWS 账户中，因此您可以保留对流量路由的控制权。

以下是创建全球云广域网的高级 step-by-step指南：

1. 在 AWS 网络管理器中，创建全局网络和相关的核心网络。
2. 创建核心网络策略 (CNP)，用于定义分段、自治系统编号 (ASN) 范围、 AWS 区域和用于附加到分段的标签。
3. 应用该网络策略。
4. 通过资源访问管理器与管理 RISE with SAP 账户的 SAP ECS 共享核心网络。
5. 创建附件并为其添加标签。
6. 更新连接中的路由 VPCs ，使其包含核心网络。

有关更多详细信息，请参与以下文档：

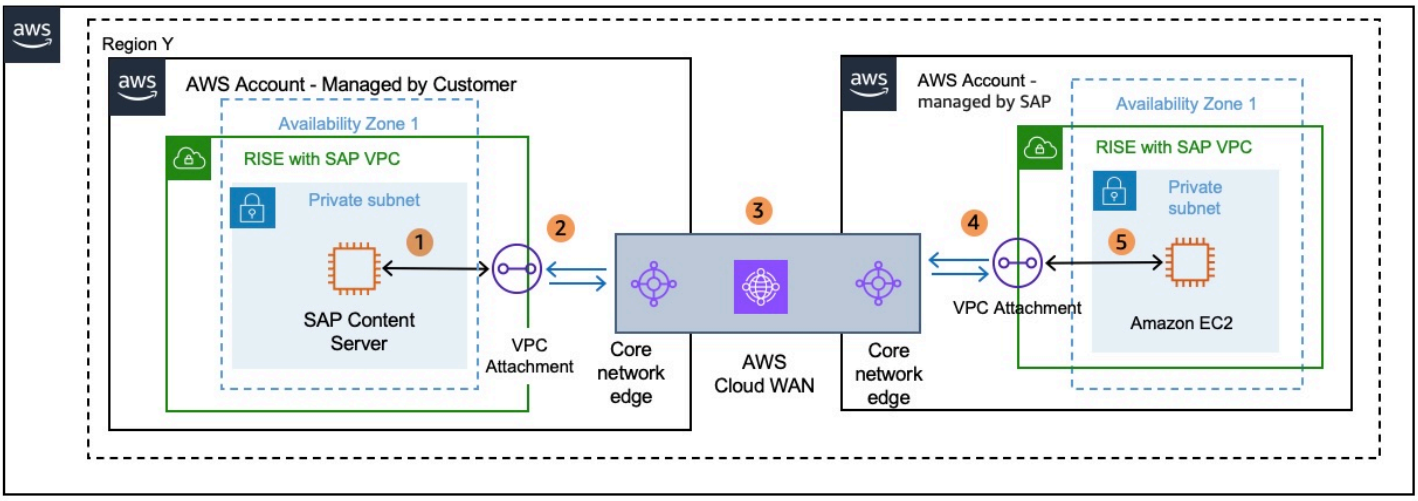
- 快速入门：创建 AWS 云广域网全球网络和核心网络
- 在 C AWS loud WAN 策略版本中配置核心网络设置
- 构建可扩展且安全的多 VPC AWS 网络基础设施 — Cloud WAN



1. 将 AWS Site-to-Site VPN (S2S VPN) 连接到 AWS 云广域网-创建 Site-to-Site VPN 连接，目标网关类型设置为 “未关联”。您可以通过亚马逊 VPC 控制台在 VPN 连接下为 AWS 云广域网创建 AWS S2S Site-to-Site VPN 附件。创建 AWS S2S VPN 后，您可以将其连接到 AWS Cloud WAN 核心网络。有关更多信息，请参阅如何为 AWS 云广域网创建 Site-to-Site VPN 连接。
2. 使用 AWS Cloud WAN 连接 AWS Direct Connect 网关 — 创建带有传输虚拟接口的 Direct Connect 网关，并将云广域网连接到您 AWS 账户中存在的 Direct Connect 网关。有关更多信息，请参阅将 AWS 云 WAN 连接到 Direct Connect 网关。有关为 Direct Connect Gateway 创建中转虚拟接口的详细步骤，您可以参考 AWS 文档-创建到 Di AWS rect Connect 网关的传输虚拟接口。

您可以从定价文档中估算部署 AWS Cloud WAN 的成本。以下是供您参考的定价示例。

场景 A. AWS Cloud WAN 连接同一个区域 VPCs 中的两个



定价示例 — AWS Cloud WAN 连接相同区域 VPCs 的两个区域

[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]。

账户中从 X 区域的 VPC 发送的 100GB 数据（由 SAP 通过位于 AWS 账户中的云广域网管理）由客户管理的 VPC 终止的客户管理。 AWS

100GB * 每 GB 0.02 美元 = 2 美元（云广域网数据处理）（按 AWS 账户计费 — 由 SAP 管理）

除了数据处理外，还会有 AWS 账户上的 VPC 连接成本 — 由 SAP 管理。云 WAN 定价会因将 SAP VPC 连接到云 WAN 的区域而异。

例如，如果 SAP VPC 在美国东部（弗吉尼亚州北部）区域，美国东部（弗吉尼亚州北部）区域的 VPC 附件费用为每小时 0.065 美元。

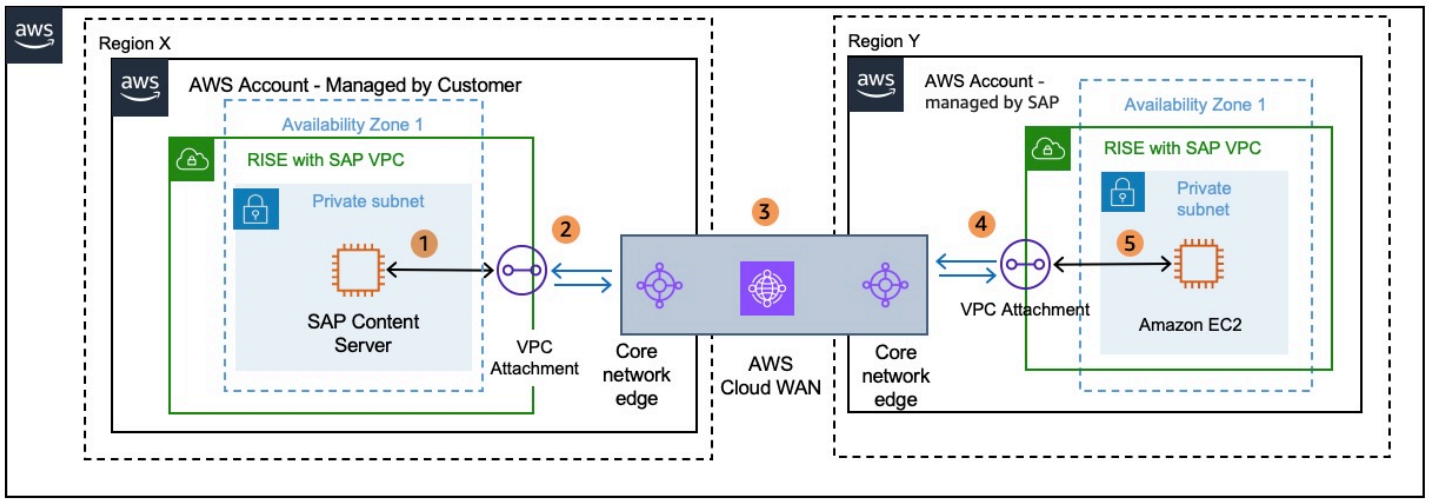
0.065 美元 * 730 = 47.45 美元（每月固定费用计入账户，由 SAP 管理） AWS

因此，总费用 = 49.45 美元

数据处理和 VPC 连接费用由向 AWS 云广域网发送流量的 VPC 所有者收取。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和连接费用。

由客户管理的 AWS 账户仅按每小时 VPC 连接的 Cloud WAN 费用计费。从可用区传出的数据将始终通过该可用区的云 WAN 端点送达其他 VPC，因此不会产生跨可用区数据传输费用。

场景 B. AWS Cloud WAN 连接不同区域 VPCs 的两个



定价示例 — AWS Cloud WAN 连接不同区域 VPCs 的两个

[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]。

从 Y 区域的 VPC 向 AWS 账户发送的 100GB 数据（由客户通过 AWS 云广域网管理到 AWS 账户）由不同区域 X 的 SAP 管理。

100GB * 每 GB 0.02 美元 = 2 美元（云广域网数据处理）+ 100GB *（每 GB 0.01 美元至 0.138 美元）= 1 美元至 13.8 美元（区域外）= 3 至 15.8 美元（总计-计入账户 — 由客户管理） AWS

数据处理费用由将流量发送到云 WAN 的 VPC 拥有者支付。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 账户将按区域 Y 中每小时 VPC 连接的价格计费。X 区域的 VPC 连接费用将由 AWS 账户收取，由 SAP 管理，费用包含在 RISE 订阅中。

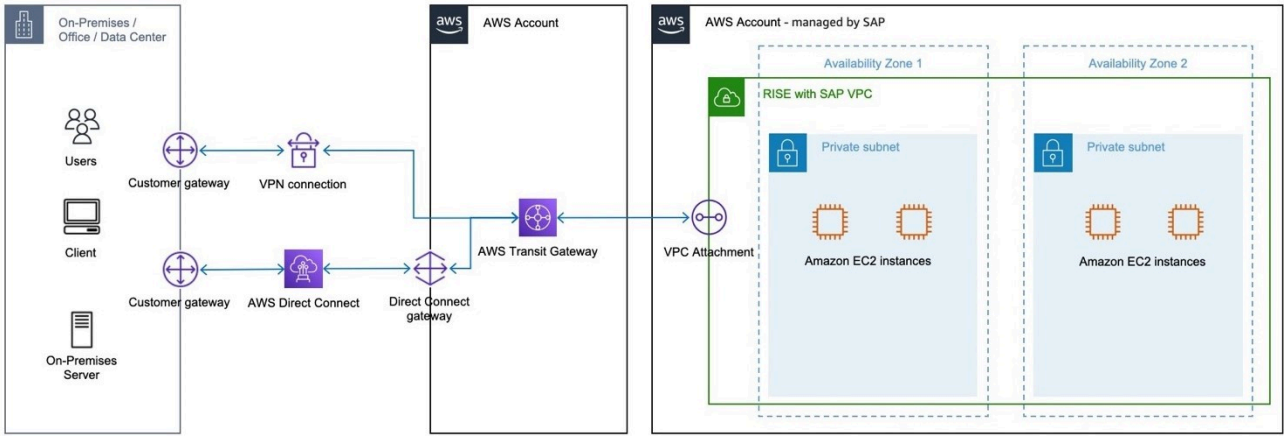
使用您的单一 AWS 账户连接到 RISE

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。您可采用以下任一方案。

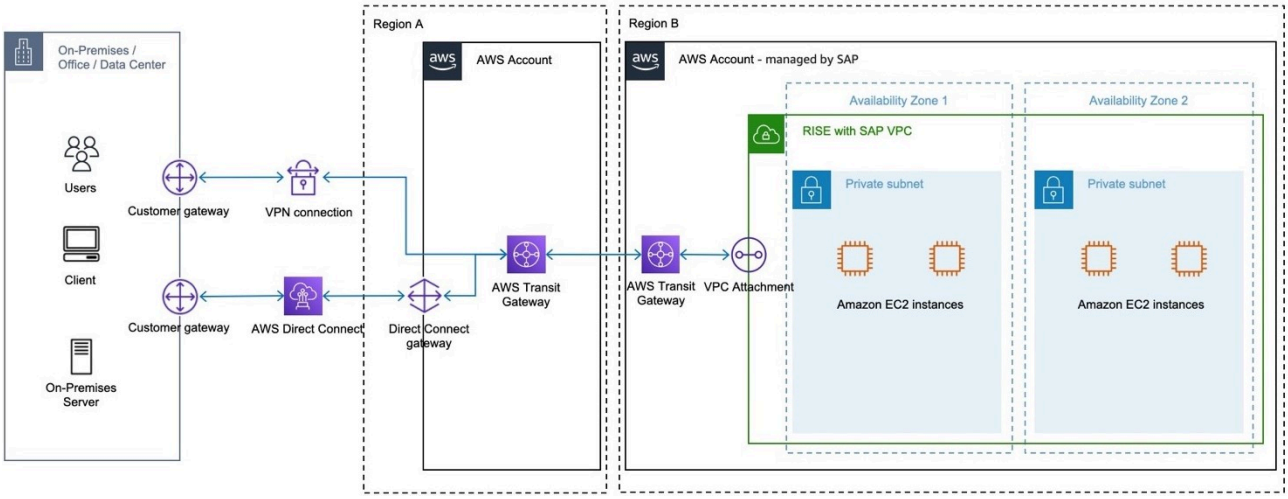
- AWS Transit Gateway — 与 AWS SAP 管理的账户共享您 AWS 账户中的 T AWS ransit Gateway 资源。
- AWS 使用 T AWS ransit Gateway 的 IPsec VPN — 通过互联网在远程网络和传输网关之间创建 VPN 连接。有关更多信息，请参阅 AWS Site-to-Site VPN 的工作原理和传输网关 VPN 附件。
- Direct Connect 网关 - 创建带中转虚拟接口的 Direct Connect 网关。有关更多信息，请参阅 Direct Connect 网关的中转网关连接。

  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 地区的此选项。



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），由客户管理，因此 AWS 直接连接端口的工时费用和公交网关连接的费用将记入 AWS 账户，由客户管理。 AWS

对于对等连接附件，每位 Transit Gateway 所有者均需按小时支付与另一 Transit Gateway 的对等连接附件费用。

数据处理费：

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。

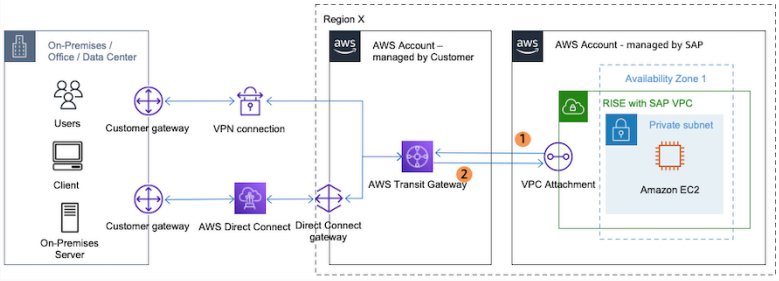
根据来源和目的地，数据处理费用各不相同，将计入由客户管理的 AWS 账户，或者已经包含在RISE订阅中（有关成本估算示例：见下文）

有关更多信息，请参阅：

- AWS Site-to-Site VPN 定价
- AWS 直接连接定价
- Transit Gateway 定价

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

或者

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

数据处理费用由将流量发送到 Transit Gateway 的 VPC 所有者支付。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

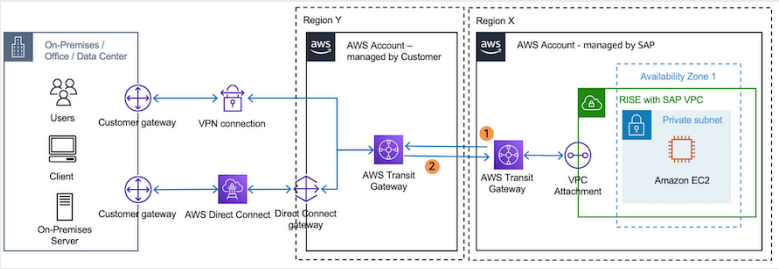
或者

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

或者

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

数据处理费用由将流量发送到 Transit Gateway 的 VPC 所有者支付。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

或者

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 账户计费。

使用共享 AWS 着陆区连接到 RISE

现代 SAP 环境具有多项连接需求。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 登录区可为 RISE with SAP 连接建立安全、可扩展且架构完善的基础。它具有以下优势：

- 通过标准化架构简化了 SAP 网络集成
- 通过冗余连接方案增强了业务连续性
- 通过分层网络控制加强了安全态势
- 集中化管理网络资源与策略
- 能够在更广泛的 AWS 解决方案中重复使用 AWS Direct Connect 连接
- 优化了网络性能，并减少了延迟
- 通过 AWS 原生服务增强治理

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。

登录区的关键组件及优势包括：

- 多账户结构 – 通过 AWS Organizations 构建组织良好的层次结构，单独配置用于生产、开发和共享服务的账户，确保明确分离关注点并强化安全边界。
- 网络架构 ——它建立了一个集中式的 T AWS ransit Gateway 作为网络中心，采用标准化 VPC 配置，将 RISE 和 SAP 账户与其他 AWS 账户连接起来。它还支持与 AWS Direct Connect 和 AWS Site-to-Site VPN 集成，在保持网络分段和安全控制的同时，将您的本地与 RISE 连接起来，同时保持网络分段和安全控制。

- S@@ ecurity Fram ework-它通过集中式日志记录和监控实现全面 AWS 的安全服务集成，包括网络防火墙的实施以及身份和访问管理控制。
- 自动化与管理 - 通过 AWS Control Tower 或 AWS CDK 与登录区加速器（LZA）实施基础设施即代码部署，以便在整个环境中实施自动化账户预调配、标准化配置以及一致的策略执行。
- 日志和监控-它AWS 配置包括 Config、AWS CloudTrail、Amazon 在内的 AWS 服务， GuardDuty 用于集中记录、监控和审核资源变更和安全事件。
- 安全控制-它通过配置规则、 CloudTrail 跟踪和 Sec AWS urity Hub 标准实施安全最佳实践，同时启用网络防火墙功能。
- 自定义选项-它允许根据特定的组织要求进行自定义，包括与现有基础架构的集成以及通过着陆区加速器配置添加 AWS 服务。

我们建议使用带有 SAP 连接的 RISE AWS 着陆区。

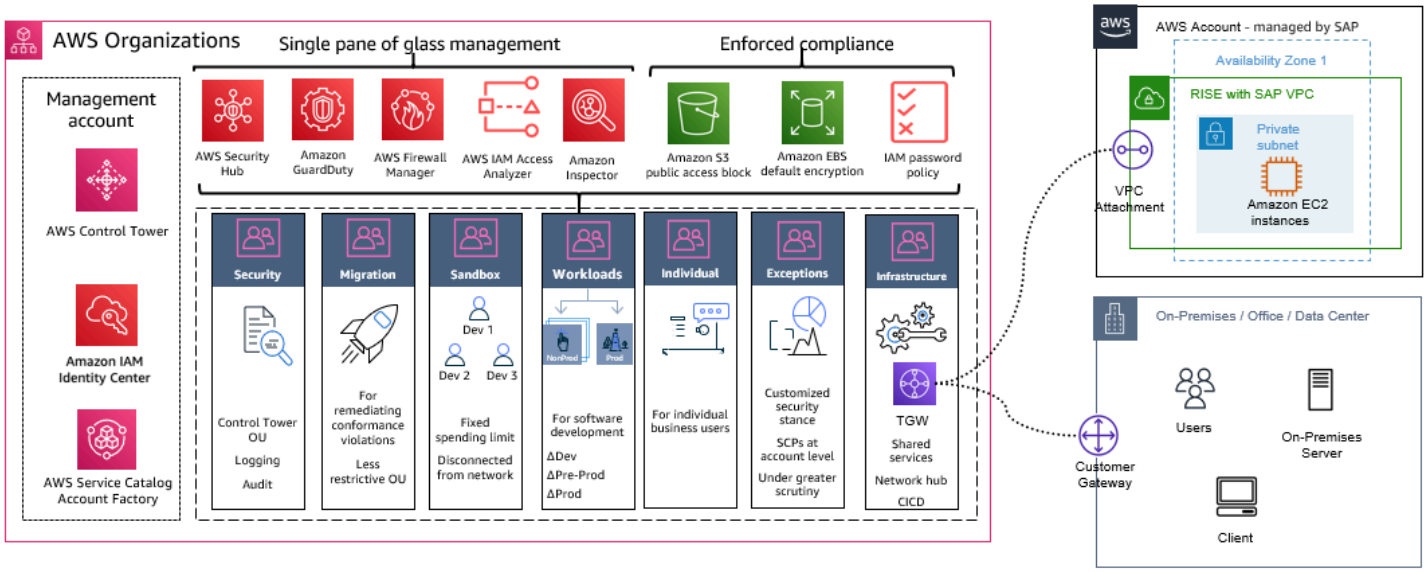
选择您的实施方式

AWS 提供了两种解决方案，用于通过SAP连接实现RISE的着陆区，每种解决方案都旨在满足不同的组织需求。

AWS Cont@@ rol Tower 通过其基于控制台的界面提供了简化的解决方案，通过标准化控件实现了快速部署。此方式适用于寻求快速实施且需要内置治理与合规控制能力的企业，尤其适合刚开始云之旅或需要简单 SAP 连接的企业。

着陆区加速器 (LZA) 通过基础设施即代码扩展了 AWS 控制塔的功能，提供了广泛的自定义和自动化。该解决方案适用于具有复杂的 SAP 联网需求、实施多区域部署或制定了大规模扩展计划的企业。拥有既定 DevOps 实践的组织将受益于 LZA 的配置驱动方法。

这两种解决方案可为 RISE with SAP 连接建立安全且可扩展的基础。选择 Control Tower 可进行快速部署和可视化管理，选择 LZA 可增强自定义与自动化能力。



建造着 AWS 陆区

您可以使用 Cont AWS rol Tower 和 Landing Zone Accelerator 实现 AWS 着陆区，后者为构建安全、可扩展的多账户环境（包括管理和治理服务）提供了自动流程。

有关详细的实施步骤或 LZA， AWS 提供了在 SAP 开启的情况下为 RISE 构建企业就绪型网络基础的指南。 AWS该指南包含经过验证的架构模式、安全配置以及专为 RISE with SAP 部署设计的操作程序。在一个简单的场景中，着陆区的占地面积最小，侧重于网络连接，而网络连接通常以Tr AWS ansit Gateway为中心。有关更多信息，请参阅 AWS 登录区。

下面是该流程的总体概述：

1. 明确需求 – 了解企业的安全、合规及运维要求。这将帮助确定登录区应包含的适当护栏、控制措施和服务。查看 SAP 企业云服务 (ECS) 团队提供的 AWS 连接问卷。
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）。对于 LZA 实施，需规划配置文件结构和自定义需求。
3. 设置 C AWS on trol 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。对于 LZA 实施，这将作为额外自定义设置的基础。
4. 部署着陆区加速器（可选）-如果实施 LZA，请使用 AWS CDK 或部署安装程序堆栈。AWS CloudFormation针对联网、安全和 RISE with SAP 连接要求，实施标准化配置文件。

5. “配置 AWS 组织-组织” 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) 和服务控制策略 (SCPs) 在 Control Tower 中配置组织。对于 LZA 实现，请确保与配置文件结构 OUs 保持一致。
6. 部署核心账户与共享服务账户 - 创建并配置核心账户，例如管理账户、共享服务账户（用于日志记录、安全工具部署）以及任何其他所需的共享账户。在共享服务账户中部署共享服务 CloudTrail，例如 Config 和 Sec AWS urity Hub。
7. 部署网络架构-设置网络架构，包括子网、路由表和 VPCs中心辐射模型的 Transit Gateway。对于 LZA 实施，请通过网络配置文件配置 Direct Connect and/or Site-to-Site VPN。如果需要，可加入 AWS Network Firewall 设置。
8. 配置 IAM - 构建 IAM 角色、策略和组，以便控制跨登录区账户的访问和权限。
9. 实施安全控制-部署安全服务和护栏，例如 Security Hub、Network Fi re AWS wall 和 Confi AWS g 规则。AWS GuardDuty
10. 配置可观察性和监控-设置集中式日志和监控解决方案，例如 Amazon CloudWatch 和 AWS Config。AWS CloudTrail
11. 使用 “ AWS 连接问卷” 与 SAP 共享 Transit Gateway 详细信息。接受传入的中转网关关联请求，并配置 RISE with SAP VPC 与登录区之间的路由。测试连接和失效转移方案。
12. 部署工作负载账户 - 使用登录区部署工作负载账户。为不同的工作负载类型创建单独的 AWS 账户，例如将开发、测试和生产环境分开，或者使用 Amazon Bedrock 的生成式 AI 工作负载，或者使用 Amaz SageMaker on 的数据分析工作负载。
13. 实施操作程序 - 建立监控、提醒和备份程序。编写操作程序文档并实施变更管理流程。考虑到多账户环境的复杂性，以及需要在整个企业内维持一致的安全与操作标准，建议构建自动化测试与验证体系。
14. 自动化和维护-使用 CloudFormation 模板或 AWS CDK 自动部署和维护。对于 LZA 实施，需要维护配置文件并定期更新 LZA 版本。建立持续维护、更新和合规性检查流程。这包括保留 LZA 版本 up-to-date的最新版本，并定期检查以确保符合安全性和合规性标准。
15. 管理成本 - 监控网络传输成本，优化连接路径并采用成本分配标签。定期检查资源利用率，并配置预算和提醒。

最佳实践：

- 至少在计划上线前 6-8 周开始实施
- 实施冗余连接方案以实现高可用性
- 使用登录区加速器进行标准化部署
- 遵循 AWS Well-Architected Framework 指南

- 定期审查并更新安全控制措施
- 维护文档和操作程序
- LZA 实施可通过配置文件自动执行大部分设置工作。

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。请参阅 AWS 定价计算器以配置符合您业务需求的成本估算。

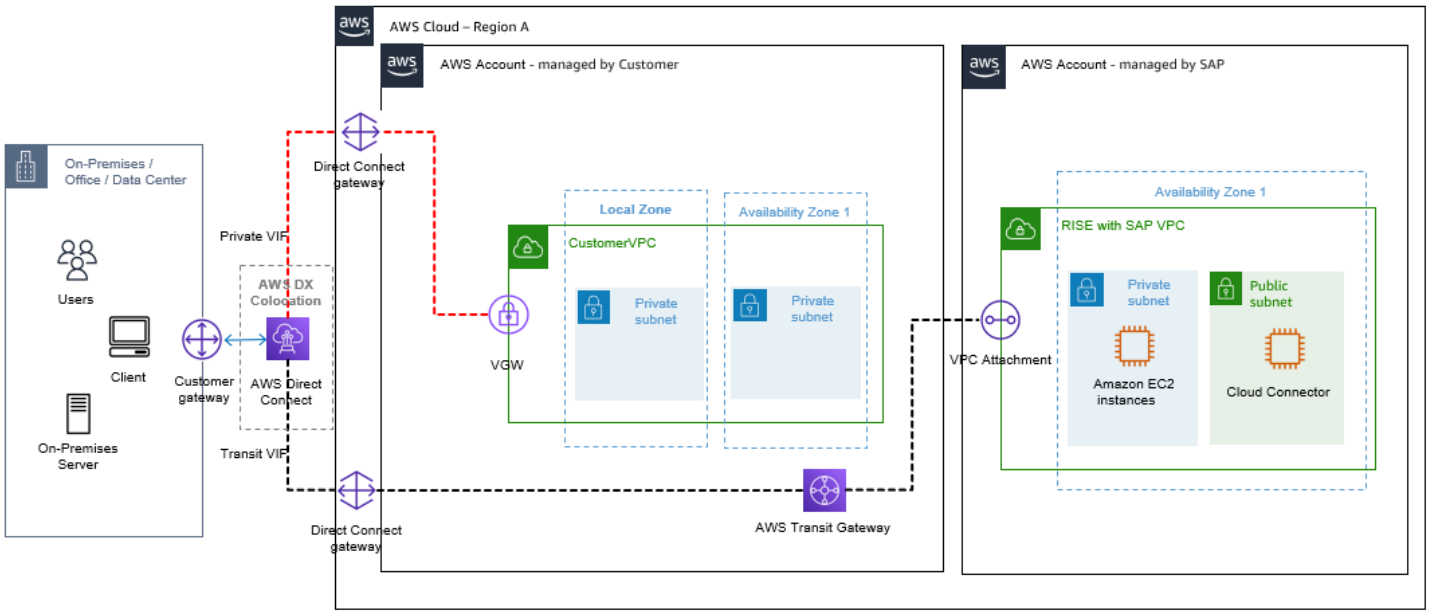
定期审查并更新登录区配置，确保其持续满足不断变化的业务需求和安全要求。

连接到最近的 Direct Connect POP（包括本地区域）

AWS Direct Connect point-of-presence (POP) 是一种物理交叉连接，允许用户建立从自己的场所到 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。您可以使用马尼拉的 Direct Connect POP，从您的本地数据中心或办事处设置 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。

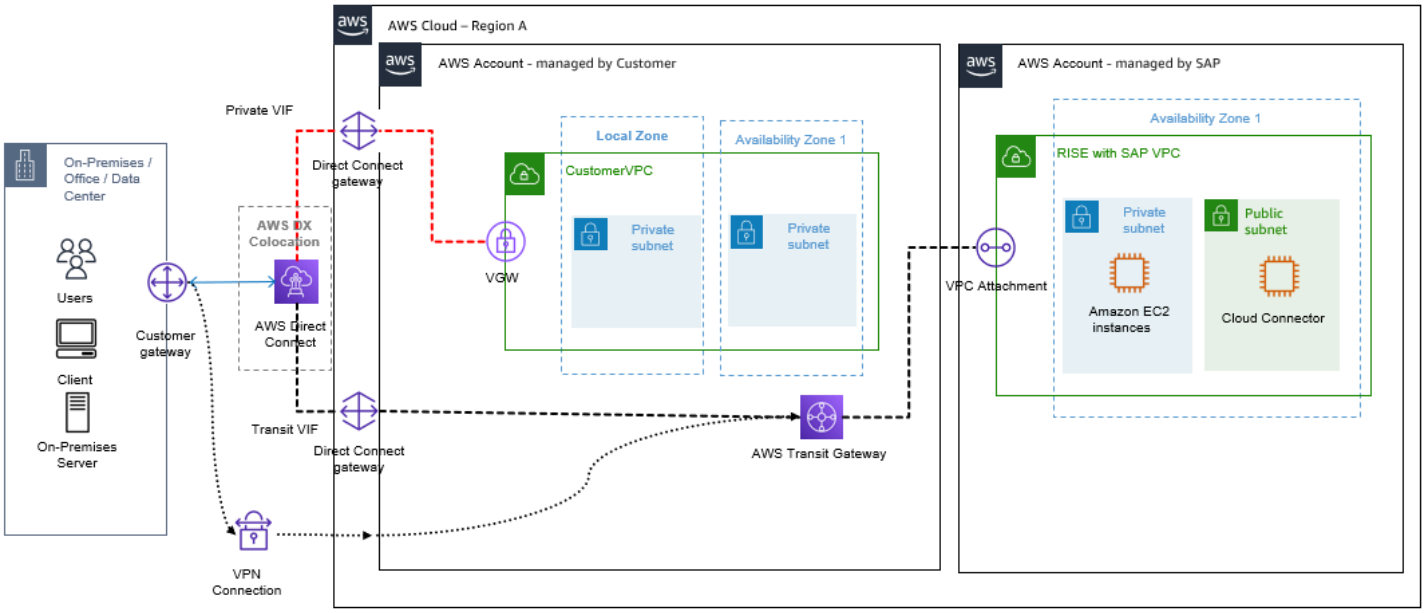
下图显示了通过最近的 Di AWS rect Connect POP 进行的 RISE 连接。



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。



在本地 AWS 区域和同一区域内的可用区之间传输数据（“进入” 和 “传出” 本地区域中的 Amazon EC2）的成本各不相同。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

RISE 连接方案决策树

您必须建立所需的连接才能在 SAP 开启的情况下继续 RISE AWS。以下是前面几个部分中所述的几种连接模式：

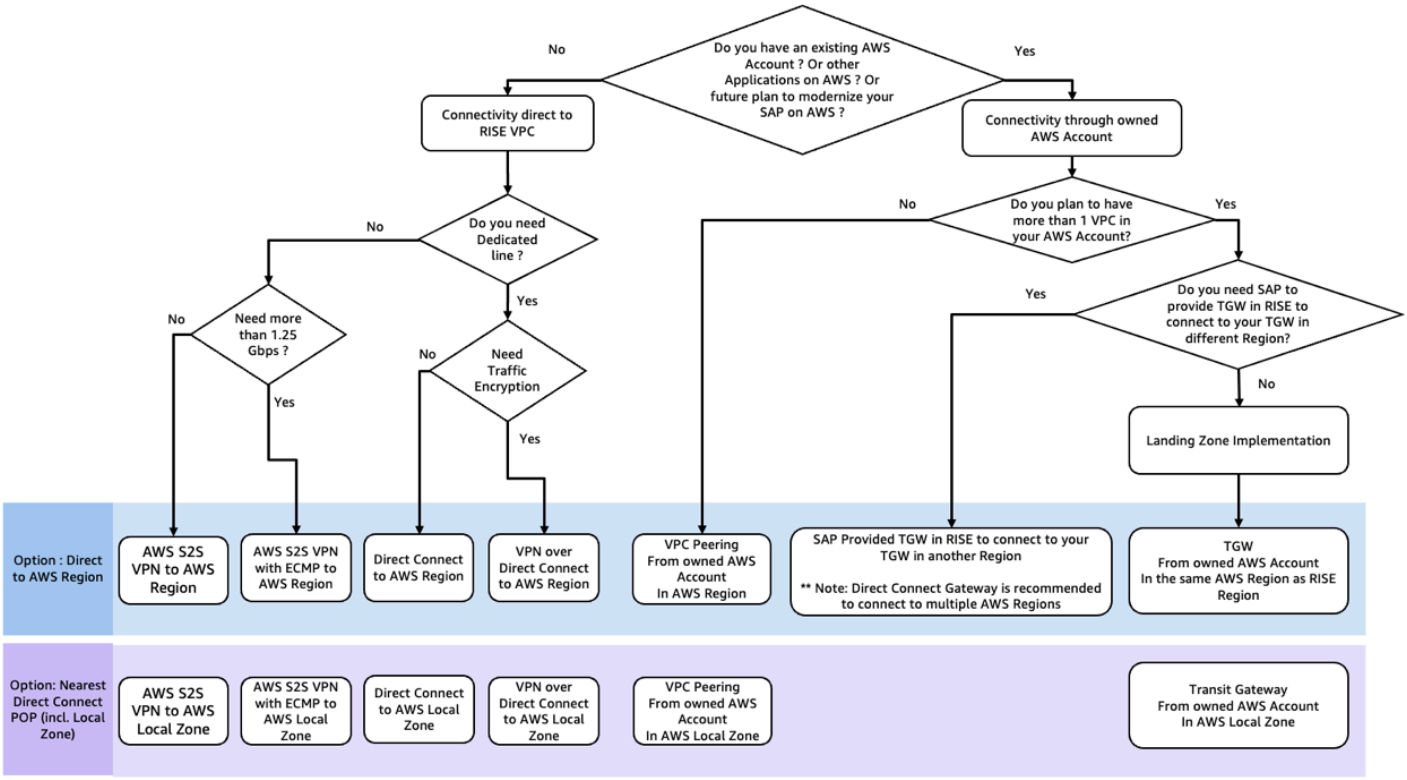
- 直接连接到 RISE VPC，支持 Site-to-Site VPN
- 直接连接至 RISE VPC，由 Direct Connect 提供支持
- 通过 VPC 对等互连通过您的 AWS 账户进行连接
- 通过 Transit Gateway 建立连接，支持多账户部署

- 通过由 SAP 管理的 Transit Gateway 建立连接，支持多账户部署

您还必须考虑连接方式：

- 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 以使用 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

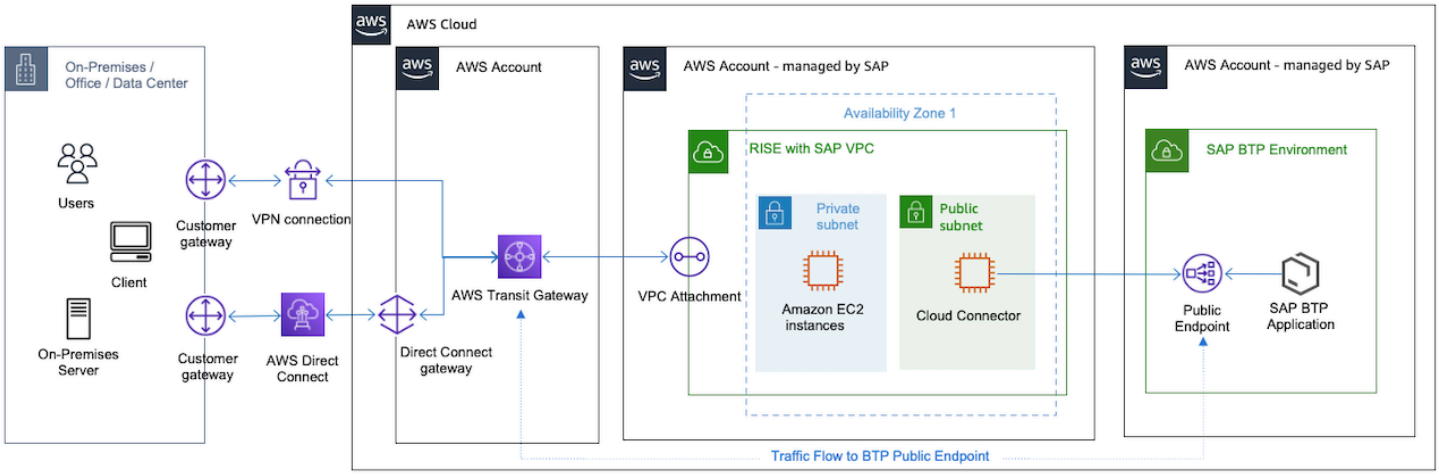
此部分介绍了连接到 RISE 时的其他注意事项。

主题

- 开启 RISE 的 SAP BTP AWS
- 从 RISE 连接到 SaaS
- 多云环境的连接模式
- 实施 RISE 连接费用分摊功能
- 在 RISE 中连接到重叠 IP 开启 AWS
- 将 DNS 集成到 RISE 和 Route 53

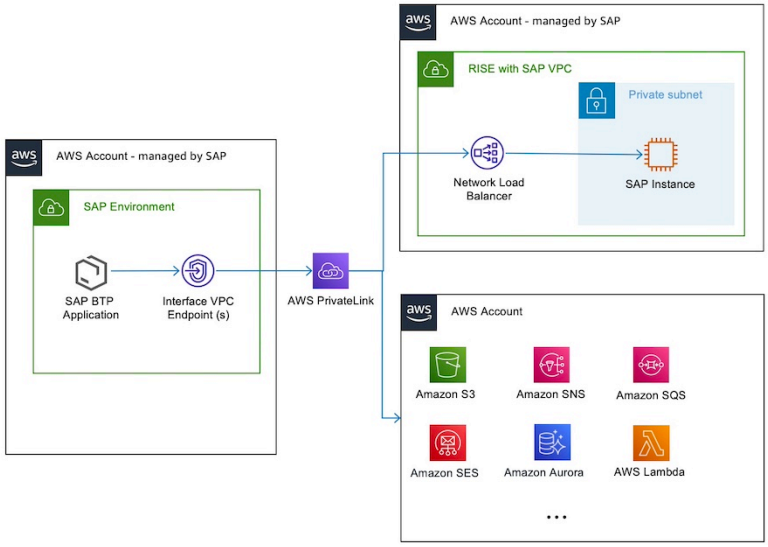
开启 RISE 的 SAP BTP AWS

你可以使用 SAP Business Technology Platf AWS orm BTP 服务，通过 SAP 扩展 RISE 的功能。SAP 建议通过 SAP Cloud 连接器，借助互联网将 RISE with SAP VPC 与 SAP BTP 相连。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 with SAP 与 SAP BTP 之间的所有集成使用案例提供了更出色的安全性和性能。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 路由来自本地环境的互联网流量？

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

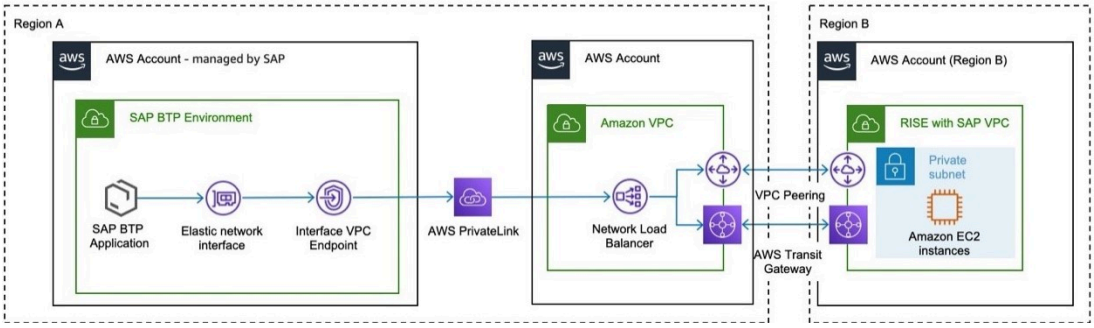


您可以从 Cloud Foundry 上运行的 SAP BTP 应用程序连接到 AWS 终端节点服务。通过建立此连接，您可以直接连接到 AWS 服务，或者例如，连接到 S/4HANA 系统。有关支持 AWS 服务的完整列表，请参阅在 SA P BTP 中使用亚马逊 Web 服务。

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），您可以减小应用程序的攻击面。该连接无需互联网网关。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。有关受支持的区域列表，请参阅 Regions and API Endpoints Available for the Cloud Foundry Environment。



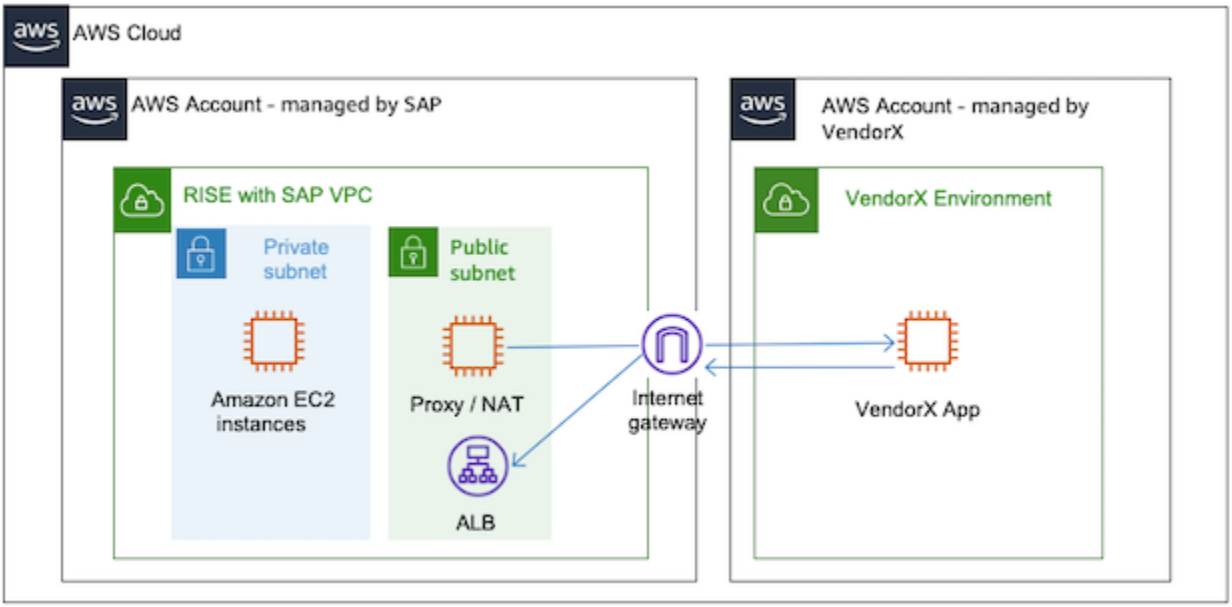
SAP Private Link Service 是 SAP 在 SAP BTP 上提供的一项付费服务。有关更多信息，请参阅：SAP Discovery Center – Services – SAP Private Link Service。

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。

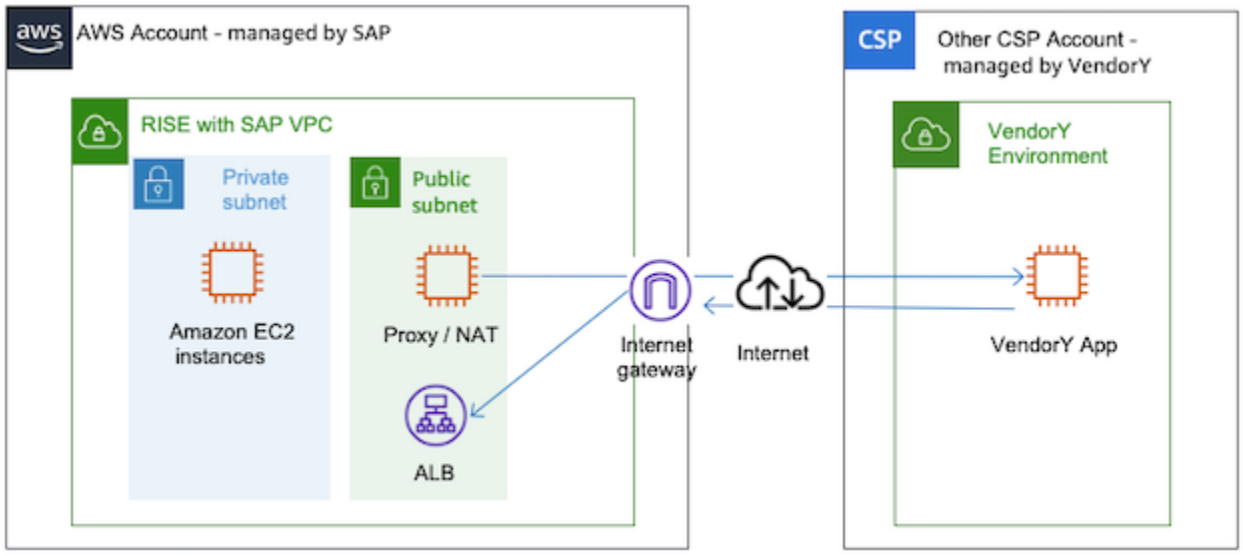
从 RISE 连接到 SaaS

在对 SAP 环境进行现代化改造时，您可以订阅多种 SAP Cloud 解决方案或来自独立软件供应商的 SaaS，以作为 RISE with SAP 解决方案的有力补充。

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运行或通过其他云服务提供商平台运行，则需要互联网连接。



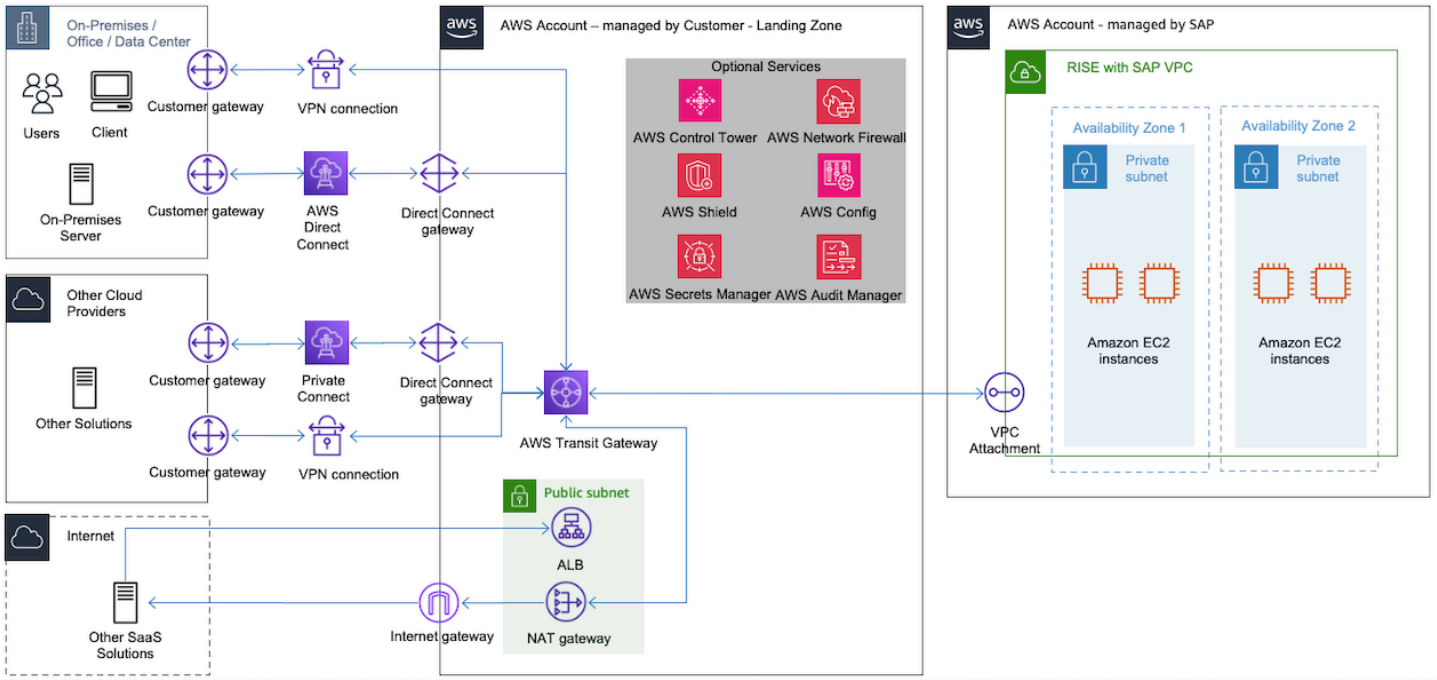
SaaS 云解决方案不支持通过 VPN、Direct Connect 或任何其他私有连接方式来建立此连接。您可以实施集中式互联网出口架构来管理此连接。有关更多信息，请参阅集中式互联网出口。

多云环境的连接模式

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。

您可以使用公有连接或私有连接将多云环境与 RISE 相连。



公有连接

连接通过公共互联网进行路由。此模式通常用于 RISE with SAP 与跨多个云运行的 SaaS 解决方案之间的连接。在建立通过公共互联网路由的连接时，请注意以下事项：

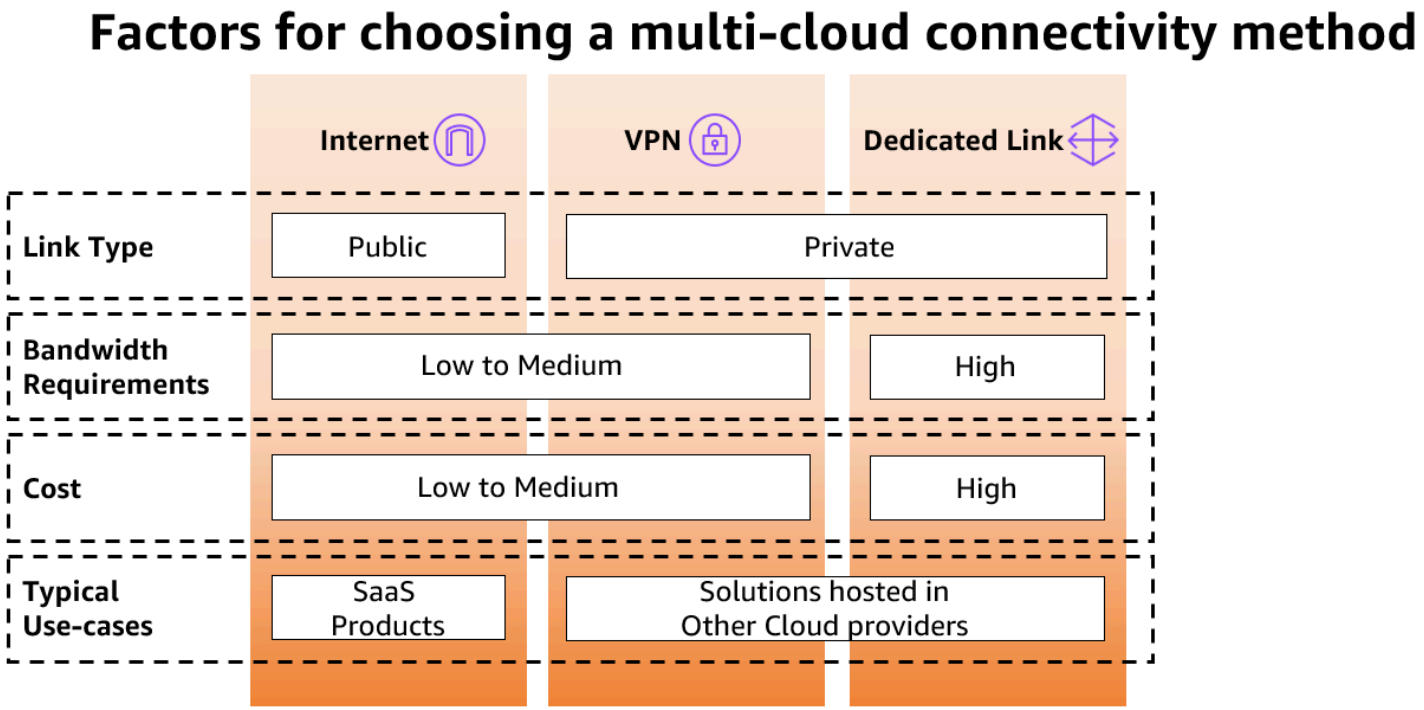
- 确保所有通信均已加密
- 使用弹性负载均衡器和 Shield 等 AWS 服务保护端点 AWS
- 使用 Amazon 监控终端节点 CloudWatch
- 确保托管的两个公有 IP 地址之间的流量通过网络路由 AWS AWS

私有连接

可使用以下三种方案，在不同的云服务提供商之间建立私有连接：

- 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式时需考虑的因素。

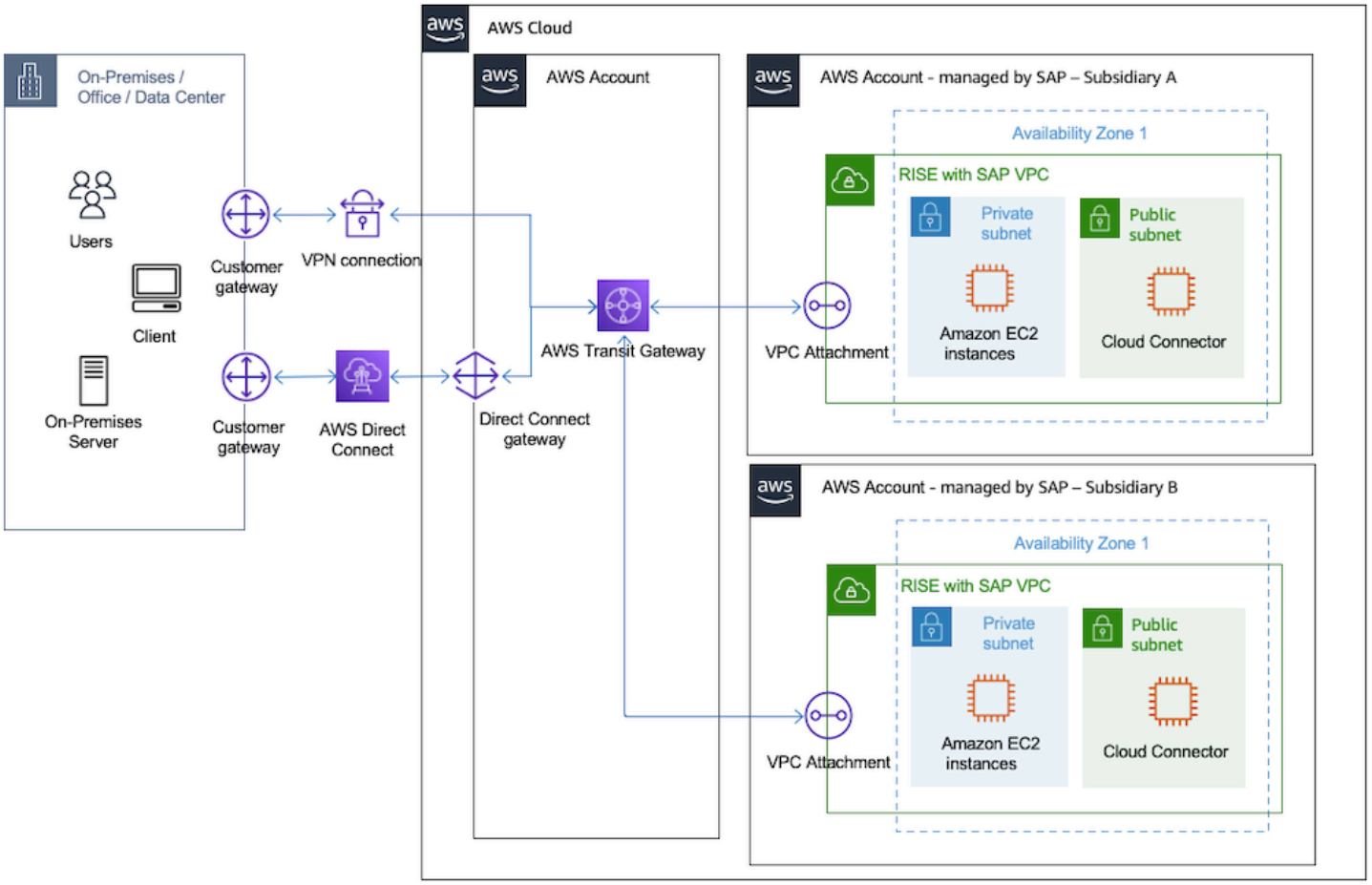


有关更多信息，请参阅设计与 Microsoft Azure AWS 之间的私有网络连接。

实施 RISE 连接费用分摊功能

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。在此情况下，您必须在登录区（多账户）环境中部署 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 流日志支持高效的成本管理。Transit Gateway 流日志可与成本和使用情况报告（CUR）集成，进而将相关成本分摊至各个业务部门。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，请参阅以下博客文章：

- 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

执行以下步骤来启用此设置：

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，并配置 Athena 以使用该报告。有关更多信息，请参阅创建成本和使用情况报告和使用 Amazon Athena 查询成本和使用情况报告。
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 - 在所有账户间平均分配成本，或按比例分配成本。
   b. 通过 AWS Transit Gateway 查询，计算每个账户的总网络流量及分配百分比。

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 = 每个使用账户的分摊成本

在 RISE 中连接到重叠 IP 开启 AWS

叠加 IP 是分配给 VPC CIDR 数据块之外的 EC2 实例的私有 IP 地址。它用于 SAP 部署中的高可用性和故障转移场景 AWS，即使活动实例位于不同的可用区，也可以将流量定向到活动实例。此 IP 地址可路由，并通过路由表进行管理，无需修改应用程序配置即可实现无缝失效转移。

在以下情况下，叠加 IP 在 RISE 构造中非常重要：

- SAP GUI 与 ASCS 实例中的 SAP 消息服务器的连接
- 应用程序服务器与 ERS 实例中的 SAP 队列服务器的连接
- 客户端与 HANA 数据库的连接（当客户端运行 XS 应用程序和 XS Advanced 应用程序时）

当主节点或主可用区出现可用性问题时，高可用集群软件会将叠加 IP 从主节点迁移至备用节点（反之亦然）。在发生此事件时，所有客户端连接都必须重新路由，以确保用户能够继续开展业务活动。

可通过以下两种方式连接到此叠加 IP 地址：网络负载均衡器（NLB）和 AWS Transit Gateway（TGW）。您可以在本 SAP “使用叠加 IP 地址路由实现 AWS 高可用性” 指南中参考更多详细信息。

NLB 配置

RISE with SAP 高可用性部署策略跨两个可用区实施，并涉及多个关键联网组件。在设置此配置时，SAP 会 NLBs 专门为两个关键叠加层实施 IPs，一个用于数据库，另一个用于 ASCS。为了管理 DNS 解析，SAP CNAMEs 在其的 RISE 托管 DNS 系统中包含了与亚马逊 NLB 地址（结尾为.amazonaws.com）相对应的 DNS 系统。

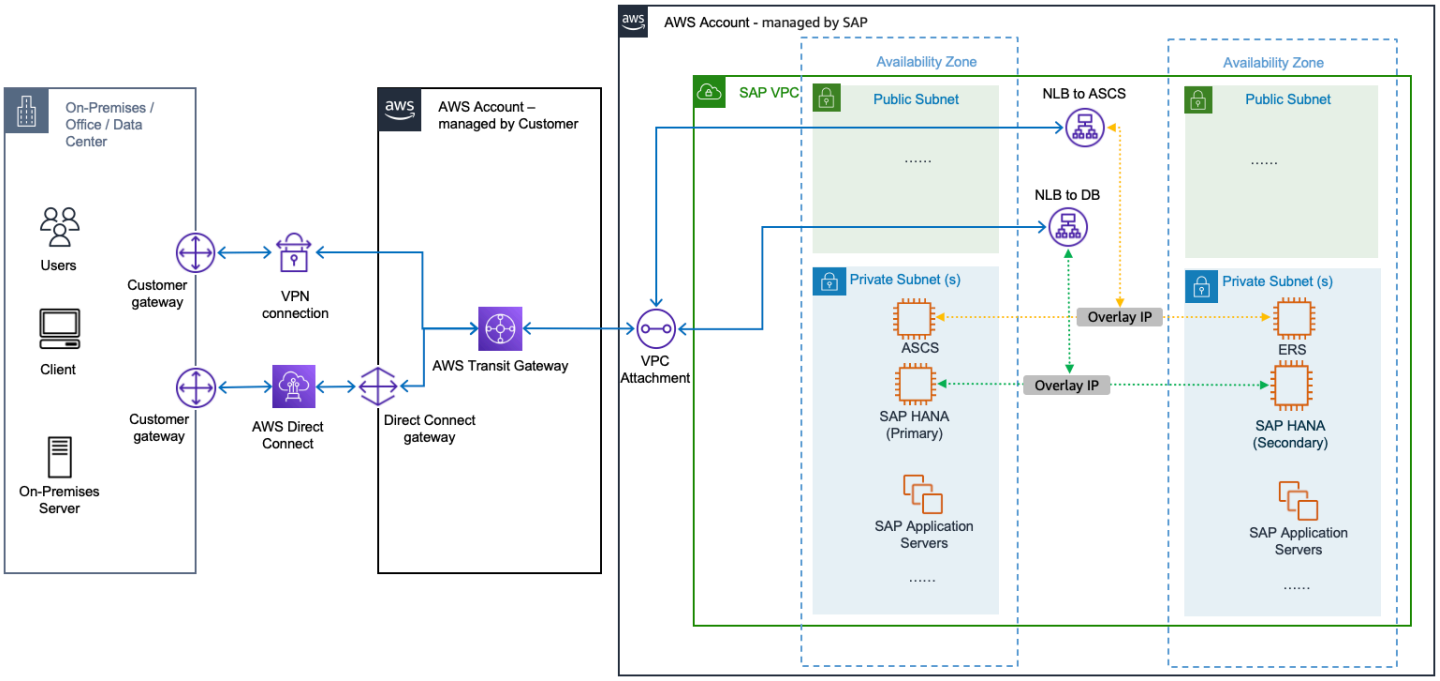
通过 VPC 对等连接来连接到 RISE with SAP VPC 时，您只能使用网络负载均衡器（NLB）地址访问该系统，而无法通过叠加 IP 地址直接访问。

Transit Gateway 配置

当您使用 TGW 时，SAP 的默认配置仅传播其当前正在使用的 VPC CIDR 范围的路由。这就要求客户必须手动为叠加 IP 所使用的 CIDR 范围（位于 VPC CIDR 范围之外）配置静态路由。这种额外的配置

至关重要，因为它允许 IPs 通过 TGW 直接访问这些叠加层。如果未进行此静态路由配置，流量便只能借助网络负载均衡器通过效率较低的路径传输，而不是直接通过 TGW 传输。

此路由配置是客户在其 SAP 部署过程中需重点关注的关键细节，因为它会对来自终端用户及 RISE with SAP 外部的其他系统的网络流量传输效率产生重大影响。



将 DNS 集成到 RISE 和 Route 53

本文档提供了有关 “RISE with SAP” 部署的域名系统 (DNS) 集成选项的指导 AWS，重点介绍企业场景，在这些场景中，客户希望在 RISE 和 SAP 工作负载与跨 AWS 外部环境的现有工作负载之间实现名称解析。

双向 DNS 集成对于将 RISE 与 SAP 系统连接到各种 AWS 云和本地资源以及企业基础设施至关重要。在制造环境中，一个常见的使用案例是将 SAP 应用程序连接至车间设备。例如，SAP 可能需要与生产车间内的打印机通信，以生成标签、工作订单或货运单据。这就要求在 RISE with SAP 环境中能够解析“printer-line1.factory.company.local”这类内部主机名。

相反，外部系统和应用程序通常需要通过 DNS 查找来访问 RISE with SAP 环境中的资源，尤其是在调用 ODATA API 端点来开展业务事务（例如，生成工作订单）时。由于合规性和安全性要求，RISE with SAP 系统与现有企业系统之间的集成场景通常需要内部网络连接。这一点对于 RISE with SAP 部署尤为重要，因此以下各部分将重点介绍私有网络内的 DNS 解析。

由于合规性和安全性要求，RISE with SAP 系统与现有企业系统之间的集成场景通常需要内部网络连接。这一点对于 RISE with SAP 部署尤为重要，因此以下各部分将重点介绍私有网络内的 DNS 解析。

架构方案

将 RISE with SAP 与您现有的 DNS 设置集成时，您可以采用两大架构方案：条件 DNS 转发和 DNS 区域传输。您还必须考虑 DNS 区域委派相关事宜。这些选项和注意事项专为 AWS仅限部署和与外部环境（例如本地环境或其他云提供商） AWS 连接的混合场景而设计。

DNS 集成架构的选择取决于您的服务可靠性需求、现有 DNS 基础设施能力，以及可接受的运维复杂度，与自运营 DNS 基础设施相比，托管服务所需的维护工作和专业知识通常会更少。

在与 RISE with SAP 进行 DNS 集成时，我们建议通过 Amazon Route 53 Resolver 端点实施条件 DNS 转发。Route 53 可提供高度可用、可扩展的 DNS 服务，从而最大限度地降低运维开销。借助此方法，您无需设置和运行自己的 DNS 服务器，并且可进一步降低运维复杂度。此外，Route 53 还可通过亚马逊与您的现有环境和监控功能直接集成 CloudWatch。不过，如果您有特定的要求或技术限制，可以参考后续部分中详细介绍的替代方案。

推荐的 DNS 分割模式是为每个环境实施专用子域（例如，aws.corp.com、dc.corp.com 和 sap.corp.com），通过有条件的跨环境转发来对每个环境进行 DNS 本地解析。此方案通过将本地 DNS 请求保持在其相应的环境中来优化性能，进而减少延迟、提升系统韧性并简化 DNS 管理。具体而言，它能够有效地减少环境间网络链路故障产生的影响。

通用基础设施要求

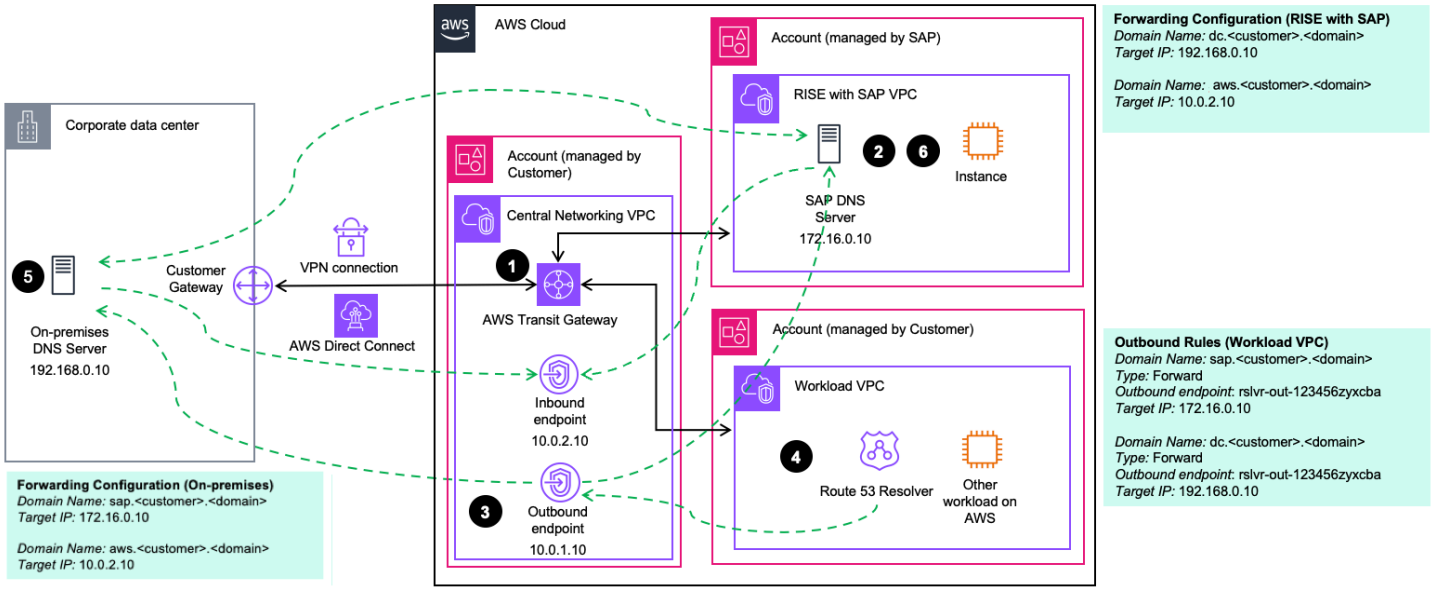
在实施 DNS 集成方案之前，请确保满足以下先决条件（另见后续图表）：

1. 网络连接：T AWS ransit Gateway（或云广域网或 VPC 对等互连）通过 AWS Direct Connect 或 AWS Site-to-Site VPN 连接外部 AWS 环境、您的环境以及使用 SAP VPC 的 RISE。
2. 域委派：在 RISE with SAP 设置过程中，SAP 要求将子域（sap.<customer>.<domain>）委派给 RISE with SAP VPC 中的 RISE DNS 服务器。这使终端用户和应用程序能够通过您组织的域访问 RISE with SAP 系统。

条件 DNS 转发（推荐方案）

条件 DNS 转发支持将特定域名的查询选择性地转发到另一台 DNS 服务器进行解析（例如，Amazon Route 53 将 sap.corp.com 的 DNS 查询转发至 RISE DNS 服务器）。我们建议实施条件 DNS 转发，除非因技术限制导致无法采用此方案。此方案的核心优势在于，客户可以利用 Route 53，而不是在 AWS上设置和运营自己的 DNS 基础设施。这样一来，客户既简化了集成路径，又获得了 Route 53 高度可用且可靠的全球基础设施带来的优势。

以下参考架构概述了此方案所需的组件：



1. 网络连接：请参阅“通用基础设施要求”
2. 域委派：请参阅“通用基础设施要求”
3. 在您的中央网络 VPC 中创建 Route 53 解析器终端节点（入站和出站），以处理您的 AWS 账户与 RISE with SAP 账户之间的 DNS 查询。请遵循 Resolver 端点的最佳运维实践。我们建议在所有可用区部署多个终端节点并监控其利用率 CloudWatch 以实现主动扩展。向 SAP 提供您的本地 DNS 服务器的详细信息以及 Route 53 Resolver 端点的 IP 地址（用于转发和防火墙配置）。
4. 在工作负载中配置 Route 53 解析器规则 VPCs 以转发 DNS 查询，如下所示：
   a. SAP 绑定的 DNS 查询：转发到出站端点以通过 SAP DNS 服务器解析查询
   b. 企业数据中心绑定的 DNS 查询：转发到出站端点以通过本地 DNS 服务器解析查询
5. 将本地 DNS 服务器配置为转发 DNS 查询，如下所示：
   a. SAP 绑定的查询：转发到 SAP DNS 服务器（或者，从 SAP DNS 服务器进行 sap.<customer>.<domain> 的区域传输）
   b. AWS绑定的查询：转发到入站端点
6. 对 SAP DNS 服务器进行如下配置：
   a. 企业数据中心绑定的 DNS 查询：转发到本地 DNS 服务器
   b. AWS绑定的 DNS 查询：转发到入站端点

确保您的工作负载 VPCs 具有所有相关的解析器规则，用于通过中央网络 VPC 转发 DNS。我们建议使用 Route 53 配置文件来管理这些配置，因为它们可以在多个 VPCs 和 AWS 账户之间实现一致

的 DNS 设置。这种方法允许您在整个 AWS 基础架构中定义和应用标准化的 DNS 配置，从而简化了 DNS 管理。

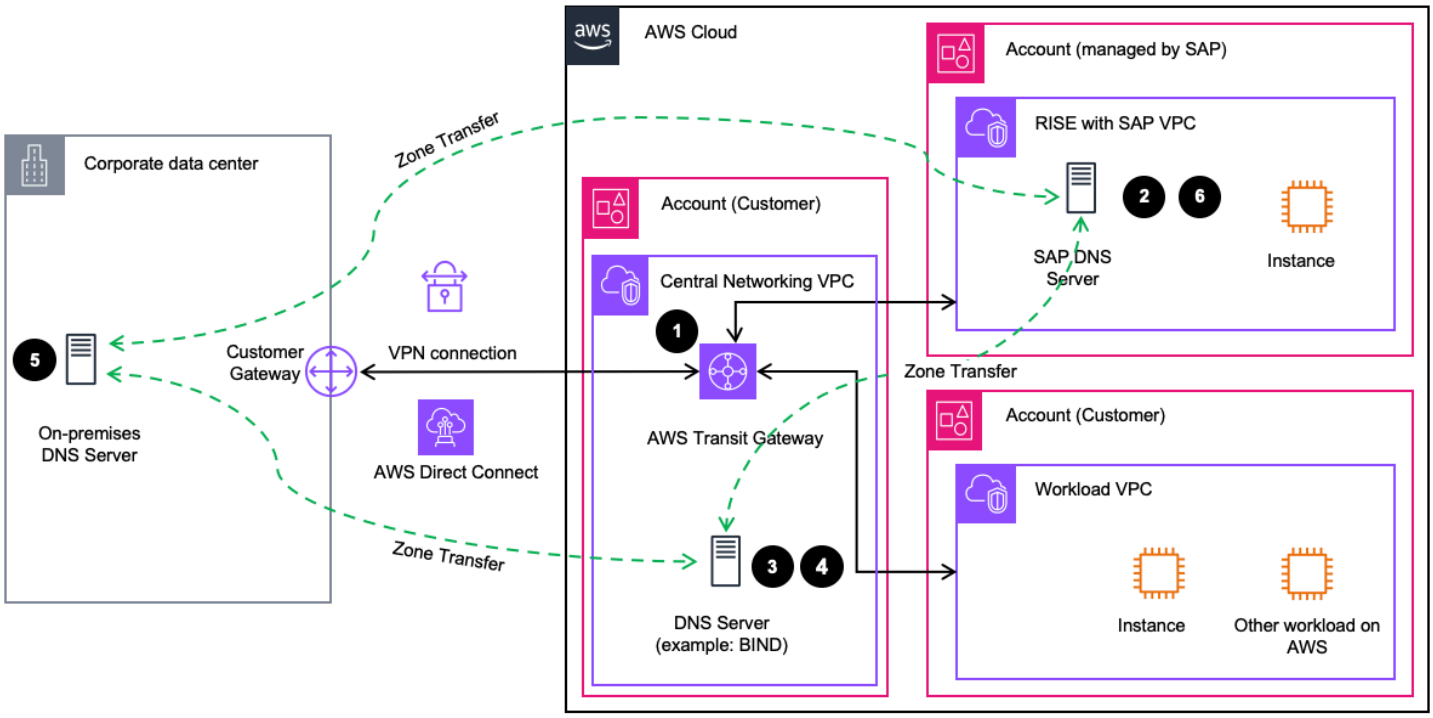
请注意，对于混合环境中的 DNS 解析，DNS 委派可作为条件转发的替代方案。虽然通常会建议您在 RISE with SAP 环境中使用条件转发，但 DNS 委派在特定场景中可能更具优势，尤其适用于存在许多分布式 DNS 解析器且没有集中式上游解析器的环境。但对于涉及 SAP DNS 服务器的场景，还需考虑其他技术注意事项，如“DNS 区域委派”部分中所述。

DNS 区域传输

通过区域传输，权威 DNS 服务器的 DNS 数据库会在一组辅助 DNS 服务器之间进行复制。您可以直接在本地 DNS 服务器和 RISE 环境中的 SAP DNS 服务器之间实现区域传输。但是，如果您想扩展区域传输以包括您的 AWS DNS 命名空间（例如 aws. <customer>。 <domain>) 要在本地和工作负载之间进行通信 VPCs，您需要在自己的 AWS 环境中操作自己的 DNS 服务器（例如 BIND）。这是因为 Route 53 不支持区域传输。请记住，与使用 Route 53 进行 DNS 转发相比，此方案会增加运维复杂性。

有关此方法的详细信息，请咨询您的 SAP 云架构师或您的 AWS 客户团队。有关运行您自己的 BIND DNS 服务器的最佳实践，请参阅此链接。

下图显示了通过区域传输将 RISE 环境与现有 DNS 环境（本地/ AWS ）集成的参考架构。



1. 网络连接：请参阅“通用基础设施要求”

2. 域委派：请参阅“通用基础设施要求”
3. 在联网 VPC 中设置中央 DNS 服务器（例如，EC2 上的 BIND），或通过相应修改 VPC DHCP 选项集，在每个工作负载 VPC 中设置分散式 DNS 服务器。请向 SAP 提供您的本地 DNS 服务器和 AWS托管的 DNS 服务器的详细信息（用于区域传输和防火墙配置）。
4. 按如下方式配置 AWS托管的 DNS 服务器：
   a. SAP 绑定的查询：从 SAP DNS 服务器进行 sap.<customer>.<domain> 的区域传输
   b. 数据中心绑定的查询：从本地 DNS 服务器进行 dc.<customer>.<domain> 的区域传输
5. 对本地 DNS 服务器进行如下配置：
   a. SAP 绑定的 DNS 查询：从 SAP DNS 服务器进行 sap.<customer>.<domain> 的区域传输
   b. AWS绑定的 DNS 查询：aws 的区域转移。 <customer>。 <domain>来自 AWS软管的 DNS 服务器
6. 对 SAP DNS 服务器进行如下配置：
   a. 客户数据中心绑定的 DNS 查询：从本地 DNS 服务器进行 dc.<customer>.<domain> 的区域传输
   b. AWS绑定的 DNS 查询：aws 的区域转移。 <customer>。 <domain>来自 AWS软管的 DNS 服务器

DNS 区域委派

如果客户运行跨多个环境分布的多个 DNS 解析器，并且未使用集中式 DNS 解析器服务，则配置并维护 DNS 转发规则或区域传输可能会带来运维挑战。利用 DNS 区域委派功能，您可以在 DNS 层次结构中的单个点上定义特定子域的权限，从而简化整个基础设施的 DNS 管理工作。

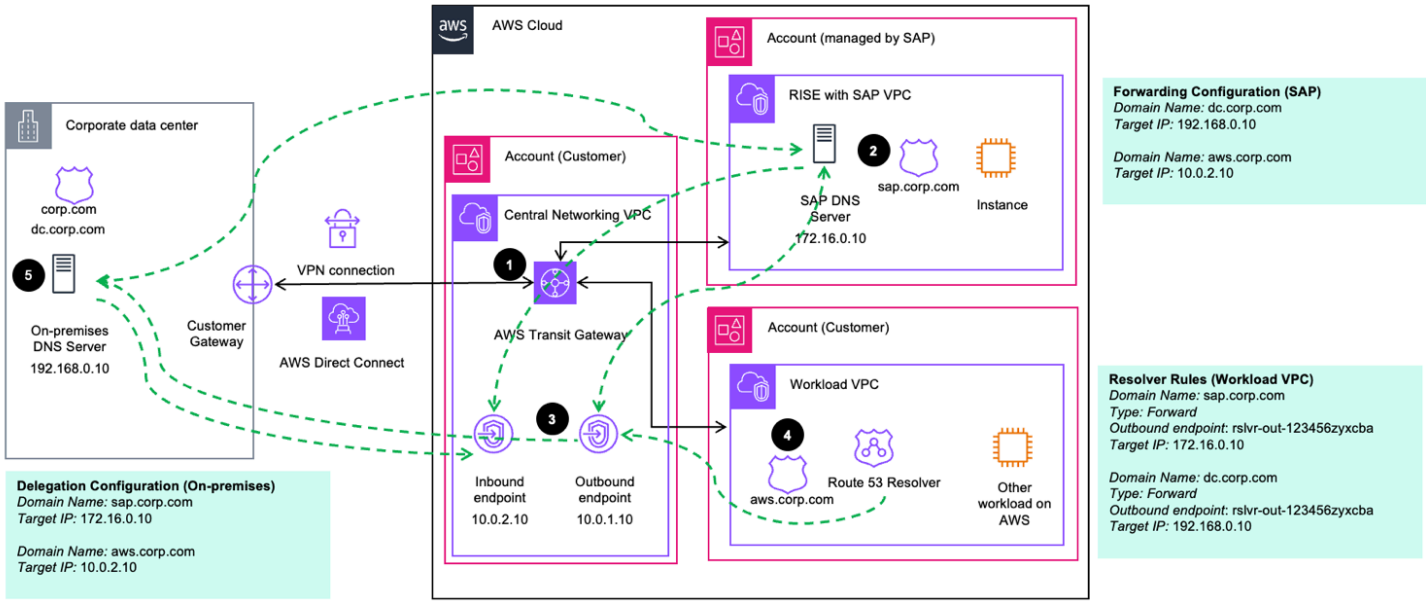
使用具有 DNS 委派功能的 Amazon Route 53 Resolver 终端节点，您可以构建和维护跨本地和 AWS 环境的统一私有 DNS 命名空间。

然而，在 RISE 环境中与将区域委派功能与 SAP DNS 服务器结合使用时，有特定的技术注意事项。如果没有集中式上游解析器，由于缓存效率降低，向 SAP DNS 服务器进行区域委派会增加并发查询负载。此外，所有 DNS 解析器都需要指向 SAP DNS 服务器的直接网络路径，这可能需要额外的连接配置。实施此方案之前，请咨询 SAP ECS。

存在两种主要场景：

场景 1 AWS 上的 Route 53 中的父域

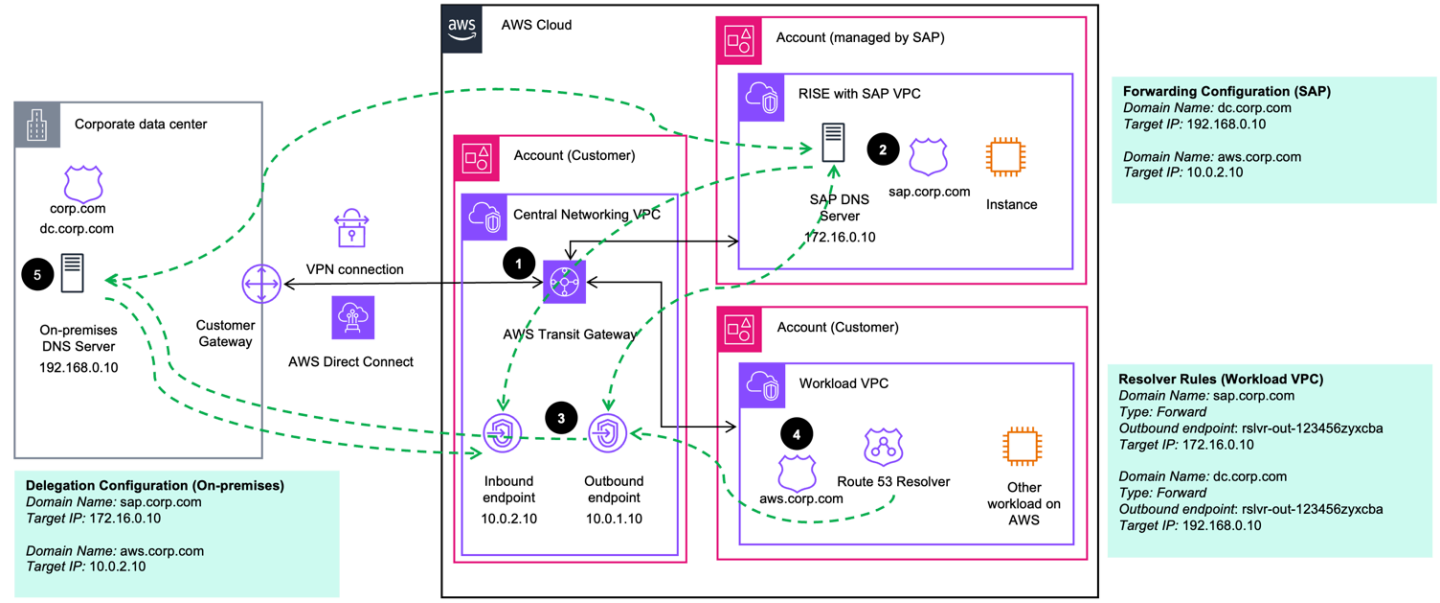
对于在云中运行大部分工作负载并 AWS 使用 Route 53 操作私有 DNS 根区域的客户，您可以将子域委托给外部 DNS 服务器。这包括同时委派给 SAP DNS 服务器（例如 sap.corp.com）和本地 DNS 服务器（例如 dc.corp.com）。



1. 网络连接：请参阅“通用基础设施要求”
2. 域委派：请参阅“通用基础设施要求”
3. 在您的中央联网 VPC 中设置 Route 53 Resolver 端点（入站和出站）
4. 将 IPs 本地和 SAP DNS 服务器配置为父域（例如 corp.com）的私有托管区域 (PHZ) 中的 NS 记录，并将 PHZ 与您的工作负载关联（Route VPCs 53 配置文件可以帮助管理 PHZ 关联和解析器规则）。如果您的 DNS 服务器在同一域（例如 ns.dc.corp.com）中，则还需在父域中配置粘附记录。为相关子域 (dc.corp.com) 创建 Route 53 解析器委托规则，并将它们与您的工作负载 VPCs 相关联（参见上图）。
5. 在本地解析器上配置条件 DNS 转发，以允许解析父域和 SAP 域（SAP 端需进行相同配置）

场景 2 本地父域

对于刚开始云之旅但仍在本地维护根区域的客户，DNS 委派提供了一种集成 SAP 和 AWS 环境的有效方法，同时保持本地的 DNS 控制。



1. 网络连接：请参阅“通用基础设施要求”
2. 域委派：请参阅“通用基础设施要求”
3. 在您的中央联网 VPC 中设置 Route 53 Resolver 端点（入站和出站）
4. 为 aws.corp.com 配置 PHZ 并将其关联到您的中央网络和工作负载。 VPCs配置条件 DNS 转发规则，以允许 VPC 解析本地工作负载和 RISE with SAP 系统的查询（SAP 端需进行相同配置）。
5. 在域的本地权威名称服务器中，使用 sap.corp.com 和 aws.corp.com 的委派（NS）记录（例如 ns1.corp.com）更新 corp.com 区域。

将你的 R AWS oute 53 Resolver 入站终端节点和 SAP DNS 服务器配置 IPs 为 ns1.corp.com 区域文件中的目标记录。如果您的 DNS 服务器在同一域中，则还需在父域中配置粘附记录。

有关区域委派功能的更多详细信息，请参阅 Route 53 文档。以下博客文章为您提供了有关如何使用私有 DNS 的 Route 53 委托功能的更深入的 step-by-step指南：使用 Amazon Route 53 Resolver 终端节点委派简化混合 DNS 管理。

有关上述集成方法的更多信息，请联系您的 SAP 云架构师或您的 AWS 客户团队。

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

- SSO — SAP 云身份服务和 AWS IAM 身份中心
- SSO – SAP Cloud Identity Services 与 Microsoft Entra
- SSO - SAPGUI 前端
- 使用 AWS 服务实现高级安全性
- 将 SAP 数据托管人 KMS 与 AWS KMS 集成
- AWS Nitro 如何通过 SAP 帮助保护 RISE？
- Amazon WorkSpaces 作为远程访问解决方案

SSO — 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者（IdP）集成来集中管理用户访问权限。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。

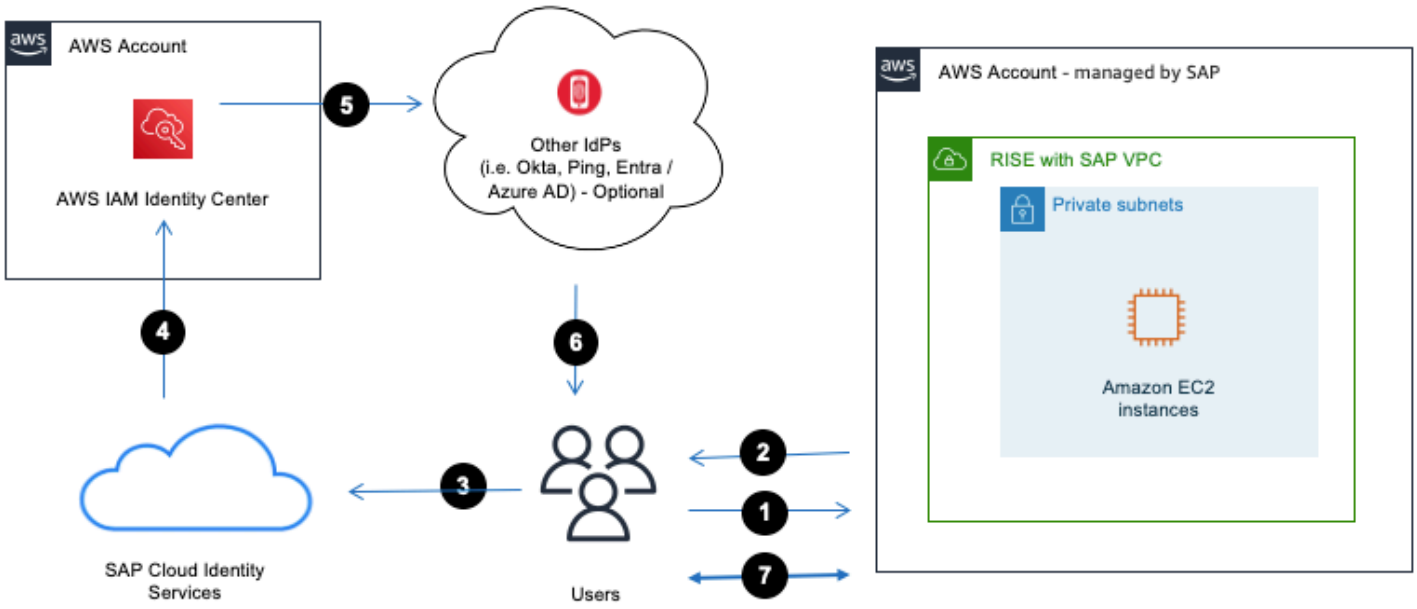
AWS IAM 身份中心是您可以与 RISE 集成以支持单点登录 (SSO) 的 IdP 之一。IAM Identity Center 为用户提供了一个集中式接入点，使他们能够在 AWS 组织内一致地管理 AWS 账户和应用程序（例如在多账户设置中）。

如果您已拥有 Okta、Ping、Microsoft Windows Active Directory、Microsoft Entra（以前称为 Azure Active Directory）等身份源，则可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 Identity Center。

有关更多信息，请参阅以下参考资料：

- 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 Cloud Identity Services - Identity Authentication。

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



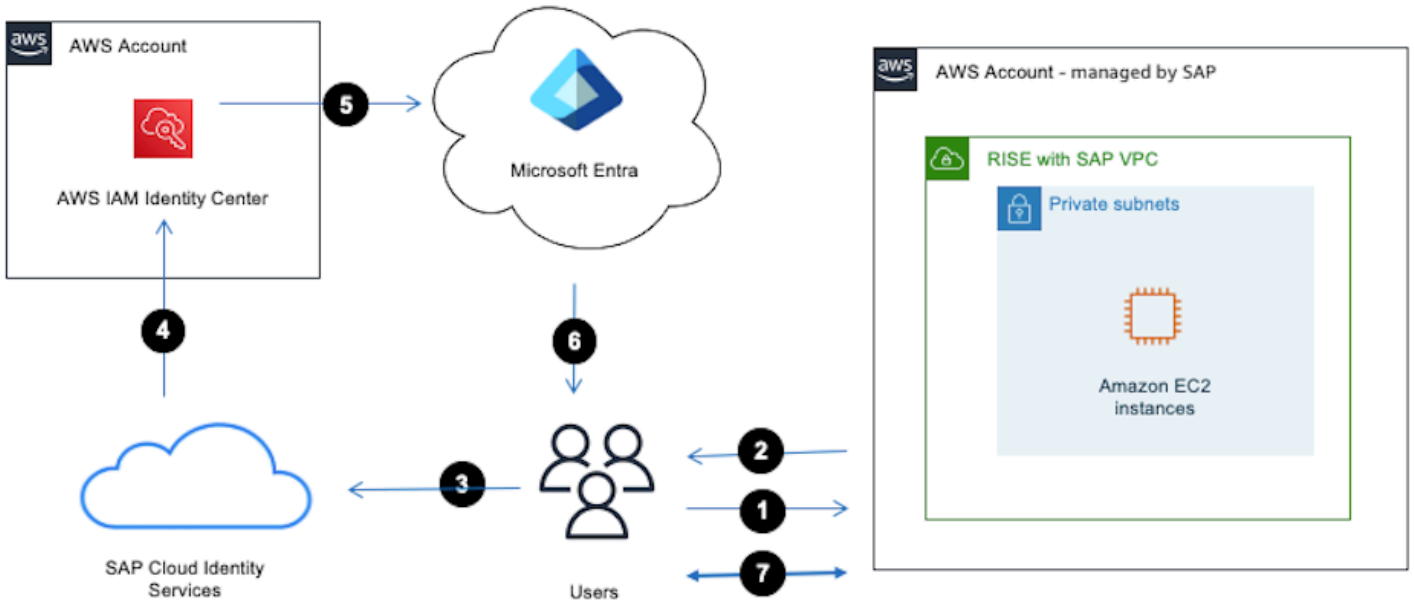
身份验证流程

1. 用户通过互联网浏览器访问 SAP Fiori。
2. SAP Fiori 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 Cloud Identity Services。
4. SAP Cloud Identity Services 将身份验证请求委派给 IAM Identity Center。
5. 如果 IAM Identity Center 与 Okta、Ping、Entra 等现有身份源集成，则 IdP 将对用户进行身份验证。
6. IdP 对用户进行身份验证后，会向互联网浏览器提供包含用户身份信息的 SAML 响应。
7. 用户可访问 RISE with SAP 系统。

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。

SSO – SAP Cloud Identity Services 与 Microsoft Entra

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 Organizations 的多账户策略）时，它支持使用单点登录 (SSO) 进行直接身份验证 AWS 。



身份验证流程

1. 用户通过互联网浏览器访问 SAP Fiori。
2. SAP Fiori 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 Cloud Identity Services。
4. SAP 云身份服务将身份验证请求委托给 IdPs。
5. IdP 对用户进行身份验证后，会向互联网浏览器提供包含用户身份信息的 SAML 响应。
6. 用户可在 RISE with SAP VPC 中访问 SAP S/4HANA。

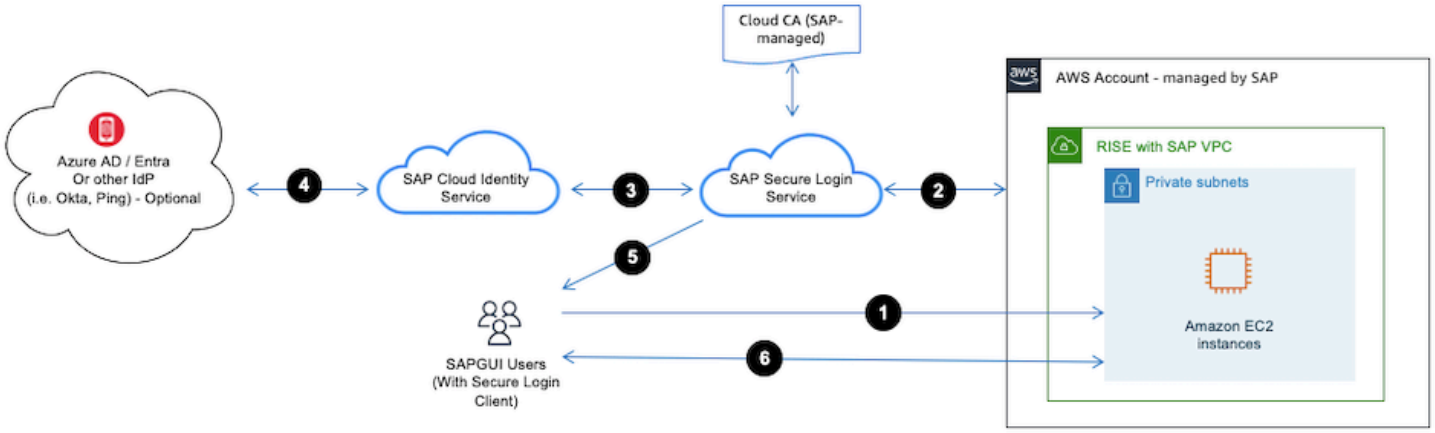
有关如何执行此操作的更多信息，您可以参阅 Enable SSO between Azure AD and SAP Cloud Platform using Identity Authentication Service。

SSO - SAPGUI 前端

SAPGUI 是 SAP ERP 三层架构（数据库、应用程序服务器和客户端）中的图形用户界面客户端，需安装在运行 Windows、macOS 或 Linux 系统的本地桌面设备上。

为了使用 SAP 在 RISE 中实现 SAPGUI 的 Single-Sign-On (SSO)，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 X.509 方法。

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. 用户通过桌面设备访问 SAPGUI。
2. SAP S/4HANA 将身份验证请求重定向到 SAP Secure Login Service。
3. SAP Secure Login Service 将身份验证工作委派给 SAP Cloud Identity Service。
4. 在 SAP Cloud Identity Service 集成到 IdP（即 Azure AD、Okta、Ping 等）后，IdP 将对用户进行身份验证。
5. 在用户通过 IdP 的身份验证后，SAP Secure Login Service 会将 X.509 提供给 SAPGUI。
6. 用户可在 RISE with SAP VPC 中访问 SAP S/4HANA。

有关如何执行此操作的更多信息，您可以参阅 Securing SAP GUI with SAP Secure Login Service。

使用 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这些服务充当一层额外的安全屏障，能在潜在威胁触及 RISE 账户之前对其进行拦截和缓解，提供强有力的防护，并协助遵循行业标准安全最佳实践。

主题

- AWS Network 防火墙
- Amazon Macie
- 亚马逊 GuardDuty
- Security Hub、Detective、Audit Manager 和 EventBridge
- 使用所有 AWS 安全服务

AWS Network 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。

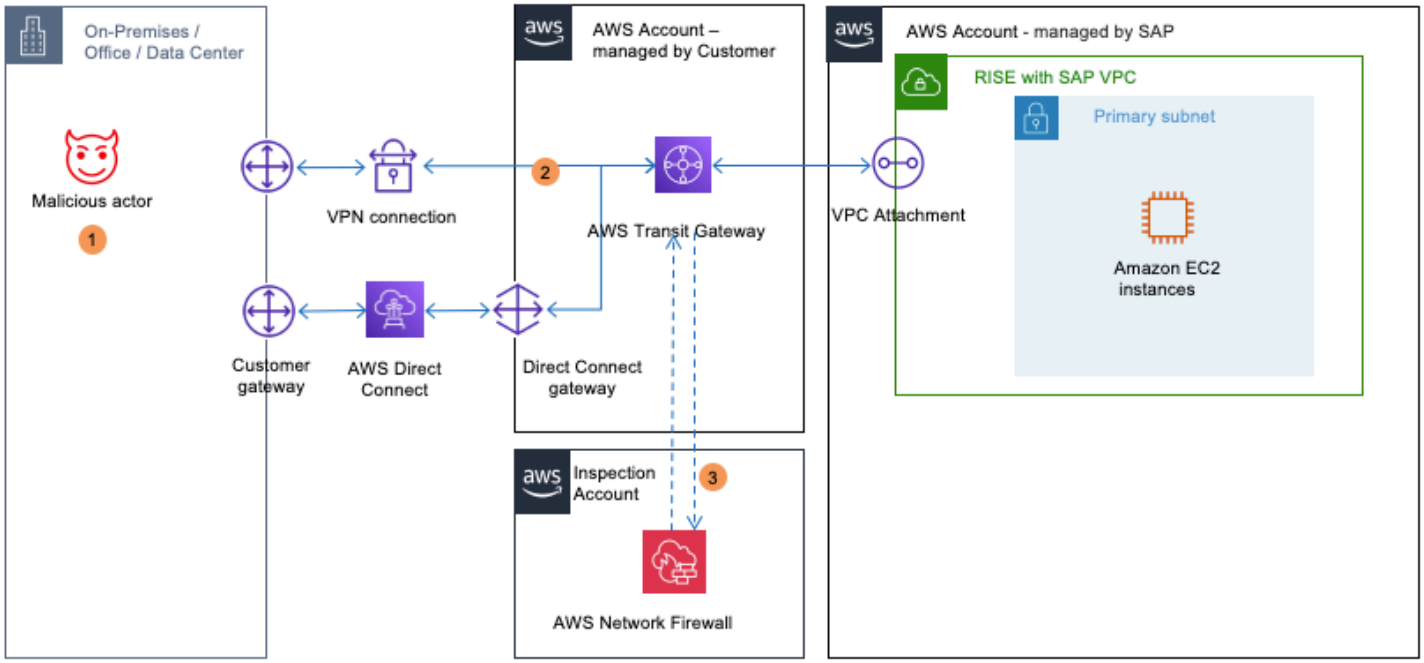
Network Fire AWS wall 的主要功能包括：

- 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。此功能可检测网络连接的完整上下文（包括源、目标、端口和协议），以检测并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。除了预定义的威胁特征外，客户还可创建并部署自定义防火墙规则，以符合 RISE 环境中 SAP 系统相关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。
- 可扩展性与高可用性。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 的示例架构，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获取对 RISE 上的 SAP 系统的访问权限。
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

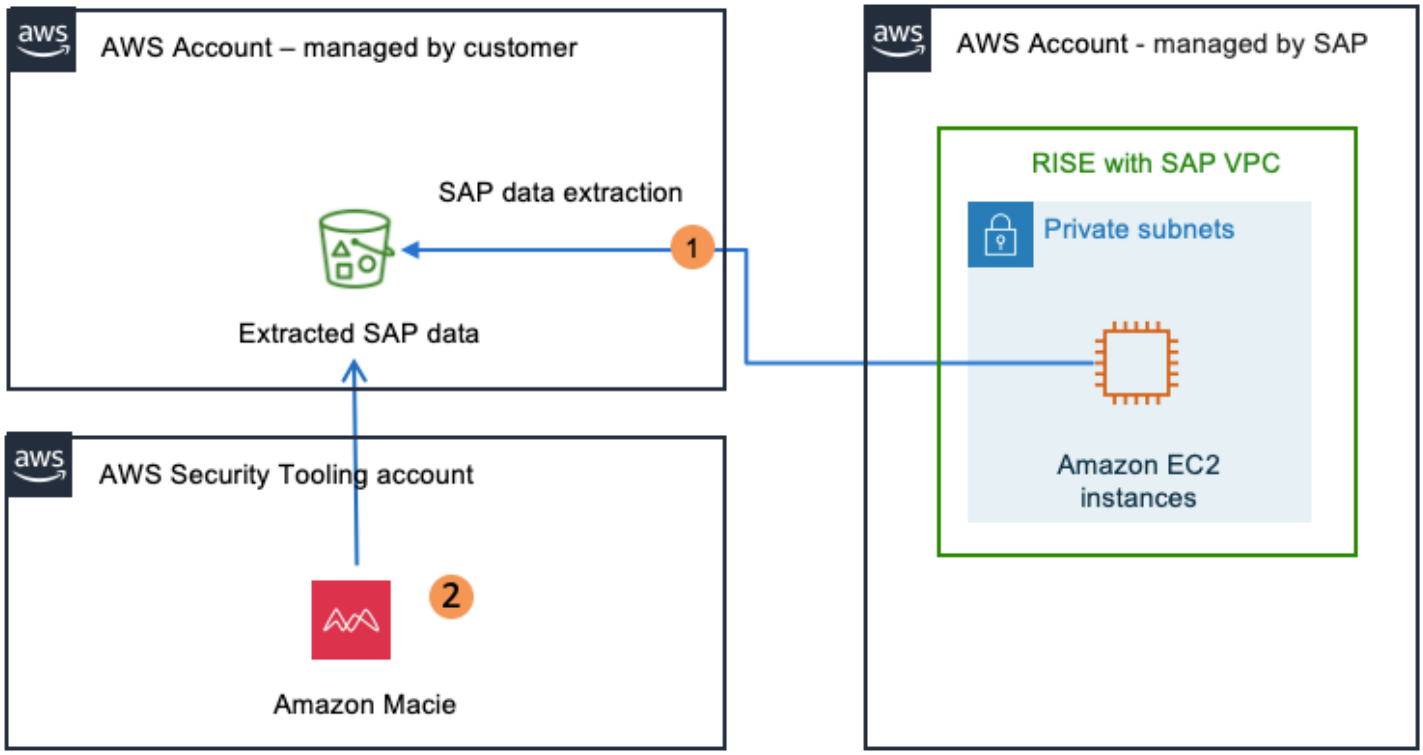
Amazon Macie 是一项数据安全服务，可持续监控潜在数据风险及未经授权的访问尝试，并在发现此类情况时向客户发送提醒，从而帮助客户发现、分类和保护存储在 Amazon S3 存储桶中的敏感数据。

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；
- 一些行业和法规（例如 GDPR、HIPAA 或 PCI-DSS）可能会要求长期存储和保留敏感数据。将此类敏感数据导出到客户自主管理型 S3 有助于满足这些合规要求，因为 S3 具备强大的安全性与持久性。
- 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。
- 客户还可从其 RISE 环境中获取安全事件日志，并将其摄入自有 S3 存储桶或 SIEM 系统。

以下是 Amazon Macie 对存储有从 RISE 提取的 SAP 数据的 S3 存储桶进行持续扫描的示例架构



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 持续分析存储桶以检测个人可识别信息。

有关配置 Amazon Macie 的说明，请参阅什么是 Macie？。

亚马逊 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。

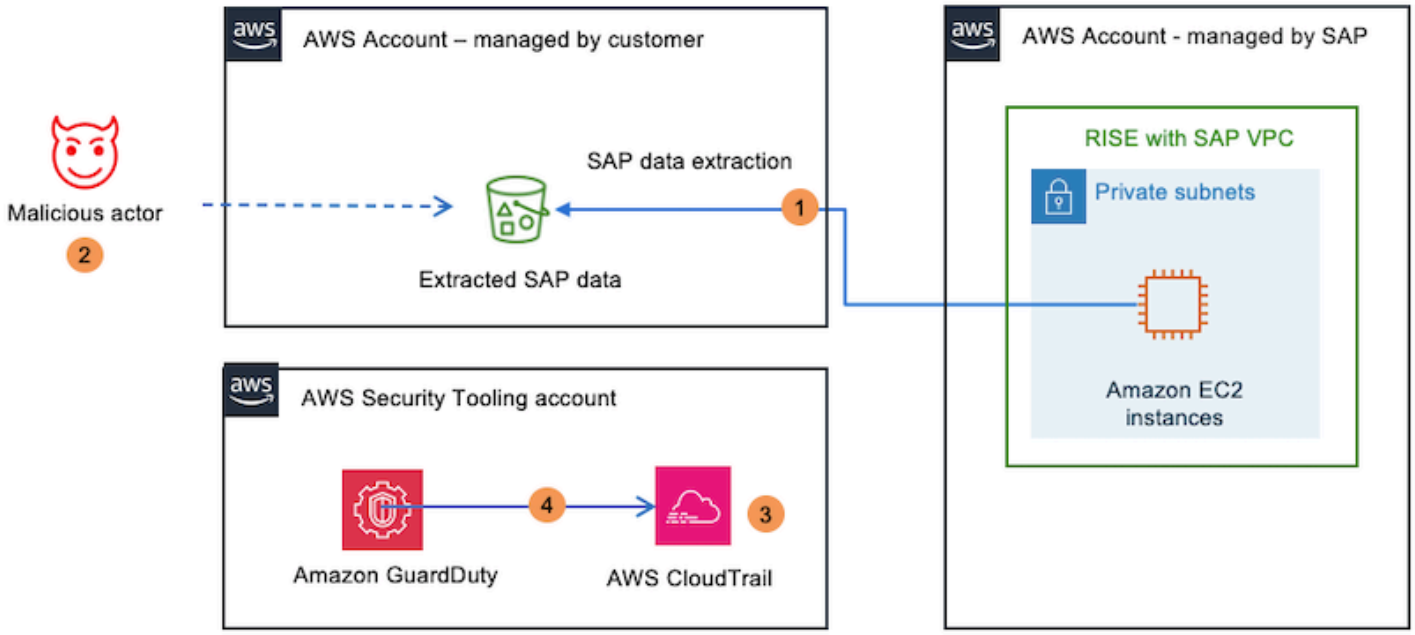
亚马逊 GuardDuty 监控以下内容：

- 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 做以下事情：

- 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，这些服务可触发自动化修复操作，例如隔离受影响的资源或向安全团队发送通知。

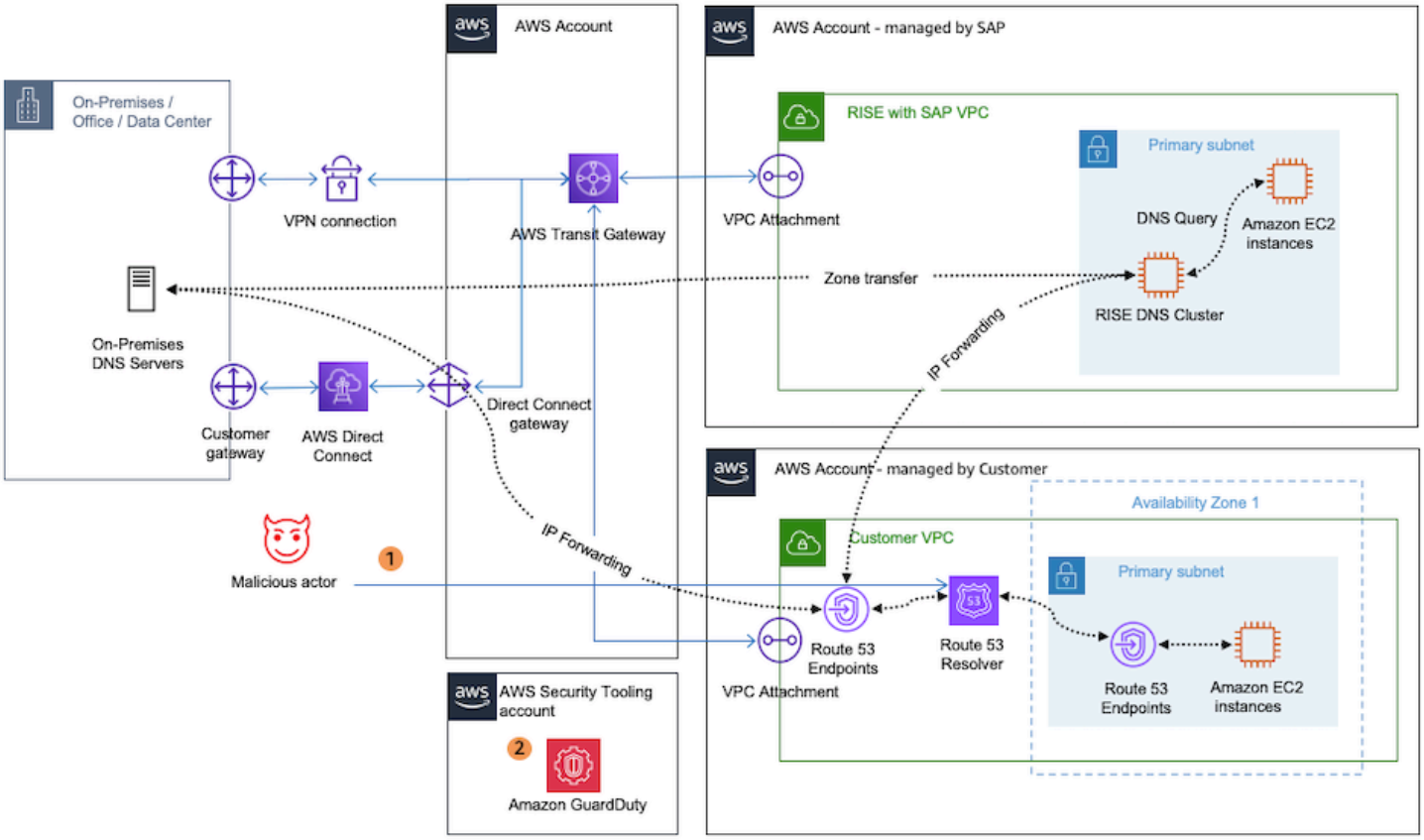
以下是在 SAP 部署状态下 GuardDuty 监控 RISE CloudTrail 跟踪的示例架构 AWS



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。

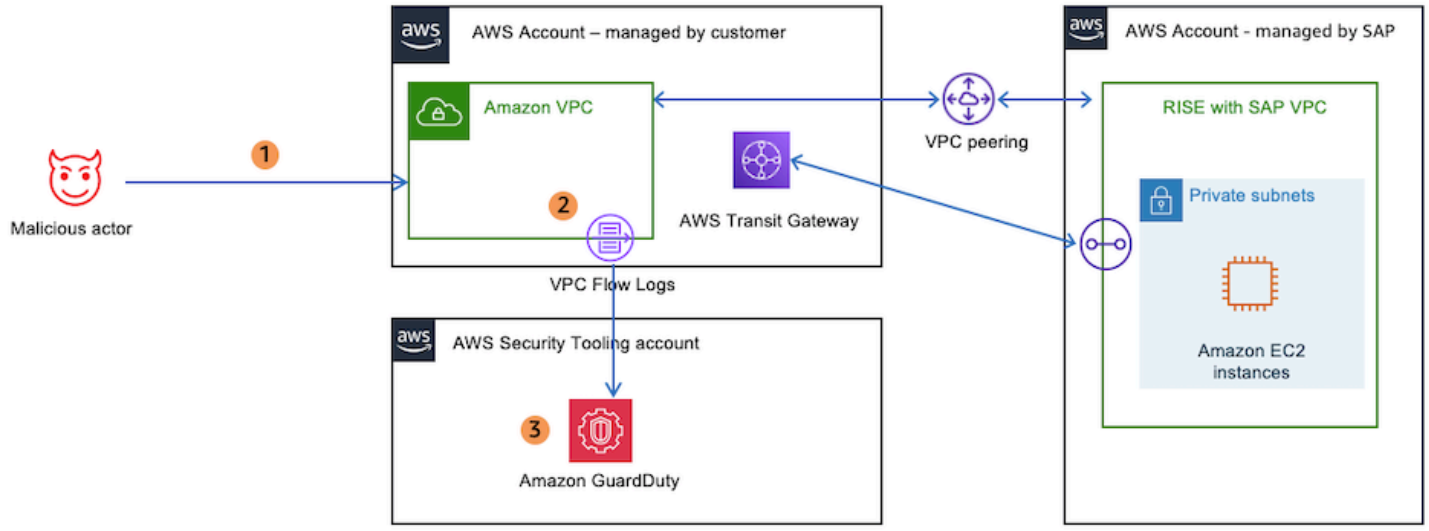
以下是在 SAP 部署开 GuardDuty 启的情况下监控 RISE 的 DNS 日志的示例架构 AWS



在上图中

1. 恶意行为者引入恶意 DNS，将用户重定向到伪造的 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. 恶意攻击者试图从与 RISE VPC 建立对等连接的客户自主管理型 VPC 访问 SAP 系统，或扫描端口。
2. 来自恶意攻击者 IP 的连接尝试被记录在 VPC 流日志中。
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。

Security Hub、Detective、Audit Manager 和 EventBridge

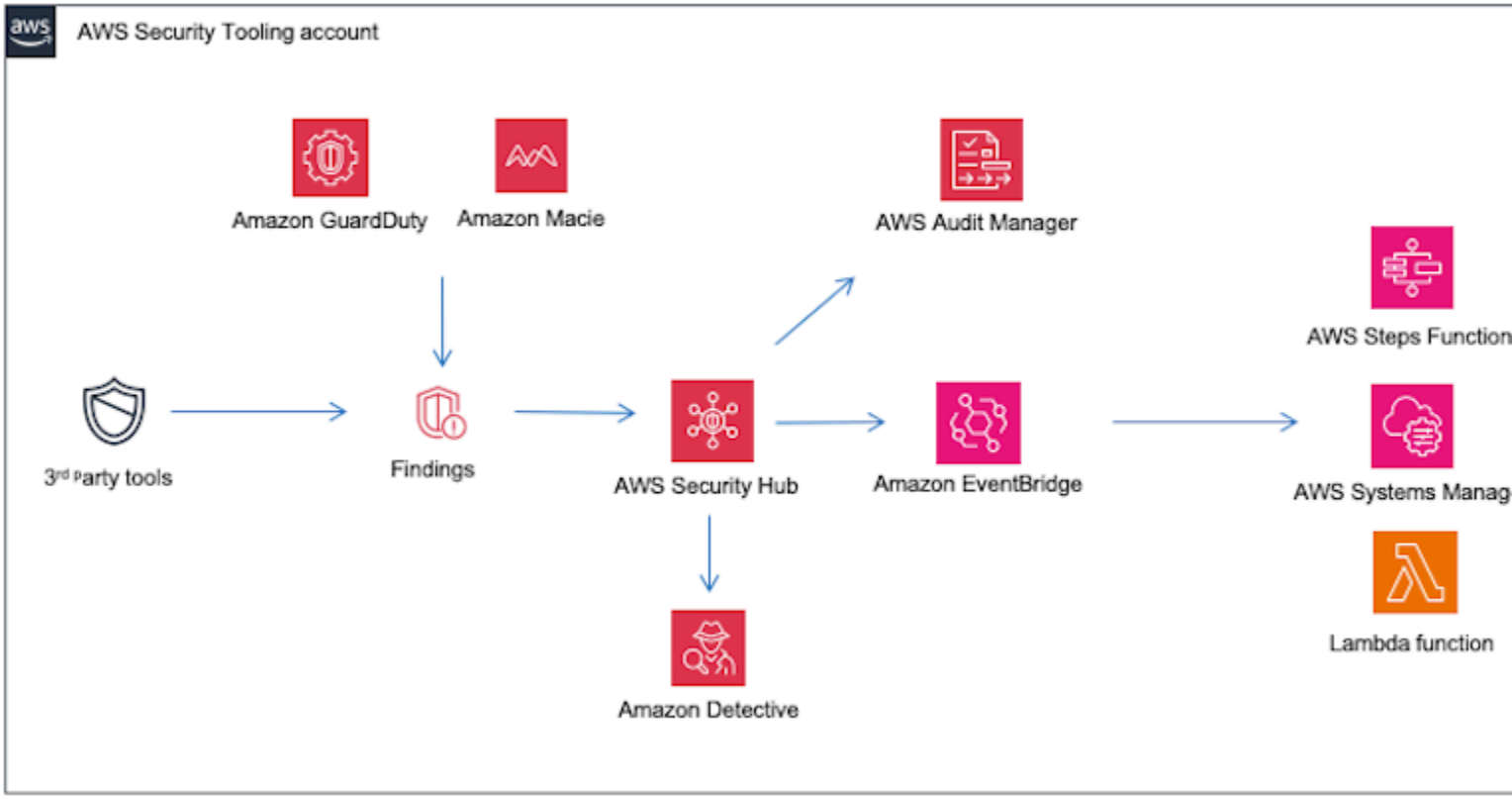
在 Amazon Macie 的 GuardDuty 实施基础上，Sec AWS urity Hub 充当中心枢纽，整合安全调查结果 AWS 安全服务并确定其优先级。 AWS Security Hub 提供了围绕 SAP 部署的 RISE 服务的安全态势的统一视图，从而可以更快地识别和解决任何安全问题。

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。此服务有助于快速确定问题的根本原因，以便能采取适当的措施来减小影响。

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。该服务可用于快速高效地处理安全事件，并最大限度地减少这些事件对 RISE with SAP 部署产生的潜在影响。

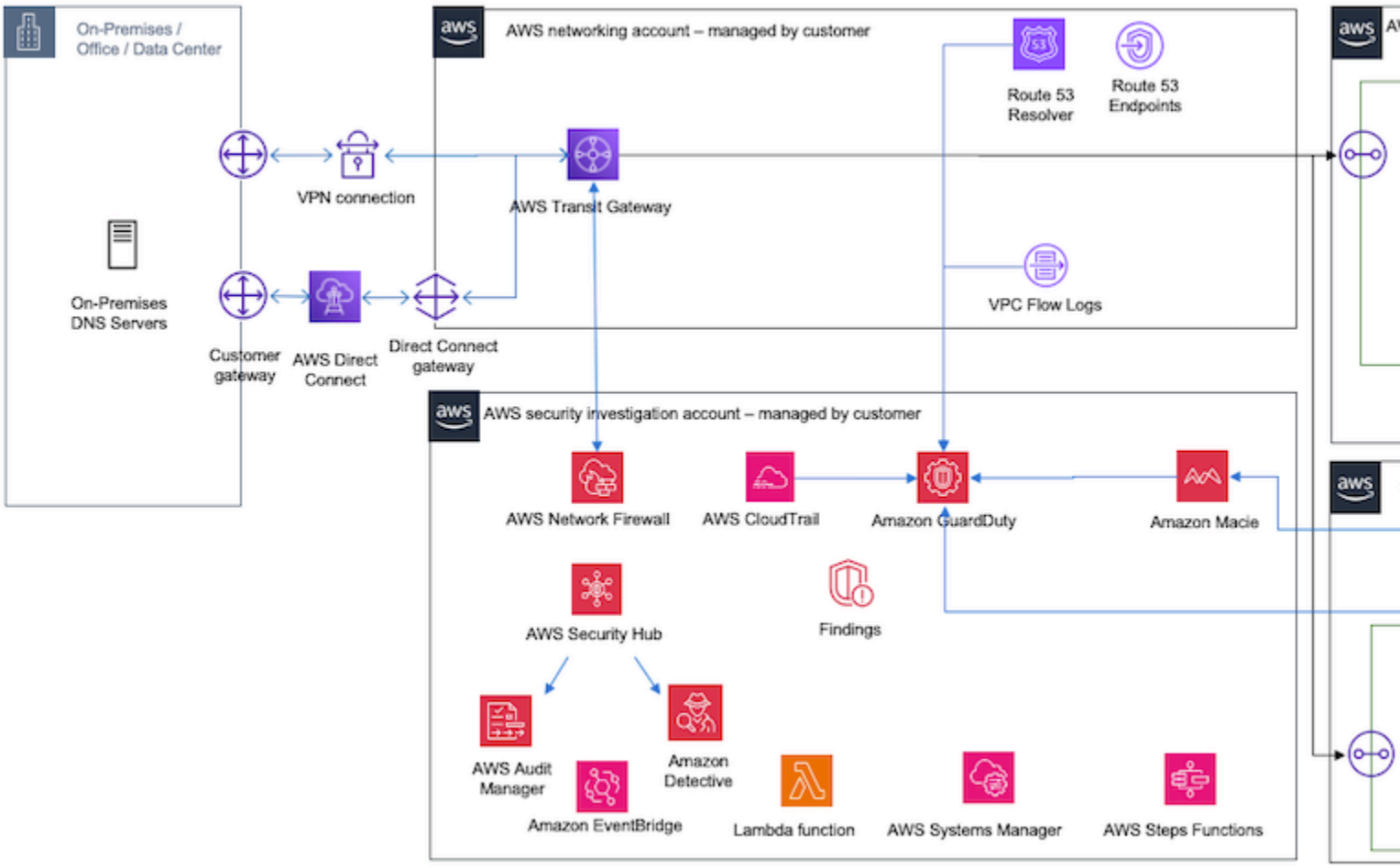
以下是 Sec AWS urity Hub、Amazon Detective、Audit AWS Manager 和亚马逊 EventBridge 与 RISE 与 SAP 配对的架构示例



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 数据托管人 KMS 与 AWS KMS 集成

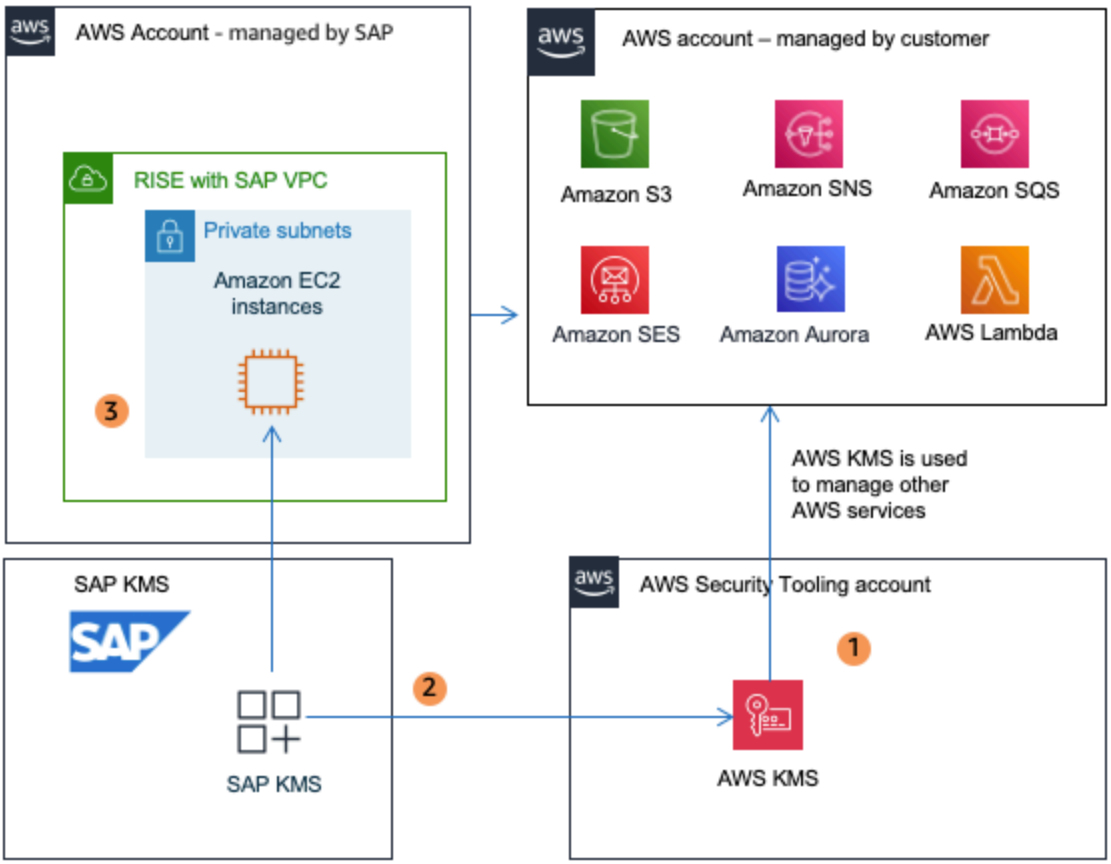
利用 SAP Data Custodian Key Management Service，客户可以管理存储在 SAP 服务中的数据的加密密钥。请注意，SAP 数据托管人密钥管理服务与 AWS 密钥管理服务 (KMS) 不同。

在 HYOK（Hold Your Own Key）场景中使用 AWS KMS 作为密钥库，SAP Data Custodian 密钥管理服务提供了一种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，通过 AWS 强大的加密和访问控制机制实现无缝集成、简化的密钥生命周期管理并增强安全性。

通过此集成，客户可管理和控制用于保护敏感数据的加密密钥，确保实现更高的安全性与合规性。在 HYOK（持有自己的密钥）场景中，SAP 数据托管人 AWS 密钥管理服务可以使用以下支持的密钥与 KMS 接口：

区域图	AWS KMS（HYOK 场景）	支持的密钥类型和密钥大小
AES（256）、RSA（3072、4096）	密钥管理	密钥已创建并存储在 AWS KMS 密钥库中

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

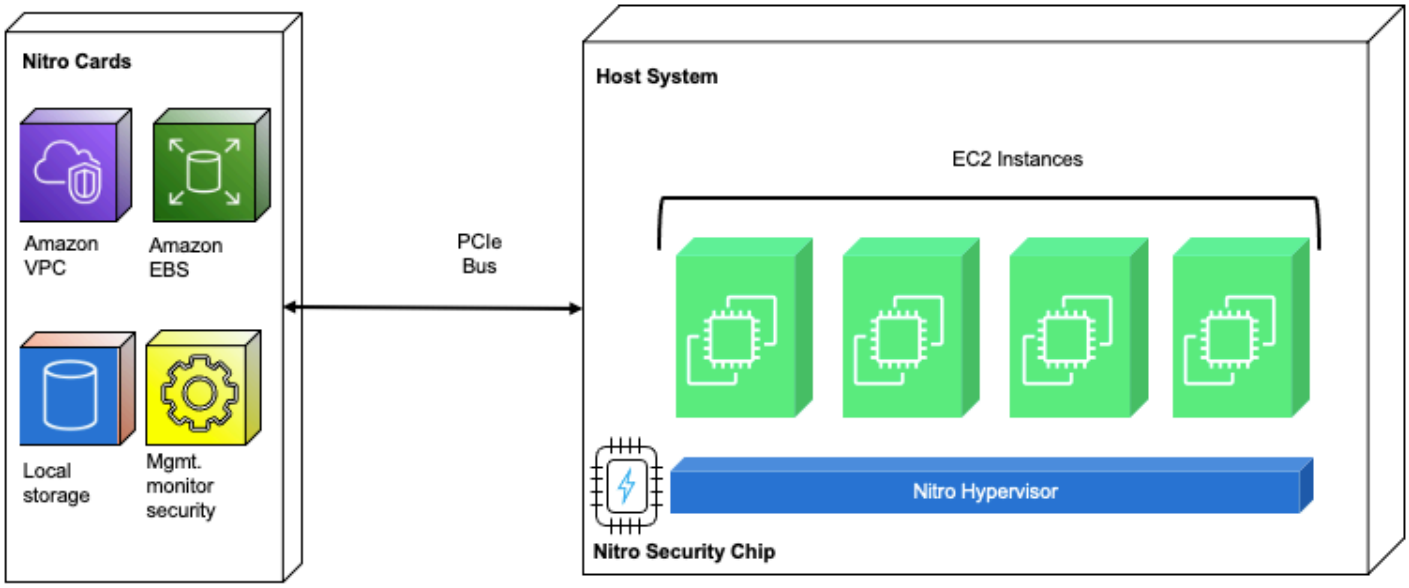
AWS Nitro 如何通过 SAP 帮助保护 RISE？

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。

传统虚拟化架构包括“虚拟机监控程序”[又称“虚拟机监视器（VMM）”] 以及在 Xen 项目中通常称为“Dom0”或在 Hyper-V 中被称为“父分区”的组件。有关传统虚拟化架构的更多详细信息，请参阅此处。

在 Nitro System 虚拟化架构中，管理域或控制域组件（具有对硬件和设备驱动程序的特权访问权限）被拆分到独立的专用服务处理器单元（SoC - 片上系统）中，这些单元被称为 Nitro 卡。尽管仍保留“虚拟机监控程序”层，但该层设计已极度精简，仅包含完成其任务所必需的服务与功能。此外，还引入了“Nitro 安全芯片”，以便增强安全性，并确保不会产生性能开销。

以下是 Nitro 高级架构



生成的 Nitro 系统已分为以下组件：

Nitro 卡

Nitro 控制器 - 它是物理服务器与 EC2、Amazon EBS 和 Amazon VPC 的控制面板之间唯一的对外管理接口，以被动式 API 端点形式实现，其中每项操作均会被记录，所有 API 调用尝试均通过精细访问控制模型进行加密的身份验证与授权。Nitro 控制器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）。系统固件存储在直接连接至 Nitro 控制器的加密 SSD 上，该 SSD 的加密密钥设计为通过可信平台模块（TPM）与 SoC 的安全启动功能协同保护。专为特定功能设计的 Nitro 卡：

联网 - 适用于 VPC 的新一代 Nitro 卡可以透明方式对发往其他 EC2 实例的所有 VPC 流量进行加密，这些实例运行于的主机也配备了支持加密功能的 Nitro 卡。它使用关联数据的身份验证加密（AEAD）算法，采用 256 位加密。在 RISE with SAP 中，根据客户的要求，选择不同系列的计算实例。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。有关此功能是否适用于您的 RISE with SAP 实例，请参阅此处。

EBS（SSD）存储 - 用于 EBS 的 Nitro 卡可对远程 EBS 卷进行加密，而不会对其性能产生任何实际影响。

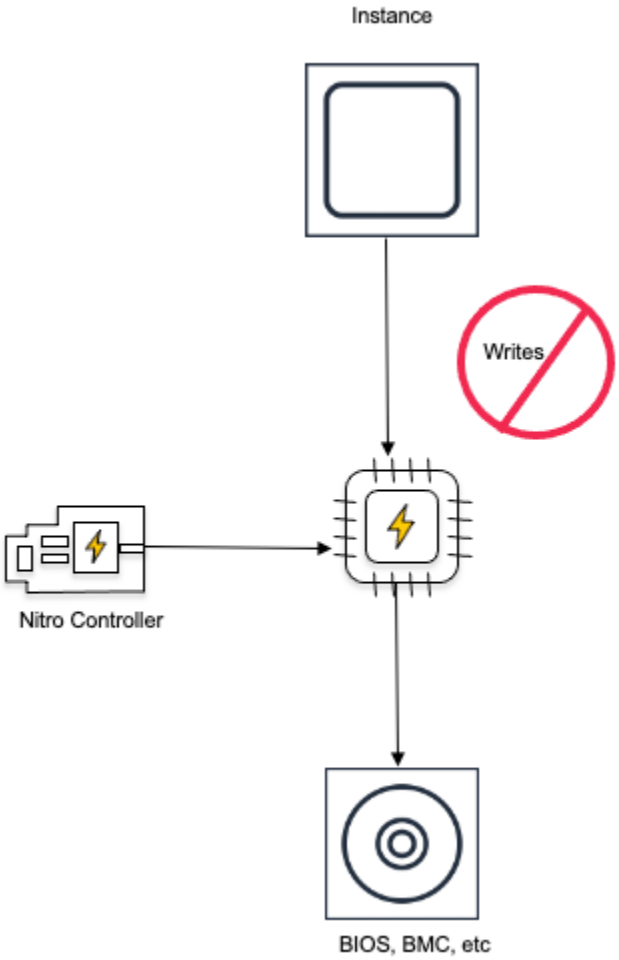
本地实例存储（临时性）- 与用于 EBS 的 Nitro 卡类似，用于实例存储的 Nitro 卡可对本地实例存储进行加密。并非所有 EC2 实例都拥有本地实例存储，这取决于为 RISE with SAP 工作负载选择的实例类型。有关详细信息，请参阅此处。

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 卡的受保护内存中。

Nitro 安全芯片

Nitro 控制器与其他 Nitro 卡构成第一个域，而运行 SAP 工作负载的系统主板构成第二个域。Nitro 控制器及其安全启动流程为 Nitro 系统各组件之间提供硬件信任根，Nitro 安全芯片用于将信任和控制权延伸至系统主板。作为这两个域之间的信任桥梁，Nitro 安全芯片将 Nitro 控制器的控制权扩展至系统主板，使其成为系统的从属组件，从而延伸 Nitro 控制器的信任链以覆盖整个系统主板。为了维护信任根，硬件层面将阻断所有对非易失性存储的写入访问。

以下是 Nitro 阻断对非易失性存储的写入访问的场景



Nitro 虚拟机监控器

与传统虚拟机监控程序不同，Nitro 虚拟机监控器并非通用型系统，它既没有 Shell，也没有任何类型的交互式访问模式。Nitro 虚拟机监控器通过排除以下关键组件来强化其安全态势：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 虚拟机监控器的主要功能仅限于：

1. 接收来自 Nitro 控制器的虚拟机管理命令（例如启动、停止等）
2. 利用服务器处理器的硬件虚拟化特性，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

与传统虚拟机监控程序相比，Nitro 虚拟机监控器的极简架构为其带来了显著的安全优势。

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 EC2 实例的加密 EBS 卷上的内容。 AWS 对 AWS Nitro System EC2 实例 APIs 的访问始终会被记录，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。有关更多信息，请参阅此处。
- 租赁保护和侧信道攻击防护 - Nitro 虚拟机监控器在 Nitro 控制器的指令下，为实例分配一整套物理内核和内存。这些硬件资源会“固定”到该特定实例。CPU 内核不会用于运行其他客户工作负载，实例的内存页也不会以任何形式在不同实例间共享。不共享 CPU 内核意味着，实例之间绝不会共享特定于 CPU 内核的资源（包括 1 级或 2 级缓存），从而能够有力地缓解侧信道攻击。有关更多信息，请参阅此处。
- 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 卡固件和虚拟机监控程序均设计为支持实时更新（客户实例的停机时间为零）。这使得无需围绕更新进行精细的权衡，提升了安全态势。有关更多信息，请参阅此处。
- 使用硬件卸载引擎与集成在 SoC 中的安全密钥存储对静态数据和传输中的数据进行数据加密。

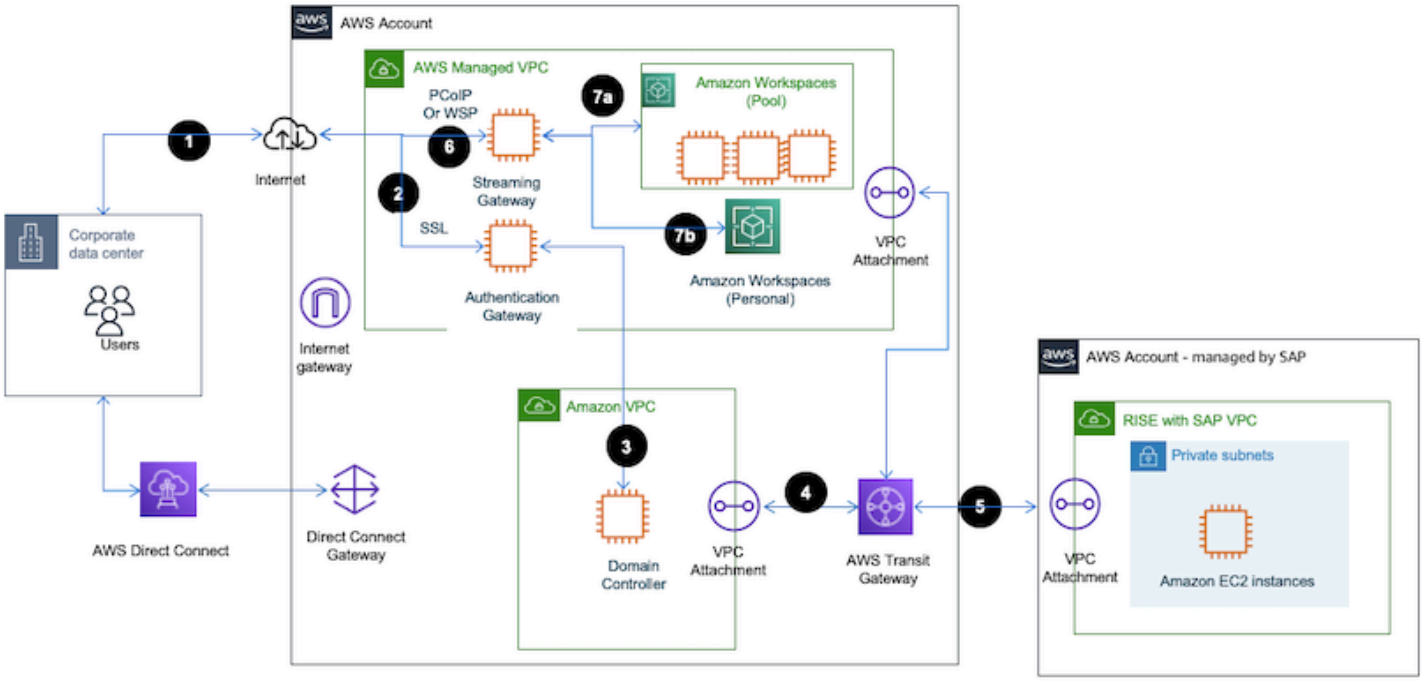
Amazon WorkSpaces 作为远程访问解决方案

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 终端用户软件（例如 SAPGUI）的集中管理的托管平台，能连接到 RISE with SAP 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。当终端用户登录时，身份验证网关会根据 Directory Services 对用户进行验证；在用户通过验证后，该网关会为用户建立安全会话，使其能够访问自己的虚拟桌面。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。此架构部分在端口 443 上将安全套接字层（SSL）与 TCP 协议结合使用。
3. 连接通过另一个 VPC 附件路由到单独的 Amazon VPC 中的域控制器。域控制器负责管理用户的权限和访问控制策略。它可确保用户拥有与其角色及组成员资格对应的资源访问权限。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。流式传输网关通过互联网将桌面流安全地传输到用户设备。此时，用户设备可通过 SAP 终端用户软件（例如 SAPGUI）访问托管在 RISE 环境中的 SAP 应用程序（例如 SAP S/4）。
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。当某个用户登录时，该用户可能并不总是连接到同一台设备，并且已安装应用程序或用户配置等更改通常不会在各个会话之间保留。

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，请按照入门指南进行操作 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，选择“Value”类型可节省成本。有关更多详细信息，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。以下是该方案的核心优势：

1. 增强的安全性与可控的访问权限

   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。这有助于防止对关键系统进行未经授权的直接访问。

   不直接接触互联网：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 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。这有助于进行安全审计并跟踪对 SAP 系统的访问。

   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 这将最大限度地降低未经授权的访问风险，并满足合规性要求。

3. 提升了运营效率：

   按需扩展性： WorkSpaces 可以快速配置并按需扩展，因此无需冗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。这对于为 SAP 环境提供支持的分布式团队或远程员工特别有用。

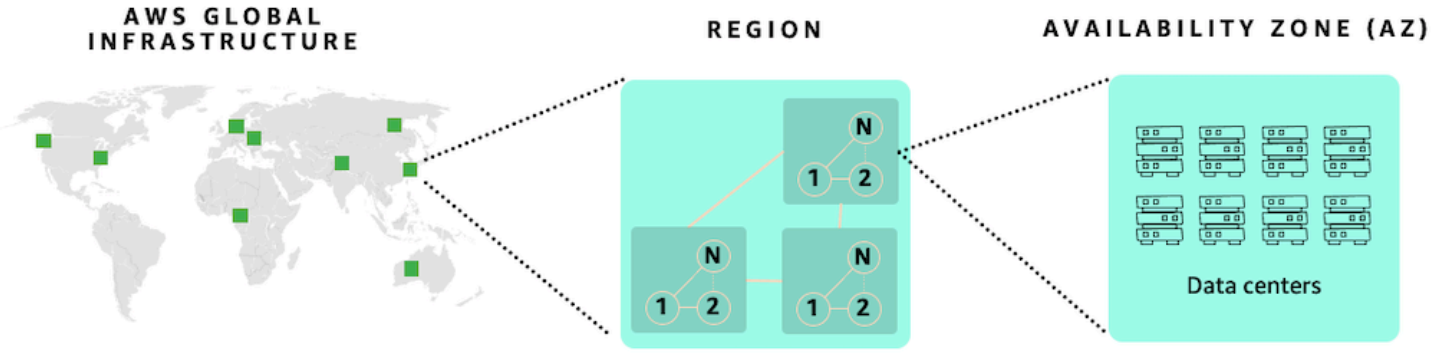
弹性和可用性： WorkSpaces 可以与 AWS 备份解决方案集成并分布在多个 AWS 可用区 (AZs)，从而确保冗余和高可用性。

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。各个区域之间相互隔离，从而实现了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。

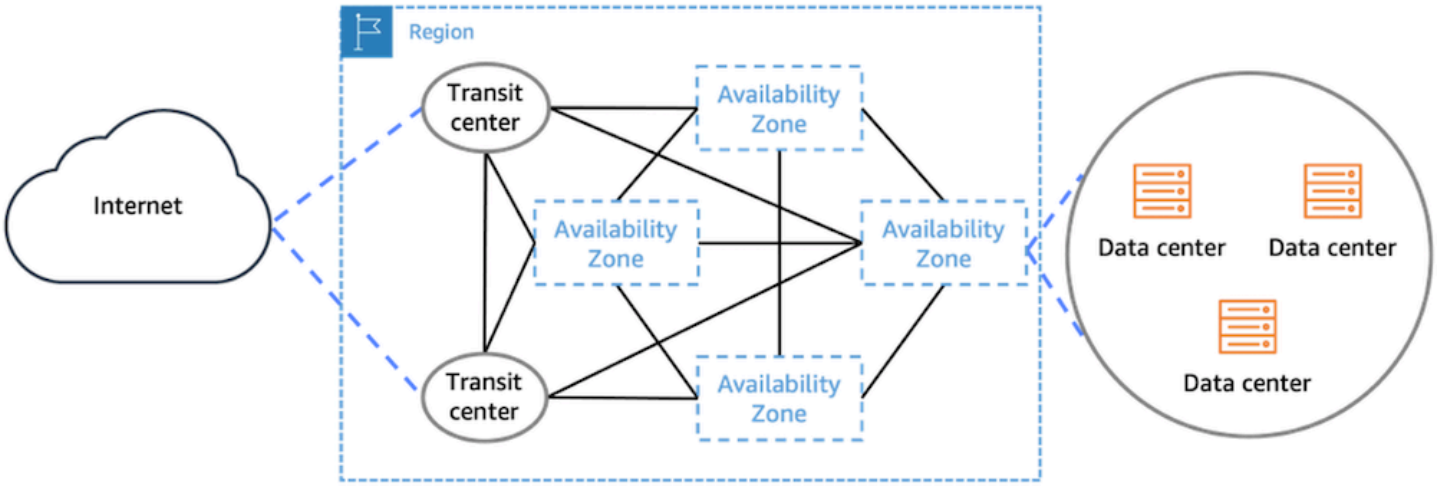


相比单个数据中心，通过可用区，您运行的生产应用程序和数据库可以获得更高的可用性。通过将应用程序分布在多个可用区中，您在面对大多数故障模式（包括自然灾害或系统故障）时能够保持韧性。

每个可用区可包含多个数据中心。在完全扩展的情况下，单个可用区可容纳数十万台服务器。它们是 AWS 全球基础设施的完全隔离的分区。各个可用区之间在物理上是相互隔离的，并拥有自己的电力和

联网资源。可用区之间有距离间隔，不过都在 100 公里以内（彼此相距 60 英里）。此距离可使可用区免受洪水、火灾、强风暴、地震等最常见的数据中心灾害影响。

一个区域中的所有可用区都采用完全冗余的专用城域光纤，实现高带宽和低延迟的网络互联。这确保了可用区间的高吞吐量、低延迟联网。网络性能足以实现同步复制。



可用区支持您以高可用方式运行应用程序，实现可用区之间的同步数据复制与自动失效转移。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。

恢复能力与成本注意事项

SAP 为 RISE 提供了多种选项，以满足不同的恢复能力需求。通过 SAP 提供的选项包，可针对 RISE 调整以下核心需求：

- 服务水平协议（SLA）- 描述解决方案的目标可用性。
- 恢复时间目标（RTO）- 描述灾难事件发生后，恢复工作应完成的目标时长。
- 恢复点目标（RPO）- 描述灾难事件恢复过程中，可能发生的数据丢失的目标级别。

有关更多详细信息，请参阅 SAP 在 RISE 协议中提供的相关定义，了解违约情况下的具体定义、条款、影响及处罚。

中断对组织造成的影响以及数据丢失，可能会导致生产率降低、收入损失，并损害声誉。权衡成本与恢复能力之间的关系，有助于评测组织面临的风险。

恢复能力与性能注意事项

当您在 RISE 中选择短距离灾难恢复选项时，SAP 应用服务器和数据库服务器将跨多个可用区进行部署。此架构支持针对您的 SAP 工作负载的高可用设计。

在主动-主动配置下，在多个可用区中使用应用程序服务器时，可提升恢复能力。同时，这也会增加从应用程序服务器到数据库服务器的跨可用区延迟。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。下一部分将对此进行详细探讨。

- 根据 SAP Note 1100926，SAP 应用程序服务器与数据库服务器之间的网络延迟应低于 0.7 毫秒
- 使用同步数据复制（实现零数据丢失所需的）的 HANA 系统复制的网络延迟应 less than 1 millisecond

您可以使用 AWS Network Manager - 基础设施性能工具自动测量可用区间、可用区内部以及区域间的网络延迟。您也可以根据 SAP Note 2986631，使用 SAP 的 NIPING 工具进行测量。

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。

跨可用区流量可能会增加执行某些需频繁调用数据库的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 组将此流量保持在同一个可用区内。这可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。

您可以参阅 AWS re:Post 文章“SAP 的可用区间延迟”，通过 C-State parameters 实现进一步的优化，从而降低网络延迟。

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，如果您发现同一可用区内的延迟对性能产生了影响，可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。

总的来说，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	自动化脚本（即 pacemaker）
活动	活动	手动调整 Logon Groups、RFC Server Groups 和 Batch Server Groups

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 Logon Groups、RFC Server Groups 和 Batch Server Groups 的自动化脚本
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化脚本

要实现 SAP 工作负载的高可靠性，我们建议完成以下任务：

1. 与 SAP 讨论 RISE 部署的可用性 SLA 要求。这将决定需跨多个可用区部署的组件（即数据库服务器和应用程序服务器），从而最大限度地提升 RISE 的可靠性与可用性。
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，您可以在应用程序服务器的主动-被动模式下运行 ABAPSetServerInactive （SAP Note 3075829）。
5. 可考虑将 RISE 之外的其他工作负载部署在同一可用区内，以实现更低的网络延迟和数据传输成本。

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。在发生罕见的本地故障或区域故障时，您的 SAP 工作负载将受到保护。

RISE with SAP S/4HANA Cloud 私有版提供以下两种选项。

- 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 区域为每个 AWS 区域提供了短距离灾难恢复选项。
- 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 Service Description: Disaster Recovery and Customer Invoked Failover。

可观测性

可观测性对于 SAP 客户来说非常重要，它能帮助客户通过分析日志、指标、跟踪数据等外部输出，了解其 SAP 场景及系统内部状态。与本地部署或本地 AWS 部署不同，使用 SAP 运行 RISE 的客户无法直接访问、管理或监控底层基础架构和依赖资源。尽管如此，客户仍需确保其系统按预期运行，并在 SAP 应用程序堆栈内主动识别和解决任何问题。

主题

- 责任共担
- 可观测性选项

责任共担

在 RISE with SAP 商业模式下，SAP 将云基础设施、S/4HANA 软件、工具及服务整合为单一订阅。尽管它是一套全面的托管服务，但可观测性仍是客户关注的核心问题，即客户仍希望能掌控可观测性，并深入了解其系统的内部状态。默认情况下，并非所有可观测性功能都包含在构造中。客户应根据最新的 RISE Roles and Responsibilities，明确了解可选的任务与排除的任务。SAP 负责管理基础设施、操作系统、数据库和应用程序层。但这会给客户带来潜在的可见性缺口，此缺口在客户本地运行 SAP 或在云中运行 SAP 时并不存在。如果缺乏合适的可观测性工具，组织将难以了解性能问题、识别瓶颈，也无法实现最佳业务运营。当问题同时涉及 SAP 系统与其他企业系统时，可见性缺失问题会变得尤为突出。

其中一个例子就是数据量管理，它需要客户主动监督。随着数据量的增长，性能会下降，同时成本会增加。客户需要借助工具来监控数据增长、使用模式和归档需求，以确保系统正常运行并控制开支。了解数据使用模式至关重要，因为它们会直接影响运维成本。对整个环境进行系统可用性和性能监控同样重要。在 SAP 监控核心系统的同时，客户需要了解 end-to-end性能，包括响应时间、系统可用性和资源利用率。不过，客户负责监控所有自定义应用程序和外部接口。

可观测性选项

使用 SAP 实现 RISE 的可观察性需要采取战略方法，考虑来自 AWS SAP 的原生工具以及第三方解决方案。该指南重点介绍了三种可观测性选项，客户可以根据具体需求和解决方案限制进行选择。

主题

- 原生 AWS
- SAP Cloud ALM
- 合作伙伴解决方案

原生 AWS

使用 Amazon 监控 SAP CloudWatch

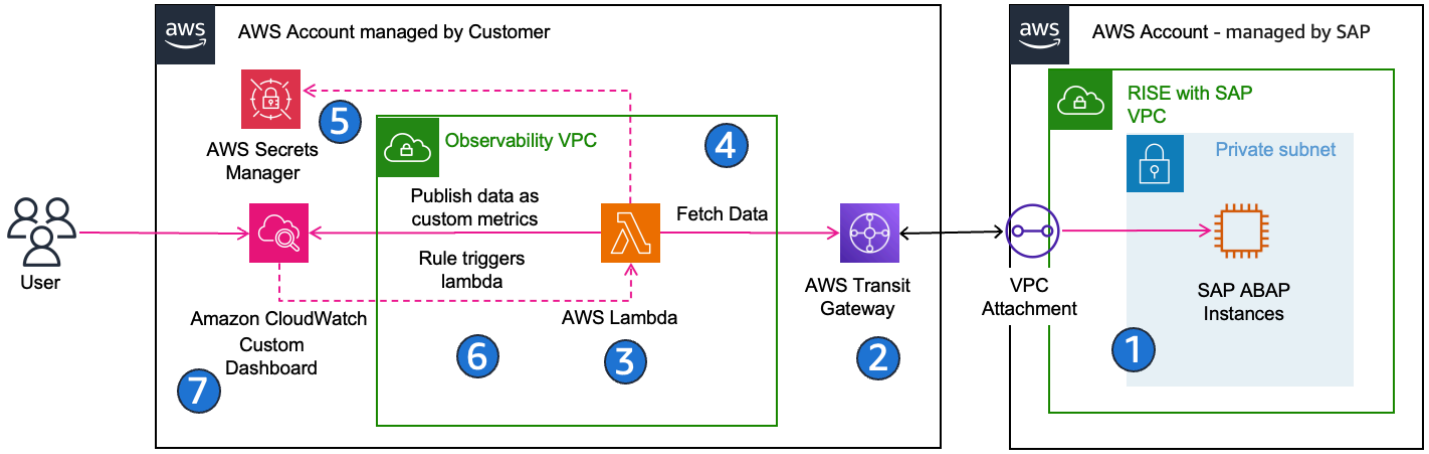
Amazon CloudWatch 是一项监控应用程序、响应性能变化、优化资源使用并提供运行状况见解的服务。Amazon CloudWatch for SAP 是一款原生 AWS 监控解决方案，可为上 AWS面运行的 SAP 工作负载提供全面的可观察性。该解决方案使组织能够使用 AWS其内置的监控功能监控、分析和优化其 SAP环境，提供与 AWS 服务的无缝集成，并为SAP系统提供自动见解。

为了提供可靠的 SAP 环境 end-to-end的可观察性 AWS，建议实施一种跨越应用程序指标、用户体验、操作工具和自动化的分层方法。在构建 SAP 的可观察性时 AWS，目标应该是主动检测整个 SAP 堆栈中的问题，从应用程序服务器和数据库到网络和用户界面，同时还要衡量 SAP Fiori 等应用程序中的真实用户体验。目标是缩短检测、诊断和修复问题所需的时间，自动执行例行监控任务以最大限度地减少人工操作，并确保在开展所有活动时，实现较高的安全性与成本效益，并遵守运营纪律。

由于您无法直接访问 CloudWatch RISE with SAP 账户，因此您可以使用下一节中描述的解决方案将指标导出到您的 AWS 账户，以便通过您的 CloudWatch 服务访问这些指标。

在 AWS 上监控基于 SAP ABAP 的系统

要在开启 RISE 的情况下为基于 SAP ABAP 的系统建立轻量级且可扩展的监控 AWS，您可以采用无服务器模式，即在您自己的 AWS 账户中配置的 L AWS ambda（使用 SAP Java Connector）从 SAP 交易（例如 ST03 SAD 和 /SDF/SMON）中提取工作负载和监控数据，并将其作为自定义指标发布在亚马逊中。 CloudWatch CloudWatch 规则安排数据收集，而凭证则在 S AWS ecrets Manager 中安全管理，Lambda 在与 SAP 托管 VPC 相连的客户托管 VPC 中运行。Lambda 函数通过 RFC 连接到在由 SAP 管理的 VPC 中运行的 SAP 系统。然后，您可以在其中构建仪表板和警报， CloudWatch 以可视化系统性能，主动检测异常并发出阈值警报，所有这些操作开销最小，成本也很低。此方法无需额外的基础设施或代理，可以跨多个 SAP 系统进行扩展，并为可观测性提供安全、经济高效的基准。



高层级实施步骤：

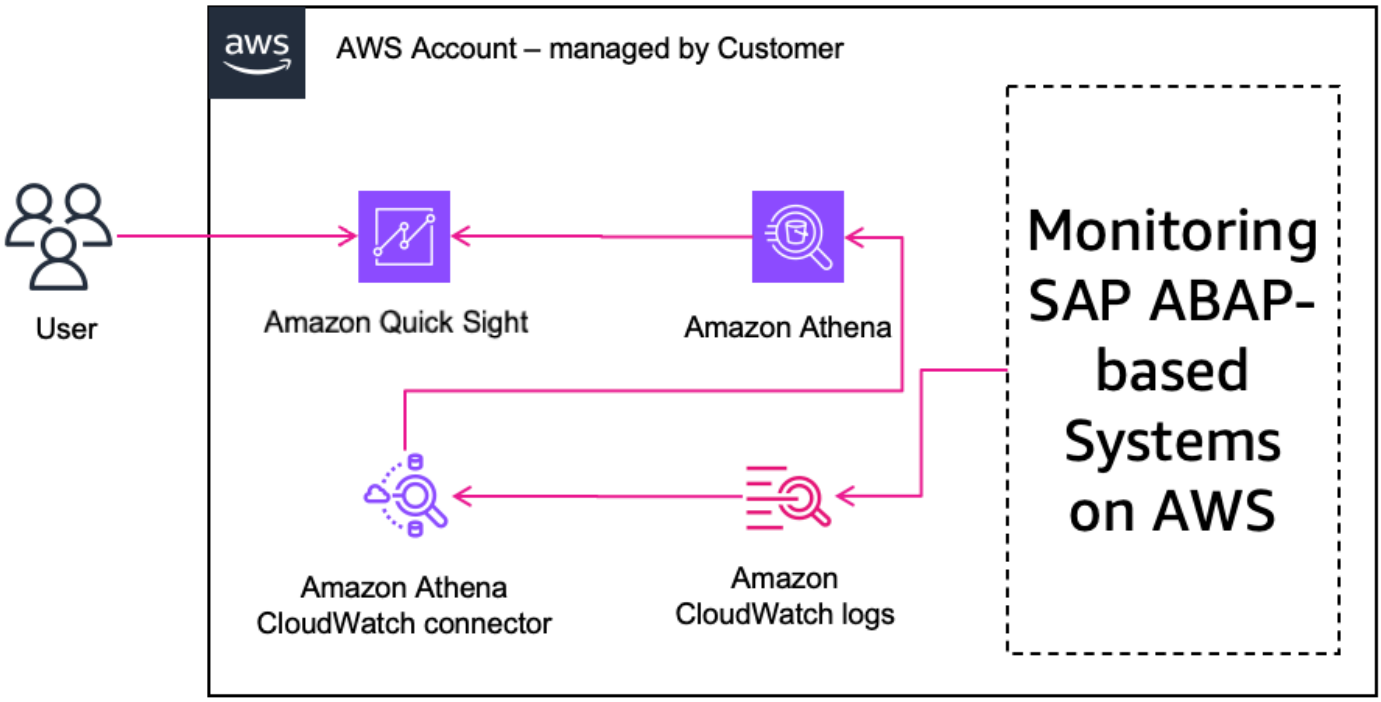
1. 创建专用的 SAP RFC 用户，并为其配置监控所需的权限。
2. 在您的 AWS 账户和RIS AWS E账户之间建立网络连接。
3. 使用 SAP Java 连接器 (JCo) 作为层，通过 AWS 无服务器应用程序存储库或模板在自己的 AWS 账户中部署 Lambda 函数。 CloudFormation
4. 将 Lambda 配置为在 VPC/subnet 具有对您的 SAP 系统的 RFC 访问权限的内部运行。
5. 在 S AWS ecrets Manager 中安全地存储 SAP 凭证。
6. 设置 CloudWatch 规则，按适当的时间间隔安排指标收集。
7. 使用自定义指标构建 CloudWatch 仪表板和警报，以可视化系统运行状况并触发警报。

您可以按照 SAP 监控：一种使用 Amazon CloudWatch 的无服务器方法获取详细步骤和实施指南。

通过采用此方法，您可以为 SAP ABAP 系统获得可扩展、安全且经济高效的监控能力，实现主动的问题检测与性能可视化。该基础使您可以随着时间的推移扩展可观察性，整合其他指标，并通过原生 AWS 服务将监控无缝集成到您的运营工作流程中。

利用 Quick Sight 可视化功能进行 SAP 监控

在 “监控基于 SAP ABAP 的系统” 的基础上 AWS，通过使用 Amazon Athena 将 Amazon Logs 与 Ama CloudWatch zon Quick Sight 集成，你可以更深入地了解你的 RISE with SAP 环境。这可让您获取原始运营日志数据，高效存储与查询这些数据，并构建非技术类利益相关者可使用的交互式控制面板和报告，同时使您能够在单个窗格中全面了解系统运行状况、用户行为及安全性。

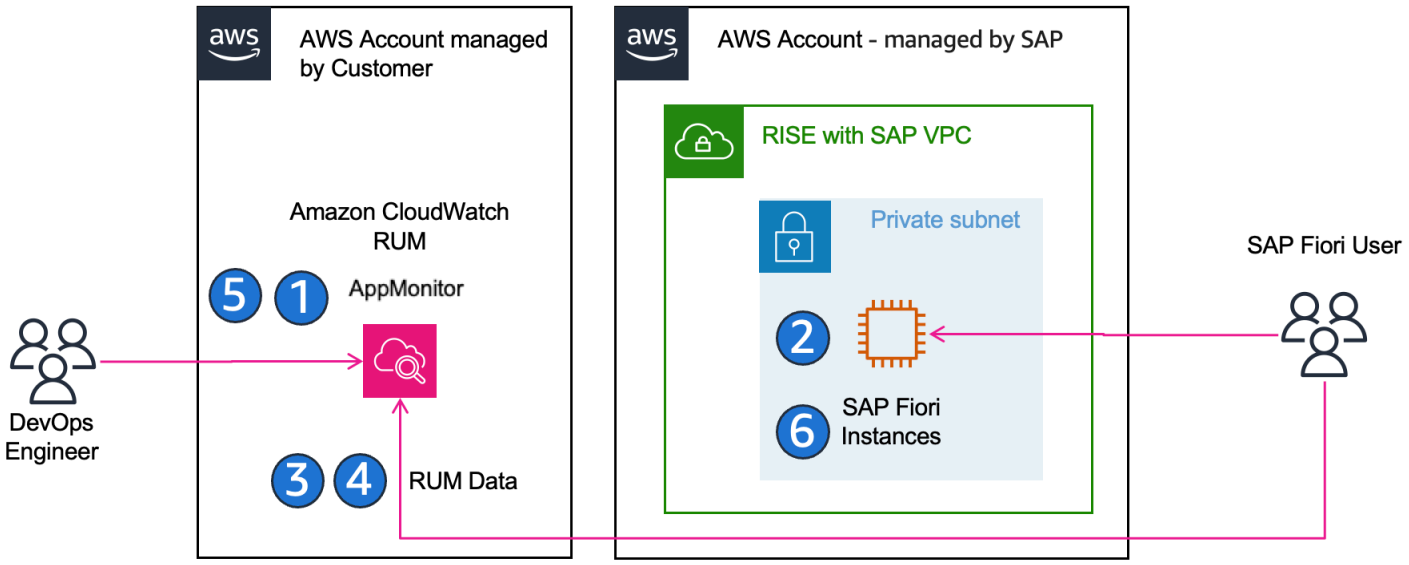


要实现此集成，您首先要通过部署一个 Lambda 函数来设置 CloudWatch Athena 日志连接器，该函数允许 Athena 查询您的日志。 CloudWatch 接下来是定义 Athena 视图，对时间戳、错误代码或自定义 SAP 日志条目等相关日志字段进行结构化处理与提取，为后续分析做好准备。视图定义完成后，通过授予必要的 IAM 权限并配置 S3 访问权限，将 Amazon Quick Sight 与 Athena 连接，随后即可导入或直接查询日志数据。最后，您可以在 Quick Sight 中构建交互式仪表板和可视化以监控趋势、错误率和操作 KPIs，还可以选择在 Quick Sight 中启用 Amazon Q，这样您的业务用户就可以在不编写 SQL 的情况下针对 SAP 日志数据提出自然语言问题。

使用自己的 AWS 账户将 SAP 指标从 RISE 环境设置到亚马逊 CloudWatch 后，您可以按照使用 Amazon Athena 将亚马逊 CloudWatch 日志与 Amazon Quick Sight 集成，了解详细步骤和实施指南。

在 AWS 上监控并优化 SAP Fiori 用户体验

您可以利用亚马逊 CloudWatch 真实用户监控 (RUM) 来监控和改善 SAP Fiori 应用程序的用户体验。这使您能够实时捕获实际用户与 SAP Fiori 启动板及应用程序的交互方式，并衡量性能、错误率和用户流失率。通过了解用户体验指标，您可以主动优化前端性能，确保实现流畅、响应迅速的 SAP Fiori 环境。



高层级实施步骤：

1. 在 AWS 控制台中创建 CloudWatch RUM 应用程序监视器。
2. 将生成的 JavaScript 代码片段作为 Fiori 插件部署到启动板中，其中包含相应的目录和角色分配。
3. 配置 RUM 以捕获关键指标：页面加载时间、Core Web Vitals（LCP、FID、CLS）和浏览器错误。
4. （可选）配置采样以平衡数据量与成本。
5. 在中创建仪表板和警报 CloudWatch ，以监控性能趋势和影响用户的问题。
6. 在必要时添加手动路由更改事件，以正确捕获单页应用程序导航。

您可以参阅在 AWS上监控和优化 SAP Fiori 用户体验，了解详细步骤与实施指导。

通过实施 CloudWatch RUM for SAP Fiori，您可以深入了解最终用户体验，从而使您的团队能够主动识别和解决前端性能瓶颈。此方法可确保提高用户满意度、持续改进 SAP Fiori 应用程序，并为 IT 团队与业务团队提供可操作的数据。

使用 AIOps 带有 CloudWatch 和应用程序信号 MCP 服务器增强 SAP 监控

您可以将 AWS MCP 服务器与 Amazon Q CLI 配合使用，实现智能的情境感知故障排除，从而利用 SAP 的可观察性增强您的 RISE。这些工具使您可以自动关联指标、跟踪、日志和服务运行状况，定义服务级别目标 (SLOs)，并使用自然语言提示与可观察性数据进行交互，从而帮助您更快地找到根本原因，更直观地诊断性能问题，并总体上提高修复 SAP 环境中问题的速度。此外，您可以监控关键网络组件，例如Direct Connect链路以及通过 AWS 着陆区部署的RISE with SAP环境 VPCs 中，确保连接可用，性能最佳，并且可以及时检测和缓解任何故障。

高层级实施步骤：

1. 使用 SAP 系统从 RISE 中提取完整的可观测性数据（指标、日志、跟踪）到 Amazon CloudWatch 并启用应用程序信号。
2. 定义与 SAP 性能目标SLOs（例如，对话响应时间、事务吞吐量、Fiori UI 延迟）一致的服务级别目标 ()。
3. 在您的环境中部署和配置 CloudWatch MCP 服务器和应用程序信号 MCP 服务器。
4. 设置具有最低权限访问权限的 IAM 角色和权限，这样 MCP 服务器就可以安全地 CloudWatch 与应用程序信号数据进行交互。
5. 安装 Amazon Q Developer CLI，将其配置为使用 MCP 服务器，然后将其映射到您的 AWS 个人资料和区域。
6. 验证 MCP 服务器是否已正确加载并能响应 Q CLI。
7. 开始在 Q CLI 中使用自然语言查询来排查问题、检测延迟峰值、验证 SLO 合规性，以及加速跨整个 SAP 堆栈的根本原因分析。

操作完成后，您可以使用 Q CLI 询问诸如 “我的 S/4HANA 系统中哪些后端操作最常失败？” 之类的 natural-language-style查询 ，“过去 24 小时内，我们 SLOs 的 SAP 服务是否存在任何漏洞？”，或者 “请在最近 7 天内从我的 cloudtrail 日志中查看我的 SAP 系统中的任何威胁线索”，让这些工具为您完成大部分关联和 log/pattern 检测。

您可以按照使用 CloudWatch MCP 服务器和 Amazon Q CLI 简化 SAP 操作来了解详细步骤和实施指南。

通过采用应用程序信号 MCP 服务器 CloudWatch 和 Q CLI，您可以让 SAP 监控不仅是被动的，而且更具预测性和对话性。这使您能够大幅缩短平均故障解决时间，由于无需手动爬取日志和控制面板数据，只需提出针对性的问题，即可获得与 SAP 环境相关的见解。在包含许多组件（应用程序服务器、数据库、网络、用户界面）的环境中，MCP 服务器可帮助您更快地关联跨层级故障（例如，数据库缓慢、应用程序服务器过载、网络延迟）。这种方法还可以帮助你（通过 SLOs）强制执行性能目标，更好地了解服务运行状况，以及更强大的事件修复工作流程，所有这些都有助于你以更高的效率和可靠性在 AWS 开启SAP的情况下运行RISE。

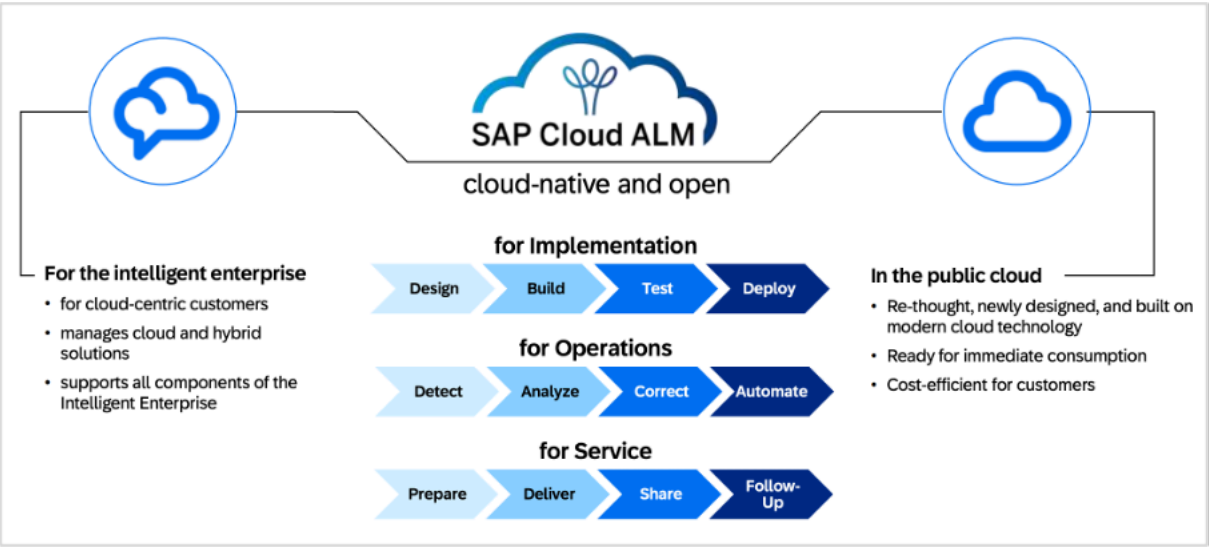
结论

通过结合亚马逊 CloudWatch、 CloudWatch RUM、Application Insights、MCP 服务器、Amazon Q CLI、Athena 和 Quick Sight，你可以在 SAP 环境开启的情况下为 RISE 创建完全集成的 end-to-end可观察性策略。 AWS此方案使您能够监控后端系统、SAP Fiori 用户体验和服务级别目标，同时关联整个 SAP 堆栈中的指标、日志和跟踪。

MCP 服务器和 Amazon Q CLI 共同提供了强大的能力，支持通过自然语言查询与可观测性数据进行交互、自动化常规运营任务、生成运行状况报告，并加速根本原因分析，这不仅减少了人工工作量，而且提升了运营效率。同时，该解决方案是完全可定制的，使您有机会设计仪表板、警报、数据收集和工作流程，以满足您的特定业务要求和合规性需求。总体而言，该策略提高了系统可靠性，提高了用户满意度，并使技术团队和业务利益相关者能够以安全、经济实惠和有弹性的方式主动优化和维护 SAP 工作负载。 AWS

SAP Cloud ALM

SAP Cloud 应用程序生命周期管理（ALM）是用于在云环境和混合环境中实现可观测性的主要工具。它采用云原生方法来监控 SAP 解决方案，强调标准化而非大量定制化。Cloud ALM 面向拥有活跃云服务的客户提供，可同时用于云端部署和本地部署的 SAP 解决方案，因此适用于混合环境。



SAP Cloud ALM 中的运行状况监控

云 ALM 的监控能力的核心是 Health Monitoring application，该应用程序会系统性地收集指标，以计算托管组件的整体运行状况。该解决方案提供了一个全面的仪表板，显示所有连接的服务和系统的当前状态，跟踪关键信息， KPIs 包括系统可用性、响应时间、内存和 CPU 利用率、数据库性能、磁盘空间使用情况、作业处理状态、队列积压、用户会话和安全事件。这种多维度的监控方式可助力组织全面掌握其 SAP 环境的状况，具备的功能涵盖系统可用性跟踪、性能监控、安全监测、证书过期提醒、基于阈值的通知，以及用于趋势分析的历史数据留存。有关 SAP Cloud ALM 运行状况监控的更多详细信息，请参阅 SAP 帮助文档。

SAP Cloud ALM 中的用户体验监控

云 ALM 通过用户体验监控增强其监控能力，此功能采用两种互补的实现方式。真实用户监控通过捕获用户与 SAP 应用程序的实际交互行为，提供关于页面加载时间、响应时间及错误率等性能指标的真实

见解。作为补充，合成用户监控通过预定义脚本定期模拟用户交互，即使在没有真实用户活动时也能测量性能。这种双重方法可确保从真实场景和受控测试双重视角，持续对应用程序性能进行可视化监测。有关 SAP Cloud ALM 用户体验监控的更多详细信息，请参阅 SAP 帮助文档。

运维自动化与视图控制面板

SAP Cloud ALM 提供运维自动化功能，可用于编排和自动化标准运维流程及问题解决流程。“运维视图”控制面板能够全面呈现系统运行状况，根据连接、异常、后台处理和性能等关键性能指标来计算系统运行状况分数。

SAP Cloud ALM 的使用成本

SAP Cloud ALM 包含在带 SAP Enterprise Support 的云订阅中。根据 SAP’s fair use policy，默认提供的资源通常足以满足标准使用案例的需求。组织可以在 SAP Cloud ALM 的“租户信息”应用程序中监控其使用指标，包括内存使用量和出站 API 使用量。要在不购买扩展功能的情况下降低内存使用量，组织可在 SAP Cloud ALM 中调整运维应用程序的清理设置。对于扩展使用场景或需要额外资源的组织，SAP 提供了 SAP Cloud ALM Tenant Extension。有关更多详细信息，请参阅 SAP 帮助文档。

结论

对于 SAP Cloud ERP 环境来说，Cloud ALM 是其订阅中自带的、极具价值的监控起点。随着环境复杂度提升和业务重要性增加，组织应持续评测云 ALM 的标准化监控方式是否足以满足自身不断变化的需求，或专业的合作伙伴监控解决方案是否能通过增强可观测性并提升运维效率，创造更多业务价值。

合作伙伴解决方案

虽然客户可以使用 AWS 服务构建 SAP 可观测性解决方案，也可以使用 SAP Cloud ALM，但选择合作伙伴解决方案有几个令人信服的理由。合作伙伴的可观测性解决方案提供预构建的集成，因此能加快实施速度。尽管 Cloud ALM 具有侧重于标准化的 out-of-the-box可观察性选项，但合作伙伴提供的产品通常可以实现广泛的定制和专业知识，而无需专门的工程团队。合作伙伴解决方案提供包含内置最佳实践、专业支持和高级功能（如 AI/ML 分析）的完整套餐，通常总拥有成本较低。这使组织能够专注于其核心业务，而不是构建和维护可观测性基础设施。

以下列出的合作伙伴解决方案并不详尽。我们建议您查看最新的 AWS Marketplace 列表，了解 SAP 可观测性解决方案，或者联系我们获取更多信息。

主题

- New Relic Monitoring for SAP
- SoftwareOne: PowerConnect 适用于 SAP 解决方案

- PowerConnect 在 Dynatrace 上使用 SAP
- Splunk Service Intelligence for SAP Solutions

New Relic Monitoring for SAP

适用于 SAP 的全新 Relic Monitoring 是一款全面的可观察性解决方案，可提供将 SAP 绩效与业务成果和非 SAP 系统联系起来的整体 end-to-end视图。借助此解决方案，组织能够通过单一管理平台监控其整个企业堆栈，通过 AI 驱动型见解和强大的可视化功能，提供对 SAP 环境的统一可见性。

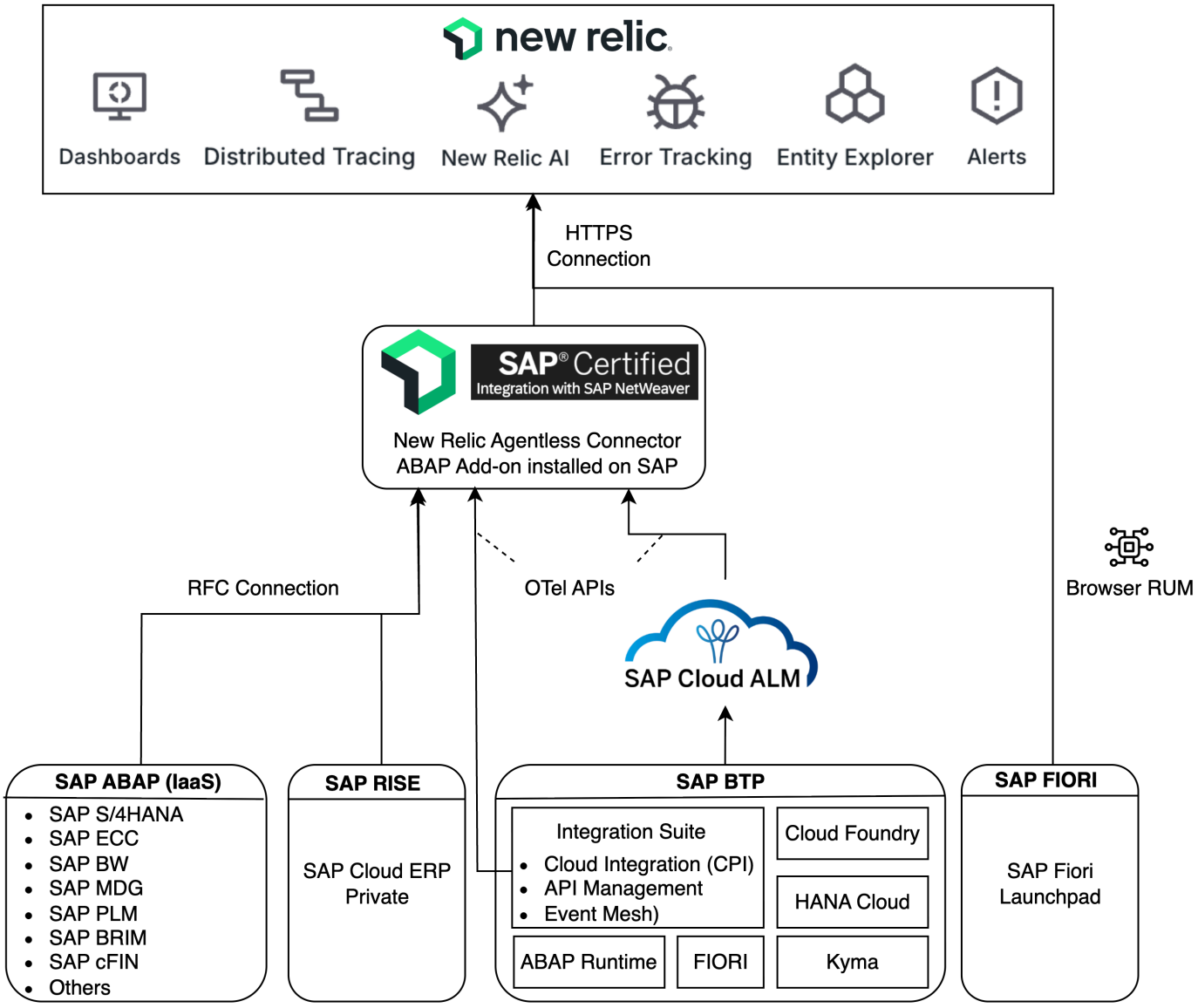
主要优势：

- 超过 175 个监控点、35 个仪表板和 17 个警报策略 out-of-the-box
- 采用无代理架构，已获得 SAP Cloud ERP 私有版认证
- 通过无代理架构与采用统一的“单一管理平台”视图的非 SAP 监控，最大限度地减小性能影响
- End-to-end 分布式跟踪，用于全面的交易流监控和带有关键流程性能指标的业务流程步骤监控

架构

此解决方案借助安装在单个中央监控系统上的原生且经 SAP 认证的 ABAP 加载项，采用真正的无代理架构。这种集中式连接器可从其他 SAP 系统拉取数据，无需在每个生产系统上安装代理。此解决方案提供针对六个关键领域的全面监控：

1. System Health：监控整体系统运行状况、 central/enqueue 服务器状态、ABAP 消息服务器和网络连接
2. 资源利用率：跟踪用户活动、内存利用率、CPU 使用率和系统效率指标
3. 数据库：提供有关 HANA 数据库和非 HANA 数据库的详细见解
4. 性能：衡量对话响应时间、RFC 响应时间和后台作业性能
5. 安全性：监控关键安全组件、证书和合规性
6. BTP 监控：与 SAP CloudAlm 集成， OpenTelemetry APIs 实现全面的 BTP 环境监控



New Relic Monitoring for SAP 解决方案产品文档详细介绍了技术细节以及安装和配置步骤。你可以从 Marketpl AWS ace 购买你的 New Relic 解决方案，也可以通过数据表快速概览。

免责声明：New Relic 以及 New Relic 徽标均为 New Relic, Inc. 的商标。所有其他商标均为其各自所有者的财产。

SoftwareOne: PowerConnect 适用于 SAP 解决方案

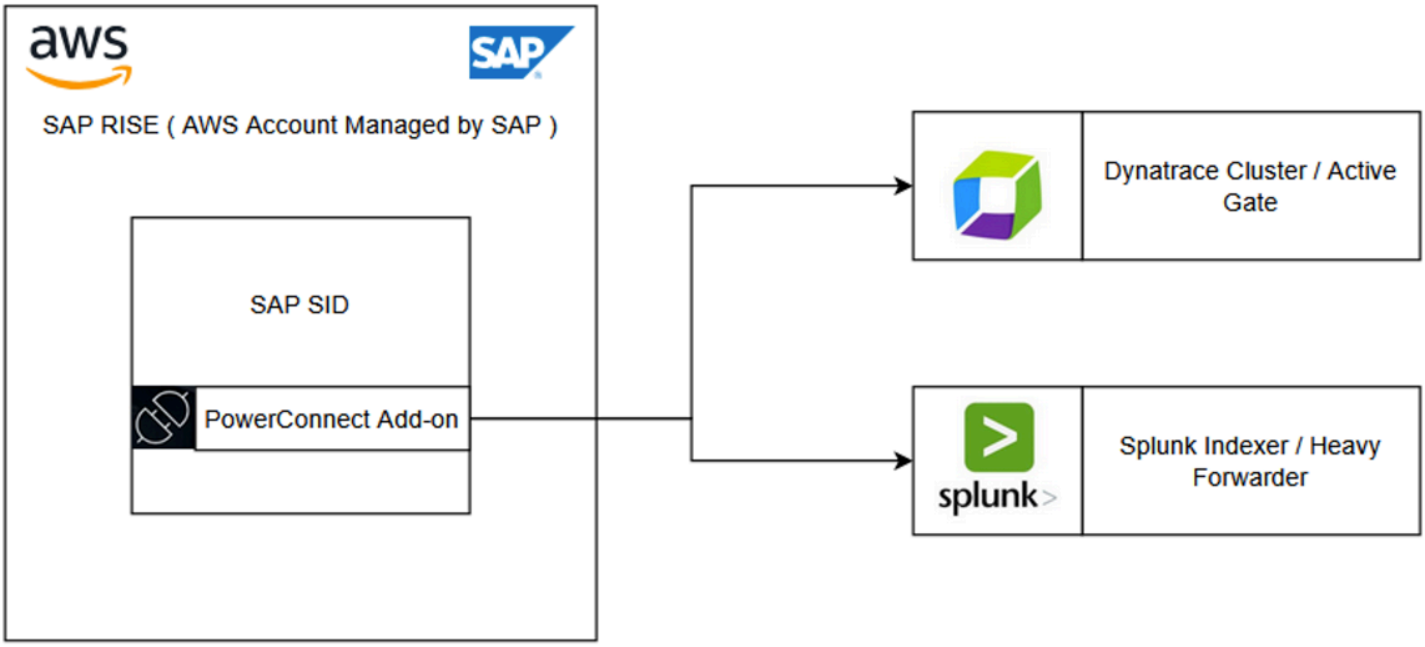
PowerConnect，这是一款经过 SAP 认证的高级可观测性和安全监控解决方案，可将来自 SAP 系统的实时遥测、性能、业务和安全数据流式传输到 Splunk 和 Dynatrace 等领先的可观测性平台。借助此解决方案，组织可以将其现有的监控投入扩展至 SAP 环境，深入了解应用性能、用户活动、安全事件以及系统运行状况，而不会中断核心业务运营。

关键功能：

- Out-of-the-box 适用于 SAP NetWeaver、S/4HANA、ECC、BW 等的连接器。
- 预先构建的仪表板和分析功能，可实现快速 time-to-value。
- 针对性能指标、更改事件和业务交易的可配置数据捕获。
- 开销较低的数据收集，不会影响 SAP 系统性能。

架构

PowerConnect 确保完全兼容并符合 SAP 标准。该解决方案可在每个 SAP 系统不到 45 分钟的时间内完成部署和配置，从而实现快速部署 time-to-value。开箱即用， PowerConnect 可以捕获性能、安全和业务流程领域的 360 多个关键 SAP 指标，并提供 1600 多个预定义的用例，可在您选择的监控或可观察性平台中使用，从而减少实施工作并加快洞察速度。



SoftwareOne PowerConnect SAP Solutions 的产品文档详细介绍了全面的技术细节以及安装和配置步骤，可通过 AWS Marketplace 获得。

免责声明: SoftwareOne, 并且 PowerConnect 是 SoftwareOne AG 的商标。所有其他商标、名称和徽标均为其各自所有者的财产。

PowerConnect 在 Dynatrace 上使用 SAP

PowerConnect for SAP on Dynatrace 是一款全面的可观察性解决方案，它将深厚 SoftwareOne的 SAP 专业知识与 Dynatrace 的人工智能平台相结合，可在 SAP 环境中提供统一的可见性。利用此解

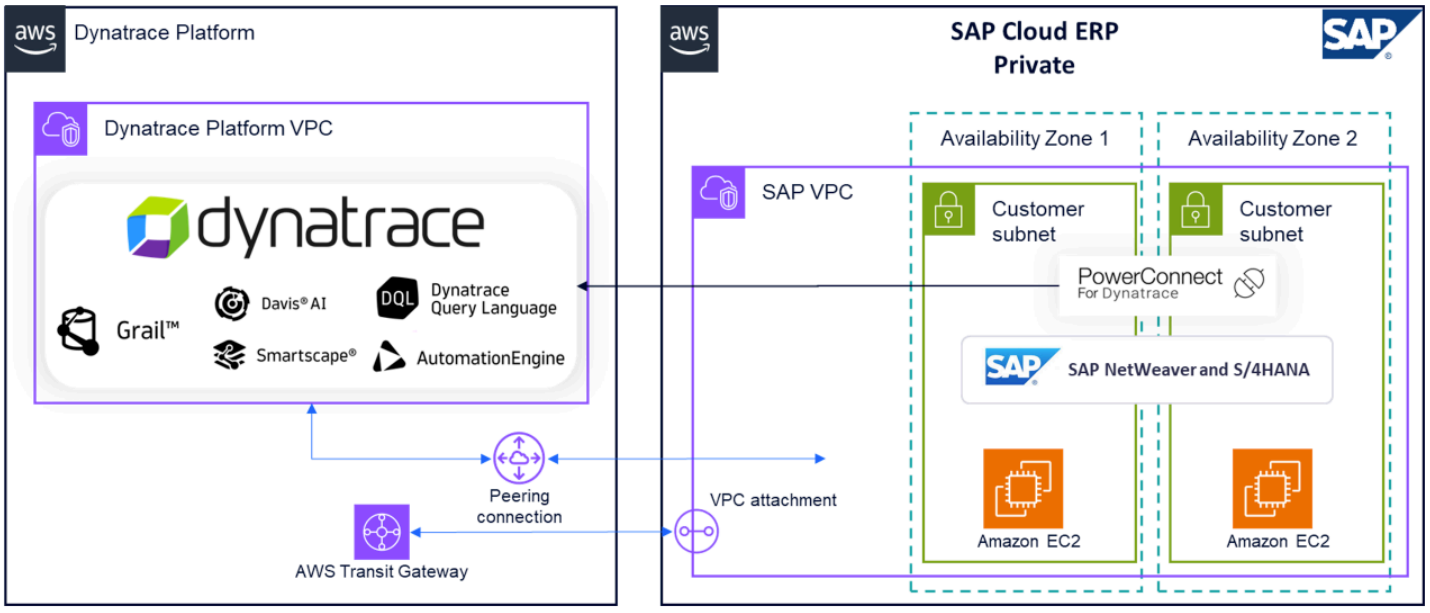
决方案，组织能够通过单一管理平台监控跨传统本地基础设施、SAP Cloud ERP、SAP 业务技术平台（BTP）以及各种云解决方案的复杂 SAP 环境。

主要优势

- 对各种 SAP 平台的全面可见性，包括 SAP S/4HANA、SAP BTP 及其他 SAP 产品
- 实时监控与见解，可确保实现业务连续性
- 全面的安全审计和应用程序日志分析
- AI 驱动型情境智能，实现事务跟踪
- 200 多种预构建的控制面板，可满足常见的 SAP 可观测性使用案例的需求
- 通过单一管理平台实现对整个 SAP 环境的可见性

架构

此解决方案提供了一个统一的可观测性框架，可与各种 SAP 部署场景无缝集成。该解决方案的核心是利用 PowerConnect 代理（ABAP和Java）与SAP Cloud ERP私有环境直接集成，而对于SaaS和公共云解决方案，它部署了运行云组件的专用 AWS 虚拟机。 PowerConnect 该虚拟机充当主动远程监控代理，建立与 SAP 的连接 APIs 并将遥测数据转发给 Dynatrace 租户。所有可观测性信号都会整合到 Dynatrace Grail 数据智能湖仓中，不管此类信号是来自 SAP Cloud ERP、BTP 还是其他 SAP Cloud 解决方案。这种统一架构支持通过单一管理平台对整个 SAP 环境进行全面监控与分析，使组织能够充分利用 Dynatrace 的 AI 驱动型分析能力，并全面了解其 SAP 生态系统的运行状况。



PowerConnect 适用于 SAP on Dynatrace 的产品文档详细介绍了全面的技术细节以及安装和配置步骤。你可以从 Marketpl ace 购买你的 Dynatr AWS ace 租户，也可以通过市场从那里 SoftwareOne获得 PowerConnect 许可。AWS

Splunk Service Intelligence for SAP Solutions

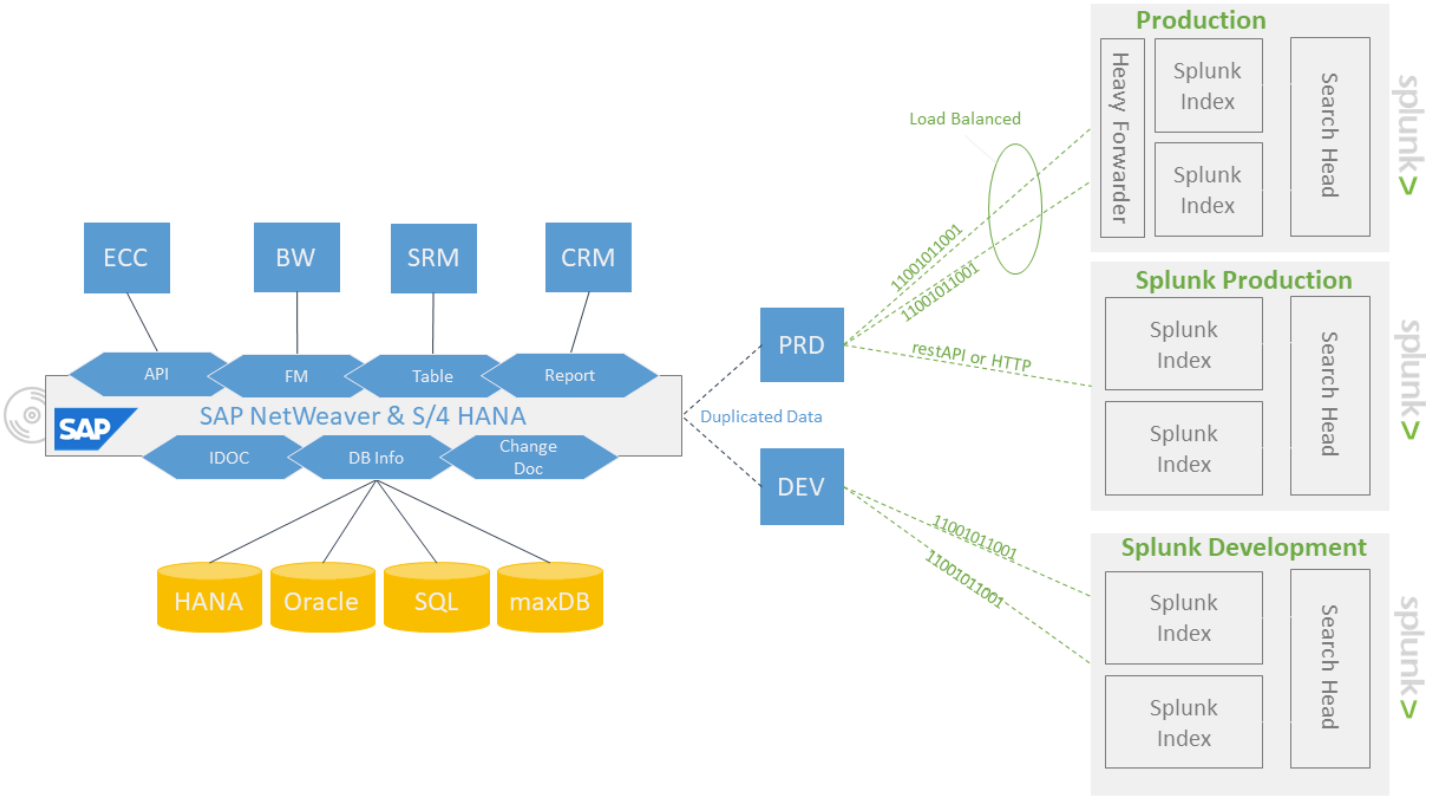
适用于 SAP 解决方案的 Splunk 服务情报是一款全面的 out-of-the-box解决方案，可对 SAP 环境进行主动 end-to-end监控。此解决方案能够监控运行 SAP 的各种基础设施元素、与之相连的应用程序组件，以及系统的底层基础设施。将此应用程序与 Splunk IT Service Intelligence（ITSI）中的监控功能结合使用，可以快速、主动地检测 SAP 环境中的问题，从而减少问题并避免代价高昂的中断。

主要优势

- Out-of-the-box 对 SAP 环境的监控能力以及对 SAP 运行状况、性能和安全状态的实时洞察
- 主动管理计划外停机时间
- 2000 多个特定于 SAP 的使用案例以及数百个预先交付的控制面板
- 即时查看事务日志、安全使用案例、系统性能和用户体验
- 先进的大数据分析与可视化功能

架构

通过向 SAP ECS 提交简易工单，可在一小时内完成 Service Intelligence for SAP Solutions 的部署。该解决方案的核心 SoftwareOne是利用 PowerConnect 代理（ABAP和Java）与SAP Cloud ERP 私有环境直接集成，而对于SaaS和公共云解决方案，它部署了运行云组件的专用 AWS 虚拟机。PowerConnect 使用 PowerConnect 实时访问 SAP 信息，利用 Splunk 机器学习、人工智能、高级大数据和可视化功能，可以获得前所未有的洞察、理解和预防措施。



Splunk Service Intelligence for SAP Solutions 产品文档详细说明了全面的技术细节，以及安装和配置步骤。

免责声明：Splunk、ITSI 和 Splunk 徽标均是 Cisco Systems, Inc 旗下的 Splunk Inc 的商标。所有其他商标均为其各自所有者的财产。

变更管理

在 RISE with SAP 中，SAP 企业云服务（ECS）负责管理与技术相关的传输，而客户负责通过 SAP 传输管理系统（TMS）进行与应用程序相关的传输。有关更多详细信息，请参阅 RISE with SAP S/4HANA Roles and Responsibilities。

虽然客户在执行传输操作时拥有灵活性，但对于超出 RISE with SAP ECS 范围的重大变更，建议进行协调，以确保获得适当的运营支持，并对潜在影响进行监控。例如，当你部署与 RISE 和 SAP 集成的 AWS 解决方案时， AWS 例如数据湖 AWS、物联AWS 网 (IoT) 和其他利用 AWS 服务的创新。

主题

- RISE with SAP 的变更管理
- AWS 服务变更管理

- 使用 Partner Solutions 进行变更管理

RISE with SAP 的变更管理

借助 SAP Cloud ALM，可以在整个环境中管理变更和编排部署。对于 RISE with SAP，Cloud ALM 与 Change and Transport System (CTS) 集成以编排传输请求的部署。

对于 SAP BTP，Cloud ALM 与 SAP Cloud Transport Management Service (cTMS) 集成，支持您将多种内容类型从开发或测试子账户传输至生产子账户（此处提供了支持传输的内容类型列表）。

对于使用 SAP 解决方案管理器的客户，Change Request Management (ChaRM) 是一项集成功能，可用于实施全面的变更管理。

SAP 提供了一个DevOps 参考框架，可以自动执行大部分部署管道，使您能够在 SAP Build 中快速设置 CI/CD 管道。

AWS 服务变更管理

您可以通过 SAP 管理与 RISE 连接的 AWS 服务的变更管理；因此，您可以 AWS 提供自动化管道配置和控制的服务。AWS f@@ DevOpso r 提供了一整套灵活的服务，旨在帮助公司使用和 DevOps 实践更快、更可靠地构建 AWS 和交付产品。

这些服务简化了基础架构配置、应用程序代码部署、软件发布流程自动化和性能监控。 AWS 提供完全托管的服务，无需设置，即可与 AWS 账户一起使用，并且可以从单个实例扩展到数千个实例。该平台支持手动任务的自动化，可通过 IAM 实现安全访问控制，并且能与庞大的合作伙伴生态系统集成。

AWS CodePipelineAWS CodeBuild，AWS CodeDeploy共同构成了一个高效的 CI/CD 自动化套件，通过启用针对多环境场景量身定制的自动构建、测试和部署工作流程，支持跨开发 (开发)、预生产 (pre-prd) 和生产 (prd) 环境的同步部署。

服务协同工作的方式

- CodePipeline 通过跨环境连接源代码、构建、测试和部署操作的各个阶段来协调工作流程。
- CodeBuild 处理每个环境（dev、pre-prd、prd）的编译、打包和测试代码，为依赖关系和配置提供隔离。
- CodeDeploy 管理向 EC2、ECS、Lambda 等目标的部署过程，并支持高级策略，例如 blue/green 用于安全发布到生产环境的金丝雀部署。

多环境设计

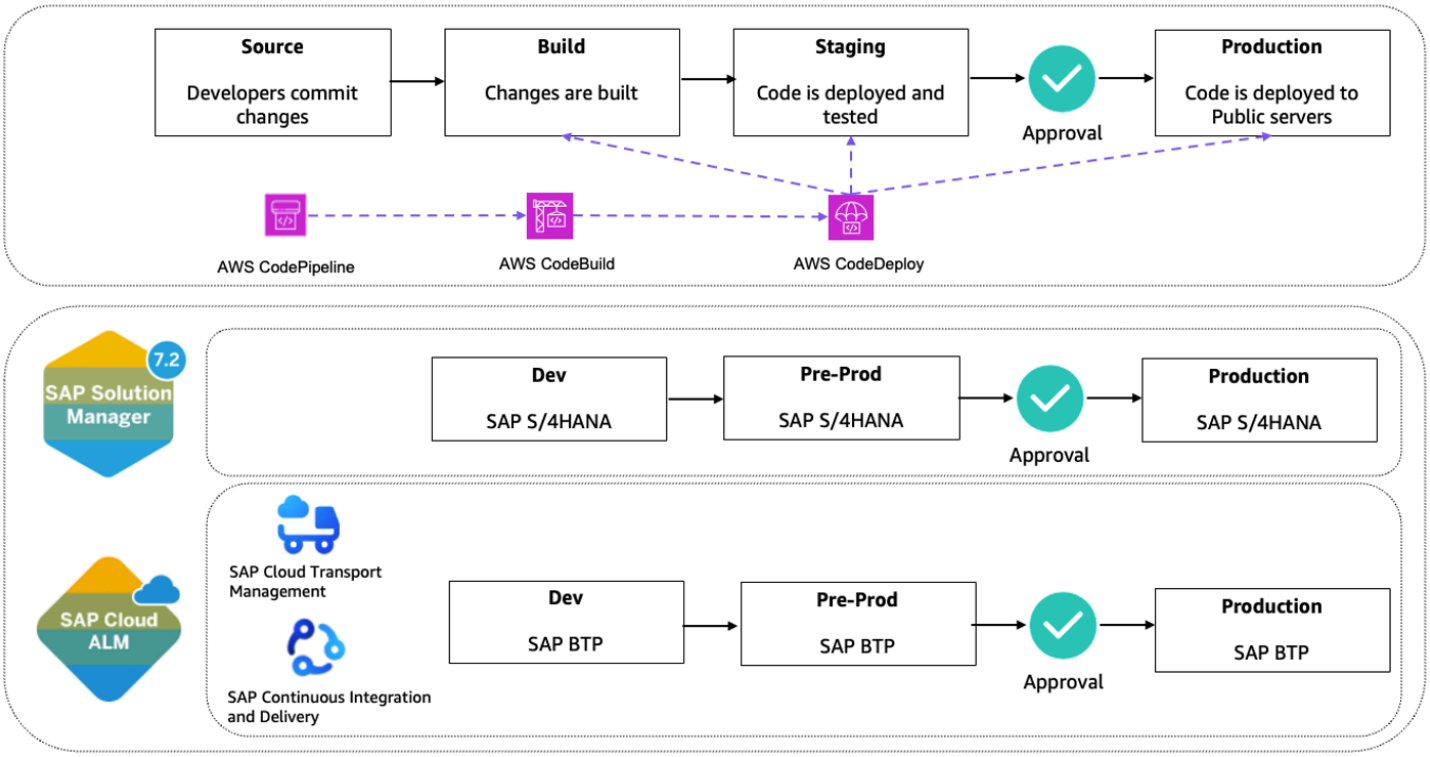
- 可以为 dev、pre-prd 和 prd 配置单独的管道或阶段。通常使用如下流程：
  - 新的提交会触发一个管道，在 dev 环境中构建、运行自动测试并部署到 dev 环境。
  - 测试成功后，手动或自动审批可将构件推送到 pre-prd 环境，以进行进一步的集成或用户验收测试。
  - 在 pre-prd 环境中完成所有检查后，另一个审批或触发操作会将构件部署到 prd 环境，并利用部署策略将风险降至最低。
- 最佳做法是使用单独的 AWS 帐户或权限界限隔离环境，以增强安全性和可追溯性。

DEV、PRE-PRD、PRD CI/CD 的关键注意事项

- 使用 infrastructure-as-code (CloudFormation/Terraform) 确保可重复、可审计的景观设置。
- 在每个阶段实现单元、集成和 end-to-end测试的自动化。
- 通过模块化管道阶段应用特定于环境的变量和配置。
- 为高风险环境设置审批关卡，尤其是针对生产发布。
- 启用监控 (CloudWatch/X-Ray) 并限制直接访问环境，尤其是在生产环境中。

每个环境都能从隔离的配置、有针对性的测试和部署策略中获益，这些措施有助于及早找出缺陷，并在进入生产环境前予以缓解。

这种模块化且具有环境感知能力的 CI/CD 设置可自动发布，支持在开发中进行快速迭代，在pre-prd中进行全面审查，并在prd中进行安全、可靠的部署，从而在保护生产稳定性的同时支持整个开发生命周期。



使用 Partner Solutions 进行变更管理

当您的需求超出标准的 SAP 和 AWS 变更管理工具时，以下是测试和变更管理方面的几个合作伙伴解决方案。

1. Tricentis - Tricentis Continuous Testing Platform 是一款部署在 AWS上的 AI 驱动型、全自动化的无代码软件测试解决方案。此平台可缩短发布周期来加速软件交付，通过自动化流程来降低成本，并提供针对企业应用程序的风险防范。该平台由三个主要组件组成：Tosca，它提供由Vision AI支持的无代码测试自动化，用于在各种环境中 end-to-end进行测试；qTest，为自动和探索性测试提供可扩展的敏捷测试管理；以及Neoload，它简化了性能测试，以实现从开发到生产的持续性能、可靠性和可扩展性。
2. Basis Technologies—— ActiveControl是一款企业级变更管理自动化平台，专门为SAP ECC、SAP S/4HANA和SAP BTP设计，同时防止变更失败。此解决方案可实施统一治理与质量检查，同时支持并行开发、自动化测试以及跨不同的 SAP 环境的同步部署，从而大幅降低出现生产问题的几率，并加速业务关键型变更的交付。

这些只是一些支持 SAP 和 AWS 变更管理场景的精选解决方案，你可以从 AWS Marketplace 中找到许多其他合作伙伴解决方案来满足你的需求。

数据集成与分析

此部分介绍了与 RISE with SAP 相关的数据集成与分析

主题

- 数据集成
- 数据分析

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。

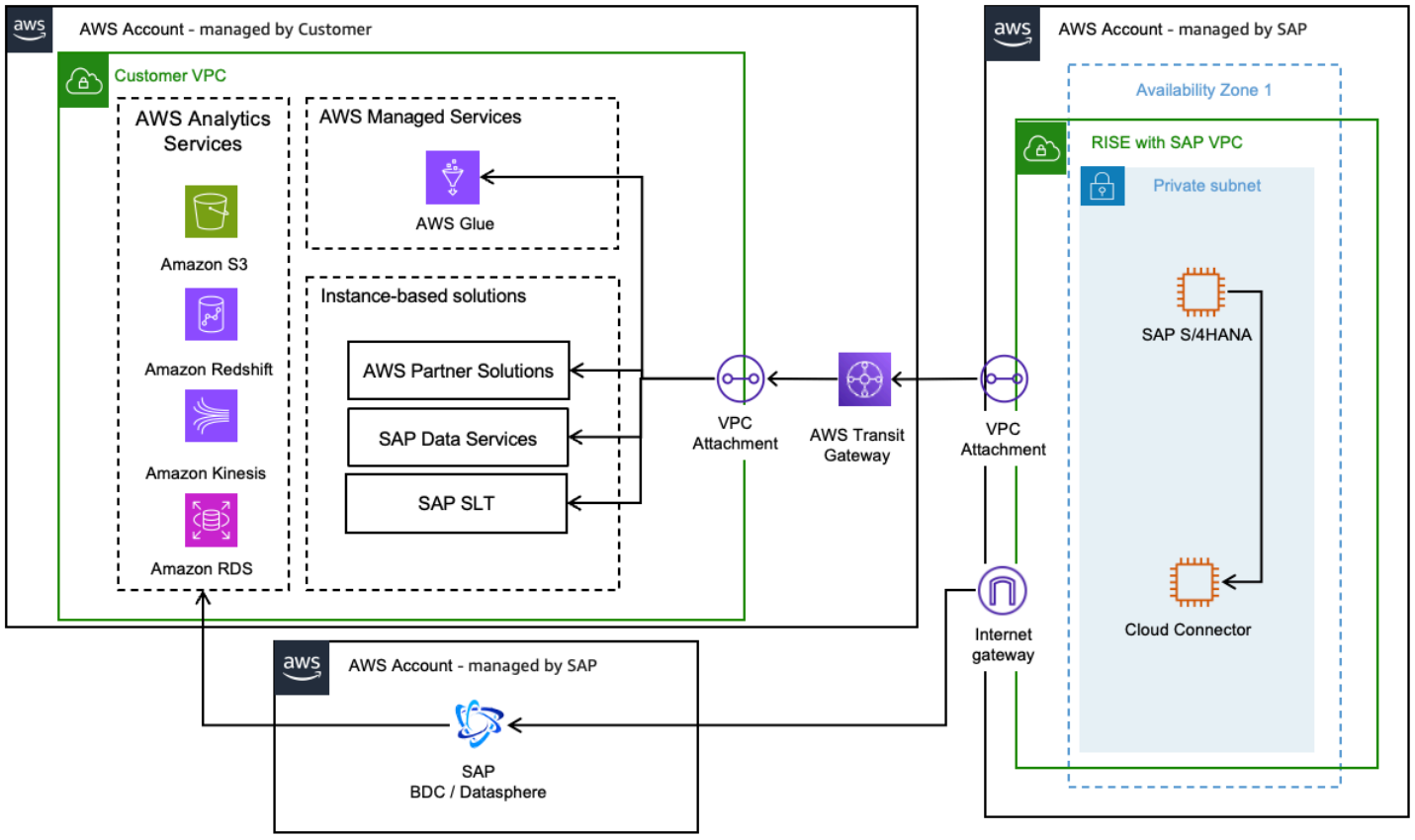
RISE with SAP 与数据集成的可扩展性框架概述了两种主要的数据处理与集成机制。

主题

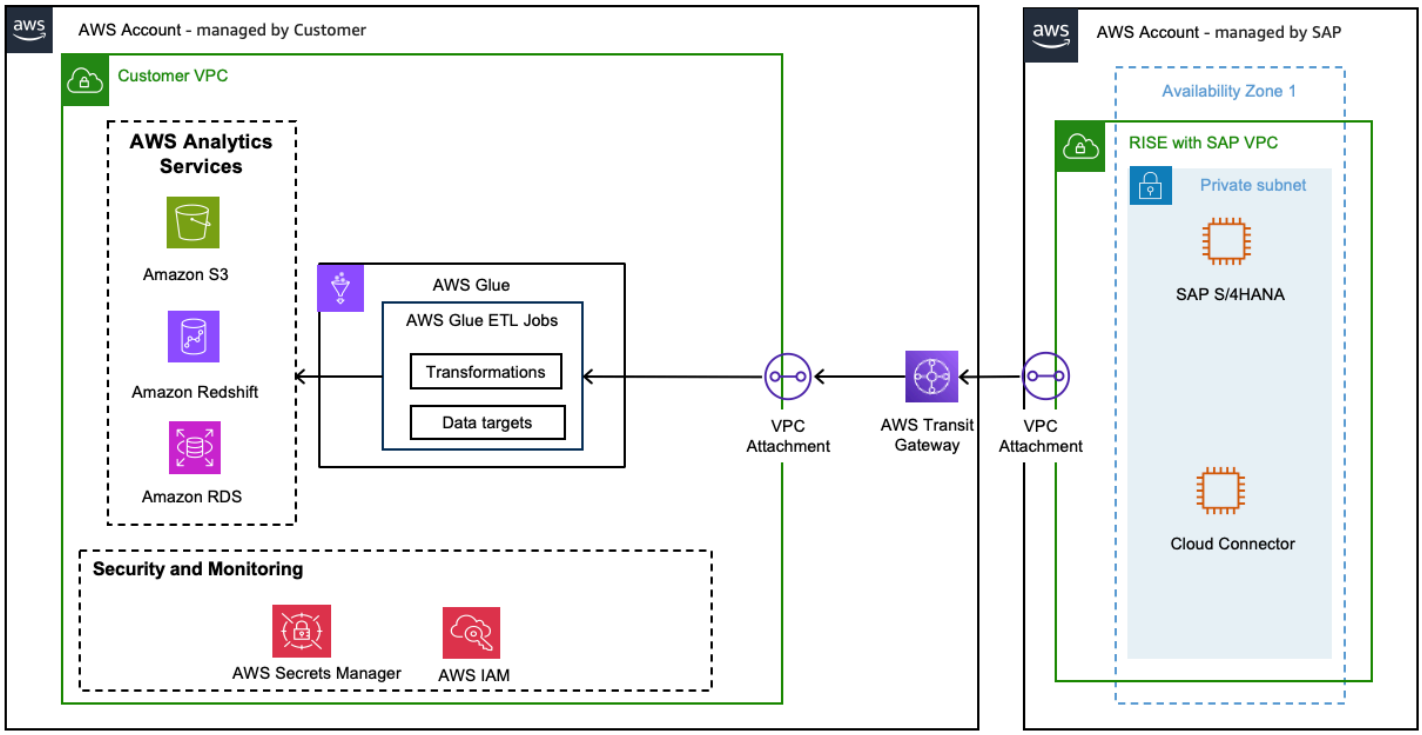
- 数据复制
- 使用 AWS 服务复制数据
- 使用 SAP 服务复制数据
- 使用 Partner Solutions 复制数据
- 使用 AWS 服务进行数据联合

数据复制

从 SAP 复制数据是使数据能够用于报告、分析以及与其他系统集成的关键步骤。以下参考架构说明了如何在 AWS中执行此操作。



使用 AWS 服务复制数据



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、加载（ETL）”管道，以将 SAP 数据加载到数据湖和数据仓库中。

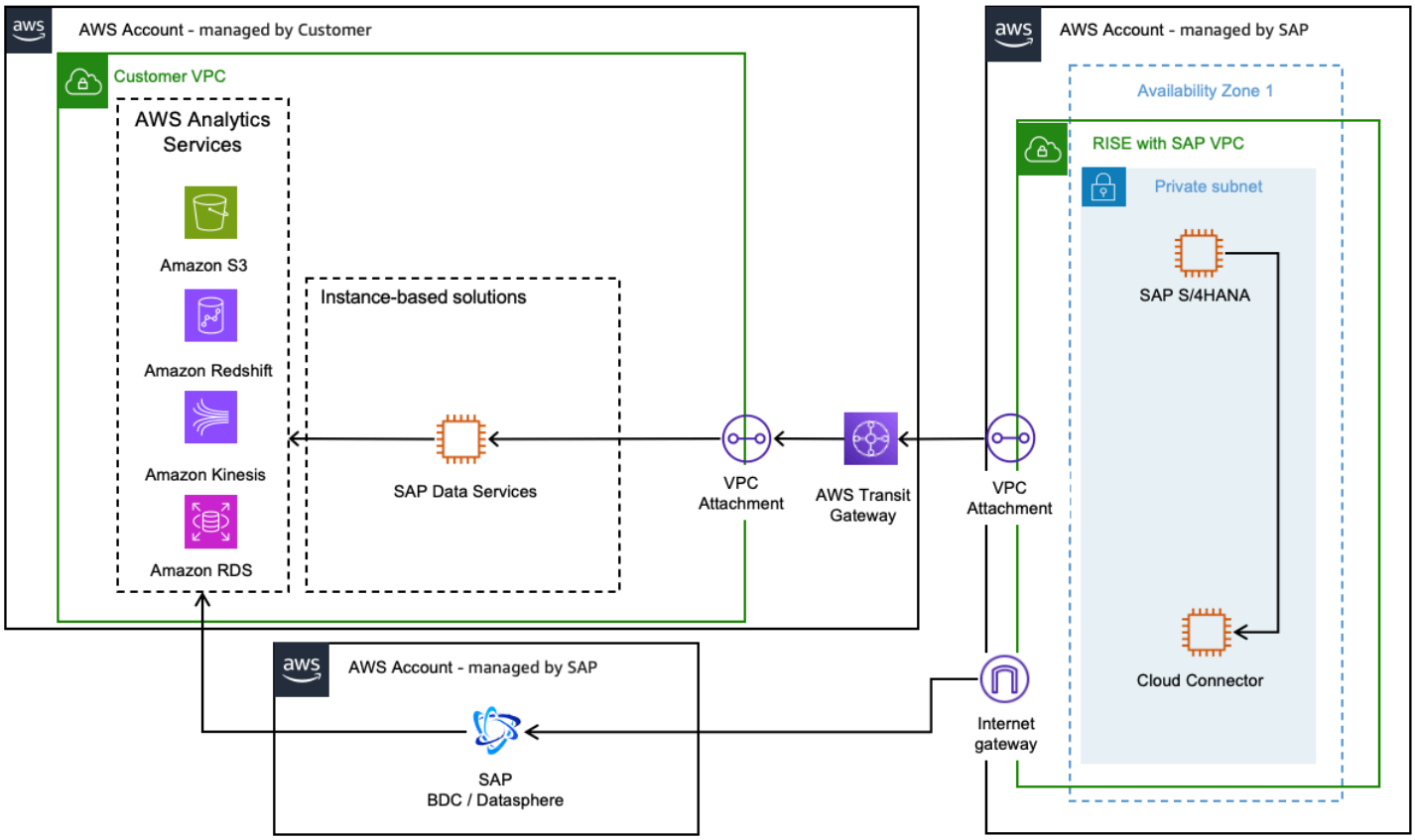
OData 使用 Glue 连接到 SAP 用户指南提供了有关设置 Glue ETL 作业、配置 SAP OData 连接和从 SAP 读取数据（包括处理增量传输）的全面说明。

AWS Glue Zero-etl 是一组完全托管的集成 AWS ，它最大限度地减少了为常见的摄取和复制用例构建 ETL 数据管道的需求。它在 Amazon SageMaker Lakehouse 和 Amazon Redshift 中提供来自多个运营、交易和应用程序来源的数据。利用 SAP OData 连接器，您可以从 SAP 创建完整的数据复制作业，包括完全托管的复制（插入、更新和删除）以及架构演进。

AWS Glue 和 Glue Zero-etl 在数据集成中扮演着不同的角色，它们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 的复制等特殊场景。 AWS Glue Zero-etl 旨在为完全托管的数据复制场景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。 AWS Glue 的性能因其无服务器横向扩展 Apache Spark 环境而得到增强，该环境允许您为可扩展计算分配数据处理单元 (DPUs)。进而支持并行处理和事件驱动型执行。

使用 SAP 服务复制数据



SAP BDC/Datasphere

SAP Datasphere 提供多种连接类型，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 BDC/Datasphere 文档，选择最适当的连接来复制 SAP 数据。使用 [Amazon Simple Storage 连接（Amazon S3）] 的高级出站集成，配置 SAP Datasphere 复制流程以将数据摄取到 Amazon S3。

SAP Data Services

SAP Data Services 提供多种连接，可从 SAP ECC 数据中复制数据。请参阅 SAP Data Services 文档，选择最适当的连接。SAP Data Services 提供 Amazon Redshift 数据存储和 Amazon S3 数据存储以将数据摄取到 AWS。它还提供 Amazon S3 file location protocol 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 Partner Solutions 复制数据

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。

要找到并部署符合您的特定需求的解决方案，您可以探索 AWS Partner Solutions Finder，或浏览 AWS Marketplace，可在其中搜索并快速部署专为您的独特 SAP 使用案例定制的合作伙伴解决方案。

更多资源

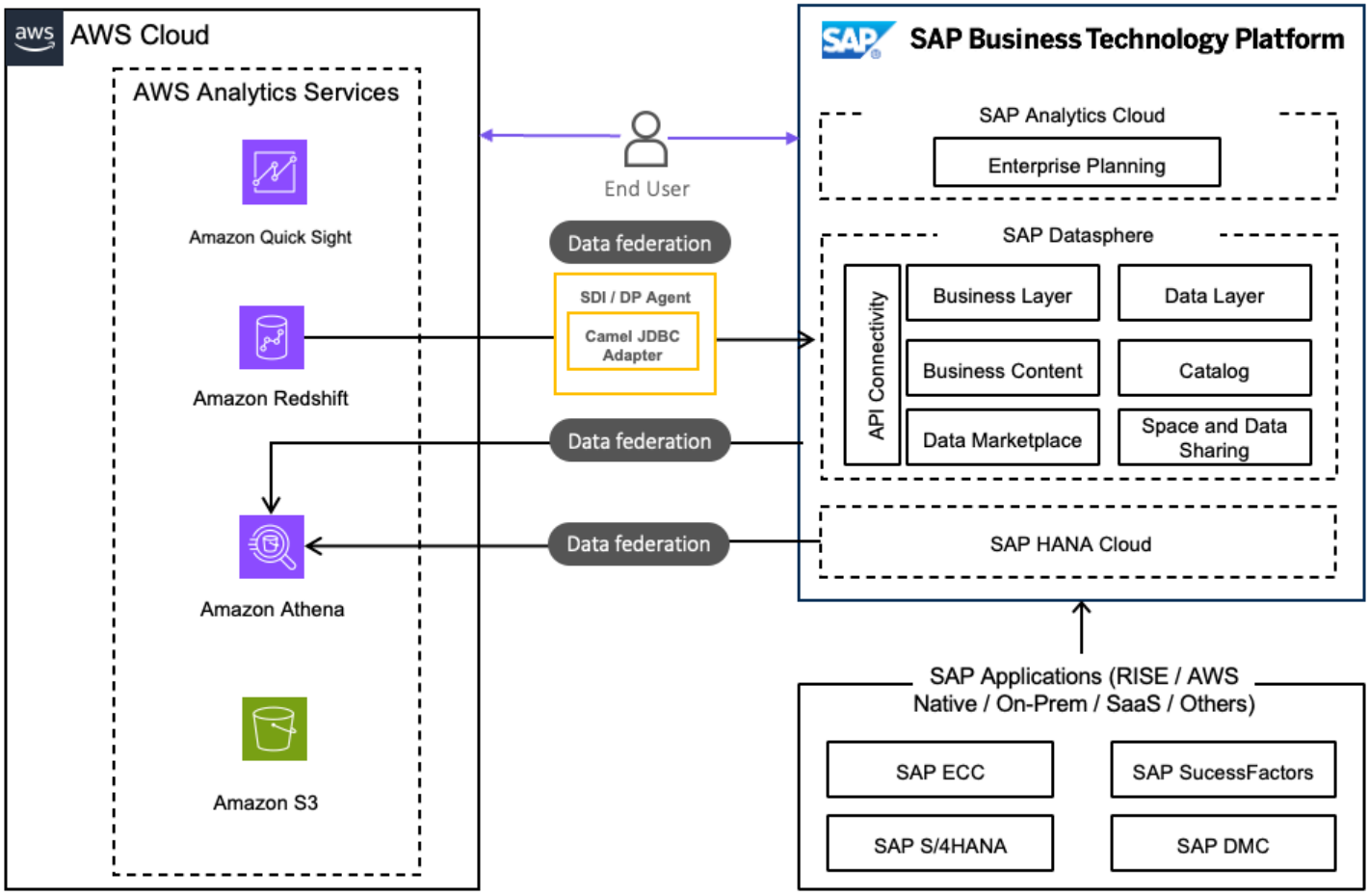
AWS上的 SAP 数据集成与管理指南提供了构建数据与分析解决方案所需的核心数据基础。它展示了如何使用 AWS 服务、SAP 产品和 AWS 合作伙伴解决方案， AWS 以实时或批处理模式将来自 SAP ERP 源系统的数据与变更数据捕获进行集成。它包括一个概述参考架构，展示了如何将 SAP 系统引入，此外还有五种详细的架构模式，这些模式使用上面重点介绍的 AWS 服务 OData、SAP 产品和合作伙伴解决方案来补充 SAP 支持的机制（例如 ODP、SLT 和 BTP）。 AWS AWS

使用 AWS 服务进行数据联合

数据联合是一种数据管理策略，可实现实时分析、单一 source-of-trust、无重复数据或昂贵的管道。

当业务需求涉及整合交易数据、分析数据和机器学习数据时，建议从数据来源直接访问数据而不是复制数据，这样做可避免延迟、数据不一致及额外的存储成本。

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。



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。存储在 Amazon S3 中的、来自多个数据来源的数据，可通过 Amazon Athena 进一步转换为表和视图，且可对这些表和视图进行查询，以结构化的方式复制有用的信息。

可通过 SAP Datasphere 连接的数据联合功能，从 SAP Datasphere 访问 Athena 中的数据。用户还可以使用 Athena Federated Query 来查询 SAP HANA，从 Athena 访问 SAP Datasphere 表和视图。

也可以使用 Smart Data Access – Athena adapter 将 Athena 配置为远程源，从而将数据联合到 SAP HANA Cloud。Athena Federated Query 连接还可用于从独立的 SAP HANA Cloud 环境中读取数据。

Amazon Redshift

Amazon Redshift 是一项完全托管的 PB 级数据仓库服务，来自于。 AWS利用此服务，客户可构建自己的数据仓库，并创建用于分析和报告的数据模型。

通过 SAP HANA Smart Data Integration（SDI）或 SAP Data Provisioning Agent，可实现从 Amazon Redshift 到 SAP Datasphere 的数据联合。此外，也可通过 Athena Federated Query 数据来源连接器，对 Amazon Redshift 数据进行联合操作。

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 客户需要实时获取业务见解，以应对业务变化并利用尚未开发的商机。为此，客户需借助现代化的云原生解决方案，从夜间数据处理转变为实时分析。利用 AWS 和 SAP 解决方案，客户可以利用专门构建的分析服务，在各自的行业中获得竞争优势。

数据湖、数据仓库和湖仓等现代数据架构提供了多种模式与服务组合，可帮助组织处理海量结构化数据与非结构化数据以进行分析和报告，同时也为人工智能（AI）、机器学习（ML）应用程序（包括生成式人工智能）奠定了坚实的基础。这些架构提供的构建数据块既能独立部署，也能相互补充，具体取决于需求和偏好。

主题

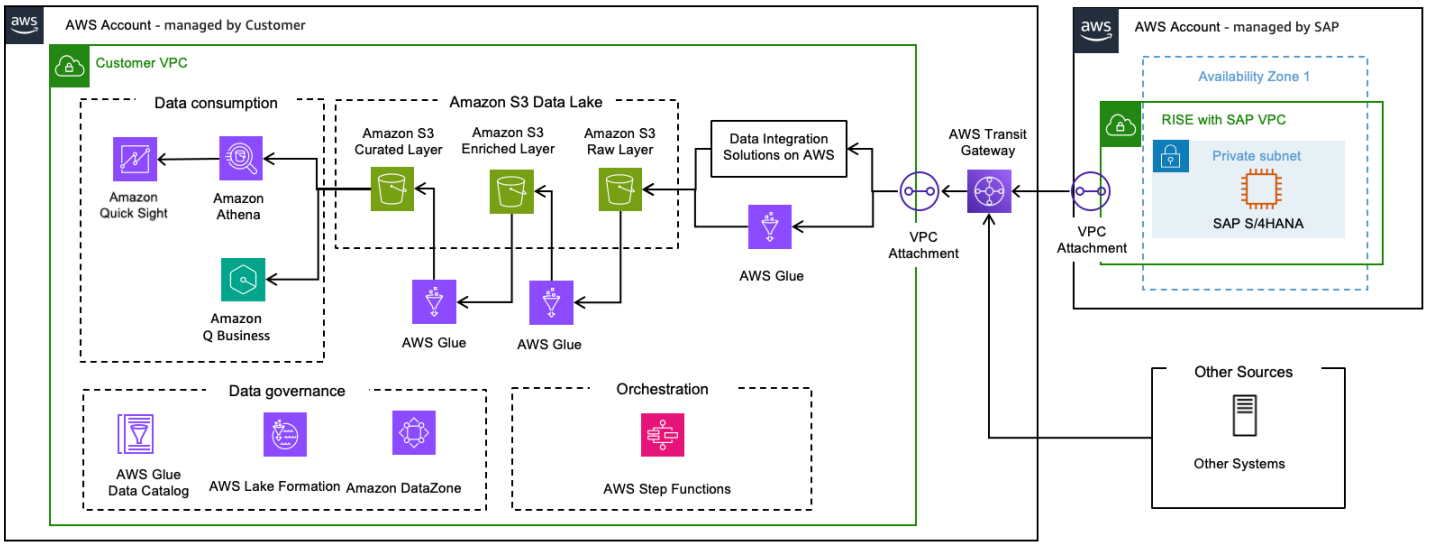
- 数据湖架构
- 数据仓库架构

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

利用数据湖，客户可以处理结构化数据和非结构化数据。它基于 “schema-on-read” 方法设计，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）。结构在从数据来源读取数据时进行定义，此时会确定数据类型和长度。因此，存储与计算实现解耦，依托低成本存储方案来扩展至 PB 级规模，且成本仅为传统数据库成本的一小部分。

借助数据湖，组织可以执行各类分析任务，例如创建交互式控制面板、生成可视化见解、处理大规模数据、开展实时分析，以及在各类数据来源中实施机器学习算法。



数据湖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：

原始层

原始层是数据湖中的初始层，基于 Amazon S3 而构建，来自源系统的数据会以原始格式直接进入该层，而不经过任何转换。该层的数据用于确定变更以及需整合到下一层的数据，这是因为原始层将包含同一数据的多个版本（变更、完全加载等）。

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（文件数由提取工具中的数据包大小或页面大小决定），因此，单次提取操作可能会生成多个文件。

扩充层

扩充层基于 Amazon S3 构建，包含源 SAP 系统中数据的真实呈现以及逻辑删除内容，并以内置 Apache Iceberg 格式存储在 Amazon S3 表类数据存储服务中。Iceberg 表文件格式支持在 Glue Data Catalog 中创建 Glue 或 Athena 表，可实现插入、更新和删除等数据库类型操作，其中文件操作（如记录删除等）采用 Iceberg 文件格式进行处理。此外，Iceberg 表还支持时间迁移概念，能够查询特定时间点的数据。

来自原始层的数据会基于表键按正确顺序插入或更新至扩充层，并以原始格式保留（不进行任何转换或修改）。每条记录均需补充特定属性，例如提取时间和记录编号，此操作可通过 AWS Glue 作业实现。

精选层

精选层用于存储数据以供使用。在此层上，将物理删除已从来源中删除的记录。任何计算结果（如平均值、日期间隔等）或数据操作（如格式更改、从其他表中查找等）均可存储在此层以供使用。使

用 AWS Glue 作业更新此层中的数据。基于这些数据表创建的 Amazon Athena 视图可通过 Amazon Quick Sight 或类似工具以供下游使用。

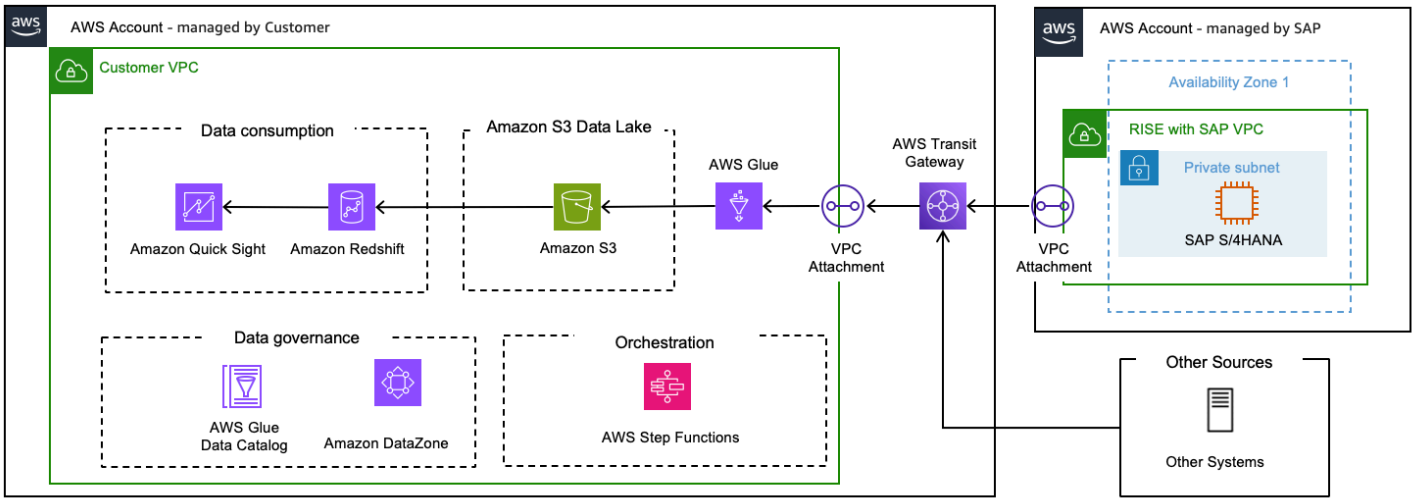
《包含 SAP 和非 SAP 数据的数据湖 AWS 解决方案指南》提供了详细的架构、实施步骤以及用于快速跟踪 SAP 和非 SAP 数据数据湖实施的加速器。有关将数据从 SAP 提取到数据湖的各种可用方案，可参考前面的“数据集成”部分。

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)。它使组织能够使用针对复杂查询（而非事务处理）优化的架构，分析海量集成数据以做出明智的决策。

业务分析师、数据工程师、数据科学家和决策者可通过商业智能（BI）工具、SQL 客户端及其他分析应用程序访问数据仓库。架构包含多个层：用于呈现结果的前端客户端、用于数据访问与分析的分析引擎，以及用于数据加载与存储的数据库服务器。

数据以表和列的形式存储在数据库中，并按模式进行组织。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。



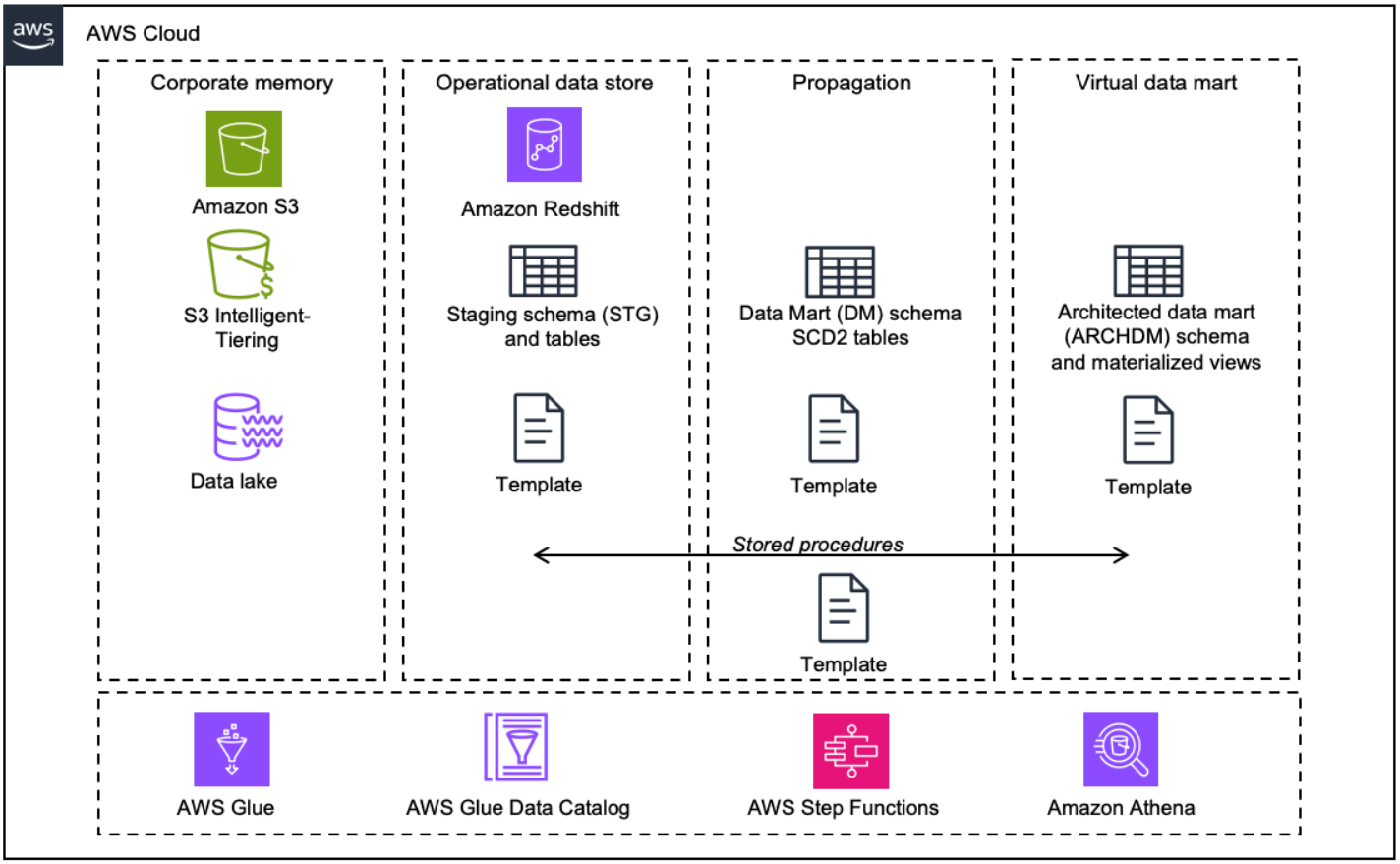
主要特征

- 整合：将来自不同来源（例如，CRM、ERP）的数据整合到统一的模式中，解决格式或命名规范不一致的问题。
- 时变：跟踪历史数据，支持数月或数年的趋势分析。
- 以主题为导向：围绕销售或库存等业务领域（而非基于运营流程）组织数据。

- 非易失性：数据在存储后保持静态；更新通过定期的提取、转换、加载（ETL）流程（而非实时更改）进行。
- 成本优化：SAP 数据与非 SAP 数据存储在成本优化的架构中。

架构组件

- ETL 工具：自动完成从来源提取数据、转换（清洗与标准化）数据并将数据加载至仓库这一流程。
- 存储层：
  - 结构化数据的关系数据库
  - 用于多维分析的 OLAP（联系分析处理）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对不同粒度的数据进行组织，这有助于确保数据的一致性和灵活性。最常见的数据仓库架构层包括源层、暂存层、仓库层和使用层。SAP 系统的数据仓库同样采用基于层的架构。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。

企业级存储

Amazon S3 Intelligent-Tiering 是一种可自动优化存储成本的存储类别，可根据数据访问模式的变化，在不同访问层间迁移数据。这可确保频繁访问的数据随时可用，同时将访问频率较低的数据或“冷”数据存储在成本更低的层中。有关更多详细信息，您可以参阅 Amazon S3 存储类别。

操作型数据存储层

Amazon Redshift 用于实现操作型数据存储、传播和数据集市功能。提供脚本以创建数据模式并部署数据定义语言（DDL），且包含加载 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 作业加载到 S3 中的增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

利用 Redshift 中的实体化视图构建结构化的数据集市模型。事务数据通过主数据（属性和文本）进行扩充，从而构建出可直接用于数据使用的分析模型。

《在 AWS 解决方案上构建 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。

代理式人工智能

什么是代理式人工智能

代理式人工智能指具备自主性的人工智能系统，能够在最少人工干预的情况下，独立进行推理、规划并执行复杂的多步骤任务，以实现预定目标。与主要基于人类提示生成内容的生成式人工智能不同，代理式人工智能具有主动性且专注于采取行动。其运行机制是通过迭代循环持续感知环境、推演可行方案、执行决策并从结果中学习。

代理式人工智能系统的类型

可使用不同的配置来部署代理式人工智能，从单一用途代理到大规模多代理系统。

- 单代理：单个人工智能代理单独工作以完成已定义的焦点式任务。

- 多代理：多个具有专业技能的人工智能代理协同合作，共同处理复杂的工作流。可采用垂直分层结构，由主管代理监督其他代理；也可采用水平去中心化结构，所有代理平等协作。

代理式人工智能的演进过程

第 1 阶段：加强人工监督（生成式人工智能助手）。在初始阶段，人工智能系统主要作为生成式人工智能助手（例如，早期版本的聊天机器人或写作辅助工具）运行，人类参与度高。此阶段下的人工智能具有被动响应性，基于提示驱动，并采用“人工介入”模式。

第 2 阶段：生成式人工智能代理。在此阶段，通过更强的上下文感知与工具使用能力来增强基础人工智能助手，并借助能够执行多步骤任务的代理创建具有扩展功能的早期生成式人工智能代理。它们受护栏控制，且仍依赖提示。

第 3 阶段：代理式人工智能系统。代理式人工智能标志着人工智能向更高自主性的重大跨越，并深度整合复杂推理、规划与记忆能力。人工智能主动执行任务而不是等待提示，具备持续学习能力，并采用“人工介入”模式，人类角色从直接参与转变为战略监督。

第 4 阶段：自主人工智能代理。在此最后阶段，将部署高度自主的多代理系统，这些系统只需最少的人为干预即可运行。它具有专门的多代理协作，可以应对复杂的端到端工作流，并且人类工作的重心从监督转移到治理。

使用 Amazon Bedrock 实现代理式人工智能

Amazon Bedrock 为构建和部署代理提供了全面而灵活的工具集，支持完全托管和 do-it-yourself（DIY）方法。这是通过将完全托管和基于配置的 Amazon Bedrock A gent 与 Amazon Bedrock 高度可定制和可组合的服务相结合来实现的。 AgentCore

主题

- Amazon Bedrock 代理
- Amazon Bedrock Agentcore
- Strands Agent
- 用于管理 ERP 异常的代理式人工智能

Amazon Bedrock 代理

Amazon Bedrock Agent 充当智能协调器，使用 reason-and-act (ReAct) 模式来满足复杂的用户请求。它使用基础模型的推理 (FMs) 和数据来分解用户请求，收集相关信息并高效地完成任务，从而使团队腾出时间专注于高价值的工作。 APIs您可以参考此链接，了解如何实现 Amazon Bedrock 代理。

- 用户请求：流程始于来自用户的自然语言请求，例如“生成销售报表并分享给财务团队”。
- 推理与规划：Bedrock 代理的编排提示和底层基础模型会解析请求，并将其拆解为逻辑连贯的多步骤操作。
- 工具执行：代理通过调用“工具”（使用 API 架构定义的操作组）来执行计划。这些工具可以通过 Generative AI Hub 调用 SAP 系统中的后端服务。例如，代理可以：
  - 调用 API，从 SAP 获取销售数据
  - 访问知识库 [通过检索增强生成（RAG）工具在 Bedrock 中执行此操作]，提取相关的业务文档。
  - 利用代码解释器或浏览器 AgentCore 进行数据分析或与基于 Web 的 SAP 用户界面进行交互。
  - 利用记忆功能，在多轮用户交互中维持上下文连贯性。这对于多步骤流程至关重要，例如通过多轮对话完成复杂采购订单的填写。

Bedrock 代理全面支持多代理协作，允许您构建并部署由专业人工智能代理组成的系统，这些代理将协同工作以完成复杂的多步骤工作流。不是通过单个代理来尝试处理复杂任务的所有环节，而是编排一组代理，使它们运用自己特定的专业知识，进而提升效率、准确性与总体性能。Bedrock 中的多代理协作的核心是分层模型，该模型一个由主管代理和一个或多个协作者代理构成。

Amazon Bedrock Agentcore

Bedrock AgentCore 是一套服务，使开发人员能够在企业规模上安全地构建、部署和操作功能强大的 AI 代理。它旨在承担开发代理人工智能的 “无差别繁重的工作”，使企业能够超越 proofs-of-concept并加快生产部署。Bedrock AgentCore 提供了一个模块化的服务工具包，可以一起使用或独立使用来创建复杂的 AI 代理。

- 运行时：一个安全的无服务器环境，用于部署和扩展动态人工智能代理，支持长时间运行的任务与异步任务，并且具备完整的会话隔离能力。
- 网关：一项服务，只需最少的代码即可将现有函数 APIs 和 AWS Lambda 函数转换为与代理兼容的工具。它支持使用模型上下文协议（MCP）等协议实现工具发现与安全通信。
- 记忆：管理代理的短期会话上下文与长期记忆，无需开发人员管理底层基础设施，即可实现更具个性化、上下文感知的交互。
- 内置工具：借助代码解释器（支持安全的代码执行）与浏览器工具（用于与 Web 应用程序交互）增强代理功能。
- 身份：提供一项专为人工智能代理设计的安全、可扩展的身份与访问管理服务，并支持与现有身份提供者集成以管理代理权限。
- 可观察性：提供用于跟踪、调试和监控生产中代理性能的工具， CloudWatch 并提供由 Amazon 提供支持的全面控制面板。 OpenTelemetry

Bedrock AgentCore 被明确设计为与模型无关，让开发人员可以灵活地在 Amazon Bedrock 生态系统内外使用他们选择的任何基础模型 (FMs)。这些是 Bedrock 中 FMs 托管的一些内容，有关完整列表，您可以参考以下文档：

- Anthropic：Claude 系列模型，包括最新的 Claude 模型。
- Meta：Llama 系列模型。
- Mistral AI：一系列 Mistral 模型。
- Amazon：Amazon 自有模型，包括 Titan 和 Nova 系列。
- OpenAI：来自 OpenAI 的精选开放权重模型。
- 其他提供商： AI21 实验室、Cohere DeepSeek、Stability AI 等。

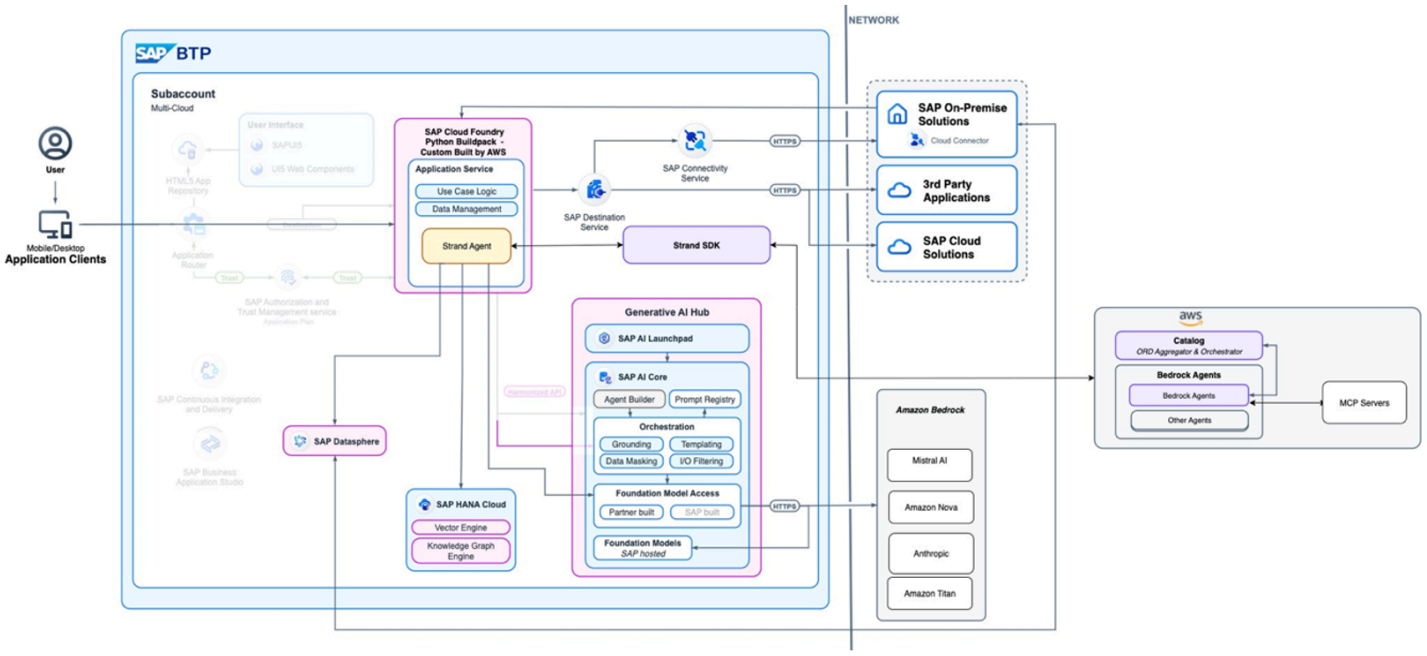
Strands Agent

Strands Agent 是一个开源 SDK，由创建， AWS 用于构建使用大型语言模型 (LLMs) 进行推理和行动的 AI 代理。Strands Agents SDK 简化了人工智能代理的创建流程，并专注于三大核心组件：

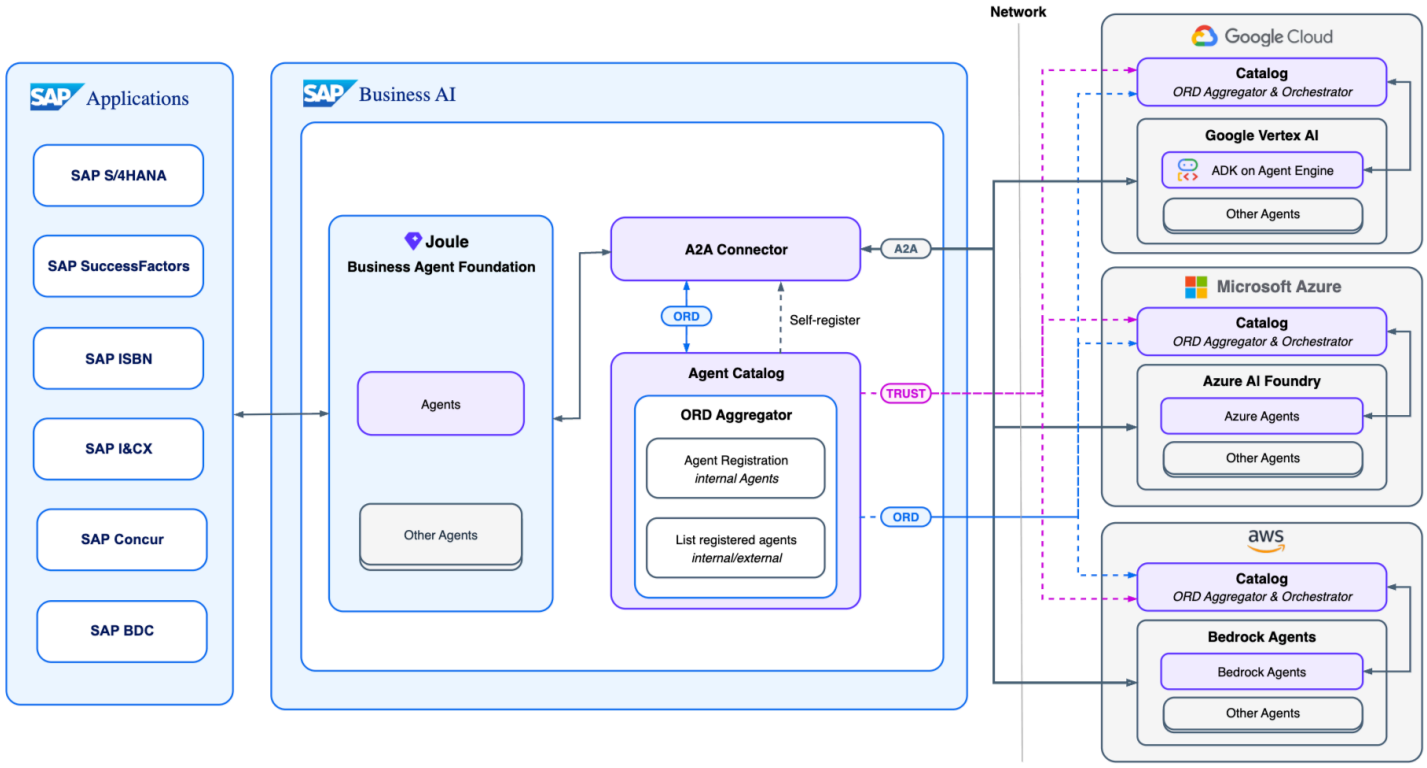
- 语言模型：Strands支持Anthropic、OpenAI和Meta等各种提供商，为开发者提供了灵活性 LLMs 。
- 系统提示：用于定义代理的角色和整体行为。
- 工具集：这些工具是代理可调用以执行任务的特定功能与能力。

Strands SDK 的优势：

- Strands SDK 支持在 SAP Generative AI Hub 上快速、安全地开发高级人工智能代理。
- 开发人员可以快速构建复杂的自动化流程，从而节省时间与资源。
- Strands SDK 支持多种人工智能模型，有助于推进未来的技术变革。
- 它具有企业级安全性和强大的监控功能，可确保使用过程安全可靠。



上述架构描述了 Strands Agents、用于访问 Amazon Bedroc FMs k 的 SAP Generation AI Hub 和 Bedrock Agent SDK 之间的集成选项，后者允许集成到模型上下文协议 (MCP) 服务器以访问可用于 APIs 自动化工作流程。



在 SAP 中，最有效的方式是让 Strands 构建的代理充当 SAP Joule 代理可调用的外部工具。这使得能够在 Strands 中开发专用的自定义逻辑，随后 SAP Joule 会在 SAP 应用程序的业务场景内编排该逻辑。上面的架构描述 Agent-to-Agent 协议的工作原理。

用于管理 ERP 异常的代理式人工智能

什么是 ERP 异常 - 企业资源规划（ERP）异常是指当实际场景或流程偏离计划的标准、策略或规则时，由 ERP 系统生成的通知。此类异常会以提醒形式提示各类问题，例如库存短缺、截止日期延误或数据不一致，这些问题需要人工介入来予以解决，以防止业务运营中断。

为什么使用代理式人工智能来管理 ERP 异常 - 代理式人工智能不仅能标记问题，还能自主推理、采取行动来解决问题，并从经验中学习。这可将 ERP 异常处理从被动响应模式转变为主动预防性流程。

代理式人工智能如何改进 ERP 异常处理

用于管理 ERP 异常处理的代理式人工智能有助于

1. 主动解决问题
2. 更快、更自主地解决问题：通过学习历史解决方案，代理式人工智能可以在没有人工干预的情况下解决大量异常
3. 持续学习与改进
4. 智能路由与升级
5. 提高合规性和可审计性，因为代理式人工智能代理执行的每项操作均可通过守护代理进行审计和保护
6. 释放人力资源

使用代理式人工智能进行 ERP 异常管理的典型使用案例

使用案例 1：三方发票匹配在该流程中，需将采购订单与收货单及发票进行匹配。匹配失败的发票异常案例会被发送至人工智能代理。此代理将执行用户通常会进行的调查操作，最终成功找到正确的采购订单编号，为负责处理异常的用户节省调查时间。负责处理异常的用户会审核代理的调查发现并予以批准。代理将处理事务，进一步为负责处理异常的用户节省事务处理时间。

使用案例 2：客户付款匹配 - 在此流程中，需将发票与银行对账单中的客户付款进行匹配。异常案例（匹配失败的客户付款）会被发送至代理式人工智能代理。人工智能代理将执行用户通常会进行的调查操作，找到发票并与银行对账单中的客户付款进行匹配，随后向用户提供推荐的解决方案，为其节省调查时间。负责处理异常的用户接受推荐方案后，代理将处理事务，进一步为负责处理异常的用户节省事务处理时间。

使用案例 3：销售订单录入 - 在此流程中，当某个销售订单行项无可用库存以满足发货需求时，代理式人工智能代理会从电子商务网站检索信息，通过电子邮件向客户发送替换 SKU，然后将此问题上报给信贷团队与供应链团队。完成调查后，代理将针对每种异常推荐解决方案。如果用户接受建议，则代理将在 SAP and/or 其他系统中执行事务以替换该项目。

使用案例 4：采购订单确认 - 代理式人工智能代理可解析每份采购订单，提取责任限制等关键条款，并将这些关键条款与中心合同进行比对，从而实现采购订单确认流程的自动化。确认完成后，代理可将采购订单作为订单录入到 ERP 系统中。

使用案例 5：现金预测 - ERP 系统包含创建现金预测所需的大部分或全部信息。该系统涵盖银行账户余额、未付供应商发票、未付客户发票，以及现金预测流程所需的其他关键输入信息。其他系统也可能包含需纳入现金预测的额外输入信息。预测由 bank/investment 账户余额、供应商发票（负债）和客户发票（资产）生成。代理式人工智能代理会从 ERP 系统及其他系统中收集必要的数据点，并依据标准操作程序计算每日现金预测。

使用案例 6：财务期末结账 - 在此流程中，人工智能代理可执行财务期末结账的部分、大部分乃至全部步骤，采用或不采用人工介入模式。该代理能够完成银行对账单核对、应收账款与应付账款核对、合并分类账，以及折旧计提、预收收入核算、预付费用核算与公司间对账等操作。它可通过与组织内的各个利益相关者沟通来处理异常。

AWS 还有 SAP JRA

AWS 而SAP联合参考架构（JRA）是一个框架，旨在指导客户如何有效地整合和利用两者 AWS 以及SAP服务来实现特定的业务成果。它为常见场景提供架构指导和最佳实践，帮助客户在两个平台上优化其 SAP 解决方案 AWS 并利用这两个平台的优势。

AWS 和 SAP JRA 的开发旨在解决共同客户和合作伙伴关于如何将 SAP 和/或 AWS 服务用于不同的业务解决方案场景的常见问题。我们在深入探讨每个使用案例时会发现，这两类服务能够相互补充，从而协同工作，从整体上解决客户各自面临的业务挑战。当你申请 AWS SAP JRA to RISE 时 AWS，你将能够解锁可能性，从投资中获得更多价值。

主题

- 将数据转化为价值
- 人工智能
- 集成
- 自定义应用程序
- 运营可靠性

- 物联网

将数据转化为价值

企业需要数据驱动型智能来交付可衡量的业务成果。运行 SAP 为将原始数据转化为可操作的价值 AWS 提供了可扩展、安全和灵活的基础。SAP和 AWS 联合参考架构（JRA）提供了一个框架，用于连接数据源，协调SAP和非SAP数据，以及通过SAP 业务数据云（SAP BDC）和Amazon S agemaker 实现人工智能和分析驱动的创新。

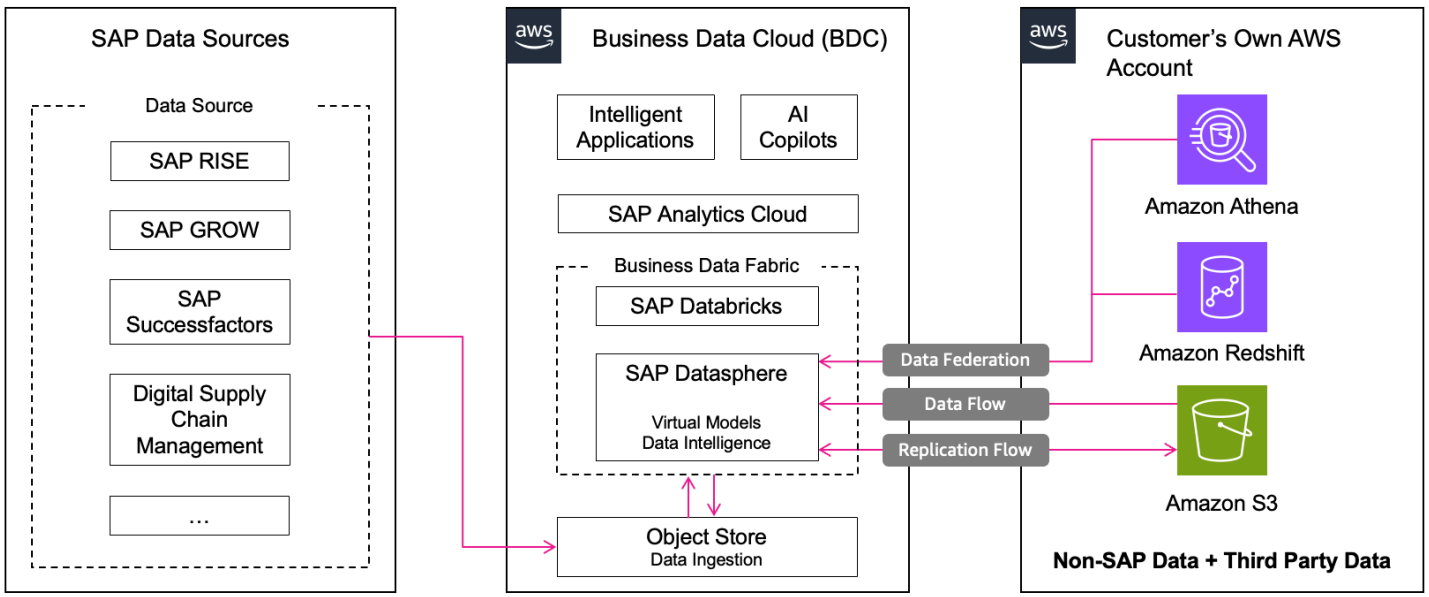
本指南概述了两个关键的联合参考架构，它们举例说明了组织如何利用 SAP 和 AWS 服务，通过人工智能驱动的洞察力最大限度地提高其企业数据的价值，同时保持灵活性、可扩展性和成本效益。

主题

- 将 SAP BDC 中的数据与 AWS 数据源集成
- 使用 FedML 和 Sagemaker 进行人工智能创新AWS

将 SAP BDC 中的数据与 AWS 数据源集成

通过带有 SAP BDC 的 SAP Datasphere 数据结构架构，可以将来自 AWS 数据源的非 SAP 数据与 SAP 数据进行协调。集成架构支持多种 AWS 服务，每种服务都有基于实时数据或复制的特定集成模式：



A. 与 Amazon Athena 的集成

集成模式：将数据实时联合至 SAP Datasphere

Amazon Athena 是 Amazon 推出的交互式查询服务，可帮助查询和分析 S3 中的数据。来自 Athena 的非 SAP 数据能够实时联合至 SAP Datasphere 的远程表中，并与 SAP 数据相结合，以便在 SAP Analytics Cloud 中进行实时分析。

以下是将 Athena 与 SAP Datasphere 集成的步骤：

1. 准备包含非 SAP 数据和第三方数据的来源
2. 配置 Athena
3. 配置必要的 IAM 用户和授权
4. 设置 SAP Datasphere 与 Athena 的连接
5. 在 SAP Datasphere 中构建模型

通过此流程，可以进行实时数据联合而无需复制数据，从而降低成本、快速提供见解，并实现企业级安全。有关详细的分步说明，请访问 Federating Queries from SAP Datasphere to Amazon S3 via Amazon Athena。

B. 与 Amazon Redshift 的集成

集成模式：将数据实时联合至 SAP Datasphere

Amazon Redshift 是一项完全托管的 PB 级数据仓库服务，已针对分析工作负载进行优化。通过 SAP Datasphere 的数据联合架构，可将 Redshift 数据与 SAP 数据相结合，以在 SAP Analytics Cloud 中构建统一的数据模型和分析。智能数据集成（SDI）通过 Camel JDBC 适配器连接 SAP Datasphere 与 Redshift，从而支持创建虚拟表以及实时复制或快照复制。

以下是将 Redshift 与 SAP Datasphere 集成的步骤：

1. 在 SAP Datasphere 中创建本地代理
2. 设置 Redshift 访问权限
3. 配置 SAP SDI DP 代理
4. 在 SAP Datasphere 中注册 Camel JDBC 适配器
5. 在 SAP Datasphere 中上传第三方驱动程序
6. 在 SAP Datasphere 中创建与 Redshift 的本地连接
7. 从 Redshift 导入远程表

此设置支持从 SAP Datasphere 向 Redshift 发起实时联合查询，而无需复制数据。优势包括实时访问 Redshift 数据、通过下推查询优化性能，以及避免 SAP Datasphere 中出现数据重复情况。有关详细的分步说明，请访问 Data Federation between SAP Datasphere and Amazon Redshift。

C. 与 Amazon S3 的集成

集成模式：使用复制流复制数据，使用数据流将数据导入 SAP Datasphere

Amazon S3 提供高度可扩展、持久、可用和安全的对象存储服务。S3 存储桶中的非 SAP 数据可通过数据流功能导入 SAP Datasphere，供 SAP Analytics Cloud 中的财务规划或业务分析等应用程序使用。

以下是将 Amazon S3 与 SAP Datasphere 集成的步骤：

1. 在 S3 存储桶中准备源数据
2. 配置必要的 IAM 用户和授权
3. 在 SAP Datasphere 中创建 S3 连接
4. 创建数据流

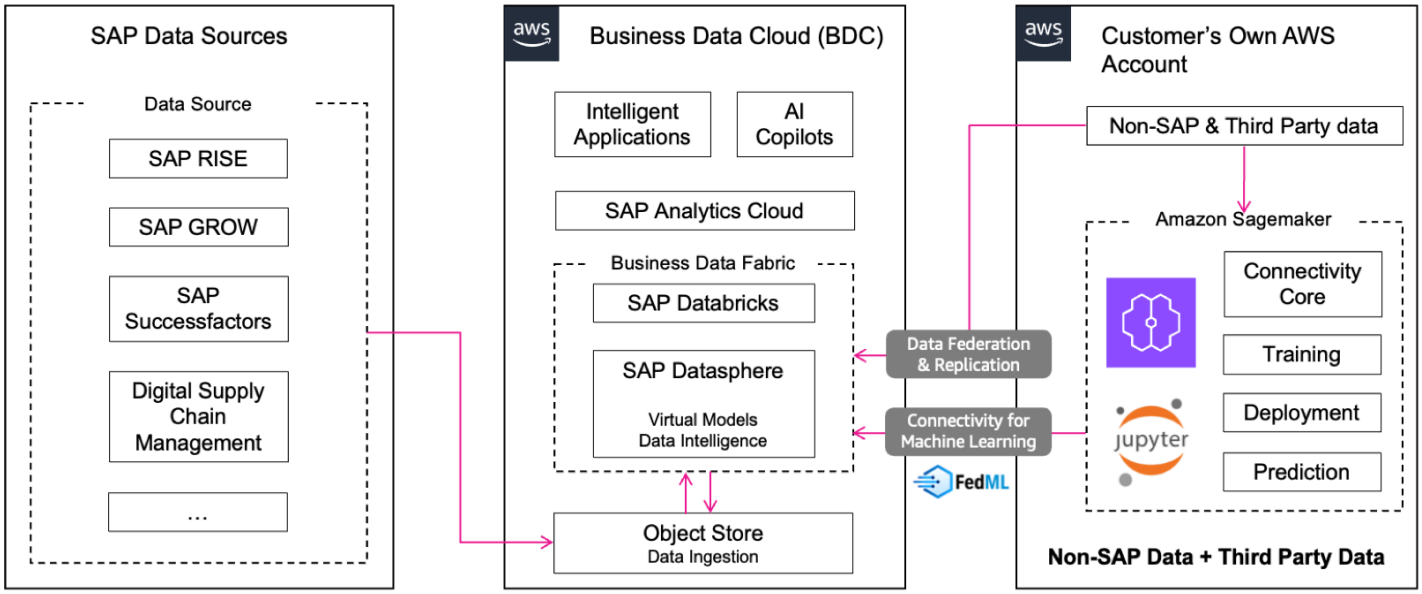
通过此流程，SAP Datasphere 可连接到 S3、访问非 SAP 数据，并借助数据流将这些数据与内部 SAP 数据集结合使用。有关详细的分步说明，请访问 Data integration between SAP Datasphere and in Amazon S3。

你可以在 SAP 架构中心的 “与 AWS 数据源集成” 下找到更多信息。

使用 FedML 和 Sagemaker 进行人工智能创新AWS

在当今数据驱动型企业中，机器学习模型的能力取决于其可访问的数据。然而，业务关键型数据通常存储在 SAP BDC 等 SAP 系统内，而高级模型开发通常在 Amazon SageMaker 等云原生平台上进行。

FedML-fo AWS r Amazon Sagemaker 通过为跨SAP和生态系统的联合模型训练和部署提供安全、高效和统一的框架来弥合这一差距。 AWS 通过消除数据重复并实现对 SAP 数据的实时访问，FedML-AWS 有助于加快 AI 计划，确保数据治理，降低运营复杂性，同时利用 SAP 的可扩展性、性能 AWS 和业务环境。FedML-只需最少的设置，AWS 即可在 SAP 和 AWS 环境中进行数据发现、模型训练和部署，从而从数据中提取价值。



FedML 是一个 Python 库，可直接导入 Amazon SageMaker Notebook 实例中。当大多数训练数据驻留在里面 AWS，但训练也需要具有业务语义的关键 SAP 数据时，它会通过 Python/SQLDBC 连接安全地连接到 SAP Datasphere（BDC 的一部分），从而可以联合访问在 Sagemaker 中进行模型训练所需的 SAP 业务数据。

有关用于从 SAP Datasphere（属于 BDC 的一部分）读取训练数据，并在 Amazon SageMaker 上使用机器学习模型训练该数据的方法的更多技术详细信息，请访问 FedML-AWS。你可以在 SAP 架构中心的 A AWS mazon Sagemaker 与 FedML 集成下找到更多信息。

通过将 SAP 业务数据云 (BDC) 和 AWS 服务的优势相结合，组织可以充分发挥其企业数据的潜力。从操作系统到高级人工智能和分析，无论是协调跨亚马逊 S3、Redshift 和 Athena 的数据集，还是使用 FedML 和 Amazon Sagemaker 实现联合模型训练，这些架构都为创新提供了可扩展AWS 且安全的基础。SAP 和 SAP 共同 AWS 使企业能够从数据孤岛转向数据驱动的智能，从而缩短获得洞察的时间，优化决策，并在整个企业中推动可衡量的业务价值。

人工智能

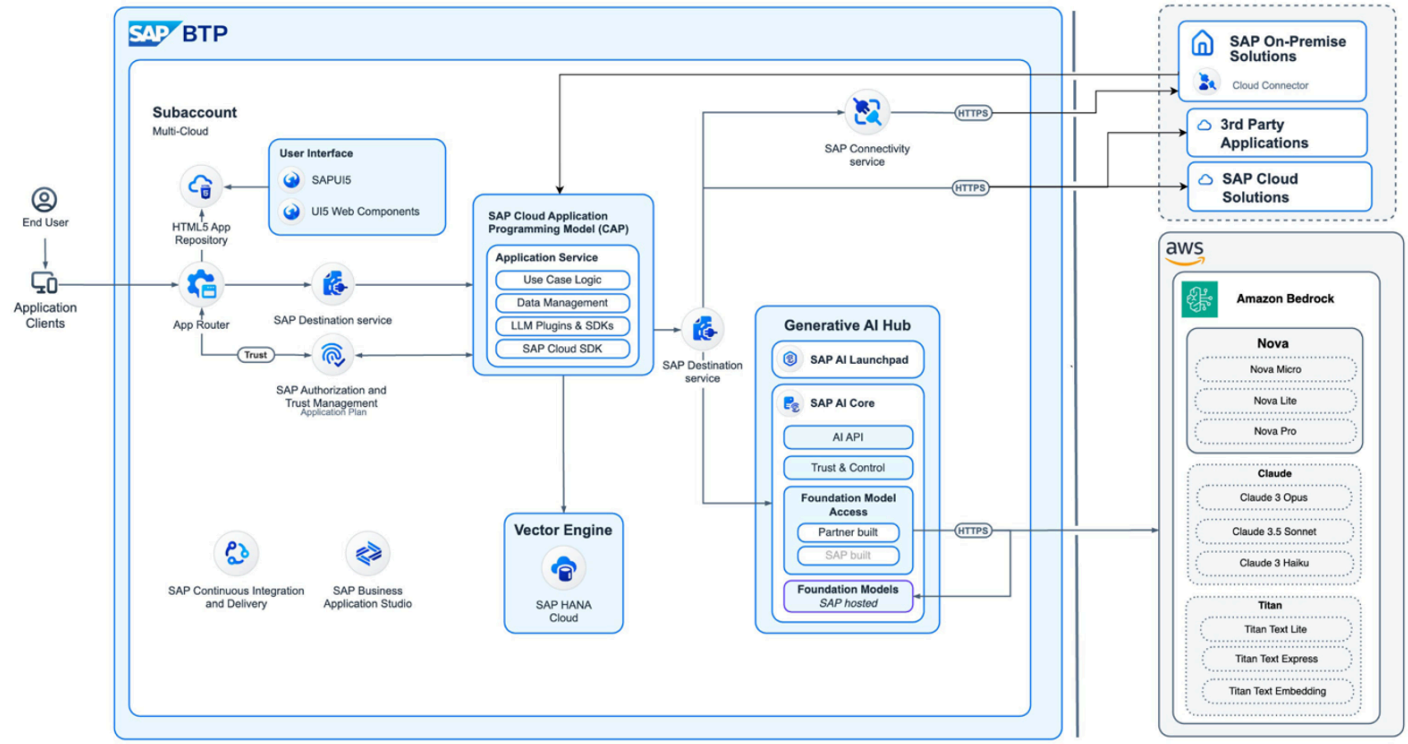
Amazon Bedrock 与 SAP Generative AI Hub 通过联合参考架构（JRA）进行整合，为 RISE with SAP 环境提供企业级人工智能功能。该集成既满足了智能流程自动化的需求，又遵循了系统安全性原则与 clean core 原则。

Amazon Bedrock 充当基础人工智能服务层，提供对多种基础模型（包括 Anthropic Claude 和 Amazon Nova）的托管访问。借助此服务，组织可使用专有数据对这些模型进行微调，并在安全的计算环境内实现检索增强生成（RAG）。

SAP Generative AI Hub 通过提供企业特定的治理与控制机制，对上述基础进行补充。该中心可管理模型选择、知识库索引编制与检索操作，同时实施必要的安全护栏与风险控制措施。这可确保人工智能部署始终符合企业标准与业务要求。

在本文档中，我们将重点介绍JRA方面，因为这些组件创建了一个强大的框架，用于在SAP流程和 AWS 服务（从客户订单管理到生产设计）中实现人工智能功能，同时保持企业安全性和可靠性标准。

生成式人工智能中的 AWS-SAP 联合参考架构



该架构中的关键组件：

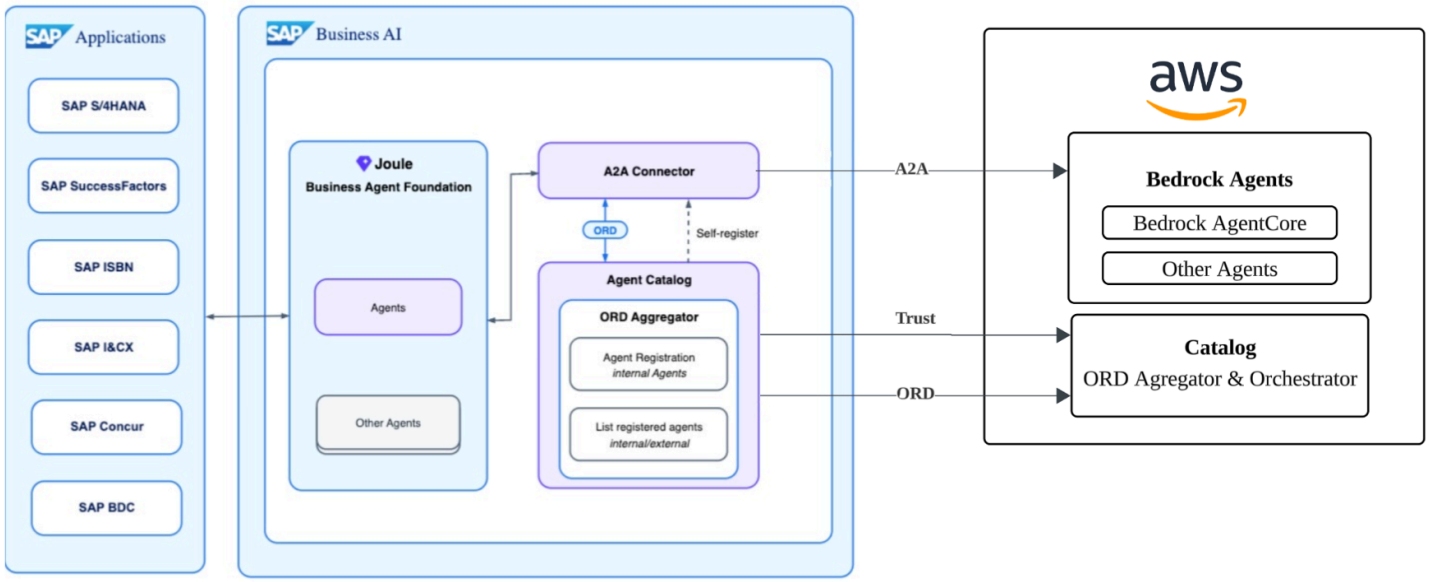
- Amazon Bedrock 是一项通过 API 接口提供对各种基础模型 (FMs) 的访问的服务。它采用亚马逊泰坦、Amazon Nova 和Ant hropic Claude 等机型，它们是 FMs 具有行业领先性价比的全新一代机型。并且用途广泛，可满足多种不同的应用场景的需求。
- 带有生成式人工智能中心的 SAP AI Core 可让客户访问人工智能功能 FMs，包括 SAP BTP 应用程序并提供标准化接口。它充当管理层，用于控制对 Bedrock 的访问并创建端点供应用程序使用 FMs。Generative AI Hub 实施集中式安全控制措施和风险缓解措施，确保企业人工智能部署安全且合规。有关 SAP 的 Generative AI Hub 通过 Bedrock 支持的模型的更多详细信息，请参阅 SAP Note 3437766。
- 将 SAP HANA Cloud 用作数据库管理平台，其向量引擎支持 RAG 实现，通过高效查找并获取与特定问题或任务相关的业务文档，为基础能力提供支持。这些信息随后会用作基础模型的上下文，提升该模型提供准确且贴合具体场景的响应的能力。

- SAP Cloud Application Programming (CAP) 模型是一类开发框架，可提供适用于企业服务和应用程序的结构化方法。CAP 通过提供带有 SAP UI5 前端的集成框架来简化开发。
- SAP Identity Provisioning Services 用于身份验证与访问管理，确保这些人工智能功能的安全交付。

上图说明了通过 SAP Generative AI Hub 使用 Amazon Bedrock 的人工智能功能的参考架构。利用此架构，SAP 工作负载现在可借助基础模型得到补充，充分发挥 SAP 数据的价值，最终以更低成本优化业务见解并提升运营效率。

您可以在 SAP Architecture Center 的 Generative AI and SAP BTP 下找到更多信息。

Agent2Agent 中的 AWS-SAP 联合参考架构



该架构中的关键组件：

- Amazon Bedrock Agen ts 是一项服务，它提供基础模型的推理能力， APIs 以及用于分解用户请求、收集相关信息并高效完成任务的数据。借助其多代理协作功能，开发人员可构建、部署和管理多个专业代理，这些代理能够无缝协作以应对日益复杂的业务工作流。
- Amazon Bedrock AgentCore 使您能够安全、大规模地部署和操作功能强大的 AI 代理。 AgentCore 服务可以一起使用，也可以独立使用，可与任何框架配合使用，包括 Crewal、 LangGraph LlamaIndex、和 Strands Agents，以及 Amazon Bedrock 内外的任何基础模型，为您提供极大的灵活性。 AgentCore 消除了构建专业代理基础设施的无差别繁重的工作，因此您可以加快代理的生产速度。

您可以在 SAP Architecture Center 的 Agent2Agent (A2A) Interoperability in Enterprise AI 下找到更多信息。

集成

在 RISE with SAP 环境中，SAP Business Technology Platform（BTP）（尤其是 SAP Integration Suite）通常用于推动各类集成场景的实现。该服务能够支持 SAP 生态系统内跨云环境、本地环境及混合环境的集成。

SAP Integration Suite 有两种部署方案

A. 标准部署

在 SAP 集成套件中，集成开发人员创建集成流程和应用程序编程接口 (APIs)。创建完成的集成内容与 API 内容会部署至 SAP Integration Suite 的运行时环境。部署完成后，集成内容（例如，一组集成流）即进入可用状态，能够支持与其连接的发送方系统和接收方系统之间的数据交换。

B. 使用 Edge Integration Cell 的混合部署

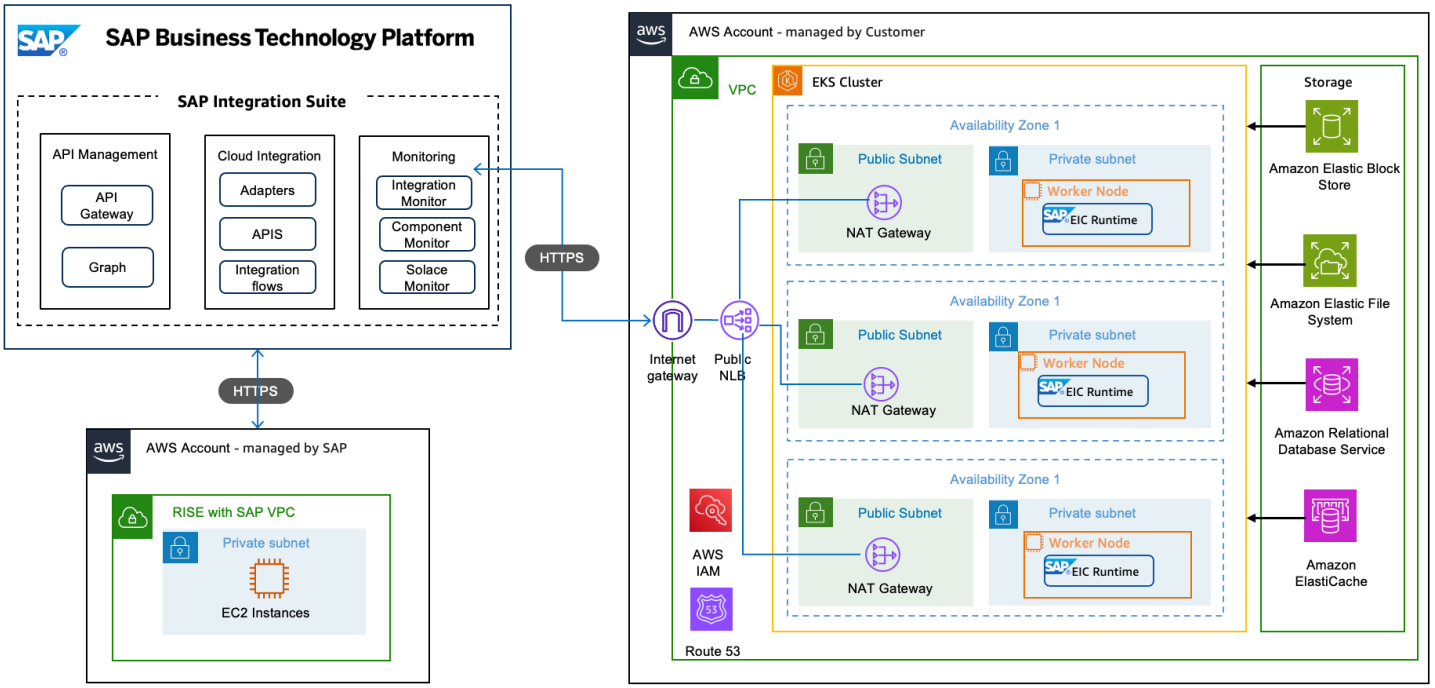
Edge Integration Cell 是作为 SAP 集成套件的一部分提供的可选混合集成运行时，它使您能够在私有环境中 APIs 管理和运行集成方案。Edge Integration Cell 的混合部署模型不仅可让您在云中设计和监控集成内容，还可让您在私有环境中部署和运行集成内容。其运行时环境以 Kubernetes 容器形式实现，有助于实现安全的内部数据交换。

有关更多详细信息，您可以参阅 SAP Note 3426066 FAQ: Edge Integration Cell simple questions 和 SAP Note 3391207 SAP Integration Suite : restrictions for the Edge Integration Cell。

在 AWS 上部署 Edge Integration Cell

可以部署边缘集成单元 (EIC)， AWS 以利用其可扩展的基础架构，同时在客户管理的环境中保持安全和受控的执行。该架构将 AWS原生服务与 EIC 的混合功能相结合，确保了无缝集成体验。边缘集成单元 AWS 可以部署在标准或高可用性 (HA) 架构中。

你可以在这个 sap-samples github 链接中参考详细的 EIC 架构、SAP AWS 先决条件和先决条件。



关键组件

- Edge Integration Cell 是一个统一的运行时管道，由以下关键组件组成：
  - Worker 是 Integration Suite 的基于 Camel 的运行时，用于执行集成流。
  - 策略引擎是基于 Envoy 的运行时，包含 SAP 构建的扩展，可对 API 代理执行安全或流量管理等策略。
- 消息服务基于 JMS 协议实施异步集成模式。对于云产品，此实例由 SAP 管理。
- PostgreSQL 数据库是用于存储结构化数据的关系数据库系统，在公有云产品中由 SAP 管理。
- Redis 是用于缓存的内存中数据存储。

Edge Integration Cell 大小调整

下文详述了 Edge Integration Cell（EIC）的最小大小。有关基于场景的更详细的大小调整，您可以参阅 SAP Notes 3247839 和 Edge Integration Cell 大小调整指南。

Worker 节点的大小调整：高可用性（HA）和非 HA（代理或 Worker 节点）的最低 CPU 和内存要求

部署类型	CPU/内存	持久性存储
非 HA	8 vCPU/32 GiB（m6a.2 xlarge）	101 GiB 的亚马逊 EBS GP3

部署类型	CPU/内存	持久性存储
HA	16 vCPU/64 GiB（m6a.4 xlarge）	204 GiB 的亚马逊 GP3

HA 和非 HA 配置中至少需要 3 个 Worker 节点。

外部存储：HA 场景下的 Postgres 和 Redis 的最小大小

数据库	CPU/内存	持久性存储
Postgres	1 CPU/2 GiB（db.t2.small）	50 GiB 的 EBS GP3
Redis	1 CPU/1 GiB（cache.t2.small）	不适用

定价示例 - 在最低配置下，我们计算出在 us-east-1 区域部署 SAP Edge Integration Cell 的月度指示性成本（以美元计）如下：

负载均衡器 (NLB)，每小时 10GB 数据 = 60.23 美元 Amazon EKS 集群 = 73.00 美元三个工作节点 m6a.2xlarge = 421.75 美元（3 年无预付 EC2 实例储蓄计划）RDS PostgreSQL 多可用区 = 104.21 美元 Redis = 24.82 美元 ElastiCache

在 HA 模式下运行 EIC 的总费用约为 684 美元，计入 AWS 客户管理的账户。

您可以在 SAP Architecture Center 的 Edge Integration Cell on AWS 下找到更多信息。

自定义应用程序

定制应用程序由客户创建，旨在解决其独特的业务需求和 off-the-shelf软件解决方案无法完全满足的挑战。组织通常需要特定的功能、工作流或集成，以便与其业务流程、行业法规或竞争优势精准匹配。通过开发自定义应用程序，组织可完全管控其软件的功能、安全要求和用户体验，同时确保实现与其现有系统及数据库的无缝集成。此外，自定义应用程序还可让组织快速适应不断变化的市场环境，并随着业务发展扩展解决方案的规模，最终为组织提供定制工具，帮助企业提升运营效率并实现战略目标。

在开发将与 SAP 系统交互的自定义应用程序时，务必遵循 SAP 的 clean core 理念，该理念强调，在核心 SAP 系统之外构建扩展功能和自定义项时，需尽力使该系统保持干净。借助此方法，可以更轻松地实施 SAP 更新、升级和创新功能，且不会中断自定义功能，从而确保实现长期可维护性，并降低总拥有成本。通过利用 SAP Business Technology Platform (BTP)、AWS 云服务并遵循简洁的核心原则，组织可以创建 side-by-side扩展、自定义应用程序和集成，以保持系统的稳定性，同时保持灵活性，以适应不断变化的业务需求。此架构策略使组织能够兼顾定制化与标准化优势，确保其应用程序在 SAP 生态系统中保持可持续性和未来适应性。

一些对这个自定义应用程序有帮助的关键 AWS 服务：

- Amazon Simple Notification Service（Amazon SNS）是一项 Web 服务，可用于在云中轻松设置、运行和发送通知。此服务为开发人员提供了一项高度可扩展、灵活且经济高效的功能，可用于从应用程序发布消息，并立即将消息传递给订阅用户或其他应用程序。例如：您可以通过电子邮件发送货物未送达通知，触发基于事件的程序等。
- 使用 Amazon Simple Queue Services（SQS），您可以在软件组件之间以任意卷发送、存储和接收消息，而不会丢失消息或要求其他服务可用。例如：您可以将突发的大量传入消息加入队列以按顺序处理。
- Amazon EventBridge 是一项无需编写代码即可实时访问 AWS 服务、您自己的应用程序和软件即服务 (SaaS) 应用程序中数据变化的服务。例如：当仓库中发生 out-of-stock情况时，您可以通过 API Gateway 触发从 SAP 到外部 SaaS 的基于 near-real-time事件的订购。
- 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。例如：您可借助此库，在 SAP 业务伙伴维护界面中，通过 Amazon Location Service 自动校验邮寄地址信息。
- AWS 人工智能服务，例如：用于将文本转换为逼真语音的 Amazon Polly、用于将语音转换为文本的 Amazon Tran scribe、用于从图像和视频中提取信息和见解的 Ama zon Rekogn ition。
- 有关您可以使用的更多 AWS 服务，请参阅此链接。

通过与 SAP 共同构建的 Amazon Web Services 学习模块，你可以提高自己和团队成员在 SAP BTP 上构建弹性应用程序的 AWS 技能。

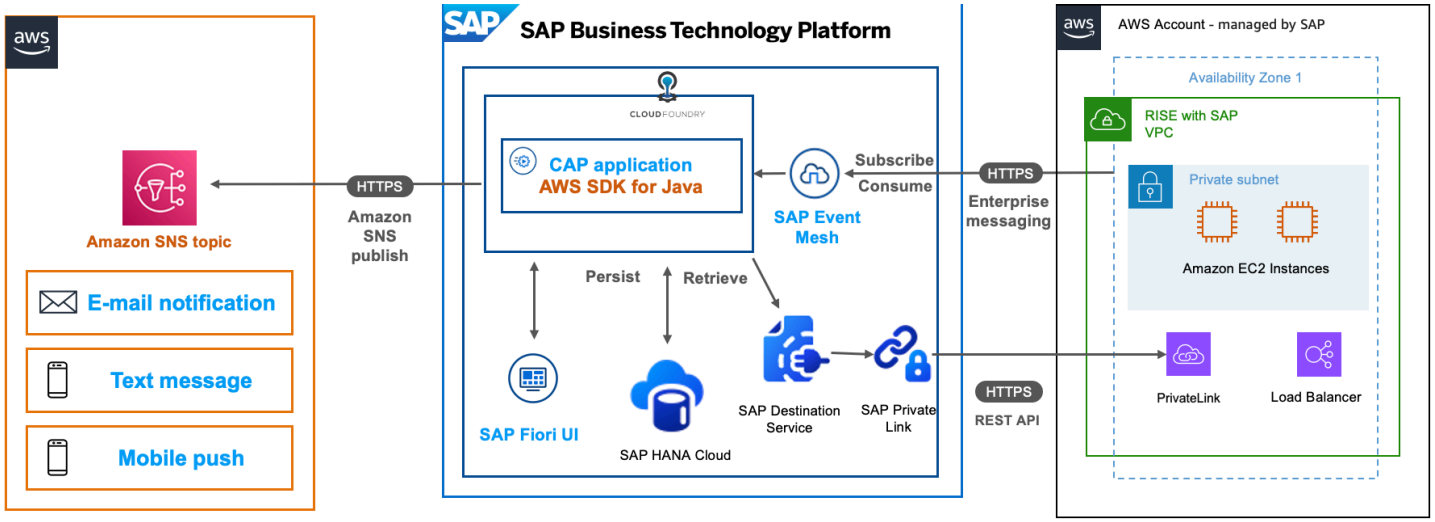
在以下各节中，我们将介绍架构模式和参考架构，它们利用 SAP AWS 和技术扩展 SAP 流程，同时保持核心清洁。

基于事件的应用程序

在传统业务流程架构中，系统通常以孤岛形式运行，采用紧密耦合的组件和僵化的预定义工作流。这种模式很难跟上现代商业环境的动态变化节奏。基于事件的架构作为打破这些限制的方案应运而生，能够应对多项关键挑战。

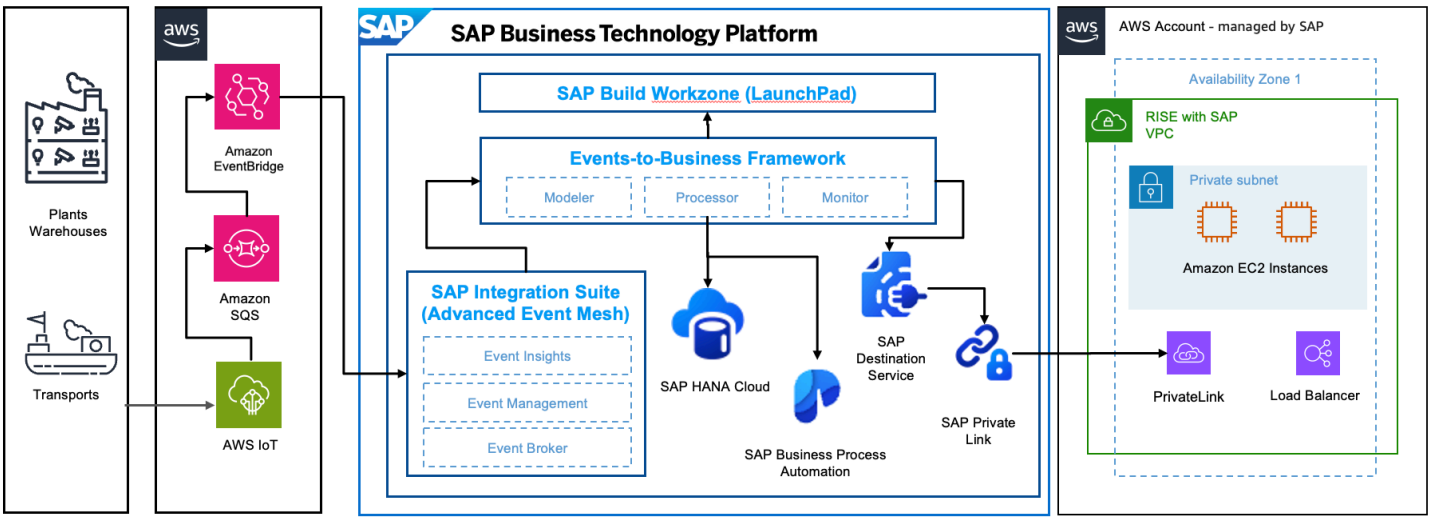
使用基于事件的架构，您可以通过使用异步通信来解耦系统组件，从而实现 end-to-end业务流程。采用这种方法，您能够根据 AWS Well Architected Framework for SAP Lens 构建更具弹性的系统和业务流程，它们能更好地应对网络问题、服务中断及其他中断。

通过 Amazon SNS 发送的基于事件的通知示例：



在上面的架构中，用户在 SAP S/4HANA 中更新业务合作伙伴，您可以通过 SAP Event Mesh 触发更新事件。使用适用于 Java 的 AWS SDK 增强的 CAP 应用程序，可触发 Amazon SNS 主题，使您能够通过电子邮件、短信和移动推送通知将此更改通知数据所有者。您可以在此 github 存储库中找到更多信息。

通过 Amazon SQS 和 EventBridge以及物AWS 联网服务发送基于事件的通知示例：

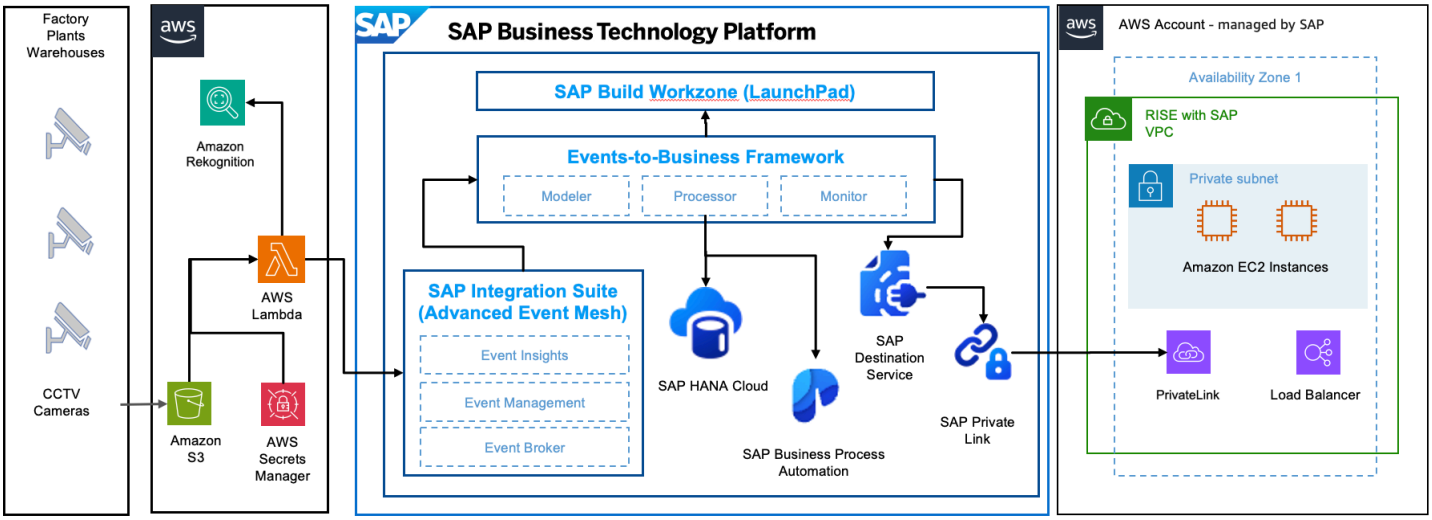


在上面的架构中，事件驱动的集成架构：在工业 4.0 场景中利用 SAP BTP，展示了 SAP AWS 集成的多功能性，可支持预测性维护场景，从而减少生产线的停机时间。这利用 AWS 物联网服务、Amazon SQS 和 A EventBridge mazon 来提供早期的传感器数据，例如速度、温度、振动和其他数据，这些数据将表明在某些机制发生任何中断或停机之前需要进行维护。

人工智能与机器学习应用

每个工作场所的安全隐患都存在多种形式，包括锋利边缘、坠落物体、飞溅火花、化学品、噪音以及其他潜在危险情况。美国职业安全与健康管理局（OSHA）、欧盟委员会等安全监管机构通常要求企业为员工和客户提供个人防护装备（PPE）并确保其规范使用，使其免受可能造成伤害的隐患影响。通过 Amazon Rekognition PPE 检测功能，客户可分析所有场所的本地摄像头拍摄的图像，自动识别图像中的人员是否佩戴了要求的个人防护装备（PPE），例如面部防护用品、手部防护用品和头部防护用品。SAP 客户通过 SAP 环境、健康与安全模块，将这些检测结果手动记录为安全观察结果。

我们在 Amazon Rekognit ion 和 SAP 环境、健康与安全 (EHS) 之间提供了一个集成框架，并采用 Events-to-Business-Actions了开源框架，该框架将自动执行创建安全观察的过程。



在上面的架构中，信息流源自 CCTV 摄像头，该摄像头会捕获工厂内的画面并将其存储到 Amazon S3 中。随后，一个 AWS Lambda 函数会触发 Amazon Rekognition 的 PPE 检测模型，对人员是否合规佩戴安全装备进行检查。如果检测到违规行为，Lambda 函数会从 S AWS ecrets Manager 检索凭证，并与 SAP 集成套件的高级事件网格进行通信。然后，该框架会处理该事件，该 Event-to-Business-Action框架使用 SAP 构建流程自动化的业务规则来确定适当的操作。最后，该系统通过 SAP Destination Service 和 Private Link Service，在 SAP S/4HANA 系统中创建 EHS 事件报告安全观察结果。您可以在此 github 存储库中找到更多信息。

运营可靠性

现代企业在维持 SAP 服务的持续可用性方面面临重大挑战，尤其是在区域中断或维护期间。在部署 SAP Business Technology Platform（SAP BTP）和 RISE with SAP 时，业务连续性和运营可靠性是需要重点关注的问题。

Amazon Route 53 是一项高度可用、可扩展的全球分布式域名系统（DNS）Web 服务，能够高效应对这些挑战。它可让客户为其 SAP 环境实施 AWS 多区域架构，从而提供强大的容错能力和更高的可靠性。通过利用 Route 53 的功能，企业可以构建具备韧性的 SAP 环境，以满足严苛的可用性要求。此 DNS 服务可与 SAP BTP 服务无缝集成，确保即使在区域中断期间，业务运营也能平稳进行。

在 SAP 场景中理解 Amazon Route 53

Amazon Route 53 充当具备韧性的 SAP 环境的基础组件，能够提供智能 DNS 路由功能。在 SAP BTP 和 RISE with SAP 的场景中，Route 53 能够应对标准可用区（AZ）配置无法单独解决的关键可靠性挑战。虽然 SAP BTP 服务支持在单个区域内进行多AZs 部署，但这种方法仍然容易出现区域范围的故障。Route 53 通过支持跨多个地理区域的流量路由，进一步增强了韧性，从而高效地构建了面向任务关键型 SAP 应用的全球安全网。

Route 53 的架构旨在通过将控制面板功能与数据面板功能分离，最大限度地提升可靠性。数据面板经过专门设计，即便在发生控制面板故障或分区事件等情况时，也能保持静态稳定性。这种架构分离确保 DNS 解析始终具备高可用性，使 Route 53 成为 SAP 环境中灾难恢复场景的理想基础组件。该服务会持续监控端点运行状况，一旦检测到故障，便自动将用户重定向至正常运行的资源。

除了基础失效转移功能外，Route 53 还提供可根据特定业务需求定制的高级路由策略。这些策略包括：基于延迟的路由（将用户定向到延迟最少的端点）、地理位置路由（用于满足数据主权法规要求），以及加权路由（按预设比例分配流量）。对于使用 SAP 服务的全球化企业而言，这些功能可为不同地理区域的用户提供一致的性能与可用性，在维护系统可靠性的同时，提升总体用户体验。

用于实现 SAP BTP 多区域故障恢复能力的 Amazon Route 53 架构

设计完善的多区域架构是通过 Amazon Route 53 构建高弹性 SAP BTP 环境的基础。此方法从地理冗余入手，将关键应用程序组件部署在不同的区域，以消除单点故障。在这个架构中，Route 53 充当智能流量指挥者，持续监控端点的运行状况，并依据可用性与性能指标制定实时路由决策。与 SAP BTP 的自定义域服务集成后，即使在故障转移事件期间流量在区域之间重定向 URLs，Route 53 也能通过一致的方式提供无缝的用户体验。

您可以在 SAP Architecture Center – Architecting Multi-Region Resiliency – Load Balancers 中找到更多信息。

Amazon Route 53 路由选项

Route 53 为 SAP BTP 实施提供了多种路由策略：

- 简单路由：将流量定向到单个资源
- 加权路由：按指定比例在多个资源之间分配流量
- 基于延迟的路由：将用户路由至网络延迟最少的区域
- 失效转移路由：自动从运行状况不佳的主资源重定向至运行正常的辅助资源
- 地理位置路由：根据用户的地理位置定向流量
- 地理位置临近度路由：基于地理位置路由流量，支持可选的偏向性设置
- 多值应答路由：随机选择最多 8 条健康记录作为响应

这些选项可组合使用，以创建符合特定 SAP 环境需求的复杂路由策略。

适用于 SAP 环境的 Amazon Route 53 实施模式

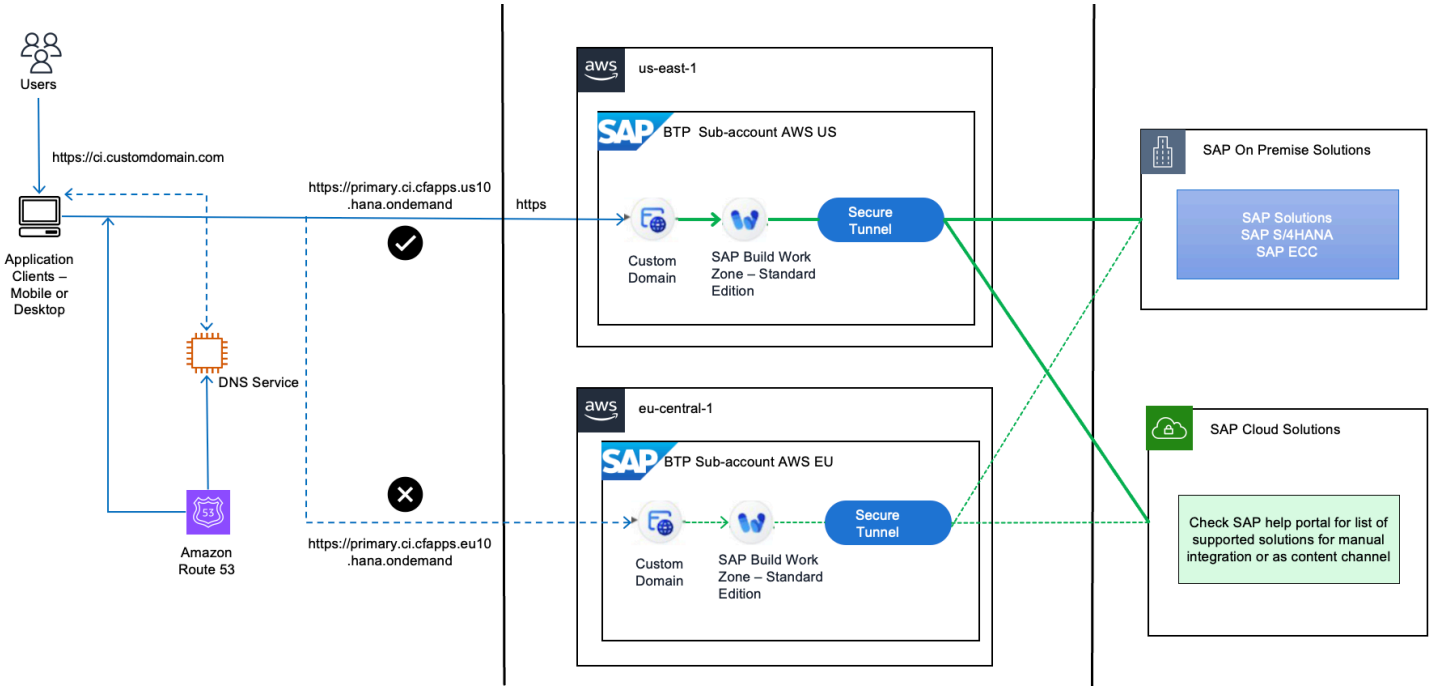
SAP 环境拥有两大实施模式：主动-被动配置和主动-主动配置。

模式 1. 主动-被动实施

在主动-被动配置中，正常运行期间，Route 53 会将所有流量定向至主要 SAP BTP 区域，而辅助区域充当备用区域。此方法兼具简洁性与成本效益，同时仍能提供灾难恢复能力。对于 SAP Build Work Zone 部署而言，主动-被动模式尤为适用，因为该部署中用户体验的一致性至关重要。

您可以通过在主区域种部署包含所有必要配置的 Work Zone 服务，然后使用 SAP Cloud Transport Management 服务，将此设置复制到辅助区域。两个区域都使用 SAP BTP Custom Domain 服务配置了相同的域，而 Route 53 则配置了失效转移路由策略和用于监控主端点的运行状况检查。当主区域中出现问题时，Route 53 会自动将用户重定向到辅助区域，最大限度地减少中断。

TTL 优化直接影响失效转移速度和 DNS 查询量。较短的 TTL 值支持快速失效转移，但会增加 DNS 查询流量。具体的 TTL 值应与恢复点目标（RPO）要求保持一致。有关详细实施步骤，请参阅 SAP blog post Route Multi-Region Traffic to SAP Build Work Zone using Amazon Route 53 以及此 github 存储库。

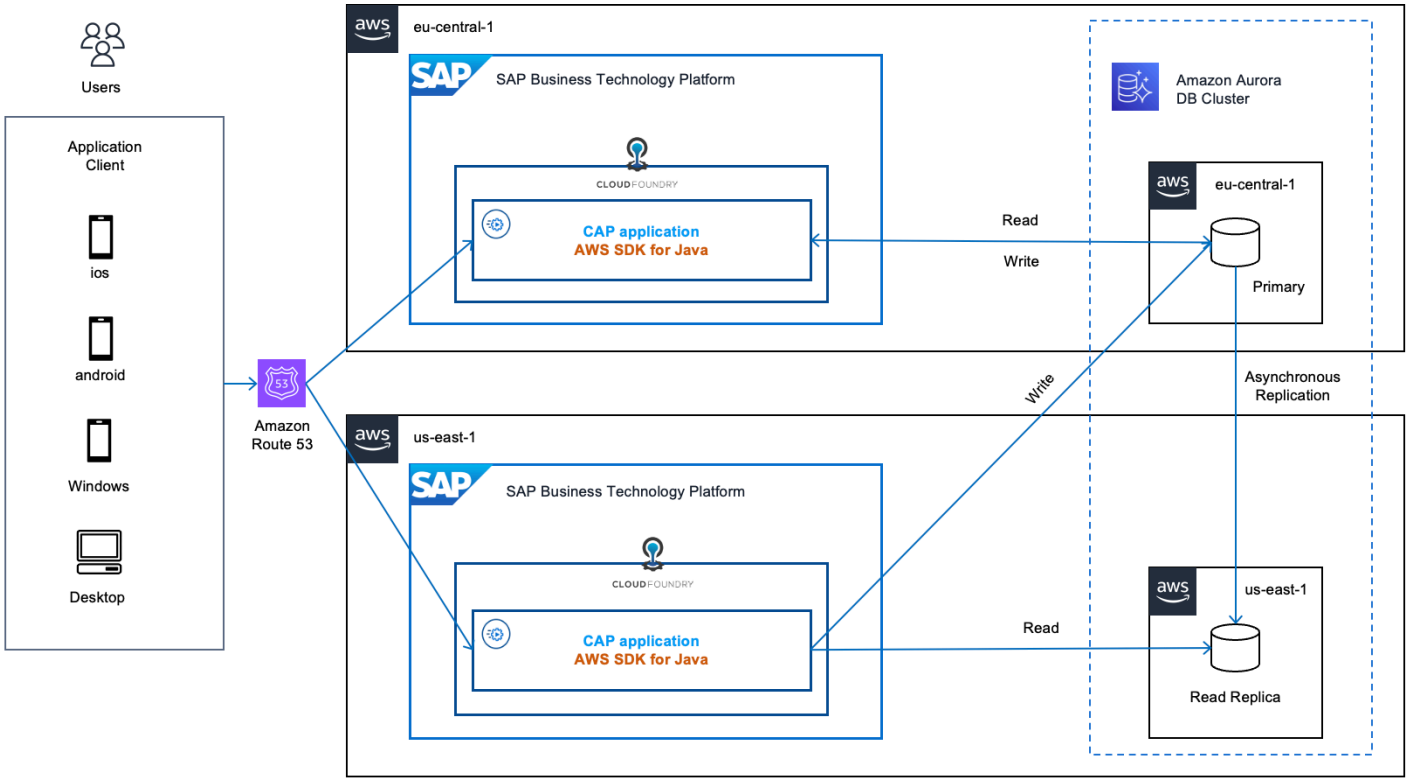


主动-主动实施

主动-主动模式可同时在多个区域间分配流量，既能优化资源利用率，又能最大限度地减小区域故障影响。此方式非常适合用户遍布不同地理位置的全球化企业。在典型的 SAP Cloud Application Programming (CAP) 实施中，会在不同区域的多个 SAP BTP 子账户中部署相同的应用程序，这些应用程序连接至 Amazon Aurora（一个跨多个区域的高性能全球数据库集群）。

通过配置 Aurora 进行 “ local/write 全局读取” 操作来维护数据一致性，将所有写入定向到主区域，同时允许从任何区域进行读取。Route 53 实施基于延迟的路由策略或地理位置路由策略，将用户定向至距离最近的正常运行区域。通过这一设置，不仅能实现对区域中断的故障恢复能力，还能通过降低全球分布的用户的延迟来提升性能。

有关实施详细信息，请参阅 Distributed Resiliency of SAP CAP applications using Amazon Aurora with Amazon Route 53 和 SAP CAP Application Dynamic Data Source Routing。您也可以参考此 github 存储库。



解决方案指南和其他注意事项

每种实施模式都需要仔细考虑数据一致性、身份验证机制和运营流程，以确保在正常运行和失效转移事件期间提供无缝的用户体验。

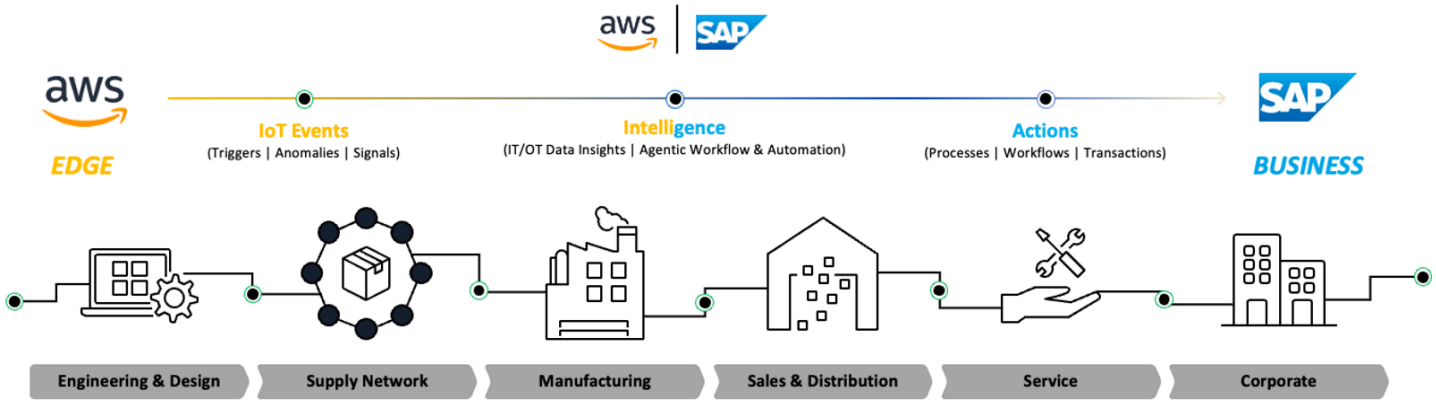
有关更广泛的架构指南，请参阅 SAP BTP 高可用性多区域参考架构和使用 Amazon Route 53 创建灾难恢复机制 AWS的指南。

物联网

物联网（IoT）是指由相互连接的物理设备、交通工具、家用电器及其他物体构成的网络，这些物体中嵌入了电子元件、软件、传感器和网络连接功能，能够实现数据的收集与交换。IoT 通过现有网络基础设施对物体进行远程感知与控制，为物理世界与计算机系统之间的直接集成创造了可能。

AWS 物联网提供了一套全面的服务，用于大规模连接、管理和保护物联网设备。AWS 物联网核心是其基础，可实现安全的设备连接和消息路由。AWS IoT Dev ice Management 可帮助注册、组织、监控和远程管理物联网设备的整个生命周期。AWS IoT Greengrass 将云功能扩展至边缘设备，使这些设备能够在本地对数据进行处理，同时仍保持与云连接。 AWS 物联网系列中的其他补充服务包括 IoT Ev ents、IoT TwinMaker ExpressLink、IoT 和 IoT FleetWise，每种服务都满足特定的物联网用例和要求。

AWS IoT 与 SAP



AWS 物联网服务与SAP业务应用程序的结合为数字化转型创造了一个强大的平台，使组织能够在从互联产品到智慧城市应用等各个领域实施智能解决方案。此集成有助于组织利用实时数据来提升运营可见性、增强客户体验并构建创新性业务模式，进而在整个企业生态系统中提升效率并加速创新。

在智能产品和服务场景中， AWS 物联网服务通过AWS 物联网 SiteWise和其他服务实现智能运营，提供与 SAP 业务模块无缝集成的实时见解。 AWS IoT Device Management 可对联网设备进行全面监控，持续的数据流丰富了 SAP 系统，便于做出明智的决策。 AWS 物联网 Greengrass 提供的边缘计算功能可确保在源头进行高效的数据处理，从而实现快速响应时间和最佳性能，这对于远程操作尤其有价值。

AWS 物联网服务可以与 SAP 业务技术平台 (BTP) 集成，以创建强大的 end-to-end物联网解决方案。通过 SAP BTP 事件驱动架构和企业消息服务，来自 SAP 的物联网数据 AWS 可以被 SAP 应用程序实时高效使用。SAP BTP 中的云应用程序编程 (CAP) 模型支持快速开发支持物联网的业务应用程序，这些应用程序可以处理和处理来自的物联网数据。 AWS可以通过多种方法实现集成，例如使用 SAP 云集成、API 管理或直接 REST APIs。例如，通过 AWS IoT Core 收集的传感器数据可以触发 SAP BTP 中的事件，然后由 CAP 应用程序处理这些事件，以更新业务流程、生成警报或触发 SAP 系统中的自动工作流程。

AWS IoT 安全

在 AWS 维护强大的云安全机制以保护 AWS 物联网与其他 AWS 服务之间的数据移动的同时，客户有责任管理设备证书（包括 X.509 证书、 AWS 凭证、Amazon Cognito 身份、联合身份或自定义身份验证令牌）并实施适当的访问策略。

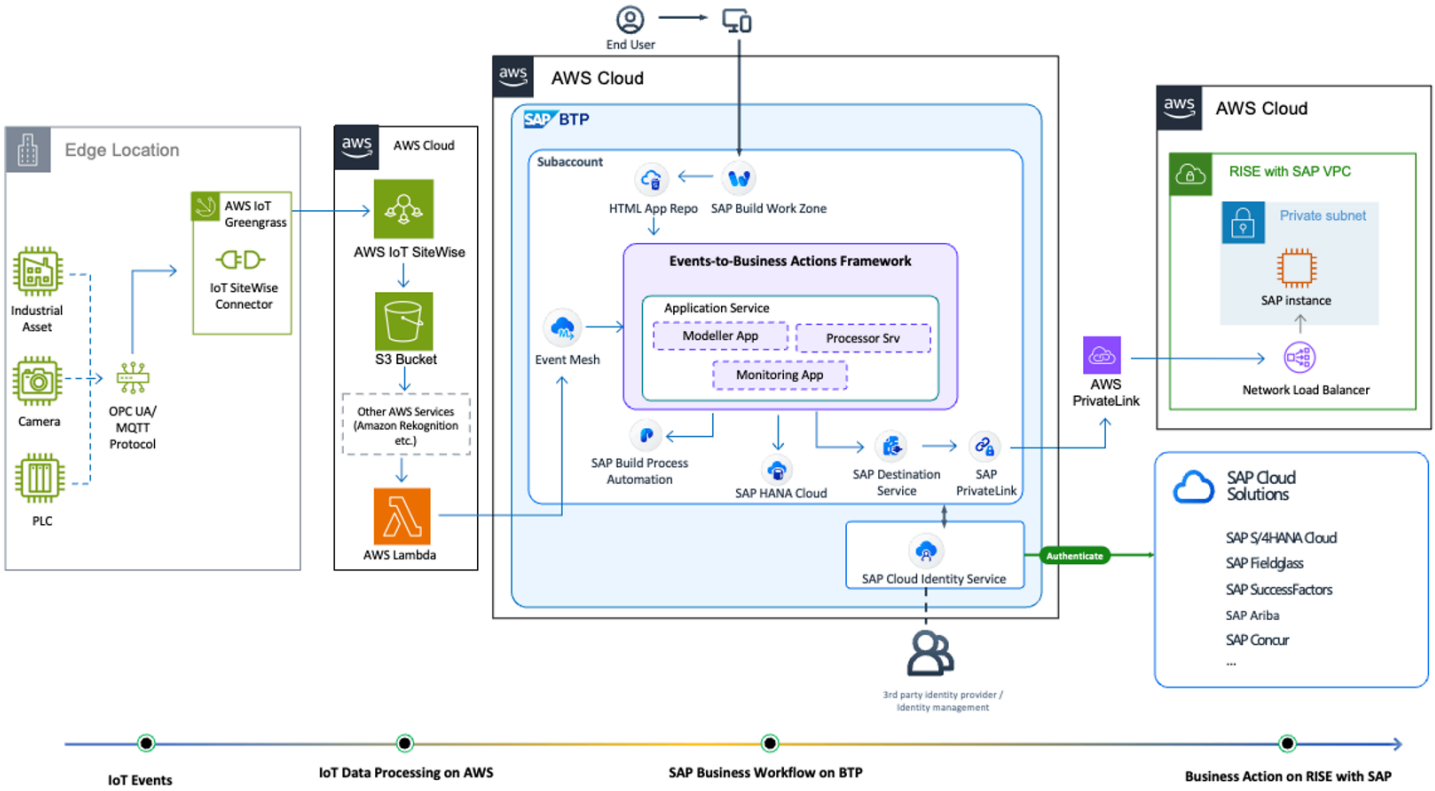
AWS 物联网实施了全面的安全措施，以确保安全的设备连接和数据传输。设备可以使用 X.509 证书或 Amazon C AWS ognito 身份通过传输层安全 (TLS) 连接连接到物联网，其他身份验证选项可用于开发和基于 API 的特定应用程序。 AWS 物联网消息代理通过物 AWS 联网策略处理设备身份验证并管理访问权限，而自定义身份验证可以使用自定义授权方实现。

此外， AWS 物联网规则引擎根据用户定义的规则将设备数据安全地转发到其他设备或 AWS 服务，利用 AWS 身份和访问管理 (IAM) 来确保将数据安全地传输到预期目的地。客户可以利用 AWS IoT Device Defender，这是一项完全托管式服务，可帮助您保护 IoT 设备实例集。

您可以了解有关AWS 物联网安全的更多信息。

适用于物联网的 AWS 与 SAP 联合参考架构

下面的 JRA 架构显示了 AWS 物联网服务和 SAP BTP 服务的组合，用于构建松散耦合 Edge-to-Business的流程架构。



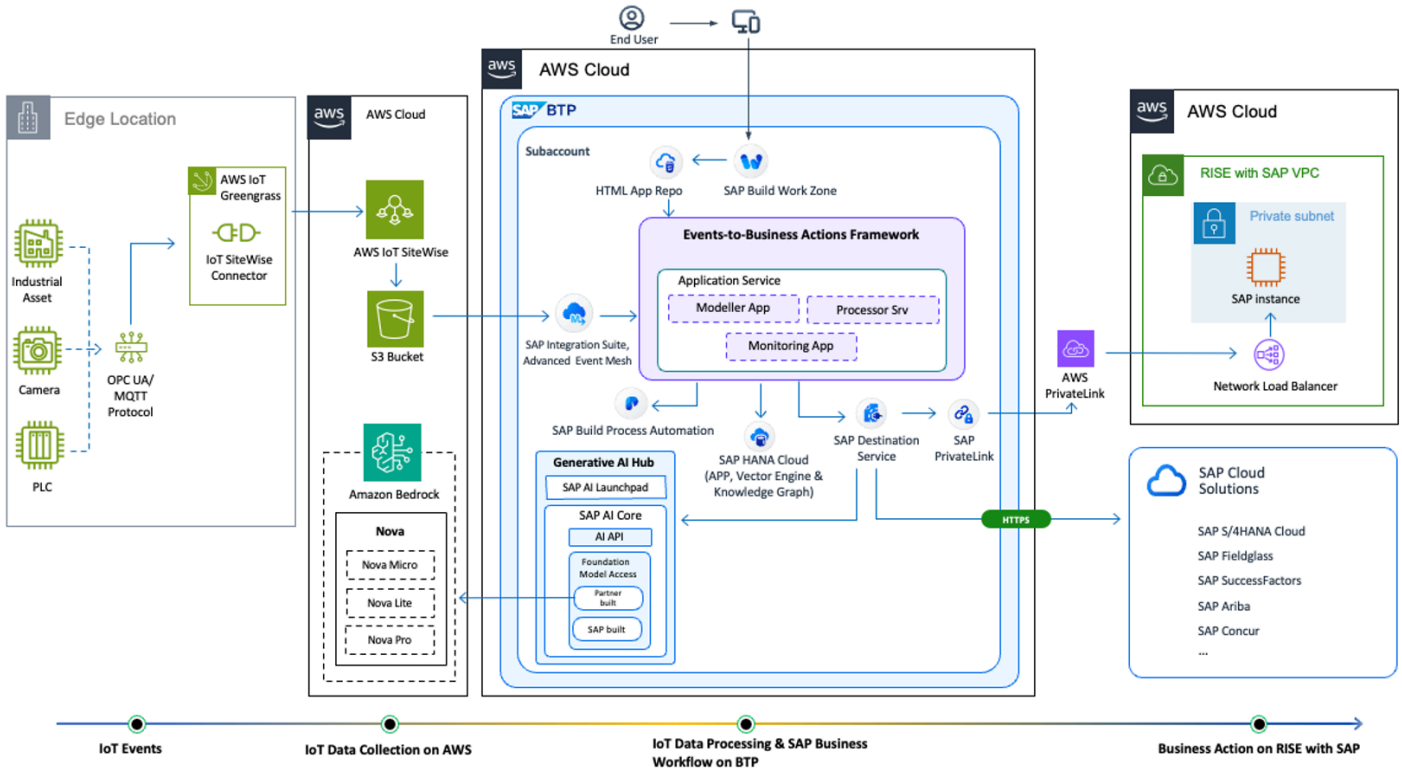
物联网事件-边缘位置可以是像工厂或车间这样的环境，物联网设备（例如摄像头 PLCs、SCADA 系统、物联网传感器或工业资产）收集包括温度、振动和其他指标在内的数据。使用在边缘运行时环境（例如 AWS IoT Greengrass）上运行的相应连接器，使用特定于每种设备类型的协议，将收集的数据传输到云中的 AWS 物联网服务。在传输到云端之前，客户可以选择使用边缘计算服务在 AWS 边缘对数据进行消毒。 AWS 物联网 SiteWise 边缘将云功能扩展到工业边缘环境，而 AWS 物联网 Greengrass 则用作通用边缘框架。这种边缘处理有助于减少数据中的干扰信息、提升数据质量并优化成本。

物联网数据处理开启 AWS ——从边缘位置接收的数据首先由诸如用于计算机视觉用例的 Amazon Rekognition AWS 或其他数据分析 AWS 服务等服务进行处理，其中 IT（信息技术）和 OT（运营技

术）数据洞察相结合，触发智能工作流程自动化。 AWS 然后，Lambda 会向 SAP BTP 触发一个事件，以供下一步采取行动

BTP 上的 SAP 业务工作流程 - 控制权会转移至 SAP BTP 服务（如 Event Mesh），该服务可让应用程序通过异步事件与 Events-to-Business-Actions-Framework 进行通信。此框架能响应来自工业生产流程、仓库等不同来源的事件，并将这些事件集成到企业业务系统中。系统会根据事件的类别与类型，在 SAP 应用程序中触发相应的操作。处理器模块利用 SAP Build Process Automation 的 decisions 功能来启动业务操作，同时还会得到其他 BTP 服务（例如，用于存储应用程序数据的 HANA Cloud）的支持。客户可以通过 SAP Private Link 和AWS PrivateLink 服务在 AWS 环境中利用 SAP BTP 和 SAP RISE 之间的私有连接。

基于 RISE with SAP 的业务操作 - 最后，根据业务规则，会在 RISE with SAP 系统上触发相应的 SAP 业务流程，例如，创建针对预测性维护的维护订单，或创建针对 EHS 的安全观察结果。



这是上一部分中所讨论架构的替代架构，二者存在以下差异。

IoT 事件 - 与图 1 相同。

物联网数据处理开启 AWS — 从边缘位置接收的数据将直接转发到 SAP BTP 层，用于后续操作，包括数据转换。在本例中，我们使用的是 SAP 集成套件，即高级事件网格，它有一个适用于 S3 的 out-of-the-box连接器。

SAP BTP 上的物联网数据处理 — 控制权转移到 SAP BTP 服务，例如 SAP 集成套件、高级事件网格和 Events-to-Business操作框架。SAP BTP上的数据转换是使用GenAI服务进行的，例如生成式人工智能中心，它利用A mazon Nov a等 AWS 生成基础模型从数据中得出见解以供进一步处理。系统会根据处理后的数据、事件类别及类型，在 SAP 应用程序中触发相应的操作。处理器模块是 Events-to-Business-Action框架的一部分，它利用 SAP 构建流程自动化的决策功能来启动业务行动。此外，除了存储应用程序数据外，SAP HANA Cloud 还可用作检索增强生成（RAG）框架和知识图的向量引擎。

这种集成通过将强大的物联网和生成式人工智能功能与SAP的企业业务流程和数据模型相结合 AWS，实现了预测性维护、实时资产监控和供应链优化等场景。

你可以在 SAP 架构中心的 “使用 SAP BTP 和 AWS 物联网 SiteWise构建 Events-to-Business操作场景” 下找到更多信息。

扩展程序

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	使用案例	AWS 服务
性能	具备主动可观测性的 SAP Fiori 与 SAP GUI 访问	亚马逊 CloudFront、加速 Site-to-Site VPN、AWS 互联网监控器
应用程序集成	应用程序集成	AWS Lambda 和 A mazon API Gateway
归档和文档管理	归档和文档管理	Amazon S3、AWS S3 文件网关、Amazon 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 进行的 mTLS 身份验证、适用于 SAP 的AWS 已验证访问

类别	使用案例	AWS 服务
人工智能	生成式人工智能	Amazon Q 企业版、Amazon Quick Sight、Amazon Bedrock

性能

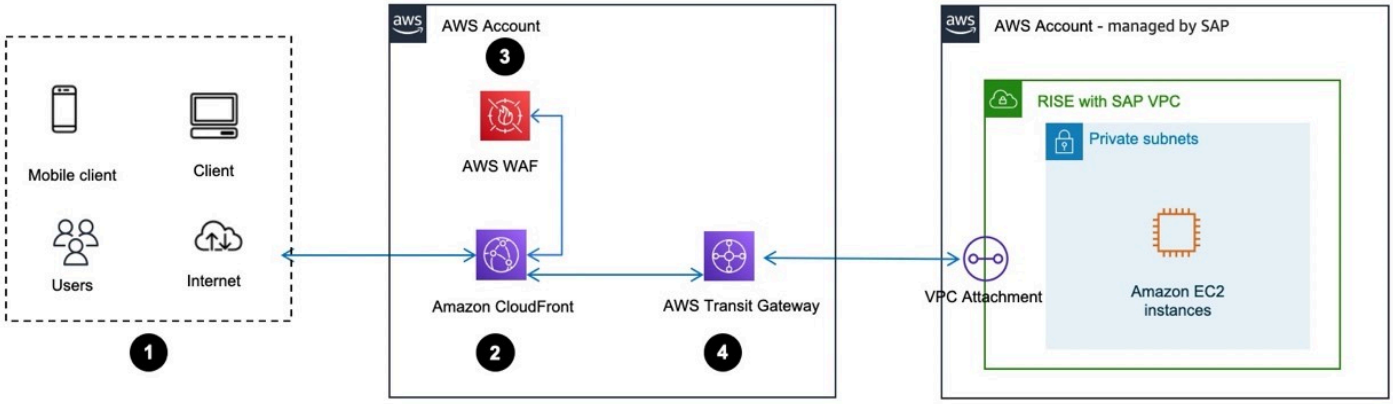
借助亚马逊提高 SAP Fiori 的绩效 CloudFront

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网络应用程序（例如 SAP Fiori）的操作，这些应用程序托管在亚马逊 VPC 的私有子网中。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。

这将通过以下方式增强 SAP 系统的安全态势：

- 避免将 SAP 服务器直接暴露在公共互联网中
- 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。这会限制进入 VPC 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

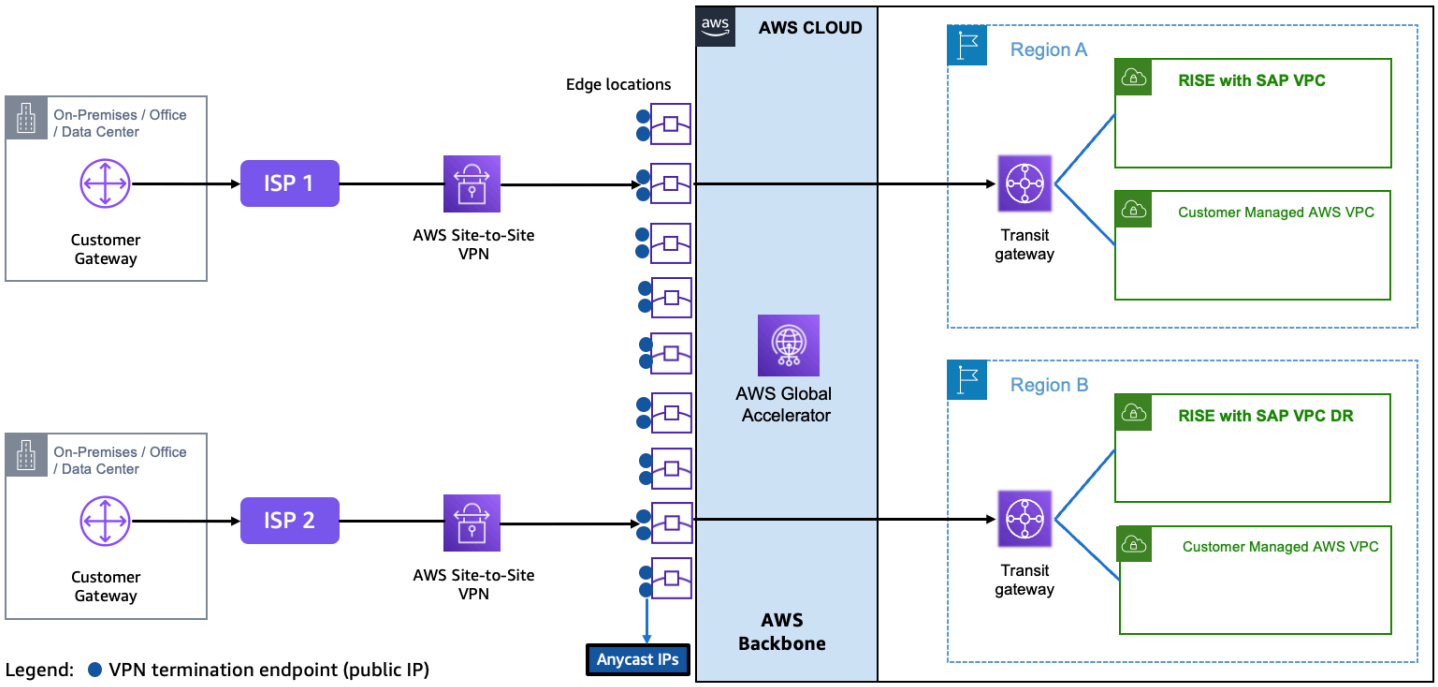
有关更多信息，请参阅 AWS 文档限制使用 VPC 源进行访问。

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。该服务可作为基础组件 Transit Gateway 和 Direct Connect 的补充，应对地理位置分散的用户所面临的性能挑战，并确保高效且安全地访问任务关键型 RISE with SAP。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。通过这种方式，可绕过公共互联网跃点，为全球分布的用户提供无拥塞路由，从而减少延迟（最多减少 75%，因位置而异）。

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。该服务能深入分析延迟增加、数据包丢失或区域连接中断等问题，帮助组织在这些问题影响 SAP 工作负载之前主动应对潜在中断。

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

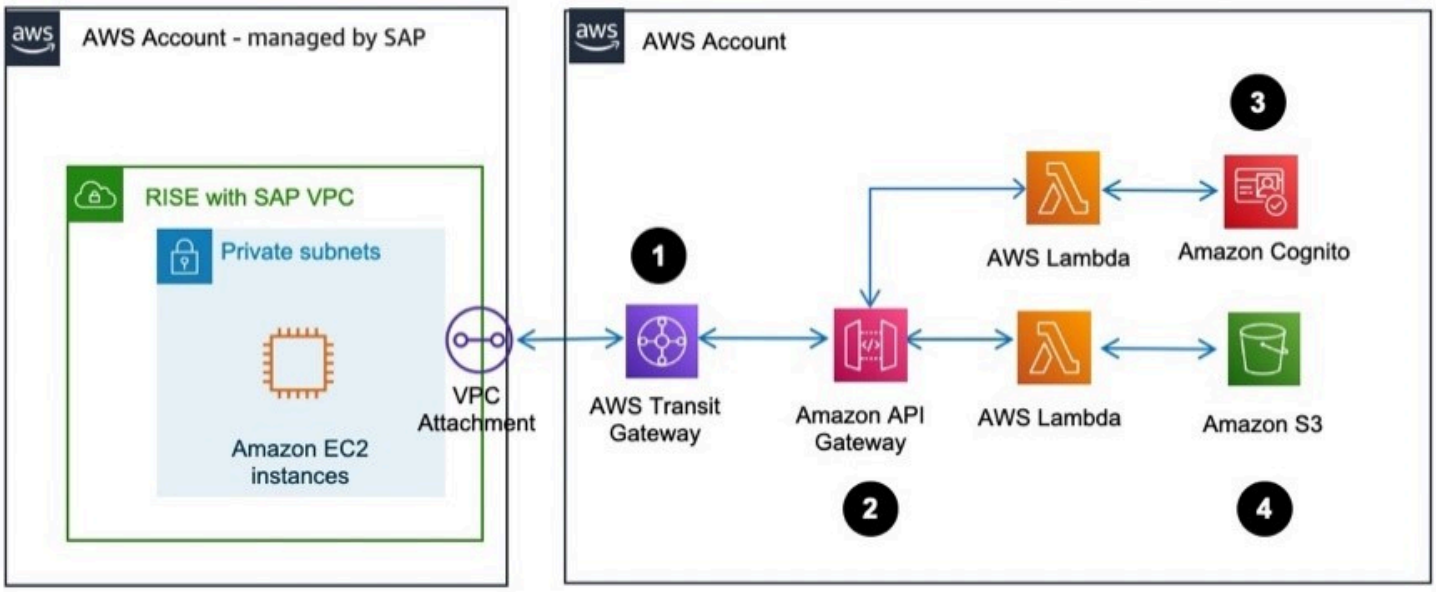
- 识别影响 SAP 响应时间的 ISP 或区域网络中断。
- 提供早期预警和可执行的建议，以缓解与网络相关的服务降级。

- 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、丢包和拥塞问题。

要做到这一点，您可以参阅“开始使用网络监测仪”。

应用程序集成

部署 Amazon API Gateway，通过 HTTP API 从 SAP S/4HANA 中提取数据。API Gateway 可使用来自 IDOC、BAPI 和 RFC 的数据。这些数据需转换为 Web 服务调用。有关更多信息，请参阅 AWS 博客。下图说明了此场景。



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 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。

归档和文档管理

无论是迁移到 RISE with SAP 之前还是之后，SAP 数据归档和文件管理系统（DMS）都发挥了至关重要的作用。该系统可帮助企业高效地管理数据库增长并优化总体成本。在迁移到 S/4HANA 之前，归档可通过减少数据量来削减迁移费用、最大限度地减少停机时间并降低风险。在迁移到 S/4HANA 之后，归档有助于控制运营成本并确保实现最佳系统性能。此外，企业可以停用旧式 SAP ECC 系统，消除不必要的开支，并保留对历史数据的访问权限。

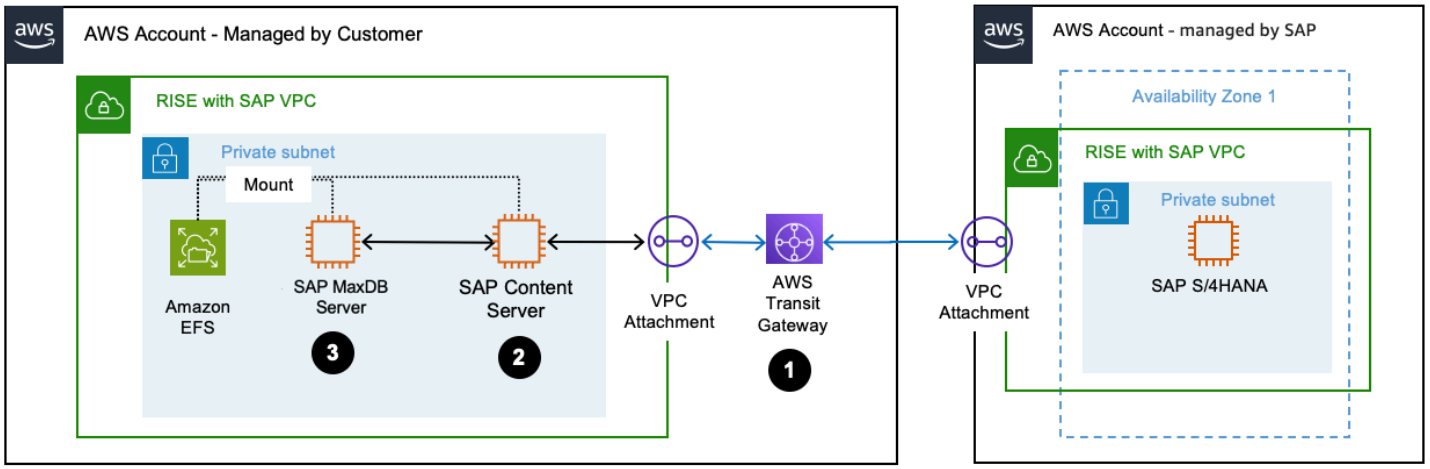
结构化数据的数据归档。数据归档意指将已完结的业务交易数据从运行的 SAP 系统中迁移至离线存储或二级存储中的过程。数据归档的核心在于制定适当的流程与策略以减少人工操作，同时确保符合数据留存的相关法规要求。

非结构化数据的文档管理。数据归档与文档归档的区别在于所归档的数据的类型。文档归档针对的是非结构化数据，例如发票、销售订单、交货单等，这类数据通常以 PDF、Word、Excel 等格式提供。此归档实时进行，可存储在任意内容服务器上，并与相关的 SAP 交易关联。

我们将探讨 SAP 内部的数据归档与文件管理系统的可用选项。

选项 1：在 MaxDB 上运行的 SAP Content Server

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，可用于存储大量不同格式的电子文档。这些文档可安全地存储在一个或多个 SAP MaxDB 实例中，或存储在文件系统内。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。这种方式可确保文档管理与 SAP 业务流程无缝集成，并保留文档的可访问性与合规性。



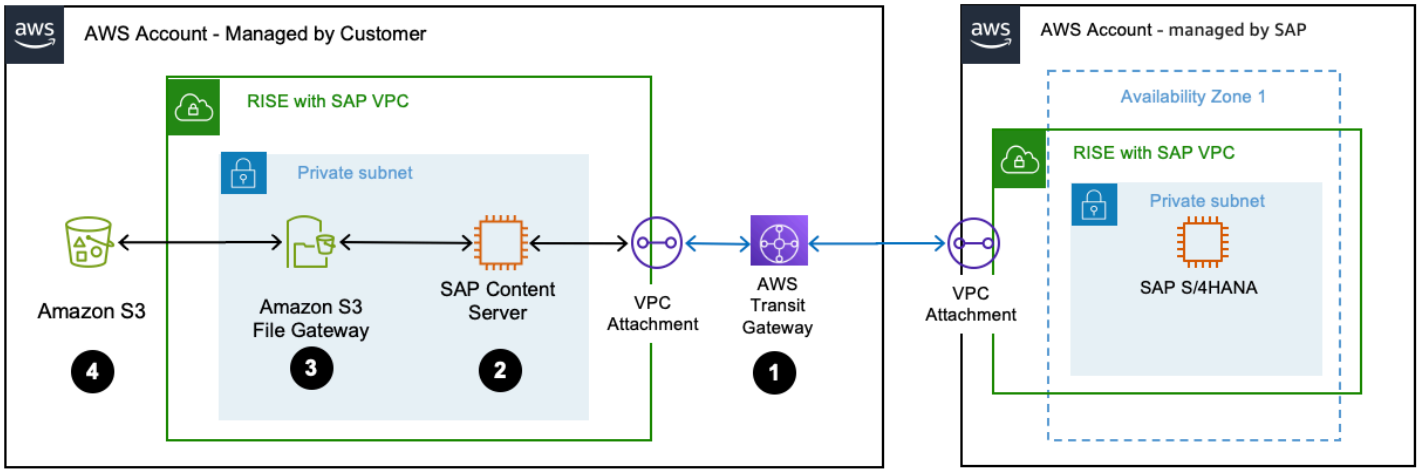
架构说明

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 内容服务器已在您的 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 实现 SAP Content Server 高可用性。对于不常访问的文档，您可以考虑使用 EFS 不频繁访问。

选项 2：Amazon S3 上的 SAP Content Server SAP Content Server 与 Amazon S3 相结合，通过为归档数据提供可扩展且安全的存储来满足 SAP 数据归档需求。它们具备多种特征，例如版本控制、访问控制、不可变性，以及与 SAP 系统的集成。此部分内容适用于满足以下条件的客户：其 SAP 数据库规模持续增长、寻求提升性能、计划降低存储成本，或需要满足其 SAP 环境中长期数据留存的合规要求。

下图说明了与 Amazon S3 集成的 SAP Content Server。



架构说明

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 内容服务器已在您的 AWS 帐户中设置，并配置为用作数据存档的目的地。
3. SAP Content Server 可与 Amazon S3 文件网关集成来充当存储网关，为基于文件的存储提供支持。S3 文件网关支持将 Amazon S3 挂载为网络文件系统（NFS）。
4. Amazon S3 存储桶存储必要的归档文件。您可以使用 S3 生命周期配置管理对象的生命周期。要加强数据保护或实现监管合规性，您可以实施采用 S3 对象锁定的保留策略。您可以使用自动化生命周期管理功能将文件移动到其他 S3 存储类别。有关更多信息，请参阅使用 Amazon S3 存储类别。

SAP Content Server 与 Amazon S3 配合使用，提供了一种将归档数据传输到长期 S3 存储（例如 Amazon S3 Glacier）的机制。随后，可以使用 SAP 的标准归档读取程序访问这些归档数据。

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。这些库可增强集成能力，并提供了更先进的功能，以便在 SAP 环境内直接管理和访问归档数据。对于使用 SAP Information Lifecycle Management（ILM）来管理数据留存和治理的组织，可了解 Syntax Cxlink for ILM 如何通过将 Amazon S3 用作 SAP ILM 的二级存储解决方案来优化 ILM 策略。通过此方法，不仅能充分利用云存储的可扩展性与成本效益，而且能保留 SAP ILM 强大的数据管理能力。

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）。它可确保符合监管要求，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

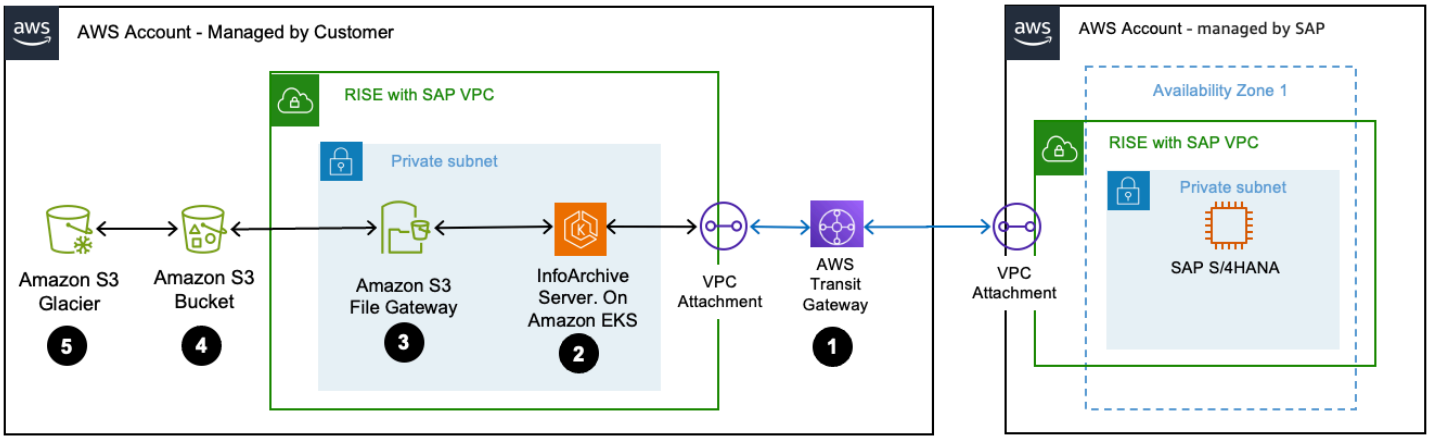
OpenText InfoArchive 是一种现代存档解决方案和基于云的服务，用于对结构化和非结构化信息进行合规存档，具有高度可访问性、可扩展性和经济性。它是一个集中式平台，可为非结构化内容提供灵活的存储选项，包括 Amazon Simple Storage Service（Amazon S3）上的存储。InfoArchive 上 AWS 的 Cloud Edition 以客户部署的形式提供，也可以在上 OpenText AWS运行作为托管解决方案提供。

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。它附带预构建的 SAP 视图。

主要功能

1. 应用程序停用 - 停用旧式应用程序，同时确保数据可访问。
2. 结构化数据和非结构化数据存档 - 存储文档、电子邮件、记录和数据库。
3. 多系统支持 - 可与 SAP、Oracle、Salesforce、Microsoft 和自定义应用程序配合使用。
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 marketplace 进行购买。



架构说明

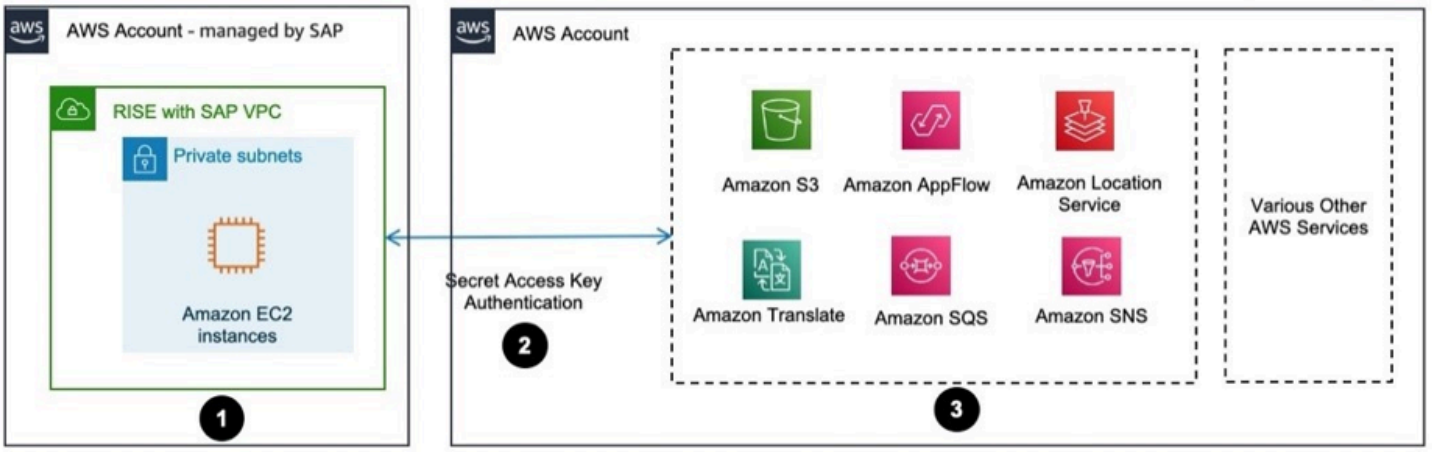
1. 带有 SAP VPC 的 RISE 通过 Tr AWS ansit Gateway 连接到你的 AWS 账户。
2. OpenText InfoArchive on 部署在 AWS 您的账户 AWS中的亚马逊 Elastic Kubernetes Service (Amazon EKS) 上，并配置为用作数据存档的目的地。
3. OpenText InfoArchive 与 Amazon S3 文件网关集成，后者充当存储网关，便于基于文件的存储。S3 文件网关支持将 Amazon S3 挂载为网络文件系统（NFS）。
4. Amazon S3 存储桶存储必要的归档文件。您可以使用 S3 生命周期配置管理对象的生命周期。要加强数据保护或实现监管合规性，您可以实施采用 S3 对象锁定的保留策略。
5. 可以将旧文档移至 Amazon S3 Glacier 以进行长期归档。
6. 您可以使用自动化生命周期管理功能将文件移动到其他 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。下图说明了此场景。



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。

兼容包和替代方案

兼容包（CP）是 SAP 在 2016 年推出的、用于在 S/4HANA 中使用经典功能的临时使用权。它包含在每份 SAP S/4HANA 合约中（无论是本地还是私有云版本）。推出兼容包的目的是，确保现有 SAP 客户能平稳过渡，并为最终确定新的简化应用架构争取时间。

在从 SAP Business Suite 过渡至 SAP S/4HANA 的过程中，业务功能将通过以下路径迁移。有关更多信息，请参阅 presentation by Michael Deller (SAP) and Roland Hamm (SAP)。

在 SAP Note 2269324 中，SAP 定义了类别，帮助组织制定其兼容包策略。这些类别可为组织从 SAP Business Suite 过渡至 SAP S/4HANA 的决策提供指导。

- 存在替代方案
- 存在含路线图的替代方案 - 存在可提供核心功能的替代方案；全面覆盖计划已纳入路线图
- 计划推出替代方案 - 开发范围和时间线的规划工作正在进行中
- 未计划推出替代方案 - 2025 年后无提供替代方案的意向或计划
- 澄清 - 策略澄清工作正在进行中

如何 AWS 帮助客户寻找替代品？

组织应评估其当前的 SAP 环境，并结合 SAP 兼容包的到期日期与可用替代方案，制定过渡策略。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。此方法与 AWS 重构和重新架构迁移策略相符，该策略侧重于重新设计应用程序与流程。具体细节如下：

- 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

双向传输层安全（mTLS）身份验证可在客户端与服务器之间建立安全的双向加密连接。与仅要求服务器提供证书的标准 TLS 不同，mTLS 要求客户端与服务器都提供数字证书。

mTLS 身份验证流程分为四个步骤：

1. 客户端向服务器发起连接请求
2. 服务器提供其证书
3. 客户端验证服务器的证书
4. 客户端提供其证书以供服务器进行验证和认证

为什么要为 SAP 系统实施 mTLS 身份验证

为 SAP 系统实施双向 TLS（mTLS）身份验证将能增强安全性、改进用户体验并减少运维开销。它可实现用户身份验证架构的现代化，为数字化转型提供支持，同时确保符合安全标准。mTLS 能够满足 SAP 环境中的以下安全要求：

1. 增强安全性：mTLS 支持双向身份验证，确保客户端与服务器双方均验证彼此身份。这大大降低了未经授权的访问和 man-in-the-middle攻击的风险。
2. 支持单点登录（SSO）的无缝用户体验：mTLS 可与 SSO 解决方案集成，使用户无需重复输入凭证即可访问多个 SAP 应用程序与服务。这将在整个 SAP 生态系统中实现更平稳且更高效的用户体验。
3. 自动化证书轮换：mTLS 支持证书自动化轮换，无需人工干预即可定期更新身份验证凭证，从而增强安全性。这不仅能降低使用过期或受损证书的风险，还能最大限度地减少管理开销。
4. 接口的主体传播：mTLS 可在不同 SAP 接口与系统间实现安全的主体传播。这样就无需使用通用帐户和特权帐户（例如拥有 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. 可扩展性与性能优化：mTLS 可在网络层实施，将身份验证流程从应用服务器卸载，进而提升 SAP 系统的性能与可扩展性。
6. 支持零信任架构：mTLS 与零信任安全模型高度契合，该模型中从不预设信任关系，而是始终进行验证。

通过应用程序负载均衡器进行 mTLS 客户端身份验证

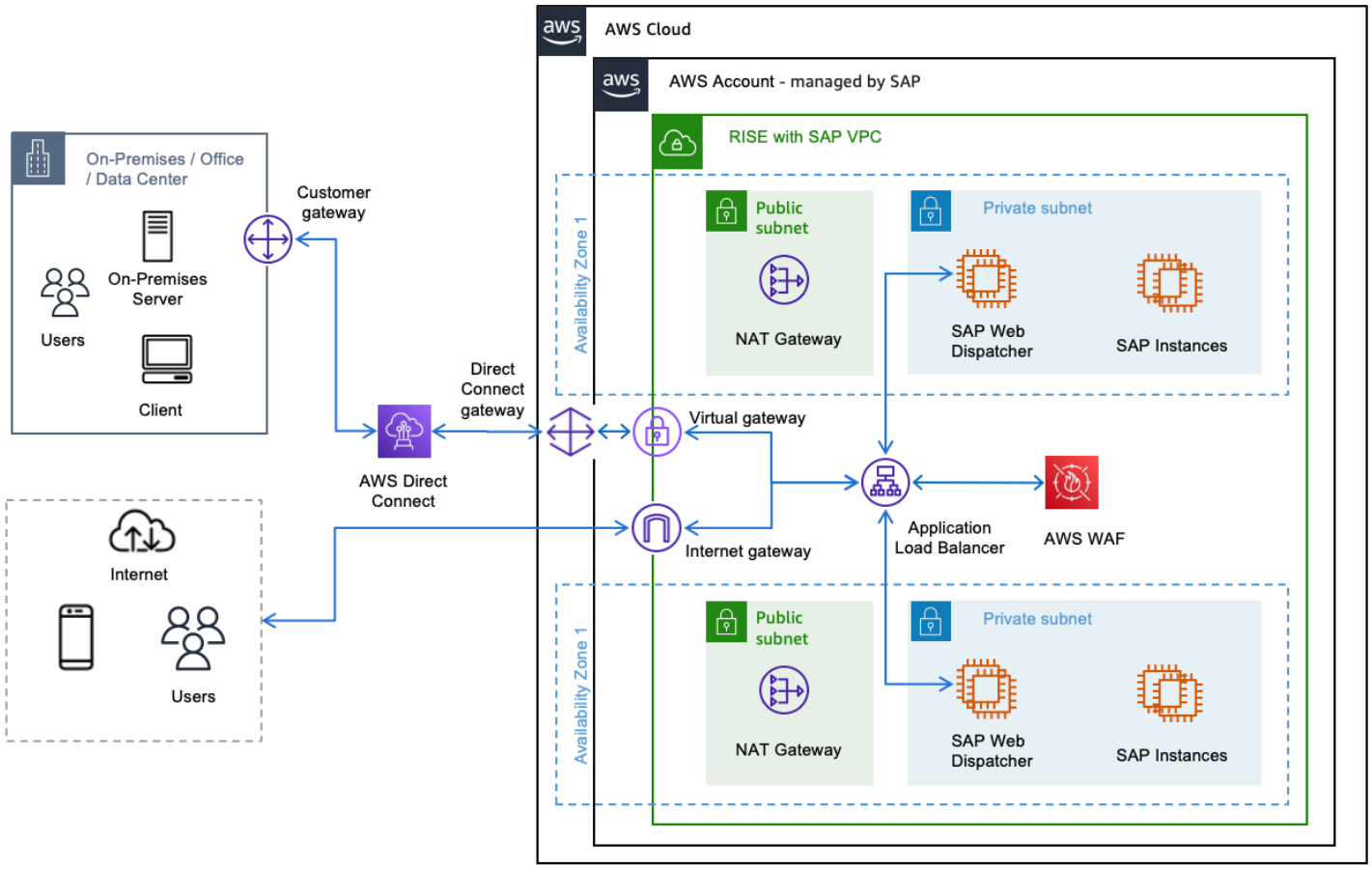
应用程序负载均衡器（ALB）支持 mTLS 身份验证，并提供两种模式：验证模式和直通模式。

先决条件

为确保无缝通信，整个架构中使用的所有 SSL（安全套接字层）或 TLS 证书（包括 ALB、SAP Web Dispatcher 以及 S/4HANA 系统上的证书），均应来自单一且受信任的根证书颁发机构，以便简化这些证书的部署与维护流程。

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，请创建一个包含 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 会依据信任存储对客户端证书进行验证，从而高效拦截未经授权的请求。此方式将从后端目标卸载 mTLS 处理流程，提升整体系统效率。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。这使得可基于证书详情在后端目标上实施额外逻辑，满足 SAP 服务器保留原始“主机头”信息的需求。

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/client ate_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 会将客户端的完整证书链转发至后端目标。这是通过名为的 HTTP 标头完成 X-Amzn-Mtls-Clientcert的。证书链（包含终端证书）以 URL 编码的 PEM 格式发送，其中 +、= 和 / 被视为安全字符。以下是使用 mTLS 直通模式时的注意事项：

- 如果没有客户端证书，ALB 不会添加任何标头；后端必须处理此情况。
- 后端目标负责客户端身份验证与错误处理。
- 对于 HTTPS 侦听器，ALB 会终止客户端与 ALB 之间的 TLS 连接，并使用目标已安装的证书发起 ALB 与后端之间的新 TLS 连接。
- ALB 的 TLS 终止功能支持使用任何 ALB 路由算法来进行负载均衡。

NLB 直通

如果您有严格的安全合规规则，要求在服务器端终止客户端 TLS 连接，则可使用网络负载均衡器（NLB）。

需要注意的关键点：

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 终止操作，这在某些安全合规场景中可能至关重要。

此方式可确保敏感的解密流程在您可管控的服务器环境中进行，从而满足特定的安全要求，并保持高效的流量分配。

mTLS 验证模式、mTLS 直通模式与 NLB 直通模式的对比。

注意事项	带 mTLS 验证模式的 ALB	带 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（客户自主管理型）	由后端完成（客户自主管理型）

注意事项	带 mTLS 验证模式的 ALB	带 mTLS 直通模式的 ALB	NLB
客户 SSL/TLS 终止	在 ALB（AWS 托管）	在 ALB（AWS 托管）	在后端目标上（客户自主管理型）
基于标头的路由	支持	支持	不支持
信任存储	需要（在 ALB 上）	非必需（在 ALB 上）	非必需（在 NLB 上）
认证吊销列表	在 ALB 上托管	后端托管（如果需要）	后端托管（如果需要）
后端处理负载	小于	小于	更高
错误处理	ALB 托管	后端托管	后端托管

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。此服务通过检查用户身份、设备运行状况和位置，对每项访问请求进行验证；它还可与 Okta、Azure Active Directory 和 IAM Identity Center 集成，并提供详细的访问日志记录与监控功能。有关更多信息，请参阅 AWS Verified Access。

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。

用户可以更快地访问 RISE with SAP 系统（在建立 VPN 连接之前）。利用该解决方案，您可以向远程用户和外部顾问授予安全访问权限，即便他们无法通过 VPN 访问企业网络。

1. 以身份为中心的安全性

   经过验证的访问权限可与现有的身份提供商 (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. 上下文访问控制

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. 增强性能

   Verified Access 为 SAP 系统提供了直接、优化的连接路径，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。它可实现自动化合规报告、实时访问监控，并减少基础设施维护工作。

实施指南

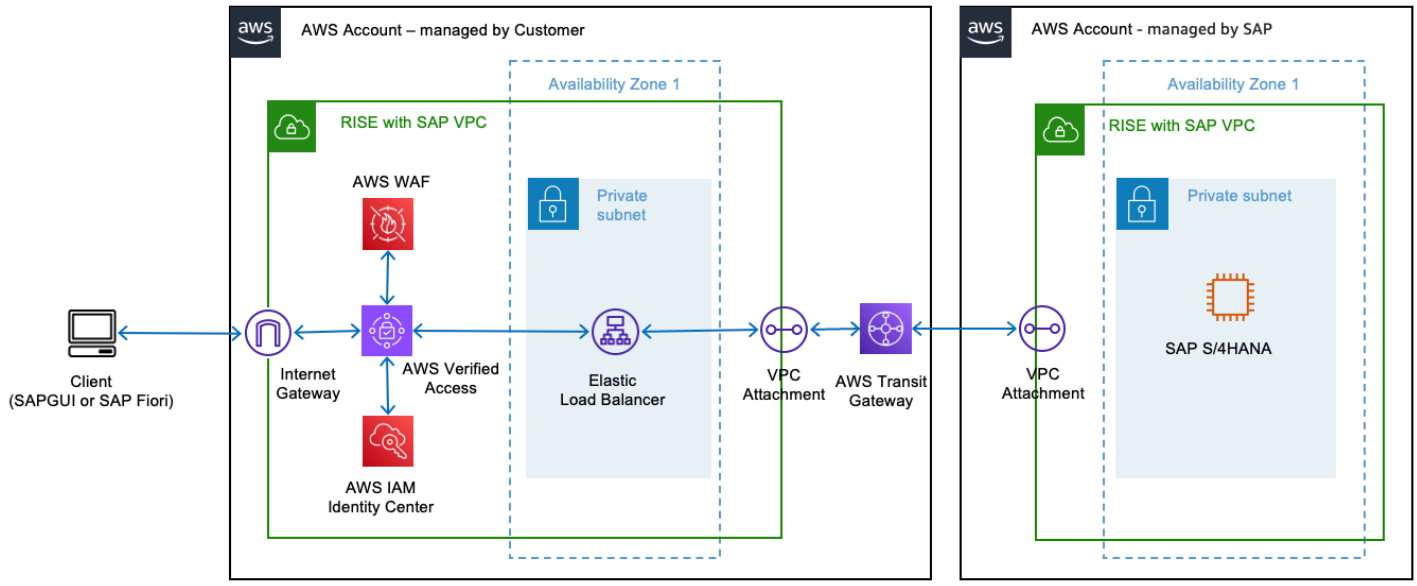
先决条件

- 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。
- 拥有允许通过网络访问 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。（您可以使用网络负载均衡器同时进行 SAP GUI 和 SAP Fiori 访问，或仅使用应用程序负载均衡器进行 SAP Fiori 访问）。
- 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。
- 拥有公共托管域以及更新该域的 DNS 记录所需的权限（示例：Amazon 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 Verified Access 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 Verified Access 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 Verified Access 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 Verified Access 实例，然后在 Verified Access 中附加或移除信任提供商。

3. 创建 Verified Access 组。使用 Verified Access 组根据端点的安全要求组织端点。创建 Verified Access 端点时，将该端点与组相关联。使用以下过程创建 Verified Access 组。
4. 为 Verified Access 创建负载均衡器端点。Verified Access 端点代表一个应用程序。每个端点都与一个 Verified Access 组相关联，并继承该组的访问策略。使用以下过程为适用于 SAP 应用程序的 Verified Access 创建负载均衡器端点。
5. 为 Verified Access 端点配置 DNS。在此步骤中，您将 SAP 应用程序的域名（例如 www.myapp.example.com）映射到 Verified Access 端点的域名。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，根据您的要求为应用程序派生一个语句。
7. 测试应用程序的连接性。对于基于 HTTP(S) 的访问（如 SAP Fiori 访问），现在可在 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性。



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 on AWS 的生成式人工智能

生成式人工智能是指能够基于经过训练的数据，创建文本、图像、音频或代码等新内容的智能系统。这类系统采用机器学习技术（尤其是深度学习和神经网络），识别训练数据中的模式与关系，进而生成与所学信息相似的全新输出内容。

随着组织为其员工和客户引入生成式人工智能，网络安全从业者必须快速评测这项不断发展的技术所涉及的风险、治理方式及管控措施。作为 Amazon Web Services（AWS）中服务于非常复杂的大规模客户的安全领域领导者，我们经常就生成式人工智能的发展趋势、最佳实践、快速演变的领域，以及相关安全与隐私影响提供咨询。生成式人工智能解决方案涵盖多个使用案例，这些使用案例会影响您的安全范围。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。

AWS 上的 SAP 数据集成与管理

数据是任何生成式人工智能解决方案获得成功的基石。数据的质量、数量和多样性是关键因素，它们直接影响人工智能模型的性能与有效性。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

RISE on AWS 的生成式人工智能解决方案的实施方式

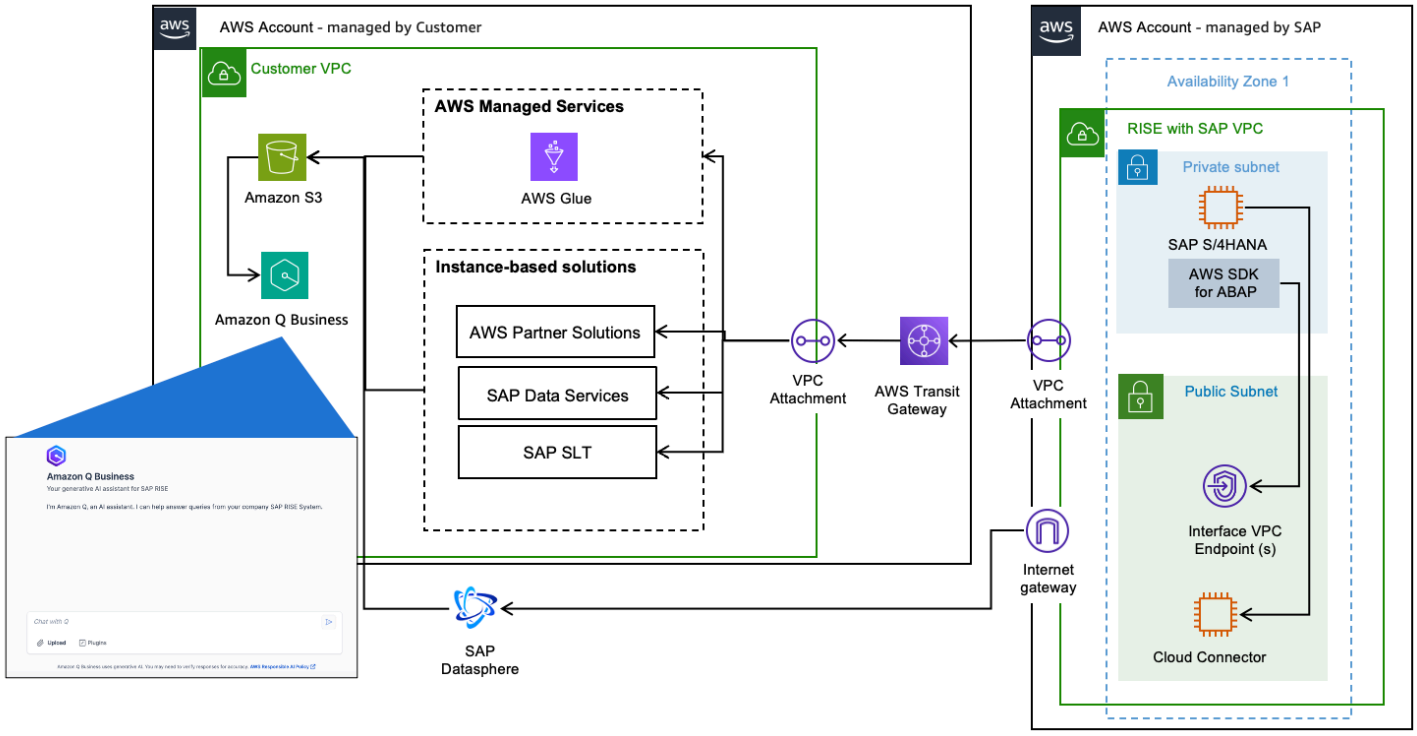
本架构指南可帮助您构建先进的人工智能解决方案，它向你展示了如何有效地将 AWS RISE 与 SAP 和 SAP 的人工智能服务相结合，以创建强大而创新的系统。

Amazon Q 企业版

RISE 客户可利用 Amazon Q Business 根据企业数据回答问题、提供摘要、生成内容并完成任务，终端用户便可根据自身的权限，从企业数据来源即时收到回复以及引文。Q Business 是一款完全托管式生成式人工智能驱动型助手，拥有 40 多种预构建的连接器，可连接到各类企业应用程序与数据来源。

选择通过构建数据仓库或数据湖解决方案来打破数据孤岛的客户，可将 SAP 及其他企业数据用作 Q Business 的数据来源，以便：

- 打造跨系统和数据的统一搜索体验，从而提取关键见解
- 创建轻量级应用程序，并与选定用户共享这些应用程序或将其添加到组织的应用程序库中
- 跨常用的业务应用程序和平台执行操作
- 创建并自动实施复杂的业务工作流



上图说明了面向 RISE 客户的、基于 Q Business 的搜索功能的设计框架。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。

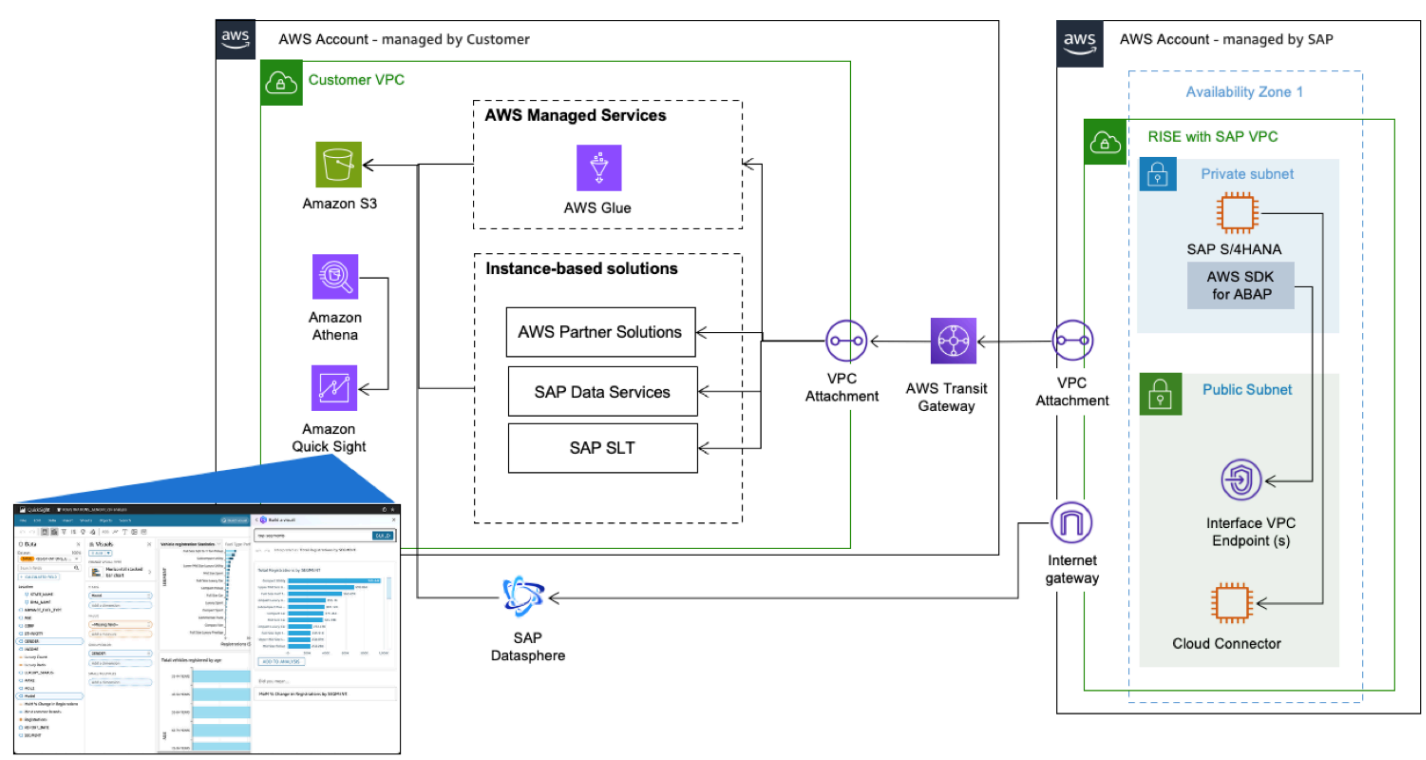
解决方案流程：

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. 利用面相各种数据来源和应用程序的预构建连接器与 Q Business 建立连接。在继承现有身份、角色和权限的同时摄取相关内容。
4. 终端用户可使用自然语言进行交互，从多个应用程序的数据中获取业务见解。

Amazon Quick Sight

Amazon Quick Sight 通过其先进的“生成式商业智能”功能，为 SAP 数据分析带来变革，并通过直观的自助式报告工具为业务用户赋能。借助自然语言提示，RISE 客户无需掌握 SQL 语言或编程技能，即可轻松创建复杂的可视化控制面板和数据叙述。

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型自动化功能可智能生成上下文关联标题、结构化章节、连贯的叙事流，以及包含具体建议的可执行见解。对于 RISE 客户而言，这意味着决策流程得以加速，并能从企业数据中获取更深入、更易理解的见解。



该图说明了 Amazon Quick Sight 与 SAP 数据相结合的框架。

解决方案流程：

1. 通过 SAP 报告处理业务逻辑，并将数据上传至 Amazon S3。
2. 借助适用于 SAP ABAP 的AWS SDK，创建 Amazon Athena 查询，该查询会关联到 S3 上的 SAP 报告数据。
3. 基于 Athena 查询，创建 Quick Sight 数据集和主题。
4. 现在，借助 Quick Sight 中的 Q 功能，您可以使用自然语言与 SAP 报告所生成的数据进行交互，获取数据见解，进而构建控制面板并生成分析报告。

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。