aws

用户指南

AWS 转换

AWS 转换: 用户指南

Table of Contents

什么是 AWS 转型？

AWS Transform 是一项服务，可通过代理的 AI 体验帮助您加速和简化基础架构、应用程序和代码的转型。它提供了专门的工具，用于简化各种工作负载的现代化和迁移工作。

使用 AWS 变换，您可以：

- 对 IBM z/OS 和富士通 GS21 进行现代化改造并将其迁移到 AWS
- 将 VMware 工作负载迁移到亚马逊 EC2
- 将.NET 应用程序现代化为 Linux-ready 跨平台.NET
- 评估工作负载是否为迁移做好准备

AWS Transform 可帮助您将发现、规划和执行阶段的劳动密集型、复杂的转型任务移交给具有语言、框架和基础架构专业知识的 AI 代理。这种方法可以让您的团队专注于创新，同时通过统一的 Web 体验高效地转变复杂的大型项目。

使用 AWS 变身无需额外付费。

术语

在本节中，斜体表示不同术语定义中的官方术语。

账号连接

在此上下文中，帐户是指客户拥有的容器或远程服务中的资源（例如 AWS 或帐户 AWS 账户 ）的安全边界。 GitHub

Artical

由 Trans AWS form 生成的输出交付内容。

管理员

管理员可以读取和更改工作区中的所有内容。他们可以使用 T AWS ransform 开始聊天、启动和停止作业以及 upload/download 工件。管理员可以与正在运行的作业进行交互以执行人机在环 (HITL) 操作，并且可以批准关键的 HITL 操作，例如合并到主节点、执行图形分解或将代码部署到生产环境。管理员可以改变工作空间、连接器和用户。

代理人

执行特定转换类型的任务特定服务。例如，VMware 迁移。

批准者

批准者的权限与管理员类似，唯一的不同是他们无权更改工作空间、连接器或用户。批准者不能改变工作空间、连接器或用户。

资产

转换作业的输入。例如，客户的源代码、服务器、数据库、网络。可通过连接器访问资产。

合作者请求

在 Tr an s AWS form 中，Transform 要求人类做点什么。

连接器

连接器是资产提供者，允许访问T AWS ransform外部系统中客户拥有的资源。

设置连接器时，您要连接的帐户的管理员必须接受连接。要接受连接，他们必须拥有连接器接受者策略中赋予的权限。

以下两个账户必须相同，或者属于同一个 AWS Organizations 组织：

- AWS 转换管理员用来启用服务的帐户。
- 将成为您转换接收端的账户。必须为该账户分配一个允许其使用连接器的 IAM 角色。

贡献者

贡献者可以阅读工作区中的所有内容。他们可以使用 T AWS ransform 开始聊天、启动和停止作业、上传或下载工件，以及与正在运行的作业进行交互以执行 HITL 操作。但是，他们无法执行关键的 HITL 操作，例如合并到主要、执行图形分解或将代码部署到生产环境。贡献者也不能改变工作空间、连接器或用户。

目标

AWS 变换可以达到的用户定义的结束状态。用户编写此内容，然后 Transform 会将目标 AWS 转换为一系列任务，并在需要时与用户协同执行。

Job

T AWS ransform 为实现用户定义的目标而正在处理的长时间运行的进程 (weeks/months+)。由多项任务和协作者请求组成。

计划

Trans AWS form（在人类用户的帮助下）为实现目标而承担的任务清单。

读者

读者可以查看 Trans AWS form 作业的状态和结果，但不能进行任何更改。他们可以读取工作区中的所有内容、下载工件、查看作业和查看人机在环 (HITL) 操作。但是，读者无法在 Trans AWS form 中执行变异操作。

任务

作为工作一部分的个人工作单元。

工作日志

记录 Trans AWS form 和用户在作业中执行的操作。

工作空间

一种包含其他资源（如连接器和作业）的 AWS 转换资源。工作空间充当权限边界。

开始使用 AWS 转换

主题

设置 AWS 转换

开始前的准备工作

在设置 Trans AWS form 之前，请确保您拥有具有管理员访问权限的 AWS 帐户

> **Note**
>
> 如果你想试用 Transf AWS orm 作为概念验证或测试环境，请参阅快速入门：尝试 AWS转换。

注册获取 AWS 账户

要开始使用 AWS，你需要一个 AWS 账户。有关创建的信息 AWS 账户，请参阅《AWS 账户管理 参考指南》 AWS 账户中的入门指南。

开始使用 IAM-only 访问权限

通过 IAM-only 访问权限，用户可以使用其现有 AWS 凭据进行身份验证。

要设置 IAM-only 访问权限，请执行以下操作：

1. 在 AWS 控制台中，导航到 “ AWS 转换”，然后选择 “开始”。
2. 完成账户设置配置。
3. 在 “用户访问权限” 下，选择IAM-only 访问权限。
4. 选择 “启用” 以创建您的个人资料。

用户通过登录到 Trans AWS form Web 应用程序AWS Sign-In。他们在 Web 应用程序中的用户标识符基于他们的 IAM 委托人。

> **Important**
>
> 安装完成后，您无法添加身份提供商。要使用 IAM Identity Center 或现有身份提供商管理用户，请在初始设置期间选择其中一个选项。

有了 IAM-only 访问权限，任何拥有配置文件资源`transform:AccessTransformProfile`权限的 IAM 委托人都可以访问 Trans AWS form。您可以通过 IAM 策略而不是通过身份提供商的用户分配来管理用户访问权限。

该`transform:AccessTransformProfile`操作仅授予对 AWS 变换的访问权限。进入 T AWS ransform 后，工作区角色将控制用户可以执行的操作。这些角色包括管理员、贡献者、批准者和。Read-only无论用户如何进行身份验证，工作区角色都适用。

使用 IAM 证书

用户信息处理

当 IAM 委托人访问 T AWS ransform 时，该服务处理用户身份的方式与基于身份提供商的访问权限不同。

用户身份

IAM 用户由其 IAM 委托人识别。

双重身份

同时拥有身份提供商身份（例如 IAM 身份中心）和 IAM 会话的用户在 Trans AWS form 中显示为两个不同的用户。他们的作品在这两个身份之间没有联系。

电子邮件通知

仅对 SSO 用户启用电子邮件通知。IAM 委托人仍然可以添加到工作区，但他们不会收到电子邮件通知。

审核

IAM API 调用 AWS CloudTrail 使用调用者的 IAM 身份登录。在 Tr AWS ansform 工作日志中也可以追踪 IAM 用户在作业中执行的操作。

与身份提供商一起启用 IAM 访问权限

如果您设置了 T AWS ransform with Identity Center 或第三方身份提供商，则还可以启用 IAM 访问权限作为另一种身份验证方式。这允许 IAM 委托人与您现有的身份提供商用户一起访问 T AWS ransform。

当您使用 IAM Identity Center 或第三方身份提供商创建个人资料时，默认情况下会启用 IAM 访问权限。要随时启用或禁用 IAM 访问权限，请执行以下操作：

1. 在 “ AWS 转换” 控制台中，导航到 “设置”。
2. 在 “使用 IAM 凭证进行访问 AWS 转换” 下，开启或关闭 “启用 IAM 访问权限”。

启用 IAM 访问权限后，身份提供商用户和 IAM 委托人均可使用 T AWS ransform。IAM 用户和身份提供商用户可以在同一个工作空间中协作。

开始使用 AWS Organizations

请按照以下步骤设置 AWS 变换：

1. 登录您的 Organiz AWS ations 管理账户。
2. 导航到 AWS 转换服务。
3. 选择为您的组织启用服务以使用 Trans AWS form。
4. 为组织成员账户配置必要的权限。
5. 通过您的会员账号访问 Trans AWS form Web 体验。

> **Note**
>
> 要使用 Landing Zone Accelerator (LZA) AWS 解决方案构建您的着陆区，同时使用 T AWS ransform 以实现迁移功能，您的 Trans AWS form 帐户和 LZA 安装必须在同一个 AWS 组织中。不支持在 LZA 和 Trans AWS form 部署中使用单独的 Organizations ID，因为这可能会导致组织管理和资源部署不一致。要了解如何使用 Organizations 设置 LZA 安装，请参阅 AWS 《实施指南》用户指南中的 Landing Zone Ac celerator 部署云基础以支持高度监管的工作负载和复杂的合规性要求。

开始使用 AWS IAM Identity Center

按照以下步骤使用 IAM 身份中心进行 AWS 转换以及添加用户和群组。

默认情况下，首次启用 Trans AWS form 时，任何用户都无法访问它。

> **Note**
>
> IAM 身份中心不仅限于其设置所在的区域。如果您已经在不受 Trans AWS form 支持的区域设置了 IAM 身份中心，则可以将其用于 AWS 转换。

1. 按照启用 IAM 身份中心实例中的说明设置 IAM 身份中心。

   将 IAM Identity Center 配置为使用外部企业身份提供商，并将其用户和群组信息复制到 IAM Identity Center 中。
2. 在 AWS 控制台中，选择 “ AWS 转换”，然后选择 “开始”。
3. 选择为您的组织启用服务以使用 Trans AWS form。
4. 选择加密密钥。默认选择是 AWS 托管密钥。要使用自定义密钥，请执行以下操作：

   a. 在 “加密密钥” 下，选择 “自定义加密设置”。

   b. 选择使用 AWS KMS 密钥。

   c. 选择现有密钥或创建新密钥。

   d. 选择 “提交” 以应用您的更改，然后选择 “启用 AWS 转换”。

   选择查看配置文件以查看配置。您的用户使用 Web 应用程序 URL 来访问 Transf AWS orm 统一的 Web 体验。
5. 在导航窗格中选择用户，然后选择分配用户或组。
6. 搜索您想要授权使用 Transform 的用户或群组的 AWS 名称。搜索引用了从您的身份提供商传播的用户和群组。
7. 选择群组或用户，选择 “完成”，然后选择 “分配”。这些用户有权使用 Transf AWS orm 统一 Web 界面。

使用第三方身份提供商

AWS Transform 支持与第三方身份提供商 (IdPs) 集成，例如 Azure 活动目录（Entra ID）和 Okta 员工身份。这允许您使用现有的身份管理系统进行用户身份验证。

先决条件

在配置第三方身份提供商集成之前，请确保您的身份提供商中的用户已配置姓名、电子邮件和用户名属性

存储的信息

当你将 T AWS ransform 与一起 IdPs使用时，会 AWS 存储最少的经过加密和安全的用户信息：

存储的用户信息

AWS Transform 会在首次登录时存储基本的用户配置文件信息，包括显示名称、电子邮件地址、用户名（preferred_username）和唯一的用户标识符。此信息使用客户拥有的 KMS 密钥或服务拥有的密钥进行加密，具体取决于客户的 Tr AWS ansform 配置文件配置。数据存储在 Trans AWS form 的身份验证数据库中，并且仅在初始登录会话期间收集。邀请其他用户加入工作区时，这会填充搜索结果。

数据生命周期

仅为至少登录过 Trans AWS form Web 应用程序一次的用户存储用户信息，如果用户在没有重新登录 Transform 的情况下更新其身份提供商中的信息，则这些信息可能会过时 AWS 。删除 Trans AWS form 配置文件后，所有存储的用户信息都将被删除。

客户机密存储

设置期间提供的客户端密钥 AWS Secrets Manager 通过服务关联密钥 (SLS) 存储在您的账户中。

用户标识符处理

Entra

使用 “oid”（对象标识符）声明作为唯一的用户标识符，该标识符是不可变的，可以唯一标识 Microsoft 租户中的用户。客户可以在 Entra 控制台中看到此值，并显示在 CloudTrail 日志中。

Okta 员工身份

根据令牌类型对用户身份使用不同的声明，即 ID 令牌中的 “订阅” 声明和访问令牌中的 “uid” 声明。AWS 在身份验证期间，转换可以验证两个声明是否包含相同的值。客户可以在 Okta 控制台中看到此值并显示在 CloudTrail 日志中。

设置 Azure Active Directory（入口 ID）

要配置 Azure 活动目录与 AWS 转换的集成，请执行以下操作：

1. 导航到 Azure 门户，然后选择 Azure 活动目录。
2. 在左侧导航窗格中，选择管理 > 应用程序注册。
3. 选择 + 新注册。
4. 输入应用程序名称，选择支持的账户类型，将重定向 URI 留空，然后选择注册。
5. 在左侧导航栏中，选择 “管理” > “清单”。
6. `requestedAccessTokenVersion`从更新`null`到，`2`然后选择 “保存”。
7. 选择管理 > 公开 API，然后选择添加范围。
8. 使用默认结构创建应用程序 ID URI `api://<client-id>`。
9. 添加范围`transform:read_write`。
10. 选择添加证书或密钥并创建新的客户机密钥。保存此值，因为这是创建个人资料所必需的。
11. 通过选择端点并选择 OpenID Connect 元数据文档来查找发行者网址。元数据中的 “发卡机构” 字段是您的发卡机构 URL。
12. 使用客户端 ID、客户端密钥和发行者 URL 在 Transf AWS orm 控制台中创建配置文件。
13. 创建配置文件后，通过选择添加平台、选择 Web 并输入来添加重定向 URI `<web-application-url>/login/callback`。

设置 Okta 员工身份

要使用 T AWS ransform 配置 Okta Workforce

1. 导航到您的 Okta 员工身份控制台。
2. 选择 “应用程序” > “应用程序”，然后选择 “创建应用程序集成”。
3. 选择 OIDC-OpenID Connect 和 Web 应用程序，然后选择 “下一步”。

4. 为您的应用程序命名，将授权类型保留为授权码，将重定向 URI 留空，配置用户分配，然后选择保存。
5. 导航到 “登录” 选项卡，将发行者设置为 Okta URL，而不是动态。
6. 复制客户端 ID，然后转到 “安全” > “API” 并添加授权服务器，将其配置为授权服务器的受众。
7. 在授权服务器中，在 “范围” 选项卡`transform:read_write`下添加范围。
8. 添加允许 OIDC 应用程序使用此授权服务器的访问策略，并为该策略配置规则。
9. 在 “授权服务器设置” 页面上，记下 Transf AWS orm 中用于创建配置文件的颁发者 URL。
10. 使用应用程序设置中的颁发者 URL、客户端 ID 和客户端密钥在 Tr AWS ansform 中创建配置文件。
11. 创建个人资料后，在应用程序的 “常规” 选项卡中添加`<web-application-url>/login/callback`为重定向 URL。

> **Note**
>
> 如果您想在注销后重定向回 Trans AWS form Web 应用程序，则需要在 “安全” > “API” 下将您的 Web 应用程序 URL 配置为可信来源。

用户入门

本节介绍已获得 Transform 访问权限的用户的 AWS 体验。

接受邀请

将用户添加到 Trans AWS form 后，他们会收到一封包含以下内容的电子邮件邀请：

- 问候语和有关邀请的信息
- 转 AWS 换 Web 应用程序网址
- 他们的用户名
- 用于接受邀请并设置密码的链接

要设置他们的账户，请执行以下操作：

1. 用户点击电子邮件中的 “接受邀请” 链接。
2. 在 “新用户注册” 页面上，他们输入并确认密码。
3. 密码必须符合安全要求，包括：

- 至少 8 个字符
- 至少有一个大写字母
- 至少有一个小写字母
- 至少有一个数字
- 至少有一个特殊字符

4. 创建密码后，他们会看到账户已成功创建的确认信息。

登录到 AWS 转换

要登录 AWS 转换，请执行以下操作：

1. 导航到邀请电子邮件中提供的 AWS 转换 Web 应用程序 URL。
2. 输入用户名。
3. 选择下一步。
4. 输入密码。
5. 选择登录。

欢迎体验

首次登录后，用户会看到带有以下内容的 T AWS ransform 欢迎页面：

- 个性化问候
- 可用的转换功能
- 创建工作空间的选项

欢迎页面提供有关 Trans AWS form 中可用的转换功能的信息，包括：

- 对 IBM z/OS 迁移进行现代化改造 AWS
- 将 VMware 工作负载迁移到亚马逊 EC2
- 将.NET 应用程序现代化为 Linux-ready 跨平台.NET
- 评估工作负载是否为迁移做好准备

用户可以先创建工作区或要求其团队将其添加到现有工作区。

使用您自己的亚马逊 S3 存储桶

默认情况下，Transf AWS orm 使用服务托管的 Amazon S3 存储桶来存储转换项目。您可以选择改用自己的 Amazon S3 存储桶，以便更好地控制数据存储、加密和访问策略。

> **Note**
>
> 如果您有用于大型机转换的 Amazon S3 存储桶，则可以继续使用该 S3 连接器，而无需使用此功能。

> **Note**
>
> 您的 Amazon S3 存储桶仅存储您与之交互的上传和转换项目。系统生成的内部项目不会存储在您的存储桶中。此外，T AWS ransform 还会对存储桶中的项目进行索引。它将索引数据存储在服务管理的知识库中，用于为您提供丰富的聊天体验。

先决条件

在配置自己的 Amazon S3 存储桶之前，请确保满足以下要求：

- 存储桶必须位于启用 AWS 转换的同一 AWS 区域。
- 必须将所需的存储桶策略应用于您的存储桶。有关更多信息，请参阅 the section called “必需的存储桶策略”。
- 如果您使用 AWS 转换 Web 应用程序，则必须在存储桶上配置 CORS。有关更多信息，请参阅 the section called “必需的 CORS 配置”。
- 如果您使用自定义 AWS KMS 密钥，则必须应用所需的密钥策略。有关更多信息，请参阅 the section called “KMS 密钥策略（可选）”。

支持的加密配置

您的存储桶必须使用以下加密配置之一：

- SSE-S3 (AES256)-将 KMS 密钥字段留空。 AWS Transform 在不指定加密标头的情况下写入对象，而 Amazon S3 会使用 S3-managed 密钥应用存储桶的默认加密。有关更多信息，请参阅 Amazon S3 用户指南中的对 Amazon S3 托管密钥使用服务器端加密 (SSE-S3)。

- SSE-KMS 使用客户管理的 KMS 密钥 — 提供 KMS 密钥 ARN。 AWS Transform `x-amz-server-side-encryption: aws:kms` 使用提供的密钥写入对象。按照the section called “KMS 密钥策略（可选）”中的说明操作。

不支持以下语句：

- SSE-KMS 使用 AWS托管的 KMS 密钥（例如，`aws/s3`）
- SSE-C
- DSSE-KMS
- 非对称 KMS 密钥或密钥规格不是 SYMMETRIC_DEFAULT 的 KMS 密钥

> **Warning**
>
> AWS不支持托管的 KMS 密钥。如果您的存储桶使用加密，请迁移到客户管理的密钥`aws/s3`，或者 SSE-S3 在使用带有 Tr AWS ansform 的存储桶之前迁移到客户管理的密钥。

配置您的亚马逊 S3 存储桶

您可以通过 AWS AWS 转换控制台将 Transform 配置为使用自己的 Amazon S3 存储桶。

使用您自己的 Amazon S3 存储桶

1. 在“ AWS 转换” 控制台中，选择“设置”。
2. 在 A rtifact 存储空间下，选择使用我自己的 S3 存储桶。您可以在当前账户 AWS 账户 或其他账户中使用存储桶。
3. 对于存储桶，请输入 Amazon S3 URI。
4. （可选）对于 KMS 密钥，输入 AWS KMS 密钥 ARN 以加密存储桶中的对象。如果您将此字段留空，Trans AWS form 会写入不带加密标头的对象，Amazon S3 会应用存储桶的默认加密设置。有关更多信息，请参阅《Amazon S3 用户指南》中的为 Amazon S3 存储桶设置默认服务器端加密行为。

   如果您的存储桶的默认加密为 SSE-KMS，请在此字段中输入客户管理的 KMS 密钥 ARN 并更新您的密钥策略。有关更多信息，请参阅 the section called “KMS 密钥策略（可选）”。
5. 选择“保存”。 AWS 在应用配置之前，Transform 会验证存储桶配置和权限。

保存配置后，T AWS ransform 会使用您的存储桶来存储转换工件。

> **Note**
>
> AWS 只有在您保存配置时，转换才会验证您的配置。如果您稍后更改了存储桶策略、CORS 配置或 KMS 密钥策略，请重新保存您的配置文件设置以重新验证。

必需的存储桶策略

您必须配置存储桶策略才能授予 Trans AWS form 访问权限。将以下存储桶策略添加到您的 Amazon S3 存储桶，以允许 Trans AWS form 服务主体读取、写入、删除和列出转换项目。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "transform.amazonaws.com"
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:PutObjectTagging"
            ],
            "Resource": "arn:aws:s3:::bucket-name/AWSTransform/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "profile-account-id",
                    "aws:SourceArn": "profile-arn"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": [
                    "transform.amazonaws.com"
                ]
            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::bucket-name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "profile-account-id",
                    "aws:SourceArn": "profile-arn"
                }
            }
        }
    ]
}
```

替换以下值：

- *bucket-name*— 您的亚马逊 S3 存储桶的名称。
- *profile-account-id*— 与您的 AWS 转换配置文件关联的 AWS 账户 ID。
- *profile-arn*— 你的 Trans AWS form 个人资料的 ARN。

必需的 CORS 配置

如果您使用 Trans AWS form Web 应用程序，则必须在 Amazon S3 存储桶上配置 Cross-Origin 资源共享 (CORS)。启用 “ AWS 转换” 后，即可找到 Web 应用程序域。有关更多信息，请参阅 开始使用。

```
[
    {
        "AllowedHeaders": [
            "host",
            "content-type",
            "if-none-match",
            "x-amz-checksum-sha256",
            "x-amz-expected-bucket-owner",
            "x-amz-server-side-encryption",
            "x-amz-server-side-encryption-aws-kms-key-id",
            "x-amz-server-side-encryption-context",
            "x-amz-source-account",
            "x-amz-source-arn"
        ],
```

```
        "AllowedMethods": [
            "GET",
            "PUT",
            "HEAD"
        ],
        "AllowedOrigins": [
            "webapp-domain"
        ],
        "ExposeHeaders": [
            "ETag",
            "x-amz-checksum-sha256",
            "x-amz-request-id",
            "x-amz-id-2"
        ],
        "MaxAgeSeconds": 3600
    }
]
```

替换以下值：

- *webapp-domain*— 您的 Web 应用程序来源 URL（例如`https://1a2b3c4d5e6f7a8b9.transform.us-east-1.on.aws`），可以在 AWS 转换设置页面上找到。请勿包含尾部的斜杠。

KMS 密钥策略（可选）

此部分仅适用于使用客户管理的 KMS 密钥对存储桶进行加密的情况。如果您的存储桶使用了 SSE-S3，请跳过此部分。

如果您为存储桶加密指定自己的 AWS KMS 密钥，请将以下语句添加到您的密钥策略中。 AWS Transform 依靠转发访问会话 (FAS) 为其服务主体创建授权。这些授权用于验证您的密钥并访问您的 Amazon S3 存储桶中的项目。

```
{
    "Sid": "AllowAWSTransformServiceAccess",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::key-owner-account-id:root"
    },
    "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey"
```

```
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "transform.region.amazonaws.com"
        }
    }
}
```

替换以下值：

- *key-owner-account-id*— 拥有 KMS 密钥的 AWS 账户 ID。
- *region*— 启用 AWS 变换的 AWS 区域（例如，us-east-1）。

切换回默认存储桶

您可以随时切换回服务管理存储桶。

要切换到 AWS 转变托管存储

1. 在 “ AWS 转换” 控制台中，选择 “设置”。
2. 在 A rtifact 存储空间下，选择编辑。
3. 选择 “AWS 转换托管存储”。
4. 选择保存。

> **Warning**
>
> 如果您在转换作业进行时切换存储配置，则这些作业会失败。这些正在进行的作业已经生成的任何构件也将无法访问。

> **Important**
>
> 当您切换回服务托管存储桶时：
>
> - 存储桶中的项目不会自动迁移。要保留任何项目，请从您的 Amazon S3 存储桶下载它们，然后通过 Transfor AWS m Web 应用程序将其重新上传到相应工作空间和任务的工件存储区。

- AWS 转换会停用对您的 KMS 密钥的授权。写入存储桶的对象仍保留在您的存储桶中；如果不再需要这些对象，请手动将其删除。

将文件直接上传到您的存储桶

您可以直接将文件上传到您的 Amazon S3 存储桶，而无需使用 Trans AWS form Web 应用程序。要使上传的文件可供转换代理使用，请将其上传到作业`User Uploads`的文件夹。此文件夹的目录路径使用以下格式：

```
AWSTransform/Workspaces/workspace-id/Jobs/job-id/User Uploads/
```

替换以下值：

- *workspace-id*— 您的 “ AWS 转换” 工作区的 ID。
- *job-id*— 转换任务的 ID。

Trans AWS form 中的每个作业都有自己的`User Uploads`文件夹。您上传到此路径的文件将显示在 Web 应用程序中，并在转换代理完成任务时可供他们使用。

文件路径不得包含`..//`、、前导或尾随空格 — 代理看不到违反这些限制的文件。

Important

如果您的存储桶使用 SSE-KMS，请在每次直接上传时都包含以下标头：

```
x-amz-server-side-encryption: aws:kms
x-amz-server-side-encryption-aws-kms-key-id: your-kms-key-arn
```

必须使用在您的 Trans AWS form 配置文件中注册的 KMS 密钥对对象进行加密。Transform 无法访问使用任何其他密钥加密 AWS 的对象。

兼容性矩阵

下表汇总了 Trans AWS form 与常见 Amazon S3 存储桶功能的兼容性。

功能	兼容性	注意
Bucket versioning	支持	使用生命周期规则管理非当前版本。
对象所有权	必需：强制执行存储桶所有者	首选存储桶所有者，不支持对象写入器。
ACL	不支持	必须在存储桶上禁用 ACL。
对象锁定（治理模式）	部分支持	保留设置可能会阻止删除操作。
对象锁定（合规模式）	不支持	—
屏蔽公共访问权限	支持	—
申请方付款	不支持	—
S3 接入点	不支持	使用存储桶名称。
S3 对象 Lambda 接入点	不支持	使用存储桶名称。
S3 on Outposts	不支持	—
S3 Express One 区域（目录存储桶）	不支持	—
Cross-Region 水桶	不支持	—
Cross-account 水桶	支持	—
Cross-account KMS 密钥	不支持	—
生命周期规则	支持	—
CloudTrail 数据事件	支持	—

Enable AWS 转换

要启用 AWS 转换：

1. 登录到 AWS 管理控制台。
2. 在控制台顶部的搜索栏中，搜索 Transf AWS orm。
3. 从搜索结果中选择 “AWS 转换”。
4. 选择 Get st arted 以在您当前的地区启用该服务。
5. 可选：配置 IAM 身份中心。您还可以在后续步骤中选择使用第三方身份提供商 (IdP)。
6. 选择加密密钥：默认 AWS 托管密钥或自定义加密设置。
7. 可选：使用您自己的 Amazon S3 存储桶。默认情况下，Transf AWS orm 使用服务托管的 Amazon S3 存储桶来存储转换项目。您可以选择改用自己的存储桶。有关更多信息，请参阅 使用您自己的亚马逊 S3 存储桶。
8. 选择要启用的 AWS 转换功能：
   - 命令行界面 (CLI)，用于创建和运行自定义转换。要启用 CLI，请查看并按照下载说明进行操作。
   - Web 应用程序，用于现代化的代理用户界面。选择 “启用 Web 应用程序” 以使用它。
9. 选择 “启用 AWS 转换”。
10. 可选：选择 “启用查看配置文件” 以访问 “ AWS 转换用户”、“设置” 和 “连接器” 选项卡，或者选择 “管理用户” 以管理用户。

    通过选择控制台左上角的菜单图标，您可以随时访问 “用户”、“设置” 和 “连接器” 选项卡。
11. 通过选择以下选项之一来配置用户访问权限：
    - IAM Identity Center
    - 第三方身份提供商 (IdP)
    - IAM-only access

    > **Note**
    >
    > 此选项已最终确定，当您启用 “ AWS 转换” 时无法更改。
12. 选择 “启用 Web 应用程序”。

13. 系统在创建必要资源时显示 “启用 AWS 转换”。

启用 AWS 转换后，“设置” 选项卡将显示以下信息：

- Web 应用程序 URL-用于访问 Trans AWS form Web 应用程序的 URL
- IDE 的起始网址-用于在集成开发环境中访问 T AWS ransform 的 URL
- 区域-启用 AWS 变换的 AWS 区域

快速入门：正在尝试 AWS 转换

试用 Tr AWS ansform 的最简单方法是使用独立 AWS 账户。您可能希望将其作为概念验证或用于测试环境。使用以下步骤：

1. 登录到 AWS 管理控制台。
2. 导航到 AWS 转换服务。
3. 选择 “开始使用” 以启用该服务。
4. 选择并设置您的身份提供商。
5. 将用户分配给 AWS 转换服务。
6. 启用该服务后，您将看到 AWS 转换 Web 应用程序 URL。
7. 在新的浏览器窗口中打开该 URL 即可访问 Trans AWS form Web 体验。

现在，您已准备好设置工作空间了。

管理用户

如何管理用户对 Trans AWS form 的访问权限取决于您在设置过程中选择的访问模式。如果您配置了 IAM 身份中心，则可以通过 IAM 身份中心添加用户。如果您配置了第三方身份提供商，则可以在该提供商中管理用户。如果您选择 IAM-only 访问权限，则通过 IAM 策略管理用户访问权限。

在 IAM Identity Center 中添加用户

要在 IAM 身份中心添加用户，请执行以下操作：

1. 导航到 IAM Identity Center 控制台。
2. 在导航窗格中选择用户。

3. 选择添加用户。
4. 输入所需信息：
   - 用户名-用户的唯一标识符（以后无法更改）
   - 电子邮件地址-用户的电子邮件地址
   - 名字和姓氏-用户的名字
   - 显示名称-出现在用户列表中的名称
5. 在“密码”中，选择用户接收密码的方式：
   - 发送电子邮件-通过电子邮件发送设置说明
   - 生成一次性密码-创建要手动共享的密码
6. 选择“下一步”查看用户信息。
7. 查看详细信息并选择添加用户。

添加用户后，他们将收到一封电子邮件邀请，要求他们设置自己的 IAM Identity Center 账户。邀请链接的有效期为 7 天。

您还可以在此视频中了解如何使用 IAM 身份中心和 AWS 转型：

VideoTitle

将用户添加到 AWS 转换

将用户添加到 IAM 身份中心后，您可以向他们授予对 Trans AWS form 的访问权限：

1. 返回 AWS 变换控制台。
2. 在导航窗格中，选择用户和群组。
3. 选择“用户”选项卡或“群组”选项卡。
4. 在 IAM Identity Center 中搜索并选择要添加的用户或群组。
5. 选择“分配用户和群组”，授予所选用户或群组访问 AWS 转换的权限。

添加用户后，他们在用户列表中显示的状态为“待定”，直到他们接受邀请并登录。

管理具有 IAM-only 访问权限的用户

如果您将 T AWS ransform 配置为 IAM-only 访问权限，则用户访问权限将通过 IAM 策略进行管理。任何拥有配置文件资源`transform:AccessTransformProfile`权限的 IAM 委托人都可以访问 Trans AWS form。

要向用户或角色授予 AWS 转换访问权限，请执行以下操作：

1. 导航到 IAM 控制台。
2. 将包含该`transform:AccessTransformProfile`操作的策略附加到 IAM 用户或角色。有关策略示例，请参阅允许用户使用 IAM 凭证访问 T AWS ran sform。

要撤消访问权限，请从 IAM 用户或角色中移除该策略。

了解合作者权限

AWS Transform 使用基于工作空间的权限模型来控制对资源和操作的访问权限。在工作区内为每个用户分配一个特定的角色，该角色决定了他们可以执行的操作。一个用户可以在不同的工作空间中扮演不同的角色。

用户角色

AWS Transform 支持每个工作区内的五个用户角色。这些角色适用于工作空间的上下文，并且将在他们所属的每个工作空间中为用户分配角色。为每个角色定义的访问权限与工作空间无关，因此在工作空间 A 中具有管理员角色的用户 A 与在工作空间 B 中具有管理员角色的用户 B 具有相同的权限。

角色权限

每个角色的详细权限：

处理建议	ResourceType	Admin	批准者	贡献者	ReadOnly
Create	Workspace	✓	✓	✓	✓
列表	Workspace	✓	✓	✓	✓
获取	Workspace	✓	✓	✓	✓
更新	Workspace	✓	✗	✗	✗

处理建议	ResourceType	Admin	批准者	贡献者	ReadOnly
删除	Workspace	✓	✗	✗	✗
Create	ChatMessage	✓	✓	✓	✗
读取	ChatMessage	✓	✓	✓	✓
Create	RoleAssociation	✓	✗	✗	✗
读取	RoleAssociation	✓	✓	✓	✓
更新	RoleAssociation	✓	✗	✗	✗
删除	RoleAssociation	✓	✗	✗	✗
读取	CriticalHitlTask	✓	✓	✓	✓
更新	CriticalHitlTask	✓	✓	✗	✗
删除	CriticalHitlTask	✓	✓	✗	✗
读取	HitlTask	✓	✓	✓	✓
更新	HitlTask	✓	✓	✓	✗
删除	HitlTask	✓	✓	✓	✗
Create	任务	✓	✓	✓	✗
读取	任务	✓	✓	✓	✓
更新	任务	✓	✓	✓	✗
删除	任务	✓	✓	✓	✗
读取	工作日志	✓	✓	✓	✓
Create	Artifact	✓	✓	✓	✗
读取	Artifact	✓	✓	✓	✓

处理建议	ResourceType	Admin	批准者	贡献者	ReadOnly
更新	Artifact	✓	✓	✓	✗
删除	Artifact	✓	✓	✓	✗
Create	Connector	✓	✓	✓	✗
读取	Connector	✓	✓	✓	✓
更新	Connector	✓	✓	✓	✗
删除	Connector	✓	✓	✓	✗

Human-in-the-loop (HITL) 行动

AWS Transform 提供两种类型的 HITL 操作——标准操作和关键操作：

标准的 HITL 行动

这些是例行操作，可以由具有 “参与者”、“批准者” 或 “管理员” 角色的用户执行。

HITL 的关键行动

这些操作会产生重大影响，因此需要更高的权限级别。例子包括：

- 将代码合并到主分支
- 执行图形分解
- 将代码部署到生产环境

关键的 HITL 操作只能由具有 “批准者” 或 “管理员” 角色的用户执行。

为了确保区分 AuthZ 策略中的标准 HITL 和关键 HITL 操作，Trans AWS form 提供了两个单独的 HITL API，一个用于完成标准 HITL 操作，另一个用于完成关键 HITL 操作。

AWS 变换环境

AWS Transform 是一项代理服务，它使用自然语言处理来帮助您规划和执行工作负载转换。您主要通过对话界 AWS 面与 Transform 互动，在该界面中，服务会根据您的讨论情境进行调整和响应。例如，您可以首先使用日常语言描述当前的架构和转型目标，例如 “我需要将本地虚拟机迁移到 EC2”。

在您与 Trans AWS form 交谈时，该服务会根据您的特定要求制定定制的工作计划。对话流程是动态的，由您驱动，允许您反复完善转型计划。在对话期间，您可以通过提出 “在生产转换之前添加测试阶段” 或 “删除备份步骤，因为我们已经有了解决方案” 之类的请求来修改工作计划。您也可以返回上一个任务并再次执行该任务。 AWS Transform 会根据您的输入不断更新计划，确保最终的转型策略满足您的技术和业务需求。

以下是你打开 “ AWS 变换” 时看到的内容。

- 视图控制窗格：这是 AWS 变换左侧的窄窗格。您可以选择其中一个图标来选择视图控制窗格右侧显示的视图。将鼠标悬停在每个图标上，即可看到解释视图的工具提示。从上到下的给出标准视图是：
  - Job Plan
  - 控制面板
  - 批准
  - 构件
  - 工作日志

  某些工作流程提供了其他视图。

  当你制定工作计划时，视图是：
  - Chat
  - 批准
  - Artical 商店
  - 工作日志

  当你在工作区中时，视图位于顶部：
  - 作业
  - 构件
  - 合作者（用户）
  - 连接器
  - 设置
- 视图窗格位于视图控件旁边。
- 聊天窗格位于中间。这是你与 Trans AWS form 进行对话的地方。

> **Note**
>
> 具有只读权限的用户无法在聊天中发送消息。

- 右边是 “协作” 窗格。当执行人为循环 (HITL) 活动时，就会出现这种情况，例如：
  - 上传数据文件
  - 审查 Trans AWS form 提供的信息和计划

语言设置

AWS Transform 支持特定工作流程的本地化。您可以通过选择右上角的设置图标并从 “语言” 菜单中选择您的首选语言来更改 Web 应用程序的显示语言。

支持以下语言：

- 英语（美国）
- 英语（英国）
- 德语（德语）
- Español（西班牙语）
- 法语（法语）
- 日本語 (日语)
- 印度尼西亚语（印度尼西亚语）
- 意大利语（意大利语）
- 葡萄牙语（葡萄牙语）
- ◦ (韩语)
- 中文（简体）（简体中文）（简体中文）
- 中文 (繁体) (繁体中文)
- 土耳其语（土耳其语）

以下工作流程支持本地化：

- 迁移（包括 VMware）

> **Note**
>
> 其他 AWS 变换工作流程目前仅提供英文版本。在未来的更新中，可能会添加对其他工作流程的本地化支持。

开始你的项目

AWS Transform 将指导您完成现代化和迁移项目。开始使用：

1. 创建工作区来托管您的项目。在 Workspaces（工作区）页面中，选择 Create workspaces（创建工作区）。按照说明进行操作，然后打开工作区。
2. 在 “聊天” 窗格中，键入 “创建作业”
3. 选择一份工作，然后按照 Trans AWS form 提供的说明进行操作。如果需要您输入，则会出现 “协作” 窗格并说明所需内容。

工作流程灵活性

Transfor AWS m 工作流程环境为现代化项目的进展提供了灵活性。在聊天窗格中使用自然语言您可以：

- 重试 Trans AWS form 已经完成的任务，在此过程中提供不同的人机在环输入。
- 例如，如果您的现代化源发生了变化，请重新运行作业。

与之聊天 AWS 转换

AWS Transform 聊天可在项目的每个阶段使用。要打开聊天，请单击 Web 控制台右下角的紫色六角形图标。

聊天室可以让你问任何问题。例如，您可以要求聊天室解释概念、指导您完成流程、解释 Trans AWS form 请求或响应，或者解释 T AWS ransform 报告。

> **Note**
>
> 具有只读权限的用户无法在聊天中发送消息。

AWS 改变聊天集成

AWS Transform 聊天集成了：

Experience-Based 加速

Experience-Based加速 (EBA) 是通过 Trans AWS form 聊天提供的。它使您能够对 Windows 工作负载执行 EBA 评估并生成计划。您可以先从 CAST 导入评估结果。它可以帮助您发现自己的应用程序组合，之后您可以使用 T AWS ransform 聊天来选择满足您业务需求的应用程序（例如，根据复杂程度或代码行筛选应用程序）。然后，您可以对所选应用程序进行更深入的评估并生成现代化计划。

AWS 倒计时高级版

AWS 集成到 Tr AWS ansform 中的 Countd@@ own Prem ium (CDP) 可提供持续的专家指导和指定的 AWS 工程支持。您指定的CDP工程师会深入研究您的技术堆栈，在出现问题时提供个性化的情境感知支持。用户可以利用 T AWS ransform 直接从其聊天界面记录支持票。支持服务单嵌入了工作日志和工作计划详细信息，以帮助支持人员了解客户的背景。如果客户或合作伙伴参与了 CDP 计划，则支持票将自动发送给指定的 CDP 工程师，他可以帮助调试问题、解释转换输出并推动加快问题解决的进度。例如：

- 对于.NET 工作负载，CDP 可以帮助解决存储库连接器问题、依赖关系解析和转换后部署。
- 在大型机场景中，CDP 可以帮助对重构的 Java 代码进行故障排除、配置数据库迁移工具和构建管道。 CI/CD
- 在 VMware 迁移中，CDP 可以加快网络配置、MGN 设置和代理安装。

AWS 技能生成器

AWS S@@ kill Builder 通过聊天提供相关的学习模块。你可以向 T AWS ransform 聊天询问你的学习需求，它会为你提供相关的课程目录。当你完成转型阶段时，Skill Builder 可提供情境化的微学习体验。

开发人员工具

您可以从代理 IDE、代理插件和 MCP 服务器访问 Tr AWS ansform 代理。选择适合您工作流程的表面。

> **Note**
>
> Kiro Power 和代理插件会自动安装 MCP 服务器。如果您想在没有 Kiro Power 或代理插件的情况下使用 MCP 服务器，则只需手动安装 MCP 服务器。

Kiro 能力

Trans AWS form Kiro Power 提供从 Kiro AWS IDE 对变身代理的完全访问权限。

要安装 AWS 变换 Kiro Power

1. 打开 Kiro IDE 并导航到“电源”面板。
2. 在列表中AWS 找到 Transform 并安装它。
3. 打开 Kiro Chat，点击电源，然后选择试用电源。

或者，在“电源”面板中，选择“添加自定义电源”>“从中导入电源” GitHub 并粘贴：`https://github.com/kirodotdev/powers/tree/main/aws-transform`

代理插件

AWS 变换代理插件可在`plugins/aws-transform`目录中的 awslabs/agent-plugin GitHub s 上找到。该插件支持 Claude Code、Codex 和 Cursor。

该插件包括`.claude-plugin`、`.codex-plugin`、和`.mcp.json`配置。它允许访问所有 AWS 转换代理，例如.NET、大型机、VMware、SQL Server 和自定义转换。

在 Claude Code 中安装

运行以下 命令：

```
/plugin marketplace add awslabs/agent-plugins
```

```
/plugin install aws-transform@agent-plugins-for-aws
```

在 Codex 或 Cursor 中安装

按照代理插件存储库 README 中的说明进行操作。

集成开发环境插件

T AWS ransform IDE 插件可在兼容 VS Code 和 Open VSX 的编辑器上使用。它公开了 Trans AWS form 自定义功能，包括创建和运行转换定义。它还公开了大型机功能，包括现代化要求、业务规则和源代码之间的可追溯性，以及按需生成技术文档的能力。要开始使用，请使用以下方法之一进行安装：

- VS Code：从 V S Code Marketplace 安装。
- 打开 VSX：从 Ope n VSX 注册表中安装。

MCP 服务器

使用 MCP 服务器以编程方式将 Trans AWS form 与任何 MCP-compatible客户端集成。你可以将 Py `awslabs.aws-transform-mcp-server` PI 中的 MCP 服务器安装为。它提供了 19 种工具，用于工作空间管理、作业管理、人机在环 (HITL) 任务、工件处理、连接器管理、聊天和资源浏览。

先决条件

- Python 3.10 或更高版本

安装

克劳德密码

```
claude mcp add awslabs.aws-transform-mcp-server -- uvx awslabs.aws-transform-mcp-
server@latest
```

Kiro

添加到`~/.kiro/settings/mcp.json`：

```
{
```

```
  "mcpServers": {
    "awslabs.aws-transform-mcp-server": {
      "command": "uvx",
      "args": ["awslabs.aws-transform-mcp-server@latest"]
    }
  }
}
```

有关您的特定 MCP 客户端的配置详细信息，请参阅上的 aws-transform-mcp-server 自述文件。 GitHub

身份验证

AWS Transform 支持 SSO（AWS Identity and Access Management 身份中心）和基于 IAM 角色的身份验证。

SSO（IAM 身份中心）

让你的 AI 助手 “使用 SSO 配置 AWS 转换”。助手会提供起始网址并打开浏览器进行登录。

IAM 角色

您的环境会自动提供 AWS 证书。`AWS_PROFILE`在 MCP 客户端配置`env`块中设置以选择特定的配置文件。

有关为 AWS 转换设置身份验证的信息，请参阅开始使用 AWS 转换。

为以下对象构建自定义代理 AWS 转换

代理生成器工具包使 AWS 合作伙伴和客户能够根据其特定现代化需求量身定制并在 Trans AWS form 中运行的代理。

安装代理生成器工具包

1. 打开 Kiro IDE 并导航到 “电源” 面板。
2. 在列表中AWS 找到 Transform Agent 工具包并进行安装。

或者，在 “电源” 面板中，选择 “添加自定义电源” > “从中导入电源” GitHub 并粘贴：`https://github.com/kirodotdev/powers/tree/main/aws-transform-agent-toolkit`

代理生成器工具包使迁移和现代化能力合作伙伴、ISV 或客户能够为特定用例创建转型解决方案。您可以将专业代理、工具、知识库和工作流程与 Trans AWS form 代理 AI 功能集成。

代理生命周期

构建

使用 Kiro Power 将基础代理和 SDK 结合起来，编写自己的自定义代理。

共享

通过团队或跨合作伙伴网络分配代理。

注册

在 T AWS ransform 中注册代理以供其他用户发现。

迁移评估

AWS 转型评估可帮助您评估将本地基础设施迁移到的成本、可行性和业务价值 AWS。评估提供自动调整规模的建议、多场景比较以及通过聊天进行交互式优化。

您可以使用迁移评估来：

- 获取适用于 SQL Server 的亚马逊 RDS、亚马逊 EC2、亚马逊 EBS、亚马逊 S3 和亚马逊 FSx 的成本估算
- 自动收到合适尺码的建议
- 评估商业价值和可持续发展影响
- 并排比较多种迁移方案
- 通过聊天以交互方式完善评估
- 生成高管演示文稿和详细报告

先决条件

在创建迁移评估之前，请确认您已具备以下条件：

- 变 AWS 换工作区
- 支持格式的库存数据，或者您可以通过聊天进行粗略估算
- 创建和运行评估的适当权限

迁移评估的工作原理

迁移评估遵循结构化的工作流程，指导您从初始数据上传到最终交付件生成。

完成迁移评估

1. 在您的 Transform 工作区中创建 AWS 迁移评估任务。
2. 上传您的本地库存数据。
3. 查看 Trans AWS form 根据您的数据生成的发现结果。
4. 通过排除服务器或调整分组来管理库存范围。
5. 使用定价和基础架构假设配置您的评估方案。

6. 进行评估。
7. 通过聊天查看和完善结果。

查看结果后，您可以创建其他方案、比较方案并生成演示文稿和报告等交付成果。

上传库存数据

AWS 转换接受来自多个来源的库存数据。下表列出了支持的数据格式。

数据来源	说明
AWS 转换发现工具导出	由 Transform 发现工具发现 AWS 的自动服务器清单
rvTools	从 VMware 环境中以 ZIP/CSV 或 Excel 格式导出。支持完全导出和 v Info-only 导出。
CMDB 数据	配置管理数据库导出
合作伙伴发现工具	来自 AWS 合作伙伴发现工具的数据
Migration Evaluator	来自迁移评估器控制台的快速见解文件
MPA 格式	迁移组合评估导入文件
AWS 转换数据模板	根据 AWS 转换评估数据模板创建的 Microsoft Excel 文件

AWS 转换会在摄取过程中自动识别文件格式。摄取过程会验证您的数据，在缺少某些字段时接受部分数据，并支持增量上传。您可以随时上传其他文件来补充库存。

查看发现结果

T AWS ransform 处理您的库存数据后，它会生成发现摘要。摘要表包含以下信息：

- 按操作系统划分的服务器数量
- 物理和虚拟服务器故障
- SQL 服务器检测
- 存储摘要

- 数据质量警告

在继续评估之前，请查看发现结果以 AWS 确认 Transform 正确识别了您的基础架构。

管理库存范围

查看发现结果后，您可以细化评估范围。使用以下操作来管理您的库存范围：

- 查询特定服务器或工作负载的清单
- 将服务器排除在评估范围之外
- 查看服务器分组和应用程序依赖关系
- 确定用于专业评估的 SQL Server 工作负载

配置评估方案

在运行评估之前，请配置 Trans AWS form 用来生成建议的假设。您可以随时修改这些假设，并使用不同的配置运行新的方案。

下表列出了可用的假设类别。

假设	说明
定价模式	数据库储蓄计划（适用于 Amazon RDS for SQL Server） On-Demand，或预留实例
目标 AWS 区域	您计划在 AWS 区域 哪里托管已迁移的工作负载
实例类型排除项	建议中应排除的 Amazon EC2 实例系列或类型
亚马逊 EBS 配置	存储的卷类型和性能设置
SQL Server 许可	自带媒体 (BYOM) 或含许可 (LI) 适用于 Amazon RDS for SQL Server；EC2 上的 SQL Server 附带许可 (LI) 或自带许可 (BYOL)

评估能力

AWS 转型评估涵盖迁移的多个维度。以下各节描述了每种评估能力。

亚马逊 EC2 调整大小

AWS Transform 会分析您的本地服务器规格并推荐大小合适的 Amazon EC2 实例。这些建议考虑了 CPU、内存和性能要求。

亚马逊 EBS 存储

AWS Transform 会根据您当前的存储使用量和性能要求推荐 Amazon EBS 卷类型和配置。

Amazon FSx

AWS Transform 会评估文件存储工作负载并为 Amazon FSx 迁移提供建议，包括支持的 Amazon FSx 文件系统类型的成本估算。

Amazon RDS for SQL Server

AWS Transform 评估将本地 SQL Server 数据库迁移到适用于 SQL Server 的 Amazon RDS 的成本。使用 AI-powered 代理，Tr AWS ansform 可以分析您的本地 SQL Server 环境，并在几分钟内提供完整的迁移业务案例，计算和内存建议与您的工作负载要求相匹配，因此您可以避免过度配置，只需为所需内容付费。

适用于 SQL Server 的 RDS 评估包括以下功能：

- 自带媒体 (BYOM) 许可，允许你使用现有的 SQL Server 许可证
- 包含许可 (LI) 许可选项
- 使用 Database Savings Plans 进行成本优化，与 On-Demand 定价相比，该计划最多可节省 20%
- Migration Acc AWS eleration Program (MAP) 的资格评估，该计划提供积分和支持以抵消迁移成本

您可以使用任何支持的数据格式启动 RDS for SQL Server 评估，包括 RVTools 导出、配置管理数据库 (CMDB) 数据、从 AWS 转换发现工具导出以及其他第三方发现工具。创建假设情景，将多个成本模型与自定义假设（包括区域、资源利用率和定价条款）进行比较。

提示示例：

- “估算将我的 SQL Server 数据库迁移到适用于 SQL Server 的 RDS 的成本”
- “比较适用于 SQL Server 的 RDS 的 BYOM 与包含许可证的定价”
- “向我展示我的 RDS 工作负载的 Database Savings Plans 选项”

亚马逊 EC2 SQL Server

AWS Transform 会评估 SQL Server 工作负载，并提供在 Amazon EC2 上运行 SQL Server 的建议，包括许可分析和专用主机映射。

On-premises 定价

AWS 转换您当前的本地成本估算值，以提供与 AWS 定价进行比较的基准。您可以通过聊天调整总体成本。 On-premises 成本调整反映在 PDF 报告和聊天回复中，但不会反映在 PPTX 导出中。

提示示例：

- “将本地服务器成本更新为每台服务器每月 500 美元”
- “再加上每年 50,000 美元的数据中心设施成本”

可持续性

AWS Transform 估算了迁移到后减少的碳足迹 AWS。您可以通过聊天探索可持续发展指标。

尝试以下提示：

- “让我看看这次迁移的预计碳减排量”
- “我的工作负载能效提高了 AWS多少？”

商业价值评估

AWS Transform 评估迁移带来的更广泛的业务价值，而不仅仅是基础架构成本节约。该评估涵盖员工的工作效率、应变能力和业务灵活性。

以下是一些示例提示：

- “估算迁移到后员工的工作效率提高 AWS”
- “迁移后我可以期待哪些弹性改进？”
- “向我展示此次迁移带来的业务灵活性优势”

网络成本

AWS Transform 估算迁移所需的网络相关成本，包括数据传输和连接要求。

Support 成本

AWS 根据您选择的 AWS 支持等级，Transform 在评估中包括支持计划成本。

最终用户计算

AWS Transform 评估最终用户计算工作负载并为 AWS 最终用户计算服务提供建议。

使用基于聊天的评估

您可以通过聊天与 T AWS ransform 互动，以创建和完善评估。聊天支持三种互动模式。

您可以通过继续对话来反复完善您的评估。 AWS Transform 可以跨消息维护上下文，并根据您的输入更新评估结果。

用有限的数据进行粗略估计

无需上传详细的库存文件，即可在聊天中描述您的环境，从而获得粗略的成本估算。粗略估算是一项独立功能，不能与上传的库存数据或通过聊天进行数据充实结合使用。

你可以使用这样的提示：

- “我有 200 台 Windows 服务器和 150 台 Linux 服务器，估计一下我的 AWS 成本”
- “请给我一个将 500 个虚拟机迁移到的粗略估计 AWS”
- “估计 50 台服务器的成本，平均配备 8 个 CPU 和 32 GB RAM”

通过聊天添加库存

您可以直接通过聊天提供库存详情，以补充或替换上传的文件。

使用如下提示：

- “包括一台在 4 个 CPU 上运行 Oracle 的数据库服务器，内存为 128 GB”
- “添加 20 台运行 Linux、具有 4 个 CPU 和 16 GB 内存的 Web 服务器”

修改成本和添加服务

您可以通过聊天调整本地成本并向评估中添加 AWS 服务。

本地调整的示例提示：

- “将本地成本提高 15%，以应对即将到来的硬件更新”
- “在本地基准的基础上再增加 100,000 美元的年度维护成本”

您还可以为 Trans AWS form 评估不完全支持的 AWS 服务添加粗略的成本估算。这提供了更完整的分析，但是这些估计值不如自动推荐那么准确。

- “添加所有迁移服务器的 AWS Backup 成本”
- “在估算中包括亚马逊的 CloudWatch 监控成本”
- “添加 10 Gbps 连接的 Di AWS rect Connect 成本”

比较场景

您可以创建具有不同假设的多个评估方案，并对它们进行比较以确定最佳迁移策略。

创建场景

尝试以下提示：

- “创建用于将 SQL Server 数据库迁移到 RDS for SQL Server 的 BYOM 方案”
- “使用适用于 SQL Server 的 RDS 的 Database Savings Plans 创建方案”
- “在 EC2 上为所有 SQL Server 工作负载创建 LI 场景”
- “创建所有工作负载均在 us-west-2 中的场景

运行比较

以下是一些示例提示：

- “给我看所有场景的成本对比”
- “哪个场景的总拥有成本最低？”

What-if 分析

无需创建全新场景即可对特定变更的影响进行建模。

提示示例：

- “如果我将我的 SQL Server 工作负载转移到适用于 SQL Server 的 RDS 而不是 EC2 会怎样？
- “适用于 SQL Server 的 RDS 的 BYOM 和随附许可证之间的成本差异是多少？”
- “如果我将 50 台最小的服务器排除在迁移之外会怎样？”
- “如果我只使用存储优化型实例会怎样？”
- “从 gp3 卷迁移到 io2 卷会有什么影响？”

生成可交付成果

完成评估后，您可以生成多种格式的可交付成果。下表描述了可用的输出格式。

Format	说明	自定义
PPTX () PowerPoint	包含调查结果和建议摘要的高管演讲	固定结构
XLSX (Excel)	详细的数据导出，包括服务器级建议和成本明细	固定结构
PDF	报告文档	可通过聊天进行自定义

相关主题

- 入门
- 自定义作业
- 发现工具

自定义

什么是 AWS 改造自定义？

AWS Transform custom 使用代理人工智能对软件、代码、库和框架进行大规模现代化改造，以减少技术债务。它可以处理各种场景，包括语言版本升级、API 和服务迁移、框架升级和迁移、代码重构以及特定于组织的转换。

通过持续学习，代理可以根据每次执行和开发人员反馈进行改进，无需专业的自动化专业知识即可提供高质量、可重复的转换。

关键功能

AWS 自定义转换提供以下功能：

- 自然语言驱动的转换定义-使用自然语言、文档和代码示例创建自定义转换
- 转换执行-在多个代码库中一致可靠地应用转换
- 持续学习-自动提高每次执行的转换质量
- AWS-托管转换 AWS-在常见场景中使用现成的、经过审查的转换

变换模式

AWS Transform custom 支持多种转型模式，以满足您的现代化需求。根据所需变更的范围和性质，每种模式都有不同的复杂性特征。

模式	说明	复杂度	示例
API 和服务迁移	在 API 版本或同等服务之间迁移，同时保持功能	中	AWS SDK v1→v2（Java、Python、JavaScript）、Boto2→Boto3、junit 4→5、javax→雅加达

模式	说明	复杂度	示例
语言版本升级	升级到同一编程语言的较新版本，采用新功能并替换已弃用的功能	Low-Medium	Java 8→17、Python 3.9→3.13、12→22、版本升级 Node.js TypeScript
框架升级	升级到同一框架的较新版本，解决重大变化	中	Spring Boot 2.x→3.x、React 17→18、Angular 升级、Django 升级
框架迁移	迁移到用途相似的完全不同的框架	高	Angular→React，Redux→Zustand，→React Vue.js
库和依赖项升级	将第三方库升级到新版本，同时保持相同的语言和框架	Low-Medium	Pandas 1.x→2.x、NumPy 升级、库升级、 Hadoop/HBase/Hive Lodash 升级
代码重构和模式现代化	在不更改外部功能的情况下实现代码模式现代化并采用最佳实践	Low-Medium	打印→日志框架、字符串连接→f-strings、类型提示采用、可观察性工具
脚本和 File-by-File 翻译	翻译独立脚本或配置文件，其中文件大多是独立的	Low-Medium	AWS CDK→Terra Form、Terraform→、Excel→Python 笔记本、Bas CloudFormation h→ PowerShell
架构迁移	只需最少的代码更改即可在硬件架构或运行时环境之间迁移	Medium-High	x86→AWS Graviton (ARM)，本地部署→Lambda，传统服务器→容器

模式	说明	复杂度	示例
Language-to-Language 迁移	将代码库从一种编程语言翻译成另一种编程语言	非常高	Java→Python，JavaScript→，C→Rust，Python→ TypeScript Go
自定义和 Organization-Specific 转换	独特的组织要求和专业的现代化需求	变化	自定义内部库迁移、组织特定的编码标准、专有框架迁移

> **Note**
>
> 对于 COBOL/mainframe 语言，请使用大型机 AWS 转换。要将.NET 框架升级到.NET Core，请考虑使用 Windows 版 AWS 转换。要将 VMware 迁移到 AWS，请考虑为 VMware 进行 AWS 转换。

操作方法 AWS 改造自定义作品

AWS Transform custom 通常用于转换多个代码库或模块的大型项目。团队通常遵循四个阶段的工作流程：

定义转换-向生成初始转换定义的代理提供自然语言提示、文档和代码示例。可以通过聊天或直接编辑来迭代完善此定义。使用 AWS管理的转换时，可以跳过此阶段。

P@@ ilot or Proof-of-Concept-在示例代码库上测试转换，并根据结果进行优化。此验证阶段有助于估算全面转型的成本和工作量。在此阶段，持续学习可以提高质量。

扩展执行-使用 CLI 设置自动批量执行，由开发人员查看和验证结果。使用 Web 应用程序监控进度并跟踪多个存储库之间的转换。

监控和审查-持续学习可自动提高转换质量。查看从前几次运行中提取的经验教训，确保它们符合质量标准，并将任何无用的内容存档。

了解主要 概念

本节介绍使用自定义 AWS 转换的关键概念。

转换定义

转换定义包含执行特定代码转换所需的指令和知识。它被表示为一项技能，包括：

- `SKILL.md`（必填）-Markdown 中带有 YAML 前缀（`name`和`description`字段）的指令，其中包含核心转换逻辑和执行指令
- `references/`文件夹（可选）-在转换执行期间根据需要加载文档
- `scripts/`folder（可选）-转换在执行期间下载并运行的脚本

AWS 在执行、检查或修改需要时，Transform CLI 会自动将转换定义下载到当前目录。

> **Important**
>
> 发布转换时，该目录必须仅`SKILL.md`包含`references/`文件夹、文件`scripts/`夹，或两者兼而有之。不允许使用其他文件或子目录。

> **Note**
>
> CLI 版本 2.0 及更高版本使用技能格式。现有的转换定义由 CLI 自动处理。

转换注册表

转换注册表是您 AWS 账户的集中存储库，用于存储和管理转换定义。注册表中的转换可以是：

- 使用列出 `atx custom def list`
- 跨多个代码库执行
- 与您 AWS 账户中的其他用户共享
- Version-controlled

> **Important**
>
> 转换定义是特定于账户的。如果您想在其他 AWS 账户中使用转换，则必须在该账户中单独发布转换。

草稿与已发布的转换

AWS 自定义转换支持注册表中的两种转换状态：

草稿转换是正在进行或未经测试的转换定义。它们另存为特定版本，引用该特定版本的用户可以检索、更新和执行。在转换准备好与团队共享之前，草稿对于迭代开发、测试和完善非常有用。草稿还与特定的对话相关联。如果重新启动 CLI，则可以使用`atx --conversation-id {id}`恢复之前的 CLI。

已发布的转换可在您账户的转换注册表中找到，供具有所需 IAM 权限的其他用户执行。可以使用`atx custom def list`发现已发布的转换。

典型的工作流程是：

1. 在本地创建转换
2. 另存为草稿以供测试 (`atx custom def save-draft`)
3. 完善和验证
4. 发布以与您的团队共享 (`atx custom def publish`)

您也可以直接发布转换，而不必将其另存为草稿。

参考文献与教训

AWS 自定义转换使用两种类型的知识来提高转换质量：

参考文献是用户提供的文档，存储在转换定义的`references/`文件夹中。参考文献仅支持文本文件（所有文件的最大总容量为 10MB），通常包含文档、API 规范、迁移指南和代码示例。在转换执行期间，根据需要加载引用。在交互模式下创建或更新转换定义时，可以添加引用。

课程是从之前的转换运行中自动提取的。持续学习系统根据执行轨迹、开发者反馈以及转换过程中遇到的代码修复生成它们。它将相关的课程分为几类，以便您可以一起复习。与您预先提供的参考不同，当您在不同的代码库中运行转换时，经验会随着时间的推移而累积，系统会自动应用这些经验来改进 future 的运行。您可以通过交互方式复习和管理课程。`atx custom def learnings`

生成和验证命令

生成或验证命令是一个可选参数，用于指定在转换过程中如何验证代码。为了确保代码的完整性，此命令在转换过程中的不同时刻执行。

提供一个命令来验证结果并在验证失败时返回问题，对于通过持续学习提高转换质量非常重要。如果不需要构建或验证，请在输入中省略。

有关示例和详细指导，请参阅 “工作流程” 部分中的生成和验证命令。

持续学习

持续学习是一种自动捕获每次转换执行中的反馈并随着时间的推移提高转换质量的系统。系统通过以下方式收集信息：

- 明确的反馈-在交互模式下提供的评论和代码修复
- 隐式观察-代理在转换和调试代码时遇到的问题

持续学习系统处理这些信息以创建经验教训，将其添加到转型定义中，从而改进 future 的转型。转换完成后，系统会自动运行学习过程，无需您额外输入。

> **Important**
>
> 课程是针对变革的，不会在不同的转型或不同的客户账户之间共享。

管理课程

系统会自动生成课程，但您可以控制将哪些课程应用于 future 的运行。该`atx custom def learnings`命令会打开一个交互式终端会话，用于查看和整理转换所积累的经验教训。

在此会话中，您可以：

- 浏览按类别分组的课程，查看每个类别包含多少活跃课程。
- 打开一节课以阅读其全部细节，包括课程正文、其影响以及之前有多少次跑步参考了它。
- 将课程存档以防止系统将其应用到 future 的运行中，如果需要，可以稍后将其恢复。
- 永久删除已不再有用的已存档课程。

如需分步指导，请参阅 the section called “持续学习”。

Client-Side 技能

Client-side 技能是在转换执行期间扩展代理的附加能力。与定义要执行什么转换的转换定义不同，客户端技能提供了辅助工具、脚本和指令，代理可以在任何转换过程中与其内置功能一起使用这些工具、脚本和指令。

Client-side 技能是从项目级和用户级目录中发现的。当技能强制执行特定于存储库的标准时，将技能放在项目级别，当这些标准适用于您的所有项目时，则将其置于用户级别。 Project-level 只有在提供了代码存储库路径时，技能才可用。有关详细的配置和用法，请参阅the section called “Client-Side 技能”。

开始使用

本节介绍如何设置自定义 AWS 转换并运行您的第一个转换。

先决条件

在安装 T AWS ransform custom 之前，请确保您具备以下条件：

支持的平台

AWS 自定义转换支持以下操作系统：

- Linux-完全支持所有 Linux 发行版
- macOS-全面支持 macOS 系统
- Windows-完全支持使用 Windows 终端的本机 Windows 和 PowerShell （ Windows 尚不支持这些`atx ct`命令 ）
- 适用于 Linux 的 Windows 子系统 (WSL)-在 WSL 下运行时支持

必需的软件

- Node.js 22 或更高版本-从中下载 https://nodejs.org/en/download
- Git-必须安装并且工作目录必须是有效的 Git 存储库才能执行转换。运行`git init; git add .; git commit -m "Initial commit"`以初始化工作目录中的 Git 存储库。

网络要求

需要能够访问以下端点的互联网连接：

- `transform-cli.awsstatic.com`
- `transform-custom.<region>.api.aws`
- `*.s3.amazonaws.com`

如果您在受互联网限制的环境中工作，请更新防火墙规则以将这些 URL 列入许可名单。

安装 AWS 转换 CLI

推荐的安装方法是使用安装脚本。选择与您的操作系统对应的选项卡。

安装 Trans AWS form CLI

1. 运行安装脚本：

   Linux and macOS

   ```
   curl -fsSL https://transform-cli.awsstatic.com/install.sh | bash
   ```

   Windows (PowerShell)

   在本机 Windows 上，使用从 Windows 终端运行安装脚本 PowerShell。

   ```
   irm https://transform-cli.awsstatic.com/install.ps1 | iex
   ```

2. 验证安装：

   ```
   atx --version
   ```

   该命令应显示已安装的 Trans AWS form CLI 版本。

配置身份验证

AWS 转换自定义需要 AWS 凭据才能使用服务进行身份验证。使用以下方法之一配置身份验证。

环境变量

设置以下环境变量。

Linux and macOS

```
export AWS_ACCESS_KEY_ID=your_access_key
export AWS_SECRET_ACCESS_KEY=your_secret_key
export AWS_SESSION_TOKEN=your_session_token
```

Windows (PowerShell)

```
$env:AWS_ACCESS_KEY_ID="your_access_key"
$env:AWS_SECRET_ACCESS_KEY="your_secret_key"
$env:AWS_SESSION_TOKEN="your_session_token"
```

您也可以使用AWS_PROFILE环境变量指定配置文件。

Linux and macOS

```
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

```
$env:AWS_PROFILE="your_profile_name"
```

> **Note**
>
> $env:中设置的环境变量仅 PowerShell 适用于当前会话。要在会话中保留它们，请通过 “系统属性” > “环境变量” 进行设置，或者使用[System.Environment]::SetEnvironmentVariable()。

AWS 凭证文件

在证书文件中配置 AWS 凭据，该文件位于 Linux 和 macOS ~/.aws/credentials 上，或者%USERPROFILE%\.aws\credentials在 Windows 上：

```
[default]
aws_access_key_id = your_access_key
aws_secret_access_key = your_secret_key
```

IAM 权限

您的 AWS 证书必须具有调用 Trans AWS form 自定义服务的权限。我们建议将AWSTransformCustomFullAccess AWS 托管策略附加到您的 IAM 用户或角色。此政策提供对 Trans AWS form custom 的完全访问权限，包括创建向账户发布 CloudWatch 指标所需的服务相关角色的权限。

为了实现更精细的控制，Trans AWS form custom 还提供了以下 AWS 托管策略：

- AWSTransformCustomExecuteTransformations— 提供执行转换的权限。
- AWSTransformCustomManageTransformations— 提供创建、更新、读取和删除转换资源以及执行转换的权限。

有关这些策略的更多信息，请参阅 Trans AWS form 的AWS 托管策略。有关具有资源级权限的自定义 IAM 策略，请参阅AWS 转换自定义 IAM 服务授权参考指南。

> **Note**
>
> - 转换定义是带有 ARN 的 AWS 资源（Amazon 资源名称）。通过在 IAM 策略资源声明中指定转换 ARN，您可以使用 IAM 策略来控制对特定转换或转换组的访问权限。标签可用于分组访问控制。
> - AWS 需要使用 IAM 身份中心才能访问 AWS 转换，但不需要使用 CLI。

配置 AWS Region

AWS Transform custom 可在特定 AWS 区域使用，并使用标准 AWS CLI 优先级自动检测您的区域配置。

支持的区域：

AWS 自定义转换可在以下 AWS 区域使用：

- us-east-1（美国东部-弗吉尼亚北部）
- eu-central-1（欧洲-法兰克福）
- eu-west-2（欧洲-伦敦）
- ca-central-1（加拿大-中部）
- ap-northeast-1（亚太地区-东京）
- ap-northeast-2（亚太地区-首尔）
- ap-southeast-2（亚太地区-悉尼）
- ap-south-1（亚太地区-孟买）

如何确定区域

CLI 按优先顺序检查这些来源，以确定要使用哪个区域：

1. `AWS_REGION`环境变量（最高优先级）
2. `AWS_DEFAULT_REGION` 环境变量
3. 配置文件中选定的 AWS 配置文件（通过`AWS_PROFILE`环境变量）
4. 配置文件中的默认 AWS 配置文件
5. `us-east-1`如果未找到配置，则默认回退为

> **Note**
>
> AWS 配置文件位于 Linux 和 macOS `~/.aws/config` 上，或者位于 Windows `%USERPROFILE%\.aws\config` 上。

> **Note**
>
> 如果`ATX_CUSTOM_ENDPOINT`已设置，则从终端节点 URL 中提取该区域并覆盖所有其他设置。

设置您的区域

选择以下方法之一来配置您的区域：

选项 1：环境变量（建议临时使用）：

Linux and macOS

```
export AWS_REGION=<your-region>
```

Windows (PowerShell)

```
$env:AWS_REGION="<your-region>"
```

选项 2： AWS CLI 配置（建议永久设置使用）：

```
aws configure set region <your-region>
```

选项 3： Profile-specific 配置：

Linux and macOS

```
aws configure set region <your-region> --profile your_profile_name
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

```
aws configure set region <your-region> --profile your_profile_name
$env:AWS_PROFILE="your_profile_name"
```

选项 4：直接编辑文件：

直接编辑 AWS 配置文件（在 Linux 和 macOS `~/.aws/config` 上，或者`%USERPROFILE%\.aws\config`在 Windows 上）：

```
[default]
region = <your-region>

[profile your_profile_name]
region = <your-region>
```

验证您的区域配置

要检查 AWS 变换自定义将使用哪个区域，请执行以下操作：

检查当前区域设置：

```
aws configure get region
```

检查环境变量：

Linux and macOS

```
echo "AWS_REGION: $AWS_REGION"
echo "AWS_DEFAULT_REGION: $AWS_DEFAULT_REGION"
echo "AWS_PROFILE: $AWS_PROFILE"
```

Windows (PowerShell)

```
echo "AWS_REGION: $env:AWS_REGION"
echo "AWS_DEFAULT_REGION: $env:AWS_DEFAULT_REGION"
echo "AWS_PROFILE: $env:AWS_PROFILE"
```

在调试日志中查看详细的区域解析：

Linux and macOS

```
tail -f ~/.aws/atx/logs/debug.log
```

Windows (PowerShell)

```
Get-Content "$env:USERPROFILE\.aws\atx\logs\debug.log" -Wait -Tail 10
```

显示区域来源的日志输出示例：

```
2026-01-07 22:34:28 [DEBUG]: Initializing FrontendServiceClient with config:
{
  "endpoint": "https://transform-custom.us-east-1.api.aws",
  "region": "us-east-1",
  "regionSource": "AWS_REGION"
}
```

该`regionSource`字段显示该区域的来源（例如，“aws-config（配置文件：默认）”、“AWS_REGION”、“默认”）。

> **Important**
>
> 如果您的区域配置指向不支持的区域，CLI 将显示一条明确的错误消息，说明如何将您的配置更新到支持的区域。

运行你的第一次转型

最快的入门方法是使用 AWS托管转换。 AWS-managed 转换是预先构建的、 AWS经过审查的转换，无需任何设置即可使用。

要以交互方式运行 AWS托管转换，请执行以下操作：

```
atx
```

然后让代理执行转换：

```
Execute the AWS/java-aws-sdk-v1-to-v2 transformation on the codebase at ./my-java-
project
```

要以非交互方式运行转换，请执行以下操作：

```
atx custom def exec -n AWS/java-aws-sdk-v1-to-v2 -p ./my-java-project -c "mvn clean
 install" -x -t
```

有关执行模式、配置选项和命令标志的详细信息，请参见the section called “Command Reference”。

了解转换结果

转换完成后，Trans AWS form custom 会提供一份描述结果的报告。如果转换未经过验证（例如，成功构建 Java 应用程序），则报告将提供进一步操作的建议。

大多数转换都是分多个步骤执行的，使用 Git 提交中间步骤。您可以使用标准 Git 命令查看转换所做的更改：

```
git status
git log
git diff <original commit-id>
```

创建自定义转换

当 AWS托管转换不能满足您的需求时，您可以根据您的特定要求创建自定义转换。

创建自定义转换

1. 在交互模式下 AWS 启动 Transform CLI：

   ```
   atx
   ```

2. 告诉代理您要创建新的转换并描述您的要求。

3. 提供参考资料，例如文档和代码样本以提高质量。
4. 反复测试和完善转换。
5. 将其发布到您组织的转型注册表。

有关创建自定义转换的详细说明，请参阅the section called “工作流”。

AWS 转换 Web 应用程序（可选）

Trans AWS form Web 应用程序是一个可选界面，用于监控跨多个存储库的大规模转型活动。在使用 T AWS ransform Web 应用程序之前，您需要启用用户身份才能在组织中访问 T AWS ransform。有关启用 AWS 转换的信息，请参阅设置 AWS 转换。

要使用 AWS 转换 Web 应用程序，请执行以下操作：

1. 使用 AWS IAM 身份中心证书访问https://aws.amazon.com/transform/并登录。
2. 在 T AWS ransform Web 应用程序中选择 “自定义/代码” 作业类型。
3. 告诉代理您要使用的转换定义的名称。
4. Web 应用程序提供了可以与您的团队共享的 Transf AWS orm CLI 命令。此命令调用转换定义并将执行结果记录到 Web 应用程序。
5. 捕获转换结果后，在控制面板中查看统计数据、节省时间的衡量标准，并询问有关工作进度的问题。

Web 应用程序专为企业级操作而设计，在这些操作中，您需要集中监控多个代码库中的转换。

> **Note**
>
> AWS 需要使用 IAM 身份中心才能访问 Trans AWS form Web 应用程序。CLI 不需要 IAM 身份中心，只需要标准 AWS 证书。

自定义转换命令简介

以下是一些可用于自定义转换的命令。命令的完整列表位于AWS 转换自定义转换命令参考中。

- `atx custom`
  - 执行自定义转换交互式体验，允许创建、发现、执行和完善转换。

  - 这是的默认命令`atx`。
  - `--trust-all-tools(-t)` 是可选的，隐式允许代理请求的所有工具请求。请谨慎使用，尤其是在生产环境中。您可以使用信任设置文件为特定工具和命令配置工具信任。
- `atx custom --help | atx custom -h`
  - 显示帮助菜单。
  - 例如，每个命令还包括一个帮助菜单`atx custom def exec --help`。
- `atx --version | atx -v`
  - 显示版本。
  - 版本号随每个版本而变化。
- `atx custom def list`
  - 打印转换注册表中可用的转换列表。
- `atx custom def exec`
  - 执行转换
- `atx custom def learnings`
  - 打开交互式会话以查看和管理转型从之前的运行中吸取的经验教训
- `atx mcp`
  - 用于管理 MCP 服务器配置

工作流

执行转换

本节介绍执行转换的不同方法和控制执行行为的选项。

执行模式

AWS 自定义转换支持三种执行模式，以适应不同的工作流程。

交互式对话模式

启动 CLI `atx` 并要求代理通过自然语言执行转换。此模式允许您与代理进行全面对话，随时中断执行，并在转换过程中提供反馈。

如果您想要最大限度地控制并能够引导代理完成复杂场景，请使用此模式。

直接交互式执行

用于`atx custom def exec -n <transformation-name> -p <path>`以交互方式开始特定的转换。此模式允许您在执行开始、执行期间或结束时查看代理并与之交互。代理将在关键决策点停下来并征求您的意见。

这非常适合在自动运行变换之前对其进行测试和完善。

你可以在非交互模式或无头模式下运行转换。 Non-interactive 模式会抑制命名转换期间的提示。Headless 模式允许您使用纯文本提示运行代理，完全绕过交互式界面。

Non-interactive 模式

`atx custom def exec -n <transformation-name> -p <path> -x -t`用于完全自动化。添加`-x`以在非交互模式下运行，并在`-t`不提示的情况下自动信任所有工具。

此模式专为无需或不需要人工干预的 CI/CD 管道集成和批量执行而设计。

无头模式

要在不与代理交互的情况下完成任务，请运行`atx -x "<prompt>" -t`并以纯文本形式提供指令。

无头转换执行

使用此模式将现有的转换定义应用于您的代码库。转换会自动运行每个步骤，无需您的批准。

```
atx -x "apply transformation definition <transformation_definition_name> to
 <codebase_path>" -t
```

Headless 转型开发

创建或修改转换定义。

要将旧的转换定义转换为新的技能格式（SKILL.md + references/），请运行以下命令：

```
atx -x "convert <legacy_transformation_definition_name> transformation definition to
 skill and save as draft" -t
```

要创建新的转换定义，请运行以下命令：

```
atx -x "create a transformation definition to <description> with references docs
 <reference_docs_path>" -t
```

常用命令标志

使用执行转换时`atx custom def exec`，通常使用以下标志：

- `-nor --transformation-name`-指定要执行的转换的名称
- `-p`或 `--code-repository-path`-指定代码库的路径（使用 “.” 表示当前目录）
- `-cor --build-command`-指定要运行的生成或验证命令
- `-x`或 `--non-interactive`-启用非交互模式（无用户提示）
- `-t`或者 `--trust-all-tools`-自动信任所有工具，无需提示
- `-d`或 `--do-not-learn`-阻止从此执行中提取课程
- `--tv`或 `--transformation-version`-指定转换的特定版本
- `-g`或 `--configuration`-提供配置文件或内联配置

> **Important**
>
> `-t`或`--trust-all-tools`标志会在不提示的情况下自动批准所有工具的执行，并绕过大多数安全防护栏（除非被覆盖，否则与您的`alwaysPromptCommands`列表匹配的命令仍需要明确的权限）。`trustedShellCommands`传入`--non-interactive`和`--trust-all-tools`是获得完全自主体验所必需的，但不是执行转换所必需的。在生产环境中请谨慎使用。

使用配置文件

AWS 自定义转换支持 YAML 或 JSON 格式的可选配置文件。配置文件允许您指定执行参数并为代理提供其他上下文。

要使用配置文件，请执行以下操作：

```
atx custom def exec --configuration file://config.yaml
```

你也可以将配置作为内联键值对提供：

```
atx custom def exec --configuration "key=value,key2=value2"
```

配置文件示例 (config.yaml)：

```
codeRepositoryPath: ./my-project
transformationName: my-transformation
buildCommand: mvn clean install
additionalPlanContext: |
  The target Java version to upgrade to is Java 17.
  Ensure compatibility with our internal logging framework version 2.3.
validationCommands: |
  mvn test
  mvn verify
```

该additionalPlanContext参数为代理的执行计划提供了额外的上下文。这对于 AWS管理的转换特别有用，可以根据您的特定需求自定义其行为。

生成和验证命令

生成或验证命令是一个可选参数，用于指定在转换过程中如何验证代码。 AWS 如果未指定，Transform custom 将尝试根据转换推断出最佳的构建命令，但建议具体考虑质量。

生成和验证命令的示例：

- Java：`mvn clean install`或 `gradle build`
- Python：`pytest`或 `python -m py_compile`
- Node.js：`npm run build` 或 `npm test`
- Linters：或 `eslint .` `pylint .`

即使对于不需要构建的语言或转换，提供一个命令来验证结果并在验证失败时返回问题，对于提高转换质量也非常重要。

如果不需要构建或验证，请在输入中省略。

控制学习行为

默认情况下，自定义 AWS 转换会从每次转换执行中提取经验教训。您可以阻止学习特定的处决。

要防止从处决中学习，请执行以下操作：

```
atx custom def exec -n my-transformation -p ./my-project -d
```

`-d`或`--do-not-learn`标志选择不允许从当前执行中提取课程。

恢复对话

AWS Transform custom 允许您在创建后的 30 天内恢复之前的对话。

要恢复最近的对话，请执行以下操作：

```
atx --resume
```

要恢复特定对话，请执行以下操作：

```
atx --conversation-id <conversation-id>
```

> **Important**
>
> 对话只能在创建后 30 天内恢复。30 天后，对话将无法再恢复。

追踪代理会议记录

AWS 自定义转换可跟踪在转换会话期间消耗的代理分钟数。座席分钟数在整个对话生命周期中累积，并在对话结束时显示：

```
Agent minutes used: 12.50
```

在中断期间，代理分钟数保持不变。如果您使用 Ctrl+C 中断会话并在稍后恢复，则先前累积的分钟数会延续并继续累积在恢复的会话中。

要在交互式会话期间查看座席会议记录，请执行以下操作：

`/usage`在输入提示符处键入以显示当前累积的座席分钟数，而不会结束对话。

要设置座席分钟数预算限制，请执行以下操作：

```
atx custom def exec -n my-transformation -p ./my-project --limit 30
```

该`--limit`选项为会话设置座席分钟数的最大预算。座席分钟数反映的是活跃座席的工作时间，而不是挂钟时间。达到限制后，CLI 会显示一条消息并退出并显示恢复指示：

```
## Budget limit reached: 30.00 / 30.00 Agent Minutes. Exiting.
```

您可以稍后恢复对话，但限制有所增加：

```
atx --conversation-id <conversation_id> -t --limit <increased_limit>
```

持续学习

本节介绍如何复习和管理持续学习所产生的课程。

理解教训

持续学习系统会自动从之前的转型中提取经验教训。系统基于以下条件异步创建它们：

- 在交互模式下提供的开发者反馈
- 转换过程中遇到的代码问题

当你跨不同的代码库运行转换时，经验会随着时间的推移而积累。系统会自动应用它们来改进 future 的运行。每节课都属于一个类别，其中包含所有属于相似领域的课程，因此您可以一起复习相关的课程。对于你不想使用的课程，你可以将课程全部存档或删除。

查看和管理课程

使用`learnings`命令打开交互式会话，用于浏览和管理转换定义的课程。

要打开课程查看器，请执行以下操作：

```
atx custom def learnings -n my-transformation
```

查看器会打开课程类别列表，每个类别都显示其包含的活跃课程数量。选择一个类别以查看其课程，然后选择一节课以查看其全部细节，包括课程正文、其影响以及之前有多少次课程参考了该课程。

归档和恢复课程

系统会自动应用课程。如果您不希望系统应用课程，则可以将其存档。系统会保留已存档的课程，但不会将其应用于 future 的课程。所有存档的课程都分组在一起，因此您可以查看它们并将任何课程恢复为活跃使用。

删除课程

永久移除无用的课程。删除操作无法撤消，系统可能会从 future 的运行中重新学习已删除的课程。

课程必须先存档，然后才能将其删除。

高级配置

本节介绍了 Transform custo AWS m 的高级功能和配置选项。

环境变量

您可以使用环境变量自定义 CLI 行为。

> **Note**
>
> 以下示例显示了 Linux 和 macOS 的语法 () `export`。在 Windows 上，在 PowerShell 使用中设置环境变量`$env:NAME="value"`。有关等效的命令，请参阅 Windows (PowerShell) 选项卡。

ATX_SHELL_TIMEOUT

覆盖 shell 命令的默认超时时间（ 900 seconds/15 分钟 ）。

Linux and macOS

```
export ATX_SHELL_TIMEOUT=1800  # 30 minutes
```

Windows (PowerShell)

```
$env:ATX_SHELL_TIMEOUT=1800  # 30 minutes
```

这对于大型代码库或长时间运行的构建过程很有用。

ATX_DISABLE_UPDATE_CHECK

在命令执行期间禁用自动版本检查和更新通知。

Linux and macOS

```
export ATX_DISABLE_UPDATE_CHECK=true
```

Windows (PowerShell)

```
$env:ATX_DISABLE_UPDATE_CHECK="true"
```

ATX_GIT_COMMITTER_NAME 和 ATX_GIT_COMMMITTER_EMAIL

配置 Transform custom 在 AWS 转换期间应用更改时在仓库中创建的检查点提交所使用的作者身份。如果未设置这些变量，则检查点提交将归因于默认身份 (ATX Bot <checkpoint@atx.bot>)。将两个变量都设置为将检查点归因于特定作者。

Linux and macOS

```
export ATX_GIT_COMMITTER_NAME="Jane Developer"
export ATX_GIT_COMMITTER_EMAIL="jane@example.com"
```

Windows (PowerShell)

```
$env:ATX_GIT_COMMITTER_NAME="Jane Developer"
$env:ATX_GIT_COMMITTER_EMAIL="jane@example.com"
```

信任设置

信任设置允许您在没有提示的情况下预先批准要执行的特定工具和命令。无论信任级别如何，您也可以要求为特定 shell 命令提供明确权限。这些设置在 ~/.aws/atx/trust-settings.yaml 文件中进行配置。

该文件包含三个列表：

- trustedTools-无需提示即可执行的工具
- trustedShellCommands-无需提示即可执行的 Shell 命令
- alwaysPromptCommands-无论-t标志或会话信任如何，除非被覆盖trustedShellCommands，否则需要显式权限的 Shell 命令模式。在非交互模式 (-x) 中不会强制使用这些模式。

默认可信工具：

- file_read
- get_transformation_from_registry

- `list_available_transformations_from_registry`

编辑信任设置：

您可以手动编辑 trust-settings.yaml 文件以添加或删除受信任的工具和命令。两者`trustedShellCommands`都`alwaysPromptCommands`支持使用 glob 通配符模式。*

> **Note**
>
> 如果命令与两个列表都匹配，`trustedShellCommands`则优先。

以下内容描述了每个命令列表并提供了示例：

- `trustedShellCommands`-与这些模式匹配的命令在不提示的情况下执行，绕过所有其他护栏。模式与完整的命令字符串相匹配。

  示例：

  - `cd *`-匹配以 cd 开头的复合命令
  - `*&&*`-信任所有带有 && 运算符的命令
- `alwaysPromptCommands`-匹配这些模式的命令需要明确的权限，除非被覆盖`trustedShellCommands`，无论`-t`标志或会话信任如何。在非交互模式 (`-x`) 中不会强制使用这些模式。模式与复合表达式（&&、||、命令替换）中的每个子命令进行匹配。

  示例：

  - `rm -rf *`-总是提示输入递归强制删除命令
  - `sudo *`-始终提示使用 sudo 运行的命令
  - `find * -exec *`-始终使用-exec 提示输入查找命令

Session-level 信任：

在交互式提示中，您可以选择：

- `(y)es`-执行一次
- `(n)o`-拒绝
- `(t)rust`-仅限当前会话的信任

Session-level 信任设置是临时的，在 CLI 重新启动时会重置，无需永久修改 trust-settings.yaml 即可提供临时批准。

> **Note**
>
> 会话信任不适用于与您的`alwaysPromptCommands`列表匹配的命令。

模型上下文协议 (MCP) 服务器

T AWS ransform CLI 支持模型上下文协议 (MCP) 服务器，该服务器通过其他工具扩展其功能。

配置：

在`~/.aws/atx/mcp.json`文件中配置 MCP 服务器。T AWS ransform CLI 支持两种类型的 MCP 服务器：基于命令的本地服务器和远程 HTTP 服务器。

基于命令的本地服务器：

本地服务器作为子进程在您的计算机上运行。使用以下`command`属性对其进行配置：

```
{
  "mcpServers": {
    "my-local-server": {
      "command": "npx",
      "args": ["-y", "@example/mcp-server"]
    }
  }
}
```

远程 HTTP 服务器：

远程服务器连接到托管在 HTTP 或 HTTPS 网址上的 MCP 服务器。使用以下`url`属性对其进行配置：

```
{
  "mcpServers": {
    "my-remote-server": {
      "url": "https://api.example.com/mcp",
      "headers": {
        "Authorization": "Bearer ${MCP_API_TOKEN}"
      }
    }
```

```
  }
}
```

该headers属性是可选的，支持使用${VAR_NAME}语法扩展环境变量。这允许您将 API 令牌等敏感值存储在环境变量中，而不是存储在配置文件中。

配置属性：

基于命令的本地服务器支持以下属性：

- command（必需）-运行服务器的命令
- args（可选）-命令行参数数组
- env（可选）-要传递给服务器进程的环境变量

远程 HTTP 服务器支持以下属性：

- url（必填）-远程 MCP 服务器的 HTTP 或 HTTPS 网址
- headers（可选）-请求中要包含的 HTTP 标头，支持${VAR_NAME}环境变量扩展

管理 MCP 服务器：

查看已配置的 MCP 服务器列表：

```
atx mcp tools
```

列出特定 MCP 服务器提供的可用工具：

```
atx mcp tools --server <server-name>
```

使用情况跟踪：

在转换执行期间，CLI 会自动跟踪 MCP 工具的使用情况。使用情况统计信息保留mcp_usage.json在旁边metadata.json的对话目录中。该文件记录每次执行的每个工具的指标，包括：

- 每个工具的调用次数
- 每个工具的错误数
- 每个工具的总执行时间

- 上次错误详情（如果有）

Client-Side 技能

Client-side 技能是在转换执行期间扩展代理的附加能力。它们允许您提供自定义工具、脚本和指令，代理可以将其与其内置功能一起使用。

技能发现目录：

技能按优先顺序从四个目录中找到。如果同名技能存在于多个目录中，则列表中的第一个目录优先：

1. `<project>/.aws/atx/skills/`- Project-level， AWS 变换 CLI-specific
2. `<project>/.agents/skills/`- Project-level，跨客户端（适用于任何兼容的代理工具）
3. `~/.aws/atx/skills/`- User-level， AWS 变换 CLI-specific
4. `~/.agents/skills/`- User-level，跨客户端（适用于任何兼容的代理工具）

这些`.aws/atx/skills/`目录特定于 Trans AWS form CLI。这些`.agents/skills/`目录是跨客户端的，这意味着除了 Trans AWS form CLI 之外，任何兼容的代理工具都可以使用放在那里的技能。

技能目录结构：

每个技能都是一个目录，其中包含一个带有 YAML frontmatter 的`SKILL.md`文件：

```
~/.aws/atx/skills/
### my-skill/
    ### SKILL.md          # Required: frontmatter + instructions
    ### references/       # Optional: reference docs the agent can read
    #   ### guide.md
    ### scripts/          # Optional: scripts the agent can execute
        ### validate.py
```

SKILL.md 格式：

```
---
name: my-skill
description: When to use this skill
---
# Skill Title

Instructions for the agent...
```

该name字段必须与父目录名称匹配。

禁用技能：

要防止在不移除技能文件的情况下加载技能，请在 frontmatt disable-model-invocation: true er 中添加：

```
---
name: my-skill
description: When to use this skill
disable-model-invocation: true
---
```

设置此属性后，CLI 将在发现期间跳过该技能。除非转换定义明确指示代理读取技能文件，否则代理无法查看或使用该技能。使用它可以暂时禁用某项技能，将其标记为正在进行中，或者保留仅供人类读者使用的参考资料。

> **Note**
>
> 已禁用技能的文件仍保留在磁盘上。如果转换定义指示代理读取特定的文件路径，则代理仍然可以访问内容。该disable-model-invocation属性可防止自动发现和上下文注入，而不是文件系统访问。

按执行模式划分的技能可用性：

- 执行模式（ atx custom def exec有--code-repository-path ）-从用户级和项目级目录中发现技能。
- 交互模式 (atx)-最初只发现用户级别的技能。当您在会话期间提供代码存储库路径时，还会加载项目级技能。

验证技能发现：

运行后查看 CLI 的调试日志，以验证发现了哪些技能：

Linux and macOS

```
grep -i "skill" ~/.aws/atx/logs/debug.log | tail -20
```

Windows (PowerShell)

```
Select-String -Pattern "skill" "$env:USERPROFILE\.aws\atx\logs\debug.log" | Select-Object -Last 20
```

未通过验证的技能将被跳过，并在调试日志中显示警告。

> **Note**
>
> Client-side 技能需要 CLI 版本 2.0 或更高版本。

在 Project-Level 和 User-Level 技能之间做出选择

你将技能放在哪里，决定谁能从中受益，以及技能何时激活。

Project-level 技能 (`<project>/.aws/atx/skills/`):

将它们提交给版本控制，这样每个对仓库运行转换的团队成员都会自动发现它们。使用项目等级技能获得：

- Repository-specific 合规性检查（Dockerfile 规则、Terraform 策略、迁移安全验证器）
- 适用于此代码库的组织编码标准（可观察性模式、错误处理、命名约定）
- 生成或测试项目特有的脚本（自定义 linter、架构适应性函数）
- 此存储库中使用的内部库的 API 迁移指南

User-level 技能 (`~/.aws/atx/skills/`):

无论您以哪个存储库为目标，它们都会保留在您的计算机上，并在所有转换过程中激活。将用户级别的技能用于：

- 个人工作流程工具（变更日志生成器、提交消息格式化工具）
- Cross-project 首选项（首选测试模式、文档风格提醒）
- 您的组织要求对所有存储库进行许可证合规性检查
- 您在使用的每个代码库上强制执行的覆盖范围阈值或质量门槛

有效技能小贴士：

- 在SKILL.md前面写下清晰的description字段。代理使用此字段来决定何时与某项技能相关。
- 成功时使用代码 0 退出验证脚本，失败时使用非零代码退出验证脚本。代理解释退出代码以确定合规性。
- 在脚本中打印清晰、可操作的错误消息。代理读取输出以了解要修复的内容。
- 将技能放在任一级别的跨客户端目录 (.agents/skills/) 中，以便与 T AWS ransform CLI 之外的其他 AI 开发工具共享这些技能。

Client-Side 技能示例

这些示例显示了两种常见模式：基于脚本的验证技能和仅供参考的技能。

示例：Dockerfile 合规性检查器 () Script-Based

该技能可根据安全和操作最佳实践验证 Dockerfile。它使用验证脚本，代理在进行更改之前和之后都运行该脚本。

目录结构：

```
.aws/atx/skills/
### dockerfile-compliance/
    ### SKILL.md
    ### scripts/
    #   ### lint_dockerfile.sh
    ### references/
        ### dockerfile-best-practices.md
```

SKILL.md:

```
---
name: dockerfile-compliance
description: Validates Dockerfiles against security and operational best practices
---
# Dockerfile Compliance Checker

When a transformation creates or modifies Dockerfiles, run the compliance checker.

## When to use

- After creating a new Dockerfile
- After modifying FROM, RUN, USER, or EXPOSE directives
```

```
- When containerizing an application as part of a transformation

## How to use

Run: `bash scripts/lint_dockerfile.sh <path-to-Dockerfile>`

If violations are found, consult `references/dockerfile-best-practices.md`
for compliant patterns.
```

验证脚本会检查未固定的基础图像标签、以 root 身份运行、ENV指令中的硬编码密钥以及缺少的定义。HEALTHCHECK代理运行脚本，使用参考文件中的模式修复违规行为，然后重新运行脚本以确认合规性。

示例：API 弃用助手 () Reference-Only

此技能指导代理在升级转换期间替换已弃用的 API 调用。它只使用没有脚本的参考文件。

目录结构：

```
.aws/atx/skills/
### api-deprecation-helper/
    ### SKILL.md
    ### references/
        ### aws-sdk-v2-to-v3.md
        ### react-class-to-hooks.md
```

SKILL.md:

```
---
name: api-deprecation-helper
description: Guides the agent through replacing deprecated API calls with modern
 equivalents
---
# API Deprecation Helper

When performing upgrade transformations, use this skill to identify and replace
deprecated API calls with their modern equivalents.

## When to use

- During any version upgrade transformation
- When build warnings mention deprecated APIs
```

```
- When transforming code that uses legacy patterns

## Process

1. Identify deprecated API calls in the codebase
2. For each deprecated call, find the replacement in `references/`
3. Apply the replacement, preserving the original behavior
4. Verify the replacement compiles and tests pass
```

参考文件包含之前和之后的代码示例。例如，使用S3Client和将模式aws-sdk-v2-to-v3.md映射s3.putObject(params).promise()到模块化 v3 等效版本PutObjectCommand。

标签和组织

您可以使用标签组织转换，以便进行访问控制和分类。

> **Note**
>
> 其中一些命令需要为转换定义指定 Amazon 资源名称 (ARN)。ARN 结构为：arn:aws:transform-custom:<region>:<account-id>:package/<td-name>

要列出转换的标签，请执行以下操作：

```
atx custom def list-tags --arn <transformation-arn>
```

要为转换添加标签，请执行以下操作：

```
atx custom def tag --arn <transformation-arn> --tags '{"env":"prod","team":"backend"}'
```

要从转换中移除标签，请执行以下操作：

```
atx custom def untag --arn <transformation-arn> --tag-keys "env,team"
```

标签可用于 IAM 策略中的分组访问控制。您可以创建策略，授予所有带有特定标签的转换（例如，所有用team:frontend或environment:production标记的转换）的权限。

日志

AWS Transform CLI 维护三种类型的日志，用于故障排除和调试。

对话日志：

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/<timestamp>-conversation.log
```

Windows

```
%USERPROFILE%\.aws\atx\custom\<conversation_id>\logs\<timestamp>-conversation.log
```

这些日志包含特定会话的完整对话历史记录。

子代理日志：

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/subagents/<name>.log
```

Windows

```
%USERPROFILE%\.aws\atx\custom\<conversation_id>\logs\subagents\<name>.log
```

这些日志包含主代理在变换期间生成的子代理的输出。您无需直接管理子代理。

开发者调试日志：

Linux and macOS

```
~/.aws/atx/logs/debug*.log
~/.aws/atx/logs/error.log
```

Windows

```
%USERPROFILE%\.aws\atx\logs\debug*.log
%USERPROFILE%\.aws\atx\logs\error.log
```

这些日志为 CLI 本身提供了高级故障排除信息。

> **Note**
>
> 日志目录中可能有多个调试日志文件（即 debug1.log、debug2.log）。查看并提供所有相关日志，例如 ~/。 aws/atx/custom/ <conversation-id>/* 和 ~/。 aws/atx/logs/ *，当打开支持请求时，可以更快地解决问题。

CLI 更新

保持您的 CLI 处于最新状态，以访问新功能和改进。

要检查更新，请执行以下操作：

```
atx update --check
```

要更新到最新版本，请执行以下操作：

```
atx update
```

要更新到特定版本，请执行以下操作：

```
atx update --target-version <version>
```

创建自定义变换

本节介绍如何创建、修改和管理自定义转换定义。

创建新的转换

使用交互式 CLI 创建新的转换定义。

创建转换定义

1. 启动 AWS 转换 CLI：

   ```
   atx
   ```

2. 告诉代理您要创建新的转换。
3. 对转型目标进行清晰、详细的描述。包含：

   - 源和目标状态（例如，“从版本 X 升级到版本 Y”）

- 需要进行特定更改（例如，“更新导入语句，替换已弃用的方法”）
- 任何特殊考虑或限制

4. 当代理人要求澄清或其他信息时，请提供具体的示例和参考材料。
5. 查看代理创建的初始转换定义。
6. 在示例代码库上测试转换。
7. 通过提供反馈、代码修复或其他示例进行迭代。
8. 将转换保存到本地或将其发布到注册表。

创建转换的最佳实践：

- 先从简单、定义明确的转换开始，然后再尝试复杂的转换
- 提供全面的参考资料，包括迁移指南和代码示例
- 发布前在多个示例代码库上进行测试
- 使用确定性构建或验证命令来实现持续学习
- 考虑将复杂的转换分解为多个较小的步骤
- 在转换定义中用 “CRITICAL:” 或 “重要:” 标记关键信息，以确保代理对这些要求进行优先排序
- 当您需要遵循确切的要求时（例如使用特定的命令或字符串值），请在转换定义中明确指定完整的字符串。你可以将它们用bash引号包起来，以清楚地表明它们是终端命令或文字字符串，这样可以减少可变性并确保一致的执行

提供参考资料

您可以通过在对话期间指定文件路径来向 T AWS ransform custom 提供参考文件。这些文件存储在转换定义的`references/`文件夹中。

推荐的参考文件类型：

- Before/after 示例代码
- 所涉及的 API、库或功能的文档
- Human-readable 迁移指南

要提供参考文件，请执行以下操作：

```
Take a look at the documentation here: /path/to/migration-guide.md
```

您也可以提供一个包含多个参考文件的目录：

```
Take a look at the docs we have here: /path/to/docs/
```

> **Note**
>
> 仅支持基于文本的文件（.md、.html、.txt、代码文件）。目前不支持二进制文件、图像和富文本文件（例如.pdf、.png、.docx）。通常可以提取文本内容并将其用作参考。如果您有许多小文本文件，可以考虑将它们连接成几个具有描述性名称的文件。所有文件的总容量限制为10MB。

修改现有转换

在将自定义变换保存为草稿或发布它们之前和之后，都可以对其进行修改。您无法修改 AWS由管理的转换。如果您需要对其进行自定义，则可以使用配置文件提供其他上下文。

修改现有转换

1. 启动 AWS 转换 CLI：

   ```
   atx
   ```

2. 告诉代理您要修改现有转换。
3. 选择是否：

   - 为本地存储的转换提供文件路径（即不是已保存的草稿或已发布的草稿）
   - 向注册表索取转换列表
4. 如果从注册表中选择，请选择要修改的转换。
5. 与代理合作，描述您要进行的更改。
6. 在示例代码库上测试更新的转换。
7. 如果需要，可以将更新发布到注册表。

发布和管理转换

您可以使用交互式体验或使用以下命令来发布和管理您的转换。

要将转换另存为草稿，请执行以下操作：

```
atx custom def save-draft -n my-transformation --description "Description of the
 transformation" --sd ./transformation-directory
```

要发布转换，请执行以下操作：

```
atx custom def publish -n my-transformation --description "Description of the
 transformation" --sd ./transformation-directory
```

要列出可用的变换，请执行以下操作：

```
atx custom def list
```

要下载转换定义，请执行以下操作：

```
atx custom def get -n my-transformation
```

这会将转换定义下载到您当前的工作目录。您可以使用标志指定目标目录和带有`--td`--`tv`标志的版本。

要删除转换定义，请执行以下操作：

```
atx custom def delete -n my-transformation
```

> **Important**
>
> 这将从您的账户中永久删除指定的转换定义。

管理转换版本

AWS 自定义转换会维护转换定义的版本。您可以在执行或下载转换时指定版本。

要执行特定版本，请执行以下操作：

```
atx custom def exec -n my-transformation --tv v1 -p ./my-project
```

要下载特定版本，请执行以下操作：

```
atx custom def get -n my-transformation --tv v1
```

如果未指定版本，则使用最新版本。

Command Reference

本节提供了所有 AWS 转换自定义 CLI 命令的全面参考。

交互式命令

atx

使用 Trans AWS form CLI 开始交互式对话。

```
atx                          # Start new conversation
atx --resume                 # Resume most recent conversation
atx --conversation-id <id>   # Resume specific conversation
atx -t                       # Start with all tools trusted
```

交互式会话命令

在交互式会话中，可以在输入提示符下键入以下命令：

- `/usage`-显示当前会话的累计代理分钟数

转换定义命令

atx custom def exec

在代码存储库上执行转换定义。

Option	长格式	参数	说明
`-p`	`--code-repository-path`	`<path>`	要转换的代码存储库的路径。对于当前目录，请使用“。”
`-c`	`--build-command`	`<command>`	构建存储库时要运行的命令

Option	长格式	参数	说明
-n	--transformation-name	<name>	注册表中转换定义的名称
-x	--non-interactive	-	在没有用户帮助的情况下运行转换
-t	--trust-all-tools	-	信任所有工具（没有工具提示）
-d	--do-not-learn	-	选择不允许从本次执行中提取课程
-g	--configuration	<config>	配置文件（JSON 或 YAML）或键值对的路径
--tv	--transformation-version	<version>	要使用的转换定义的版本
--limit	--limit	<limit>	设置代理分钟数预算限制。当达到限制时会退出转换，并且可以通过增加限制来恢复
-h	--help	-	显示命令帮助

atx 自定义定义列表

列出可用的转换定义。

```
atx custom def list
atx custom def list --json    # Output in JSON format
```

atx 自定义防御获取

获取特定转换定义的详细信息。

Option	长格式	参数	说明
-n	--transformation-name	<name>	要检索的转换定义的名称
--tv	--transformation-version	<version>	要检索的转换定义的版本
--td	--target-directory	<directory>	保存转换定义的目标目录（默认：“。”）
--json	--json	-	以 JSON 格式输出响应
-h	--help	-	显示命令帮助

atx 自定义定义删除

永久删除转换定义。

```
atx custom def delete -n <transformation-name>
```

atx 自定义定义发布

将转换定义发布到注册表。

Option	长格式	参数	说明
-n	--transformation-name	<name>	要发布的转换定义的名称
--tv	--transformation-version	<version>	要使用的转换定义的版本（不适用于--description或--source-directory）

Option	长格式	参数	说明
--sd	--source-directory	<directory>	从中读取本地转换定义文件的源目录（不适用于--transformation-version）
--description	--description	<description>	对转换定义的描述（不适用于--transformation-version）
--json	--json	-	以 JSON 格式输出响应
-h	--help	-	显示命令帮助

atx 自定义 def 保存草稿

将转换定义另存为注册表中的草稿。草稿将在 30 天后过期，并且不会显示在注册表中。此命令返回草稿的版本号。必须使用转换名称和版本号显式执行和检索草稿。

```
atx custom def save-draft -n <transformation-name> --description "Description" --sd
 <directory>
```

课程命令

atx 自定义防御学习

打开交互式会话，查看和管理转换定义从之前的运行中吸取的经验教训。按类别浏览课程，查看课程详情，并存档、恢复或删除课程。

```
atx custom def learnings -n <transformation-name>
```

标记命令

atx 自定义定义列表标签

列出转换定义的标签。

```
atx custom def list-tags --arn <transformation-arn>
```

atx 自定义 def 标签

向转换定义添加标签。

```
atx custom def tag --arn <arn> --tags '{"env":"prod","team":"backend"}'
```

atx 自定义定义取消标记

从转换定义中移除标签。

```
atx custom def untag --arn <arn> --tag-keys "env,team"
```

更新命令

税务局更新

更新 AWS 转换 CLI。

```
atx update                    # Update to latest version
atx update --check            # Check for updates only
atx update --target-version <version>  # Update to specific version
```

MCP 命令

atx mcp 工具

允许客户使用 view/confirm 其 MCP 工具配置。必须通过 ~/ 文件直接管理配置的更新。 aws/atx/mcp.json

```
atx mcp tools     # View list of MCP servers
atx mcp tools -s    # List tools for the specified server
```

AWS-托管转型

AWS-managed 转换是预先构建的、 AWS经过审查的转换，适用于常见用例，无需任何其他设置即可使用。

概述

AWS-管理的转换具有以下特征：

- 验证者 AWS-这些转换经过审核 AWS ，质量很高
- 随时可用-无需额外设置
- 持续增长-不断添加其他转换
- 可定@@ 制-可以通过使用`additionalPlanContext`配置参数提供针对组织需求的额外指导或要求来定制 Pre-built 转换
- 抢先体验支持-某些变更可能会被标记为抢先体验，因为它们经过进一步的测试和完善

可用 AWS-托管转型

以下目录按用例分组列出了当前可用的 AWS托管转换。每个表都显示转换名称、其适用的语言或堆栈及其状态。要快速找到转换，请使用本页顶部的搜索框按名称、语言或用例进行搜索。

此目录是托管转换的 AWS规范列表。Kiro Power、代理插件、VS Code 插件和 CLI 都运行相同的转换。要列出注册表中可用的转换，请运行`atx custom def list`。

> **Note**
>
> 标有 “抢先体验” 的转换可以正常运行，但可能会根据客户反馈经常更新。

运行时升级

将语言或运行时升级到新版本，或者更改运行时分布。

转换	语言/堆栈	Status	说明
`AWS/java-version-upgrade`	Java	正式发布	使用任何编译系统将 Java 应用程序从任何源 JDK 版本升级到任何目标 JDK 版本，依赖关系现代化包括 Jakarta EE 迁移、数据库驱动程序、ORM

转换	语言/堆栈	Status	说明
			框架和 Spring 生态系统更新。在聊天中或使用additionalPlanContext 参数指定目标 JDK 版本。
AWS/python-version-upgrade	Python	正式发布	将 Python 项目从 Python 3.8 或 3.9 迁移到 Python 3.11、3.12 或 3.13，同时保持功能和性能。在聊天中或使用additionalPlanContext 参数指定目标 Python 版本。
AWS/nodejs-version-upgrade	Node.js	正式发布	将 Node.js 应用程序从任何源 Node.js 版本升级到任何目标 Node.js 版本。在聊天中或使用additionalPlanContext 参数指定目标版本。
AWS/lambda-nodejs-runtime-upgrade	Node.js (Lambda)	抢先体验	将 AWS Lambda 函数从较旧的 Node.js 运行时（nodejs4.3 到 nodejs22.x）升级到 nodejs24.x，以解决 Lambda 运行时接口客户端 (RIC) 和 24 语言运行时中的重大变化。 Node.js

转换	语言/堆栈	Status	说明
AWS/oracle-java-to-corretto	Java（JDK 发行版）	抢先体验	将 Java 项目从 Oracle JDK 迁移到 Amazon Corretto。将 Oracle-specific 内部 API 替换为标准 Java 等效项，更新编译配置（Maven 和 Gradle）和容器基础镜像，移除商用 JVM 标志，并生成许可报告。
AWS/ruby-upgrade	Ruby	抢先体验	将 Ruby 应用程序从 Ruby 2.x 升级到 Ruby 4.0，将其框架升级到 Rails 8.0 或 Sinatra 4.1。你可以将这种转换与 Rails 和 ActiveRecord 应用程序、Sinatra 应用程序和独立 gem 一起使用。该转换将每个 Ruby 版本与匹配的框架升级配对，然后运行测试套件。然后，它会在升级到下一个版本之前隔离故障。

软件开发工具包迁移

在 AWS SDK 的主要版本之间迁移。

转换	语言/堆栈	Status	说明
AWS/java-aws-sdk-v1-to-v2	Java	正式发布	使用 Maven 或 Gradle 将 Java 项目的 AWS SDK 从 v1 升级到 v2。
AWS/python-boto2-to-boto3	Python	正式发布	根据官方迁移文档，将 Python 应用程序从 boto2 迁移到 boto3。AWS
AWS/nodejs-aws-sdk-v2-to-v3	Node.js	正式发布	无需更改版本，即可将 Node.js 应用程序从 JavaScript v2 Node.js 版 AWS SDK 升级到 v3，以获得模块化架构、一流 TypeScript 支持和更高的性能。

框架升级和迁移

将框架升级到新版本，或迁移到其他框架。

转换	语言/堆栈	Status	说明
AWS/spring-boot-version-upgrade	Java /春靴	正式发布	将较旧的 Spring Boot 应用程序升级到目标 Spring Boot 版本，包括构建文件和启动程序、属性、Jackson 3 软件包、Spring Security 7 DSL、测试基础架构和可观察性依赖项。

转换	语言/堆栈	Status	说明
AWS/JBoss-to-Spring-Boot	Java (JBoss 或者 WildFly 到 Spring Boot)	抢先体验	将在 JBoss EAP 上运行的 Java EE 或 Jakarta EE 企业应用程序迁移 WildFly 到 Spring Boot，从而消除云原生容器化部署模型对应用程序服务器的依赖。
AWS/early-access-angular-to-react-migration	反应有角度	抢先体验	将 Angular 应用程序转换为 React。
AWS/angular-version-upgrade	Angular	抢先体验	将较旧的 Angular 应用程序升级到目标 Angular 版本，包括组件、服务、模板和路由。
AWS/vue.js-version-upgrade	Vue.js	抢先体验	执行从 Vue.js 2 到 Vue.js 3 的主要版本升级，对组件、状态管理、路由和全局 API 进行现代化改造。次要更新和补丁更新不在范围内。

GenAI 和模型迁移

将生成式 AI 工作负载迁移到.

转换	语言/堆栈	Status	说明
AWS/GenAI-to-Bedrock-Migration-Assessment	生成式 AI 工作负载	抢先体验	评估生成式人工智能工作负载，以便从第三方提供商（OpenAI、Google Gemini、Anthropic direct 和开源模型）迁移到。发现 SDK 的使用情况和模型，阐明需求，设计模型映射，估算成本和风险，并生成评估项目。 Assessment-only; 不修改源代码。还涵盖代理框架，例如 Crewal LangGraph、和 Strands。

Language-to-language 迁移

将代码库从一种编程语言翻译成另一种编程语言。

转换	语言/堆栈	Status	说明
AWS/vba-to-python-migration	VBA 到 Python	抢先体验	使用 openpyxl、pandas、tkinter 或 6 以及标准库将 Excel VBA 宏、模块和嵌入式逻辑迁移到等效的 Python 脚本和模块。 UserForms PyQt目标语言是 Python 3.8 或更高版本。在转换 .bas、.cls、.frm 或嵌

转换	语言/堆栈	Status	说明
			入.xlsm 的 VBA 代码时使用。

数据库迁移

目前没有特定于数据库的 AWS托管转换可用。要将微软 SQL Server 数据库及其关联的.NET 应用程序现代化为亚马逊 Aurora PostgreSQL，请参阅。the section called “SQL 服务器现代化”

可观测性

将日志记录和监控现代化为 AWS原生服务。

转换	语言/堆栈	Status	说明
`AWS/early-access-log4j-to-slf4j-migration`	Java（日志记录）	抢先体验	使用 Logback 后端将 Java 应用程序从 Log4j（1.x 或 2.x）迁移到带有 Logback 后端的 SLF4J。处理源代码、依赖关系管理（Maven 和 Gradle）和日志配置文件，并通过编译、测试和剩余导入扫描进行验证。
`AWS/datadog-monitors-to-cloudwatch-alarms`	基础设施即代码/监控	抢先体验	将跟踪 AWS 服务指标和自定义指标的指标监控器作为基础架构即代码迁移 DataDog 到原生 CloudWatch 警报。生成 CloudFormation YAML、CDK

转换	语言/堆栈	Status	说明
			TypeScript 和 Terraform HCL。

架构

Re-architect、重新构建平台或优化应用程序。 AWS

转换	语言/堆栈	Status	说明
`AWS/java-performance-optimization`	Java（性能）	正式发布	通过分析 JFR 分析数据来检测 CPU 和内存热点以及反模式，然后应用有针对性的代码修复，从而优化 Java 应用程序的性能。有关收集 JFR 数据的说明，请参阅 JFR 运行时指南。
`AWS/early-access-java-x86-to-graviton`	Java（Arm64 / Graviton）	抢先体验	验证 Java 应用程序与 Grav AWS iton 处理器的 Arm64 架构的兼容性，并通过更新依赖关系、检测特定架构的代码模式以及在源代码可用时重新编译原生库来解决不兼容问题。许多现代 Java 应用程序已经存在 Arm64-compatible。
`AWS/oracle-service-bus-to-aws`	Java/集成到无服务器	抢先体验	将 Oracle 服务总线 (OSB) 和 BPEL 流程配置迁移到

转换	语言/堆栈	Status	说明
			AWS原生无服务器架构， TypeScript 使用 Amazon API Gateway、Lambda AWS 和 Step Functions 生成可部署的 CDK 项目。 AWS
AWS/mulesoft-to-aws-native	Java/ MuleSoft 到无服务器	抢先体验	将 MuleSoft Mule 3.x 和 4.x 应用程序转换为以 Lambda 上的 Java 17 为目标的 AWS 无服务器架构（亚马逊 API Gateway AWS 、Lambda 和 Step F AWS unctions） AWS SnapStart 转换将流触发器映射到 AWS 事件源，转换 DataWeave 和 MEL（MuleSoft 表达式语言）表达式为 AWS 等效表达式，并将连接器替换为 AWS SDK for Java v2 调用。它生成 SAM 模板、 AWS Lambda 处理程序和 JUnit 5 测试。

转换	语言/堆栈	Status	说明
AWS/payshield-hsm-to-aws-payment-cryptography	Java（从密码管理到 AWS 支付密码学）	正式发布	将 Java 应用程序从泰雷兹 PayShield 硬件安全模块 (HSM) 协议迁移到 AWS 支付密码学 SDK v2。迁移包括命令映射、密钥迁移、依赖关系设置和奇偶校验测试。

代码库分析

分析代码库和产品组合以规划现代化。这些转换会生成报告，并且不会修改您的代码。

转换	语言/堆栈	Status	说明
AWS/comprehensive-codebase-analysis	多种语言	正式发布	对代码库进行深度静态分析，生成分层、交叉引用的文档，该文档结合了行为分析、架构文档和商业智能，重点是技术债务见解。
AWS/agentic-readiness-analysis	多种语言	抢先体验	评估系统是否已准备好被 AI 代理安全调用，包括 API、身份、状态管理、人机在环和可观察性。
AWS/modernization-readiness-analysis	多种语言	抢先体验	扫描产品组合以了解云原生成熟度差距，并将发现结果与 AWS 现代化路径对应起来。

转换	语言/堆栈	Status	说明
AWS/portfolio-agentic-readiness-analysis	Portfolio	抢先体验	汇总应用程序组合中的各个代理就绪情况分析报告，以确定跨领域障碍、共同的补救模式和按优先顺序排列的建议。
AWS/portfolio-modernization-readiness-analysis	Portfolio	抢先体验	将整个投资组合中的个人现代化分析报告汇总成一个合并的路线图，其中包含优先考虑的迁移浪潮和推荐的现代化路径。
AWS/business-rules-extraction	多种语言	抢先体验	此转换会静态分析整体代码库以生成可重写的文档，而无需构建、运行或修改源代码。它将系统分解为有界域，并提取每个域的业务规则、工作流程、跨领域问题和数据库结构。输出包括机器可读的清单、交互式仪表板以及每个域的语言中立实现规范，以指导现代化或完全重写。

自定义 AWS-托管转型

您可以通过`additionalPlanContext`配置 AWS参数提供其他上下文，自定义托管转换以满足组织的特定需求。

示例：自定义 Java 版本升级

```
codeRepositoryPath: ./my-project
transformationName: AWS/java-version-upgrade
buildCommand: mvn clean install
additionalPlanContext: |
  The target Java version to upgrade to is Java 17.
  Update all internal library dependencies to versions compatible with Java 17.
  Ensure compatibility with our custom authentication framework.
```

示例：自定义 AWS SDK 迁移

```
codeRepositoryPath: ./my-project
transformationName: AWS/java-aws-sdk-v1-to-v2
buildCommand: gradle build
additionalPlanContext: |
  Maintain our existing error handling patterns.
  Use our organization's standard credential provider chain.
  Update logging to use our internal logging framework.
```

常见使用案例

本节为使用 Transf AWS orm CLI 的常见转换场景提供分步指导。

Lambda 运行时升级

Lambda 会定期弃用旧语言运行时，要求团队将其的 Lambda 函数升级到支持的版本。 AWS Transform custom 可以使用 AWS托管语言版本升级转换自动进行这些升级。例如，要将用 Python 3.9 编写的 Lambda 函数升级到 Python 3.13，你可以使用转换。`AWS/python-version-upgrade`Java (`AWS/java-version-upgrade`) 和 Node.js (`AWS/nodejs-version-upgrade`) 也有类似的转换，涵盖了最常见的 Lambda 运行时语言。

要以交互方式升级单个 Lambda 函数，请导航到函数源存储库的根目录，然后使用启动 Transform AWS CLI。`atx`在交互式会话中，描述您需要的升级，例如，“将此 Python 3.9 Lambda 函数升级到 Python 3.13”。代理将选择适当的 AWS托管转换，分析您的代码，更新语言语法，调整依赖关系，并对已弃用的 API 调用进行现代化改造。您可以提供编译或验证命令，例如`pytest`代理可以验证转换后的代码是否已编译并通过测试。`python -m py_compile *.py`在整个互动会话中，在接受最终结果之前，您可以查看代理提出的变更、提供反馈和请求调整。

当您需要在多个存储库中升级 Lambda 运行时时，请使用非交互模式大规模运行转换。对于每个存储库，调用带有相应标志的 CLI，无需用户输入即可运行。例如，要将 Node.js 16 Lambda 函数升级到 22，请 Node.js 执行以下操作：

```
atx custom def exec \
  -n AWS/nodejs-version-upgrade \
  -p ./my-lambda-repo \
  -c "npm test" \
  -g "additionalPlanContext='Upgrade from Node.js 16 to Node.js 22'" \
  -x -t
```

该-x标志以非交互方式运行转换，并且-t信任所有工具的执行，因此不需要提示。您可以使用简单的 shell 循环在数十或数百个存储库中编写此命令的脚本。每次转换完成后，请查看 Git 差异以验证更改，然后运行测试套件以确认升级后的功能正常运行。您还可以将 Trans AWS form 自定义集成到您的 CI/CD 管道中，以持续识别已弃用的 Lambda 函数。这种方法不仅解决了运行时已过时的直接问题，而且还建立了一个持续的流程，以便在功能达到支持终止状态之前对其进行检测和升级。

中央平台团队可以通过 Trans AWS form Web 应用程序创建活动，以定义转换、指定目标 Lambda 存储库并跟踪整个组织的进度。有关使用 Batc AWS h 构建生产级扩展部署解决方案的详细演练，请参阅使用 Transform cust om 构建可扩展的 AWS 代码现代化解决方案。

AWS Transform 自定义端点和接口端点 (AWS PrivateLink)

您可以通过创建接口 VPC 终端节点在您的 VPC 和 AWS Transform 自定义 VPC 之间建立私有连接。接口端点由一项技术提供支持 AWS PrivateLink，该技术使您无需互联网网关、NAT 设备、VPN 连接或 Direct Connect 连接即可私密访问 AWS Transform 自定义服务。您的 VPC 和 AWS Transform 自定义 VPC 之间的流量不会离开 Amazon 网络。

每个接口端点均由子网中的一个或多个弹性网络接口表示。

有关更多信息，请参阅《Amazon VPC 用户指南》中的接口 VPC 端点 (AWS PrivateLink)。

> **Note**
>
> - 您必须为 Amazon S3 启用 AWS PrivateLink 集成，因为 AWS Transform 自定义会调用 S3 API。有关详细说明，请参阅AWS PrivateLink 适用于 Amazon S3 的文档。如果您在使用 AWS Transform 自定义时遇到 S3 访问问题，请参阅我们的故障排除指南。
> - 如果您没有使用 AWS PrivateLink 私有 DNS 功能（请参阅私有 DNS），则必须：
>   - 配置到 VPC 接口终端节点的路由（参见 VPC 接口终端节点的路由文档）
>   - 设置ATX_CUSTOM_ENDPOINT环境变量以指定您的自定义域，例如：

```
ATX_CUSTOM_ENDPOINT=https://transform-custom.<region>.api.aws atx
```

的注意事项 AWS Transform 自定义 VPC 终端节点

在为 AWS Transform 自定义设置接口 VPC 终端节点之前，请务必查看 Amazon VPC 用户指南中的接口终端节点属性和限制。

AWS Transform custom 支持通过接口端点调用其所有 API 操作。

先决条件

在您开始下面的任何流程之前，请确保您满足以下条件：

- 具有创建和配置资源的适当权限的 AWS 账户。
- 已在您的 AWS 账户中创建了 VPC。
- 熟悉 AWS 服务，尤其是 Amazon VPC 和 AWS Transform 自定义服务。

为创建接口 VPC 终端节点 AWS Transform 自定义

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为 AWS Transform 自定义服务创建 VPC 终端节点。有关更多信息，请参阅《Amazon VPC User Guide》中的 Creating an interface endpoint。

使用此服务名称创建以下 VPC 终端节点以供 AWS Transform 自定义：

- com.amazonaws。 *region*.transform-

替换*region*为你想要使用 AWS Transform 自定义 CLI 的 AWS 区域，例如 com.amazonaws. us-east-1.transform-custom。

有关更多信息，请参阅《Amazon VPC 用户指南》中的通过接口端点访问服务。

为创建 VPC 终端节点策略 AWS Transform 自定义

您可以将终端节点策略附加到控制 AWS Transform 自定义访问权限的 VPC 终端节点。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问。

示例：的 VPC 终端节点策略 AWS Transform 自定义操作

以下是 AWS Transform 自定义终端节点策略的示例。当连接到终端节点时，此策略授予所有委托人对所有资源上列出的 AWS Transform 自定义操作的访问权限。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "transform-custom:*"
         ],
         "Resource":"*"
      }
   ]
}
```

使用本地计算机连接到 AWS Transform 自定义端点

本节介绍使用本地计算机通过您的 AWS VPC 中的 AWS PrivateLink 终端节点连接到 AWS Transform 自定义的过程。

1. 在本地设备和 VPC 之间创建 VPN 连接。
2. 为 AWS Transform 自定义创建接口 VPC 终端节点。
3. 设置入站 Amazon Route 53 端点。这将使您能够在本地设备上使用 AWS Transform 自定义终端节点的 DNS 名称。

问题排查

本节提供有关如何解决 Trans AWS form 自定义常见问题的指导。

记录位置

AWS Transform CLI 在以下位置维护日志：

对话日志：

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/<timestamp>-conversation.log
```

Windows

```
%USERPROFILE%\.aws\atx\custom\<conversation_id>\logs\<timestamp>-conversation.log
```

这些日志包含用于调试特定转换执行的完整对话历史记录。

子代理日志：

Linux and macOS

```
~/.aws/atx/custom/<conversation_id>/logs/subagents/<name>.log
```

Windows

```
%USERPROFILE%\.aws\atx\custom\<conversation_id>\logs\subagents\<name>.log
```

这些日志包含主代理在变换期间生成的子代理的输出。您无需直接管理子代理。

开发者调试日志：

Linux and macOS

```
~/.aws/atx/logs/debug*.log
~/.aws/atx/logs/error.log
```

Windows

```
%USERPROFILE%\.aws\atx\logs\debug*.log
%USERPROFILE%\.aws\atx\logs\error.log
```

这些日志提供有关 CLI 操作和错误的详细信息。每个日志文件在滚动前都有 5MB 的限制。此目录中可能有多个调试日志，例如 debug1.log 和 debug2.log。

常见问题

安装问题：

如果安装失败，请确保安装了 Node.js 22 或更高版本：

```
node --version
```

https://nodejs.org/en/download如果需要，可以 Node.js 从中下载。

身份验证问题：

验证您的 AWS 凭证配置是否正确：

```
aws sts get-caller-identity
```

确保您的 IAM 用户或角色具有所需的`transform-custom:*`权限。

网络连接问题：

如果遇到连接错误，请验证对所需端点的网络访问权限：

- `transform-cli.awsstatic.com`
- `transform-custom.<region>.api.aws`
- `*.s3.amazonaws.com`

如果在受互联网限制的环境中工作，请更新防火墙规则以将这些 URL 列入许可名单。

区域配置问题：

如果您遇到与区域相关的错误：

- 确认您的地区是否受支持
- 检查是否存在可能覆盖您的配置的环境变量：`echo $AWS_REGION $AWS_DEFAULT_REGION`
- 检查您的地区配置：`aws configure get region`

- 如果需要，请更新您所在的地区：`aws configure set region <your-region>`
- 查看调试日志以了解区域解析的详细信息

Git 问题：

确保已安装 Git 并且您的存储库受 git 源代码控制：

```
git --version
git status
```

AWS 自定义转换要求存储库受到 git 源代码控制。

转换执行问题：

如果转换失败：

1. 查看对话日志，网址为 `~/.aws/atx/custom/<conversation_id>/logs/`
2. 检查转换输出中的构建或测试失败
3. 验证您的项目的构建命令是否正确
4. 尝试在交互模式下运行转换以提供反馈

对话恢复问题：

如果您无法恢复对话：

- 确认对话的时间少于 30 天
- 检查对话ID是否正确
- 确保您有网络连接

获取支持

如需其他帮助，请通过AWS 控制台访问 Su AWS pport。

打开支持请求时，请包括：

- 对话日志来自 `~/.aws/atx/custom/<conversation_id>/logs/`
- 子代理日志来自 `~/.aws/atx/custom/<conversation_id>/logs/subagents/`

- 调试日志来自 ~/.aws/atx/logs/
- 重现问题的步骤
- AWS 转换 CLI 版本 (atx --version)

S3 访问问题

Trans AWS form 自定义服务提供 S3 预签名 URL，以便于上传和下载 to/from 客户端计算机上可能很大的转换文件。这意味着 CLI 不仅与 Trans AWS form 服务端点交互，而且还与 S3 服务端点交互。这些交互使用预签名 URL，因此您的客户的 IAM 凭证不需要任何 S3 权限，但有时您本地计算机的代理服务器配置和网络的 S3 VPC 终端节点策略可能会限制此流量。

请查看以the section called “记录位置”获取更详细的错误消息，以帮助从根本上解决与下载和上传转换文件相关的任何工具故障或 S3 访问被拒绝。

如果您使用的 VPN/Proxy 服务器利用https_proxy和no_proxy环境变量，请考虑将以下值添加到您的no_proxy环境变量值中，以绕过 S3 和 Trans AWS form 自定义服务端点的代理，例如：

Linux and macOS

```
export no_proxy=.s3.amazonaws.com,transform-custom.<region>.api.aws
```

Windows (PowerShell)

```
$env:no_proxy=".s3.amazonaws.com,transform-custom.<region>.api.aws"
```

如果您在 VPC 中使用AWS PrivateLink 适用于 Amazon S3 的，则该策略可能已定义为限制 S3 流量。请确保您的 S3 VPC 终端节点策略允许GetObject对 AWS 转换自定义服务拥有的存储桶进行PutObject操作。这可以通过在您的 VPC 终端节点策略中添加以下语句来实现：

```
{
    "Effect": "Allow",
    "Principal": "*",
    "Action": ["s3:PutObject","s3:GetObject"],
    "Resource": "arn:aws:s3:::aws-transform-custom-*/*"
}
```

策略中的明确Deny声明优先于Allow声明。查看 S3 VPC 端点策略，了解可能限制访问的Deny声明。

AWS 转换 CLI 版本历史记录

有关当前和过去版本的 Trans AWS form CLI 的详细信息，请查看下表。该表包括每个版本的版本、发布日期和发行说明。

版本	发行日期	发行说明
3.6.0（最新）	2026年7月17日	• 添加了`atx custom def learnings` 子命令，该命令可打开交互式 TUI 会话，以查看和管理根据先前运行为转换定义自动生成的学习内容。 • 添加了转换执行期间的使用情况遥测收集。要禁用遥测，请设置`ATX_DISABLE_TELEMETRY=true` 环境变量。有关更多信息，请参阅 用法遥测。 • 修复了 Windows 上使用~（主目录）路径的文件操作解析到意外目录的问题。这会导致会话期间 read/write 出现文件故障。 • 修复了包含特殊字符的 MCP 服务器和工具名称可能导致连接失败的问题。现在，CLI 会自动对名称进行清理，使其仅使用有效字符。
3.5.0	2026 年 7 月 8 日	• 添加了原生 Windows 支持。现在，你可以直接在 Windows 上运行 “ AWS 转换自定义” 命令。（Windows 尚不支持这些`atx ct`命令） • 添加了指导输入，`atx ct analysis run`因此代理就绪情况和现代化就绪性分析可以反映您的偏好。`--context` 用于战略框架，设置代理访问权限`--agent-scope` 以备代理就绪，`--prefer`/`--avoid`用于引导现代化建议转向或远离特定技术。 • 技能格式的转换定义现在可以包含一个`scripts/`文件夹，允许您将辅助脚本与`SKILL.md`和引用捆绑在一起。 • 已添加`--wait`到`atx ct remediation create` ，等待修复完成。 • 添加了用于单枪执行的无头模式。运行`atx -x "prompt" -t`以传递提示，获得响应，然后在没有交互式提示的情况下退出。无头模式需要信任所有工具。

版本	发行日期	发行说明
3.4.1	2026 年 7 月 2 日	• 修复了 3.4.0 版本引入的交互式会话问题。代理完成响应后，CLI 可能会停留在 “Thinking” 提示符上（在用户界面中用省略号显示），而不是返回输入提示。现在，每次响应后，CLI 都会返回到输入提示符。
3.4.0（不推荐使用）	2026 年 6 月 29 日	⚠ 已知问题 在交互式会话中，代理完成响应后，CLI 可能会停留在 “Thinking” 提示符（界面中用省略号显示）。这可以防止您输入下一条消息。要解决此问题，请运行`atx update`升级到 3.4.1 或更高版本。 • 添加了`atx ct schema`机器可读的完整`atx ct`命令界面清单，用于脚本编写和自动化。 • 添加或更新源时添加了令牌范围验证，可以立即显示凭证或权限问题，而不是稍后在分析过程中失败。 • 改进了自动修复拉取请求，包括查找上下文，并支持草稿模式，以获得更多可审查的 PR。 • 改进了 CLI 进度反馈，包括有关当前活动、预计代理分钟数和子代理活动的实时背景信息。 • 通过`ATX_GIT_COMMITTER_NAME` 和`ATX_GIT_COMMITTER_EMAIL` 环境变量添加了可配置的检查点提交作者身份。 • 各种小错误修复和改进。
3.3.0	2026 年 6 月 18 日	• 增加了跨`atx ct`命令的一致`--json`性和`--help`支持。 • 修复了安全代理设置，因此代理空间是在安装期间创建的，并在拆卸时删除。 • 各种小错误修复和改进。

版本	发行日期	发行说明
3.2.0	2026 年 6 月 15 日	• 在标准 CLI 发行版中为所有用户添加了持续现代化命令 (`atx ct`)。 • 改进了子代理执行力，在等待服务器响应时显示 “Thinking...” 微调器，从而提供工作正在进行中的清晰视觉反馈。 • 改进了微调器，可在代理输出后静音 3 秒钟后自动以 “正在工作...” 重新启动，因此终端在处理步骤之间永远不会出现冻结状态。 • 改进了思维旋转器，带有微妙的微光动画，使视觉外观更加精致。
3.1.0	2026 年 6 月 3 日	• 添加了`ATX_MAX_VALIDATION_LOOPS` 环境变量以配置最大验证循环。 • 当已安装的版本已经比注册表版本更新时，修复更新检查不再显示错误的 “可用更新” 警告。 • Fixed `delete --transformation-name ""` 不再显示荒谬的确认提示；空值现在会被拒绝，并显示明显的验证错误。 • 修复了无法识别的子命令现在显示 “未知命令”，而不是令人困惑的内部错误消息。 • 修复了版本比较，使用数字比较而不是字符串不等式进行更新检查。
3.0.0	2026年5月21日	• 添加了飞行前转换名称验证，当找不到名称时，可以从注册表中建议相似的名称，无需单独的列表命令即可帮助捕捉错别字。 • 添加了对 shell 命令的可选解释，显示了它们的作用和原因。 • 改进了信任设置横幅，以包含有关工具权限的更多信息。 • 在使用 do-not-learn 标志时添加了禁用学习的横幅，让人们可以看到学习功能以及如何启用该功能。 • 重大更改：现在需要 Node.js 22 或更高版本。https://nodejs.org/如果您使用的是旧版本，请从中升级。

版本	发行日期	发行说明
2.0.0	2026 年 5 月 14 日	• 增加了远程 MCP 服务器支持 — 通过自动 SSE 回退功能连接到 HTTP 和 HTTPS MCP 服务器，使用标头中的环境变量扩展进行持有者令牌身份验证，以及代理支持 ()。HTTP_PROXY/HTTPS_PROXY • 添加了`atx resume`子命令作为别名。`atx --resume` • 添加了具有输出控制功能的多文件文本搜索`grep`工具 — 支持正则表达式模式、文件全局过滤、不区分大小写的搜索、可配置 depth/result 的限制和输出截断。 • 改进了 MCP 实现，使用标准 MCP SDK 实现更一致的行为，更轻松地支持 future MCP 功能。 • 改进了 shell 输出处理——现在，输出被优雅地截断为每个流 30K 个字符，而不是导致严重错误，保留了输出的开头和结尾以供上下文参考。 • 修复了交互式会话期间的 Ctrl+C 可能会过早退出 CLI Linux/macOS ，而不是中止当前操作并返回提示符的问题。 • 修复了信任拒绝消息，以显示信任不可用的具体原因，与命令需要授权的原因分开。 • 修复了命令进入时不再提及信任的危险命令警告。`alwaysPromptCommands`
1.10.0	2026 年 4 月 29 日	• 通过跨工具指导改进了工具描述，可帮助代理为每项任务选择最佳工具，并减少不必要的外壳使用。 • 已添加 `alwaysPromptCommands` `trust-settings.yaml` — 配置无论信任设置如何，始终需要明确权限的 shell 命令模式。支持 glob 通配符并与复合表达式中的每个子命令进行匹配。 `trustedShellCommands` 可以覆盖这些模式。为了避免破坏自动管道，在非交互模式下不强制执行。 • 修复了相对路径无法解析为绝对路径的问题。
1.9.0	2026 年 4 月 23 日	• 改进了工具批准提示 — 每个选项现在都显示其内联作用，“为什么” 消息解释了为什么需要批准，信任确认中包含`trust-settings.yaml` 有关永久信任的提示。

版本	发行日期	发行说明
1.8.0	2026 年 4 月 16 日	• 将代理输出前缀从更改为> ，ATX： 以便更清楚地区分用户输入和代理输出。 • 修复了 CLI 重试用尽时显示恢复命令的问题。 • 修复了来自不同工作目录的简历。在交互模式下，提示输入更正的路径；在非交互模式下，由于描述性错误而快速失败。
1.7.1	2026 年 4 月 9 日	• 修复了凭证提供者区域与配置文件不同时 SSO 登录失败（“未找到会话令牌或会话令牌无效”）。sso_region • 修复了凭据缓存问题，因此在磁盘上轮换凭据时，长时间运行的会话不会再失败。
1.7.0	2026 年 4 月 2 日	• 修复了在输入验证错误时使用代码 1 退出的exec命令，从而使 CLI 在脚本和 CI/CD 管道中非常可靠。 • 添加了显示来自该服务的警告消息。 • 为 AWS 凭证配置文件添加了 MFA 提示支持。 • 修复了 STS 凭据调用以遵守 HTTP (S) 代理设置的问题。
1.6.0	2026 年 3 月 18 日	• 添加了为exec和interactive 命令设置代理分钟数预算的--limit <minutes> 选项。达到限制后，CLI 会显示使用情况并退出并显示恢复指令。 • 修复了对话日志中初始用户消息的日志记录。
1.5.0	2026年3月11日	• 增加了对并发任务执行的支持，从而实现了更快的转换。 • 添加了在每次对话结束时显示代理分钟使用情况，以及在交互模式下随时查看使用情况的/usage命令。
1.4.0	2026 年 3 月 2 日	• 改进了使用不支持的文件保存转换定义时的错误消息。 • 为服务调用添加了超时，以防止 CLI 在连接中断时挂起。 • 修复了成功完成后CLI进程挂起的问题。 • 修复了恢复对话时的区域验证问题。

版本	发行日期	发行说明
1.3.0	2026 年 2 月 19 日	• 移除了 MCP 服务器路径的限制 — 用户现在可以在 MCP 配置中为该command属性指定任何路径。 • 提高了 MCP 服务器连接的稳定性。
1.2.0	2026年2月9日	• 增加了对通过环境变量（https_proxy no_proxy、等）进行代理配置的支持。 • 常规稳定性改进和错误修复。
1.1.1	2026 年 1 月 16 日	错误修复和稳定性改进。
1.1.0	2026 年 1 月 13 日	添加了 AWS CLI 区域配置支持、早期凭证验证检查和修复了活动恢复功能。
1.0.1	2025 年 12 月 18 日	优雅的关机、更清晰的错误日志和一般改进。
1.0.0	2025 年 12 月 1 日	AWS 转换 CLI 的初始版本。

AWS 转变持续现代化

什么是 AWS 实现持续现代化转型？

AWS Transform 持续现代化为您的源代码存储库提供分析和补救。您可以连接 GitHub 组织、 GitLab 群组、Bitbucket 工作空间和本地存储库，然后运行自动分析以识别整个代码库中的技术债务、安全漏洞、现代化机会和代理准备情况。

所有分析和补救都 AWS 账户 使用您的证书在您中运行。您的源代码由您控制。

> **Note**
>
> 我们建议从 Kiro Power 或代理插件开始。代理技能可以协调持续现代化的设置、入职和持续使用，包括基础设施配置、源配置、分析执行、调查结果分类和补救。有关安装说明，请参阅开发人员工具。

关键功能

AWS Transform 持续现代化提供以下功能：

- 技术债务分析 — 扫描存储库中是否存在过时的依赖关系、安全漏洞、代码质量问题和现代化机会。对软件包清单进行快速元数据扫描或全面的代码级分析。使用针对您的环境量身定制的转换定义来定义自定义分析标准。
- 自主修复-大规模生成经过验证的拉取请求。每个发现都可以使用其关联的转换定义进行自动修正。修复会创建分支并在 GitHub GitLab、和 Bitbucket 上 PRs/MRs 自动打开。
- 报告-生成 HTML 报告，按严重性、存储库和分析类型显示调查结果。随着时间的推移，跟踪修复进度并找到解决方案。
- 持续监控 — 使用 Amazon EventBridge 计划程序安排定期分析。配置每日、每周或自定义 cron 时间表，持续监控您的投资组合中是否有新发行。

分析类型

AWS Transform 持续现代化支持以下分析类型，以满足您的现代化需求。

Type	说明
rapid-techdebt-analysis	对软件包清单（pom.xml、、requirements.txt ）进行仅限元数据的快速扫描package.json ，以识别过时的版本和过时的依赖关系。不分析源代码。
tech-debt-comprehensive	使用 AWS 转换代理进行深入的代码级技术债务分析。检查源代码以确定债务模式、代码质量问题、架构问题和改进机会。
security	使用安全代理进行安全漏洞和 CVE 检测。 AWS 扫描源代码和依赖关系，以查找已知漏洞、不安全的编码模式和可利用的漏洞。需要一次性基础架构设置。
agentic-readiness	AI 和代理集成准备情况评估。在五个类别中评分 56 个标准：基础设施和平台、应用程序架构、数据基础以及运营与可观测性。 Identity/Security/Governance
modernization-readiness	云现代化机会评估。评估基础架构、应用程序、数据、安全和运营方面的准备情况。确定容器化、无服务器迁移和平台升级的候选对象。
custom	将任何变换定义 (TD) 作为分析运行。使用此类型来定义自己的分析标准或运行内置类型未涵盖的 AWS 托管变换。

了解关键概念

来源

消息来源告诉持续现代化您的存储库在哪里。支持的源类型：

- GitHub— 拥有个人访问令牌的 Organizations（经典）
- GitLab— 群组或用户，包括自托管实例

- Bitbucket — 工作空间（云端）或项目（数据中心）
- 本地-包含 git 存储库的父目录

Repositories

存储库是通过扫描源发现的。发现后，您可以按来源、标签或其他标准进行筛选；为组织应用标签（团队、优先级、迁移浪潮）；并针对特定的存储库进行分析或修复。

分析

分析是使用特定分析类型对一个或多个存储库进行扫描。每次分析都会生成发现结果，以识别代码中的问题。您可以按需运行分析，也可以安排分析自动运行。分析类型包括快速技术债务分析、技术债务综合分析、安全性、代理就绪性、现代化准备情况和自定义。每项分析都会跟踪其状态（待处理、正在运行、已完成、已取消或失败）及其扫描的存储库。

结果

结果是分析的结果。每项发现都包括严重性（高、中或低）、状态（打开、已解除或已过时）以及可以对其进行补救的修复转换（如果可自动修复）。新的发现一开始是开放的。用户可以驳回调查结果并说明理由。 Re-analysis 自动将已解决的结果标记为已过时。

补救措施

修正应用转换定义来修复发现。三种模式：基于结果（每个查找结果都使用自己的修复变换）、TD 覆盖（覆盖指定查找结果的转换定义）和直接 TD（对没有发现结果的存储库运行转换）。输出取决于源提供商（GitHub PR、 GitLab MR、Bitbucket PR 或本地分支机构）。

转换定义

转换定义包含执行特定代码转换所需的指令和知识。持续现代化使用转换定义进行自定义分析 (`--type custom --transformation-name` *`name`*) 和修复 (`--transformation-name` *`name`*)。使用列出可用的转换定义`atx custom def list`。

操作方法 AWS 转变持续的现代化工作

AWS Transform 持续现代化通常用于需要持续分析和修复多个代码库的大型项目。团队通常遵循以下工作流程：

1. Connect Sources — 添加 GitHub 组织、 GitLab群组、Bitbucket 工作空间或本地目录作为源。提供具有适当范围的身份验证令牌。
2. 发现存储库-运行发现扫描以枚举源中的所有存储库。使用标签按团队、优先级或迁移浪潮来组织仓库。
3. 运行分析-对您的投资组合执行分析。选择快速扫描以获得快速结果，或选择全面分析以获得详细结果。安全分析需要一次性基础架构设置。
4. 分类结果-按严重性、存储库或分析类型查看结果。驳回带有记录原因的误报。 Re-run分析以将已解决的问题标记为已过时。
5. 修复-创建修正以修复发现的问题。持续现代化会自动创建分支并打开包含修复的 pull/merge 请求。跟踪补救状态和重试失败。
6. 设置持续分析-使用 Amazon EventBridge 计划程序安排重复分析。配置分析节奏（每日、每周或自定义 cron），持续监控您的投资组合中是否有新问题。与自动修复相结合，随着时间的推移保持代码的运行状况。

计算选项

持续现代化支持三种计算选项，用于运行分析和修复。Kiro Power 和代理插件中的代理技能可帮助您为每个选项设置基础架构。

> **Note**
>
> 无论使用哪种计算选项，所有分析和补救都是在您 AWS 账户 使用凭据时进行的。您的源代码仍处于您的控制之下。

本地（默认）

默认情况下，分析在您的本地计算机上运行。此选项不需要额外的基础架构。服务器在本地运行，并使用本地计算资源执行分析。适合试用该工具、小型存储库或个人使用。

Amazon EC2

在您的永久性 Amazon EC2 实例上运行分析 AWS 账户。此选项可将计算从本地计算机上卸载，支持更大规模的分析，并允许定期进行分析。实例在两次提交之间保持运行。

代理技能提供的堆 AWS CloudFormation 栈包括：

- 带有 Docker 和持续现代化容器的亚马逊 EC2 实例（亚马逊 Linux 2023）
- 一个具有 Trans AWS form、Amazon S3、 AWS KMS、Secrets Manager 和安全代理权限的 IAM 角色
- `AmazonSSMManagedInstanceCore`用于通过 SSM 进行外壳访问（不需要 SSH 密钥对或入站端口）
- 没有入站规则的安全组

您的 IAM 用户或角色需要获得 Amazon EC2 生命周期管理、 AWS CloudFormation 堆栈操作、IAM 角色创建、Amazon S3 存储桶操作、Secrets Manager 机密管理和 SSM 命令的权限。

要设置 EC2 执行，请安装 Kiro Power 或代理插件（参见开发人员工具），然后询问代理："设置 EC2 实例以进行持续的现代化分析"。代理配置基础架构，验证容器是否运行正常，并通过 SSM 提交您的分析，无需使用 SSH。

AWS Batch (Fargate)

使用 Fargate 在 Bat AWS ch 上以孤立作业的形式运行分析，实现无服务器计算。每项分析都在自己的容器中运行，无需管理永久基础架构。适用于对多个来源或分析类型进行并行分析。

此选项重复使用 AWS 转换 CDK 基础架构堆栈。代理技能部署所需的基础架构，包括：

- AWS Batch 作业队列和计算环境
- 使用持续现代化容器镜像定义 Job
- 用于执行批处理作业的 IAM 角色
- 用于提交任务的 Lambda 函数

要设置批量执行，请安装 Kiro Power 或代理插件（参见开发人员工具），然后询问代理："在 Fargate 上运行我的分析" 或 "设置批处理执行以实现持续现代化"。代理部署 CDK 堆栈，将您的源凭据存储在 Secrets Manager 中，并将分析作业提交到 Batch AWS 。

安全代理设置

`security`分析类型使用 AWS 安全代理服务进行漏洞和 CVE 检测。与其他分析类型不同，它需要在您的中进行一次性基础架构设置 AWS 账户。

setup 命令提供的 AWS CloudFormation 堆栈包括：

- 用于上传源代码的 Amazon S3 存储桶
- 由担任的 IAM 角色 `securityagent.amazonaws.com`
- 安全代理角色的托管策略

您的 IAM 用户或角色必须具有以下额外权限才能运行安装程序：

- `cloudformation:CreateStack`, `cloudformation:UpdateStack`, `cloudformation:DescribeStacks`
- `iam:CreateRole`, `iam:PutRolePolicy`, `iam:AttachRolePolicy`, `iam:CreatePolicy`
- `s3:CreateBucket`, `s3:PutBucketEncryption`, `s3:PutBucketPublicAccessBlock`

使用以下命令管理安全代理基础架构：

```
# Provision the security agent infrastructure
atx ct setup security-agent

# Check the status
atx ct setup security-agent --status

# Delete the infrastructure
atx ct setup security-agent --delete
```

设置完成后，您可以像其他分析类型一样运行安全分析。

开始使用

先决条件

要有效地使用持续现代化，您应该对 Git 版本控制有基本的了解，熟悉您的源代码平台（GitHub、GitLab或 Bitbucket）、 AWS IAM 权限的工作知识以及使用命令行工具的经验。

在使用持续现代化之前，请确认您具备以下条件：

- AWS 已安装转换 CLI：

```
curl -fsSL https://transform-cli.awsstatic.com/install.sh | bash
```

- Node.js 22 或更高版本
- 有效 AWS 凭证（`AWS_PROFILE`或环境变量）
- `AWSTransformCustomFullAccess`附加到您的 IAM 用户或角色的 AWS 托管策略

快速入门

1. 启动持续现代化服务器：

   ```
   atx ct server &
   ```

2. 添加来源：

   ```
   atx ct source add --name name --provider provider --org org-or-group --token token
   ```

   其中*name*是来源的描述性标识符，*provider*是平台（`github`、`gitlab`或`bitbucket`、`local`），*org-or-group*是您的组织或群组名称，*token*是您的身份验证令牌。

3. 发现存储库：

   ```
   atx ct discovery scan --source name
   ```

4. 运行分析：

   ```
   atx ct analysis run --type type --source name --wait
   ```

5. 探索发现：

   ```
   atx ct findings list --json
   ```

6. 修复调查结果：

   ```
   atx ct remediation create --ids id1,id2 --name "remediation-name"
   ```

进行持续的现代化改造

来源管理

使用`atx ct source`命令连接存储库。支持的提供商： GitHub、 GitLab、Bitbucket、本地。

GitHub 组织

令牌：带repo范围的个人访问令牌（经典）。 Read-only 为了进行分析，请使用完整存储库进行修复。

```
atx ct source add --name name --provider github --org org --token pat
```

GitLab 群组和用户

令牌：带api范围的个人访问令牌。

```
atx ct source add --name name --provider gitlab --org group-or-user --token pat
# Self-hosted:
atx ct source add --name name --provider gitlab --org group-or-user --token pat --url
 https://gitlab.example.com
```

Bitbucket 工作空间和项目

Bitbucket Cloud — 范围：read:repository:bitbucket、write:repository:bitbucket、read:pullrequest:bitbu
还需要--email和--username。

```
atx ct source add --name name --provider bitbucket --org workspace --token api-token --
email email --username username
```

Bitbucket 数据中心：

```
atx ct source add --name name --provider bitbucket --org project-key --token http-
access-token --url https://bitbucket.example.com
```

本地存储库

```
atx ct source add --name name --provider local --path parent-directory
```

> **Important**
>
> --path必须指向包含 git 存储库作为子目录的父目录，而不是指向单个存储库。

管理来源

```
atx ct source list
atx ct source remove --name name
```

存储库发现和管理

```
atx ct discovery scan --source name
atx ct discovery status --source name
atx ct discovery scan --source name --path new-directory
```

发现后：

```
atx ct repository list
atx ct repository list --source name
atx ct repository list --labels "team:frontend,priority:high"
atx ct repository update --source name --repo "source::slug" --labels
 "team:frontend,priority:high"
atx ct repository update --source name --labels "migration:wave-1"
```

跑步分析

该`--type`标志指定要运行的分析类型：

- `rapid-techdebt-analysis`— 过时的依赖关系和轻松的胜利。
- `tech-debt-comprehensive`— 更深入的 AI-powered 分析，涵盖依赖关系、安全性、模式、性能、可维护性、架构、代码质量和基础架构发现。
- `security`— 安全漏洞和风险敞口。
- `agentic-readiness`— 您的存储库已准备就绪，可供人工智能代理（框架、API、文档）使用。
- `modernization-readiness`— 基础架构、应用程序、数据、安全和运营方面的现代化机会。

```
atx ct analysis run --type type --source name [--repo source::slug] [--wait]
atx ct analysis get --id id --json
atx ct analysis list --json
atx ct analysis list --status pending|running|complete|cancelled|failed --json
atx ct analysis list --type type --json
atx ct analysis cancel --id id
atx ct analysis delete --id id [--cascade-findings]
```

自定义分析

```
atx ct analysis run --type custom --transformation-name name --source source --
repo source::slug --wait
```

带-g标志的配置：键值、JSON 或文件路径。

列出 TD：`atx custom def list`

管理调查发现

```
atx ct findings list --json
atx ct findings list --repo source::slug --source name --severity high|medium|low
 --type analysis-type --status open|dismissed|obsolete --analysis-id id --fix-
transform transform-name --json
```

查找状态

- `open`— 活跃
- `dismissed`— 手动解雇（需要原因）
- `obsolete`— System-set 当重新分析不再得出发现结果时

```
atx ct findings update --id id --status dismissed --reason "reason"
atx ct findings update --id id --status open
atx ct findings batch-update --ids id1,id2 --status dismissed --reason "reason"
atx ct findings get --id id
atx ct findings delete --id id
```

寻找过时产品

Re-analysis 将已解决的发现标记为已过时。无法重新打开。保留以供审计。

创建补救措施

三种模式：基于发现、TD 覆盖、直接 TD。

```
atx ct remediation create --ids id1,id2 --name "name"
atx ct remediation create --ids id1,id2 --transformation-name TD
atx ct remediation create --transformation-name TD --repo source::slug
```

按提供商划分的输出： GitHub PR、 GitLab MR、Bitbucket PR、Local 分支

> **Note**
>
> 令牌必须具有写入权限才能 PR/MR 创建。

带`--local`标志的本地执行。

```
atx ct remediation create --transformation-name TD --repo source::slug -g
 "additionalPlanContext=Upgrade to Node.js 22"
atx ct remediation list
atx ct remediation status --id id
atx ct remediation retry --id id
atx ct remediation delete --id id
```

AWS 转换 Web 应用程序（可选）

Trans AWS form Web 应用程序是一个可选界面，用于监控整个代码源组合中的持续现代化分析、发现和修复。

在使用 Tr AWS ansform Web 应用程序之前，您需要启用用户身份才能在组织中访问 T AWS ransform。有关启用 AWS 转换的信息，请参阅设置 AWS 转换。

要使用 AWS 转换 Web 应用程序，请执行以下操作：

1. 使用 AWS IAM 身份中心证书访问`https://aws.amazon.com/transform/`并登录。
2. 如果登录后未出现持续现代化，请改用 IAM 凭证登录。要启用 IAM 证书登录，请执行以下操作：
   a. 在 AWS 管理控制台中，打开 “ AWS 转换”，然后选择 “设置”。
   b. 在 “使用 IAM 凭证进行访问 AWS 转换” 部分中，启用 IAM 凭证访问权限。
   c. 在同一设置页面上，复制 Web 应用程序 URL（使用 IAM）下方显示的登录链接。
   d. 将登录 URL 粘贴到打开 AWS 管理控制台的同一浏览器窗口中。这样可以确保 Web 应用程序使用该账户的 AWS 凭证。
3. 打开左侧导航菜单并选择持续现代化。控制面板显示摘要统计信息，包括来源、存储库、按严重性划分的发现总数以及分析类型。
4. 使用 “分析”、“发现结果” 和 “修复” 选项卡查看详细结果。
5. 直接通过 Web 应用程序与 T AWS ransform 聊天，询问有关您的分析、发现或补救措施的问题。

Web 应用程序专为企业级运营而设计，在这些运营中，您需要集中查看跨多个代码库的持续现代化分析和修复。

开发人员工具

你可以使用 Tr AWS ansform Power 和代理插件从代理 IDE 访问持续的现代化。该代理通过对话互动协调设置、入职和持续使用持续现代化。

- Kiro IDE — 安装 Trans AWS form Kiro Power。打开 Kiro Chat，让代理帮助他们完成持续的现代化工作流程。
- Claude Code、Codex、Cursor — 安装awslabs/agent插件（目录）`plugins/aws-transform`。代理插件提供的功能与 Kiro Power 相同。

代理技能

Kiro Power 和代理插件包括通过对话互动协调持续现代化工作流程的技能：

技能	说明
Guide	交互式入门指导，逐步引导您完成完整的工作流程
来源	添加、列出和移除源连接
Discovery	扫描来源以发现存储库
分析	运行和管理所有类型的分析
结果	查询、筛选和管理分析结果
修复	创建和管理补救措施以修复发现的问题
EC2 执行	预置和管理 Amazon EC2 实例以进行远程分析
批量执行	使用 Fargate 将分析作业提交 AWS 给 Batch
Schedule	使用 Amazon EventBridge Scheduler 按照 cron 计划设置定期分析

技能	说明
报告	生成自包含的 HTML 报告，其中包含显示调查结果、严重性分布和修复进度的图表

CLI 引用：

下表汇总了所有`atx ct`子命令。

子命令	说明
`atx ct server`	启动持续现代化服务器
`atx ct status`	查看系统状态，包括来源、存储库、分析、发现和补救措施
`atx ct source add`	添加来源（GitHub、 GitLab、Bitbucket 或本地）
`atx ct source list`	列出已配置的来源
`atx ct source remove`	移除来源
`atx ct discovery scan`	从来源发现存储库
`atx ct discovery status`	检查发现扫描状态
`atx ct repository list`	列出带有可选筛选器的仓库
`atx ct repository get`	获取单个存储库
`atx ct repository update`	更新仓库标签
`atx ct repository delete`	删除存储库
`atx ct analysis run`	对存储库进行分析
`atx ct analysis get`	获取分析详情
`atx ct analysis list`	列出带有可选状态和类型筛选器的分析

子命令	说明
`atx ct analysis cancel`	取消正在运行的分析
`atx ct analysis delete`	删除分析
`atx ct findings list`	列出调查结果，并筛选存储库、来源、严重性、类型、状态和分析
`atx ct findings get`	获取单一发现
`atx ct findings update`	更新查找状态（打开或已关闭）
`atx ct findings batch-update`	批量更新多个发现结果
`atx ct findings delete`	删除已被驳回或过时的调查结果
`atx ct remediation create`	根据调查结果或转换定义创建补救措施
`atx ct remediation list`	列出所有补救措施
`atx ct remediation status`	检查修复状态并查看 PR/MR 链接
`atx ct remediation retry`	重试失败的修复
`atx ct remediation delete`	删除补救措施
`atx ct setup security-agent`	配置或管理安全代理基础架构
`atx ct schema`	打印完整的`atx ct`命令界面（每个命令、选项和参数）的机器可读的 JSON 清单，这样代理和自动化人员就可以在不解析帮助文本的情况下发现 CLI

问题排查

连接被拒绝或服务器未运行

持续现代化 CLI 需要一台正在运行的服务器。从开始`atx ct server &`并使用进行验证`atx ct status --health`。

发现扫描返回的存储库为零

对于本地源，请验证它`--path`指向包含存储库作为子目录的父目录（例如，`/home/user/repos`），而不是直接指向存储库（例如`/home/user/repos/my-app`）。扫描器会查找包含`.git`文件夹的子目录。

SETUP_必填错误

来源存在于您的账户中，但未在此计算机上配置凭据。运行`atx ct source add --name name`以在本地配置凭据。

需要进行身份验证错误

未找到该来源的有效令牌。验证您的令牌是否正确且具有所需的范围。对于 GitHub，请确保令牌具有`repo`作用域。对于 GitLab，请确保`api`范围。

INVALID_INPUT 错误

验证您使用的分析类型名称是否正确。有效值为: `rapid-techdebt-analysis`, `tech-debt-comprehensive`, `security`, `agentic-readiness`, `modernization-readiness`, `custom`。

修复期间出现权限错误

修复会创建分支和 pull/merge 请求，这需要对存储库的写入权限。使用写入权限更新您的令牌。对于 GitHub，请确保全`repo`范围。对于 GitLab，请确保`api`范围。对于 Bitbucket，请确保`write:repository:bitbucket`和`write:pullrequest:bitbucket`作用域。

安全代理安装失败

验证您的 IAM 用户或角色是否具有安全代理设置部分中列出的必需 AWS CloudFormation IAM 和 Amazon S3 权限操作方法 AWS 转变持续的现代化工作。使用检查状态`atx ct setup security-agent --status`。

在 Web 应用程序中看不到持续的现代化

如果在登录 Trans AWS form Web 应用程序后未出现持续现代化，请使用启用转换的 AWS 账户 位置 AWS 的 IAM 凭证登录，而不是 AWS IAM 身份中心。要查看步骤，请参阅AWS 转换 Web 应用程序（可选）。

发现工具

该 AWS Transform 发现工具可帮助您自动发现组织中的服务器清单，为迁移做好准备。该工具支持 VMware vCenter Hyper-V、微软和导入的服务器。要使用发现工具，您需要配置一个或多个发现源，让该工具运行，然后在 “已发现清单” 窗格中查看结果。

配置发现源后，发现工具开始收集信息。发现工具全面分析您的网络所需的时间取决于您的环境规模。对于定向迁移业务案例，您可以使用该工具在服务器收集完成后生成的迁移组合评估 (MPA) 文件。

发现工具工作流程

发现工具工作流程由两种类型的活动组成：

- 配置活动
- 数据审查和使用

以下步骤描述了如何安装和使用发现工具以及如何使用收集的数据：

1. 安装发现工具。
2. 配置发现源。您可以通过导入 CSV 文件配置以下一项或多项：VMware vCenter、Microsoft Hyper-V 主机或服务器。配置任何数据源后，数据发现就开始了。
3. 设置操作系统访问权限，然后查看服务器、数据库和网络连接的收集状态。
    - 根据需要调整操作系统凭据。
4. （可选）配置 Oracle 凭据以启用直接 SQL 收集，或者通过 SSH 或 WinRM 使用 OS-level 回退检测。
5. 要生成迁移业务案例，请将.zip 文件上传到迁移评估，或者将其解压并从 mpa_exports 目录中上传 M PA 文件。导出内容包括来自所有已配置来源的数据，并包含 VMware 的 MPA 文件和导入的服务器。 Hyper-V

该发现工具支持以下发现路径：

- VMware vCenter 自动发现 — 自动发现由 VMware vCenter 管理的服务器。
- Hyper-V 自动发现-自动发现由 Microsoft Hyper-V 主机管理的服务器。
- 服务器导入-通过 CSV 文件手动导入服务器清单。

设置发现工具

先决条件

以下是使用 AWS Transform 发现工具的先决条件：

一般先决条件

- 该工具需要 4 个 vCPU、16 GB 内存和一个 35 GB 的硬盘。
- 发现工具 VM 的网络中必须有 DHCP 可用。
- 该工具使用集中式方法收集数据。范围内的服务器必须允许来自发现工具 VM 的入站连接（支持默认端口，支持自定义端口配置）：
  - Linux — SSH TCP/22
  - Windows — TCP/5985 适用于 HTTP， TCP/5986 适用于 HTTPS
  - SNMP — UDP/161 （仅用于网络收集，不用于操作系统指标）
- 对于 Linux，可以使用 SSH 连接到服务器的用户帐户。该发现工具通过 SSH 运行命令以获取网络收集和操作系统指标。大多数命令都以普通用户身份运行。如果 sudo 不可用，少数命令会尝试 sudo 并自动回退：`dmidecode`（服务器 UUID 和制造商）、`lvdisplay`（LVM 检测）和`ss`或`netstat`（带有进程信息的网络连接）。如果没有 sudo，发现工具仍会收集大部分数据，但是 UUID、LVM 和进程级网络详细信息将丢失。我们建议为 SSH 用户配置无密码 sudo，以确保完整的数据收集。有关完整细分，请参阅the section called “所需的权限”。

VMware

- VMware vCenter Server 版本 6.5、6.7、7.0 或 8.0。
- 在 VMware vCenter 中部署 OVA 的权限。
- 对于 VMware vCenter Server 设置，需要在根数据中心级别分配 Read-Only 角色的 vCenter 用户。有关更多信息，请参阅 the section called “所需的权限”。

Hyper-V 先决条件

- 启用了该 Hyper-V 角色的 Windows 服务器。
- 在主机上 Hyper-V 启用了 WinRM。

- 一个用户帐户，它是每台 Hyper-V 主机上远程管理用户、Hyper-V 管理员和性能监控用户组的成员，拥有 WMI 对`root\cimv2`命名空间的读取权限。有关更多信息，请参阅 the section called “所需的权限”。
- 支持的身份验证：NTLM（仅限 HTTPS）和 Kerberos（HTTP 或 HTTPS）。

服务器导入先决条件

- 一个 CSV 文件，其中包含服务器主机名或 IP 地址以及与在发现工具上配置或要配置的操作系统凭据的友好名称对应的凭据名称（可选）。CSV 必须使用以下标题：

```
hostname_or_ip,os_credential_name,oracle_credential_name
```

- 必须能够通过发现工具 VM 访问服务器。默认端口：适用于 Linux 的 SSH 端口 22，适用于 Windows 的 WinRM 端口 5985/5986 。支持自定义端口。

Linux 安装程序必

- 支持的 Linux 发行版：亚马逊 Linux 2、亚马逊 Linux 2023、RHEL 8—9、Rocky Linux 8—9、9、Ubuntu 20.04—24.04、Debian 10—12 或 SLES 15 SP5。 AlmaLinux
- 至少 4 个 vCPU、16 GB 内存、35 GB 可用磁盘空间。
- 端口 5000 必须可用（其他服务未使用）。
- systemd 是服务管理所必需的。
- 发现工具 VM 必须能够通过网络访问您的目标基础架构。默认端口：端口 443 上的 vCenter、端口上的 Hyper-V 主机 5985/5986、端口 22 上的服务器。SSH、WinRM 和 SNMP 支持自定义端口。

甲骨文数据库先决条件

- 通过端口 1521（或自定义端口）从发现工具对 Oracle 主机的网络访问。
- 支持的 Oracle 版本：您可以通过直接 SQL 连接收集 Oracle Database 12c 发行版 1 (12.1) 及更高版本。 OS-level 回退检测适用于所有 Oracle 版本。
- 一个拥有 SELECT_CATALOG_ROLE 权限的只读 Oracle 服务帐户。有关更多信息，请参阅 the section called “甲骨文数据库 (SQL)”。
- 用于 OS-level 回退检测：通过 SSH 或 WinRM 访问 Oracle 主机（使用现有的操作系统凭据）。

部署在 VMware

VMware 虚拟机规格

- 操作系统 — 亚马逊 Linux 2023
- 内存 — 16 GB
- 中央处理器 — 4 个内核
- 磁盘 — 35 GB
- VMware 要求 — 参见在 VMware 上运行 AL2023 的 VMware 主机要求 AL2023

部署VMware OVA

1. 从以下网址下载 OVA 文件：https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.ova
2. 以 VMware 管理员身份登录 vCenter。
3. 使用以下方法之一安装 OVA 文件：

   a. 使用用户界面：选择文件，选择部署 OVF 模板，选择您在步骤 1 中下载的发现工具 OVA 文件，然后完成向导。确保服务器管理仪表板中的代理设置配置正确。

   b. 使用命令行：要从命令行安装发现工具 OVA 文件，请下载并使用 VMware 开放虚拟化格式工具 (ovftool)。要下载 ovftool，请从 OVF 工具文档页面中选择一个版本。这是使用 ovftool 命令行工具安装发现工具 OVA 文件的示例。

   ```
   ovftool --acceptAllEulas --name='discovery tool' --datastore=datastore1 -
   dm=thin AWS-Transform-discovery-tool.ova 'vi://username:password@vcenterurl/
   Datacenter/host/esxi/'
   ```

   示例中对可替换值的描述：

   - 该名称是您要用于发现工具 VM 的名称。
   - 数据存储是 vCenter 中数据存储的名称。
   - OVA 文件名是已下载的发现工具 OVA 文件的名称。
   - username/password 这些是您的 vCenter 凭证。
   - vcenterurl 是你的 vCenter 的网址。
   - vi 路径是指向 VMware ESXi 主机的路径。

4. 在 vCenter 中找到已部署的发现工具。 Right-click 虚拟机，然后选择 “开机”、“开机”。
5. 几分钟后，发现工具的 IP 地址将显示在 vCenter 中。您使用此 IP 地址连接到发现工具。

在上部署 Hyper-V

Hyper-V 虚拟机规格

- 操作系统 — 亚马逊 Linux 2023
- 内存 — 我们建议至少分配 16 GB
- CPU — 我们建议至少分配 4 个内核
- 磁盘 — 35 GB（包含在虚拟硬盘中）
- Hyper-V 要求 — 参见在上运行 AL2023 Hyper-V 的主机要求 Hyper-V AL2023

部署 Hyper-V VHD

1. 从以下网址下载 VHD 文件：https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.vhd
2. 将 VHD 文件复制到启用了该 Hyper-V 角色的 Windows 服务器计算机上。
3. 打开 Hyper-V 管理器。
4. 选择 “新建”，然后选择 “虚拟机”。
5. 完成安装向导。在 “指定层代” 页面上，选择 “第 1 代”。第 2 代虚拟机不支持 VHD 格式。在 “分配内存” 页面上，至少分配 16384 MB。在 Connect Virtual Hard Disk 页面上，选择 “使用现有虚拟硬盘”，然后选择您复制的 VHD 文件。
6. 启动虚拟机。几分钟后，在 Hyper-V 管理器中查看虚拟机的网络选项卡以找到 IP 地址，或者连接到虚拟机控制台并运行`ip addr`。您使用此 IP 地址连接到发现工具。

在 Linux 上部

该发现工具可作为独立的 Linux 安装程序使用，可在支持的 Linux 发行版上部署。如果要将发现工具直接安装在现有 Linux 服务器上，而不是部署虚拟机，请使用此选项。

Linux 服务器规格

- 内存 — 我们建议至少分配 16 GB

- CPU — 我们建议至少分配 4 个内核
- 磁盘 — 35 GB

支持的发行版

- 亚马逊 Linux — 亚马逊 Linux 2、亚马逊 Linux 2023
- 红帽企业 Linux 及其衍生产品 — RHEL 8—9、Rocky Linux 8—9、9 AlmaLinux
- Ubuntu — 20.04、22.04、24.04
- Debian — 10、11、12
- SUSE — SLES 15 SP5

安装发现工具

从以下 URL 下载安装程序脚本：https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh

在 Linux 上安装发现工具

1. 将安装程序脚本下载到您的 Linux 服务器。

```
curl -O https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/
latest/AWS-Transform-discovery-tool.sh
chmod +x AWS-Transform-discovery-tool.sh
```

2. （可选）运行兼容性检查以验证您的系统是否符合要求。

```
sudo ./AWS-Transform-discovery-tool.sh check
```

3. 安装发现工具。请选择以下选项之一：

   选项 1：使用自动依赖项安装进行安装（推荐）

   在安装服务之前，此选项会自动安装所有缺少的系统依赖项。

```
sudo ./AWS-Transform-discovery-tool.sh install --install-deps
```

   选项 2：安装时无需自动安装依赖项

此选项会检查是否缺少依赖项，如果缺少关键依赖项，则会显示带有手动安装说明的错误。如果您的组织限制自动安装软件包，并且您更喜欢手动管理系统软件包，请使用此选项。

```
sudo ./AWS-Transform-discovery-tool.sh install
```

4. 启动发现工具服务。

```
sudo ./AWS-Transform-discovery-tool.sh start
```

5. 访问发现工具，网址为https://*ip_address*:5000。

要卸载发现工具，请运行sudo ./AWS-Transform-discovery-tool.sh uninstall。

您也可以使用以下命令来管理服务：

- sudo ./AWS-Transform-discovery-tool.sh status— 检查服务是否正在运行。
- sudo ./AWS-Transform-discovery-tool.sh stop— 停止服务。
- sudo ./AWS-Transform-discovery-tool.sh logs— 查看服务日志。

系统依赖关系

安装程序会检查以下系统依赖关系：

依赖关系	严重性	用途
OpenSSL	重大	生成数据库加密密钥
libcrypt	重大	Python 运行时所必需的
Kerberos 库	警告	对 Windows 服务器进行 Kerberos 身份验证所必需的。否则，NTLM 和基本身份验证仍然有效。

启动发现工具需要关键的依赖关系。如果缺少它们，而您选择了选项 2（没有--install-deps），则安装程序会显示一条错误，其中包含手动安装它们的说明。 Warning-level 依赖关系是可选的 — 安装程序会向您发出警告，但会继续安装。

> **Note**
>
> 安装程序会检查系统兼容性，包括 glibc 版本和系统可用性。在装有 systemd 250 或更高版本的系统上（亚马逊 Linux 2023、RHEL 9、Rocky 9、 AlmaLinux 9、Ubuntu 24.04+、Debian 12+），数据库加密密钥使用系统凭据进行静态加密。在较旧的系统上，加密密钥存储为受权限保护的文件。

配置发现工具

访问发现工具控制台

1. 在 Web 浏览器中访问：`https://ip_address:5000`，部署发现工具的 IP 地址在哪里*ip_address*。发现工具使用自签名证书进行 HTTPS 连接，这会导致安全警告。选择接受风险并继续进入发现工具控制台。
2. 如果您是首次访问发现工具控制台，请创建发现工具登录密码。创建密码，供将来登录时使用。

> **Important**
>
> 记住这个密码——没有密码恢复机制。

访问发现工具 VM

- 默认情况下，发现工具 VM 带有用户名和密码（“发现”、“密码”）。为了提高安全性，我们建议您在通过虚拟机管理程序的控制台（例如，适用于 VMware 的 vSphere Client 或适用于 Manager 的 Manager）登录虚拟机`sudo passwd discovery`后使用更新密码。 Hyper-V Hyper-V
- 默认情况下，SSH 访问处于禁用状态。用户可以使用预先配置`enablessh`的`disablessh`别名 enable/disable 通过 SSH 访问发现工具 VM。启用 SSH 访问`ssh discovery@<VM-IP>`后，用户可以通过通过 SSH 进入虚拟机。鼓励用户在大多数情况下禁用 SSH 访问权限，并且仅在需要时才启用 SSH。运行时会强制更改密码`enablessh`。
- 要访问位于的发现工具数据目录`/home/ec2-user/.local/share/DiscoveryTool`，我们建议`ec2-user`通过运行切换到`sudo su ec2-user`。

配置 Kerberos 身份验证

Kerberos 身份验证是通过发现工具连接到 Windows 服务器的推荐方法。发现工具 VM 使用原生 Amazon Linux 2023 Kerberos 库对你的 Active Directory 域进行身份验证。

以下是发现工具 VM 上的 Kerberos 身份验证的要点：

- 使用`kinit`命令获取 Kerberos 票证`klist`并验证票证。
- Kerberos 配置文件位于。`/etc/krb5.conf`
- 在配置发现工具之前，请通过发现工具 VM 上的 CLI 验证发现工具是否`kinit`成功。

Kerberos 先决条件

在配置 Kerberos 身份验证之前，请确认您有以下信息和网络连接。

1. 请从您的活动目录管理员那里获取以下信息：
   - Kerberos 领域名称（通常是大写的域名，例如，）。`EXAMPLE.COM`
   - 密钥分发中心 (KDC) 的主机名或 IP 地址，该中心通常是域控制器（例如`dc01.example.com`）。
   - 具有针对目标 Windows 服务器进行身份验证的权限的服务帐户。
2. 验证发现工具 VM 是否具有与以下内容的网络连接：
   - 端口 88（TCP 和 UDP）上的 KDC 用于 Kerberos 身份验证。
   - WinRM 端口上的目标 Windows 服务器（HTTP 为 5985，HTTPS 为 5986）。

配置 Kerberos

完成以下步骤，在发现工具 VM 上配置 Kerberos 身份验证。

1. 通过 SSH 连接到发现工具虚拟机。

   ```
   ssh discovery@<discovery-tool-vm-ip>
   ```

2. 编辑 Kerberos 配置文件，网址为。`/etc/krb5.conf`

   ```
   sudo nano /etc/krb5.conf
   ```

   添加以下配置，用您的环境详细信息替换占位符值。

```
[libdefaults]
    default_realm = EXAMPLE.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
    EXAMPLE.COM = {
        kdc = dc01.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM
```

> **Important**
>
> Kerberos 区分大小写。领域名称必须为大写（例如`EXAMPLE.COM`，不是`example.com`）。该`[domain_realm]`部分中的域名必须为小写。

多个活动目录域

该发现工具支持不同的 Active Directory 域的多个 Kerberos 凭据。每个凭证都独立进行身份验证，因此您可以正常配置多个凭证，并且隔离是自动进行的。

如果您的服务器位于多个域中，请在`/etc/krb5.conf`文件中为每个领域添加条目：

```
[libdefaults]
    default_realm = DEV.COMPANY.COM
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
    DEV.COMPANY.COM = {
        kdc = dc01.dev.company.com
    }
    PROD.COMPANY.COM = {
        kdc = dc01.prod.company.com
    }
```

```
[domain_realm]
    .dev.company.com = DEV.COMPANY.COM
    dev.company.com = DEV.COMPANY.COM
    .prod.company.com = PROD.COMPANY.COM
    prod.company.com = PROD.COMPANY.COM
```

3. 通过运行命令验证是否可以获取 Kerberos 票证。`kinit`

```
kinit username@REALM.COM
```

出现提示时输入密码。如果命令完成时没有错误，则身份验证成功。

4. 通过运行`klist`命令来验证票证。

```
klist
```

预期输出类似于以下内容。

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: username@REALM.COM

Valid starting       Expires              Service principal
01/01/2025 12:00:00  01/01/2025 22:00:00  krbtgt/REALM.COM@REALM.COM
```

5. 使用与您使用的相同区分大小写的主体配置发现工具`kinit`（例如，`username@REALM.COM`）。

如果您的环境已为 Kerberos 服务发现`krb5.conf`配置了 DNS SRV 记录，则可能不需要进行显式配置。有关 Kerberos 配置选项的更多信息，请参阅 MIT Kerberos krb5.conf 文档和示例 krb5.conf 文件。

从加入域的计算机中查找 Kerberos 配置

如果您没有 Kerberos 配置详细信息，则可以从已加入该域的 Windows 计算机上检索它们。在加入域的计算机上使用命令提示符运行以下命令。

要查找域名，请运行以下命令。

```
echo %USERDNSDOMAIN%
```

输出示例：

```
EXAMPLE.COM
```

要查找域控制器主机名，请运行以下命令。

```
nltest /dsgetdc:EXAMPLE.COM
```

输出示例：

```
           DC: \\dc01.example.com
      Address: \\10.0.1.100
     Dom Guid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
     Dom Name: EXAMPLE.COM
   Forest Name: example.com
  Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
         Flags: 0xe00033fd
The command completed successfully
```

将输出映射到您的`krb5.conf`配置，如下所示：

- Realm-使用大写`%USERDNSDOMAIN%`的值（例如，`EXAMPLE.COM`）。
- KDC — 使用`nltest`输出中的 DC 主机名（例如`dc01.example.com`）。

配置 vCenter 访问权限

1. 在 “发现” 工具页面的 “步骤 1” 下。配置发现源，选择配置来源。
2. 在配置发现源页面上，提供友好名称、vCenter FQDN/IP、用户名和密码。
3. 选择 Save configuration。

   发现工具开始收集 vCenter 信息，如已发现清单中所述。

完成初始配置后，在发现工具状态框中选择编辑 vCenter 访问权限以更改您的 vCenter 访问设置。

该发现工具并行收集来自所有已配置的 vCenter 服务器的数据。如果在收集过程中无法访问一个 vCenter 服务器，则该工具会报告部分成功并继续从其余的 vCenter 服务器进行收集。

如果虚拟机出现在多个 vCenter 服务器上（例如，由于共享 ESXi 主机或跨vCenter vMotion），则发现工具会自动对虚拟机进行重复数据删除。每个唯一的 VM 在清单中仅出现一次。

配置 Hyper-V 访问权限

1. 在 “发现” 工具页面的 “步骤 1” 下。配置发现源，选择配置来源。
2. 在 “配置发现源” 页面上，提供友好名称、主机 FQDN 或 IP 地址、身份验证类型（NTLM 或 Kerberos）、WinRM 用户名和 WinR M 密码。
3. 选择 Save configuration。

   发现工具开始收集 Hyper-V 信息，如已发现清单中所述。

保存凭证后，会自动开始收集。

对于 Hyper-V 故障转移群集，您可以在同一个群集中添加多个主机。该工具会自动对出现在多台主机上的虚拟机进行重复数据删除。

导入服务器

1. 从 Discovery 工具主页导航到 “导入服务器” 页面。
2. 准备包含以下列的 CSV 文件：`hostname_or_ip`（必填）、`os_credential_name`（可选）和`oracle_credential_name`（可选）。
   - 该`hostname_or_ip`值必须是有效的 IPv4 地址或完全限定的域名 (FQDN)。
   - 该`os_credential_name`值（如果提供）必须与您已经配置的操作系统凭证（SSH、WinRM 或 SNMP）的友好名称相匹配。对于尚未配置操作系统凭据的服务器，请将其留空。
   - 该`oracle_credential_name`值（如果提供）必须与您已经配置的 Oracle 凭据的友好名称相匹配。
3. 上传 CSV 文件。该工具会验证所有行，如果有任何行无效，则拒绝该文件。

成功导入后，如果配置了操作系统凭据，该工具将自动开始为导入的服务器收集数据库、网络和操作系统指标。如果您上传另一个 CSV 文件，则会在不创建重复记录的情况下更新现有记录，并将新记录合并到清单中。

将自签名证书颁发机构导入发现工具（可选）

当您通过 HTTPS 使用 WinRM 和目标服务器使用由自签名证书颁发机构 (CA) 签名的 WinRM HTTPS 证书，并且您想在发现工具上启用 “验证服务器 SSL 证书” 时，这是必需的。

先决条件

1. Self-signed 用于在目标服务器上签署 WinRM HTTPS 证书的 CA 证书
2. PEM 格式的证书（.pem 或.crt 扩展名）

要在发现工具 VM 上导入自签名证书颁发机构，请执行以下操作：

1. SSH 到发现工具 VM
2. 将签署目标服务器 WinRM 证书的 CA 证书放入发现工具 VM `/etc/pki/ca-trust/source/anchors/` 上的信任存储目录中。例如：`sudo cp winrm-ca.pem /etc/pki/ca-trust/source/anchors/winrm-ca.pem`。注意：如果您的目标服务器使用由不同 CA 签名的证书，请将所有相关的 CA 证书复制到此目录中。
3. 更新证书信任存储：`sudo update-ca-trust`
4. 重启虚拟机
5. （可选）要验证证书是否已成功导入，可以运行以下命令。`sudo trust list –filter=ca-anchors | grep -A 5 "<certificate_name>"`

请参阅 Windows 远程管理的安装和配置

为操作系统访问配置发现工具

配置操作系统访问权限，以便发现工具能够：

- 发现数据库以执行数据库评估并协助虚拟机迁移，
- 跟踪清单中服务器之间的网络连接，包括与每个连接相关的进程，以帮助进行应用程序依赖关系映射和波浪规划。仅包括两个端点都在发现工具清单中的连接。

启用发现工具 OS Access

1. 导航至设置操作系统访问权限页面以提供 Windows 和 Linux 凭据。
2. 选择要为其添加凭据的协议。
3. 提供所选协议所需的凭据。
4. 选择Auto-connect启用发现工具，在找到每台服务器的匹配凭据之前，在发现的服务器上尝试所有提供的凭据。

   有关自动连接功能的重要安全建议，请参阅the section called “谨慎使用 Auto-Connect 功能”。

5. 选择 “设置并连接”。

操作系统匹配过程完成后，您会看到一条消息，提示数据收集正在进行中，以及一条有关未找到凭据匹配的服务器的错误。

支持的协议设置

您必须在目标服务器上设置 WinRM、SSH 和 SNMP 协议，发现工具才能与它们通信。

设置 WinRM 和 WMI

WinRM 会自动与当前支持的所有版本的 Windows 操作系统一起安装。

要验证或编辑 WinRM 配置，请使用`winrm`命令行工具：

- 验证已安装的 WinRM 侦听器：`winrm enumerate winrm/config/listener`
- 验证 WinRM 配置：`winrm get winrm/config`
- 设置 WinRM 的命令示例：`winrm quickconfig -transport:https`

监听器端口

默认 HTTP 端口为 5985；HTTPS 为 5986。您可以根据需要使用其他端口。发现工具和目标服务器之间的端口必须处于打开状态。

加密

发现工具使用加密的 WinRM 通信。我们建议目标服务器上的 WinRM 侦听器也使用加密：`winrm set winrm/config/service '@{AllowUnencrypted="false"}'`

NTLM vs Kerberos

发现工具支持 WinRM 身份验证协议 Kerberos 和 NTLM。NTLM 只能与 HTTPS 一起使用，Kerberos 可以同时与 HTTP 或 HTTPS 一起使用。

WMI 要求

发现工具查询以下 WMI 命名空间。WinRM 账户需要对与您的集合模块相关的每个命名空间具有读取权限：

WMI 命名空间	使用者
`root\cimv2`	操作系统指标、 Hyper-V 主机元数据、SQL Server 集合
`root\virtualization\v2`	Hyper-V 虚拟机清单
`root\StandardCIMV2`	网络收藏
`root\Microsoft\SqlServer\ComputerManagement*`	SQL 服务器集合
`root\Microsoft\SqlServer\ReportServer\*`	SQL 服务器集合 (SSRS)

对于网络收集，请确保满足以下条件：

- 允许通过 ICMP 进行网络连接
- 允许通过 TCP 端口 135 + 临时 TCP 端口范围 (49152-65535) 进行网络连接
- 禁用 UAC
- 已设置远程 DCOM 权限
- 创建所需权限最少的专用服务账户
- WMI 命名空间权限是为具有命名空间:、类的 Windows 账户设置的 `\\root\\standardcimv2` `MSFT_NetTCPConnection`

对于 SQL Server 集合，由于复杂的 WMI 对象权限要求，需要一个属于本地管理员组的 Windows 帐户（本地或域）。

设置 SSH

- 默认端口为 22。支持自定义端口。必须在发现工具和目标服务器之间打开配置的端口。
- 为使 SSH 网络收集正常工作，请提供配置为使用无密码 sudo 的用户。
- 确保目标 Linux 服务器上有以下命令（默认安装在大多数发行版上）：`ss`或`netstat`用于网络收集，以及、`lsblk`、`iostat`、`dmidecode`、`smartctl`、`top`、`psfreeip`、和，`df`用于操作系统指标收集。

该发现工具支持 SSH 的两种身份验证方法：

选项 1：用户名和密码

提供 SSH 用户名和密码。这是默认的身份验证方法。

选项 2：SSH 私钥

提供 SSH 用户名和 PEM 格式的私钥。要使用此选项，请在配置 SSH 凭据时从 “身份验证类型” 下拉列表中选择 SSH 密钥。如果私钥使用密码加密，请在可选的密钥密码字段中输入密码。

支持以下密钥格式：

- RSA
- ECDSA
- ed25519
- OpenSSH 格式
- PKCS #8 格式

两种身份验证方法都支持自动连接。凭证以静态加密方式存储。

设置 SNMP

- 默认端口为 161/UDP。支持自定义端口。必须在发现工具和目标服务器之间打开配置的端口。
- 对于 SNMP v2：提供一个可以访问 TCP 连接 OID 的只读社区字符串。
- 对于 SNMP v3：提供 username/password 具有可访问 TCP 连接 OID 的只读权限的 auth/privacy 详细信息

发现工具需要访问以下内容：

- `"1.3.6.1.2.1.6.13.1.1." (tcpConnState)`
- `"1.3.6.1.2.1.6.19.1.8." (tcpConnectionProcess)`
- `"1.3.6.1.2.1.25.4.2.1.2." (hrSWRunName)`

配置 Oracle 数据库访问权限

将 Oracle 数据库访问权限配置为直接通过 SQL 连接收集详细的 Oracle 数据库元数据。收集的元数据包括 CDB 和 PDB 拓扑、功能使用情况和已安装的选项。这些数据可以帮助您更准确地规划 Oracle 数

据库迁移。你可以通过直接 SQL 连接收集 Oracle Database 12c 版本 1 (12.1) 及更高版本。 OS-level 回退检测适用于所有 Oracle 版本。

在发现工具中配置 Oracle 凭据

1. 在发现工具页面的边栏中，选择数据库访问权限。
2. 选择添加 Oracle 凭据。
3. 提供以下信息：
   - 友好名称-此凭证的描述性名称（例如）。`Oracle Production`
   - 端口 — Oracle 监听器端口（默认为 1521）。
   - 服务名称-目标数据库的 Oracle 服务名称。
   - 用户名-Oracle 服务帐户的用户名。
   - 密码-Oracle 服务帐户密码。
   - Auto-connect— 启用此选项可尝试使用库存中的所有服务器的凭证。关闭此选项可手动将凭据分配给特定服务器。
4. 要添加更多凭据（例如，针对不同的 Oracle 环境），请再次选择添加 Oracle 凭据。
5. 选择保存。

凭证模式

配置 Oracle 凭据时，可以在两种模式之间进行选择：

- 手动 — 将凭据固定到特定服务器。发现工具将该凭据专门用于该服务器。如果连接失败，则不会发生回退。修复凭证配置以解决问题。
- Auto-connect— 发现工具会针对清单中的每台服务器尝试使用每个自动连接凭证。当服务器成功获得证书时，发现工具将使用该凭证进行后续的所有收集回合。

检测流程

配置 Oracle 凭据时，发现工具会首先尝试直接 SQL 连接。如果所有数据库凭据都失败，则该工具会回退到通过 SSH 或 WinRM 进行 OS-level 检测，因此您仍然可以在不访问数据库的情况下发现 Oracle 安装。

更新发现工具

该发现工具没有自动更新功能，但是在安装 30 天后，您将收到提醒通知以进行更新。建议使应用程序保持最新状态，以接收最新的功能和安全补丁。

手动更新工具

1. 从提供的链接下载最新的发现工具映像文件（适用于 VMware 的 OVA 或适用于 VHD 的 VHD Hyper-V）。
2. （可选）我们建议您在部署最新的发现工具图像文件之前删除以前的发现工具映像文件。
3. 按照 “部署发现工具” 部分中的步骤部署更新版本。

撤消访问权限

您可以单独撤消对每个发现源的访问权限。当您撤消对一个源的访问权限时，来自其他来源的数据不会受到影响。

- 撤消 vCenter 访问权限-删除 v Center 凭据和数据。 VMware-collected 不删除 Hyper-V 数据、导入的服务器数据或操作系统凭据。
- 撤消 Hyper-V 访问权限-仅删除 Hyper-V 凭据和 Hyper-V-collected 数据。
- 删除导入的服务器-从清单中移除导入的服务器。保留从这些服务器收集的下游收集数据（网络、数据库）。

发现工具所需的权限

该发现工具使用多种协议连接到您的基础架构。每个协议和收集模块都需要特定的账户权限。本节介绍完成数据收集所需的最低权限，以及如果某些权限不可用，您将丢失哪些数据。

VMware vCenter

该发现工具通过端口 443 (HTTPS) 连接到 VMware vCenter Server 并执行只读操作。未对您的 vCenter 环境进行任何更改。

最低要求角色： Read-Only，在 vCenter 根级别分配。

该 Read-Only 角色提供发现工具收集虚拟机清单（名称、UUID、CPU、内存、磁盘、网络、电源状态、客户机操作系统）和性能指标（CPU 利用率、内存利用率、磁盘 IOPS 和吞吐量）所需的所有访问权限。

建议：在根数据中心级别创建具有内置 Read-Only 角色的专用 vCenter 用户。

Hyper-V 主机 (Windows)

该发现工具通过 WinRM 连接到 Hyper-V 主机（HTTP 端口 5985，HTTPS 端口 5986），并运行 PowerShell 命令来收集虚拟机清单、主机元数据和存储性能。

每位 Hyper-V主持人@@ 所需的最低群组成员资格：

Windows 群组	为什么需要它
远程管理用户	基准 WinRM 远程访问
Hyper-V 管理员	虚拟机清单收集（虚拟机列表、磁盘、网络、内存、客户机操作系统）
性能监控器用户	存储 I/O 性能计数器（每个 VM 的 read/write IOPS 和吞吐量）

该账户还需要 WMI 对主机操作系统版本和硬件 UUID 的`root\cimv2`命名空间的读取权限。默认情况下，本地管理员会授予此访问权限，但必须为非管理员帐户明确配置此访问权限。

建议：创建一个专用的域服务帐户，并将其添加到每台 Hyper-V 主机上的 “远程管理用户”、“管理 Hyper-V 员” 和 “性能监控器用户” 组中。避免使用域管理员帐户。

Linux 服务器 (SSH)

该发现工具通过 SSH（端口 22）连接到 Linux 服务器，以收集操作系统指标、网络连接和服务器清单。大多数数据收集都是以普通用户身份进行的。如果 sudo 不可用，少量命令会尝试`sudo`并自动回退。

所需的最低访问权限：可以登录目标服务器的 SSH 用户帐户。

推荐访问权限：同一个 SSH 用户配置了无密码 sudo 以进行完整的数据收集。

什么需要 sudo 以及没有 sudo 会发生什么：

收集的数据	需要 Sudo 吗？	没有 sudo 你会失去什么
服务器名称、操作系统、CPU、内存、IP、磁盘数量	否	什么都没有 — 以普通用户身份收集
CPU、内存和网络利用率	否	什么都没有 — 以普通用户身份收集
磁盘 IOPS、吞吐量和空间	否	什么都没有 — 以普通用户身份收集
网络接口配置	否	什么都没有 — 以普通用户身份收集
正在运行的进程（名称、PID、命令）	否	什么都没有 — 以普通用户身份收集
服务器 UUID 和 SMBIOS UUID	是	导出时的 UUID 字段为空
硬件制造商（物理检测与虚拟检测）	是	在较旧的发行版中，资源类型检测不太准确
LVM 逻辑卷检测	是	未检测到 LVM 卷；卷类型可能显示为 “未知”
带有进程名称和 PID 的网络连接	是	连接仍会被收集，但没有流程归因（PID 和流程名称列为空）
Oracle 数据库 OS-level 检测（未配置 Oracle 凭据时的回退）	是	基本的 Oracle 在线状态检测（oratab，进程监视器）无需使用 sudo 即可运行。详细收集（opatch、lsnrctl、ASM、Grid Infrastructure）需要无密码`sudo -u oracle`访问 Oracle 主目录二进制文件。

> **Note**
>
> 由于缺乏 sudo，发现工具永远不会完全失败。它尽其所能收集并报告部分结果。但是，要获得最完整的数据，尤其是带有进程名称的网络依赖关系映射，我们建议使用无密码 sudo。

目标服务器上必需的实用程序：以下命令应可用（在大多数 Linux 发行版中默认安装）：ss或netstat、lsblk、top、ps、、free、ip、df、、hostname、cat、nproc、、和grep。对于其他数据，可选：iostat（磁盘 I/O 详细信息）、dmidecode（硬件 UUID）、smartctl（磁盘接口类型）、lvdisplay（LVM 检测）。

Windows 服务器 (WinRM) — 操作系统指标

该发现工具通过 WinRM 连接到 Windows 服务器，以收集操作系统指标（服务器清单、性能、存储、网络接口和正在运行的进程）。

所需的最低访问权限：可以远程访问目标服务器的 WinRM-enabled 用户帐户。

推荐访问权限：本地管理员组中的用户，用于完成数据收集。

权限级别	它能做什么	没有它你会失去什么
远程管理用户（WinRM 访问权限）	所有 Windows 数据收集	未从服务器收集任何数据
WMI 的读取权限 root\cimv2	服务器名称、操作系统版本、内存、UUID、BIOS 序列号、磁盘空间	服务器清单字段为空
性能监控器用户	CPU 利用率、网络吞吐量、磁盘 IOPS 和吞吐量	未收集绩效指标
本地管理员	正在运行的进程所有者姓名	已收集进程列表但该 user/owner 列为空

> **Note**
>
> 本地管理员成员资格隐式授予性能监控器用户访问权限和 WMI 读取权限，因此它满足上述所有要求。

> **Note**
>
> 未配置 Oracle 凭据时，Windows 上的 Oracle 数据库 OS-level 回退检测使用注册表查询`Get-Service`和`Get-Process`命令。这些命令只需要标准的远程管理用户访问权限。除了操作系统指标要求之外，不需要其他权限。

Windows 服务器 (WinRM) — SQL Server 集合

SQL Server 集合发现 Windows 服务器上的 SQL Server 实例、报告服务 (SSRS) 和集成服务 (SSIS)。

推荐访问权限：每台目标 Windows 服务器上本地管理员组中的一个用户。

建议使用本地管理员，因为 SQL Server 发现会查询多个 WMI 命名空间，并且某些操作需要提升访问权限：

发现了什么	需要许可	没有它你会失去什么
SQL Server 数据库引擎实例（版本、版本、状态）	WMI 对命名空间的读取`root\Microsoft\SqlServer\ComputerManagement*` 权限	未发现 SQL 服务器实例
SQL Server Reporting Services (SSRS)	WMI 对命名空间的读取`root\Microsoft\SqlServer\ReportServer` 权限	未发现 SSRS 组件
SSRS 网址和端口配置	提升权限（本地管理员）	SSRS 网址预留详情缺失
SQL Server Integration Services (SSIS)	注册表读取权限 (HKLM)	SSIS 版本和版本缺失
Port-to-service 协会	访问 TCP 监听器枚举	无法将侦听端口与 SQL Server 服务相关联

> **Note**
>
> SQL 服务器集合是 Windows-only。该发现工具会跳过 Linux 服务器进行 SQL Server 发现。

甲骨文数据库 (SQL)

Oracle 数据库集合通过端口 1521（或自定义端口）直接连接到 Oracle 实例，以收集数据库元数据。该发现工具不需要 DBA 或 SYSDBA 权限。

所需的最低访问权限：具有 SELECT_CATALOG_ROLE 权限的只读 Oracle 服务帐户。

发现工具无法访问诊断包或调整包视图，因此无需额外的 Oracle 许可证即可进行数据收集。

创建账户的 SQL：

```
CREATE USER discovery_user IDENTIFIED BY <password>;
GRANT CREATE SESSION TO discovery_user;
GRANT SELECT_CATALOG_ROLE TO discovery_user;
```

OS-level 回退：如果未配置数据库凭据或连接失败，则发现工具将使用现有的 SSH 或 WinRM 操作系统凭据来检测 Oracle 的安装。除了 Oracle-specific 操作系统指标模块要求的权限外，不需要其他操作系统权限。

网络收藏

网络收集使用不同的协议，具体取决于服务器的操作系统：

服务器操作系统	协议	所需权限
Linux	SSH	连接数据的普通用户。对于进程级别的详细信息（PID 和进程名称），建议使用无密码 sudo。
Linux	snmpv2	一个只读社区字符串，可以访问 TCP MIB（tcp ConnState、tcpConnectionProcess）和主机资源 MIB（hrSWR unName）。
Linux	snmpv3	对与 SNMPv2 相同的 MIB 具有读取权限的 USM 用户。支持 “否” AuthNoPriv、“身份验证” NoPriv 和 “AuthPriv” 安全级别。

服务器操作系统	协议	所需权限
Windows	WinRM	WMI 对`root\StandardCIMV2` 命名空间（msft_nettcpConnection 类）的读取权限。

快速参考：按用例划分的最低权限

使用案例	账户类型	最小权限
VMware VM	vCenter 用户	Read-Only 根数据中心级别的角色
Hyper-V 虚拟机发现	Windows 域名或本地账户	远程管理用户 + 管理 Hyper-V 员 + 每台主机上的性能监控器用户
Linux 操作系统指标-完整数据	SSH 用户	无密码 sudo
Linux 操作系统指标 — 部分数据	SSH 用户	普通用户（没有 sudo）。UUID、制造商、LVM 和网络进程信息将丢失。
Windows 操作系统指标-完整数据	WinRM 用户	本地管理员
Windows 操作系统指标-基本数据	WinRM 用户	远程管理用户 + WMI 读取权限 `root\cimv2`
SQL 服务器数据库发现	WinRM 用户	本地管理员
甲骨文数据库发现 (SQL)	甲骨文服务账户	SELECT_CATALOG_ROLE（只读，没有 DBA 或 SYSDBA）
网络集合 — Linux (SSH)	SSH 用户	无密码 sudo 用于处理级数据；普通用户仅用于连接数据
网络集合 — Linux (SNMP)	SNMP 社区字符串或 USM 用户	对 TCP 和主机资源 MIB 的读取访问权限

使用案例	账户类型	最小权限
网络集合 — Windows	WinRM 用户	WMI 的读取权限 `root\StandardCIMV2`

数据收集

发现工具收集时间表

收集初始发现后，发现工具将继续按错开计划运行，以避免资源争用：

- VMware 发现 — 每小时一次（世界标准时间 0:00）
- Hyper-V 发现 — 每小时一次（世界标准时间：20 点）

该发现工具还通过以下独立模块收集操作系统指标，每个模块都有自己的错开时间表：

- 网络指标 — 每 15 秒，对于大型环境，可能不那么频繁
- 服务器性能指标 — 每 10 分钟（世界标准时间:03、:13、:23、:33、:43、:43、:53）
- 存储性能指标 — 每 10 分钟（世界标准时间:07、:17、:27、:37、:47、:47、:57）
- 正在运行的进程 — 每小时（世界标准时间:40 分）
- 服务器配置数据-每日（世界标准时间 00:05）
- 存储配置数据 — 每天（世界标准时间 00:35）
- 网络接口-每天（世界标准时间 01:05）
- SQL Server 发现 — 每天（世界标准时间 03:05）
- Oracle 数据库发现 — 每天（世界标准时间 05:05）

您可以使用 “立即收集数据” 独立启动、停止或触发每个操作系统指标模块。

要手动运行收藏夹，请从 “操作” 菜单中选择：

- 启动-启用发现模块。
- 停止 — 禁用发现模块。
- 立即收集数据-立即开始发现。例如，在网络中进行更改后使用此选项。

这些操作适用于每个模块。您可以单独控制操作系统指标模块。

操作系统数据收集尝试

当发现新服务器时，发现工具会尝试为每个 IP 地址和主机名配置的每个凭据。发现工具找到有效凭证后，除非您添加新凭证，否则将继续使用该凭证。

收集失败后，发现工具会在 3 分钟、30 分钟、2 小时和 6 小时后尝试为服务器收集网络数据。在 4 次尝试失败后，发现工具继续每 6 小时尝试一次所有已配置的凭证。

已发现的库存

配置发现源后，发现工具状态框中的已发现服务器数量值开始增加。在集合模块框架中，已配置源的发现状态更改为 “启用”。清单页面显示来自所有已配置来源的服务器：VMware 虚拟 Hyper-V 机、虚拟机和导入的服务器。每台服务器都显示其每个模块的源和集合状态。

导航到 “已发现清单” 页面，查看发现工具找到的服务器。在此页面上，选择 “下载清单” 以下载一个 ZIP 文件 (`discovery_tool_export.zip`)，其中包含长达 30 天的收集数据，包括所有已配置来源的 MPA 文件、性能利用率数据、数据库信息以及服务器到服务器的通信信息。

您可以在发现工具继续运行的同时下载 ZIP 文件，并获得部分结果。将此文件上传到迁移评估以获取迁移业务案例。

导出选项

导出数据时，您可以使用以下选项自定义导出：

日期范围

选择开始日期和结束日期，以便仅导出在该时间段内收集的数据。两个日期均包含在内。最长日期范围为 30 天。

> **Note**
>
> 该发现工具最多可存储 30 天的收集数据。如果您需要跨度超过 30 天的数据，请每 30 天运行一次增量导出以捕获所有数据。

模块选择

选择要包含在导出中的数据模块。您可以导出所有模块或选择特定模块：

模块	说明
VMware	来自 vCenter 服务器的虚拟机清单
Hyper-V 数据	来自 Hyper-V 主机的虚拟机清单
网络数据	服务器之间的网络连接
服务器清单	服务器硬件和操作系统信息
服务器性能指标	CPU、内存和网络利用率
服务器存储性能	磁盘 IOPS 和吞吐量
存储配置	磁盘和卷配置
网络接口	网络适配器详细信息
进程指标	运行的进程
SQL 服务器数据	SQL 服务器数据库清单
甲骨文数据库数据	Oracle 数据库清单 — CDB、PDB、功能、选项和组件

如果您未选择任何模块，则发现工具会导出所有可用数据。

收集的数据点

该发现工具可收集有关 VMware、 Hyper-V、操作系统指标、数据库和网络组件的全面数据。以下各节详细介绍了为每个组件收集的具体数据点。

VMware 数据集

下表描述了发现工具收集的 VMware 虚拟机信息：

Name	Type	类别	示例值
vm_name	字符串	虚拟机信息	“w2k22-snmpd-v2-en-us-mssql-2022-testcase4-1”

Name	Type	类别	示例值
vm_id	字符串	虚拟机信息	“vm-30920"
vm_uuid	字符串	虚拟机信息	“4201ecf8-cc44-ee7e-01df-34dfb2acf6c0”
权力状态	字符串	虚拟机信息	“PowerEdon”
host	字符串	虚拟机信息	“esxi-70-node1.testlab.local”
主要的 IP 地址	字符串	虚拟机信息	“192.168.0.52”
cpus	整数	虚拟机信息	2
memory	整数	虚拟机信息	4096
总磁盘容量_mib	整数	虚拟机信息	32768
os_according_to_to_the_configuration	字符串	虚拟机信息	“微软 Windows Server 2016 或更高版本（64 位）”
max_cpu_usage_pct_dec	浮点型	虚拟机性能	79.33
avg_cpu_usage_pct_dec	浮点型	虚拟机性能	45.06
max_ram_usage_pct_dec	浮点型	虚拟机性能	63.99
avg_ram_utl_pct_dec	浮点型	虚拟机性能	29.27

Hyper-V 数据收集

下表描述了发现工具收集的 Hyper-V 虚拟机信息：

Name	Type	类别	示例值
vm_name	字符串	虚拟机信息	“win2022-hyperv-test-01”
vm_id	字符串	虚拟机信息	“a1b2c3d4-e5f6-7890-abcd-ef1234567890”

Name	Type	类别	示例值
权力状态	字符串	虚拟机信息	“跑步”
cpus	整数	虚拟机信息	4
memory_mb	整数	虚拟机信息	8192
磁盘路径	字符串	磁盘	“C:\\ vM\\ disk1.vhdx”
磁盘大小_gb	浮点型	磁盘	127.0
网络适配器	字符串	Network	“00:15:5D:01:02:03”
IP 地址	字符串	Network	“10.0.1.50"
host_name	字符串	主机	“hyperv-host-01.example.com”
主机操作系统版本	字符串	主机	“Windows 服务器 2022 数据中心”
cluster_name	字符串	主机	“FailoverCluster01"
hypervisor	字符串	虚拟机信息	"Hyper-V"

已导入的服务器数据

导入的服务器不会自动被发现。它们是通过 CSV 文件导入的。该发现工具不会为导入的服务器收集虚拟机管理程序级别的数据。相反，它在导入过程中使用与每台服务器关联的操作系统凭据来收集数据库、网络和操作系统指标数据。

发现工具 OS-related 的数据

该发现工具通过 SSH (Linux) 和 WinRM (Windows) 收集服务器清单、性能、存储、网络接口和流程数据。下表描述了收集的数据点。

服务器清单 (server_inventory.csv)

将服务器配置（硬件和操作系统配置）与聚合存储性能相结合。每 24 小时收集一次。

Name	Type	类别	示例值
服务器_ID	字符串	服务器信息	“vm-web-server-01”
server_name	字符串	服务器信息	“网络服务器-01"
resource_type	字符串	服务器信息	“虚拟机”
电源状态	字符串	服务器信息	“跑步”
os_type	字符串	服务器信息	“Linux”
os_name	字符串	服务器信息	“亚马逊 Linux”
os_version	字符串	服务器信息	“2023”
主主机名	字符串	服务器信息	“web-server-01.example.com”
主要的 IP 地址	字符串	服务器信息	“10.0.2.101”
网络掩码	字符串	服务器信息	“255.255.255.0”
网络卡总数	整数	服务器信息	2
磁盘总数	整数	服务器信息	1
cpu_count	整数	服务器信息	4
总内存_GB	浮点型	服务器信息	15.88
server_uuid	字符串	服务器信息	“4201ecf8-cc44-ee7e-01df-34dfb2acf6c0”
smbios_uuid	字符串	服务器信息	“4201ecf8-cc44-ee7e-01df-34dfb2acf6c0”
cluster_name	字符串	服务器信息	“生产集群 01”
虚拟机管理程序_object_id	字符串	服务器信息	“vm-30920"
虚拟机管理程序类型	字符串	服务器信息	“VMware”

Name	Type	类别	示例值
虚拟机管理程序版本	字符串	服务器信息	“8.0.0"
虚拟机管理程序_主机名	字符串	服务器信息	“esxi-node1.example.com”
虚拟机管理程序_host_id	字符串	服务器信息	“host-1234”
虚拟机管理程序_id	字符串	服务器信息	“4201ecf8-cc44-ee7e-01df-34dfb2acf6c0”
disk_read_iops_avg	浮点型	存储性能	12.5
disk_read_ips_peak	浮点型	存储性能	245.0
disk_write_iops_avg	浮点型	存储性能	8.3
disk_write_ips_peak	浮点型	存储性能	180.0
disk_total_iops_avg	浮点型	存储性能	20.8
磁盘总数 iops_peak	浮点型	存储性能	425.0
磁盘读取吞吐量_avg_mbps	浮点型	存储性能	1.2
磁盘读取吞吐量峰值mbps	浮点型	存储性能	24.5
disk_write_trougput_avg_mbps	浮点型	存储性能	0.8
disk_write_trougput_peak_mbps	浮点型	存储性能	18.0
磁盘总吞吐量_avg_mbps	浮点型	存储性能	2.0
磁盘总吞吐量_峰值_mbps	浮点型	存储性能	42.5

服务器性能指标 (server_performance_metrics.csv)

CPU、内存和网络吞吐量利用率。每 10 分钟采样一次，在 30 天内汇总一次。

Name	Type	类别	示例值
服务器_ID	字符串	服务器信息	“vm-web-server-01”
data_source	字符串	服务器信息	“OS”
cpu_utilization_avg_pct	浮点型	CPU	45.06
cpu_ustilization_peak_pct	浮点型	CPU	79.33
cpu_count	整数	CPU	4
内存总量_GB	浮点型	内存	15.88
内存利用率_avg_pct	浮点型	内存	29.27
内存利用率峰值peak_pct	浮点型	内存	63.99
network_in_avg_mbps	浮点型	Network	0.52
network_in_in_peak_mbps	浮点型	Network	12.3
network_out_avg_mbps	浮点型	Network	0.31
network_out_peak_mbps	浮点型	Network	8.7
网络总量_avg_mbps	浮点型	Network	0.83
网络总计 peak_mbps	浮点型	Network	21.0

存储性能 (server_storage_performance.csv)

Per-volume 磁盘 I/O 和空间利用率。每 10 分钟采样一次，在 30 天内汇总一次。

Name	Type	类别	示例值
服务器_ID	字符串	服务器信息	“vm-web-server-01”
data_source	字符串	服务器信息	“OS”

Name	Type	类别	示例值
磁盘卷 ID	字符串	卷信息	"/dev/nvme0n1p1"
磁盘挂载点	字符串	卷信息	"/"
文件系统	字符串	卷信息	“xfs”
disk_total_GB	浮点型	磁盘空间	30.0
disk_used_gb	浮点型	磁盘空间	12.5
disk_free_gb	浮点型	磁盘空间	17.5
disk_read_iops_avg	浮点型	磁盘 I/O	12.5
disk_read_ips_peak	浮点型	磁盘 I/O	245.0
disk_write_iops_avg	浮点型	磁盘 I/O	8.3
disk_write_ips_peak	浮点型	磁盘 I/O	180.0
disk_total_iops_avg	浮点型	磁盘 I/O	20.8
磁盘总数 iops_peak	浮点型	磁盘 I/O	425.0
磁盘读取吞吐量_avg_mbps	浮点型	磁盘吞吐量	1.2
磁盘读取吞吐量峰值mbps	浮点型	磁盘吞吐量	24.5
disk_write_trougput_avg_mbps	浮点型	磁盘吞吐量	0.8
disk_write_trougput_peak_mbps	浮点型	磁盘吞吐量	18.0
磁盘总吞吐量_avg_mbps	浮点型	磁盘吞吐量	2.0
磁盘总吞吐量_峰值_mbps	浮点型	磁盘吞吐量	42.5

存储配置 (storage_config.csv)

物理磁盘硬件详细信息。每 24 小时收集一次。

Name	Type	类别	示例值
服务器_ID	字符串	服务器信息	“vm-web-server-01”
磁盘控制器_ID	字符串	磁盘信息	"/dev/sda"
vmdk_vhd_file_name	字符串	磁盘信息	“网络服务器 01.vmdk”
磁盘卷类型	字符串	磁盘信息	“虚拟”
磁盘配置_gb	浮点型	磁盘信息	30.0
磁盘设备类型	字符串	磁盘信息	“SCSI 硬盘”
磁盘接口类型	字符串	磁盘信息	“SCSI”
磁盘协议	字符串	磁盘信息	“LSI Logic SAS”

网络接口 (network_interfaces.csv)

网络适配器配置。每 24 小时收集一次。

Name	Type	类别	示例值
服务器_ID	字符串	服务器信息	“vm-web-server-01”
接口_名称	字符串	接口信息	“eth0"
接口索引	整数	接口信息	2
mac 地址	字符串	接口信息	“0A:1B:2C:3D:4E:5F”
适配器类型	字符串	接口信息	“vmxnet3”
虚拟网络名称	字符串	接口信息	“虚拟机网络”

Name	Type	类别	示例值
虚拟网络 ID	字符串	接口信息	“dvportgroup-1234”
虚拟交换机	字符串	接口信息	“vSwitch0”
IPv4_address	字符串	IP Config	“10.0.2.101”
ipv4_subnet_mask	字符串	IP Config	“255.255.255.0”
ipv4_gatew	字符串	IP Config	“10.0.2.1”
IPv6_address	字符串	IP Config	“fe80:: a1b: 2cff: fe3d: 4e5f”
IPV6_prefix_length	整数	IP Config	64
ipv6_gatew	字符串	IP Config	“fe80:: 1"
dns_servers	字符串	IP Config	“10.0.0.2”
dhcp_enabled	布尔值	IP Config	false
接口状态	字符串	接口信息	“向上”
vlan_id	整数	接口信息	100
is_primary	布尔值	接口信息	true

正在运行的进程 (process_metrics.csv)

正在运行的进程的快照。每小时收集一次，在 30 天内进行重复数据消除。

Name	Type	类别	示例值
服务器_ID	字符串	服务器信息	“vm-web-server-01”
process_name	字符串	流程信息	“sshd”
process_id	整数	流程信息	1234

Name	Type	类别	示例值
进程_命令_行	字符串	流程信息	“/usr/sbin/sshd-D”
进程_用户	字符串	流程信息	“根”

网络收藏

网络收集模块可帮助您发现本地数据中心内服务器之间的依赖关系。这些网络数据提供了应用程序在服务器之间的通信方式的可见性，从而加快了您的迁移计划。

该模块从所有配置的来源（包括 VMware）和导入的服务器收集服务器的网络数据。 Hyper-V它使用 WinRM 从 Windows 服务器收集数据，并使用 SSH、SNMPv2 和 SNMPv3 从 Linux 服务器收集数据。

网络数据收集

网络收集模块捕获已发现清单中服务器之间处于 “已建立” 或 TIME_WAIT 状态的 TCP IPv4 连接。只有当源和目标 IP 地址都属于发现工具发现或已导入的服务器时，连接才会出现在输出中。不包括与清单之外的 IP 地址（例如外部服务、云端点或尚未添加到发现工具中的服务器）的连接。

此设计将网络数据重点放在环境中服务器到服务器的依赖关系上，这是应用程序依赖关系映射和迁移浪潮规划所需的信息。

为每个连接收集以下数据点：

Name	Type	类别	示例值
源 IP	字符串	Connection	“192.168.1.10"
源端口	整数	Connection	49152
源进程 ID	整数	流程	1234
源进程名称	字符串	流程	"java"
目标 IP	字符串	Connection	“192.168.1.20"
目标端口	整数	Connection	5432

Name	Type	类别	示例值
目标进程 ID	整数	流程	5678
目标进程名称	字符串	流程	“postgres”
州	字符串	Connection	“已建立”
传输协议	字符串	Connection	“TCP”
IP 版本	字符串	Connection	“IPv4"
计数	整数	Connection	42

> **Tip**
>
> 要最大限度地提高网络依赖关系图的完整性，请在查看网络数据之前配置所有发现源（ VMware 和服务器 CSV 导入）并添加操作系统凭据。 Hyper-V库存中的服务器越多，网络模块可以捕获的连接就越多。

私有地址网络集合

默认情况下，网络收集模块仅捕获您发现的清单中两个端点均为服务器的连接。您可以启用私有地址收集，以捕获来自 RFC 1918 私有 IP 地址 (10.0.0) 的连接。 0/8，172.16.0。 0/12，192.168.0。 0/16) 不在您的库存中。

开始私有地址收集

1. 在收集器配置页面上，找到 “收集模块” 部分。
2. 在 “应用程序发现” 下找到 “网络连接发现”。
3. 打开 “操作” 下拉列表。
4. 选择 “开始私有地址收集”。
5. 如果模块状态为 “已启用”，则可以看到它变为 “已启用·私有地址已开启”。

要停止私有地址收集，请打开操作下拉列表并选择停止私有地址收集。以前收集的私有地址数据即使在停止后仍会保留。

私有地址连接仅出现在完整的 CSV 导出文件中（在 ZIP 文件中），而不显示在 MPA CSV 文件中。如果某个 IP 地址属于您的清单中已有的服务器，则无论此设置如何，都始终使用其发现的服务器 ID 来标识该地址。

此设置在重新启动后仍然存在。您可以随时启动或停止私有地址收集。无论当前设置如何，都会导出之前收集的私有地址数据。

SQL 服务器集合

SQL Server 收集模块从 Windows 服务器收集来自所有已配置来源的 SQL Server 信息，包括 VMware 和导入的服务器。 Hyper-V该模块使用 WinRM 远程连接到每台 Windows 服务器并运行 PowerShell 查询。它使用 WMI 命名空间、注册表和文件属性收集有关所有已安装的 SQL Server 服务（组件）的信息。

SQL Server 组件是作为在 Windows 服务器上部署 SQL Server 的一部分而安装的特定服务或功能实例。发现工具收集数据库引擎、分析服务、报告服务和集成服务。

SQL 服务器数据收集

SQL Server 收集模块收集 SQL Server 组件信息。下表描述了收集的关键数据点：

Name	Type	类别	示例值
引擎类型	字符串	组件	sql_server
是发动机组件	布尔值	组件	Y
Status	字符串	服务	正在运行，已停止，StartPending
版本	字符串	服务	2015.131.5026.0
Edition	字符串	服务	开发者版（64 位）
SQL 服务名称	字符串	服务	MsDtsServer130，mssql
SQL 服务类型	字符串	服务	SQL Server 服务、集成服务服务
实例名称	字符串	实例	MSSQLSERVER

Name	Type	类别	示例值
显示名称	字符串	服务	SQL Server (MSSQLSERVER2017)
启动模式	字符串	服务	自动、手动、已禁用
服务账户名称	字符串	服务	NT Service/MsDtsServer130
是群集的	布尔值	配置	N

> **Note**
>
> 完整格式包括所有服务类型。MPA 格式仅包括数据库引擎组件。并非所有字段都可用，具体取决于 SQL 服务类型和配置。

甲骨文数据库集合

借助 Oracle 数据库集合，您可以跨所有已配置的来源（包括 VMware）和导入的服务器来发现 Oracle 数据库实例。 Hyper-V该模块收集以下数据：

- 容器数据库 (CDB) 和可插拔数据库 (PDB) 枚举
- 版本和版本
- 已安装的选项
- 功能使用情况统计
- 组件清单（DBA_REGISTRY）
- 数据文件大小
- 拓扑标志（RAC、Data Guard 和多租户架构）

Database-connected (SQL)

配置 Oracle 凭据时，发现工具使用只读服务帐户直接连接到 Oracle 数据库。这提供了完整的 SQL-level 集合，包括 PDB 详细信息、功能使用情况和已安装的选项。所有 CSV 文件都包含完整的数据。

OS-level 后备

如果您尚未配置数据库凭据，或者连接失败，则发现工具会使用 SSH 或 WinRM 来检测 Oracle 的安装。它无需访问数据库即可发现 Oracle 主目录、侦听器、补丁、版本和版本。对于 OS-detected 主机，导出的 CDB CSV 包含实例名称、主机名、版本和版本。PDB、功能、选项和组件 CSV 文件不包含任何行。

Oracle 集合在导出 ZIP 文件中生成以下 CSV 文件。每个表都描述了每个文件收集的数据点。

CDB 数据 (oracle_data_cdbs_full.csv)

每个 CDB 实例一行。下表描述了收集的 CDB 数据点：

Name	Type	类别	示例值	来源
实例名称	字符串	身份	“兽人”	SQL，OS
主机名称	字符串	身份	“oracledb01.example.com”	SQL，OS
数据库名称	字符串	身份	“兽人”	仅限 SQL
数据库唯一名称	字符串	身份	“ORCL_PRIMARY”	仅限 SQL
DBID	整数	身份	1234567890	仅限 SQL
版本	字符串	版本	“19.0.0.0"	SQL，OS
版本完整	字符串	版本	“19.21.0.0.0"	仅限 SQL
Edition	字符串	版本	“企业版”	SQL，OS
数据库类型	字符串	配置	“单曲”	仅限 SQL
数据库角色	字符串	配置	“主要”	仅限 SQL
打开模式	字符串	配置	“读写”	仅限 SQL
日志模式	字符串	配置	“存档日志”	仅限 SQL
平台	字符串	配置	“Linux x86 64 位”	仅限 SQL
国开行旗帜	字符串	配置	“是的”	仅限 SQL
是 RAC	字符串	拓扑	“是” 或 “否”	仅限 SQL

Name	Type	类别	示例值	来源
数据防护是否处于待机状态	字符串	拓扑	“是” 或 “否”	仅限 SQL
保护模式	字符串	拓扑	“最高性能”	仅限 SQL
数据卫士代理	字符串	拓扑	“已启用”	仅限 SQL
NLS 角色集	字符串	配置	“AL32UTF8"	仅限 SQL
PDB 计数	整数	调整大小	3	仅限 SQL
闪回开启	字符串	配置	“是的”	仅限 SQL
检测路径	字符串	元数据	“第 2 阶段” 或 “第 1b 阶段”	SQL，OS

PDB 数据 (oracle_data_pdbs_full.csv)

每个 PDB（可插拔数据库）一行。下表描述了收集的 PDB 数据点：

> **Note**
>
> PDB 数据需要 Oracle 数据库凭据（SQL 连接）。 OS-level 回退不会填充此 CSV。

Name	Type	类别	示例值	来源
CDB 实例名称	字符串	身份	“兽人”	仅限 SQL
PDB 名称	字符串	身份	“APPDB1"	仅限 SQL
打开模式	字符串	Status	“读写”	仅限 SQL
生命周期状态	字符串	Status	“正常”	仅限 SQL
表空间计数	整数	调整大小	5	仅限 SQL
数据文件计数	整数	调整大小	12	仅限 SQL

Name	Type	类别	示例值	来源
总大小字节	整数	调整大小	5368709120	仅限 SQL
用户架构计数	整数	调整大小	8	仅限 SQL
数据库链接计数	整数	连接	2	仅限 SQL
已安装的组件	字符串	配置	“APEX；JVM；XML”	仅限 SQL
加密表空间计数	整数	安全性	1	仅限 SQL

功能使用情况数据 (oracle_data_features_full.csv)

来自 DBA_FEATURE_USAGE_STATISTICS 的每个功能使用情况条目各占一行。下表描述了收集的功能使用情况数据点：

> **Note**
>
> 功能使用数据需要 Oracle 数据库凭据（SQL 连接）。 OS-level 回退不会填充此 CSV。

Name	Type	类别	示例值	来源
CDB 实例名称	字符串	身份	“兽人”	仅限 SQL
Name	字符串	功能	“分区（用户）”	仅限 SQL
检测到的用法	整数	用量	42	仅限 SQL
当前使用	字符串	用量	“真的”	仅限 SQL
首次使用日期	DateTime	用量	“2024-01-15T00:00:00”	仅限 SQL
上次使用日期	DateTime	用量	“2026-06-01T00:00:00”	仅限 SQL

期权数据 (oracle_data_options_full.csv)

每个 CDB 每个 V$OPTION 条目各占一行。下表描述了收集到的已安装选项数据点：

> **Note**
>
> 选项数据需要 Oracle 数据库凭据（SQL 连接）。 OS-level 回退不会填充此 CSV。

Name	Type	类别	示例值	来源
CDB 实例名称	字符串	身份	“兽人”	仅限 SQL
选项名称	字符串	Option	“高级分析”	仅限 SQL
已安装	字符串	Option	“真的”	仅限 SQL
容器 ID	整数	Option	0	仅限 SQL

组件数据 (oracle_data_components_full.csv)

每个 DBA_REGISTRY 组件各占一行。下表描述了收集的组件数据点：

> **Note**
>
> 组件数据需要 Oracle 数据库凭据（SQL 连接）。 OS-level 回退不会填充此 CSV。

Name	Type	类别	示例值	来源
CDB 实例名称	字符串	身份	“兽人”	仅限 SQL
PDB 名称	字符串	身份	“APPDB1"	仅限 SQL
组件 ID	字符串	组件	“顶点”	仅限 SQL
组件名称	字符串	组件	“甲骨文应用程序快递”	仅限 SQL
版本	字符串	组件	“22.1.0.15.0”	仅限 SQL
Status	字符串	组件	“有效”	仅限 SQL
架构	字符串	组件	“APEX_2201000”	仅限 SQL

安全注意事项

保护发现工具 VM 的安全

发现工具 VM 安全性至关重要，因为发现工具会将所有凭据、日志和客户数据存储在发现工具 VM 上。

默认情况下，发现工具 VM 已禁用 ssh 访问权限，只能从客户端访问vCenter UI -> "Launch Web Console"。

发现工具 VM 带有用户 “发现” 的默认登录密码 “密码”。

- 我们建议您在部署后立即更新此密码。
- 如果您想在使用 v Launch Web Console Center 登录enablessh后使用命令启用 ssh，我们要求您更新密码。请注意，每次调用此命令时，都需要将其重置。

保护凭证

凭据管理的一般最佳实践

- 安全地存储凭证
- 定期轮换所有证书
- 使用密码管理器或安全保管库
- 监控凭证使用情况
- 遵循最低权限原则，只授予所需的最低必要权限

SNMP v2 凭证

- 使用复杂的非默认社区字符串
- 避免使用诸如 “公共” 或 “私有” 之类的常见字符串
- 像对待密码一样对待社区字符串

SNMP v3 凭证

- 同时启用身份验证和隐私
- 使用强身份验证协议（SHA优先于MD5）

- 使用强加密协议（AES 优先于 DES）
- 使用复杂的密码进行身份验证和隐私
- 使用唯一的用户名（避免使用常用名）

WinRM 凭证

- 避免禁用 WinRM 证书检查。
- 我们建议您创建一个所需权限最少的专用服务帐户。
- 除非需要 SQL Server 集合，否则请避免使用域管理员或本地管理员帐户。SQL Server 集合需要本地管理员访问权限，因为它会查询多个 WMI 命名空间并使用提升的命令。对于未发现 SQL Server 的操作系统指标，拥有远程管理用户、性能监控用户和 WMI 读取权限的非管理员帐户就`root\cimv2`足够了。有关每个模块the section called “所需的权限”的详细信息，请参阅。

Hyper-V 凭证

- 使用具有最低 Hyper-V 管理权限的专用服务帐户。
- 避免使用域管理员帐户。
- Hyper-V 凭据支持 NTLM（仅限 HTTPS）和 Kerberos 身份验证。
- 该发现工具存储使用 SQLCipher 进行静态加密的凭据。

甲骨文凭证

- 使用仅具有 SELECT_CATALOG_ROLE 的专用只读服务帐户。请勿使用 DBA、SYSDBA 或 SYSOPER 权限。
- 发现工具仅执行读取操作，从不向 Oracle 数据库写入数据。
- 发现工具无法访问诊断包或调整包视图，因此不需要其他 Oracle 许可。
- 定期轮换 Oracle 服务帐户密码并在发现工具中更新凭据。

凭证存储

发现工具使用数据库加密密钥对存储的静态凭证进行加密。在装有 systemd 250 或更高版本的系统上，此密钥使用 systemd-creds 进行加密。在较旧的系统上，密钥存储为受权限保护的文件。在这两种情况下，对发现工具主机具有根访问权限的攻击者都可以访问加密密钥并解密存储的凭据。限制对发现工具主机的访问权限，并将其视为环境中的特权系统。

谨慎使用 Auto-Connect 功能

在OS-level 收集过程中，发现工具使用两种机制向服务器分配凭据：自动连接和手动。 OS-level 集合包括网络、SQL Server、Oracle 数据库和操作系统指标模块。这些模块连接到来自所有来源的单个服务器，包括 VMware 虚拟机、 Hyper-V 虚拟机和导入的服务器。

手动：可以将服务器与特定凭据手动关联。在这种情况下，无论成功还是失败，发现工具都只使用该凭证。您必须手动监控该服务器的收集状态并进行调整。

Auto-connect：如果没有与服务器手动关联的凭据，则发现工具将使用该服务器的自动连接机制。这意味着：

- 在每轮收集开始时，发现工具都会获得该服务器可用的凭据列表（基于操作系统类型），并配置为“可自动连接”。
- 然后，发现工具在循环中针对服务器测试所有凭据。
  - 如果找到了有效的凭证，则服务器的收集回合将成功。发现工具会记住它，下次会先试一试。
  - 如果找不到有效的凭据，则服务器的收集回合已失败。
    - 网络模块：服务器使用退避计划，在每次失败后的 3 分钟、30 分钟、2 小时和 6 小时内开始下一轮收集（类似于指数退缩）。
    - SQL Server 集合：发现工具不会重试。它每天对每台服务器进行一次尝试。

Impacts/Risks:

只有在确定系统风险已得到缓解时，才使用自动连接：

风险 1：如果在多个错误的凭据上配置了自动连接，则在配置了锁定策略的生产环境中自动尝试使用自动连接可能会触发账户封锁。例如，数据中心可以将其虚拟机设置为在 3 次 SSH 登录尝试失败后锁定。在这种情况下，如果为 3 个错误的 SSH 凭据配置了自动连接，则会发生合法的账户封锁。如果多个系统发生封锁，则关键业务流程可能会受到影响，从而可能导致依赖系统出现级联故障。此外，安全运营中心可能会遇到来自大规模身份验证失败事件的警报风暴，从而造成误报安全事件，从而消耗资源并可能掩盖真正的攻击。

风险 2：有权访问发现工具（知道发现工具密码）的操作者可以通过配置大量测试凭据并使用自动连接来查找成功的凭据，从而在所有服务器上使用暴力破解操作系统凭据。

缓解措施：

请遵循以下准则：

- 确保发现工具密码得到妥善保护，并且只有经过授权的参与者才能知道
- 如果有封锁策略，请确保为环境输入正确的凭证。即使没有账户锁定策略，我们也建议仅配置已知的有效凭证，以确保将单个虚拟机的操作负载降至最低。
- “Auto-connect” 是一项可选功能。如果环境担心账户锁定，请不要选择它并使用手动分配凭证。

CSV 导入安全性

使用 CSV 文件导入服务器时，请考虑以下安全隐患：

- CSV 文件可能包含内部服务器的主机名或 IP 地址。将其视为敏感数据。
- `os_credential_name`和`oracle_credential_name`列通过友好名称引用预配置的凭据。CSV 不包含机密。
- All-or-nothing 验证：如果 CSV 中的任何一行无效，则整个上传都将被拒绝。这样可以防止可能造成混乱状态的部分导入。
- 导入的服务器会立即显示在清单中，并且符合收集条件。在导入之前，请确保操作系统和 Oracle 凭据的范围正确。

撤消访问权限注意事项

撤消访问权限时，删除的范围仅限于特定的来源：

- 撤消 vCenter 访问权限只会删除 vCenter 数据。它不会影响 Hyper-V 或导入的服务器数据。
- 撤消 Hyper-V 访问权限只会删除 Hyper-V 数据。它不会影响 VMware 或导入的服务器数据。
- 删除导入的服务器会将其从清单中删除，但会保留下游集合数据（网络、数据库、操作系统指标）。
- 要移除所有特定来源的库存数据，您必须单独撤销或删除每个来源。即使撤消了所有来源，下游收集数据（网络、数据库、操作系统指标）仍会保留。

问题排查

验证发现工具与 vCenter 的连接

当您遇到 VMware 模块配置错误时，请按照以下步骤验证连接：

访问发现工具 VM

- Log-in 进入发现工具 VM，在 vCenter 中打开远程控制台

- 用户名：发现
- 密码：密码

测试 vCenter 连接

1. 测试 vCenter API 访问权限：

```
curl -v --insecure -u <username>:<password> https://<vcenter-ip-or-hostname>:443/
mob
```

2. 预期成功输出：

```
[ec2-user@discoverytool ~]$ curl -v --insecure -u <user>:<password> https://vcsa/
mob > tmp.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*
 Trying 192.168.2.125:443...
* Connected to vcsa (192.168.2.125) port 443 (#0)
...
</xml>
* Connection #0 to host vcsa left intact
```

测试 SSL 证书

1. 运行以下命令：

```
openssl s_client -showcerts -servername <hostname> -connect <hostname>:443
```

2. 预期成功输出：

- 应显示 vSphere 证书详细信息
- 验证端口 4 SSL/TLS 43 上的连接

```
[ec2-user@discoverytool ~]$ openssl s_client -showcerts -servername vcsa -connect
 vcsa:443
CONNECTED(00000003)
depth=0 CN = vcsa.onpremsim.env, C = US
```

```
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = vcsa.onpremsim.env, C = US
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/CN=vcsa.onpremsim.env/C=US
   i:/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
 Engineering
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
---
Server certificate
subject=/CN=vcsa.onpremsim.env/C=US
issuer=/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
 Engineering
---
```

WinRM 疑难解答

如果您在使用 WinRM 时遇到连接问题，请按照以下步骤测试连接。这些步骤也适用于 Hyper-V 连接问题，因为发现工具使用 WinRM 与 Hyper-V 主机通信。

使用端口 5985 (HTTP) 和 5986 (HTTPS) 测试基本的 WinRM 连接。我们需要确保在端口 5986 (HTTPS) 上连接正常

```
# Check WinRM listener configuration
winrm enumerate winrm/config/listener

# Note: Replace <HOST> with the target computer's hostname or IP address. Adjust the
 username and password as needed.
# Test WinRM connection on port 5985 (HTTP)
$cred = Get-Credential
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5985

# Test WinRM connection on port 5986 (HTTPS)
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5986
```

如果上述测试失败，请尝试在禁用证书验证的情况下建立 PowerShell 会话：

```
$cred = Get-Credential
$so = New-PsSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
Enter-PSSession -ComputerName <HOST> -Credential $cred -Port 5985 -SessionOption $so
```

Kerberos 故障排除

如果您在从 Windows 服务器收集数据时遇到 Kerberos 身份验证失败，请使用以下各节来诊断和解决常见问题。

验证网络要求

在对 Kerberos 身份验证进行故障排除之前，请验证发现工具是否可以到达所需的网络端点。

验证 Kerberos 的网络要求

1. 验证域控制器的 DNS 解析。从发现工具 VM 中运行以下命令：

   ```
   nslookup dc01.example.com
   ```

   或者，您也可以使用 `dig`：

   ```
   dig dc01.example.com
   ```

   如果 DNS 解析失败，请验证发现工具 VM 是否已配置为使用可以解析您的 Active Directory 域的 DNS 服务器。检查`/etc/resolv.conf`并确认域名服务器条目是否指向您的域 DNS 服务器。
2. 通过端口 88 验证与密钥分发中心 (KDC) 的连接。运行以下命令：

   ```
   nc -zv dc01.example.com 88
   ```

   预期输出：

   ```
   Connection to dc01.example.com 88 port [tcp/kerberos] succeeded!
   ```

   如果连接失败，请确认没有防火墙规则阻止从发现工具 VM 到端口 88 上的域控制器的流量。
3. 通过 WinRM 端口验证与目标 Windows 服务器的连接。运行以下 命令：

   ```
   nc -zv <windows-server> 5985
   nc -zv <windows-server> 5986
   ```

如果连接失败，请确认目标服务器上已启用 WinRM，以及防火墙规则是否允许端口 5985 和 5986 上的入站流量。

常见的 Kerberos 问题

以下是常见的 Kerberos 问题及其解决方案。

区分大小写错误

症状：在身份验证期间，您收到 “在 Kerberos 数据库中找不到服务器” 错误。

当 Kerberos 领域名称不是大写时，通常会发生此错误。在您的文件中必须以大写形式指定 Kerberos 领域。`krb5.conf`例如，使用 `EXAMPLE.COM` 而不是 `example.com`。

账户锁定预防

该发现工具使用退避机制来防止因身份验证尝试重复失败而导致账户锁定。如果您的服务帐号被锁定，则可以通过以下方式重置收集过程：通过发现工具 Web UI 停止收集模块，然后启动收集模块，网址为`https://<discovery-tool-vm-ip>:5000`。

来自 CLI 的 kinit 失败

下表列出了常见`kinit`错误及其解决方案。

错误	原因	解决方案
找不到领域的 KDC	无法访问 KDC 主机名或 IP 地址，或者未在中`krb5.conf` 配置领域。	确认该`krb5.conf` 文件包含正确的 KDC 主机名和领域。在端口 88 上确认 DNS 解析和与 KDC 的网络连接。
预身份验证失败	服务帐户的密码不正确。	请验证密码并重试。如果该帐户已被锁定，请在重试之前在 Active Directory 中将其解锁。
在 Kerberos 数据库中找不到客户端	主体名称与 Active Directory 中的任何账户都不匹配。	验证主体名称是否与账户名称完全匹配，包括大小写。使用领域为大写的格式`username@REALM` 。

错误	原因	解决方案
无法解析 KDC 的网络地址	DNS 无法解析 KDC 主机名。	在中验证 DNS 配置/etc/resolv.conf 。确认 DNS 服务器可以解析 KDC 主机名。使用nslookup或进行测试dig。

尽管成功了 kinit，但收集失败了

如果kinit成功但数据收集仍然失败，请检查以下内容：

1. 验证用于收集的主体名称是否与期间使用的大小写kinit完全匹配。
2. 验证服务帐户在目标服务器上是否具有所需的权限。
3. 确认目标服务器上已启用 WinRM。
4. 验证用于收集的主机名是否与 Active Directory 中注册的主机名相匹配。

Kerberos 适用于某些服务器，但不适用于其他服务器

如果某些服务器的 Kerberos 身份验证成功但其他服务器失败，请调查以下方面：

如果您的服务器跨越多个 Active Directory 域，请为每个域配置单独的 Kerberos 凭据。确保您的/etc/krb5.conf文件包含所有领域的条目。每个域名都需要自己的凭证，且username@REALM主体正确。

将工作服务器上的 WinRM 配置与故障服务器上的 WinRM 配置进行比较。在每台服务器上运行以下命令：

```
winrm get winrm/config
```

测试与远程桌面的连接以找出问题。发现工具使用该格式username@DOMAIN，而远程桌面使用该格式DOMAIN\username。

确认服务帐户是故障服务器上本地管理员组的成员。在目标服务器上运行以下命令：

```
net localgroup Administrators
```

WMI 需要本地管理员权限才能访问操作系统信息。SQL Server 收集还要求服务帐户在目标服务器上具有本地管理员访问权限。

Kerberos 配置清单

在开始数据收集之前，请使用以下清单验证您的 Kerberos 配置。

- 该`krb5.conf`文件存在于发现工具 VM 上。
- 中的领域名称是大写的。`krb5.conf`
- `kinit`使用服务帐号成功运行，不会出现错误。
- 跑步`klist`会显示一张有效的、未过期的门票。
- 主体名称与 Active Directory 账户名完全匹配。
- DNS 解析适用于 KDC 主机名。
- 已确认通过端口 88 与 KDC 的网络连接。
- 通过端口 5985 和 5986 与目标 Windows 服务器的网络连接已得到确认。
- (Multi-domain) 每个 Active Directory 域都有在发现工具中配置的自己的凭据，`[realms]`并且`krb5.conf`包含所有域名和`[domain_realm]`条目。

甲骨文数据库故障排除

要诊断 Oracle 数据库收集问题，例如数据丢失或错误，请检查以下内容。

连接被拒绝或超时

症状：Oracle 收集状态显示服务器的连接错误。

要对此问题进行故障排除，请检查以下步骤：

- 验证 Oracle 监听器是否正在目标主机上运行：`lsnrctl status`
- 验证通过端口 1521（或您的自定义端口）从发现工具到 Oracle 主机的网络连接：`nc -zv <oracle-host> 1521`
- 确认防火墙规则允许 Oracle 侦听器端口上的入站连接。
- 通过在 Oracle 主机`lsnrctl services`上运行来验证服务名称。如果服务名称不正确，Oracle 监听器会拒绝连接。

身份验证失败 (ORA-01017)

症状：由于用户名或密码无效错误，收集失败。

要对此问题进行故障排除，请检查以下步骤：

- 验证 Oracle 服务帐户是否存在且未被锁定：`SELECT account_status FROM dba_users WHERE username = 'DISCOVERY_USER';`
- 通过手动连接来验证密码是否正确：`sqlplus discovery_user/<password>@<host>:1521/<service_name>`
- 如果账户已被锁定，请将其解锁：`ALTER USER discovery_user ACCOUNT UNLOCK;`

权限不足 (ORA-01031)

症状：连接成功但收集返回的数据不完整。

要对此问题进行故障排除，请检查以下步骤：

- 确认已授予 SELECT_CATALOG_ROLE：`SELECT * FROM dba_role_privs WHERE grantee = 'DISCOVERY_USER';`
- 如果缺少所需角色，则授予该角色：`GRANT SELECT_CATALOG_ROLE TO discovery_user;`

手动凭证显示错误但自动连接起作用

当您将凭据手动固定到服务器时，如果连接失败，发现工具不会回退。验证您在凭据上配置的端口和服务名称是否与该特定服务器上的 Oracle 监听器相匹配。如果服务器具有非标准端口或服务名称，请相应地更新凭据配置。

OS-level 回退未检测到 Oracle

如果未配置数据库凭据，并且 OS-level 回退操作未检测到 Oracle：

- 验证 SSH 或 WinRM 操作系统凭据是否已配置且适用于服务器（检查操作系统指标收集状态）。
- 对于 Linux 主机，请验证是否`/etc/oratab`存在或 Oracle 进程监视器 (pmon) 进程是否正在运行。
- 对于 Windows 主机，请验证 Oracle 注册表项是否存在`HKLM\SOFTWARE\Oracle`或`oracle.exe`进程正在运行。

SNMP 故障排除

访问发现工具 VM

- Log-in 进入发现工具 VM，在 vCenter 中打开远程控制台

- 用户名：发现
- 密码：密码

安装 SNMP 工具（如果需要）

- `sudo yum install net-snmp-utils -y`

测试与 Linux 服务器的 SNMP 连接

1. `snmptable -v 2c -c <COMMUNITY_STRING> <REMOTE_SERVER_IP> .1.3.6.1.2.1.6.13.1`
2. 示例：

```
#SNMPv2c:
snmptable -v 2c -c public 192.168.1.100 .1.3.6.1.2.1.6.13.1

#SNMPv3 (with authentication):
snmptable -v 3 -u <username> -a MD5 -A <auth_password>
 192.168.1.100 .1.3.6.1.2.1.6.13.1

#SNMPv3 (with privacy):
snmptable -v 3 -u <username> -a MD5 -A <auth_password> -x DES -X <priv_password>
 192.168.1.100 .1.3.6.1.2.1.6.13.1
```

网络收集错误

需要终端才能读取密码

错误：

```
ss command failed on <host>: sudo: a terminal is required to read the password; either
 use the -S option to read from standard input or configure an askpass helper sudo: a
 password is required
```

ss 命令提示输入用户密码。配置的 ssh 用户必须在 sudoers 组中，并且必须为该命令配置无密码 sudo。 ss/netstat 要配置无密码 sudo，请执行以下操作：

1. 创建一个新的 sudoers 文件：

```
sudo vi -f /etc/sudoers.d/<username>
```

2. 添加以下行：

```
<username> ALL=(ALL) NOPASSWD: /usr/sbin/ss, /usr/bin/netstat
```

3. 进行此更改后，运行`sudo ss -tnap`并`sudo netstat -tnap`应在不提示输入密码的情况下执行

网络集合在没有 sudo 的情况下运行

如果您在 “已发现库存” 页面上看到以下警告：

```
Network collection ran without sudo. Process-level connection data may be missing.
```

此警告表明 SSH 用户帐户在目标服务器上没有 sudo 访问权限。如果没有 sudo，发现工具仍然可以收集网络连接数据，但它无法确定哪个进程拥有每个连接。要收集完整的进程级连接数据，请确保 SSH 用户在目标服务器上具有 sudo 访问权限。

操作系统指标收集错误

缺少 Linux 服务器的服务器 UUID

如果发现工具无法收集 Linux 服务器的服务器 UUID（显示为空或缺失），请验证为这些服务器配置的 SSH 凭据是否具有 sudo 权限。该工具用于读`dmidecode`取服务器 UUID。如果未安装，`dmidecode`则该工具将恢复读取`/sys/class/dmi/id/product_uuid`，这也需要 sudo 访问权限。如果没有 sudo，则两种方法都无法检索 UUID。

解决方案：确保提供给发现工具的 SSH 用户帐户在目标 Linux 服务器上具有 sudo 访问权限。

已发现清单中的访问问题

如果您看到服务器收集状态的消息，例如缺少凭据或访问被拒绝：

1. 在搜索到的服务器列表中选择服务器。
2. 选择管理访问凭证您可以选择：

   a. 从 “选择凭据” 下拉列表中选择备用凭据。

b. 选择 “使用新凭据并提供新凭据”。

3. 保存 。

保存更改后，发现工具会重试连接。

SSH 密钥认证疑难解答

通过发现工具测试 SSH 密钥连接

如果 SSH 密钥身份验证失败，请验证发现工具与目标服务器的连接：

1. 登录发现工具（通过 vSphere 控制台或 SSH 登录到 Linux 主机）。
2. 使用您的私钥测试 SSH 连接：

```
ssh -i /path/to/private_key -o StrictHostKeyChecking=no <username>@<target_ip>
```

3. 如果连接成功，则问题在于如何将密钥上传到发现工具。 Re-upload 密钥并验证用户名是否匹配。
4. 如果连接失败，请查看下表中的错误消息。

错误消息	原因	解决方案
`Permission denied (publickey)`	公钥不在目标服务器`authorized_keys` 的文件中，或者用户名错误。	在目标服务器`~/.ssh/authorized_keys` 上为正确的用户添加公钥。验证文件权限:`chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys` .
`Connection timed out after 20s`	发现工具无法访问端口 22。	确认发现工具和目标服务器之间的端口 22 已打开。检查防火墙和安全组。
`Connection refused`	目标服务器上未运行 SSH 服务。	启动 SSH 服务：`sudo systemctl start sshd`。
`Invalid SSH key for credential 'name'`	不支持密钥格式，密钥数据已损坏，或者密码缺失或不正确。	验证密钥格式是否为 PEM、OpenSSH 或 PKCS #8 格式的 RSA、ECDSA 或 Ed25519。如果密钥已加密，请确保密码正确。

Linux 安装程序故障

端口 5000 已在使用中

症状：安装后发现工具服务无法启动。

解决方案：使用端口 5000 识别并停止进程：

```
sudo ss -tlnp | grep :5000
```

停止冲突进程，然后重新启动发现工具：

```
sudo ./AWS-Transform-discovery-tool.sh start
```

常见错误消息

下表描述了常见的错误消息及其解释：

Message	位置	说明
密码已创建	创建密码页面	两个用户同时创建密码时的竞争条件；刷新
导出失败	库存页面	重试或发送日志
按需收集已在进行中	库存页面	两个用户同时开始手动收集时的竞争条件；当前手动收集完成后重试
`Command timed out after 60s`	服务器集合状态	目标服务器上的命令未在 60 秒内完成。这可能发生在负载较重的服务器上。重试收集或调查目标服务器的负载。
一个或多个凭证包含未知的 UUID	操作系统访问页面	两个用户同时编辑操作系统凭据时的竞争条件；重试
密码无效	Sign-in 页面	登录密码不正确；请联系管理员或联系我们
您的会话已过期。请重新登录。	Sign-in 页面	会话已超时，需要重新登录

Message	位置	说明
发生了内部错误	各种页面	重试或发送日志

发行说明

本节按发布日期介绍 AWS Transform 发现工具的功能、改进和错误修复。

日期	版本	发行说明
2026 年 6 月 30 日	1.0.1646	新特征 • 添加了 Oracle 数据库发现。该工具收集 CDB 和 PDB 拓扑、版本、版本、已安装的选项、功能使用情况和组件清单。该发现工具支持直接 SQL 连接（使用 SELECT_CATALOG_ROLE）和通过 SSH 或 WinRM 进行 OS-level 回退检测。 • 增加了对跨不同活动目录域的多个 Kerberos 凭据的支持。每个凭据都独立进行身份验证，因此可以从多个域中的 Windows 服务器进行收集，而不会发生身份验证冲突。 改进 • 改进了旧版主机的操作系统指标收集。为无法使用现代命令的旧操作系统（RHEL 5、SLES 11、Windows Server 2008 R2）添加了后备数据收集。存储、性能和网络接口数据现在是使用备用系统接口收集的。 错误修复 • 修复了通过发现的服务器的 Kerberos 身份验证失败问题。Hyper-V发现工具现在可以正确解析 Hyper-V 客户机元数据中的服务器主机名 (FQDN)，这是 Kerberos SPN 匹配所必需的。
2026 年 5 月 14 日	1.0.1363	新特征

日期	版本	发行说明
		• 添加了 Linux 安装程序，用于在支持的 Linux 发行版（亚马逊 Linux 2、亚马逊 Linux 2023、RHEL 8—9、Rocky Linux 8—9、9、Ubuntu 20.04—24.04、 AlmaLinux Debian 10—12、SLES 15 SP5）上部署发现工具。 • 增加了对配置多台 VMware vCenter 服务器的支持，使其能够在 vCenter 之间自动删除虚拟机重复数据。 • 添加了 SSH 私钥身份验证作为用户名和密码的替代方案，便于访问 Linux 操作系统。支持的密钥格式包括 RSA、ECDSA、Ed25519、OpenSSH 和 PKCS #8。 • 添加了私有地址网络集合，用于捕获与您发现的清单中未包含的 RFC 1918 私有 IP 地址的连接。 • 添加了导出选项，用于选择自定义日期范围并选择要包含在导出中的数据模块。 改进 • 通过错开收集器计划，提高了定期收集的可靠性。 • 通过 SSH 命令批处理提高了操作系统指标收集性能。 • 现在，凭据更改会立即重试以前出现故障的服务器。 • 现在，当某些命令返回空结果时，操作系统指标收集会报告部分状态。 • 改善了控制面板中对 vCenter 连接问题的错误可见性。
2026 年 4 月 7 日	1.0.1074	新特征 • 增加了对 Microsoft Hyper-V 发现的支持，包括通过故障转移群集重复数据删除功能自动发现来自 Hyper-V 主机的虚拟机。 • 增加了对通过 CSV 文件上传进行服务器导入的支持。 • 添加了包含六个独立模块的操作系统指标集合：服务器性能、存储性能、服务器配置、存储配置、网络接口和运行进程。 • 添加了使用 VHD 映像文件的 Hyper-V 部署选项。 • 通过移除 EC2-specific 服务并阻止对实例元数据终端节点的访问，增强了本地安全性。

日期	版本	发行说明
2026 年 3 月 26 日	1.0.1014	错误修复和改进 • 将 Kerberos 域名大小写验证从后端移至前端。 • 从切换 Python-kerberos 到 Python-pykerberos 并将基于文件的缓存设为默认缓存。 • 修复了不区分大小写的批量编辑服务器 ID 验证。 • 修复了导出 ZIP 文件名（现已修复`discovery_tool_export.zip`）。 • 修复了服务运行检查，并添加了系统凭据的调试日志。 • 添加了用于构建构件的网络配置脚本。
2025 年 12 月 16 日	1.0.718	新功能和改进 • 添加了 SMBIOS UUID 支持，以防止下游服务中的虚拟机重复。 • 引入了 Min/Max/Avg 跟踪和扩展存储指标，以改善资源监控。 • 添加了 API 验证改进。 • 添加了带有上下文指导的帮助面板功能。 • 在整个界面中将术语从 “收集器” 更新为 “工具”。
2025 年 10 月 31 日	1.0.0	初始版本 AWS Transform 发现工具的首次启动。此版本包括： • 离线收集（不依赖 AWS 账户或 Application Discovery Service）。 • VMware 发现和监控。 • SQL 服务器数据库发现。 • Server-to-server 通过 SSH、WMI 和 SNMP 收集通信。

AWS 转换连接器

AWS Transform 连接器使您能够跨账户安全地访问资源，以进行迁移和现代化工作流程。这使您能够跨账户访问和管理资源，同时保持安全控制和权限。连接器代表您的 AWS Transform-enabled 源账户与 AWS 目标账户或第三方系统中的外部资源之间的连接。

连接器需要来自源连接器的访问请求以及目标账户所有者的批准。您在设置源连接器时会发出此请求。同样，您可能会收到批准目标连接器以允许其他账户访问您的账户的请求。

- 创建连接器：在 AWS Transform-enabled 源账户中创建连接器，指定目标账户和所需权限
- 权限设置： AWS 转换需要目标账户中的特定 IAM 角色和权限才能执行迁移操作，包括：
  - 使用管理迁移数据 AWS KMS
  - 进行跨区域 API 调用
  - 在 VMware 服务器上安装复制代理
  - 创建网络基础架构（VPC、子网、路由）
  - 启动 Amazon EC2 实例并部署 CloudFormation 堆栈
  - 通过 Migration Hub 执行迁移工作流程
- 批准流程：您必须先批准目标连接器请求，T AWS ransform 才能访问您的资源。
- A@@ ctive Connection：一旦你批准了连接器，它就会使 AWS 转换作业能够安全地访问和管理目标账户中的资源。

代理操作的用户可追溯性

默认情况下，在 Transfor AWS m 服务标识下 AWS CloudTrail 记录代理对您的 AWS 资源的操作。用户可追溯性将这些操作归因于发起任务或与之交互的特定 AWS IAM Identity Center 用户，从而实现个人用户级别的安全审计和事件调查。

> **Note**
>
> 只有 IAM 身份中心 (IDC) 用户支持用户可追溯性。

要启用用户可追溯性，请在您的 Trans AWS form 配置文件设置中启用后台会话。启用后，T AWS ransform 会在您与任务交互时自动创建 IAM Identity Center 后台会话，并使用该会话为连接器操作生

成身份增强型 IAM 角色会话。这些会话将您的用户身份嵌入下游 AWS 服务调用和 AWS CloudTrail 事件中。禁用后台会话后，T AWS ransform 会回退到没有用户身份上下文的标准假设角色会话。

新的连接器会自动配置为支持用户可追溯性。对于现有的连接器，您必须手动`sts:SetContext`添加到连接器角色的信任策略中：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": ["transform.amazonaws.com"] },
      "Action": ["sts:AssumeRole", "sts:SetContext"],
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "your-account-id" }
      }
    }
  ]
}
```

您可以从作业页面的后台会话选项卡中查看和撤消活动的后台会话。撤消会话会立即使该会话以及从该会话派生的任何连接器会话失效。

有关更多信息，请参阅《IAM Identity Center 用户指南》AWS 中的可信身份传播概述。

管理连接器

在 “连接器” 页面上，您可以看到：

- “源连接器” 选项卡：列出您为连接其他账户而创建的所有连接器，显示目标账户和连接器状态
- “目标连接器” 选项卡：显示来自其他想要访问您的资源并需要您批准或拒绝的账户的传入连接器请求

AWS Transform 需要确认关键操作（例如批准、拒绝或删除连接器），以避免意外更改可能会中断您的活动迁移工作流程。

创建连接器

1. 导航到 “源连接器” 选项卡。
2. 指定目标账户和资源类型。
3. 配置所需的权限和访问范围。

设置 权限

1. 选择创建具有所需权限的新 IAM 角色，或者
2. 选择您之前为连接器创建的现有角色。
3. 确保该角色拥有 AWS 转换操作的所有必要权限。

管理传入的请求

1. 在 “目标连接器” 选项卡中查看连接器请求。
2. 批准允许跨账户访问的合法请求。
3. 拒绝未经授权或不必要的连接尝试。

管理您的连接器

1. 监控您的活动连接器的安全性和合规性。
2. 当您不再需要连接器时，请将其删除。请注意，这将导致使用连接器运行的作业失败。
3. 随着需求的变化，更新权限。

迁移（包括 VMware）

AWS Transform 可以使用生成式 AI（包括 VMware）和其他来源，帮助您将虚拟和裸机服务器环境迁移到 Amazon EC2。 Hyper-V本章概述了 T AWS ransform 迁移功能和迁移过程的工作流程。

功能和关键特性

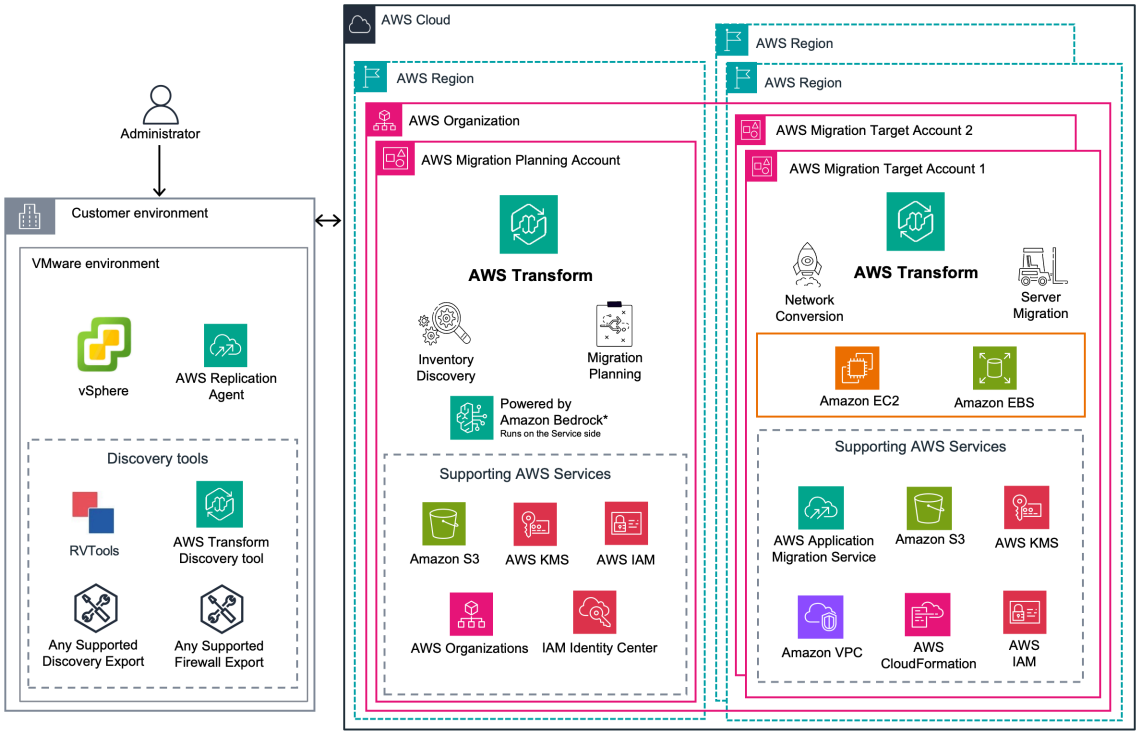
AWS Transform 为将服务器环境迁移到提供了以下功能和关键功能 AWS。

- 多种发现选项：
  - 使用来自的收集器协助发现您的 VMware 环境 AWS Application Discovery Service。
  - 使用开源 vCent er 导出工具（V Mware 环境）。
  - 导入独立收集的发现数据（任何源环境）。
- AI-driven 将您的源网络配置转换为 Amazon VPC 网络架构。
- AI-driven 制定迁移计划，包括应用程序分组和建议的迁移浪潮。
- 重新托管您的服务器，使其在 Amazon EC2 上以原生方式运行。
- 本地化的 Web 应用程序界面，允许您使用首选语言使用 Trans AWS form 进行迁移。有关更多信息，请参阅 语言设置。

AWS Transform 支持迁移支持的操作系统的 Windows 和 Linux 服务器。有关支持的操作系统的完整列表，请参阅AWS Transform MGN 用户指南中的支持的操作系统。

AWS 转变迁移架构

此图表显示了 Trans AWS form 迁移架构的概述。



迁移工作

要使用 Transfor AWS m 进行迁移，首先需要一个工作空间，这是一个逻辑容器，可以在其中创建一个或多个转换作业。本主题中的各节介绍如何获取工作空间以及如何在其中创建和启动迁移作业。

获取工作空间

有关获取工作空间的信息，请参阅入门。

您使用的工作空间决定了可以在 AWS 区域 何处创建转换作业。那就是 AWS 区域 你的工作所在地。您的发现数据和 AWS 转换建议也将保存在此中 AWS 区域。要在其他工作空间中创建工作空间和作业 AWS 区域，请让您的管理员为您创建不同的工作空间。有关支持的信息 AWS 区域，请参阅支持的区域：。

尽管您可以创建任务、存储发现数据和建议的 AWS 区域 位置由您的 Trans AWS form 管理员决定，但您可以指定不同的位置 AWS 区域 作为迁移目标。换句话说，您可以同时运行发现并接收 Trans AWS form 建议 AWS 区域，然后在不同的环境中创建目标环境 AWS 区域。如果你这样做，你就会将数据传输过来 AWS 区域。有关更多信息，请参阅 the section called “Connect 目标 AWS 账户 s 和区域”。

Job 类型

AWS Transform 提供了以下类型的迁移任务，您可以根据自己的迁移需求从中进行选择。除了这些预设选项外，您还可以随时在作业中动态添加或删除任何步骤，以自定义迁移工作流程。

End-to-end 迁移

1. 执行发现
2. 制定迁移计划
3. Connect 目标账户
4. 建造着陆区
5. 迁移网络
6. 迁移服务器

发现和迁移规划

1. 执行发现
2. 制定迁移计划

网络迁移

1. Connect 目标账户
2. 迁移网络

登录区

1. Connect 目标账户
2. 建造着陆区

着陆区、网络和服务器迁移

1. Connect 目标账户
2. 建造着陆区
3. 迁移网络

4. 迁移服务器

迁移规划和服务器迁移

包括发现、波浪计划和重新托管。

1. 执行发现
2. 制定迁移计划
3. Connect 目标账户
4. 迁移服务器

创建和启动作业

迁移项目的第一步是创建 AWS 转换作业。对于迁移项目，您可以根据自己的目标选择不同的任务类型。以下过程介绍如何创建和启动任何类型的新迁移作业。有关不同作业类型的信息，请参阅the section called “Job 类型”。

创建并启动新的迁移作业

1. 在工作空间登录页面上，选择创建作业。
2. 选择迁移选项，然后指定要创建的迁移任务的类型。有关每种迁移任务类型中包含的步骤的信息，请参阅the section called “Job 类型”。
3. 回答完所有聊天问题后，选择创建工作。

下载工作空间摘要报告

在迁移过程中，您可以随时生成可下载的 PDF 格式的工作空间摘要报告。该报告提供了工作空间中所有迁移任务的综合视图，包括作业状态和当前工作流程步骤、用户操作和批准、波浪规划细节、网络迁移拓扑、着陆区配置、重新托管进度、容器化决策以及生成的关键工件。要生成报告，请向聊天中的代理询问工作空间摘要，例如，“向我提供所有作业迁移进度的工作空间摘要。” 代理编译所有作业的数据，并将PDF作为可下载文件直接在聊天中交付。您可以使用此报告来跟踪整体迁移进度或与利益相关者共享状态。

限制

AWS 变换有以下限制：

- 如果您停止正在运行的迁移作业，然后要求代理重新启动该作业，则该作业将从头开始重新启动，并且您将失去在作业中取得的任何进展。但是，在重新启动任务之前在作业中创建的工件仍然可用。
- 您可以为 AWS 区域 每个迁移任务指定一个目标。要将应用程序迁移到不同的目标区域，请创建多个迁移任务。
- Multi-account 迁移-仅限单个区域-您可以在单个区域内迁移到多个账户 AWS 区域。对于多区域迁移，您必须为每个目标区域创建单独的项目。
- Multi-account 迁移 — 每波一个账户 — 每个迁移浪潮只能针对一个账户。需要不同目标账户的应用程序必须分批放置。
- Multi-account 迁移 — 需要 AWS 组织 — 所有目标客户都必须是 AWS 组织的一部分。

发现源数据

要发现和收集本地数据，您可以使用AWS 转换发现工具、 AWS迁移评估器收集器，或者上传来自 RVTools 和 ModelizeIt 的导出，以及由 Cloudamize 等工具生成的 AWS迁移组合评估 (MPA) 格式导出。 AWS Transform 可以 AWS 将转换发现工具导出为 ZIP 文件格式的 CSV 和 JSON 文件，rvTools 导出为包含 CSV 文件的 Excel 文件或 ZIP 文件，将 ModelizeIt CSV 导出为 ZIP 文件。对于每个数据源，Tr AWS ansform 分别接受主服务器文件。但是，诸如连接之类的补充文件只有在包含服务器文件的 ZIP 文件或服务器工作表的 Excel 文件中包含在 Excel 文件中时，才会对其进行处理。

我们建议您在上传之前上传最详细的数据，并查看您的导出文件，以确保数据的完整性和准确性。验证上传文件中是否包含所有必需的文件，并确认数据反映了您当前的环境状态。此初步审查有助于最大限度地减少重新上传的需求，并确保 Trans AWS form 可以更准确地捕获您的本地环境并更好地支持迁移规划，包括应用程序分组和波浪规划。您还可以在获得更好的数据时以增量方式添加数据。

AWS Transform 会自动检测文件格式和结构，解析和提取结构化实体记录，删除多个文件中的重复项，验证数据质量并报告问题，然后为下游迁移计划准备一份摘要。

共享并确认本地数据后，您可以通过在作业计划中展开发现本地数据并选择库存准备情况摘要来查看发现数据。您还可以询问有关您上传的数据的问题，以验证 T AWS ransform 是否正确摄取了所有内容，或者识别和纠正数据处理中的任何错误。例如，您可以询问操作系统和版本。如果您需要更正错误，可以从您使用的发现工具重新上传库存数据，Trans AWS form 将自动处理、删除重复数据并合并更新的记录。如果您不想再使用之前上传的库存数据，也可以移除该文件。

制定迁移计划

T AWS ransform for VMware 中的迁移规划工作步骤是一种基于聊天的协作体验，用于规划大型迁移。 AWS Transform 代理采用 AWS 规范性指导来指导客户从分析本地数据到最终确定迁移浪潮计划。

Discover 本地数据作业成功完成后，T AWS ransform 使用发现数据将应用程序分组为迁移浪潮。AWS Transform 将指导您完成分析和确定服务器范围、将其分组为应用程序、生成移动组和构建迁移浪潮的步骤。在分析本地环境时，您可以提问以更好地了解 T AWS ransform 是如何分析已安装软件的，例如服务器依赖关系和网络架构。

AWS Transform 支持在应用程序组和波浪中调整范围。您可以随时重新上传发现数据，Trans AWS form 将自动处理、删除重复数据，并将新记录与现有数据合并。当检测到更改（例如新发现的依赖项或基础架构的添加）时，Trans AWS form 将标记受影响的依赖组，并为波浪计划调整提供建议。迁移规划还可以利用非结构化文本数据来丰富规划流程。

迁移规划分为四个阶段：

- 在 Sco pe and analyze 中，您可以查看发现数据，询问有关您的软件和网络环境的问题，并确定迁移范围内的资源。
- 在群组应用程序中，您可以提供有关主机名分析、网络依赖关系和业务规则等业务和技术规则的组合，以便迁移计划可以将您的基础架构分组为应用程序。如果您已经有了应用程序清单，则迁移计划可以改用该清单。
- 在 G enerate move groups 中，您可以为迁移计划提供技术和业务需求，以便它可以确定哪些应用程序必须一起移动。技术依赖关系包括数据库、消息队列或多个应用程序之间共享的其他资源。业务和运营依赖关系包括业务关键程度、RPO 和 RTO、数据中心位置以及应用程序所有者。
- 最后，在 B uild waves 中，您可以为迁移计划提供有关时间表和优先事项的背景信息，以便它可以制定可以迁移的波浪计划。您可以根据优先级分数、移动组规模、用户数量和应用程序复杂性等因素选择要包含在波浪中的移动组。

迁移规划术语：

- 迁移波是一起迁移的逻辑组。迁移波由一个或多个移动组组成。
- 移动组是一组相互依赖的应用程序，必须一起移动。它们可能有技术依赖关系，例如共享数据库，也可能有业务依赖关系，例如支持共享业务功能。
- 依赖关系是系统之间的关系。依赖关系有几种类型，包括：

- 关键依赖关系或硬依赖关系，即没有依赖关系系统就无法运行。这方面的常见示例是依赖于数据库、其他应用程序或服务的应用程序。
- 软依赖关系，它们对系统的运行并不重要。这方面的常见示例包括可以独立迁移的延迟不敏感依赖项。
- Non-technical 依赖关系包括业务、组织、运营和合规依赖关系。这些依赖关系与您的组织及其优先级有关。这方面的例子包括共享业务职能和组织所有权。

工作流

迁移规划是一个交互式的迭代工作流程。您可以随时返回并对之前的步骤进行更改。典型的迁移规划工作流程是：

1. 迁移规划从汇总可用的发现数据开始。查看可用数据并随时返回发现步骤以提供其他数据。
2. 在范围界定和分析步骤中，您可以询问有关本地环境的问题，以验证您收集的数据。示例问题包括：
   a. 按操作系统列出我的服务器
   b. 总结一下我的本地网络拓扑
   c. 列出我的环境中运行的最常用技术。
3. 在分析您的环境时，如果您发现不应该在迁移范围内的服务器，则可以让 Trans AWS form 排除这些资源。这种情况的示例包括：
   a. 移除所有主机名中包含旧版的服务器
   b. 移除 10.0.2 版本中的所有服务器。 0/24 子网
   c. 移除所有运行 2022 年之前版本的 Windows 的服务器
4. 充分探索环境并确定迁移范围后，您可以让 Trans AWS form 进入下一个迁移规划步骤。
5. 下一步是应用程序分组。如果您已经将服务器映射到应用程序，则可以让 Trans AWS form 使用该映射并跳过此步骤。如果您没有预定义应用程序，则可以提供定义应用程序的技术和业务逻辑。AWS Transform 将指导您完成应用程序分组过程，并建议您可以提供的数据点，以便有效地将服务器分组为应用程序。您可以提供的有关本地应用程序的信息越多，Transform 就越 AWS 能有效地将您的服务器分组为应用程序。提供足够信息后，即可指示 Trans AWS form 执行应用程序分组。
6. 执行应用程序分组后，请查看应用程序组。您可以指示 Tr AWS ansform 进行任何必要的更改，例如：
   a. 将服务器示例服务器移至应用程序 5
   b. 重命名 application-5 “HR 应用程序测试环境”

c. 从 IIS 开发群中移除所有 Linux 服务器

7. 对应用程序进行分组后，指示 Tr AWS ansform 进入下一步
8. 下一步是移动分组。在移动分组步骤中，您可以确定必须一起移动的应用程序。提供有关您的技术和非技术依赖关系的背景信息。 AWS Transform 将指导您完成整个过程，并建议您可以提供的数据点来对应用程序进行分组。在此阶段需要考虑几个因素，包括：
   a. 移动组的目标大小应该是多少？
   b. 您是想为每个应用程序组合环境（例如开发、测试和生产），还是要将它们拆分？
   c. 您想如何考虑网络依赖关系？ 是否所有依赖关系都很重要，还是某些依赖关系可以被视为软依赖关系并在移动组之间进行拆分？
9. 提供移动分组规则后，请指示 Trans AWS form 执行移动分组策略。然后，您可以查看和修改您的移动组。查看移动组后，您可以指示 Trans AWS form 进入最终的迁移计划步骤。
10. 波浪规划是迁移规划的最后一步。在此步骤中，您将移动组分为迁移浪潮，并对这些浪潮进行优先排序。在波浪计划步骤中，T AWS ransform将指导您提供所需的业务优先级，将您的移动组分为波次，然后确定这些波浪的优先级。波浪规划中的注意事项包括：
    a. 每个搬迁组的业务重要性
    b. 每个移动组的迁移时间表和时间表
    c. 与每个移动组相关的风险
    d. 每波要迁移的服务器数量
11. 在为如何分组波浪提供了足够的指导后，请指示 Trans AWS form 执行波浪规划。然后，您可以查看您的波浪并对其进行修改。
12. 一旦您最终确定了波浪计划，就可以完成迁移计划并开始执行。您可以随时返回迁移规划，以完善和迭代您的计划。
13. 对于每个浪潮，您可以分配迁移策略：重新托管（将服务器迁移到 Amazon EC2）和容器化（将源代码容器化并部署到亚马逊弹性容器服务或亚马逊 Elastic Kubernetes Service）。当您为某波分配容器化策略时，Trans AWS form 会在迁移执行期间为该波浪运行源代码容器化工作流程。有关更多信息，请参阅 源代码容器化。要在分配策略之前获取 7R 框架中的 AWS推荐策略，请参阅。the section called “7R 建议”

迁移策略 (7R) 建议

在迁移规划期间，T AWS ransform 可以分析您发现的库存，并为每台服务器和应用程序推荐迁移策略（行业标准的 7R 之一）。每项建议都包括建议的 AWS 目标服务、置信度分数及其背后的原因。这为你的波浪计划提供了一个可以防御的起点，也为你提供了原本可能会错过的现代化机会。

这七个策略是重新托管、重构平台、重构、回购、停用、保留和搬迁。 AWS 转换数据中的读取信号（例如操作系统、利用率和工作负载类型），以提出可解释的建议。例如，它可以建议停用闲置或使用寿命终止的服务器，将 SQL Server 或开源数据库迁移到 Amazon RDS，将电子邮件和协作工作负载转移到 Microsoft 365，保留专门的传统系统，并将剩余的工作负载重新托管在 Amazon EC2 上。建议从单个服务器汇总到应用程序以及整个产品组合，并按策略和波级摘要提供重要性视图。

要生成迁移策略 (7R) 报告，请执行以下操作：

1. 完成 “发现本地数据” 步骤，将服务器分组为应用程序。两者都是必需的，这样 T AWS ransform 才能提供每台服务器和每个应用程序的建议。
2. 在迁移计划聊天中，向 Tr AWS ansform 索要迁移策略 (7R) 报告，例如，生成报告。 R-strategy 应用程序分组完成后，Transfor AWS m 还会为您生成报告。
3. AWS Transform 会分析您的库存，应用 7R 框架，然后生成报告。您可以提供诸如组织名称和任何筛选条件之类的详细信息，以确定分析范围。
4. 查看建议。要调整建议，请在聊天中告诉 T AWS ransform — 更改单个服务器或应用程序，或者批量应用更改（例如，按操作系统、环境、波浪或优先级）。 AWS Transform 会根据您的更改更新报告。

默认情况下，Trans AWS form 会生成一个交互式 HTML 仪表板，你可以对其进行筛选和浏览。根据要求，您还可以生成 PDF 文档与利益相关者共享，或者生成 Microsoft PowerPoint (PPTX) 幻灯片来演示；PDF 和 PowerPoint 输出是同一分析的时间点快照。该报告包括针对每台服务器和应用程序的推荐策略和 AWS 目标服务、信心分数和推理、重点介绍的现代化机会、按策略划分的关键性视图、波浪级摘要和风险标志。

本报告中建议的策略是对您在波浪计划期间分配的每波策略的补充。有关源代码容器化的信息，请参阅。源代码容器化

绘制图表和报告

在迁移计划期间，Transform 会将您发现的库存和计划结果 AWS 转换为可视化图表和分析报告。您可以在规划聊天中以对话方式生成它们，例如，“给我看网络拓扑图” 或 “生成风险报告”。 AWS Transform 使用您已经提供的数据构建它们，无需进行任何设置。

图表是交互式的，可让您直观地探索您的环境。可用的图表包括：

- 网络拓扑 — 服务器及其网络关系的交互式地图，旨在扩展到包含数千个节点的大型环境。
- 应用程序依赖关系 — 根据您观察到的网络连接得出的定向应用程序到应用程序的关系。

- Wave Gantt 图 — 迁移浪潮的时间表视图，显示时间表、依赖关系、里程碑和进度（在波浪计划后可用）。
- 常规图表-饼图、条形图、直方图、树状图和摘要表，这些维度与您选择的数据维度对比。

报告对您的迁移数据提供叙述性分析和建议。可用报告包括：

- 风险评估 — 根据每个应用程序、每波和整个产品组合的摘要，根据技术复杂性、依赖性风险、迁移准备情况和运营风险对每个应用程序进行评分。
- 迁移策略 (7R) — Per-server 以及每个应用程序的策略建议。有关更多信息，请参阅 the section called “7R 建议”。
- 一般报告和自定义报告 — 针对请求的分析报告，例如高管准备情况摘要、成本与风险的权衡以及集装箱化候选人评估。

有些产出取决于您的计划进度。例如，应用程序依赖关系图使用您的网络连接数据。波浪规划完成后，即可获得波浪甘特图和波级报告摘要。如果缺少先决条件，T AWS ransform 会告诉你需要什么，然后可以先运行所需的步骤。

AWS Transform 以交互式 HTML 形式提供图表，您可以对其进行筛选和浏览。默认情况下，Tr AWS ansform 会将报表作为自包含的 HTML 文件提供。根据要求，T AWS ransform 还可以生成 PDF 文档与利益相关者共享，或者生成微软 PowerPoint (PPTX) 幻灯片来演示。PDF 和 PowerPoint 输出是同一分析的时间点快照。

Connect 目标 AWS 账户 s 和区域

为网络迁移、landing zone 构建和服务器迁移配置目标 AWS 账户 连接器。这包括三个步骤：选择您的迁移类型，提供您的 MAP 协议详细信息（如果适用），然后设置连接器。这些设置适用于所有迁移阶段——网络迁移、landing zone 和服务器重新托管。

步骤 1：选择迁移类型

选择是执行单账户迁移还是多账户迁移：

- Single-account 迁移 — 所有工作负载都迁移到一个目标 AWS 账户。连接器目标账户和目标账户相同。
- Multi-account 迁移 — 工作负载迁移到不同的目标帐户。连接器必须连接到组织管理帐户或同时为 AWS Transform MGN 和注册的委派管理员 (DA) 帐户 CloudFormation StackSets。

第 2 步：MAP 协议

如果您的迁移是迁AWS 移加速计划 (MAP 2.0) 的一部分，请提供您的迁移组合体验 (MPE) ID，这是一个使用大写字母和数字的 10 个字符的代码（例如 ABCDE12345）。当您提供 MPE ID 时，MAP 标签将应用于在网络迁移、landing zone 和服务器重新托管阶段创建的所有资源。标签格式为：

- 密钥：`map-migrated` 值：`mig`*`MPE_ID`*

您必须使用 MAP 标签才能获得 MAP 积分。有关 MAP 的更多信息，请参阅 Migration Accel AWS eration Progra m。

步骤 3：连接器配置

您可以使用目标账户连接器将迁移任务连接到迁移后工作负载所在的 AWS 环境。在开始之前，请验证您的目标是否 AWS 账户 具有必要的权限、配额和配置来支持您的迁移基础架构。

批准连接器请求后，即向以下人员授予 AWS 转换权限：

- 管理用于 VMware 迁移的 Amazon S3 存储桶操作 (read/write)，以及对 Migr AWS ation Hub 和 AWS 应用程序迁移服务 (MGN) 的访问权限。这包括对以下项目的权限，所有权限仅限于目标账户中标有`CreatedBy:AWSTransform`或的资源`CreatedFor:AWSTransform`：
  - 管理迁移浪潮。
  - 管理网络配置（Amazon EC2、VPC、Transit Gateway、Direct Connect、负载均衡器、网络防火墙）。
  - 管理 CloudFormation 堆栈部署。
  - 通过 Systems Manager 自动安装代理。
- 使用存储在发现区域中的信息，将本地工作负载迁移到目标 AWS 账户 和区域。
- 在目标 AWS 账户 和区域中配置和管理着陆区基础设施。这包括对以下项目的权限，仅限于标有标签的资源（`CreatedBy:AWSTransform`如果适用）：
  - 对以开头的存储桶执行 Amazon S3 存储桶操作（创建、读取、写入、删除）。`transform-vmware-landing-zone-`
  - 管理 CloudFormation 堆栈部署和更改 landing zone 堆栈的集合。
  - 执行 Cont AWS rol Tower 操作。您可以管理着陆区、启用基线和启用控件。
  - 管理 AWS 组织。您可以创建和管理组织单位、创建帐户和移动帐户。
  - 通过 Control Tower 管理服务 AWS 控制策略 (SCP)。
  - 管理 S AWS ervice Catalog 配置对象。

> **Note**
>
> 当需要更改权限的新功能时，连接器类型可能会更新。目标账户连接器类型的当前版本为 2.0。创建新连接器时，它将使用最新版本。

在设置连接器之前，请了解迁移中涉及的账户角色：

Account	说明
AWS 转换账户	AWS 组织中您在其中设置 Transform 的任何成员 AWS 帐户。这是您的 “AWS 转换” 工作区运行的地方。它不一定是管理账户。
连接器目标账户	您的 Trans AWS form 连接器配置到的帐户。这取决于您的迁移类型： • Single-account迁移 — Connect 连接到您要将工作负载迁移到的账户。连接器目标账户和目标账户相同。 • Multi-account迁移 — Connect 连接到组织管理帐户或委派管理员 (DA) 帐户。DA 账户必须同时注册为 MGN 和 CloudFormation StackSets 贵 AWS 组织的委托管理员。 AWS Transform 会检查关联的账户是管理账户还是 DA 账户，并相应地调整其行为。
目标账户	您的工作负载迁移到 AWS 账户 哪里。在单账户迁移中，这与连接器目标账户相同。在多账户迁移中，这些账户是接收迁移工作负载的个人成员账户。

使用委派管理员账号

对于多账户迁移， AWS 建议您使用委派管理员 (DA) 帐户，而不是直接使用组织管理帐户。DA 账户遵循最低权限原则，限制迁移操作所需的权限范围。DA 账户必须同时注册为 MGN 和 CloudFormation StackSets 贵 AWS 组织的委托管理员。

这两个选项之间的主要区别在于：

- 管理账户 — 可以为 MGN 和 CloudFormation StackSets 整个组织启用可信访问权限。 AWS 使用转换通话 CloudFormation StackSets API `CallAs: SELF`。

- 委派管理员帐户-无法直接启用可信访问权限（必须通过管理账户完成），但可以管理 MGN 源服务器、启动实例和 CloudFormation StackSets 跨成员账户部署。 AWS 使用转换通话 CloudFormation StackSets API `CallAs: DELEGATED_ADMIN`。

有关更多信息，请参阅 MGN 用户指南中的 MGN 委派管理员。

在连接器设置期间创建的 IAM 角色

在连接器设置过程中，T AWS ransform 会在您的目标账户中创建以下 IAM 角色：

- `AWSTransform-Connector-role-`— 在您 AWS 组织的管理账户或委托管理员账户中设置目标账户连接器时创建。此角色允许 AWS Transform 连接到您的目标账户，并代表您执行迁移操作。

目标账户连接器设置

> **Important**
>
> 在连接器设置过程中，将在您的目标中创建一个 Amazon S3 存储桶 AWS 账户。默认情况下，此存储桶不会强制执行 HTTPS-only 访问权限 (`SecureTransport`)。如果您希望存储桶策略包含安全传输，则必须自行更新该策略。有关更多信息，请参阅 Amazon S3 的安全最佳实践。

使用现有的目标账户连接器

1. 在 Job Plan 窗格中，展开选择目标帐户，然后选择创建或选择连接器。
2. 在 “协作” 选项卡中，选择现有连接器，然后选择 “使用连接器”。如果连接器不可用，则其版本与您选择的作业类型不兼容。

   > **Important**
   >
   > 如果您指定的连接器的目标与 AWS 变换区域不同 AWS 区域 ，则 AWS 转换会将您的数据传输到该区域 AWS 区域。

3. 选择继续。

创建新连接器

1. 在 Job Plan 窗格中，展开 Connect 目标帐户，然后选择创建或选择连接器。
2. AWS 区域 为目标指定 AWS 账户 和，然后选择 “下一步”。

> **Important**
>
> 如果目标与发现的目标 AWS 区域 不同 AWS 区域，Trans AWS form 会将您的数据传输到另一个地方 AWS 区域。

3. 选择是否使用 Amazon S3 托管密钥进行加密。如果您指定自己的 KMS 密钥，则可以使用默认密钥策略或不太宽松的密钥策略。有关创建 KMS 密钥的信息，请参阅 AWS Key Management Service 开发人员指南中的创建 KMS 密钥。

   AWS Transform 使用该`kms:DescribeKey`权限来验证密钥是否存在，`kms:GenerateDataKey`以及`kms:Decrypt`加密和解密 Amazon S3 存储桶中的任务数据。有关更多信息，请参阅 SSE-KMS 使用 Amazon S3 存储桶密钥降低成本。
4. 选择继续。
5. 复制验证链接，与目标管理员共享 AWS 账户，并要求他们批准连接请求。
6. 管理员批准请求后，从列表中选择新创建的连接器，然后选择使用连接器。
7. 选择 “发送到 AWS 转换”。

如果您计划修改 AWS Transform MGN 模板以启用启动后操作，请向目标连接器角色添加以下权限。此 JSON 政策声明授予发布后操作角色的`iam:PassRole`权限。创建连接器后，您可以在 “协作” 选项卡中找到角色名称。有关为角色添加权限的信息，请参阅 IAM 用户指南中的更新角色权限。

```
{
      "Sid": "MGNPostLaunchActions",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::target-account-ID:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
}
```

支持的目标区域

迁移目标区域是部署迁移资源 AWS 区域 的地方，包括着陆区、网络基础设施和服务器再托管。创建连接器时，请指定一个目标 AWS 区域。您可以使用以下任何一项 AWS 区域：

- 美国东部（弗吉尼亚州北部）
- 美国东部（俄亥俄州）
- 美国西部（北加利福尼亚）
- 美国西部（俄勒冈州）
- 非洲（开普敦）
- 亚太地区（香港）
- 亚太地区（台北）
- 亚太地区（孟买）
- 亚太地区（海得拉巴）
- 亚太地区（东京）
- 亚太地区（首尔）
- 亚太地区（大阪）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（雅加达）
- 亚太地区（墨尔本）
- 亚太地区（马来西亚）
- 亚太地区（新西兰）
- 亚太地区（泰国）
- 加拿大（中部）
- 加拿大西部（卡尔加里）
- 欧洲地区（法兰克福）
- 欧洲（苏黎世）
- 欧洲地区（爱尔兰）
- 欧洲地区（伦敦）
- 欧洲地区（巴黎）
- 欧洲地区（斯德哥尔摩）

- 欧洲地区（米兰）
- 欧洲（西班牙）
- 以色列（特拉维夫）
- 墨西哥（中部）
- 南美洲（圣保罗）

> **Important**
>
> 如果您指定的目标不同 AWS 区域 于 AWS 变换 AWS 区域，则您的一些数据将被传输 AWS 区域。
> 请注意，您的服务器复制数据直接从源环境传送到目标账户和区域。

建造着陆区

AWS 作为迁移项目的一部分，Transform 将指导您设计和部署 AWS 着陆区。landing zone 是一种多账户 AWS 环境，可作为工作负载的基础，在任何工作负载到来之前，组织边界、治理控制和账户结构都已到位。 AWS Transform 会分析您的迁移清单和业务需求，以推荐组织单位 (OU) 和账户结构，应用推荐的服务控制策略 (SCP)，并生成基础架构即代码 and/or 部署 (IaC)。

landing zone 特工将引导你完成两个阶段：

- 基础设置 — 建立核心着陆区结构：Cont AWS rol Tower、基础 OU 和核心账户。
- 工作负载账户设计 — 根据您的迁移流程、业务部门和环境分离要求设计和创建工作负载 OU 和帐户。

AWS Transform 同时支持绿地环境（没有现有 landing zone）和棕地环境（现有 OU 和已部署的账户）。在棕地场景中，T AWS ransform 会检测您现有的组织结构，并根据 AWS 最佳实践仅建议填补空白所需的更改。

连接器设置

landing zone 代理需要目标 AWS 账户 连接器才能在您的组织管理账户中配置资源。连接器有权执行以下操作：

- 设置 Cont AWS rol Tower

- 创建组织单位和账户
- 配置服务控制策略 (SCP)

批准连接器请求后，即向以下人员授予 AWS 转换权限：

- 在目标 AWS 账户 和区域中配置和管理着陆区基础设施。这包括对以下项目的权限，仅限于标有`CreatedBy:AWSTransform`和由其标记的资源（`ATWorkspace:{workspace-id}`如果适用）：
  - 以开头的存储桶的 S3 存储桶操作（创建、读取、写入、删除）`transform-vmware-landing-zone-`
  - CloudFormation landing zone 堆栈的堆栈部署和变更集管理
  - AWS Control Tower 操作（管理着陆区、启用基线和控制）
  - AWS O rganizations 管理（创建和管理组织单位、创建账户和移动账户）
  - 通过 Control Tower 管理服务 AWS 控制策略 (SCP)
  - AWS S@@ ervice Catalo g 配置对象管理

创建连接器时，需要指定一个目标 AWS 区域。该区域应与您所在的 Control Tower 区域相同。有关控制塔区域的更多信息，请参阅如何 AWS 区域 使用 AWS 控制塔。

在 I AWS anding zone 设置开始时，Transform 会检索您的连接器配置，并显示 AWS 组织管理账户 ID 和目标区域以供确认。有关更多信息，请参阅 连接器。

> **Important**
>
> IAM 身份中心区域依赖关系 — AWS 转换需要 AWS IAM 身份中心（IAM 身份中心），这意味着您的连接器区域必须同时匹配您的 Cont AWS rol Tower 主区域和 IAM 身份中心区域。如果您的组织中已经配置了 IAM Identity Center，则当连接器针对不同的区域时，Cont AWS rol Tower 初始化将失败。有关更多信息，请参阅 Cont AWS rol Tower 用户指南中的 IAM 身份中心客户注意事项。

基础设置

基础设置阶段使用 Cont AWS rol Tower 建立核心着陆区基础架构。当 Cont AWS rol Tower 设置着陆区时，它会自动在您的管理账户中配置一组托管资源，这些资源构成了整个 AWS 组织的治理基础：

- Root — 包含着陆区域内所有 OU 的顶级父级。
- 安全 OU — 由 Control Tower 自动创建。包含两个共享账户：日志存档账户（用于组织内所有 AWS API 活动和资源变更的集中式不可变日志）和审核账户（对所有账户进行安全与合规性审查的只读访问权限）。这些帐户在初始设置后无法重命名或替换。
- 强制性控制措施（护栏）— Control Tower 会自动在整个组织中应用预防和侦查控制，以强制执行基线治理策略。这些无法禁用。
- IAM Identity Center 目录 — Control Tower 创建一个云原生目录，其中包含预配置的群组和单点登录访问权限，供您的着陆区域用户使用。有关更多信息，请参阅 AWS IAM 身份中心。

Control Tower 用于CloudFormation StackSets在组织中的所有账户和区域中一致地部署和管理这些资源。您不得在支持的方法之外修改或删除 Control Tower 托管的资源，因为这样做可能会导致您的着陆区进入未知状态。

账户电子邮件惯例

AWS 要求每个账户都有一个唯一的电子邮件地址。这些电子邮件会收到有关该帐户的重要通知。AWS Transform 使用加地址从单个邮箱生成唯一的账户电子邮件。

格式：`prefix+account-name@domain`

您提供前缀（例如`aws-admin`）和域（例如`acme.com`），Transform 会 AWS 自动派生所有账户电子邮件。例如：

- 审计账户：`aws-admin+audit@acme.com`
- 日志存档账户：`aws-admin+log-archive@acme.com`
- 沙盒账号：`aws-admin+sandbox@acme.com`

在棕地场景中，T AWS ransform 会检查现有的账户电子邮件以推断出已经在使用的加号寻址惯例，并提议继续使用相同的模式。

推荐的基础结构

根据 AWS 最佳实践，T AWS ransform 建议使用以下基础组织结构。您可以在创建之前对其进行自定义。

OU	用途	账户
安全性	集中式审计记录和监控。将这些服务隔离在专用账户中旨在帮助将您的审计跟踪与工作负载团队分开。	审计，日志存档
Infrastructure	共享网络（Transit Gateway、VPN）、DNS 和公共服务。建议将它们集中起来，以帮助减少重复，并为您的网络团队提供一个管理连接的地方。	无（创建时为空）
沙盒	开发者尝试支出限制和访问受限。建议在不冒生产资源风险的情况下为开发人员提供实验空间。	沙盒
工作负载	包含生产 Non-Production、以及可选的受监管子OU。工作负载帐户将在下一阶段根据您的迁移要求进行设计。	无（创建时为空）

> **Note**
>
> 带有审核和日志存档帐户的安全 OU 是作为 Control Tower 基础设置的一部分创建的。基础架构、沙盒和工作负载 OU 是在您确认结构后分别创建的。

在棕地场景中，T AWS ransform 会将您的现有基础与推荐的结构进行比较，并仅报告差距。例如：“您的基金会有安全和基础架构 OU，但没有沙盒 OU。”

服务控制策略 (SCP)

SCP 是组织级别的权限护栏，用于设置组织中所有账户的最大权限。 AWS 他们不授予访问权限，相反，他们定义了账户中任何人都不能超越的界限，即使是账户管理员也是如此。

作为 Control Tower 部署的一部分，将自动应用基线护栏。 AWS Transform 还会推荐其他旨在帮助增强组织地位的 SCP。它们基于 AWS 最小可行着陆区的最佳实践。

SCP 可以应用于基础架构、沙盒和工作负载 OU。安全 OU 由 Control Tower 管理，SCP 无法通过此工具将其作为目标。

> **Important**
>
> 安全 OU 是由 Control Tower 管理的基础组织单元。您无法通过 landing zone 代理向其添加账户、SCP 或任何资源。

在棕地场景中，Trans AWS form 会检查已应用了哪些 SCP，并且只推荐能够填补空白的 SCP。

基础部署

基础设计完成后，您可以选择部署方式：

- 为我部署 — Tr AWS ansform 将基础 OU、账户和 SCP 部署到您的 AWS 组织。
- 我将自己部署 — Trans AWS form 生成基础设施即代码 (IaC) 工件，以你的首选格式下载（参见the section called “IaC 格式”）。
- 首先设计工作负载帐户-跳过部署，继续工作负载帐户设计阶段。您可以稍后将所有内容一起部署。

Control Tower 初始化

如果 AWS Transform 检测到您的组织中尚未初始化 Cont AWS rol Tower，它会为用户提供指向 T AWS ransform 控制台页面的链接。在链接中生成操作将创建一个用于引导 Control Tower 的 CloudFormation 堆栈。该过程将在 CloudFormation 控制台中为您的目标区域创建此堆栈。堆栈创建完成后，Trans AWS form 会继续部署。

工作负载账户设计

在工作负载账户设计阶段，T AWS ransform 会根据您的迁移清单、业务需求和环境分离首选项为您的应用程序工作负载设计 OU 和账户结构。

迁移规划背景

AWS Transform 会检索迁移计划阶段的数据，包括波浪计划、服务器到应用程序的映射和共享上下文。如果迁移计划数据可用，T AWS ransform 会显示摘要并要求您进行确认或调整。如果没有可用的迁移计划数据，Trans AWS form 会直接询问发现问题。

Discovery

AWS Transform 会询问问题以了解您的工作负载需求。你可以跳过任何问题。主题包含：

- 使用的业务部门或团队数量 AWS
- 行业和任何适用的框架（HIPAA、SOC2 PCI-DSS、FedRAMP）
- 工作负载是否处理敏感数据（PII、PHI、财务）
- 环境分离首选项（dev/test/staging/prod 作为单独账户或共享）
- 工作负载隔离要求
- 业务应用程序及其用途
- 将服务器分组为应用程序
- 成本跟踪和分配需求（按业务部门、项目、环境划分）
- 未来 12-24 个月的预期增长
- 账户策略偏好（每个账户单个应用程序、分组或基于环境）

拟议的工作量结构

根据您的答案和迁移计划数据，Trans AWS form 在工作负载组织单元下提出组织单位和账户结构。该提案包括每个设计决策背后的理由。

AWS 变换遵循以下设计原则：

- 迁移浪潮中的所有服务器都使用同一个账户——不能在不同账户之间分配。这是波次执行期间的重新托管限制。
- 如果您请求隔离环境，Trans AWS form 会创建 Workloads/Production 和 Workloads/Non-Production 子 OU。
- 如果确定了适用的框架，则Trans AWS form会创建 Workloads/Regulated Workloads/Standard 子 OU。
- 如果多个业务部门需要不同的治理，T AWS ransform 会在工作负载下创建特定于业务部门的 OU。
- 关键或敏感数据应用程序每个账户只能获得一个应用程序。在这种情况下，可能会要求您迭代波浪计划。
- 具有共享依赖关系的紧密耦合应用程序分组到一个帐户中。

每个建议的账户包括：名称、用途、目标 OU 和业务部门。 AWS 转换显示正在使用的命名约定（例如，`<business-unit>-<environment>-<workload>`）。

在 Trans AWS form 应用更改之前，您可以查看和修改建议的结构。申请后，您可以进行迭代，即进行其他更改，直到您满意为止。

工作负载 SCP 配置

创建工作负载结构后，Tr AWS ansform 会显示可用的 SCP，并询问您是否要将任何 SCP 应用于工作负载 OU。您可以选择要应用哪些 SCP 以及哪些 OU。 AWS 转换应用 SCP，并使用 SCP 摘要表显示更新的组织树。

工作负载部署

工作负载设计完成后，您可以选择部署方式：

- 为我部署 — Tr AWS ansform 会将工作负载 OU、账户和 SCP 部署到您的 AWS 组织。
- 我将自己部署 — Trans AWS form 生成 IaC 工件以你的首选格式供下载（参见the section called “IaC 格式”）。

IaC 格式

当您选择自行部署时，Trans AWS form 会生成以下格式的 “基础设施即代码” 构件：

- AWS Cloud Development Kit (AWS CDK)— 程序化基础架构部署 TypeScript 项目。
- HashiCorp Terraform — 生成用于管理着陆区资源的 HashiCorp 配置语言 (HCL) 模板。
- 着陆区域加速器 (LZA) — 基于 LZA 通用配置版本 1.1.0 的配置 YAML 文件。这些企业就绪模板与着陆区加速器配合使用 AWS ，可以建立多账户环境 AWS 。生成的文件包括预先配置的治理、组织结构和网络设置，这些设置符合 AWS 最佳实践。要了解更多信息，请参阅 LZA 通用配置。

> **Note**
>
> 通过 Landing Zone Accelerator (LZA) 管道进行部署时，您的 Trans AWS form 帐户和 LZA 安装必须在同一个 AWS 组织中。如果 Transform 中使用的组织 ID 与 LZA 中使用的组织 ID 不匹配，则部署 AWS 将失败。要了解如何使用 Organizations 设置 LZA 安装，请参阅基于AWS 组织的安装。

选择格式后，Transf AWS orm 会生成工件并使其可供下载。

要验证下载的文件没有被损坏或篡改，请生成并下载校验和，然后使用以下命令将其与本地生成的哈希值进行比较：

```
openssl dgst -sha256 -binary <file.zip> | base64
```

部署批准流程

着陆区部署请求需要明确批准才能执行。当您提交部署请求时，它会通过 “ AWS 转换批准” 选项卡自动发送给授权批准者。

批准者会审查 CloudFormation 模板和着陆区配置。只有在 Trans AWS form 中具有管理员角色的用户才能批准部署请求。每次提交都会触发一个新的审核周期，并且只有在收到确认后才会进行部署。

如果批准者拒绝了您的请求，请直接与他们联系以讨论必要的修改。系统会跟踪所有批准决策以供审计，并维护部署历史记录。

标签 landing zone 资源

AWS Transform 会自动标记所有生成的资源`"CreatedBy": "AWSTransform"`以及用于跟踪目的的定义和执行 ID。

自动标记

所有 landing zone 资源都将获得以下标签：

- `CreatedBy`— awsTransform
- `ATWorkspace`— 工作区标识符

> **Note**
>
> 如果您的迁移是迁移加速计划 (MAP 2.0) 的一部分，则可以包含所需的 MAP 标签：密钥：`map-migrated`值：`migMPE_ID`（其中 MPE_ID 是您的迁移组合评估标识符）。 AWS MAP 标签是在连接器设置阶段请求的。 AWS Transform 在 landing zone 部署期间会应用这些标签。

撤消更改

只能移除未部署的元素。一旦部署 OU 或账户，就无法通过 landing zone 代理将其删除。

移除元素时，顺序很重要——你必须在父元素之前移除子元素：

1. 首先删除账户（通过电子邮件）。
2. 从 OU 中移除 SCP。
3. 移除子 OU — 如果 OU 仍有帐户或嵌套 OU，则无法将其删除。

相关资源

- the section called “Connect 目标 AWS 账户 s 和区域”
- the section called “将您的网络迁移到 AWS”
- AWS Control Tower 用户指南
- AWS 《组织用户指南》
- AWS IAM Identity Center 用户指南
- CloudFormation 用户指南
- 着陆区加速器已开启 AWS
- AWS Well-Architected Framework
- AWS 规范性指导：建造着陆区

将您的网络迁移到 AWS

借助 AWS Transform，您可以将网络迁移到 AWS。 AWS Transform 可根据需要将源环境配置转换为AWS等效的网络资源，即 VPC、子网、安全组、NAT 网关、中转网关、弹性 IP、路由和路由表。在部署之前，您可以查看和修改生成的网络配置。您可以使用 “ AWS 转换” 部署配置并分析网络连接。或者，您可以选择自行部署并以首选格式接收基础设施即代码 (IaC)： AWS Cloud Development Kit (AWS CDK)着陆区加速器 (LZA) 或 Terraform。 HashiCorp

要迁移您的网络，请执行以下步骤：

1. 上传您的源网络文件。
2. 上传其他配置文件（可选，对于 RvTools 环境）。
3. 选择网络拓扑。
4. 选择安全组映射策略。
5. 查看并优化您的网络。
6. 生成网络图（可选）。

7. 配置资源标记。
8. 部署您的网络。

> **Note**
>
> 对于多账户部署，在开始网络迁移之前，您必须为 Organizations 配置跨账户 IAM 角色和可信访问权限。 AWS 有关迁移类型的更多信息，请参阅the section called “步骤 1：选择迁移类型”。

步骤 1：源网络映射

网络映射过程要求您从源环境上传配置文件。您选择的工具取决于您的源网络类型：

- 软件定义网络 (SDN)：适用 Import/Export 于 VMware NSX 网络虚拟化或思科以应用为中心基础设施的 Cisco ACI 配置。
- VMware vSphere 网络：rvTools。当您使用 RvTools 文件时，Transform 仅生 AWS 成 Amazon VPC 配置。安全组配置需要来自防火墙或软件定义的网络文件的其他输入。有关通过其他文件生成安全组的更多信息，请参阅其他配置文件。
- 基于防火墙配置数据的网络：从 Palo Alto Networks 防火墙、Fortinet Firewall 或 Cisco FortiGate ACI 导出文件。有关支持的版本和解压缩说明的更多信息，请参阅配置文件提取。
- 同时运行 VMware 和非 VMware 工作负载的混合网络：Trans AWS form 发现工具或 M odelizeIT。
- 其他文件类型：如果您的配置文件不是上面列出的支持格式之一，则该文件会自动转换为支持的格式。根据文件大小和复杂程度，这种转换最多可能需要两个小时。

> **Note**
>
> 支持的最大源网络文件大小为 70 MB。

> **Warning**
>
> 只能从戴尔官方网站下载 RVTools，网址为。https://www.dell.com/en-us/shop/vmware/sl/rvtools不要从非官方来源下载 RVTools。

每个源网段都映射到其自己不同的 VPC。网络分段因来源类型而异：

- vNetwork：按虚拟交换机和虚拟局域网 (VLAN) AWS 转换虚拟机组。VLAN 可以出现在多个 vSwitch（VLAN 0 除外）下。
- NSX 网络：根据 AWS 路由器对网络进行分段，对 Tier-1 路由器进行分组并收集其分段。

步骤 2：其他配置文件

对于 RvTools 源环境，您可以选择上传其他配置文件以启用安全组生成。如果您不上传其他配置文件，则不会为您的 RVTools-based 迁移生成任何安全组。

AWS 转换支持以下其他配置文件类型。您只能从一个平台上传一个配置文件。

- 思科以应用为中心的基础设施 (ACI) 提供网络策略配置。
- 帕洛阿尔托网络提供防火墙安全策略。
- Fortinet FortiGate 提供防火墙安全策略。

上传防火墙或 Cisco ACI 文件时，Transfor AWS m 会生成网络基础设施和安全组。当你单独上传 RVTools 文件时，Transform 只 AWS 会生成网络基础架构。

有关支持的版本和解压缩说明的更多信息，请参阅配置文件提取。

步骤 3：网络拓扑

在网络定义步骤中，您可以选择网络拓扑。您可以选择隔离 VPC 拓扑或中心和分支拓扑。

隔离的 VPC

部署了什么

隔离 VPC 是独立的网络环境，在其中作为独立的单元运行。 AWS您的 VPC 是完全隔离的，它们之间没有内置的通信路径。这种分离提供了最高级别的网络边界保护。

AWS 转换会创建以下资源：

- 每个检测到的源网段都有一个专用 VPC。
- 私有子网基于您的源网络配置。
- 安全组（如果您提供了防火墙或 SDN 配置文件）。

完成您的设置

AWS Transform 部署网络基础设施，但将互联网访问和 VPC 间连接留给您，因此您可以选择符合组织要求的配置。

要为隔离的 VPC 启用互联网访问，请完成以下步骤：

1. 创建互联网网关并将其连接到 VPC。
2. 在每个需要互联网访问的可用区中创建公有子网。添加`0.0.0.0/0`指向互联网网关的路由。有关子网配置的更多信息，请参阅您的 VPC 的子网。
3. 在公有子网中创建 NAT 网关（每个可用区一个，以实现高可用性）。为每个 NAT 网关分配一个弹性 IP。
4. 更新您的私有子网路由表 — 添加一条用于`0.0.0.0/0`指向同一可用区中的 NAT 网关的路由。
5. 查看您的安全组规则 — 确保出站规则允许您的工作负载所需的流量（HTTPS、DNS 等）。

要进行 VPC-to-VPC 通信，请设置 VPC 对等互连或 T ransit Gat eway，并更新每个 VPC 中的路由表，将流量路由到对等连接或 TGW 附件。

集线器和辐条

在此模型中，Tr AWS ansit Gateway 充当连接多个工作负载 VPC（分支）的中心枢纽。

部署了什么

AWS 转换会创建以下资源：

- 分@@ 支 VPC：每个检测到的源网段一个 VPC，带有私有子网和 Transit Gateway 附件。
- 检查 VPC：托管您的防火墙设备以进行流量检查。所有跨虚拟私有云流量均通过此 VPC 路由。Transit Gateway 连接使用设备模式，该设置可确保流量在连接的两个方向上对称地流经同一台设备。
- 入站 VPC：处理从公共互联网进入您的网络的流量（南北入站）。包括跨多个可用区的互联网网关和公有子网。
- 出站 VPC：处理从您的网络流向公共互联网的流量（南北向出站）。包括互联网网关、在每个可用区中具有弹性 IP 地址的 NAT 网关以实现高可用性，以及用于 Transit Gateway 连接的私有子网。
- Transit Gateway 路由表：两个路由表引导流量通过检查 VPC。未经检查的表与分支 VPC、入站 VPC 和出站 VPC 相关联，它会路由所有流量 (0.0.0. 0/0) 到 Inspection VPC 附件，并且是默认的关

联路由表。Inspected 表与检查 VPC 相关联，它包含来自所有分支 VPC 的传播路由，并且是默认的传播路由表。

对于多账户部署，Transit Gateway 通过AWS 资源访问管理器 (RAM) 在账户之间共享。

流量流

所有跨VPC流量都遵循以下路径：

1. 来自分支 VPC 的流量将发送到 Transit Gateway（默认路由 0.0.0）。 0/0)。
2. 未经检查的路由表将流量路由到检查 VPC。
3. 您在检查 VPC 中的防火墙会检查流量并将其转发回 Transit Gateway。
4. 已检查的路由表使用传播的路由将流量路由到目标分支 VPC。

对于出站互联网流量，“已检查” 的路由表会将流量路由到出站 VPC。在流量转发到互联网网关之前，NAT 网关会转换私有 IP 地址。出站 VPC 公共路由表包括返回 Transit Gateway 的每个分支 VPC 无类 Inter-Domain 路由 (CIDR) 范围的特定路由。这些路由使返回流量能够到达正确的分支 VPC。

入站互联网流量通过入站 VPC 的互联网网关进入，并沿着相同的检查路径到达分支 VPC。

完成您的设置

AWS Transform 部署网络基础架构，但将防火墙配置和入站服务设置留给您，因此您可以选择满足组织要求的安全设备和策略。

> **Note**
>
> 默认情况下，跨VPC流量无需检查即可通过检查 VPC。必须部署防火墙才能启用流量检查。

部署防火墙：在检查 VPC 中为防火墙端点创建其他子网。 AWS 转换仅为 Transit Gateway 连接创建子网。将流量从 TGW 连接子网路由到防火墙端点，然后将来自防火墙子网的流量路由回 Transit Gateway。您可以部署 AWS Network Firewall 或第三方设备。有关使用 Transit Gateway 部署防火墙的更多信息，请参阅使用 Tran sit Gateway 创建防火墙。

验证连接：部署防火墙后，测试来自分支 VPC 实例的出站 Internet 访问（例如`curl https://aws.amazon.com`）。您可以使用 Reachability Analyzer 对连接问题进行故障排除。

设置入站服务：要托管面向公众的服务，请在入站 VPC 公有子网中部署 App lication Load Bal ancer 或 Network L oad Balancer。通过 Transit Gateway 配置指向分支 VPC 中实例的目标组，并验证已检查的路由表中是否有通往入站 VPC 的返回路由。

如果要精细控制 VPC 之间的通信，请选择隔离 VPC 选项并修改生成的网络以创建所需的特定通信路径。

步骤 4：安全组映射

选择您的源安全策略如何转换为 AWS 安全组。 AWS Transform 会根据您的源环境配置创建安全组。安全策略、安全策略规则、网关策略和网关策略规则将转换为安全组。

> **Important**
>
> AWS Transform 会尽最大努力创建与您的源环境相匹配的安全组。查看和修改生成的安全组，确保它们符合贵公司的需求和安全策略。

引用安全组

生成安全组时，T AWS ransform 会在支持的情况下使用安全组引用。安全组引用根据另一个安全组 ID 而不是特定的 IP 地址范围（CIDR 块）来设置安全规则。这种方法提供了更灵活和更易于维护的安全配置。

您的安全组规则只能引用同一 VPC 内或在同一区域内连接的 VPC 中的其他安全组。 Cross-account 还支持引用。您不能在未连接的 VPC 中或跨区域引用安全组。对于连接的 VPC，只有入站规则支持跨 VPC安全组引用——出站规则必须使用 CIDR-based 规则。T AWS ransform 如何创建安全组规则取决于您选择的网络拓扑：

- 中心和分支：T ransit Gateway 提供 VPC 之间的网络连接。 AWS Transform 对 VPC 内规则和跨入口规则使用引用。VPC/cross-account Cross-VPC/cross-account 出口（出站）规则使用 CIDR-based 规则。
- 隔离的 VPC：您的 VPC 之间没有网络连接。 AWS 转换仅对 VPC 内规则使用引用。所有越 VPC 和跨账户的规则都使用 CIDR-based 规则。

CIDR-based 当源配置不对称时，也会使用规则。

选择以下安全组映射策略之一：

- MA@@ P：将源环境中的安全规则转换为 AWS 安全组和规则。使用此选项进行使用静态 IP 寻址的迁移。
- MAP_DHCP（支持 DHCP 的 Translate）：使用 DHCP 兼容性转换源环境中的安全规则。DHCP 根据子网的 CIDR 范围动态分配 IP 地址。因此，跨VPC的出口规则被扩展到与完整的目标子网 CIDR 相匹配。较窄的 CIDR 将屏蔽超出该范围的 DHCP-assigned IP，请在迁移后查看这些规则。

  使用此选项可通过 VPC Transit Gateway 通信获得 DHCP 支持。也适用于静态 IP，但可能产生比 MAP 更广泛的规则。
- SKIP：不转换安全规则。迁移后手动配置 AWS 安全组。适用于静态 IP 和 DHCP 环境。对于没有其他配置文件的 RvTools 源环境， AWS 转换会自动使用 SKIP。

> **Note**
>
> 您的映射策略决定了您的 IP 分配选项。MAP 仅支持静态 IP。MAP_DHCP 和 SKIP 同时支持静态和 DHCP。

IP 迁移方法

您可以选择两种网络配置进行迁移：

网络范围选择

- 保留现有范围（保留 IP 地址范围）：迁移期间保留原始 IP 地址范围。非常适合 AWS 无需修改（移动）即可将应用程序迁移到的迁移，特别是对于具有硬编码 IP 依赖关系或现有防火墙规则的传统应用程序。
- 更新到新 IP 范围（CIDR 更新）：您可以在迁移期间修改每个 VPC CIDR 范围，Trans AWS form 会自动将更改传播到子网、路由表和安全组。

IP 地址分配

- 固定 IP 地址（静态）： AWS 转换基于 CIDR 分配静态 IP。这最适合需要可预测的网络行为、DNS 管理或 IP-based 访问控制的应用程序。IP 通过弹性网络接口 (ENI) 在实例重启后持续存在，弹性网络接口 (ENI) 是连接到您的实例的虚拟网卡。
- 动态 IP 分配 (AWS DHCP)：实例启动时自动从子网池分配 IP。最适合专为在云中运行和自动缩放工作负载而设计的应用程序。减少运营开销，但要求应用程序使用 DNS 或服务发现。

您可以将任一范围选择与任一 IP 分配方法结合使用。

> **Note**
>
> IP 地址分配策略是在波浪级别设置的。您可以通过自定义 wave 文件为特定服务器分配不同的策略。例如，如果您为该浪潮选择了静态 IP 地址方法，但想为特定服务器分配动态方法，则应按照 MGN 用户指南中编辑配置[RESET_VALUE]中所述使用。

第 5 步：查看和优化您的网络

T AWS ransform 生成目标网络配置后，您可以查看与 AWS 基础设施融合的本地网段。使用可视界面查看您的网络，使用聊天界面进行更改并接收指导性建议。 AWS Transform 执行级联影响分析并实施所需的更改，以保持网络一致性并符合最佳实践。您也可以让 T AWS ransform 分析您的网络并提出优化建议，请参阅指导建议。

目标账户中的现有 VPC

如果您的目标账户已经包含来自先前迁移阶段或并行基础架构项目的 VPC，Trans AWS form 会自动检测它们，并在审核过程中将其显示在映射的 VPC 旁边。对于多账户迁移，Trans AWS form 会检测组织中所有账户中的现有 VPC。 AWS

这种可见性可帮助您了解规划的网络与现有基础设施的关系，识别潜在的 CIDR 冲突，并在部署之前做出明智的决策。

> **Note**
>
> AWS 转换仅检测现有 VPC（不检测子网或其他资源）。检测是只读的- AWS 转换不会修改您的现有 VPC。

优化您的网络

> **Note**
>
> 这些操作仅适用于工作负载 VPC。对于中心和分支拓扑（检查、入站、出站）中的设备 VPC，仅支持更改 IP 地址。
> 您无法撤消删除、合并和拆分操作。在应用这些更改之前，请仔细检查您的配置。

VPC 有以下操作可用：

- 删除：从配置中永久删除 VPC。将其用于不应迁移到的过时网段 AWS。
- 排除：暂时将 VPC 从迁移中移除，以制定分阶段迁移策略。已排除的 VPC 不会部署，但可以稍后重新添加。
- 包括：将之前排除的 VPC 重新添加到迁移中。
- 合并：将两个 VPC 合并为一个。第一个 VPC 保留其身份并吸收第二个 VPC 中的所有子网。安全组将移至合并的 VPC，并相应地重建其关联。第一个 VPC 的 CIDR 扩展到包含两个原始 CIDR 的最小 CIDR 范围，并且路由会自动更新。第二个 VPC 已从配置中删除。

  合并要求：

  - 子网 CIDR 不能在两个 VPC 之间重叠。
  - 合并后的 CIDR 不得超过 /16。
  - 对于多账户部署，必须将两个 VPC 分配给同一个账户。
- 更改 IP 地址：更改 VPC CIDR 的基本 IP 地址，同时保持相同的前缀长度。 AWS 转换会自动按相同的偏移量转换所有子网 CIDR。例如，将 VPC 从更改`10.0.0.0/16`为会将子网从`10.20.0.0/16`变`10.0.1.0/24`为`10.20.1.0/24`。

  与旧 VPC CIDR 完全匹配的安全组规则会自动更新。部分重叠或与旧 CIDR 不匹配的规则不会更改，请在更改后查看这些规则。
- 重命名：更改 VPC 的名称，使其与组织的成本分配、合规性跟踪和运营标准的命名惯例保持一致。
- 调整大小：更改 VPC CIDR 的前缀长度以扩大或缩小 IP 地址范围。
  - 前缀长度减少（IP 越多，例如 /20 到 /16）：子网仍然适合更大的范围。无需更改子网。
  - 前缀长度增加（IP 更少，例如 /16 到 /20）：必须先使用子网调整大小操作调整新范围之外的子网的大小。

  与旧 VPC CIDR 完全匹配的安全组规则会自动更新。部分重叠或与旧 CIDR 不匹配的规则不会更改，请在调整大小后查看这些规则。

  调整大小要求：

  - 新的 CIDR 必须介于 /16 和 /28 之间。
  - 新 CIDR 不得与网络中的其他 VPC 重叠（中心和分支拓扑）。
  - 减少 CIDR 时，所有现有子网都必须适合新 CIDR。如果需要，请先调整子网的大小。

- 拆分：根据您提供的 CIDR 边界将一个 VPC 划分为两个 VPC。子网将分配给包含子网的 CIDR 的新 VPC。安全组会克隆到两个新 VPC 上，但安全组规则 CIDR 不会自动更新，拆分后请查看您的规则，确保跨虚拟私有云通信按预期进行。原来的 VPC 被两个新的 VPC 所取代。

  拆分要求：

  - 您必须恰好提供两个 CIDR 范围。
  - 两个 CIDR 不得重叠。
  - 每个 CIDR 必须介于 /16 和 /28 之间。
  - 每个子网必须恰好适合两个 CIDR 中的一个。如果有任何子网不适合，则该操作将被拒绝。

以下操作可用于子网：

- 更改 IP 地址：更改子网 CIDR 的基本 IP 地址，同时保持相同的前缀长度。
- 删除：在不影响父 VPC 的情况下将子网从配置中永久移除。
- 调整大小：更改子网 CIDR 的前缀长度以扩大或缩小 IP 地址范围。

  子网大小调整要求：

  - 新的 CIDR 必须介于 /16 和 /28 之间。
  - 新 CIDR 不得与同一 VPC 中的其他子网重叠。
  - 新 CIDR 必须位于父 VPC 网段内。

每次操作后，T AWS ransform 都会重新评估安全组引用，这可能会将 CIDR-based 规则转换为安全组引用，反之亦然。进行更改后，请查看您的安全组规则，以确认它们符合您的要求。

引导式网络推荐

AWS Transform 会分析您映射的网络，并通过聊天界面提供按优先顺序排列的建议。建议基于您的网络数据，在应用任何更改之前都需要您的确认。

AWS Transform 可能会推荐以下优化：

- CIDR 冲突解决方案：标记组织中所有账户中映射的 VPC 和现有 VPC 之间的重叠的 CIDR 范围。AWS 首先显示冲突的 VPC。您可以通过重新寻址映射的 VPC、将其排除或删除，或者确认冲突并在部署后自行解决来解决冲突。
- 命名标准化：标记不遵循一致模式的 VPC 名称（例如，包含硬件引用的名称）。 AWS 在提出替代方案之前，Transform 会要求您提供云命名惯例。

- 范围审查：确定可能不需要迁移到的网段 AWS，例如待停用的旧系统或结构。 AWS 在排除任何构造之前，转换会要求您进行确认。
- 适当调整 VPC 容量：显示其所包含子网的 CIDR 过大或过小的 VPC。 AWS Transform 会显示当前容量数据，并允许您决定是否调整大小。
- 安全审查：标记允许不受限制的入站流量的安全组规则 (0.0.0. 0/0) 供您审阅。
- VPC 整合：识别分散的 VPC，这些VPC似乎被物理基础设施限制而不是逻辑隔离要求分开，并建议将其合并。

> **Note**
>
> 在 Trans AWS form 应用任何更改之前，所有建议都需要您的明确确认。 AWS 当建议影响网络的多个方面时，Transform 会进行权衡取舍。

步骤 6：网络图

查看生成的 VPC 配置后，您可以选择生成网络图来可视化您的网络拓扑。 AWS 变换支持以下图表格式：

- M@@ ermaid 代码 (.mmd)：此格式生成一个基于文本的图表定义文件，您可以使用工具进行渲染。 Mermaid-compatible
- 图片 (.png)：此格式生成网络拓扑的渲染图像。

步骤 7：配置资源标记

您的网络资源已标记为启动和复制。您还可以添加自定义标签和 Migration Accel AWS eration Program (MAP) 标签。

用于启动和复制的自动标记

AWS 使用以下标签自动转换您迁移的网络资源（VPC、子网、安全组和路由表）的标签：

- 密钥：`CreatedBy` 值：`AWSApplicationMigrationService`
- 密钥：`ATWorkspace` 值：*`workspace-id`*

这些标签允许使用 VPC 和子网在中启动测试和直接转换实例。 AWS

> **Note**
>
> 默认情况下，迁移的 VPC 和子网不包括互联网连接，因此它们不适合作为复制的暂存区域。

要同时使用 VPC 和子网作为中转区域（复制），请手动添加以下标签：

- 密钥：`CreatedFor` 值：`AWSTransform`
- 密钥：`ATWorkspace` 值：*`workspace-id`*

您也可以将这些标签应用于任何现有的 AWS 网络资源，使其可用于复制。

在 Transfor AWS m Web 应用程序网址中找到你的工作空间 ID：https://.../workspace//*workspace-id*-id job/job

自定义标签

除了 Tr AWS ansform 自动应用的标签外，您还可以选择添加自定义标签来组织、跟踪成本和管理迁移网络资源的合规性。您可以在两个级别上应用自定义标签：

- Job-level 标签：应用于此任务创建的所有资源，包括所有 VPC、子网、安全组和路由表。
- VPC-level 标签：应用于特定 VPC 并自动级联到其所有关联资源（子网、安全组、路由表）。

> **Note**
>
> 每个请求最多 40 个标签。每个标签都需要一个键和值。 AWS 标签约定适用。

AWS Transform 在生成 “基础架构即代码” 模板时会应用这些标签。

AWS 迁移加速计划

如果您的迁移是迁移加速计划 (MAP 2.0) 的一部分，则 Trans AWS form 会对您的资源应用 MAP 标签。AWS 如果您在迁移过程的早期提供了 MPE ID，则标签会自动应用。否则，在您查看完生成的 VPC 配置后，T AWS ransform 会询问您是否有 MAP 协议，并提示您提供您的 MPE ID，即使用大写字母和数字的 10 个字符的代码（例如 ABCDE12345）。应用的标签使用以下格式：

- 密钥：`map-migrated` 值：`mig`*`MPE_ID`*

第 8 步：部署您的网络

标记后，选择您的部署策略：

- AWS Transform-managed 部署：Transfor AWS m 使用 CloudFormation 模板部署您的网络，并运行 Reachability Analyzer 来检查多个 VPC 和同一 VPC 内的子网之间的连接。

  > **Note**
  >
  > 在您的网络部署请求运行之前，您必须获得明确的批准。请参阅部署批准流程。

- Self-deployment: T AWS ransform 生成基础设施即代码 (IaC) 模板。 CloudFormation 默认情况下会生成模板。您还可以选择其他输出格式：
  - AWS CDK 生成一个用于编程基础架构部署的 TypeScript 项目。
  - HashiCorp Terraform 生成用于管理网络资源的 HashiCorp 配置语言 (HCL) 模板。
  - 着陆区域加速器 (LZA) 为 LZA 网络配置生成网络配置.yaml 文件。

> **Note**
>
> 当您通过着陆区加速器 (LZA) 管道进行部署时，您的 Trans AWS form 帐户和 LZA 安装必须位于同一个 AWS 组织中。如果组织 ID 不匹配，则部署将失败。

对于自行部署，请使用提供的链接下载包含生成的模板的 zip 文件。zip 文件夹中包含一个说明如何使用生成的模板的 README.md 文件。

要验证下载的文件没有被损坏或篡改，请生成并下载校验和，然后使用`openssl dgst -sha256 -binary <file.zip> | base64`命令将其与本地生成的哈希值进行比较。

部署批准流程

为确保网络变更符合组织的安全标准和架构要求，所有部署请求都要经过批准工作流程。在您的网络部署请求运行之前，您必须获得明确的批准。当您提交部署请求时，它会通过 “ AWS 转换批准” 选项卡自动发送给授权批准者。审批者验证 CloudFormation 模板和网络配置，以确保符合安全标准和架构要求。每次提交都会触发一个新的审核周期，并且只有在收到确认后才会进行部署。如果批准者拒绝了您的请求，请直接与他们联系以讨论必要的修改。 AWS Transform 会跟踪所有审批决策以供审计，并维护部署历史记录。

删除已部署的网络资源

如果您需要回滚部署，可以删除 Transfor AWS m 部署的网络资源。部署完成后，您可以立即删除资源。如果您在部署后修改已部署的网络资源，则无法自动删除这些资源。

- AWS Transform-managed 部署： AWS 转换会移除部署期间创建的所有 CloudFormation 堆栈。此操作需要通过 “ AWS 转换批准” 选项卡进行批准。
- Self-deployments：您必须通过 AWS 管理控制台或 AWS CLI 手动删除已部署的资源。

配置文件提取

如果您的源环境使用 Cisco ACI、Palo Alto Networks 或 Fortinet FortiGate，则需要提取配置文件以提供给 Transform。 AWS 您可以将这些文件用作独立源文件来生成网络基础设施和安全组，也可以将这些文件与 RVTools 上传文件一起用作补充文件，以添加安全组生成。两种情况下的提取过程都是一样的。

要从防火墙和网络环境中提取配置文件，请按照以下步骤操作。有关最新信息，请查阅供应商文档。

Fortinet FortiGate

- 固件版本必须为 7.0 或更高版本。
- 您需要`super_admin`或全球级别的`super_admin_readonly`权限。
- 步骤：
  1. 通过 SSH 或内置 CLI 客户端连接到防火墙
  2. 运行:`show | grep ""`（`| grep ""`禁用分页）
  3. 从`show`命令开始将所有输出保存到一个文件中

Palo Alto Networks

- 固件版本必须为 10.1 或更高版本。
- 你需要超级管理员角色。
- 通过 SSH 连接到防火墙，运行以下命令以禁用分页、设置输出格式、进入配置模式以及导出配置和预定义对象。保存输出：

```
set cli pager off
set cli config-output-format set
```

```
configure
show              # Save as palo-conf.txt
show predefined   # Save as palo-default.txt
```

思科 ACI

- 固件版本必须为 6.0 或更高版本。
- 您需要具有所有权限的管理员角色以及已配置的安全复制协议 (SCP)、SSH 文件传输协议 (SFTP) 或文件传输协议 (FTP) 目标。
- 步骤：
  1. 通过浏览器连接到应用程序策略基础架构控制器 (APIC)
  2. 打开管理菜单并选择 Config Rollbacks
  3. 在 “拍摄快照” 对话框中，选择 “远程位置” 选项，然后选择 “立即创建快照”。
  4. 收到 “传输成功” 消息后，连接到远程位置服务器并检索最新的快照文件（.gz 文件）

迁移服务器

AWS Transform 使用 AWS Transform MGN (MGN) 将您的服务器重新托管到 Amazon EC2。迁移服务器工作流程将指导您完成每个迁移浪潮、验证服务器清单、部署复制代理、监控数据复制、测试迁移的实例以及执行最终切换。要了解更多相关信息，请参阅什么是 AWS Transform MGN？ 在 MGN 用户指南中。

服务器迁移是按波浪组织的。每波都代表一组一起迁移的服务器。对于每个波次，您都要完成以下阶段：

对于采用容器化迁移策略的浪潮，Trans AWS form 运行的是源代码容器化工作流程，而不是下面描述的重新托管步骤。容器化工作流程将指导您完成克隆源代码、生成 Docker 工件、发布容器镜像以及部署到亚马逊弹性容器服务或亚马逊 Elastic Kubernetes 服务。有关完整的容器化工作流程，请参阅。源代码容器化

1. 先决条件和配置迁移默认值
2. 步骤 1：设置迁移浪潮
3. 第 2 步：验证并确认库存
4. 步骤 3：部署复制代理
5. 步骤 4：数据复制

6. 第 5 步：测试
7. 第 6 步：切换

先决条件和配置迁移默认值

先决条件

在开始重新主机迁移之前，请确保您已做好以下准备：

> **Note**
>
> 如果您在 Transf AWS orm 中完成了端到端迁移任务的所有步骤，则您的目标账户和库存文件已准备就绪，将在迁移计划步骤中为您生成清单文件。通过 Transfor AWS m 网络迁移设置的网络基础设施也已准备就绪。如果您没有通过 T AWS ransform 构建网络基础架构，请确保在开始重新托管迁移之前提前对其进行设置。
>
> 在开始重新主机迁移之前，请确认您有足够的网络资源和基础设施来托管服务器。你可以使用 Trans AWS form landing zone 和网络迁移功能或任何其他工具来实现此目的。

- 支持的操作系统-源服务器必须运行支持的操作系统。有关完整列表，请参阅 MGN 用户指南中的支持的操作系统。
- 要迁移的目标帐户-需要将服务器迁移到哪里 AWS 账户 ID。你可以使用 Trans AWS form landing zone 或任何其他工具来设置基础架构。
- 网络基础设施到位 — 部署和配置 VPC、子网和安全组。您可以使用 T AWS ransform 网络迁移或任何其他工具来设置您的网络基础架构。
- 清单文件-包含服务器详细信息、波次分配、目标账户信息和 Amazon EC2 实例类型首选项。你可以使用 T AWS ransform 迁移计划来生成此文件。

配置迁移默认值

在开始执行多账户迁移之前，应配置适用于所有目标账户的默认设置。这些默认值定义了如何启动您的 Amazon EC2 实例以及如何配置常规迁移。在波浪设置期间，你可以在波浪级别上覆盖这些默认值。

亚马逊 EC2 推荐偏好

AWS Transform 根据源虚拟机的使用规格提供 Amazon EC2 实例类型建议。您可以配置 Amazon EC2 推荐首选项，以控制如何为迁移的服务器选择实例类型。

有关生成 Amazon EC2 建议的更多信息，请参阅中的生成 Amazon EC2 建议 AWS Migration Hub。

> **Note**
>
> 您可以修改建议的 Amazon EC2 实例类型，以纳入迁移评估员、AWS 优化和许可评估 (OLA) 或 AWS 转型评估任务的建议。

迁移初始化

要开始迁移， AWS Transform 会为你计划迁移的每个 AWS 区域 账户以及将要使用该服务的所有目标账户初始化 MGN。在初始化过程中：

- 已创建所需的 IAM 角色和策略。
- 已配置所需的默认模板。

有关初始化过程的信息，请参阅 MGN 用户 AWS Transform MGN 指南中的使用控制台初始化。

Amazon EC2 启动模板

启动设置包括两部分：常规启动设置和 Amazon EC2 启动模板，后者决定如何为中的每台源服务器启动测试或直接转换实例。 AWS

启动设置（包括 Amazon EC2 启动模板）可以在账户级别定义，然后在每次向 Trans AWS form MGN 中添加源服务器时自动应用于每台源服务器。本节中定义的启动设置默认值可以自动应用于您的所有目标账户。

AWS Transform 显示了可用的启动模板设置列表。您可以选择继续使用默认设置或配置启动模板。如果您选择配置，T AWS ransform 会提供指向人机在环 (HITL) 审阅的链接，其中包含启动模板设置的所有参数。你也可以直接通过聊天界面修改任何你想要的参数。

源服务器是使用账户启动模板设置创建的。使用这些默认设置创建源服务器后，可以在源服务器启动设置级别对其进行更改。您可以使用聊天界面更改源服务器对任何参数的设置，或者在此期间使用清单 Excel 文件进行批量操作第 2 步：验证并确认库存。

要查看启动模板设置和详细信息的完整列表，请参阅 MGN 用户指南中的启动常规设置。

Amazon EC2 启动模板的其他变更

对于其他 Amazon EC2 启动模板的更改，您应该对每个目标账户的模板 ID 进行更改。此选项在波形设置中可用。 AWS Transform 会引导你完成它并提供相应的链接。

步骤 1：设置迁移浪潮

在此阶段，T AWS ransform 通过配置目标账户、验证服务权限、设置资源标签、向清单中添加网络数据以及配置复制和启动设置来准备迁移浪潮。

迁移模式和账户配置

AWS 转换支持两种迁移模式：

- Single-account 迁移 — 浪潮中的所有服务器都迁移到连接器中配置的相同目标帐户。
- Multi-account 迁移-服务器迁移到库存文件中指定的不同目标账户。对于多账户迁移，您的库存文件必须包含一`mgn:account-id`列，其中包含每台服务器的目标账户 ID。

AWS Transform 确认目标账户配置，并验证每个目标账户中是否已初始化 MGN。如果 MGN 尚未初始化，则 T AWS ransform 会提供完成初始化的指令。在初始化期间，MGN 会为复制和启动操作创建以下 IAM 服务角色：

- `AWSApplicationMigrationReplicationServerRole`
- `AWSApplicationMigrationConversionServerRole`
- `AWSApplicationMigrationMGHRole`
- `AWSApplicationMigrationLaunchInstanceWithDrsRole`
- `AWSApplicationMigrationLaunchInstanceWithSsmRole`
- `AWSApplicationMigrationAgentRole`

要了解有关这些角色的更多信息，请参阅 MGN 用户指南中的使用控制台初始化 MGN 或使用 API 初始化 MGN。

对于多账户迁移，Trans AWS form 还会在初始化步骤中创建以下角色：。`AWSTransformRehostSharingRole_<management-or-delegated-admin-account-id>`此角色部署在所有迁移目标账户中。

资源标签验证

确认服务权限后，T AWS ransform 会验证代理成功操作迁移所需的所有资源都已正确标记。如果有任何资源缺少必需的标签，T AWS ransform 会提供一个指向标记页面的链接，您可以在其中应用缺少的标签，然后再继续。以下标签是必需的：

- 现有的源服务器必须有标签`CreatedBy: AWSTransform`和`ATWorkspace: <workspace_id>`。如果您已经在源服务器上开始复制并在 Transfor AWS m MGN 服务中创建了它们，则需要标记这些服务器，以便 Transfor AWS m 可以将它们与从本地环境中发现的源服务器相关联，并避免不必要地创建重复的源服务器。 AWS 转换使用用户提供的 ID、FQDN 或主机名密钥在它们之间自动关联。
- 必须为复制（暂存区）和启动实例正确标记网络资源。 AWS Transform 显示目标账户中网络资源的完整列表，并指明每个资源是否已被标记。您可以查看列表并选择要添加的任何未标记的资源。对于您选择的每个资源，T AWS ransform 都会应用相关的标签：
  - `CreatedBy: AWSTransform`或者`CreatedFor: AWSTransform`，视资源类型而定。
  - `ATWorkspace: <workspace_id>`应用于所有选定的资源。

  系统会自动标记由 Trans AWS form 网络迁移代理创建的 VPC 和子网。
- 除了 VPC 和子网外，Trans AWS form 还会显示目标账户中所有现有的弹性网络接口 (ENI)。如果您想让 T AWS ransform 在实例启动时使用它们，则必须使用`CreatedFor: AWSTransform`和标记`ATWorkspace: <workspace_id>`。有关如何在 Amazon EC2 启动模板中附加或添加 ENI 的更多信息，请参阅 MGN 用户指南中的详细注意事项。

将网络数据添加到清单

AWS Transform 会将网络迁移中的网络信息添加到清单文件中。此步骤根据在迁移网络阶段生成的网络配置，将您的服务器映射到相应的目标子网和安全组。

复制和启动设置

复制设置配置

复制设置决定了如何将数据从源服务器复制到 AWS。在将源服务器添加到 Trans AWS form MGN 之前，请在复制模板中配置复制设置。 AWS Transform 会显示所有复制设置参数，您可以通过专用 HITL 或聊天界面对其进行配置。

有关复制设置参数的更多详细信息，请参阅 MGN 用户指南中的复制设置模板。

启动模板设置

启动模板允许您控制 T AWS ransform MGN 在中启动实例的 AWS方式。模板中定义的默认配置会自动应用于每台新添加的服务器。您可以通过专用 HITL 或聊天界面配置启动模板设置。

有关启动模板设置参数的更多详细信息，请参阅 MGN 用户指南中的启动模板。

AWS Transform 还提供了指向与启动模板关联的 Amazon EC2 启动模板 ID 的链接，允许您更改其他 Amazon EC2 启动模板属性。要编辑 Amazon EC2 启动模板，请按照 MGN 用户指南中的启动模板中的说明进行操作。

知识产权分配策略

您可以选择如何为迁移的服务器分配 IP 地址：

- 静态 IP — 保留源服务器的 IP 地址。如果需要 CIDR 转 AWS 换，转换会自动转换 IP 地址以匹配新的 CIDR。
- 动态 IP (DHCP)-从子网的 IP 池中为每台服务器分配一个新的 IP 地址。

> **Note**
>
> 如果您在网络迁移期间选择了 MAP 安全组映射策略，则只有静态 IP 分配可用。有关更多详细信息，请参阅安全组映射。

第 2 步：验证并确认库存

在将服务器数据加载到 MGN 之前，T AWS ransform 会准备库存文件供您查看。您可以下载 CSV 或 XLSX 格式的文件，查看服务器配置，并在需要时进行更改。

清单文件包括服务器名称、操作系统、Amazon EC2 实例类型建议、目标子网、安全组、IP 分配和许可选项等详细信息。必填字段包括：

- 服务器信息-服务器名称、VMID 和源规格。
- 波浪分配-迁移波分组。
- 应用程序分组-逻辑应用程序关联。
- 目标配置-目标账户、地区和 Amazon EC2 实例类型。
- 网络配置-目标子网和安全组。

您可以修改文件以调整 Amazon EC2 配置、更改操作系统许可选项（BYOL 或包含许可）以及更新租赁设置。

查看库存后，您可以接受如图所示的库存或上传修改后的版本。 AWS 然后，Transform 将数据加载到 MGN 中，后者会为波浪中的每台服务器创建源服务器记录。

> **Note**
>
> 请勿删除库存文件中的列或更改列标题。 AWS 转换需要原始文件结构才能正确处理数据。

> **Note**
>
> AWS 变换允许一次导入给定目标 AWS 账户 和目标 AWS 区域 。如果您同时处理多个浪潮，或者有多个迁移任务使用同一个目标账户运行，则必须等待导入完成，然后才能在不同的浪潮或任务中执行另一次导入。

您可以通过在清单文件列`mgn:launch:placement:operating-system-licensing`和中指定配置来控制操作系统许可选项（BYOL 或包含许可证）和租期。`mgn:launch:placement:tenancy`有关更多信息，请参阅 MGN 用户指南中的导入参数。

步骤 3：部署复制代理

要开始将数据从源服务器复制到 AWS，请在每台源服务器上安装 AWS 复制代理。 AWS Transform 提供三种安装方法：

- 组织工具-使用组织现有的部署工具（例如 SCCM、Ansible 或 Chef）在服务器上安装代理。 AWS Transform 为安装命令提供了用于静默安装的其他参数`--no-prompt`，包括`--aws-access-key-id`、`--aws-secret-access-key`、、和`--aws-session-token`。
- MGN 连接器-使用 MGN 连接器自动安装代理。该连接器通过 SSH (Linux) 或 WinRM (Windows) 连接到源计算机，并自动安装复制代理。配置完成后，连接器可以在多个波浪和不同的目标 AWS 账户上重复使用。有关 MGN 连接器的更多信息，请参阅 MGN 用户指南中的设置 MGN 连接器。

> **Note**
>
> 在 AWS 将 MGN 连接器与 Transform 一起使用之前，必须使用以下标签在 AWS Systems Manager Fleet Manager 中标记连接器的托管实例：
>
> - 关键：`CreatedFor`值：`AWSTransform`
> - 关键：`ATWorkspace`值：*`workspace-id`*
>
> 要标记托管实例，请打开 AWS Systems Manager 控制台，导航到“节点工具”下的 Fleet Manager，选择 MGN 连接器的托管实例，然后应用上面的标签。在 AWS 转换 Web 应用程

序网址中找到您的工作空间 ID: `https://.../workspace/workspace-id/job/job-id`。

- 手动安装-直接在每台源服务器上安装代理。此方法需要直接访问每台服务器，但允许您完全控制安装过程。

AWS 转换 MGN 连接器设置

T AWS ransform MGN 连接器可自动将复制代理部署到源服务器。该连接器是部署在本地环境中的专用 Linux 计算机上的轻量级客户端。它通过 SSH (Linux) 或 WinRM (Windows) 连接到源服务器以安装和配置复制代理，无需在多个 AWS 服务之间进行手动协调。

连接器的工作原理

该连接器通过以下组件运行：

- 连接器客户端-部署在您环境中的专用 Linux 计算机上。
- SSM 代理-安装在同一台计算机上以实现与 AWS的安全通信。
- SSM 混合激活 — 将连接器计算机链接到 S AWS ystems Manager，以便安全地执行命令。
- 凭据管理-从 S AWS ecrets Manager 检索源服务器凭据。

部署代理时，Trans AWS form 会向连接器计算机发送 SSM 文档。然后，连接器从 S AWS ecrets Manager 检索源服务器凭据，与每台源服务器建立连接，验证源服务器是否满足先决条件，安装和配置复制代理，并验证安装成功。

连接器机器要求

要求	说明
操作系统	支持的 Linux 操作系统。有关完整列表，请参阅 MGN 用户指南中的 MGN 连接器先决条件。
网络访问	必须访问所有源服务器（Linux 通过 SSH，Windows 通过 WinRM）
互联网连接	到 AWS 端点的出站 HTTPS (443)（Systems Manager、Secrets Manager、MGN）

要求	说明
磁盘空间	至少 200 MB 可用空间
Permissions	root 或 sudo 访问权限

> **Note**
>
> 连接器必须安装在 Linux 计算机上，但它可以将代理部署到 Linux 和 Windows 源服务器。

设置过程

AWS Transform 将引导您完成以下步骤来设置连接器：

步骤 1：连接器配置

为您的连接器提供一个名称，或者使用自动生成的默认名称。连接器可以安装在管理账户上，也可以安装在 MGN 中的委托管理员账户上。对于多账户迁移，连接器可以跨成员账户将代理部署到服务器。

步骤 2： AWS 资源设置

AWS Transform 会打开一个使用您的 AWS 凭据在浏览器中运行的设置页面。您必须使用 AWS 管理帐户或委托管理员帐户登录管理控制台。该帐户必须与您的 Trans AWS form 目标连接器所连接的帐户相同。

设置页面会自动创建以下资源：

- IAM 角色（以等效方式创建 — 如果已存在则跳过）：
  - `AWSApplicationMigrationConnectorManagementRole`— 在代理安装期间用于访问凭据。
  - `AWSApplicationMigrationConnectorSharingRole_<ACCOUNT-ID>`— 包含代理安装权限。
- SSM 混合激活 — 30 天的到期期。将连接器计算机链接到 AWS Systems Manager 并生成安全激活凭证。

或者，您可以从设置页面下载 CloudFormation 模板来自己部署 IAM 角色。

安装页面生成包含所有必要凭据和配置的单行安装命令。

> **Important**
>
> 保持安装页面处于打开状态，直到安装完成。关闭它需要重新启动该进程。所有凭据仅存在于您的浏览器中，不会由 T AWS ransform 存储。

第 3 步：连接器安装

在您环境中的 Linux 计算机上安装连接器：

1. 从设置页面复制安装链接。
2. 通过 SSH 连接到你选择的 Linux 机器。
3. 粘贴并执行安装命令。
4. 等待安装完成（通常为 2 到 3 分钟）。

步骤 4：连接源服务器

安装后，T AWS ransform 会识别属于当前浪潮的所有源服务器，并自动将它们连接到 MGN 连接器。

步骤 5：配置凭证

为您的源服务器凭据提供 S AWS ecrets Manager ARN。 AWS Transform 提供三个凭据配置选项：

- Linux 服务器的单一密钥 — 一个包含 SSH 密钥或所有 Linux 源服务器 username/password 的共享密钥。
- Windows 服务器的单一密钥 — 一个包含所有 Windows 源服务器的用户名和密码的共享密钥。
- 每台服务器有多个密钥 — 每台服务器或每组服务器都有不同的密钥。当服务器具有不同的凭据时，请使用此选项。 AWS Transform 会生成一个预先填充了您的服务器列表的 CSV 文件。您填写每台服务器的`secret_arn`列并上传已完成的文件。

> **Note**
>
> 如果两种服务器类型各有一个共享密钥，则可以组合使用 Linux 和 Windows 单密选项。每台服务器的密钥选项与单密选项是互斥的。

凭证密钥格式。要了解更多信息，请参阅 MGN 用户指南中的 MGN 连接器凭证：

```
{
  "WinConnectionProtocol": "HTTPS",
  "WinUserName": "windows_username",
  "WinPassword": "windows_password",
  "LinuxUserName": "linux_username",
  "LinuxPrivateKey": "linux_private_key",
  "LinuxHostKeyValidation": false
}
```

代理部署

配置并验证凭据后，Trans AWS form 会将复制代理部署到您的源服务器。您可以部署到当前浪潮中的所有服务器，也可以选择特定的服务器。

每台服务器的部署过程：

1. AWS 转换通过 SSM 向连接器发送部署命令。
2. 连接器从 S AWS ecrets Manager 检索凭证。
3. 连接器使用配置的凭据连接到源服务器。
4. 连接器验证源服务器是否满足运行复制代理所需的所有先决条件。
5. 连接器安装和配置复制代理。
6. 连接器可验证安装和连接是否成功。

您可以通过每台服务器的状态跟踪来实时监控部署进度，包括当前安装步骤、已用时间和预计剩余时间。如果有任何服务器出现故障，T AWS ransform 会显示失败原因并提供每台服务器的重试选项。成功部署的服务器可以在重试失败的服务器时独立运行。

连接器重用和生命周期

在为后续波浪部署代理时，您可以重复使用现有的连接器或创建新的连接器。 AWS Transform 列出了在您的账户中配置的所有连接器，显示连接器名称、状态（活动或已过期）、连接的服务器数量和混合激活到期日期。

- 活动连接器-混合激活仍然有效。 AWS Transform 会验证新浪潮的 IAM 角色并继续进行证书配置。无需新的混合激活。
- 连接器已过期-SSM 混合激活已过期。已过期的激活无法续订。必须选择其他连接器或创建新的连接器。

SSM 混合激活将在 30 天后过期。只有在 Linux 计算机上安装连接器时才需要激活。安装连接器后，即使激活到期，您也可以继续使用它在源服务器上安装复制代理。如果需要在激活到期后在新计算机上安装连接器，则需要通过安装过程创建一个新的连接器。

手动安装代理

要进行手动安装，首先要生成 AWS 凭据（临时或永久凭证），然后在每台源服务器上安装代理。

凭证选项：

- 临时证书（推荐）-使用`AWSApplicationMigrationAgentInstallationPolicy`托管策略创建 IAM 角色，然后使用`aws sts assume-role`该角色生成临时证书。要了解更多信息，请参阅 MGN 用户指南中的代理安装权限。
- 永久证书-使用`AWSApplicationMigrationAgentInstallationPolicy`托管策略创建 IAM 用户并生成访问密钥。

安装步骤：

对于 Linux 服务器，请下载并运行安装程序：

```
wget -O ./aws-replication-installer-init \
  https://aws-application-migration-service-region.s3.region.amazonaws.com/latest/
linux/aws-replication-installer-init
sudo chmod +x aws-replication-installer-init
sudo ./aws-replication-installer-init --region region --user-provided-id server-
identifier
```

对于 Windows 服务器，请使用管理员 PowerShell 身份下载并运行相应的安装程序：

```
Invoke-WebRequest -Uri "https://aws-application-migration-
service-region.s3.region.amazonaws.com/latest/windows/
AwsReplicationWindowsInstaller.exe" `
  -OutFile "C:\AwsReplicationWindowsInstaller.exe"
C:\AwsReplicationWindowsInstaller.exe --region region --user-provided-id server-
identifier
```

> **Important**
>
> `--user-provided-id` 参数是必需的。*`server-identifier`*替换为库存文件中该`mgn:server:user-provided-id`列的确切值。此标识符将物理服务器链接到其 MGN 源服务器记录。

有关代理安装的更多信息，请参阅 MGN 用户指南中的 Linux 代理和 Windows 代理。

安装后，T AWS ransform 会通过检查服务器的复制状态是否为`INITIATING`或`INITIAL_SYNC`来验证所有代理是否已成功连接。

> **Note**
>
> AWS 转换不支持 MGN 无代理复制。有关无代理复制的信息，请参阅 MGN 用户指南中的无代理复制概述。

> **Note**
>
> 您必须立即在所有服务器上安装复制代理。断开连接并存档未安装复制代理的服务器。您可以使用`disconnect-from-service`命令断开服务器连接，使用`mark-as-archived`命令存档已断开连接的服务器。存档命令仅适用于生命周期状态为的源服务器`DISCONNECTED`。

有关复制的配额，请参阅《MGN 用户指南》中的 MGN 服务配额限制。

步骤 4：数据复制

安装复制代理后，数据复制将自动开始。 AWS Transform 使用连续的块级复制将数据从源服务器同步到。 AWS

复制过程包括两个阶段：

- 初始同步-源服务器数据的完整副本 AWS。数据以亚马逊弹性块存储 (Amazon EBS) 快照的形式存储在目标账户的亚马逊 FSx NetApp for ONTAP（ ONTAP 的 FSx）卷上，具体取决于您配置的目标存储类型。有关更多信息，请参阅 MGN 用户指南中的目标存储类型。持续时间取决于数据量和网络带宽。

- 连续复制 — 持续同步已更改的数据块，对源服务器性能的影响最小。在中维护最新副本 AWS。

复制服务器是部署在暂存区域子网中的临时 Amazon EC2 实例。它们从源服务器接收复制的数据，并由 MGN 自动管理。要了解更多信息，请参阅 MGN 用户指南中的复制服务器设置。

AWS Transform 监控复制进度并提供状态更新，包括复制状态、复制延迟（源数据和复制数据之间的时间差）和带宽使用情况。

在复制过程中，每台服务器都将进入以下状态：

- 未就绪 — 服务器正在进行初始同步过程，尚未准备好进行测试。
- 已准备好进行测试 — 服务器已成功添加且数据复制已开始。现在可以启动测试或直接转换实例。

一旦浪潮中的所有服务器都已超出该NOT_READY状态，数据复制阶段就完成了，您可以继续进行测试了。

您可以随时控制单个服务器或整个浪潮的复制：

- 暂停复制-暂时暂停特定服务器或整个浪潮的复制。
- 恢复复制-恢复先前暂停的复制。
- 停止复制-永久停止复制。可以重新启动已停止的复制，但它从初始同步开始。

第 5 步：测试

数据复制完成后，您可以启动测试实例来验证迁移的服务器，然后再执行最终的直接转换。要了解更多信息，请参阅 MGN 用户指南中的启动测试实例。 AWS 转换支持两个测试选项：

- 全波测试 — 为浪潮中的所有服务器启动测试实例。
- 选择性测试-通过提供清单文件中用户提供的 ID，为您选择的特定服务器启动测试实例。

AWS Transform 从复制的数据启动 Amazon EC2 实例，并提供实例 ID，以便您可以连接和验证测试实例。测试完成后，您可以：

- 如果测试成功，则继续切换。
- 启动新的测试实例进行重新测试。
- 在重新测试之前，请终止测试实例并解决所有问题。

步骤 5b：将应用程序标记为已准备好进行切换

测试完成并且您对结果感到满意后，请将您的应用程序标记为已准备好进行切换。 AWS 在允许您继续操作之前，Transform 会查看每个应用程序的复制状态并解决所有复制警报。只有复制状态为干净的应用程序才能标记为直接转换。

第 6 步：切换

直接转换是您的生产工作负载迁移到的最后一个迁移步骤。 AWS要了解更多信息，请参阅 MGN 用户指南中的启动直接转换实例。与测试类似，Trans AWS form 支持特定服务器的全波切换或选择性切换。

在 AWS 转换期间，Transform 会从最新复制的数据启动 Amazon EC2 实例，并为每台服务器提供实例 ID。验证直接转换实例后，即可完成直接转换，这将停止正在进行的源计算机复制。

转换过程包括以下步骤：

1. 启动 AWS 转换实例 — Transform 为所选服务器启动 Amazon EC2 实例。您可以选择全波切换或选择性切换。
2. 验证直接转换实例 — C onnect 连接到已启动的实例并验证它们是否正常运行。
3. 完成直接转换-确认直接转换以停止源计算机复制。您可以最终确定浪潮中的所有服务器，也可以选择特定的服务器。完成操作会阻止复制代理发送数据，从源服务器上移除复制代理，并锁定服务器生命周期状态。此操作无法轻易撤消。要了解更多信息，请参阅《MGN 用户指南》中的 “完成切换”。
4. 存档源服务器（可选）-完成后，您可以将源服务器标记为已存档，以腾出账户中的源服务器配额。

> **Important**
>
> 完成直接转换将停止正在进行的源计算机复制。在最终确定之前，请确保您已经验证了您的直接转换实例。

> **Note**
>
> 停机时间发生在源代码关闭和切换实例可用性之间。相应地规划您的转换窗口。

服务器生命周期状态

在迁移过程中，每台服务器都会经历以下生命周期状态。要了解更多信息，请参阅 MGN 用户指南中的源服务器生命周期。

- 未就绪 — 服务器正在进行初始同步过程，尚未准备好进行测试。
- 已准备好进行测试 — 数据复制已启动，可以启动测试或直接转换实例。
- 测试进行中-当前正在启动测试实例。
- 准备好切换-服务器已经过测试并准备好进行切换。
- 正在@@ 进行直接转换-当前正在启动一个直接转换实例。
- 直接转换完成-服务器已切换。所有数据均已迁移到直接 AWS 转换实例。
- 已断开连接-服务器已与 MGN 断开连接。

在迁移过程中，您可以随时向 Trans AWS form 询问服务器的状态。 AWS Transform 提供了一个交互式波形状态表，其中显示了所有相关的服务器信息，包括迁移生命周期、复制状态和建议的后续步骤。你也可以用自然语言提问，例如：

- 我的服务器状态如何？
- 我的浪潮状态如何？
- 我目前所处步骤的状态如何？

在波次迁移期间，您可以让 T AWS ransform 更新或更改各个服务器的状态。例如，如果您的浪潮中 10 台服务器中有 9 台通过了测试阶段但有一台失败了，则可以允许 T AWS ransform 继续将 9 台服务器移至下一阶段，同时在失败的服务器上重新运行测试。

部署批准

某些迁移操作需要在执行之前获得明确的批准。当操作需要批准时，Trans AWS form 会通过 “批准” 选项卡将请求传送给授权的批准者。只有在 Trans AWS form 中具有管理员角色的用户才能批准部署请求。只有在收到确认后才会进行部署。

发布说明

以下发行说明涵盖了的最新更改迁移（包括 VMware）。有关支持的 AWS 转换区域，请参阅支持的区域。有关支持的目标区域，请参阅账户连接器设置页面。

2026 年 6 月

- AWS 迁移转换现在支持本地化。在处理迁移工作流程时，您可以更改 Web 应用程序的显示语言。了解有关语言设置的更多信息。
- AWS 现在，Transform 允许您配置复制设置和启动迁移设置。您可以根据目标账户或跨特定源服务器设置配置。了解有关复制和启动设置的更多信息。
- AWS 现在，Transform 允许您将现有的弹性网络接口 (ENI) 附加到启动模板。您可以在目标账户中标记 ENI，这样它们就可以在实例启动时使用。了解有关网络资源标记的更多信息。
- AWS Transform for Migrations 现在支持所有 AWS 商业区域作为迁移目标，不包括中东（巴林）和中东（阿联酋）。详细了解支持的目标区域。

2026 年 5 月

- AWS Transform 现在可以在网络迁移审查期间检测目标账户中的现有 VPC。您可以在映射的 VPC 旁边查看现有 VPC，识别 CIDR 冲突并在部署之前解决这些冲突。了解有关现有 VPC 检测的更多信息。
- AWS Transform 支持在迁移到容器期间将源代码存储库重新平台化为容器。 AWS了解有关容器化的更多信息。

2026 年 4 月

- 添加了直接在迁移工作流程中创建着陆区。 AWS 转换现有基金会的支票，推荐组织单位 (OU) 结构和目标客户，并提供自动部署或基础设施即代码 (IaC) 输出（CloudFormation AWS CDK、或着陆区加速器 (LZA) 格式）。详细了解如何创建着陆区。
- 在网络迁移期间添加了对带有安全组映射的 DHCP 的支持。了解有关创建安全组的更多信息。

2026 年 3 月

- 添加了用于网络迁移的公共 API，使合作伙伴和编程人员能够访问网络迁移功能。请参阅网络迁移 API 参考。

2026 年 2 月

- 网络迁移现在支持在不需要 R VTools 发现数据的情况下接收防火墙或 Software-Defined 网络 (SDN) 配置文件。您可以单独使用防火墙或 SDN 配置文件，也可以将它们与 RvTools 导出文件结合使用。

2026 年 1 月

- 增加了对网络迁移元素上的 Migration Acceleration Program (MAP) 标记和用户定义标签的支持，使您能够跟踪迁移资源以获得 MAP 积分和组织目的。

2025 年 12 月

- 通过重新设计的工作流程和改进的可用性，增加了全新的迁移体验。有关更多信息，请参阅加速 VMware 迁移： AWS 转型的新体验。
- 添加了着陆区加速器 (LZA) 网络配置，用于自动设置着陆区。
- 在迁移执行中增加了对多个目标 AWS 账户的支持，使您能够跨账户迁移工作负载。
- 增加了对思科 ACI、Palo Alto 和 ModelizeIT 源 FortiGate格式的网络迁移支持。

2025 年 10 月

- 新增亚太地区（大阪），将迁移执行范围扩大到16个目标地区。

2025 年 9 月

- 增加了对重新托管浪潮中的许可配置的支持，使您能够在每个版本中指定自带许可证 (BYOL) 或包含许可证的选项。
- 在网络迁移中添加了对 Terraform 的支持，使您能够使用 Terraform 模板部署网络基础架构。
- 增加了对更新复制子网配置的支持，取消了目标账户中默认 VPC 的要求。

2025 年 8 月

- 将迁移执行（网络迁移和重新托管）扩展到 15个目标地区，增加了美国东部（俄亥俄州）、欧洲（斯德哥尔摩）和欧洲（爱尔兰）。
- 为网络迁移添加了灵活的 CIDR 范围功能，使您能够在网络部署期间自定义 IP 地址范围。

2025 年 5 月

- 首次推出服务迁移（包括 VMware），提供端到端迁移功能，包括发现、评估、迁移规划、网络迁移和服务器重新托管。
- 支持在 12 个目标地区执行迁移：美国东部（弗吉尼亚北部）、美国西部（俄勒冈）、加拿大（中部）、南美洲（圣保罗）、欧洲（法兰克福）、欧洲（伦敦）、欧洲（巴黎）、亚太地区（孟买）、亚太地区（孟买）、亚太地区（首尔）、亚太地区（东京）、亚太地区（新加坡）和亚太地区（悉尼）。

源代码容器化

AWS Transform 支持在迁移到容器期间将应用程序重新平台化为容器。 AWS本章介绍了 Tr AWS ansform 用于自动实现源代码容器化的代理人工智能功能。您可以并行迁移和现代化，从而减少从本地架构迁移到云原生架构的时间和复杂性。你可以对来自 GitHub Bitbucket 或.zip 文件的源代码进行容器化 GitLab，生成 Docker 镜像，发布到亚马逊弹性容器注册表 (Amazon ECR)，然后部署到亚马逊弹性容器服务 (Amazon ECS) 或亚马逊弹性 Kubernetes 服务 (Amazon EKS)。这使容器化与您用于规划和执行重新托管迁移的工作流程相同。

> **Note**
>
> 源代码容器化专为尚未实现容器化的应用程序而设计。它需要访问您的应用程序源代码，并且不支持迁移现有的容器化工作负载。要将现有容器迁移到 AWS，请使用亚马逊弹性容器服务或亚马逊弹性 Kubernetes 服务的标准部署方法。

功能和关键特性

AWS Transform 提供了以下功能来实现应用程序的容器化。

- AI-driven 源代码分析-分析您的应用程序源代码并自动生成 Docker 工件，包括 Dockerfiles 和相关的配置文件。
- 容器映像构建和发布 — 使用 AI-driven Docker 版本构建和测试容器镜像，并通过自动漏洞扫描将其发布到 Amazon Elastic Container Registry。
- 基础设施即代码生成 — 通过自动验证和安全扫描，为亚马逊 Elastic Kubernetes Service（Helm 图表）或亚马逊弹性容器服务（Terraform 模块）生成部署基础设施。
- 私有依赖支持 — 您可以选择将 AWS CodeArtifact 存储库（Maven、PyPI、npm）和私有 Amazon ECR 基础映像配置为构建的依赖源。
- 迭代测试和直接转换部署 — 部署测试基础架构进行验证，然后部署最终确定的基础架构进行生产切换。

容器化的工作原理

AWS Transform 使用 AI-powered 代理在基于聊天的工作流程中指导您完成容器化过程。 AWS Transform 协调特殊任务，例如源代码分析、Docker 图像生成和基础架构创建。在工作流程的关键时刻，您需要审核并批准输出，然后再继续。

您可以通过创建 VMware 迁移任务来访问源代码容器化。在作业中，您可以将容器化作为独立工作流程运行，也可以在浪潮的迁移策略设置为容器化时作为端到端迁移的一部分运行。有关 VMware 迁移的更多信息，请参见迁移（包括 VMware）。

先决条件

在您开始之前，请确保您已拥有以下各项：

- 变 AWS 换工作区。有关获取工作空间的信息，请参阅入门。
- 您的应用程序源代码位于 Git 存储库中 AWS CodeConnections，可通过访问或打包为 zip 文件进行上传。单个文件不得超过 1 GB，所有源代码的总大小不得超过 8 GB。
- （可选）用于发布容器映像的 Amazon ECR 存储库。您可以在工作流程的稍后准备发布时配置 Amazon ECR 访问权限。
- 对于 Amazon EKS 部署：现有的 Amazon EKS 集群，或创建所需基础设施的权限。
- 对于 Amazon ECS 部署：使用 Terraform、或创建 Amazon ECS 集群 AWS CloudFormation、服务和相关资源的权限。 AWS Cloud Development Kit (AWS CDK)

容器化工作流程

容器化工作流程包括以下步骤。T AWS ransform 代理会引导你完成聊天界面的每个步骤。

1. the section called “步骤 1：安全免责声明”— 查看并接受安全免责声明。
2. the section called “第 2 步：克隆源代码”— 提供您的应用程序源代码。
3. the section called “第 3 步：容器化”— AI 代理会分析你的代码并生成 Docker 工件。
4. the section called “步骤 4：查看工件”— 查看生成的构件并批准代码更改。
5. the section called “第 5 步：发布图片”— 将容器映像发布到 Amazon ECR。
6. the section called “第 6 步：生成 IaC”— 生成 Amazon EKS 或 Amazon ECS 部署模板。
7. the section called “步骤 7：部署测试基础架构”— 部署和验证测试基础架构。
8. the section called “步骤 8：清理测试基础架构”— 拆除测试资源。
9. the section called “步骤 9：部署直接转换基础架构”— 部署生产基础架构。

启动容器化作业

要对应用程序进行容器化，您需要先在 Trans AWS form 工作空间中创建 VMware 迁移作业。在任务中，您可以选择运行独立的容器化工作流程或包括容器化的端到端迁移流程。

- 独立容器化 — 无需执行完整的 VMware 迁移，即可对源代码进行容器化。如果您想独立于任何基础设施迁移而对应用程序进行容器化，请选择此选项。
- End-to-end 使用容器化迁移 — 运行完整的 VMware 迁移工作流程，为一个或多个浪潮分配容器化迁移策略。容器化工作流程是这些浪潮迁移的一部分。有关 VMware 迁移的更多信息，请参见迁移（包括 VMware）。

启动容器化作业

1. 在工作空间登录页面上，选择创建作业。
2. 选择 VMware 迁移。
3. 选择是运行独立的容器化工作流程还是包括容器化的端到端迁移流程。
4. AWS 转换将引导您完成工作流程步骤，首先是the section called “步骤 1：安全免责声明”。

容器化权限

在容器化工作流程中，Trans AWS form 会向您部署一个 IAM 角色 AWS 账户 ，该角色用于构建容器镜像和部署基础设施。在工作流程继续之前，您需要审核并批准此角色的创建。

该角色已命名`AWSTransformCodeBuildExecutionRole`并通过 AWS CloudFormation 堆栈部署。它包括以下托管策略。

基本政策

为容器化工作流程提供核心权限：

- Amazon S3 — 读取和写入存储`aws-transform-*`桶中的对象
- Amazon ECR — 进行身份验证、提取映像（标有`Project: atx-migration`），并将图像推送到标有标签的存储库 `CreatedBy: AWSTransform`
- AWS CodeArtifact — 从标有标签的存储库中读取`Project: atx-migration`、列出存储库、获取授权令牌和读取存储库端点。这些权限支持在工作流程中配置的公共依赖关系解析和私有依赖关系源
- Amazon CloudWatch 日志 — 创建日志组和流，并为 Amazon ECS 日志组写入日志事件

- AWS KMS — 描述和解密密钥（范围限于 Amazon S3 通过服务条件）
- Amazon EC2 — 为 VPC-enabled项目创建和管理网络接口
- AWS CodeConnections — 使用连接通过配置的 CodeConnections ARN 访问源代码存储库

网络政策

管理已部署应用程序的网络资源：

- Elastic Load Balancing — 创建、描述和管理负载均衡器、目标组、侦听器和规则（标有）`CreatedBy: AWSTransform`
- Route 53 — 创建和管理托管区域和 DNS 记录
- AWS Cloud Map — 创建和管理用于服务发现的命名空间和服务（标有）`CreatedBy: AWSTransform`

存储策略

管理已部署应用程序的存储资源：

- Amazon S3 — 创建和管理存储桶，包括加密、版本控制、生命周期和访问策略
- Amazon EFS — 创建和管理文件系统、挂载目标和接入点（标有`CreatedBy: AWSTransform`）
- Amazon EBS — 创建和管理卷和快照（标有`CreatedBy: AWSTransform`）

AWS KMS policy

管理加密密钥操作：

- 描述密钥、列出别名并阅读密钥策略
- 加密、解密和生成数据密钥（范围为亚马逊日志、亚马逊 EFS CloudWatch 、亚马逊 EC2 和 Amazon S3 通过服务条件）

亚马逊 ECS 政策

管理用于容器部署的 Amazon 弹性容器服务资源：

- 创建和管理集群、服务和任务定义（标有`CreatedBy: AWSTransform`）

- 注册和取消注册任务定义、运行任务
- 将 IAM 角色传递给 Amazon ECS 任务和服务
- 阅读 IAM 角色信息和 ACM 证书
- 描述 Amazon EC2 VPC、子网、安全组和网络接口

亚马逊 EKS 政策

管理用于 Kubernetes 部署的亚马逊 Elastic Kubernetes 服务资源：

- 访问 Kubernetes API、描述集群并列出插件
- 将 IAM 角色传递给 Amazon EKS

> **Note**
>
> 所有权限的范围均限于您的 AWS 账户 和。 AWS 区域 Trans AWS form 创建的资源使用标记`CreatedBy: AWSTransform`，写入操作仅限于带有此标签的资源（如果适用）。

步骤 1：查看安全免责声明

在容器化工作流程开始之前，Transf AWS orm 会提供一份安全免责声明，您必须查看并接受该免责声明。

免责声明涵盖的内容

容器化过程需要访问互联网才能下载应用程序依赖项（例如来自 npm、PyPI 或 Maven Central 等公共注册表的包）。安全免责声明告知您：

- 构建环境将具有出站 Internet 访问权限，以解析和下载应用程序编译配置中指定的依赖关系。
- 您负责审查您的应用程序所需的依赖关系，并确保它们符合您组织的安全策略。
- 您可以选择在后续步骤中配置私有依赖项源（例如 AWS CodeArtifact 存储库或私有 Amazon ECR 基础映像），以避免从公共注册表下载。

您需要了解的内容

查看并接受安全免责声明

1. 阅读 Trans AWS form 提供的安全免责声明。
2. 接受免责声明以继续容器化工作流程。

接受免责声明后，T AWS ransform 会继续执行下一步，即您提供源代码。

> **Note**
>
> 不再需要预先配置 AWS CodeConnections 和 Amazon ECR 的连接器。 AWS 只有在需要时，Transform 才会提示您稍后在工作流程中配置对这些服务的访问权限。例如，您可以配置 CodeConnections 何时选择从 Git 存储库进行克隆，并在准备发布容器映像时配置 Amazon ECR 访问权限。

第 2 步：克隆源代码

在此步骤中，您将向 Transform 提供您的应用程序源 AWS 代码。您可以从 Git 存储库或通过上传 zip 文件来提供源代码。

选项 1：Git 存储库

您可以从 Git 存储库中提供源代码。如果您尚未配置 AWS CodeConnections，此时 AWS 转换会提示您提供 CodeConnections ARN。您可以通过两种方式来指定存储库：

- 上传 CSV 文件-准备包含列`repo_name`和的 CSV 文件`branch`。`repo_name`必须是`owner/repo-name`格式化的。该`branch`列是可选的；将其留空即可使用存储库的默认分支。示例：

```
repo_name,branch
owner/my-app,main
owner/api-service,develop
owner/another-repo,
```

- 在聊天@@ 中提供存储库详细信息 — 直接在聊天中告诉 Trans AWS form 存储库名称和分支，而不是上传 CSV。

AWS Transform 会验证每个存储库是否存在且可通过您的 CodeConnections 配置进行访问，然后克隆存储库。

> **Note**
>
> 单个文件不得超过 1 GB，所有存储库的总大小不得超过 8 GB。 AWS 同时转换克隆多个存储库以加快处理速度。

> **Important**
>
> Git clone 选项不支持跨多个存储库的应用程序。如果您的应用程序需要来自多个存储库的源代码，请将它们打包成一个 zip 文件，然后改用 zip 上传选项。

选项 2：上传 Zip 文件

如果您没有配置 CodeConnections，或者更喜欢直接上传源代码，则可以上传 zip 文件。

将源代码作为 zip 文件上传

1. 出现提示时，为每个应用程序上传一个 zip 文件。您可以将文件拖到聊天中或使用附件按钮。
2. 每个 zip 文件都应包含一个应用程序的源代码。
3. 单个文件不得超过 1 GB，所有上传的总大小不得超过 8 GB。

可选：配置私有依赖关系

如果您的应用程序依赖私有注册表中的包，则可以在此步骤中配置私有依赖源。 AWS Transform 支持以下私有依赖项类型：

- AWS CodeArtifact 存储库 — 配置托管在中的 Maven、PyPI 或 npm 存储库。 AWS CodeArtifact AWS Transform 会显示您账户中可用存储库的列表供您选择。
- 私有 Amazon ECR 基础映像 — 如果您的 Dockerfiles 使用私有 Amazon ECR 存储库中的基础映像，请提供存储库详细信息，以便构建环境可以提取这些映像。

配置私有依赖关系时，T AWS ransform 会提示您连接到托管这些资源 AWS 账户 的地方。仅当您使用私有依赖项时，才需要配置此连接器。

确认容器化首选项

源代码可用后，Trans AWS form 会询问您是否有关于如何完成容器化的具体说明。您可以选择指定：

- 是生成新的 Dockerfile 还是重复使用现有的 Dockerfile。
- 是在 monorepo 中处理特定服务，还是处理所有服务。
- 容器化过程的任何其他偏好。

默认值为：

1. 使用亚马逊 Linux 2023 基础镜像 (`public.ecr.aws/amazonlinux/amazonlinux:latest`)。
2. 处理存储库中的所有应用程序。
3. 重复使用现有的 Dockerfile（如果有），如果需要，可以稍作修改。

您可以确认继续使用默认设置，也可以提供具体说明。

第 3 步：容器化

在此步骤中，Trans AWS form AI 代理会分析您的应用程序源代码并生成 Docker 工件。 AWS Transform 会检查应用程序的结构、依赖关系和运行时要求，以生成相应的 Dockerfile 和相关的配置文件。

容器化期间会发生什么

容器化代理执行以下任务：

1. 源代码分析 — T AWS ransform 会检查应用程序的项目文件、依赖关系、构建配置和运行时要求。AWS 转换还会替换硬编码的值（例如数据库 IP 地址或 DNS 名称），识别环境变量，检测卷并尝试将日志重定向到标准输出。
2. 生成 Dockerfile — 根据分析，Transf AWS orm 会生成一个为您的应用程序量身定制的 Dockerfile。
3. 容器映像构建和测试 — T AWS ransform 生成容器镜像并运行测试以验证 Dockerfile 是否生成了有效的映像。如果构建失败，Transf AWS orm 会自动迭代 Dockerfile。
4. 安全分析 — T AWS ransform 会扫描生成的工件以查找硬编码值，例如凭证、API 密钥或其他敏感数据，并标记任何发现供您查看。

如果您提供了多个存储库或包含多个服务的 monorepo，则会并行处理每项服务。

支持的应用程序类型

AWS Transform 支持对以下应用程序类型进行容器化：

- .NET 7 及更高版本-针对在版本 7 或更高版本上运行的.NET 应用程序优化了容器化。
- 通用应用程序 — 适用于使用任何语言或框架构建的应用程序的容器化，包括 Java、Python Node.js、Go 等。
- 不支持的应用程序 — 不支持 Windows、Xcode 或任何专有编译环境。

您需要了解的内容

此步骤将自动运行。 AWS Transform 在分析和容器化每个应用程序时会显示进度更新。如果 AWS Transform 遇到问题，它可能会要求您进行澄清或提供更多信息。

容器化完成后，Trans AWS form 将移至下一步，您可以在其中查看生成的工件。输出保存在Artifactic Store中。

第 4 步：查看 Docker 工件和代码更改

在此步骤中，您将查看 Transform 在容器 AWS 化期间生成的 Docker 工件和代码更改。

查看 Git 存储库中的更改

如果您提供了来自 Git 存储库的源代码，Tr AWS ansform 会将容器化更改提交到每个仓库中的新分支。如果您有多个存储库，Trans AWS form 会将所有更改作为批量显示以供合并审阅。

查看和批准更改

1. 查看 Transf AWS orm 提供的代码差异链接。每个差异都会显示所有已添加或修改的文件，包括 Dockerfiles、配置文件和任何源代码更改。
2. 当 T AWS ransform 显示批准对话框时，请批准或拒绝更改。对于多个存储库，您可以在单个批处理操作中批准所有更改。
3. 如果您同意，T AWS ransform 会将更改推送到仓库中的新分支。
4. 确认您已准备好继续下一步。

查看 zip 上传后的更改

如果您 AWS 将源代码作为 zip 文件上传，Transform 会提供容器化工件的下载链接。下载并查看工件，其中包括生成的 Dockerfiles 和任何源代码修改。

请求更改

如果生成的构件需要修改，则可以向 Tr AWS ansform 提供反馈，使用更新的说明重新启动容器化步骤，并生成新的构件供您查看。

第 5 步：发布图片

在此步骤中，Trans AWS form 会将您的容器镜像发布到 Amazon 弹性容器注册表。如果您尚未配置 Amazon ECR 访问权限，此时 Trans AWS form 会提示您提供您的 Amazon ECR 存储库详细信息。

发布期间会发生什么

AWS Transform 会为每个容器镜像执行以下任务：

1. 连接器配置 — 如果您尚未配置 Amazon ECR 访问权限，Tr AWS ansform 会显示一个连接器表单，您可以在其中提供您的 Amazon ECR 存储库 ARN 并连接到您的。 AWS 账户
2. 批准请求 — T AWS ransform 会显示要发布的图像列表并请求您的批准。您可以批准或拒绝发布操作。
3. 图片推送 — 获得批准后，Tr AWS ansform 会使用将容器映像发布到您的 Amazon ECR 存储库。如果您有多个服务，Trans AWS form 会通过一次批处理操作发布所有图像。
4. 漏洞扫描 — Amazon ECR 会自动扫描已发布的图像中是否存在已知漏洞。 AWS 转换报告扫描结果。要进行更全面的分析，请启用 AWS ECR 增强型扫描和 AWS GuardDuty 运行时监控。

> **Note**
>
> 图像发布使用异步运行。如果您的会话在发布期间中断，T AWS ransform 会在您重新连接时自动恢复操作。

您需要了解的内容

- 查看要发布的图像列表。

- 批准或拒绝发布操作。如果您拒绝，T AWS ransform 将跳过图像发布，您可以在不发布图像的情况下继续执行下一步操作。
- 发布完成后查看漏洞扫描结果。

发布后，Tr AWS ansform 会提供基础设施部署步骤中使用的图像 URI。

步骤 6：以代码形式生成基础架构

在此步骤中，Trans AWS form 会生成用于部署容器化应用程序 AWS 的基础架构模板。您可以选择亚马逊 Elastic Kubernetes Service 和亚马逊弹性容器服务作为目标平台。

亚马逊 Elastic Kubernetes Service（Kubernetes）

如果你选择 Amazon EKS，T AWS ransform 会为你的应用程序生成包含 Kubernetes 清单的 Helm 图表。生成的模板包括：

- 部署和服务
- 入口规则
- ConfigMaps 和 SecretProviderClass 资源
- 服务账户
- 永久卷声明（EBS 和 EFS）
- Route 53 的 DNS 记录
- Health 检查配置

可选： CloudWatch 日志

AWS Transform 会询问您是否要为自己的 Amazon EKS 部署添加 CloudWatch 日志记录。如果你选择加入，Trans AWS form 会生成 Fluent Bit DaemonSet 配置，用于收集 pod 日志并将其发送到 CloudWatch 日志。

如果您选择 CloudWatch 日志记录，则您的集群管理员在部署之前必须满足以下先决条件：

1. 在集群中创建`amazon-cloudwatch`命名空间。
2. 为具有 CloudWatch 日志写入权限的 Fluent Bit 服务账户创建一个 IAM 角色。在部署期间，系统会提示您输入角色 ARN。

亚马逊弹性容器服务 (Terraform)

如果你选择 Amazon ECS，Trans AWS form 会生成用于部署应用程序的 Terraform 模块。生成的模板包括：

- ECS 集群
- 带有任务定义的 ECS 服务
- 带有访问日志功能的 Application Load Balan
- 用于永久存储的 Amazon EFS
- 用于服务发现的私有托管区域
- Health 检查配置

自动验证和安全扫描

AWS Transform 会自动验证生成的基础架构模板，然后再将其呈现给您。验证包括：

- 对于 Terraform：`terraform fmtterraform validate`并检查语法和配置的正确性。
- 对于 Helm：进行图表验证，以验证生成的清单格式是否正确。
- 使用Checkov进行安全扫描，以识别生成的基础设施代码中潜在的安全错误配置。

AWS Transform 会报告任何验证问题并在继续操作之前解决这些问题。

在没有已发布图像的情况下生成 IaC

即使您在上一步中没有发布容器镜像，也可以生成基础设施模板。生成的模板使用占位符图像 URI，您可以稍后使用实际图像位置对其进行更新。

您需要了解的内容

生成基础架构模板

1. 出现提示时，选择您的目标平台：Amazon EK S 或 A mazon ECS。
2. 如果您选择了 Amazon EKS，T AWS ransform 会询问是否包含 CloudWatch 日志记录。回答 “是” 或 “否”。
3. 如果出现提示，请提供应用程序的运行状况检查端点详细信息（例如`/health`路径）。

4. AWS Transform 会生成并验证基础架构模板。此步骤会自动运行，T AWS ransform 会显示进度更新，包括所有验证或安全扫描结果。
5. 当 Transfor AWS m 呈现生成的模板时，请查看它们。

步骤 7：部署测试基础架构

在此步骤中，Trans AWS form 部署了测试基础架构，以便您可以在生产转换之前验证您的容器化应用程序。

测试部署期间会发生什么

AWS Transform 会将上一步中生成的基础架构模板部署到您的 AWS 账户。对于 Amazon EKS 部署，这使用 Helm。对于亚马逊 ECS 部署，这使用 Terraform。

在部署之前，T AWS ransform 会显示一个基础架构值表单，您可以在其中配置部署参数，例如资源名称、副本计数和特定于环境的设置。 AWS Transform 还会生成部署预览，显示将创建哪些资源，因此您可以在批准之前查看更改。

您需要了解的内容

部署和验证测试基础架构

1. 使用您的部署配置填写基础架构价值表。该表单包括集群名称、命名空间、副本计数和其他特定于环境的设置等参数。
2. 查看显示将要创建或修改的资源的部署预览。
3. 在 Trans AWS form 请求时批准基础架构部署。
4. 等待部署完成。 AWS 转换显示部署结果。
5. 测试已部署的应用程序，以验证它是否在容器中正常运行，以及基础架构是否符合您的要求。
6. 告诉 AWS Transform 您是否对部署感到满意，或者是否要修改基础架构并重新部署。

对基础架构进行迭代

如果您需要修改基础架构模板，可以上传更新的模板并重新部署：

1. 告诉 T AWS ransform 你想修改 IaC。
2. 上传包含您修改过的基础架构模板的 zip 文件。

3. AWS Transform 会替换模板并执行增量更新（Terraform 应用或 Helm 升级）。
4. 查看更新的部署结果。

您可以重复此周期，直到您对部署感到满意为止。

会话恢复

基础架构部署使用异步运行。如果您的会话在部署期间中断，T AWS ransform 会在您重新连接时自动恢复操作并显示部署结果。

步骤 8：清理测试基础架构

完成验证后，Trans AWS form 会拆除测试基础架构，以避免不必要的成本。

您需要了解的内容

清理测试基础架构

1. AWS Transform 会通知您测试基础架构将被拆除。
2. 在 Trans AWS form 请求销毁操作时批准销毁操作。
3. 等待清理完成。 AWS 转换显示移除所有测试资源后的结果。

对于 Amazon ECS 部署，此步骤将删除测试部署期间创建的所有资源，包括计算资源、负载均衡器、存储和联网组件。

对于 Amazon EKS 部署，清理范围按标签限定到您的特定项目。只有为此容器化工作流程标记的资源才会被移除。在同一 Amazon EKS 集群上运行的其他工作负载不受影响。

步骤 9：部署直接转换基础架构

在最后一步中，Tr AWS ansform 部署最终的基础架构以供生产使用。直接转换部署使用的基础设施模板与您在测试部署步骤中验证的模板相同。

您需要了解的内容

部署直接转换基础架构

1. 使用您的生产部署配置填写基础架构价值表。您可以调整测试部署中的参数或使用相同的值。

2. 查看显示将要创建的生产资源的部署预览。
3. 在 Trans AWS form 请求时批准生产部署。
4. 等待部署完成。 AWS 转换显示直接转换部署结果。
5. 验证您的应用程序在生产环境中是否正常运行。

> **Important**
>
> 与您的团队一起审查生成的基础架构配置，确保它们符合您组织的安全、合规和业务需求。虽然 T AWS ransform 提供自动配置建议，但在继续进行直接转换部署之前，您需要负责验证和调整设置以满足您的需求。

会话恢复

生产部署使用异步运行。如果您的会话在部署期间中断，T AWS ransform 会在您重新连接时自动恢复操作并显示部署结果。

大型机应用程序的现代化

AWS Transform 旨在加快传统大型机应用程序的现代化。它协调对大型机代码库的分析，生成文档，提取业务逻辑，分解整体结构，转换遗留代码，并在需要时使用人工输入 (HITL) 管理整个旅程。Trans AWS form 用于现代化和迁移大型机应用程序的转型功能使您能够更快地实现关键大型机应用程序的现代化，同时在整个转型过程中保留关键业务逻辑。

主题

功能和关键特性

AWS Transform 为大型机现代化提供了以下功能：

- 支持以 COBOL（通用 Business-Oriented 语言）和 PL/I （编程语言一）编写 z/OS 的大型机应用程序以及相关的 JCL（作业控制语言）、CICS（客户信息控制系统）事务、BMS（基本映射支持）屏幕、Db2 数据库和 VSAM（虚拟存储访问方法）数据文件进行现代化。
- 支持使用 PSAM（演示服务访问方法）、日语字符集和 NDB（网络数据库）数据文件重构富士通 GS21 大型机应用程序。
- 执行目标驱动的推理、分析、分解、规划、文档生成和代码重构。
- 自动将 COBOL-based 大型机工作负载重构为经过云优化的现代 Java 应用程序。
- 编排并与执行分析、文档、分解、规划和代码重构的底层工具无缝集成。
- 通过提供即用型基础设施即代码 (IaC) 模板，帮助您为现代化大型机应用程序设置云环境。

High-level 演练

以下是 Trans AWS form 的高级演练，用于实现大型机应用程序的现代化和迁移。

1. 使用 Transf AWS orm 开始聊天，然后输入目标。
2. 根据您的目标，T AWS ransform提出了一个现代化计划——将高级目标分解为中间步骤。
3. 根据您提供的目标，Trans AWS form 可以：
   - 评估和重新构想代码库
   - 根据目标创建自定义作业

在此过程中，T AWS ransform 可能会要求您提供信息以执行任务。

> **Note**
>
> 有关大型机 AWS 变换重构功能的更多信息，请参阅大型机重构 AWS 转换文档中的创建项目。

Human in the Loop (HITL)

在大型机应用程序的整个转换过程中，您可以通过 Transf AWS orm Web 体验监控转换任务的进度和状态。

AWS 在以下情况下，Transform 将从您那里收集其他信息：

- 当需要其他信息来执行任务时。
- 当中间工件（例如，域分解或波浪规划）需要批准时。
- 当出现 AWS 转换无法自动解决的问题时。

支持的大型机应用程序转换文件类型

支持的文件类型 z/OS 包括：

- COBOL 工件和相关的 CPY（副本）
- PL/I 源文件
- JCL（作业控制语言）和 JCL 程序（PROC）

- CICS 系统定义 (CSD)
- BMS（基础映射支持）
- Db2 数据库
- VSAM（虚拟存储访问方法）
- IMS TM（交易管理器）

富士通 GS21 支持的文件类型包括：

- PSAM（演示服务访问方法）
- ADL（AIM 定义语言）
- NDB（网络数据库）

有关 Fujitsu GS21 的更多信息，请参阅大型机AWS 转型迁移指南中的以下主题：

- GS21
- 捕捉和重播-GS21 终端
- 大型机、AS400、Open VMS 和 GS21

支持的区域和配额 AWS 改造大型机

有关支持区域的列表，请参阅支持的区域 AWS Transform。

> **Note**
>
> 您的数据可能在与您使用 AWS 转换的区域不同的区域进行处理。有关跨区域处理的信息，请参阅the section called “Cross-region 处理”。

有关配额限制，请参阅配额。

High-level 大型机现代化之旅概述

大型机应用程序的现代化 AWS 通常分四个阶段实现：(a) 评估，(b) 移动化，(c) 迁移和现代化，以及 (d) 运营、优化和创新。详细描述了每个阶段，并附有目标和相关活动，以支持您的现代化之旅。

阶段

第 1 阶段：评估

目标：了解您的现代化准备情况并制定初步的现代化计划。

借助 Tr AWS ansform，您可以评估您的大型机应用程序、基础架构和运营，以确定满足业务需求的正确现代化方法。

> **Note**
>
> 每个阶段都包含一份清单，列出了在对大型机应用程序进行现代化改造时可以进行的所有可能的活动。你可以跳过一些与你的用例或目标不一致的活动。

活动

- 从关于现代化的非正式对话开始，然后通过让合适的人进入会议室来研究机会资格
- 确定机会资格
- 使用应用程序依赖关系映射计划和应用程序架构进行首次通话演示
- 确定 ROM（粗略数量级），包括迁移期间的基础架构成本、迁移人力、后期制作成本、项目持续时间
- 快速投资组合检测：
  - 执行模式和工具指导评估
  - 进行源代码分析
  - 确定概念验证 (POC) 候选人
- 创建技术支持培训：
  - 沉浸式日子
  - 带有一般主题的研讨会
- 为大型主机现代化项目或新客户创建迁移准备情况评估 (MRA) 报告 AWS
- 为动员阶段创建工作说明书

第 2 阶段：动员

目标：通过成功的概念验证或试点现代化来建立基础并验证方法。

在移动阶段，您可以建立必要的框架、工具和流程，以支持大规模的大型机现代化。

活动

- 通过试点和确定的 POC 来启动现代化计划：
  - 分析试点并设置现代化代码
  - 构建和测试试点现代化数据
  - 交付结果并审查试点计划，为更大规模的数据现代化创建详细的解决方案
- 对于平台：
  - 制定安全、合规和监控计划
  - 使用 AWS 大型机着陆区和账户结构设置着陆区环境
  - 确定架构、基础架构、应用程序、集成等
- 想想人员和流程：
  - 云卓越中心是一个很好的资源
  - 操作模型
- 针对不同的应用场景创建全面的投资组合分析：
  - 全面发现，包括高级文档
  - 分解计划（适用于所有应用程序）
  - 适用于所有应用的模式和刀具指南
  - 制定初步的现代化和迁移计划
- 考虑试点、平台、人员和流程以及全面的投资组合分析，制定详细的解决方案
- 确定商业案例
- 成功完成试运行，为下一阶段的工作说明书提供解决方案

第 3 阶段：迁移和现代化

目标：在计划的时间表和预算内完成现代化和迁移。

在此阶段，您可以将大型机应用程序和数据迁移到并对其进行现代化改造。 AWS

活动

- 为生产就绪的应用程序代码分配资源
- 使用现有文档或采访主题专家 (SME) 来审查和分析设计
- 定义测试场景
- 使用适当的运行时、数据库和第三方软件设置现代化环境
- 迁移源代码和数据并对其进行现代化改造：
  - 您可以根据应用程序代码库中的业务领域对应用程序进行迭代现代化
  - 根据需要扩展现代化环境以支持您的现代化工作负载
- 建立 CI/CD （持续集成、持续交付）管道
- 迁移选定的工作负载以启动现代化改造。
- 根据需要传输应用程序并调整环境缩放比例：
  - 您可以根据需要向上或向下扩展环境
  - 通过运行代码健全性测试对工作包进行现代化改造
  - 必要时与源代码重新同步
- 运行全面测试并验证您的迁移：
  - 收集初始状态数据
  - 在大型机上记录测试场景
  - 舞台环境、应用程序和数据
  - 在云上执行测试场景
  - 比较源测试结果和目标测试结果
  - 构建自动测试场景执行管道
  - 生成 KPI 和报告
- 验证您的数据以进行生产设置
- 通过以下方式验证您的进度：
  - 运行集成和系统测试
  - 运行性能测试
  - 正在运行用户验收测试
  - 正在运行 HA/DR 测试
- 与应用程序所有者一起制定推出计划，并制定培训和知识转移计划
- 考虑切换并执行生产切换

- 为后期制作活动（例如运营、监控、能力规划和应用程序功能保修）建立持续支持

第 4 阶段：运营、优化和创新

目标：支持卓越运营和现代化应用程序的持续改进。

现代化后，您可以优化应用程序的性能、安全性和成本，同时利用 AWS 服务进行创新。

活动

- 监控应用程序：
  - 性能指标
  - 安全实践
  - 合规指南
  - 成本
- 日志详情
- 管理应用程序操作：
  - 基础设施管理
  - 交易和任务管理
  - 运行时环境支持
- 应用程序优化和现代化
- 应用程序开发和维护：
  - 编程集成开发环境
  - 构建
  - 集成
  - 测试
  - 部署

大型机应用程序的转型

AWS Transform 可加速大型机现代化应用程序的转型。本主题描述了可用功能。

主题

- 先决条件：在 S3 中准备项目输入

- 大型机源文物集合
- Sign-in 并创造一份工作
- 跟踪转换进度
- 设置连接器
- 评估和重新构想工作计划
- 重新构想工作计划
- 自定义工作计划

先决条件：在 S3 中准备项目输入

AWS Transform 能够处理复杂的大型机代码库。要使用代码库，请确保将所有资产都放在您的 S3 位置。

关键项目投入：

- 源代码：您必须将大型机源代码文件上传到 S3。这包括 COBOL 程序、JCL 脚本、抄本和任何其他相关的源文件。
- 数据文件：如果您有大型机应用程序使用的任何 VSAM 文件或其他数据文件，则需要将其上传到 S3。
- 配置文件：包括特定于您的大型机环境的配置文件。

其他项目投入

- 系统管理工具 (SMF) 记录：如果适用，请将 SMF 记录上传到存储源代码的 S3 存储桶中的新文件夹，这些记录应采用.zip 文件格式。
- 格式：要生成技术文档，您可以利用可选的配置文件生成符合所需格式和标准的 PDF 文档，包括页眉、页脚、徽标和自定义信息。
- 词汇表：T AWS r AWS ansform Transform 利用自动化和生成式 AI 来生成文档和提取业务规则。在 zip 文件的根目录中加入包含重要缩写和术语信息的词汇表 CSV 文件将有助于提高生成的文档质量。
- 测试数据：如果有，请上传可用于验证现代化应用程序的测试数据集。这些数据应存储在存储源代码的 S3 存储桶中的新文件夹中。

有关项目投入的详细信息可以在这里找到。

大型机源文物集合

本主题概述了使用 AWS Transform 收集大型机源代码和相关工件以支持大型机现代化计划的过程。正确收集和准备源文物对于成功的分析、迁移规划和实施至关重要。

源代码清单

应用程序源代码类型

支持以下应用程序源代码类型：

- COBOL 计划
- JCL 脚本
- 汇编程序
- PL/I 节目
- CICS 交易
- 自然节目
- REXX 脚本
- Easytrieve 程序
- 复印本和内含
- Proc 库

数据库资产

支持以下数据库资产：

- DB2 DCLGEN 和 DDL 脚本
- IMS 数据库定义（PSB 和 DBD）
- VSAM 文件定义
- 物理和逻辑数据库架构
- 数据库过程和触发器

源代码文件扩展名

如果您不确定扩展名，请将其保留为空白或.txt，然后 Transfor AWS m 会为您对其进行分类。

下表列出了大型机源构件的常用文件扩展名。

大型机源代码文件扩展名

Language/Type	常用扩展	说明
COBOL	.cbl、.cob、.cobol	COBOL 源程序
JCL	.jcl	Job 控制语言脚本
汇编器	.asm	汇编语言程序
PL/I	.pl1	PL/I 语言节目
CICS 的定义	.csd	CICS 系统定义 (CSD)
天然	.nat	自然节目
REXX	.rex、.rexx	REXX 脚本
Easytrive	.ezt	Easytrieve 举报程序
抄本	.cpy	COBOL 字帖
BMS	.bms	基础映射支持 (BMS)
PL/I 字帖	.pl1_copy	PL/I 字帖
Db2 DCLGEN	.dcl	Db2 声明生成器
Db2 的定义	.sql、.ddl	Db2 数据库定义
IMS 定义	.ims	IMS 资源定义数据集（IMS 第 1 阶段）
MFS	.mfs	IMS MFS（消息格式服务）
PSB	.psb	IMS PSB（程序规格模块）
DBD	.dbd	IMS 数据库定义
JCL Proc	.prc、.proc	JCL 过程库
JCL 包括	.inc	JCL 包含文件

Language/Type	常用扩展	说明
宏	.mac	汇编器宏
控制卡	.ctl	JCL 实用控制卡

收集方法

源代码提取

使用安全 FTP 客户端 (WinSCP/FileZilla) 从大型机 PDS 库中提取交互式源代码。

DB2 架构提取

DB2 LUW（Linux、UNIX 和 Windows）客户机软件将该db2look实用程序作为其安装包的一部分。该db2look实用程序从 DB2 数据库中提取 DDL（数据定义语言）语句。

运行以下命令：

```
db2look -d DATABASE_NAME -i userid -w password -a -e -m -l -x -f -createdb -printdbcfg
 -o DATABASE_NAME.sql
```

以下列表描述了参数：

- `-d DATABASE_NAME`：指定要从中提取架构的数据库的名称
- `-i userid`: 用于数据库身份验证的用户 ID
- `-w password`: 数据库身份验证的密码
- `-a`: 提取授权信息（授权）
- `-e`：提取所有数据库对象（表、视图、索引等）
- `-m`: 提取统计数据和物理特征
- `-l`: 提取表格和列注释
- `-x`: 数据提取解释表
- `-f`: 格式化输出以提高可读性
- `-createdb`：包括数据库创建语句
- `-printdbcfg`：包括数据库配置参数

- `-o DATABASE_NAME.sql`：指定输出文件名

从大型机中提取目录信息

IDCAMS 中的 LISTCAT 命令是一种用于检索有关大型机上数据集的目录信息的实用程序。在大型机现代化项目中，这对于清点数据集并了解其特征非常有用。

```
//LSTCATJ JOB 'LISTCAT',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//STEP1 EXEC PGM=IDCAMS
//*
//SYSPRINT DD DSN=AWS.M2.CATALOG.LIST,
//            DISP=(NEW,CATLG,DELETE),
//            SPACE=(CYL,(1,1),RLSE),
//            DCB=(RECFM=FBA,LRECL=133,BLKSIZE=0)
//*
//SYSIN DD *
  LISTCAT ENT('AWS.M2.CARDDEMO.*') ALL
  LISTCAT ENT('SYS1.*') ALL
/*
```

提取 CICS 定义

IBM-provided DFHCSDUP 实用程序可以从 CICS 系统定义 (CSD) 文件中提取 CICS 资源定义。

使用以下 JCL 从 DFHCSD 中卸载现有定义：

```
//CSDEXTJ JOB 'EXTRACT CSD',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//STEP1 EXEC PGM=DFHCSDUP,REGION=0M,
//          PARM='CSD(READONLY),PAGESIZE(60),NOCOMPAT'
//*
//STEPLIB  DD DSN=your-hlq.SDFHLOAD,DISP=SHR
//DFHCSD   DD DSN=your-hlq.DFHCSD,DISP=SHR
//*
//CBDOUT   DD DSN=your-hlq.CSD,
//            DISP=(NEW,CATLG,DELETE),
//            SPACE=(CYL,(1,1),RLSE),
//            DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
  EXTRACT GROUP(cics-group) USERPROGRAM(DFH0CBDC) OBJECTS
```

```
/*
```

提取 IMS 定义

要提取 IMS 定义，您可以使用 DFSURDD0 实用程序生成 IMS 事务文件。此实用程序创建了可用于迁移目的的第 1 阶段宏语句。目前仅支持 IMS 第 1 阶段。

使用以下 JCL 提取 IMS 定义：

```
//IMSEXTJ JOB 'IMS STAGE 1',CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//*
//STEP1 EXEC PGM=DFSURDD0,MEMLIMIT=12G
//*
//STEPLIB  DD DISP=SHR,DSN=your-hlq.SDFSRESL
//*
//RDDSDSN DD DISP=SHR,DSN=your-rdds
//*
//SYSOUT   DD DSN=your-hlq.STAGE1.IMS,
//            DISP=(NEW,CATLG,DELETE),
//            SPACE=(CYL,(1,1),RLSE),
//            DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
  OUTPUT=MAC
/*
```

正在提取 CA-7 调度器信息

CA-7 工作计划信息包含在 LJOB 报告中。使用带LIST=NODD参数的 LJOB 实用程序在大型机上生成报告。报告必须有.ca7扩展名。每份报告的第 1 列中必须有 ANSI 回车控制字符。通过在用于运行 LJOB 实用程序的 JCL 中指定DCB=RECFM=FBA（或 FA），可以创建第 1 列中包含回车控制字符的报告。

例如：LJOB,JOB=ZBN*,LIST=ALL

有关更多信息，请参阅 Broadcom 文档。

正在提取 SMF 数据

系统管理工具 (SMF) 记录提供了 Transfor AWS m 用来分析批处理作业和 CICS 事务使用情况的活动指标。支持以下 SMF 记录类型：14、15、30（子类型 5）、64、102、110（数据类别为 1、3 和 4 的子类型 1）。

SMF 记录的格式要求：

- 必须包括记录类型 30 和 110（至少）
- 必须采用原始二进制 EBCDIC 格式，并包含 RDW（记录描述符 Word）字节
- 必须作为以下内容之一提供：
  - 以.zip 格式压缩的最大 600 MB 的文件
  - 以.tar.gz 或.gz 格式压缩的最大 5 GB 的文件
- 必须存储在与 Amazon S3 中的源代码不同的文件夹中

提供至少 13 个月的 SMF 记录，以捕捉较短的时间范围可能会错过的年度批次周期和季节性模式。

选项 1：提取和排序 SMF 记录

使用以下示例 JCL 提取和排序 SMF 记录：

```
//SMFEXTR  JOB (ACCT),'EXTRACT SMF',CLASS=A,
//             MSGCLASS=X,NOTIFY=&SYSUID
//*--------------------------------------------------------------------*
//* SMF RECORD EXTRACTION TEMPLATE
//* CUSTOMIZE: Job card, dataset names, date range, record types
//*--------------------------------------------------------------------*
//*
//* STEP 1: EXTRACT SMF RECORDS
//*
//EXTRACT  EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//*
//* INPUT: Specify your SMF datasets (MAN files or GDG)
//*
//DUMPIN   DD DISP=SHR,DSN=SYS1.MAN1
//         DD DISP=SHR,DSN=SYS1.MAN2
//         DD DISP=SHR,DSN=SYS1.MAN3
//*
//* OUTPUT: Extracted SMF records
//*
//DUMPOUT  DD DSN=your.hlq.SMF.EXTRACT,
//            DISP=(NEW,CATLG,DELETE),
//            UNIT=SYSDA,
//            SPACE=(CYL,(500,100),RLSE),
//            DCB=(RECFM=VBS,LRECL=32760,BLKSIZE=27998)
//*
```

```
//* CONTROL CARDS
//*
//SYSIN    DD *
  INDD(DUMPIN,OPTIONS(DUMP))
  OUTDD(DUMPOUT,TYPE(14,15,30,110))
  DATE(yyyy/ddd,yyyy/ddd)
  START(0000)
  END(2359)
/*
//*
//* STEP 2: SORT EXTRACTED RECORDS (OPTIONAL)
//*
//SORT     EXEC PGM=SORT
//SORTIN   DD DISP=SHR,DSN=your.hlq.SMF.EXTRACT
//SORTOUT  DD DSN=your.hlq.SMF.SORTED,
//            DISP=(NEW,CATLG,DELETE),
//            UNIT=SYSDA,
//            SPACE=(CYL,(500,100),RLSE),
//            DCB=(RECFM=VBS,LRECL=32760)
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(50))
//SORTWK02 DD UNIT=SYSDA,SPACE=(CYL,(50))
//SORTWK03 DD UNIT=SYSDA,SPACE=(CYL,(50))
//SYSOUT   DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  SORT FIELDS=(11,4,CH,A,7,4,CH,A,15,4,CH,A),EQUALS
/*
```

在前面的 JCL 中自定义以下值：

1. Job 卡片：更新账号、班级和 msgclass
2. DUMPIN：指向你的 SMF 数据集
3. DUMPOUT：指定输出数据集名称和 HLQ
4. 类型：选择记录类型（14、15、30、110 或其他）
5. 日期：格式 yyyy/ddd （例如 2026/055、2026/056）
6. 空间：根据预期的数据量进行调整
7. 如果不需要，请移除排序步骤

选项 2：使用 DFSORT 提取 SMF 数据

您可以使用 DFSORT 来合并和报告 SMF 历史数据。如果您按天或每周将SMF记录存储在GDG中，这将很有帮助。以下作业使用 DFSORT 来合并 SORTIN 文件中的 SMF 记录，并根据 INCLUDE COND 参数中指定的记录进行筛选。

```
//EXTRSMF JOB 'EXTRACT SMF RECORDS',CLASS=S,MSGCLASS=H,
// MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID,TIME=1440
//SORTJES2 EXEC PGM=SORT,REGION=0M
//SYSOUT DD SYSOUT=*
//SORTMSG DD SYSOUT=*
//SORTIN DD DISP=SHR,DSN=your.hlq.SMF.EXTRACT
//SORTOUT DD DSN=your.hlq.SMF.OUTPUT,
// DISP=(MOD,CATLG,DELETE),
// DCB=(BUFNO=20,
// RECFM=VBS,LRECL=32760,BLKSIZE=27998),
// SPACE=(CYL,(1400,900),RLSE)
//SORTWK1 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK2 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK3 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SORTWK4 DD UNIT=SYSDA,SPACE=(CYL,(30,50))
//SYSIN DD *
OPTION COPY
INCLUDE COND=(6,1,BI,EQ,X'0E',OR,6,1,BI,EQ,X'0F',OR,
6,1,BI,EQ,X'1E',OR,6,1,BI,EQ,X'40',OR,
6,1,BI,EQ,X'50',OR,6,1,BI,EQ,X'59',OR,
6,1,BI,EQ,X'5C',OR,6,1,BI,EQ,X'65',OR,
6,1,BI,EQ,X'66',OR,6,1,BI,EQ,X'6E')
```

要在保留 RDW 数据的同时下载数据，可以使用 FTP 服务器接收提取的文件。确保数据以二进制格式传输并使用 RDW 选项，以便将 RDW 包含在数据传输中。以下作业显示了用于传输此文件的 FTP 任务示例。

```
//EXTRSMF JOB 'EXTRACT SMF RECORDS',CLASS=A,MSGCLASS=H,
// MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID,TIME=1440
//STEP1 EXEC PGM=FTP,REGION=2048K
//SYSIN DD *
10.10.10.10
userid
password
type i
LOCSITE RDW
```

```
put 'your.hlq.SMF.OUTPUT' SMFREQS.SMF
quit
```

正在上传 SCRT 报告

您也可以将 Sub-Capacity 报告工具 (SCRT) 报告上传到 Tr AWS ansform。

上传应用程序清单

收集完所有工件后，完成以下步骤：

1. 按构件类型（例如 /cobol、/jcl、/copybooks、/db2、/ims、/cics、/ca7）将文件整理到子文件夹中。
2. 将顶级文件夹压缩为单个.zip 文件。
3. 将.zip 文件上传到连接到您的 AWS 转换工作空间的 Amazon S3 存储桶。

> **Note**
>
> SMF 记录必须放置在 Amazon S3 存储桶中与源代码不同的文件夹中，并且必须采用.tar.gz 或.gz 格式。

有关将 Amazon S3 存储桶连接到 T AWS ransform 的详细说明，请参阅the section called “设置连接器”。

Sign-in 并创造一份工作

要登录 T AWS ransform Web 体验，请按照文档开始使用 AWS 转换部分中的所有说明进行操作。

要创建并开始工作，请执行启动项目中的步骤。

创建工作空间：命名并描述您的工作空间，用于存储作业、协作者和相关工件。

创建作业：通过从预配置的工作计划中进行选择来创建作业，或者从支持的功能列表中进行选择，根据您的目标自定义工作计划。

> **Important**
>
> AWS 如果您没有适当的权限，Transform 将拒绝您的操作。例如，贡献者不能取消大型机应用程序的任务转换或删除作业。只有管理员才能执行这些功能。

创建作业时，您可以从以下功能中进行选择，但是 Kickoff 步骤始终是必需的，因为它是项目源代码所在的位置。在工作空间中设置的第一项任务中，您需要设置指向 Amazon S3 存储桶的连接器。

跟踪转换进度

您可以通过两种方式跟踪整个过程中的转换进度：

- 工作日志 — 它详细记录了 Trans AWS form 采取的操作、人工输入请求以及您对这些请求的响应。
- 仪表板 — 它提供了大型机应用程序转型的高级摘要。它显示了有关已转换任务数量、应用的转换以及完成大型机应用程序转换的估计时间的指标。您还可以查看每个步骤的详细信息，包括按文件类型划分的代码行、按每种文件类型生成的文档、分解后的代码以及迁移计划。

设置连接器

AWS Transform 使用连接器访问您账户中大型机现代化功能所需的资源。您的连接器将自动配置为您在工作区中运行的第一个作业。根据您选择的工作计划，Trans AWS form 会指导您创建连接器。

大型机重新构想连接器

大型机重新构想连接器适用于运行评估和重新构想工作流程的作业。它使用 S3 存储桶来访问和存储转换资源，并使用 Amazon Neptune 集群来存储提取的项目。Neptune 集群充当统一的知识图谱，用于存储与您的工作有关的所有提取工件，知识图解答 Transf AWS orm 聊天界面中的所有问题。

在 VPC 中部署 Amazon Neptune 集群，Trans AWS form 可以在其中创建弹性网络接口 (ENI)。这些网络连接允许 Transfor AWS m 与 VPC 中的 Neptune 安全通信，以加载数据和查询您的知识图谱。

AWS CloudFormation

我们建议使用以下 CloudFormation 模板来创建大型机重新构想连接器所需的资源。运行 CloudFormation 模板时，使用您计划用于连接器的 S3 存储桶。有关使用 CloudFormation 模板的更多信息，请参阅使用模板。

要下载 CloudFormation 模板，请选择 nept une-kg-setup.yaml。

该模板接受以下参数：

- BucketName – 必需。用于访问 Neptune 批量加载器的 S3 存储桶名称。您必须使用计划在 Trans AWS form 连接器中使用的 S3 存储桶。
- KmsKeyId：可选。用于海王星加密的 KMS 密钥。接受密钥 ID、ARN、别名或别名 ARN。如果省略，则默认为 AWS 托管密钥。

配置连接器时，请提供以下详细信息：

- S3 存储桶 ARN
- Neptune 集群 ARN
- Neptune 集群资源 ID
- 应用程序子网 ID
- 应用程序安全组 ID
- Neptune S3 批量加载器角色 ARN

> **Important**
>
> CloudFormation 模板的 “输出” 选项卡包含配置连接器时需要向 AWS 转换提供的详细信息。

自定义配置

如果您更喜欢使用现有 VPC 或其他工具来创建所需的基础架构，则您的环境必须满足以下要求：

Neptune 星团

- 引擎版本 1.4.5.1 或更高版本的亚马逊 Neptune Serverless
  - 启用 IAM 身份验证
  - 已启用存储加密（AWS 托管密钥或客户管理的 KMS 密钥）
- 无服务器扩展配置（推荐：1—128 个 NCU）
- （推荐）在第二个可用区中使用只读副本以实现高可用性并提高读取性能

Networking

- 支持 DNS 且已启用 DNS 主机名的 VPC
- 在不同的可用区中至少有两个子网。 AWS Transform 在这些子网中创建 ENI 以访问 Neptune 集群，该集群可以位于相同的子网中，也可以位于专用子网中。将子网大小调整为 /20 以适应 VPC 终端节点和应用程序 ENI。
- 通过 VPC 接口终端节点（AWS PrivateLink）从子网到以下 AWS 服务的网络连接：
  - AWS Transform Agents API — 协调大型机现代化工作
  - Amazon Bedrock Runtime — 调用基础模型进行分析和推理

  - 亚马逊关系数据库服务（亚马逊 RDS）— Neptune 集群管理
  - Amazon Elastic Compute Cloud (Amazon EC2) — ENI 的管理
  - Amazon CloudWatch — AWS 变革可观测性的指标
- 连接到与您的子网关联的路由表的 S3 网关终端节点。 AWS Transform 使用此端点将数据从 S3 存储桶加载到 Neptune 集群。

安全组

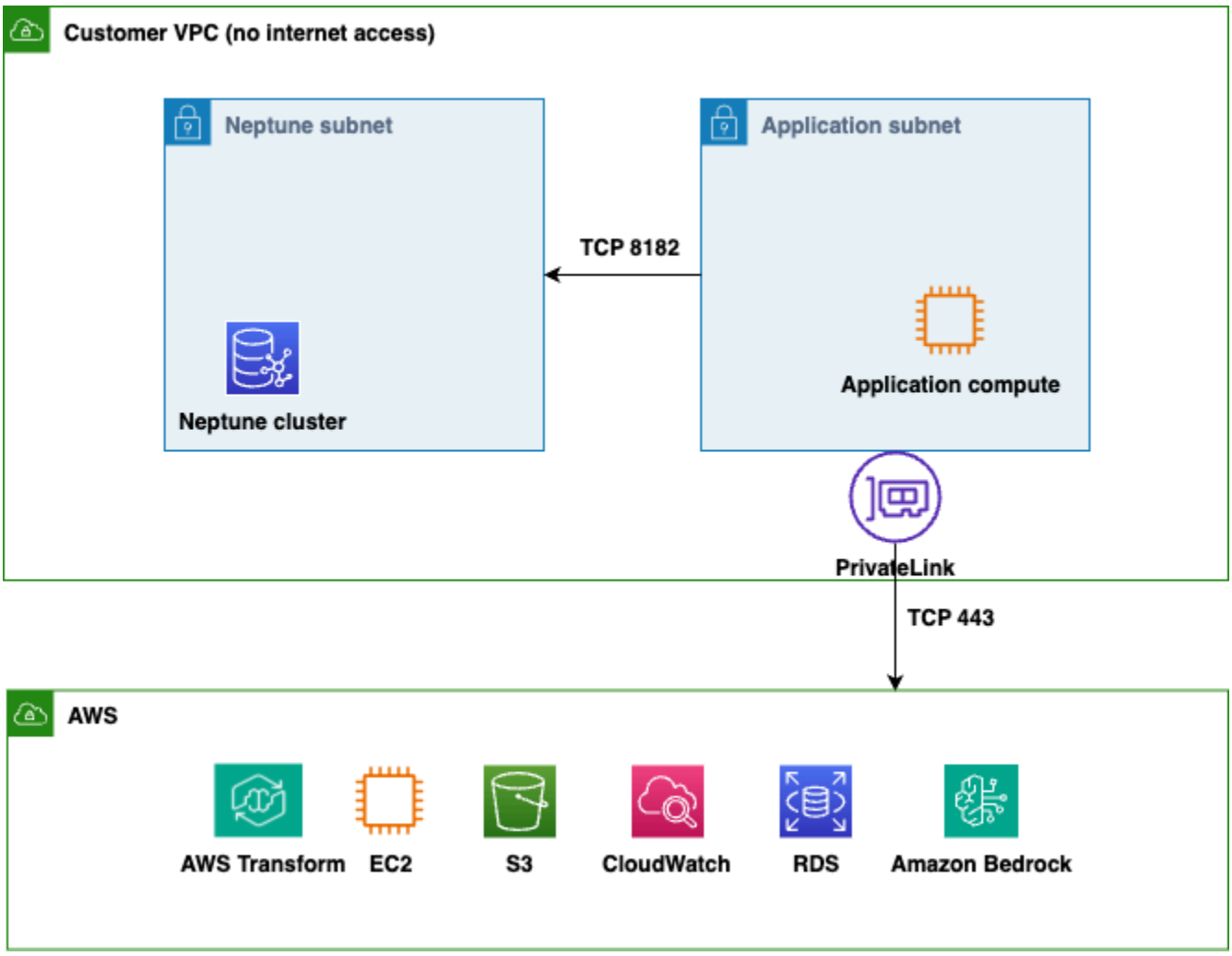
安全组附加到弹性网卡而不是子网。即使 T AWS ransform ENI 和 Neptune 位于同一个子网中，不同的安全组也会控制它们之间的访问权限。

- 一个安全组（附加到由 Transform 创建的 ENI 上 AWS ），它允许：
  - 向 Neptune 安全组出站 TCP 8182
  - 用于到达 VPC 终端节点的出站 TCP 443
- 一个安全组（连接到 Neptune 集群），它允许：
  - 来自应用程序安全组的入站 TCP 8182
- VPC 终端节点安全组（连接到接口终端节点 ENI），允许：
  - 来自应用程序安全组的入站 TCP 443

IAM

- 具有信任策略的 IAM 角色`rds.amazonaws.com`，该角色`s3:GetBucketLocation`在您的 S3 存储桶上授予`s3:GetObjects3:ListBucket`、和
- 此角色必须与 Neptune 集群关联才能批量加载知识图谱数据

下图显示了推荐的架构。



S3 连接器

对于具有自定义计划的作业，Trans AWS form 可以使用 S3 连接器。S3 连接器使用 S3 存储桶来访问和存储转换资源，并使用 S3 向量存储桶用于索引输出。

> **Important**
>
> 您的数据存储并保留在工作区的 Tr AWS ansform 工件存储中，并且仅用于运行作业。

S3 矢量存储桶的可选配置。

在提供 S3 矢量存储桶的区域，Transfor AWS m 会将任务输出的可搜索矢量编码存储在您账户的此 S3 矢量存储桶中，以提供 AI 驱动的搜索和聊天体验。在此作业之外不使用数据，也不用于训练模型。要

启用此功能，您必须创建并提供 S3 矢量存储桶。 AWS Transform 会自动创建并附加一个具有写入此存储桶所需权限的角色。

S3 存储桶 CORS 权限

配置连接器后，将以下 CORS 策略添加到您的 S3 存储桶，以便您可以直接在 Transfor AWS m 控制台中查看和比较项目。如果此政策设置不正确，则可能无法使用 Tr AWS ansform 的内联查看或文件比较功能。

```
[
    {
        "AllowedHeaders": [],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedOrigins": [
              "https://*.transform.eu-central-1.on.aws",
              "https://*.transform.ap-south-1.on.aws",
              "https://*.transform.ap-northeast-1.on.aws",
              "https://*.transform.ap-northeast-2.on.aws",
              "https://*.transform.ap-southeast-2.on.aws",
              "https://*.transform.ca-central-1.on.aws",
              "https://*.transform.eu-west-2.on.aws",
              "https://*.transform.us-east-1.on.aws",
              "https://*.transform.sa-east-1.on.aws"
        ],
        "ExposeHeaders": [],
        "MaxAgeSeconds": 0
    }
]
```

评估和重新构想工作计划

评估和重新构想工作计划是用于实现大型机应用程序现代化的预定义工作流程。它会指导您完成两个阶段：评估您的代码库以识别业务功能，以及重新构想您选择的函数。要改为选择个人能力，请使用自定义工作计划。

评测

大型机现代化之旅通常从评估代码库开始，以识别内容并了解关系和依赖关系。评估完成后，您可以开始分解并选择源代码的某些部分进行现代化改造。分解的界限是根据业务功能确定的。

业务功能目录将您的代码库分解为离散的业务函数，这些函数建立在确定性数据路径的基础上，这些路径从头到尾映射每个业务功能。数据路径是数据所走的路线，从业务触发器开始，一直到大型机代码的最终写入。该系统没有将分析局限于单个入口点，而是跨越批处理作业、CICS 事务及其共享数据存储，以识别连贯的业务工作单元。

业务职能是一系列工作，从业务触发因素开始，以可衡量的业务结果结束。 AWS Transform 提供了业务部门可以采取行动的业务职能目录，从而能够就首先实现哪些现代化做出明智的决策。

使用业务功能评估代码库以实现现代化的好处：

- Full-estate 可见性 — 了解您的批处理作业、在线交易和数据存储如何连接到对您的业务有意义的功能。
- 可操作的界限 — 每个已确定的业务职能部门都是一个独立的单元，您的业务线利益相关者可以对其进行审查并确定优先顺序，以进行现代化工作。
- 从代码到规范的一致性 — 使用定义业务功能的相同代码块来生成其规范，无需转换层，也不需要对账。
- 缩短发现时间 — 自动检测用系统、可重复的分析取代了数月的手动部落知识访谈。

通过聊天提供的评估结果

通过聊天提供的评估结果包括业务功能列表，包括数据路径的数量、每个功能在批处理和CICS交易方面的跨度以及业务描述。您将获得指向 Amazon S3 存储桶中生成的项目的链接，您也可以通过聊天访问它们。提供了两个工件：业务功能详细信息和业务功能摘要。

- 业务功能摘要-提供业务函数列表以及代码中元素正在执行的功能的自然语言描述。
- 业务功能详细信息-提供描述源代码之间关系的交互式图表。

要与图表交互，请选择一个元素以显示有关它的更多详细信息，或者打开一个元素来询问其详细信息。在每个页面中，都有该级别所有元素的摘要以及一个图形界面，供您与每个组件交互并详细了解每个组件，包括以下内容：

- 业务职能-描述哪些业务职能相互关联，并概述每个业务职能。选择业务功能时，将提供以下信息：
  - 数据路径数量
  - 代码行数
  - 业务描述：业务功能概述，用自然语言描述代码中的元素正在执行哪些功能。
  - 接口：详细说明业务功能中数据元素的关系（例如，交换或写入）。

- 业务功能详细信息-描述单个业务职能中数据路径之间的连接，使您可以更深入地了解业务职能的构成。当你选择一个元素时，你会看到该元素是如何跨业务职能连接的，以及以下细节：
  - 数据存储：数据存储的写入器和读取器。
  - 其他元素：相关数据路径的概述，该路径以自然语言描述了数据路径中处理的操作和结果、程序列表以及读者和写入者。
- 数据路径-描述一条数据路径的详细信息以及数据路径中的元素如何相互关联。
  - 描述：数据路径概述，用自然语言描述在数据路径中处理的操作和结果。
  - 数据路径的内容：
    - 入口点
    - 写入
    - 读取
    - 计划

通过聊天，您可以询问输出以了解每个业务职能中包含的元素，并通过业务功能图探索边界。

确定现代化的界限后，聊天会提示您选择要重新构想的业务功能。您可以选择单个业务功能或多个业务功能。 AWS Transform 将选定的界限和所需的评估结果发送到重新构想流程，以继续现代化之旅。

完成首次现代化改造后，您可以使用聊天功能选择一组额外的业务功能进行现代化改造。

重新构想

在重新构想阶段，您可以选择一个或所有经过评估的业务职能，为现代化做好准备。这会触发业务逻辑提取，然后生成所选业务功能的需求。生成的需求是前瞻工程的主要输入，可以将对遗留系统的理解转化为现代化应用程序必须提供的精确规范。

提取业务逻辑

选择一个或多个业务功能后，Trans AWS form 将开始为所选业务功能生成业务逻辑。提取完成后，Tr AWS ansform 会以 JSON 格式将结果存储在 Amazon S3 存储桶中，供下游使用。您可以直接在 Trans AWS form 控制台中监控提取进度并查看任何问题。

查看业务逻辑提取结果

1. 在左侧导航窗格中，选择提取业务逻辑步骤将其展开。
2. 从步骤详细信息中查看以下内容：
   - S3 存储桶链接：提取的业务逻辑结果以 JSON 格式存储的位置。

- 问题：业务逻辑提取过程中遇到的所有问题的列表。

如果在解压缩过程中有任何文件遇到问题，则会显示每个受影响文件的以下详细信息：

- 文件名：遇到问题的文件的名称。
- 文件类型：文件的类型（例如，COBOL 或 JCL）。
- 文件路径：文件在应用程序中的位置。
- 状态：文件提取的当前状态。
- 详细信息：对遇到的问题的描述。

> **Note**
>
> 提取步骤完成后，Trans AWS form 会自动开始生成需求。在此过程开始之前，系统不会提示您输入任何其他输入。

生成需求

业务逻辑提取完成后，生成需求代理使用提取的工件（代码分析、数据分析、业务规则）并生成现代化需求。这些要求是正式的功能规范，与技术无关，包括可测试的验收标准。 AWS Transform 会为您选择的每个业务函数生成一个`requirements.md`文件，并将输出存储在 Amazon S3 存储桶中。要查看输出的 Amazon S3 位置，请选择生成要求步骤。

每个`requirements.md`文件分为以下几个部分：

- 标题-命名业务职能及其所代表的工作流程。
- 全局先决条件 — 在处理之前和处理过程中必须适用于整个工作流程的条件。可配置值显示为参数占位符。
- 带编号的工作流程部分 — 每个部分代表业务职能的一个独立阶段。每个部分都包含以下内容：
  - 一个用户故事，其中陈述了作为角色的目标、该角色想要采取的行动以及由此产生的结果。
  - 采用 EARS（简易需求语法）格式的需求列表，每个要求都有一个唯一的标识符。

> **Note**
>
> 选择第二组业务功能会重新启动新选择的功能的重新构想步骤。然后，控制台仅显示新选择的结果，因此不再显示您之前的业务功能中的业务规则以及存储业务逻辑和要求输出的 Amazon S3 链接的任何问题。您之前的输出不会丢失。您仍然可以从 “构件” 选项卡或 Amazon S3 存储桶中访问它们。

转换工件之间的可追溯性

AWS Transform 在整个评估和重新构想工作流程中保持其生成的工件之间的可追溯性。可追溯性使您可以将每个需求追溯到提取的业务规则，或者直接追溯到产生该需求的原始源代码。

您可以使用该`traceability.yaml`文件查看每个业务职能的所有可追溯性详细信息。它描述了每条业务规则如何与需求对应。

为了实现交互式可追溯性，您可以在 VS Code 和 Open VSX 兼容编辑器中使用 IDE 插件。有关更多信息，请参阅开发者工具。

重新构想工作计划

对于已确定现代化范围并准备重新构想的应用程序，您可以运行独立的重新构想作业。该任务分析您的代码和数据，提取业务逻辑，识别业务域，并为每个业务领域生成现代化需求。

自定义工作计划

自定义任务计划允许您通过选择要运行的功能来构建自己的现代化工作流程。它使您可以完全控制包含哪些功能。根据您的现代化目标，从以下功能中进行选择。有些功能依赖于先运行其他功能。例如，大多数其他功能都需要代码分析。

分析代码

在您与 T AWS ransform 共享 Amazon S3 存储桶路径后，它将分析每个文件的代码，包括文件名、文件类型、代码行及其路径等详细信息。

> **Note**
>
> 您可以通过作业或工作空间级别的构件选项卡下载分析代码结果。在作业级别，转到左侧导航菜单中的 “Artifacts” 选项，然后打开 “结果” 文件夹，或者在工作空间级别找到作业名称，然后

打开 “结果” 文件夹。这将下载一个 zip 文件，其中包含手动分类工作流程的分类文件、资产列表、依赖关系 JSON 文件和缺失文件列表。

在作业计划中，选择左侧导航窗格中的分析代码以查看结果。您可以通过多种方式查看代码分析结果：

- 列表视图 — 您要为大型机转换的 Amazon S3 存储桶中的所有文件
- 文件类型视图 — 按文件类型显示 Amazon S3 存储桶中的所有文件。有关支持的文件类型的列表，请参阅支持的文件。
- 文件夹视图 — Amazon S3 存储桶中的所有文件均以文件夹结构显示。

在文件结果中，根据您选择的文件视图，T AWS ransform 会提供以下信息：

- Name
- 文件类型
- 代码总行数
- 文件路径
- 评论行
- 空行
- 有效的代码行
- 文件数量
- Cyclomatic Complexity-Cyclomatic 复杂度表示通过程序源代码的线性独立路径的数量。 AWS 转换将显示每个文件的循环复杂度。

文件丢失 — 大型机现代化代码分析中缺少文件。理想情况下，应将这些文件作为源输入的一部分添加到 Amazon S3 存储桶中，并且应重新运行分析步骤以获得更好、更具凝聚力的结果。

同@@ 名 — T AWS ransform 为您提供具有相同名称且可能具有相同特征（例如，代码行数）的文件列表。它将无法同时比较任意两个文件内容之间的差异。

重复的 ID — 在 Cobol 程序中，“程序 ID” 字段用作文件的唯一标识符。此 ID 必须是唯一的，因为它用于在整个项目中调用程序。但是，某些项目可能有名称不同但程序 ID 相同的 COBOL 文件。在评估期间获取这些文件的列表可以帮助了解所有程序之间的依赖关系。

> **Note**
>
> 这特定于 COBOL 代码和文件。

当您的程序具有重复的 ID 时，建议在 COBOL 代码中更改这些文件的程序 ID，使其每个文件都有一个唯一的标识符。然后，您可以重新运行作业，以获得更准确、更全面的代码分析结果。

通过解析重复的程序 ID，您可以：

- 提高代码的清晰度和可维护性
- 减少程序调用中的潜在冲突
- 提高依赖关系映射的准确性
- 简化 future 的现代化工作

代码库问题 — 在代码库中检测到的潜在问题，在继续现代化项目之前，应先解决这些问题。这些问题可能包括缺少带有关联语句的引用或代码中不支持的链接。

更新分类-通过手动重新分类，您可以使用批量更新功能对文件进行重新分类，方法是上传包含新分类的 JSON 文件。

> **Important**
>
> 这仅适用于UNKNOWN和TXT文件。

重新分类后， AWS 转换将：

1. 更新分类结果
2. Re-runs 使用新文件类型进行依赖性分析
3. 刷新所有受影响的分析结果

> **Note**
>
> 只有在初始分析循环完成后，才能对文件进行重新分类。

内联查看器和文件比较

Inline Viewer 是 Trans AWS form for 大型机功能中的一项功能，它提供了两个关键的可视化功能：

- 文件视图：查看作业中选定旧文件的内容
- 文件比较：并排比较两个旧文件的内容

查看输入文件

要在中查看您的文件 分析代码 step

- 在 “查看代码分析结果” 下，使用列表中的复选框选择一个文件。

  选择 “查看” 操作按钮（选择 1 个项目时启用）。

  文件内容将在屏幕上的 “文件视图” 组件中呈现。

文件比较

要比较中的文件 分析代码 step

1. 在 “查看代码分析结果” 下，使用列表中的复选框选择两个文件。
2. 选择 “比较操作” 按钮（仅在选择 2 个项目时启用）。
3. 文件将在文件比较组件中并排显示。

> **Note**
>
> 您不能选择两个以上的文件来比较文件。

> **Important**
>
> 如果您在内联查看器或文件比较方面遇到问题，请确保 S3 存储桶设置正确。有关 S3 存储桶的 CORS 策略的更多信息，请参阅the section called “S3 存储桶 CORS 权限”。

数据分析

AWS Transform 提供数据分析，以帮助了解数据关系和元素对大型机现代化项目的影响。提供的两个输出是：

- 数据沿袭：通过映射数据源、作业和程序之间的关系来追踪数据的生命周期
- 数据字典：用作存储库，记录传统数据元素的结构元数据

分析完成后，每个输出将显示两个选项卡，然后有多个视图可供选择，分别用于数据谱系和字典，如下所述。

> **Note**
>
> 当您请求数据分析时。 AWS Transform 执行代码分析，这是执行数据分析所必需的。

数据世系

AWS Transform 根据需要了解的数据关系提供了多个视图，这些视图需要在进行现代化的代码库中进行理解。数据谱系中可用的四个表格视图包括：

- 数据集：此视图提供全面的影响分析，包括操作跟踪，以帮助区分读取、写入、更新和删除
- Db2 表：提供与 Db2 表和操作相关的影响分析
- Program-to-data: 确定哪些 COBOL 程序引用了每个数据集
- JCL-to-data 关系：确定哪些 JCL 脚本引用了每个数据集

摘要概述了数据源及其与程序和 JCL 的关系，并提供了有关如何利用数据源和代码库中总操作的摘要信息。

数据词典

下一步是了解代码库中存在的数据源中的数据元素，以了解各种数据源是如何相互依赖的。数据字典是一种数据目录，提供字段级元数据和业务语言描述，以实现精确的转换映射。

- COBOL 数据结构：提供代码库中存在的 COBOL 抄本和内联引用的字段信息，包括字段属性和业务定义
- Db2 表：提供代码库中存在的 Db2 表的列和表属性，包括主键和外键、架构和索引信息以及数据类型

通过选择数据源，然后使用数据谱系或数据字典按钮来更深入地了解数据源和数据元素之间的关系，即可获得数据谱系和字典之间的关系。数据谱系和字典之间的导航提供了集成的数据可见性，数据谱系提供了 “什么”（结构和含义）以及 “在哪里” ——用法和关系。

活动指标分析

活动指标分析允许您分析 14、15、30、64、102 和 110 类型的系统管理设施 (SMF) 记录。该分析提供了有关大型机应用程序中元素的使用方式的见解。它可以帮助淘汰未使用的代码或决定现代化应用程序的目标架构。如果您在作业中包括活动指标分析，则首先完成代码分析步骤会提供更丰富的 SMF 输出，尽管这不是必需的。

> **Note**
>
> 在协商大型机现代化的工作计划时，首先完成代码分析和分解步骤可以提供更丰富的输出。

载入 SMF 记录以供分析

作为 SMF 分析的第一步，您必须提供 Amazon S3 存储桶中的 SMF 记录位置。提供至少 13 个月的记录，以捕捉较短时间范围内可能错过的年度事件。尽管建议使用 13 个月，但任何具有可检测到 SMF 记录的时间范围都会产生分析结果。

您的 SMF 数据提取必须满足以下格式要求：

- 包括类型 14、15、30（子类型 5）、64、102 和 110。
- 使用 EBCDIC 格式的原始二进制文件。
- 包括 RDW 字节。

提供指向 Amazon S3 存储段内的 SMF 记录的链接，确保这些记录位于与源代码分开的文件夹中。格式选项包括压缩后的.zip（最大 600 MB）或.tar.gz（最大 5 GB）。如果您提供指向未检测到 SMF 记录的文件夹的链接，则会收到一条错误消息，并且分析未完成。

分析输出

根据记录的类型，分析输出包含两个组成部分：表格视图和.csv 输出（可在您的 Amazon S3 存储桶中找到）。在 “ AWS 转换” 中，将显示类型 30 和 110 的输出。通过 Amazon S3 存储桶中的项目，您可以浏览对其他类型记录的分析。在用户界面中，标题显示您提供的记录的时间范围，以便您可以识别任何缺少的关键日期。例如，如果您的记录跨越了 5 月 1 日到 10 月 31 日，但不包括感恩节之后的繁忙日子，则可以看到关键记录缺失。Web 应用程序中的时间戳反映了系统的时区和 SMF 记录。

Amazon S3 中提供的项目可对所提供的记录中发现的任何记录类型进行分析。

表格视图

表格视图仅适用于 SMF 30 和 110，最多包含三个用于批处理作业和 CICS 事务的主要组件：

- 摘要-提供关键任务和交易。
- Batch job/CICS 交易分析 — 提供跨任务和交易的汇总分析。
- 代码分析比较（仅限批处理）-在 SMF 分析之前运行代码分析步骤时提供比较数据。

发现摘要提供了三组任务和事务，可帮助您快速识别项目以进行更深入的分析。

Batch job 和 CICS 交易分析提供跨任务和交易的汇总分析。默认情况下，分析结果中的某些列处于隐藏状态。选择齿轮图标以显示其他字段。

事务密钥为 CICS 交易生成唯一的数据聚合，将四个字段组合成一个键值：

- 事务 ID
- 程序名称
- SysPlex 身份证
- sysID

您可以按完整密钥或分析输出中密钥的任何组成部分进行搜索。

代码分析比较会突出显示在 SMF 记录或分析代码步骤中找到但两者中都不存在的作业。这将显示在 SMF 记录时间段内未运行或未出现在分析代码步骤中的作业。只有在作业中 SMF 分析之前运行代码分析步骤时，此输出才可用。

最佳实践

要获得批处理作业（类型 30）的全面输出，请确保您的 JCL 文件名与作业名称相匹配，以便在代码分析比较中获得有意义的输出。

生成技术文档

您可以为正在进行现代化的大型机应用程序生成技术文档。通过分析您的代码，T AWS ransform 可以自动创建应用程序的详细文档，包括对旧系统中存在的程序逻辑、流程、集成和依赖关系的描述。此文档功能有助于弥合知识差距，使您能够在将应用程序过渡到现代云架构时做出明智的决策。

> **Note**
>
> 当您请求生成技术文档时，Tr AWS ansform 会执行代码分析，包括代码依赖性分析，这是生成文档所必需的。

生成技术文档

1. 在左侧导航窗格的生成技术文档下，选择选择文件并配置设置。
2. 在 Amazon S3 存储桶中选择要为其生成文档的文件，然后在 “协作” 选项卡中配置设置。

   > **Note**
   >
   > 所选文件应具有相同的编码类型（即全部采用相同的 CCSID-UTF8 或 ASCII）。否则，生成的技术文档可能包含空白字段或部分。

3. 选择文档详细信息级别：

   - 摘要 – 提供范围内每个文件的简要概述。并为每个文件提供一行摘要。
   - 详细的功能规格 – 提供大型机应用程序转换范围内每个文件的详细信息。一些细节包括逻辑和流程、依赖关系、输入和输出处理以及各种交易细节。

   > **Note**
   >
   > 只能为 COBOL 和 JCL 文件生成文档。

4. 选择继续。
5. T AWS ransform 生成文档后，请按照控制台中生成和存储结果的 Amazon S3 存储桶路径查看文档结果。
6. 生成文档后，您还可以使用 Tr AWS ansform 聊天来询问有关生成的文档的问题，并决定下一步行动。

将用户信息添加到文档中

```
ARTIFACT_ID.zip
### app/
    ### File1.CBL
```

```
    ### File2.JCL
    ### subFolder/
    #   # File3.CBL
### glossary.csv
### pdf_config.json
### header-logo.png
### footer-logo.png
# ...
```

可以在 zip 文件中添加可选文件，以帮助提高生成的文档质量并提供自定义 PDF 封面。其中一些可以是：

- glossary.csv 文件：您可以选择在 S3 存储桶的 zip 文件中提供和上传可选词汇表。词汇表采用 CSV 格式。此词汇表有助于创建包含与客户词汇相一致的相关描述的文档。示例`glossary.csv`文件如下所示：

```
LOL,Laugh out loud
ASAP,As soon as possible
WIP,Work in progress
SWOT,"Strengths, Weaknesses, Opportunities and Threats"
```

- pdf_config.json：您可以利用此可选配置文件生成符合公司格式和标准的 PDF 文档，包括页眉、页脚、徽标和自定义信息。样本`pdf_config.json`如下所示：

```
{
    "header": {
    "text": "Acme Corporation Documentation",
    "logo": "header-logo.png"
  },
  "customSection": {
    "variables": [
      {
        "key": "business Unit",
        "value": "XYZ"
      },
      {
        "key": "application Name",
        "value": "ABC"
      },
      {
        "key": "xxxxxxxxxx",
        "value": "yyyyyyyyyyyy"
```

```
      },
      {
        "key": "urls",
        "value": [
          {
            "text": "Product Intranet Site",
            "url": "https://example.com/intranet"
          },
          {
            "text": "Compliance Policies",
            "url": "https://example.com/policies"
          }
        ]
      }
    ]
  },
  "footer": {
    "text": "This document is intended for internal use only. Do not distribute
 without permission.",
    "logo": "footer-logo.png",
    "pageNumber": true
  }
}
```

- 标题：
  - 对于封面 PDF 文件，默认文本将是项目名称。
  - 对于每个程序 PDF 文件，默认文本将是程序名称。
  - 没有默认徽标。如果未配置标题徽标，则不会显示任何徽标。
  - 字体大小和徽标大小应根据字数或徽标文件大小动态更改。
- 自定义部分：
  - 如果未配置自定义部分，则将从 PDF 中省略该部分。
  - 该链接必须是可点击的。
- 页脚：
  - 页脚没有默认文本或徽标。
  - 除非另有明确配置，否则默认情况下，页码将显示在页脚中。
  - 字体大小和徽标大小应根据字数或徽标文件大小动态更改。

生成文档内联查看器

您可以在 “生成技术文档” 步骤中查看 PDF 文件。

要查看 PDF 文件

1. 导航到 “查看文档结果” 选项卡。
2. 在列出生成的 PDF 的表格中找到 PDF。
3. 要么选择文件，然后选择 “查看”，要么选择叠加在文件名上的链接元素。

PDF 在 “ AWS 转换” 中打开，右上角有展开屏幕的选项。

> **Note**
>
> AWS 通过转换，您还可以下载生成的技术文档的 XML 或 PDF 版本。

> **Important**
>
> 如果您在使用文档内联查看器时遇到问题，请确保 S3 存储桶设置正确。有关 S3 存储桶的 CORS 策略的更多信息，请参阅the section called “S3 存储桶 CORS 权限”。

提取业务逻辑

您可以从正在进行现代化的大型机应用程序中提取基本业务逻辑。 AWS Transform 会自动分析您的代码，以识别和记录关键业务元素，包括详细的流程以及嵌入在应用程序中的业务逻辑。此功能可为您的现代化之旅中的多个利益相关者提供服务。业务分析师可以利用提取的逻辑来创建精确的业务需求，并识别当前实施中的差距或不一致之处。开发人员无需丰富的大型机专业知识即可快速理解复杂的传统系统功能。

> **Note**
>
> 当您请求业务逻辑提取时。 AWS Transform 执行代码分析，包括代码依赖关系和入口点分析，这是执行业务逻辑提取所必需的。

提取业务逻辑

1. 在左侧导航窗格的 “提取业务逻辑” 下，选择 “配置设置”。
2. 在 “协作” 选项卡中，选择要如何提取业务逻辑：
   - 应用程序级别：为所有业务功能、交易、批处理作业和文件生成业务文档。这将选择应用程序中的所有文件。
   - 文件级别：仅为您从文件表中选择的文件生成业务文档。

   > **Note**
   >
   > - 对于任一选项，您都可以选择 “包括详细的功能规范”，这样 T AWS ransform 就会包括所选文件的控制流和全面的业务规则。
   > - 所选文件应具有相同的编码类型（即全部采用相同的 CCSID-UTF8 或 ASCII）。否则，生成的文档可能包含空字段或部分。
   > - 只能为 COBOL 和 JCL 文件生成文档。
   > - 对于应用程序级别，CICS 事务处理和批处理作业使用的程序被组合在一起，而所有其他程序则归类为 “未分配”。
3. 选择继续。
4. T AWS ransform 提取业务逻辑后，它会以 JSON 格式将结果存储在 Amazon S3 存储桶中，以便您可以在线查看。

> **Note**
>
> 生成的业务规则文件数量可能比您最初选择的要多。某些选定的文件可能会触发业务规则提取以包括其他依赖文件，这些文件也将出现在结果表中。

在线查看提取的业务文档

您可以在 “提取业务规则” 步骤中查看业务逻辑。要做到这一点，

1. 导航到查看业务逻辑提取结果。
2. 从表格中选择要查看的文档，然后单击 “查看结果” 按钮。

业务文档页面将在新的浏览器选项卡中打开。

分解

您可以将代码分解为考虑到程序和组件之间依赖关系的域。这有助于将相关的文件和程序适当地分组到同一个域中。它还有助于在分解过程中保持应用程序逻辑的完整性。

> **Note**
>
> 当您请求分解时，Tr AWS ansform 会执行代码分析，包括代码依赖性分析，这是执行分解所必需的。我们还建议您在分解之前进行业务逻辑提取，以获得更好的结果。

要开始分解应用程序，请执行以下操作：

1. 从左侧导航窗格中选择 “分解代码”。

   > **Note**
   >
   > 系统会为所有未与域关联的文件自动创建一个名为 “未分配” 的域。初始导航时，所有文件都应关联到 “未分配”，除非域是从应用程序级业务逻辑提取中提出的。

2. 通过 “操作” 菜单创建新域，然后选择 “创建域”。
3. 在创建域中，提供域名、可选描述，并将某些文件标记为种子。
   - CICS 配置文件 (CSD) 和调度器配置文件 (SCL) 可用于自动种子检测。
   - 您也可以仅将一个域设置为公共组件。此域中的文件在多个域中是通用的。
4. 选择创建。

   > **Note**
   >
   > 您可以使用不同的文件作为种子创建多个域。

5. 确认所有域和种子后，选择分解。
6. AWS Transform 将检查源代码文件，然后分解为具有相似用例和高度依赖编程的程序和数据集的域。

   AWS Transform 为你提供了将分解后的域作为依赖关系的表格和图表视图。坐标图视图有三个选项：

- 域视图-可以以可视格式查看不同域名之间的关系。
- 依赖关系视图 — 可以以复杂依赖关系图的形式查看每个域中的所有文件。如果添加到域的节点没有收到来自同一域中种子的信息，则该节点要么被预测为未分配（节点未收到任何信息）、已断开连接（在未收到种子信息的子图中），要么被预测到另一个域（节点至少从该域接收了信息）。
- 子图视图-用户可以创建子图来可视化节点子集，从而更清楚地了解该节点集合的关系影响和边界。
  - 要创建子图，请选择一组节点，然后从工具栏中选择 “提取子图” 选项。
  - 合并子图是可用的，合并时除了要合并的两个子图之外还会创建新的第三个子图。

> **Note**
>
> 如果您不喜欢当前的域名结构，请重复这些步骤以添加更多域名，或者使用不同的种子集重新配置已创建的域名。

7. 完成后，选择 “继续”。

种子

种子是分解代码阶段的基础输入。每个组件或文件（例如 JCL、COBOL、Db2 表、CSD 和调度器文件）只能作为种子分配给一个域，从而确保分解过程中边界清晰且对齐。

种子的鉴定取决于应用或投资组合的结构。对于典型的大型机遗留应用程序，通常可以通过遵守既定的命名约定、调度器中的批级分组以及CICS系统中定义的事务级分组来确定种子。此外，数据库表也可以用作种子，为分解提供另一层结构。

导入 and/or 更新依赖关系文件

在分解过程中，您可以为依赖项上传一个 JSON 文件，该文件将替换 Transf AWS orm 执行的依赖关系分析生成的现有文件。

导出依赖项功能允许你下载在分解步骤中生成的依赖关系 json 文件。下载后，您可以根据需要修改文件。然后，您可以使用Tr AWS ansform的上传功能导入依赖关系，该功能允许您上传依赖关系的新 JSON 文件，该文件将替换依赖关系分析生成的文件。之后，分解步骤中的图表将更新。

导出、修改和导入依赖关系

1. 在查看分解结果页面上，选择操作。

2. 在下拉列表中，选择 “其他操作” 下的 “更新依赖关系文件” 选项。
3. 在 “更新依赖关系文件” 模式中，
   a. 下载根据现有分析结果创建的依赖文件 “ AWS 转换”。
   b. 在下载的文件中，根据你想要实现的内容修改依赖关系。
   c. 修改后，使用上传依赖文件按钮保存并上传此文件。

> **Note**
> 唯一可接受的文件格式是 JSON 文件。

4. 接下来，选择导入。

AWS Transform 将导入依赖关系文件并根据您的输入创建新的依赖关系图。

导入 and/or 更新域名

对于在分解步骤之前映射了域、种子、 and/or 文件关系的客户，您可以通过 “操作” 菜单中提供的导入域名文件功能上传此域定义。何时可以使用此函数的一些示例：

- 从另一份工作中提前进行分解
- 提供此映射的主题专家

导入域文件后，用户可以对域定义进行分解，或者如果满意，可以保存然后提交域定义。

Parent/child/neighbor 档案

在依赖关系图中，程序通过不同类型的连接相互关联。了解这些关系有助于您在大型机应用程序转换期间分析程序依赖关系。它还有助于理解域的边界。例如，如果您选择一个域，然后选择父一级，它将显示连接的节点。

父关系-父文件调用或控制其他程序。在等级制度中，家长高于其受抚养计划。您可以选择一个级别或所有级别的父级。

子级关系-子文件由父程序调用或控制。在文件层次结构中，子级位于其父级的下方。

邻居关系-邻居是处于相同分层级别的文件。它们共享同一个父程序，并且可能直接相互交互。

重铸代码

Reforge 使用大型语言模型 (LLM) 来提高重构代码的质量。初始 COBOL-to-Java 转换保留了功能等同性，同时保留了旧系统中的 COBOL-influenced 数据结构和变量名。Reforge 会重构此代码以遵循现代 Java 实践和惯用语，将 COBOL-style构造替换为原生 Java 集合和命名约定。这使得代码对于 Java 开发者来说更具可读性和可维护性。

> **Note**
>
> 重铸配额为：
>
> - 每个作业有 300 万行代码
> - 每位用户每月有 500 万行代码

按照以下步骤在重构后重构代码：

1. 在左侧导航窗格中选择 Reforge java 代码，然后选择配置代码重构。
2. 向压缩后的可构建源项目提供 S3 位置，然后选择 “继续”。使用这个 zip 结构：

```
input.zip
        ### PROJECT-pom
        ### PROJECT-entities
        ### PROJECT-service
        ### PROJECT-tools
        ### PROJECT-web (optional)
        ### pom.xml
```

   AWS Transform 会分析你的 zip 包以在 PROJECT-service 目录中找到文件，这样它就可以提供可供你重铸的可选类列表。这些类有后缀`ProcessImpl.java`。
3. 完成 “选择要重铸的职业” 页面，然后选择 “继续”。在 “工作日志” 选项卡上跟踪重铸状态。
4. 在查看结果页面上查看已完成的重铸结果，该页面显示了每个职业的重铸状态。它还指定了在您的 S3 存储桶中哪里可以找到 Reforge 结果。

一旦 T AWS ransform 从你那里得到这个输入，它就会为你提供一个包含 Reforge 结果的可下载文件。

这是成功重铸后产生的 zip 结构：

```
reforge.zip
### maven_project
### reforge.log
###tokenizer_map.json
```

- maven_project 包含经过改造的源代码。
  - 已重构但未成功完成编译的文件位于`/src/main/resources/reforge/originalClassName.java.incomplete`并命名。`originalClassName.java.incomplete`将它们与文件的原始版本进行比较，以选择要保存的重制函数。
  - 提供给 Tr AWS ansform 且成功重构的源文件将备份到`src/main/resources/reforge/originalClassName.java.original`并命名。`originalClassName.java.original`这些文件的重构版本取代了提供给 Transform 的源文件。 AWS

> **Note**
>
> 只有在`originalClassName.java`重铸过程成功的情况下，文件才会被重新伪造的文件所取代。否则，他们会保留原始内容。

- reforge.log 包含可用于诊断任务失败或在出现问题时提供给 AWS 支持人员的日志。
- tokenizer_map.json 包含令牌 ID 与您的数据（例如文件路径和 class/method 名称）的映射，这些数据在日志中进行标记化以保护隐私。如果出现问题，您可以将此文件提供给 AWS 支持人员。

规划您的现代化应用程序测试

您可以根据提取的代码属性、作业复杂性和调度程序路径为大型机现代化应用程序创建和管理测试计划。 AWS Transform 有助于确定要测试的作业的优先级，并确定每个测试用例所需的特定工件。测试计划过程分为三个主要阶段：配置、范围界定和审查。

创建测试计划

1. 配置测试计划设置

   a. 在左侧导航窗格的 “计划测试” 下，选择 “配置设置”。

   b. （可选）为您的业务逻辑提取 (BLE) 提供 S3 路径。这些工件提高了测试计划的质量。如果没有 BLE 工件，测试计划中的某些字段可能仍然不完整。

2. 定义测试计划范围

a. 选择要包含在测试计划中的入口点，例如批处理作业。

b. 根据多个属性对作业进行筛选和排序：

- 业务职能（摘自 BRE BLE）
- 域（从分解阶段开始）
- 文件路径和位置
- 自定义搜索条件

c. 选择单个作业或整个组进行测试。

d. 查看工作关系和依赖关系。

3. 查看并调整测试计划

生成的测试计划提供了全面的信息，包括：

- 基于依赖关系的首选执行顺序
- 来自调度程序的 Job 组分配
- 复杂度分数，即测试用例的总分数
- 商业领域协会
- 循环复杂度指标
- 数据集和表依赖关系
- 代码行指标
- 业务函数映射

测试计划自定义选项

您的测试计划可以根据特定需求进行定制。例如，您可以：

- 通过选择多个入口点来创建新的测试用例
- 合并现有测试用例以组合相关功能
- 拆分测试用例以进行更精细的测试
- 删除不必要的测试用例
- 为现有测试用例添加或删除入口点
- 修改测试用例描述和属性
- 调整执行顺序

详细的测试用例信息

每个测试用例都提供了描述其内容和相关数据集或数据文件的详细信息：

- 测试范围的全面描述
- 包括完整的入境点清单
- 显示复杂性和规模的汇总指标
- 业务规则和自动测试用例指南
- 带方向的数据集和表依赖关系 (input/output)
- 交互式依赖关系图可视化
- 执行先决条件和要求

数据管理功能

这些详细信息可帮助您了解与测试用例相关的数据。你可以：

- 按 input/output 方向筛选数据集
- 确定执行测试所需的工件
- 跟踪测试用例之间的数据依赖关系
- 监控测试计划中数据集的使用情况

> **Note**
>
> AWS Transform 会自动分析调度程序依赖关系并分配复杂度分数，以帮助确定测试工作的优先顺序。较高的复杂性分数表示在测试过程中可能需要更彻底的测试或隔离的工作。

业务规则和测试用例指南

T AWS ransform 测试计划根据业务规则提取为您的测试用例计划提供建议：

- 使用 LLM 自动处理业务规则
- 生成综合测试用例
- 特定业务场景的测试指南
- 规则和测试用例之间的可追溯性

最终测试计划存储在指定的 S3 位置，包括有效执行测试策略所需的所有必要信息。您可以导出测试计划，以便与其他测试工具或文档系统集成。

> **Note**
>
> 虽然提供了综合测试用例指导，但必须根据指南单独创建实际的测试工件。测试计划可作为测试策略的全面蓝图，但不生成测试数据或执行脚本。

测试用例创建规则-摘要

一般规则

- 一个测试用例按计划执行顺序包含 1 到多个 JCL
- 测试用例由支持的有效调度程序（CA7 和）创建 Control-M
- 测试执行 JCL，而不是调度器本身或计划任务
- 计划任务是唯一的，只能执行一个 JCL
- 一个 JCL 可以由多个计划任务执行
- 一个 JCL 可以在没有时间表的情况下存在

默认测试用例创建规则

- 如果测试用例中有一个 JCL：
  - JCL 不参与日程安排
  - JCL 由分成多个分支的定时任务执行
  - 计划中的一个分支仅包含此 JCL
- 如果测试用例中有多个 JCL：表示计划分支中的线性执行路径序列
- 如果 JCL 正在执行不同的计划任务：JCL 将成为自己的独立测试用例
- 如果 JCL 正在执行趋同计划任务：JCL 可以启动新的测试用例，但不会包含在以前的分支中
- 丢失的 JCL 将被跳过并继续执行（计划在 future 上进行增强，在缺少 JCL 点时减少测试用例）

用户操作规则

- 创建测试用例：用户从可用的 JCL 中进行选择
  - 如果 JCL 存在于调度执行分支序列中，则成功

  - 遵循计划执行顺序
- 将 JCL 添加到测试用例：用户从可用的 JCL 中进行选择
  - 如果 JCL 可以存在于测试用例的调度执行中，则成功 branch/path
- 从测试用例中删除 JCL：用户可以从测试用例中移除任何 JCL
  - 即使它会导致执行路径间隙，也允许
- 合并测试用例：用户选择两个测试用例进行合并
  - 如果 JCL 可以一起存在于同一个调度执行分支中，则成功
  - 维护计划执行顺序
- 拆分测试用例：用户在测试用例中选择一个 JCL 进行拆分
  - 从分割点向前创建新的测试用例
  - 修改了原始测试用例，以排除超过分割点的 JCL
- 删除测试用例：用户可以删除任何已创建的测试用例

> **Note**
>
> 您不能从不同的调度器 branches/path创建、添加或合并测试用例。计划在未来进行一项增强，以允许在调度程序中 divergent/convergent 执行任务以外的操作。

生成测试数据收集脚本

您可以生成 JCL 脚本，根据上一步中创建的测试计划从大型机系统收集测试数据。 AWS Transform 会自动为全面测试所需的数据集、数据库表和顺序文件创建数据收集脚本。数据收集过程分为四个主要阶段：输入配置、测试用例选择、脚本配置和脚本生成。

生成测试数据收集脚本

1. 提供测试计划输入

   a. 在左侧导航窗格的测试数据收集下，选择提供测试计划输入。

   b. 从 “规划现代化应用程序测试” 中指定测试计划 JSON 文件的 S3 路径。

   c. 如果测试计划是在上一个作业步骤中生成的，则会预先填充输入字段。

   d. 您还可以通过指定相应的 S3 位置从其他作业中选择测试计划。

2. 选择用于数据收集的测试用例

a. 查看测试计划中测试用例的完整列表。

b. 根据多个属性对测试用例进行筛选和排序：

- 业务职能和领域
- 数据库表依赖关系
- 数据集要求
- 复杂度指标
- 自定义搜索条件

c. 选择单个测试用例或使用批量选择选项。

d. 点击一个测试用例查看详细信息，包括入口点、指标和业务规则，即可查看详细信息。

3. 配置数据收集脚本

a. 下载示例模板和配置文件以供参考。

- AWS Transform 为 Db2 数据库卸载、VSAM 文件 REPRO 和顺序数据集处理提供了示例模板，可用作流程预期模板类型的指导。
- 标准可能因站点而异，因此期望客户修改或替换这些符合他们自己标准的模板。
- 需要将这些修改后的模板上传到 S3 存储桶，测试数据收集可以在该存储桶中对其进行处理。

b. 提供包含以下内容的变量配置文件（JSON 格式）：

- 用户前缀和特定于环境的常量
- 数据库配置参数
- 目标端点设置和数据传输参数
- 用户定义并要在 JCL 模板中使用的其他必需参数

c. 为不同的数据收集方法上传 JCL 模板：

- Db2 模板：用于数据库表卸载（针对 BMC、IBM DSN 或其他卸载实用程序进行自定义）
- VSAM 模板：用于 VSAM 文件处理（通常使用 REPRO 实用程序）
- 顺序数据集模板：用于处理顺序数据集、分区数据集、GDG 等

4. 查看和管理生成的脚本

生成的脚本提供了全面的数据收集功能，包括：

- “之前” 和 “之后” 测试执行数据收集的脚本分开

- 按测试用例和数据类型整理脚本结构
- 脚本会自动存储到 S3 存储桶中，便于访问和传输
- 生成的 JCL 脚本已准备好在大型机上执行
- 变量替换基于模板中定义的用户配置

脚本生成功能

生成的脚本会根据您的模板和配置自动定制：

- Template-based 生成：使用您提供的 JCL 模板进行变量替换
- 环境：整合您的特定大型机配置
- 数据类型处理：为顺序数据集、VSAM 文件和数据库表创建相应的脚本
- 测试用例的集合：生成 “之前” 和 “之后” 的数据收集脚本
- 顺序数据集处理： AWS 提供的示例提供了文件传输功能，但可以根据您的站点提供的压缩工具或实用工具（例如 Connect Direct 或托管文件传输等）对其进行自定义。

数据收集策略

生成的脚本支持全面的数据收集策略：

- 顺序数据集收集：用于 VSAM 和平面文件的复制和复制工具
- 数据库表卸载：可自定义的 Db2 卸载过程
- 顺序数据集处理：对序列数据集进行可自定义的后处理，例如压缩、托管文件传输服务等。
- 依赖关系管理：基于测试用例定义的协调收集

> **Note**
>
> AWS Transform 会根据您的模板和配置生成脚本。在大型机环境中执行之前，请检查所有生成的 JCL，以确保与您的特定系统配置和安全要求兼容。

模板自定义和最佳实践

ATX 测试数据收集提供灵活的模板自定义功能：

- Multi-utility 支持：为不同的大型机实用程序（BMC、IBM、DSN）调整模板
- Variable-driven 配置：使用常量作为特定于环境的参数
- 可重复使用的模板：创建标准化模板以实现一致的脚本生成
- 数据处理：纳入组织特定的数据处理要求
- 安全集成：包括适当的安全和访问控制
- 性能优化：配置以实现高效的数据收集和传输

生成的输出结构

生成的脚本按以下结构组织在您的 S3 存储桶中：

- 测试用例组织：按关联测试用例分组的脚本
- 收集时间：分别存放 “之前” 和 “之后” 数据收集的文件夹
- 数据类型分类：按顺序数据集、数据库表和传输组织的脚本
- 元数据文件：摘要信息和执行指南
- Ready-to-transfer 格式：JCL 格式化为直接部署大型机

最终的脚本集合存储在指定的 S3 位置，包括有效执行数据收集策略所需的所有必要的 JCL。您可以下载脚本以传输到您的大型机环境或与自动部署流程集成。

> **Note**
>
> 在生成全面的 JCL 脚本时，必须在大型机环境中执行实际执行。这些脚本可用作即用型数据收集工具，但需要相应的大型机访问和执行权限。

测试自动化脚本生成

您可以生成测试自动化脚本，以便根据上一步中创建的测试计划在现代化应用程序上执行测试用例。AWS Transform 会自动创建全面的测试脚本，这些脚本利用从测试数据收集过程中收集的数据。测试自动化脚本生成过程包括三个主要阶段：输入配置、测试用例选择和脚本生成结果。

生成测试脚本

1. 提供测试计划输入

a. 在左侧导航窗格的 “测试自动化脚本生成” 下，选择 “提供测试计划输入”。

b. 从 “规划现代化应用程序测试” 中指定测试计划 JSON 文件的 S3 路径。

c. 如果测试计划是在上一个作业步骤中生成的，则会预先填充输入字段。

d. 您还可以通过指定相应的 S3 位置从其他作业中选择测试计划。

e. 系统使用此测试计划作为生成自动化脚本的基础。

2. 选择用于生成脚本的测试用例

a. 查看测试计划中测试用例的完整列表。

b. 根据多个属性对测试用例进行筛选和排序：

- 业务职能和领域
- 数据库表依赖关系
- 数据集要求
- 复杂度指标
- 自定义搜索条件

c. 选择单个测试用例或使用 “全部选中” 和 “取消全选” 按钮的批量选择选项。

d. 点击各个测试用例，查看测试用例的详细信息，包括入口点、指标和业务规则。

选定的测试用例将生成自动化脚本，以便在现代化应用程序上执行。

3. 查看和管理生成的测试自动化脚本：

- 系统将显示一条成功消息，确认脚本生成已完成。
- 生成的测试脚本会自动存储在您指定的 S3 存储桶位置。
- 访问生成的测试脚本的完整列表及其相应的 S3 位置。
- 每个测试用例都有相应的自动化脚本存储在各个 S3 位置。
- 脚本已准备就绪，可以在您的现代化应用程序环境中部署和执行。

测试自动化脚本功能

生成的自动化脚本提供了全面的测试功能：

- 现代化应用程序测试：脚本专为在转换后的应用程序上执行测试用例而设计
- 数据集成：利用从上一个测试数据收集步骤中收集的测试数据，需要将这些数据复制到每个测试用例的文件夹中

- 自动执行：脚本可用于设置数据接收器、运行测试用例和比较结果，某些参数必须根据您的部署环境进行设置
- 有条理的结构：脚本按您的 S3 存储桶中的测试用例系统地组织
- Ready-to-deploy 格式：脚本已格式化，可直接部署到您的测试环境中

生成的输出结构

生成的测试自动化脚本按以下结构组织在您的 S3 存储桶中：

- 测试用例组织：每个测试用例都有自己的专用脚本存储在单独的 S3 文件夹中
- Execution-ready format：脚本的格式化可在根据您的环境设置一些变量后立即部署和执行
- 集中访问：所有脚本均可从单个 S3 存储桶位置访问，便于管理

测试执行策略

生成的脚本支持全面的测试执行工作流程：

- 环境设置：脚本包括用于设置初始数据以执行测试的功能
- 数据准备：与从测试用例数据收集步骤收集的测试数据集成
- 测试用例执行：在现代化应用程序上自动执行单个测试用例
- 结果比较：用于比较测试结果和验证应用程序行为的 Built-in 功能

> **Note**
>
> AWS Transform 会根据您的测试计划和选定的测试用例生成测试自动化脚本。这些脚本专为在现代化应用程序环境中执行而设计，并利用上一步中收集的测试数据。在部署之前，请查看所有生成的脚本，以确保与您的特定应用程序配置和测试要求兼容。

测试自动化的最佳实践

- 环境验证：在执行脚本之前，请确保您的现代化应用程序环境已正确配置
- 数据验证：验证收集阶段所需的测试数据是否可用且可访问
- 脚本自定义：根据需要查看和自定义生成的脚本，以满足您的特定测试要求
- 执行监控：在测试脚本执行期间实施适当的监控和日志记录

- 结果分析：建立分析测试结果和识别应用问题的流程

测试自动化脚本的最终集合提供了一个完整的测试框架，用于验证您的现代化应用程序功能。这些脚本可以集成到您的持续测试流程中，也可以作为应用程序验证工作流程的一部分执行。

中的部署功能 AWS 转换

AWS Transform 通过提供即用型基础设施即代码 (IaC) 模板，帮助您为现代化大型机应用程序设置云环境。通过 T AWS ransform 聊天界面，您可以访问预先构建的模板，这些模板可创建计算资源、数据库、存储和安全控制等基本组件。这些模板提供包括 CloudFormation (CFN)、 AWS Cloud Development Kit (AWS CDK)和 Terraform 在内的流行格式，使您可以灵活地部署基础架构。

这些模板可作为构建块，减少为现代化大型机应用程序配置环境所需的时间和专业知识。您可以自定义这些模板以满足您的需求，从而为构建部署环境奠定基础。

要检索 IaC 模板，请在 Trans AWS form 聊天中询问 Infrastructure-as-Code 模板，说明您的首选现代化模式（例如用于大型机重构的 AWS 转换）、您的首选拓扑（独立与高可用性）以及您的首选格式（对比 Cloud Development Kit CloudFormation 与 Terraform）。

重构后构建和部署您的现代化应用程序

使用 T AWS ransform 完成重构过程后，您可以构建和部署现代化的 Java 应用程序。本指南将引导您检索现代化代码、配置环境以及部署和测试应用程序。

> **Note**
>
> 除了此处提供的指导外，Trans AWS form 生成的代码包还将包括一个 “设置 AWS 自动重构开发环境” 文档，该文档提供了使用开发者运行时设置 IDE（集成开发环境）的说明。

主题

先决条件

开始之前，请确保您已具备以下条件：

- 使用 Transform 成功完成重构作业。 AWS
- 访问您的现代化代码。
- 已在开发计算机上安装并配置生成软件工具堆栈，例如 Apache Maven 或 Apache Tomc a t。有关 Runtime 版本控制的更多信息，请参阅 Trans AWS form for 大型机运行时版本说明。
- 已安装并配置了 Amazon Corretto 或 Java 运行时的一个版本。有关安装 Amazon Corretto 的更多信息，请参阅 Amazon Corretto 24。
- 如有必要，可以为运行时组件创建和配置 Amazon Aurora PostgreSQL 数据库。有关创建 Aurora PostgreSQL 数据库的更多信息，请参阅使用亚马逊 A urora PostgreSQL。
- 将应用程序部署到您的运行时环境的管理权限。
- 查看了大型机运行时AWS 转换概念，了解有关使用 AWS 自动重构解决方案实现现代化的应用程序的基本概念。

步骤 1：检索现代化代码

检索现代化代码

1. 下载并解压缩生成的代码包。
2. 打开`codebase/app-pom/pom.xml`并记下所需的运行时引擎版本。例如 `<gapwalk.version>4.6.0</gapwalk.version>`。
3. 从下载的代码包中找到 “设置 AWS 自动重构开发环境” 文档以供参考。

第 2 步：构建现代化应用程序

构建您的现代化应用程序

1. 从 “大型机 AWS 变换” 工具箱中访问运行时。
2. 在本地开发计算机上下载并安装相应的运行时版本（在中标识the section called “步骤 1：检索现代化代码”）。

> **Note**
>
> 有关在本地计算机上安装运行时依赖项的其他信息，请参阅设置 AWS 自动重构开发环境文档的第 3.1 节。

3. 打开命令提示符并导航到应用程序的根目录。
4. 要为现代化应用程序构建可部署的软件包，请运行 Maven build 命令：

```
mvn package
```

有关现代化代码的基本组织的详细信息，请参阅应用程序组织页面。例如，对于包含前端 Web 应用程序的现代化应用程序，除了运行时组件之外，您可能至少还需要以下可部署的`.war`聚合：

- 服务项目：包含传统业务逻辑现代化元素

```
<business-app>-service.*.war
```

- Web 项目：包含用户界面相关元素的现代化改造

```
<business-app>-web.*.war
```

步骤 3：配置测试环境

配置您的测试环境

1. 配置您的现代化应用程序运行时。有关更多信息，请参阅AWS Mainframe Modernization 用户指南中的设置运行时配置部分。

> **Note**
>
> 有关特定于运行时组件的配置示例，请参阅《设置 AWS 自动重构开发环境》指南的第 5 节。

2. 为现代化应用程序准备输入和输出 (I/O) 数据集。现代化的应用程序可以处理顺序 I/O 数据集、VSAM 数据集或其他数据集。

> **Note**
>
> 有关示例，请参阅设置 AWS 自动重构开发环境的第 6 节。

3. 运行时环境-您可以使用现有的运行时环境或创建新的运行时环境。
   - 要配置非托管运行时环境，请参阅设置非托管应用程序。
   - 要配置托管运行时环境，请参阅设置托管应用程序。

配置完测试环境后，您将进入部署现代化应用程序的下一步。

步骤 4：部署现代化应用程序

在您创建的运行时中部署应用程序构件，这些运行时在the section called “第 2 步：构建现代化应用程序”和the section called “步骤 3：配置测试环境”部分中 and/or 进行了配置。

使用以下链接可以找到部署现代化应用程序的其他指南：

- 在 Amazon EC2 上部署
- 在 Amazon ECS 和 Amazon EKS 的容器上部署
- 创建 AWS Mainframe Modernization 应用程序

步骤 5：测试现代化应用程序

部署后，

1. 查看可用的 Runtime API，了解与现代化应用程序交互的方法。
2. 测试您的应用程序，使其功能等效性与旧版应用程序保持一致。例如，请参阅AWS Mainframe Modernization 用户指南中的测试示例应用程序。

其他示例

有关使用 Tr AWS ansform 实现大型机应用程序现代化的具体示例，请参阅对大型 CardDemo 机应用程序进行现代化改造。

Full-stack Windows 现代化

AWS Transform 提供全栈的 Windows 现代化，包括.NET 现代化和 SQL Server

适用于.NET 的 AWS 转换代理可以帮助您对.NET 应用程序进行现代化改造，使其与跨平台.NET 兼容。您可以使用.NET Web 应用程序或.NET IDE 对.NET 进行现代化改造。

AWS SQL Server 现代化转型是一项 AI-powered 服务，可自动将微软 SQL Server 数据库及其关联的.NET 应用程序的全栈现代化改造到亚马逊 Aurora PostgreSQL。该服务协调了从架构转换、数据迁移和修改应用程序代码以匹配新目标 PostgreSQL 的整个迁移过程，通过自动执行复杂和劳动密集型任务来提高团队的工作效率。

主题

- 使用现代化.NET AWS 转换
- SQL 服务器现代化

使用现代化.NET AWS 转换

适用于.NET 的 AWS 转换代理可以帮助您对.NET 应用程序进行现代化改造，使其与跨平台的.NET 兼容。此功能称为.NET 现代化。AWS 变换环境在 T AWS ransform 之后，您可以创建.NET 现代化转换作业。

体验

AWS Transform 有多种体验可供选择：

- Web 控制台：用于一次对多达 500 个存储库进行大规模转换。
- Visual StudioIDE：由开发人员主导的解决方案或项目的转换，与代理交互和迭代协作。推荐用于大中型项目。

您可以在 Web 控制台和 IDE 之间自由切换以处理转换作业。

你也可以从其他 IDE 和 AI 代码伙伴调用 T AWS ransform：

- Kiro：使用变身为 Kiro 的力量从 Kiro AWS 变身。
- 其他 AI 代码伙伴：使用 Transform MCP 代理从你首选的 AI 编码助手进行 AWS 转换。

功能和关键特性

- 分析源代码控制系统中的.NET Framework 代码库，包括私有 NuGet 支持、识别跨存储库依赖关系以及提供分析报告。
- 自动将传统.NET Framework 应用程序转换为跨平台.NET、电子邮件通知和转换摘要报告。
- 可轻松与源代码管理平台（BitBucket GitHub、和 GitLab）集成，以提取现有代码并将转换后的代码提交到新分支。
- 通过单元测试验证转换后的代码。

支持的版本和项目类型

AWS 转换支持以下.NET 版本的转换：

- .NET 框架 3.5+
- .NET Core 3.1
- .NET 5.x+
- .NET 8

AWS 转换可以转换为以下目标.NET 版本：

- .NET 8
- .NET 10

AWS Transform 支持以下类型的项目的转换（仅限 C#）：

- 类库
- 控制台应用程序
- ASP.NET:
  - 模型视图控制器 (MVC)，包括前端 Razor 视图
  - 单页应用程序 (SPA) 后端（业务逻辑层）
  - Web API
  - 网络表单
- 单元测试项目（nUnit、xUnit 和 MSTest）

- Windows 通信基金会 (WCF) 服务
- 为第三方或私有 NuGet 包提供跨平台版本的项目。如果缺少跨平台的等效项或其不可用，则 Trans AWS form for .NET 将尝试尽力进行转换。

AWS 转换还可以将以下项目类型转换为现代.NET。这是一项预览功能，可能无法像支持的项目类型那样完全转换。

- WinForms 桌面项目。
- WPF 桌面项目。
- Xamarin 移动项目。
- 项目已写入 VB.NET。

限制

有关 Transform 的配额和限制 AWS 的更多信息，请参阅的配额 AWS 转换。

AWS 变换不会转换以下内容：

- Blazor 用户界面组件
- 没有核心兼容库的 Win32 DLL
- 不包含任何解决方案的存储库。

AWS Transform 不会修改原始存储库分支，只能写入转换计划中指定的单独目标分支。

人为干预

在将.NET Framework 应用程序移植到跨平台.NET 的过程中，可能会要求您在以下情况下提供输入或批准：

- 为您的源代码和权限设置连接器
- 验证提议的现代化计划
- 将缺少的软件包依赖项上传为 NuGets
- 查看并接受转换后的代码

更多信息

您可以使用 Transfor AWS m Web 应用程序或 AWS 工具包对.NET 代码进行现代化改造Visual Studio。

- 使用对.NET 代码进行现代化改造 AWS 转换 Web 应用程序
- 在 IDE 中实现.NET 现代化
- .NET 转换的最佳实践

使用对.NET 代码进行现代化改造 AWS 转换 Web 应用程序

AWS Transform for .NET 是一种新的生成 AI-powered 代理，旨在实现传统.NET 应用程序的现代化 您可以使用 Transfor AWS m Web 应用程序或 Visual Studio AWS Toolkit 扩展程序对旧版.NET 代码进行现代化改造。

要使用 Transfor AWS m Web 应用程序对.NET 代码进行现代化改造，请按照以下详细步骤导航到 Web 应用程序：

1. 正在创建 AWS 转换.NET 工作计划
2. 创建源代码存储库连接器
3. 确认您的仓库为转型做好准备
4. 解析软件包依赖关系以准备转换
5. 审查您的计划，为转型做好准备
6. 转换您的.NET 代码

正在创建 AWS 转换.NET 工作计划

创建工作空间后，在 “作业” 选项卡上，选择 “创建作业”。然后使用自然语言按照聊天窗格中的 T AWS ransform 中的提示进行操作。这些是创建.NET 现代化任务的典型步骤。

1. AWS Transform 会询问你要创建哪种类型的转换作业。在聊天中，进入 .NET 现代化。
2. AWS Transform 将建议一个任务名称，并询问您是否要更改作业名称。如果您想更改作业名称，请使用自然语言告诉 AWS Transform，例如，将作业名称更改为 ExampleCorpDotNet1。否则，在聊天中，您可以接受建议的职位名称。在您接受作业名称后，T AWS ransform 会在聊天窗口中通知您它正在创建作业。
3. AWS 转换会创建转换作业。

的组成部分 AWS 转换.NET 工作计划

T AWS ransform .NET 作业显示屏有 5 个选项卡，您可以从最左边的垂直图标中进行选择：任务、仪表板、批准、构件和工作日志。每个选项卡都有一个左侧窗格和一个中心聊天窗格。有时可能会出现右侧的协作窗格，以显示更多详细信息并请求人工输入。

任务（Job 计划）

此选项卡在左侧窗格中显示您的工作计划。.NET 作业有 5 个步骤：

1. 获取要转换的资源：在此阶段，您可以使用创建指向代码存储库的连接器 AWS CodeConnections。根据您的存储库权限，代码存储库的管理员可能需要批准连接器并授予 T AWS ransform 对存储库的访问权限。
2. 发现用于转换的资源：在此阶段，T AWS ransform 会发现源代码管理中的存储库，然后选择其中部分或全部进行评估。
3. 评估代码以进行转换：对选定的存储库进行评估，您可以查看评估报告。
4. 为转换做准备：在此阶段，如果仓库中缺少任何依赖项，T AWS ransform 会通知您。您可以上传缺少的依赖项或忽略它们。如果您不是 repo 的管理员，则可能需要管理员批准最终的转换计划。
5. 转换：在此阶段，Transform 会 AWS 转换您的存储库，并在转换期间为您提供持续状态，直到转换完成。您可以查看转换报告，以了解更改的内容和原因。

你可以看到每个步骤的状态：

- 还没开始
- 等待用户输入
- 正在进行
- Completed

控制面板

“仪表板” 选项卡提供了转换的高级摘要。它显示转换的任务数量、应用的转换以及完成转换的估计时间的指标。仪表板下方是存储库及其状态（失败或成功）的表。 In-progress

审批

此选项卡上显示并完成任务的批准请求。

构件

Jjob-related 可从此选项卡上传或下载工件。

工作日志

AWS Transform 在 “工作日志” 选项卡中记录其操作。工作日志详细记录了 Transfor AWS m 采取的操作、人工输入请求以及您对这些请求的响应。

创建源代码存储库连接器

之后正在创建 AWS 转换.NET 工作计划，在 “任务” 选项卡上，“ AWS 转换” 窗口的左窗格列出了转换作业的各个阶段。第一阶段是获取要转换的资源。在此阶段，您可以邀请合作者并连接 Connect 源代码存储库。您可以在 “ AWS 转换” 窗口的右侧窗格中指定详细信息。

每个转换作业都必须只有一个源代码存储库连接器。T AWS ransform 代理使用此连接器通过使用从 GitHub GitLab、或 Bitbucket 下载您的.NET 代码库。AWS CodeConnections您必须在与 AWS 变换任务相同的区域 AWS CodeConnections 中进行设置。或者，您可以连接到 Amazon S3 中的源代码，而不是源代码存储库。

> **Note**
>
> 如果您已有源代码存储库连接器，Trans AWS form 会通知您。选择 “使用现有连接器” 以使用此连接器。如果您不想使用现有的连接器，请参见删除现有连接器前文添加新的连接器。每个作业只能有一个源存储库连接器。

添加新的连接器

要创建新的源代码存储库连接器，请执行以下操作：

1. 输入您要用于 AWS CodeConnections 连接器的 AWS 账号。
2. 如果您尚未为同一个 AWS 账户 AWS CodeConnections 进行设置，请设置 AWS CodeConnections。
3. 使用AWS 开发者工具控制台创建与您的 Bitbucket、GitHub、GitHub 企业服务器或AzureDevOps存储库的连接。GitLab
4. 复制您创建的连接的亚马逊资源名称 (ARN)。
5. 返回到 AWS 转换，然后粘贴您创建的连接的 ARN。

6. 输入连接器的名称。

> **Note**
>
> 请勿在连接器名称中输入个人信息。

7. 选择 “启动连接器创建”。
8. AWS Transform 会请求为您输入的 AWS 账户创建一个连接器，该连接器位于与当前转换任务相同的区域，并通知您批准请求已准备就绪，可供 AWS 管理员在 AWS 管理控制台中批准。选择 “复制验证链接”。
9. 如果您是 AWS 管理员，请登录该 AWS 帐户并转到验证链接以批准连接请求。如果您不是 AWS 管理员，请将验证链接提供给您的 AWS 管理员。
10. AWS 管理员批准连接器请求后，选择完成连接器以完成连接器创建过程。如果您想使用其他连接器，请选择 “重新启动”，以重新启动连接器创建过程。

“协作” 选项卡还包含有关您的连接器的详细信息，其中包括：

- 状态-已批准或待批准
- AWS 账号
- AWS 区域
- 连接 ARN

删除现有连接器

> **Note**
>
> 如果您已有源代码存储库连接器，Trans AWS form 会通知您。选择 “使用现有连接器” 或 “删除” 并创建新的连接器。

如果您选择删除现有的源代码存储库连接，Trans AWS form 将在实际删除连接器之前向您发出警告。

1. 您可以通过以下几种方式删除现有连接器：
   a. 如果 AWS Transform 提示您这样做，则可以选择删除并创建新的连接器。
   b. 您也可以在提示中选择 “重新启动”，要修改此连接器，必须重新启动。
2. AWS Transform 警告您重新启动会删除连接器。要删除连接器，请再次选择 “重新启动”。

3. AWS Transform 再次警告您，删除连接器将移除与您的第三方存储库（例如 Bitbucket GitHub、和 GitLab）的连接。此外，如果删除该连接器，任何使用此连接器的 AWS 转换作业都将失败。要确认删除，请键入删除并选择删除。
4. 要添加新的源代码存储库连接器，请参阅添加新的连接器。

连接亚马逊 S3 中的源代码

您可以将 T AWS ransform 连接到 Amazon S3 中的源代码，作为连接源代码存储库的替代方案。

S3 存储桶组织

原始源代码和转换后的代码存储在通用 S3 存储桶中，其组织方式如下所示。您必须在与 AWS 转换任务相同的区域中设置 S3 存储桶。将您的源代码作为根级别的 zip 文件上传到存储桶。zip 文件必须包含每个存储库的顶级文件夹。

在 AWS 转换过程中，Transform 会创建一个转换输出文件夹，并将转换结果存储在该文件夹中。转换会创建一个名为 transformed-code.zip 的 zip 文件，其中包含转换后的代码。这包括一个名为 diff.txt 的代码差异报告文件，该文件突出显示了项目级别的文件更改。

```
<customer-bucket>/
### source-code.zip
         ### repo 1
         ### repo 2
         ### ......
         ### repo n
### transform-output/
      ### transformed-code.zip
```

添加新的 S3 连接器

要创建新的 S3 源代码存储库连接器，请执行以下操作：

1. 在 AWS 控制台中，创建 S3 存储桶。
2. 将您的源代码作为 zip 文件上传到 S3 存储桶。
3. 在 AWS 转换 Web 应用程序中，启动.NET 转换作业。在 “连接源代码存储库” 步骤中，选择 “在 S3 存储桶中连接您的源代码”，然后选择 “保存”。
4. 在下一页上，输入您的 S3 存储桶详细信息并选择提交。

a. 连接器名称

b. AWS 账户编号

c. S3 水桶手臂

d. S3 存储桶加密密钥（可选）

5. 批准连接器：

a. 在下一页上，复制验证链接。

b. 让批准者浏览链接以访问 Trans AWS form 连接器创建请求页面。

c. 选择创建新角色或使用现有角色。

d. 审核请求后，选择 “保存并批准” 以批准该请求。

6. 指定 S3 压缩文件的位置：

a. 在 AWS 转换 Web 应用程序中，等待状态显示为已批准。

b. 在 “指定资产位置” 页面上，输入格式为 zip 代码文件的 S3 URL，`s3://bucket-name/zip-file-name`然后选择 “发送到 AWS 转换”。

c. 任务继续执行 “发现” 步骤以继续转换。

删除 S3 连接器

要删除现有 S3 连接器，请执行以下操作：

1. 在 T AWS ransform Web 应用程序中，选择右上角的管理连接器。
2. 在 “管理连接器” 窗口中，选择连接器。
3. 选择删除。

确认您的仓库为转型做好准备

之后创建源代码存储库连接器，确认您的存储库是准备转换的第一步。你可以：

- 审查和更改默认设置影响计划内容的内容。
- 查看已发现的存储库，然后选择要评估哪些仓库进行转换。
- 查看存储库评估报告，并与 Trans AWS form 聊一聊其内容。
- 使用由生成的计划 AWS 转换.
- 自定义转型计划使用 Web 应用程序或下载 JSON 文件，对其进行修改并将其上传到 Transf AWS orm。

默认设置

在 “协作” 选项卡的 “Job 详细信息” 部分，您可以设置以下内容：

在 “任务” 选项卡上的 “准备转换-确认要转换的存储库” 步骤中，您可以设置以下内容：

- 设置将转换后的代码写入存储库的目标分支名称。
- 设置目标.NET 版本：
  - .NET 8：将所有项目转换为.NET 8
  - .NET 10：将所有项目转换为.NET 10
- 您可以更新默认 Job 设置，也可以保持原样。这些方法包括：
  - 将.NET 标准项目排除在转换计划之外。默认情况下，此设置处于选中状态。选中后，“ AWS 转换” 会将任何.NET 标准项目排除在转换计划之外。如果取消选择此设置，将转换.NET 标准项目，这将使它们不再与.NET Framework 兼容。
  - 查看 NuGet 源代码并获取与.NET 兼容的软件包版本 Allow Transform 搜索要 AWS 转换的代码并获取与.NET 兼容的软件包版本。

查看存储库评估报告

存储库评估报告提供了有关 T AWS ransform 检测到的每个存储库的信息的表格视图。这包括：

- 存储库所有者
- 经评估的分支
- 解决方案数量
- 项目数量
- 代码总行数
- 检测到.NET 版本
- 检测到的项目类型
- 私有 Nuget 依赖项的数量
- 公共 Nuget 依赖项的数量
- 转型的复杂性

要下载文件，请执行以下操作：

1. 在您的工作空间中，选择 “协作” 选项卡。

2. 在 “选择存储库” 窗格中，选择 “下载”，然后选择 “下载为 HTML” 或 “下载为 JSON”

聊聊仓库摘要报告

您的存储库摘要可能很长。使用聊天可以更好地了解其内容。当你在 “工作日志” 选项卡上看到以下消息时，你的报告就可以聊天了：评估报告现在可以在聊天中进行查询。要打开聊天，请单击 Web 控制台右下角的紫色六角形图标。以下是一些示例提示：

- 列出所有发现或评估过的存储库。
- 评估中发现了多少.NET 6 项目？
- 哪些项目的复杂性最高？

使用由生成的计划 AWS 转换

您可以选择使用通过发现 AWS 转换成功概率更高的存储库创建的转换计划，其中包括上次修改的存储库、根存储库和交叉依赖存储库。

AWS Transform 列出了有关转型计划的一些高级细节，其中包括：

- 已@@ 发现的存储库总数 T AWS ransform 使用您的源代码存储库连接器发现的旧版.NET 存储库数量。 AWS 在每个作业中，Transform 最多可以扫描 1,000 个存储库。如果您有更多仓库需要扫描或转换，则可以创建多个转换作业。
- 选定的存储库选择进行 AWS 转换的旧版.NET 存储库的数量。
- 选定的依赖关系选定存储库所需的依赖项数量，T AWS ransform 会自动检测到这些依赖关系并将其添加到转换计划中。

“选定存储库” 表列出了所选存储库。您可以按名称搜索存储库，导航到存储库的其他页面，并下载列出所选存储库及其依赖项的 JSON 格式的文件。您可以在此视图中进行任何更改。

“选定存储库” 表列出了有关选择进行转换的 “ AWS 转换” 存储库的以下详细信息：

- 存储库名称
- 源分支
- 上次修改日期和时间
- 代码行这使您可以查看自己是否接近配额限制。有关更多信息，请参阅 的配额 AWS 转换。
- 依赖存储库您可以单击依赖存储库的数量以查看有关这些依赖项的更多详细信息。

如果您对 AWS 转换生成的转换计划感到满意，请选择确认存储库。

如果要对 AWS 转换生成的转换计划进行更改，请选择自定义转型计划。

自定义转型计划

如果您选择不这样做使用由生成的计划 AWS 转换，则可以使用以下选项之一自定义要转换的存储库列表：

1. 在 “所选存储库” 表中选择存储库。
   a. 当您将存储库添加到计划时，Trans AWS form 将为您选择存储库的依赖关系，并自动将其添加到转换计划中。
   b. 您也可以在表中取消选择存储库。
2. 下载 AWS 转换生成的 JSON 存储库和分支列表。
   a. 选择 “下载”，然后选择 “下载为 JSON”。
   b. 查看并修改 JSON。您可以删除不想转换的存储库或存储库中的解决方案。
   c. 选择 “上传自定义计划”，上传修改后的 JSON。
   d. 如果 JSON 成功上传，“选定存储库” 表格将显示您所做的选择。
3. 您可以选择 “显示依赖存储库” 来显示 Tr ans AWS form 发现的存储库列表，这些存储库是您所选存储库的依赖关系。
4. 如果需要，您可以重复这些步骤。如果您对自定义计划感到满意，请选择 “确认存储库”。

解析软件包依赖关系以准备转换

之后确认您的仓库为转型做好准备，如果 T AWS ransform 发现缺少包依赖关系，则必须完成此步骤。您可以运行 Windows PowerShell 脚本从与Visual Studio开发环境相同的设备上获取缺失的软件包依赖关系，也可以手动检索缺失的软件包。然后，上传丢失的软件包。

可以通过两种方式更新 “缺失的 Package 依赖关系”：

- 使用 Artifact Connector 解决问题：通过专用的 Connect Artifact Repository HITL 工作流程配置工件存储库（ADO NuGet 连接器）来解决问题，该工作流程将在未配置工件连接器且缺少包时显示。
- 更新缺失的软件包：T AWS ransform 在 “缺少的包依赖关系” 表中列出了缺失的软件包。您可以在搜索框中按名称搜索丢失的包裹。此表包含有关丢失包裹的以下详细信息：
  - Name
  - 关联的存储库

- 框架版本状态
- 核心版本状态

要解决缺少的软件包依赖关系，上传丢失的软件包.

上传丢失的软件包

1. 如果您愿意，可以下载 Windows PowerShell 帮助脚本，以便从Visual Studio开发环境中检索缺少的软件包依赖关系。或者你可以手动找到丢失的包裹。

   要使用 Windows PowerShell 脚本，请执行以下操作：

   a. 选择 “下载 Windows PowerShell 脚本”。

   b. 在本地运行脚本，并与包含缺少软件包依赖文件的存储库保持活动连接。

   c. 此脚本允许您将缺少的软件包依赖项下载到本地环境。
2. 该脚本将创建一个 zip 文件供您上传，其中包含一个存档中的所有依赖项。您也可以为每个依赖项上传单个文件.nupkg或 zip 文件。
3. 选择 “上传包文件”。
4. 在 “上传依赖文件” 模式中，选择 “选择文件”，然后浏览到设备上丢失的压缩包文件的位置。
5. 选择上传。
6. AWS 转换会验证您上传的文件。在验证期间，您无法进行任何更新。 AWS Transform 会报告 “缺少包依赖关系” 表上方的验证状态。
7. AWS Transform 还会将 “缺少包依赖关系” 表中的状态列从 “缺失” 更新为 “已解决”。如果包验证失败，则其状态将变为 “无效”。对于无效文件，请执行以下操作：

   a. 在 “缺少软件包依赖关系” 表中，使用复选框选择无效的软件包。

   b. 选择 “移除已上传的文件”。

   c. 这会将其状态更改回 “缺失”。
8. 上传缺失的软件包并解决了软件包依赖关系后，选择 “继续查看”。

   如果您选择继续查看而不解决缺失的包依赖关系，T AWS ransform 会询问您是否要在不丢失包的情况下启动转换作业。如果选择 “忽略缺少的包依赖关系”，则 Trans AWS form 将使用程序集引用来转换代码。继续执行此操作可能会影响相关资源。

文件夹结构要求

要 NuGet 上传， AWS 转换需要以下任一条件：

- 要放置在根级别的.nuspec文件，用于手动上传的软件包，或
- 使用提供的 PowerShell 脚本生成正确的结构

版本匹配要求

- 框架状态：T AWS ransform 尝试将.csproj文件（源代码）中指定的依赖项版本与上传的依赖项版本相匹配。完全匹配的结果为 “成功” 状态。
- 核心状态：T AWS ransform 需要在上传.nuspec文件的依赖项部分中提供核心版本规范。如果找到一个，则核心状态为 “成功”。

  格式示例：

```
<dependencies>
    <group targetFramework="net8.0" />
</dependencies>
```

  常见版本包括：

  - .NET 5.0 (net5.0)
  - .NET 6.0 (net6.0)
  - .NET 7.0 (net7.0)
  - .NET 8.0 (net8.0)

审查您的计划，为转型做好准备

在确认您的仓库为转型做好准备、和之后解析软件包依赖关系以准备转换，AWS 账户管理员必须审核转换计划并在 Trans AWS form 中批准该计划。

AWS Transform 显示作业中选定进行转换的存储库、依赖存储库和依赖包的列表。

审查转型计划

AWS Transform 显示作业中选定进行转换的存储库、依赖存储库和依赖包的列表。

> **Note**
>
> AWS 对于每个转换计划，Transform 最多可以转换 100 个依赖项和存储库。

1. 如果您不是 AWS 账户管理员，请查看工作计划，如果接受，请选择 “发送以供批准”。
2. 如果您是 AWS 账户管理员，则必须查看计划，准备就绪后，批准计划才能开始转换。查看工作计划后，选择以下任一选项：
   a. 拒绝如果任务是由非 AWS 账户管理员的用户创建的，我们建议您通知任务创建者重新启动该作业。
   b. 批准并开始转型。

工作审查包括以下细节：

1. Job 摘要这包括：
   a. AWS 变换将放置转换后的代码的目标分支。
   b. 目标.NET 版本，.NET 8.0 或.NET 10。
   c. 作业设置：
      i. 排除.NET 标准项目
   d. 选择进行转换的存储库数量
   e. 依赖存储库的数量
   f. 私人 NuGet 套餐数量
   g. 作业的代码总行数
2. 已选择的存储库这些是选定进行转换的存储库。它们必须是 MVC、Web、Windows 通信基金会 (WCF)、控制台、类库、用户界面框架-Razor 页面或单元测试包。该表格包含以下信息：
   a. Name
   b. 源分支
   c. 支持的项目
   d. 代码行
   e. 检测到的项目
   f. 已跳过的项目
   g. 检测到依赖关系
3. 已添加的依赖存储库这些是为转换而添加的依赖存储库。它们必须是 MVC、Web、Windows 通信基金会 (WCF)、控制台、类库、用户界面框架-Razor 页面或单元测试包。该表格包含以下信息：
   a. Name
   b. 需要由
   c. 源分支

d. 支持的项目

e. 代码行

f. 检测到的项目

g. 已跳过的项目

4. 依赖包这些是为转换而添加的依赖包。它们必须是 MVC、Web、Windows 通信基金会 (WCF)、控制台、类库、用户界面框架-Razor 页面或单元测试包。该表格包含以下信息：

   a. Name

   b. 关联的存储库

   c. 框架版本状态

   d. 核心版本状态

转换您的.NET 代码

AWS 账户管理员完成后审查您的计划，为转型做好准备，您可以在转换任务的 “控制面板” 选项卡上查看转换进度。

> **Note**
>
> 除了转换存储库和依赖关系外，Trans AWS form 还可以执行完全转换的（零构建错误）单元测试项目。 AWS 在转换之前，Transform 无法访问单元测试结果，只能共享转换后的结果。然后，您可以将转换前的基线数据与转换后的结果进行比较，以了解任何潜在的差距。

在右上角，您可以看到作业状态，该状态具有以下值之一：

- 正在等待用户输入
- 时间流逝
- 运行

您还可以看到以下图标：

- 停止转换图标
- 刷新图标
- 设置图标

控制面板提供了转换的高级摘要。它显示转换的任务数量和应用的转换数量的指标，以及完成转换的估计时间。

控制面板包括：

1. 转换 Job 详情部分，其中列出了转换作业的默认设置和详细信息，包括：
   a. 目标分支目标为了转换您的代码，Trans AWS form 会在您的代码存储库中为转换后的代码创建一个新的分支。
   b. 目标.NET 版本，.NET 8.0 或.NET 10
   c. AWS 转换任务 ID。
   d. 作业设置：
      i. 排除.NET 标准项目
2. 转换摘要部分包含：
   a. 选择进行转换的存储库数量
   b. 要转换的项目数量
   c. 这些存储库和项目中的代码总行数

转换开始后，“存储库状态”、“Package 状态” 和 “单元测试状态” 部分会显示饼图，实时显示进度。单元测试状态显示位于存储库中的单元测试的状态， AWS Transforms 在转换后运行这些单元测试以测试转换后的代码。 AWS Transform 共享已执行的测试结果以及单个测试名称，供客户查看通过和失败的单元测试列表。

> **Note**
>
> 存储库部分列出了 Trans AWS form 推荐的存储库或您选择进行转换的存储库。选择 “下载 JSON”，下载转换计划中的存储库、依赖项和包的列表。

查看转换报告

转换任务完成后，您可以下载转换报告：

- 转换摘要报告：此报告以 HTML 或 JSON 格式概述了转换。从 “控制面板” 选项卡下载转换摘要报告。选择 “下载”，然后选择 “下载为 HTML” 或 “下载为 JSON”。
- 转换详细信息报告：此报告以 HTML 格式提供有关转换的深入信息。从 “控制面板” 选项卡下载转换详细信息报告。在存储库列表中选择 “下载详细报告” 链接以下载详细报告。

与之聊天 AWS 关于转型报告的转换

在完全处理存储库后或 AWS 转换作业完成后，您可以与 Transform 聊一聊转换报告。Worklog 选项卡显示每个可供聊天的存储库的此消息：存储库*repository_name*转换详细信息现在可以在聊天中查看以供查询。转换作业完成后，它会显示以下消息：AWS 转换作业已完成。

要打开聊天，请单击 Web 控制台右下角的紫色六角形图标。

以下是一些示例提示：

- 哪些项目成功转型？
- 哪些项目已部分移植？
- 对repo_name存储库进行了哪些更改？
- project_name项目中升级了哪些软件包？

在 IDE 中实现.NET 现代化

AWS Transform 的 AWS 工具包中包含一个交互式、代理的 AI 助手，用于。Visual Studio它使您能够直接在 IDE 中通过对话式分步指导体验实现应用程序现代化。要转换.NET 解决方案或项目，Transfor AWS m 代理会分析您的代码库，确定移植应用程序所需的更新，并在转换开始之前生成评估报告和转换计划。

Visual StudioIDE 体验仅支持通过 IAM 身份中心进行身份验证。有关更多信息，请参阅 在 IAM Identity Center 中添加用户。

IDE 体验提供自主模式和交互模式。使用自主模式进行无人值守的转换，适用于夜间或长时间运行的工作。使用交互模式在聊天中与代理一起工作，对转型具有很高的可见性、可自定义的转型计划以及对每个项目的分步审查。您可以迭代以细化结果或改变方向，直到满意为止。

当转换作业处于活动状态时，您可以与三个窗口进行交互：

- 聊天窗口是您与转换代理的主要互动点。使用聊天功能提问、讨论选项、引导转型和迭代。
- T AWS ransform Job Plan 窗口显示进度步骤，您可以在其中下载或上传构件或查看代码更改差异。
- Worklog 窗口以自然语言显示转换活动日志。

AWS Transform 执行四项关键任务将.NET 应用程序移植到 Linux

- 升级.NET 和语言版本-将较旧的.NET C# 代码升级到当前的.NET 和语言版本。

- 从 .NET Framework 迁移到跨平台 .NET：将依赖 Windows 的 .NET Framework 项目及包迁移到兼容 Linux 的跨平台 .NET。
- 重写代码以实现 Linux 兼容性：对已废弃、低效的代码组件进行重构和重写。
- 生成 Linux 兼容性就绪报告 — 对于需要用户干预才能在 Linux 上构建和运行代码的开放式任务，Transform 会提供一份详细报告，说明 AWS 转换后配置应用程序所需的操作。

有关 AWS 转换如何执行.NET 转换的更多信息，请参见操作方法 AWS 转换可实现.NET 应用程序的现代化。

要使用 Visual Studio IDE 中的 AWS 转换实现.NET 代码的现代化，请参阅以下内容：

- 使用现代化.NET AWS 变身 Visual Studio
- 操作方法 AWS 转换可实现.NET 应用程序的现代化
- 在 IDE 中排查 .NET 转换问题

配额

有关 IDE 中的 AWS 转换.NET 转换配额，请参见的配额 AWS 转换。

使用现代化.NET AWS 变身 Visual Studio

在 2026 年或 Visual Studio 2022 年完成以下步骤，使用 T AWS ran Windows-based sform 将.NET 应用程序移植到 Linux-compatible 跨平台的.NET 应用程序。

步骤 1：先决条件

在继续操作之前，请确保已从 Visual Studio Marketplace 下载并安装了 Amazon Q 的AWS Toolkit 扩展程序。查看.NET 现代化的 AWS 转换功能和限制，确认您的代码可以转换。

第 2 步：在视觉工作室中进行身份验证

要通过 Visual Studio 的 Toolkit for Visual Studio 连接到您的 AWS 帐户，请打开 AWS Toolkit 用户界面入门（连接用户界面）：

1. 在 Visual Studio 主菜单中，导航到扩展 > AWS 工具包 > 入门，打开 “入门： AWS 工具包” 页面。
2. 选择 “AWS 转换身份验证”。

3. 选择现有个人资料或创建新个人资料。创建新配置文件时，请输入配置文件的名称和您的 AWS 转换起始网址，该网址是在管理员将您添加到 IAM Identity Center 后通过电子邮件发送给您的。
4. 选择连接。按照提示登录并通过 Web 浏览器授予访问权限。在 Visual Studio 中，您应该看到已连接到 IAM 身份中心。
5. 登录后，您将被带到AWS 转换控制面板。在此登录页面上，您可以执行以下操作：

   - 选择 AWS 转换配置文件（区域）
   - 选择或创建工作区
   - 查看转换任务的状态

第 3 步：转换您的应用程序

要转换您的 .NET 解决方案或项目，请完成以下步骤：

开始转型

1. 打开要转换的任何 C# 或 VB.NET 基于 C# 或基于 Visual Studio C# 的解决方案或项目。
2. 在解决方案资源管理器中，右键单击要转换的解决方案或项目，然后选择 Port with Tran sfor AWS m。
3. 出现 “带 AWS 变换的端口” 对话框。

   a. 在 “选择工作空间” 下拉列表中，创建工作区或选择现有工作空间。工作区使您的活动在 Transfor AWS m Web 应用程序中可见，您可以在其中邀请协作者查看和聊聊转换作业。
   b. 在选择 .NET 目标版本下拉菜单中，选择您要升级到的 .NET 版本。
   c. 在 “转换模式” 中，选择 “自主” 进行无人值守转换，选择 “交互” 进行交互式转换。
   d. 选择 “开始” 开始转换。
4. 转换作业开始后，将出现 “AWS 转换作业计划”、“聊天” 和 “工作日志” 窗口。

评估和转型计划

1. Trans AWS form 分析您的代码后，将在聊天中显示评估报告和转换计划。在互动模式下，聊天将暂停供您查看。如果您不想在聊天中评论，则可以使用以下替代方法：

   - 要在代码编辑器中查看评估或计划，请在 Trans AWS form Job Plan 窗口中选择显示评估或显示转换计划。
   - 要下载评估或计划，请使用 Job Plan 窗口中的下载图标。

2. （可选）修改转换计划。您可以通过聊天来讨论计划，例如探索其他选项。您可以通过在聊天中给出说明来更改计划，或者使用 Job Plan 窗口中的下载图标上传修改后的转换计划。您可以自由添加、删除或修改步骤。Chat 将通过修改后的计划来确认其对您的指示的理解。
3. （可选）上传转向文件。在聊天窗口中，使用上传图标上传指导文档，例如应用程序规范、组织技术堆栈偏好和惯例或编码示例。上传指导文档后，在聊天窗口中对其进行描述以向代理提供上下文。
4. 一旦你对计划感到满意，在聊天中给予批准，转换就会开始。
5. 在交互模式下，您可以将检查点设置为在项目转换以供审阅后停止。“Job Plan” 窗口中 “转换代码” 下的步骤将带有圆形检查点图标。默认情况下，所有项目都启用了检查点。使用复选框清除或设置检查点。

转型和检查点审查

1. AWS 转换开始转换您的代码。您可以在 “转换 Job Plan” 窗口中监控 AWS 转换步骤的进度。Job Plan 窗口显示预计的最长剩余时间和您的作业 ID。
2. 项目转换后，会在聊天中显示摘要并应用代码更改。
3. 在交互模式下，当到达检查点时，代理将暂停，以便您可以查看结果。在 “Job Plan” 窗口中，您将看到一个查看结果按钮，该按钮暂停在该按钮上，您可以查看代码差异。查看更改后，您可以在聊天中要求进一步更改或在聊天中自行更改代码Visual Studio。
4. 您可以根据需要在检查点进行迭代。当你满意时，请指示聊天继续，聊天将转到下一个项目。

转型结束

1. 转换项目后，.NET 代理将触发本地构建Visual Studio，以确认代码在本地计算机上成功构建。如果存在错误，它将努力解决这些错误。
2. 转换完成后，可能需要执行其他步骤，例如 Trans AWS form 无法执行的转换任务，或者为 Linux 兼容性而需要进行更改。后续步骤 markdown 文件 (NextSteps.md) 可供下载，您可以将其用作 AI 代码伴侣的提示。使用 Job Plan 窗口的下载图标按钮进行下载NextSteps.md。
3. 您可以继续在聊天中互动，提问或请求其他更改。
4. 当你准备好结束转型工作时，告诉聊天室。

操作方法 AWS 转换可实现.NET 应用程序的现代化

有关使用转换进行.NET AWS 转换的工作原理的详细信息，请查看以下各节。

分析应用程序并生成转换计划

在 AWS 转换开始之前，Transform 会在本地构建您的代码，以验证代码是否可构建并正确配置以进行转换。如果代码未生成，Trans AWS form 将提示是否继续转换。 AWS 然后，Transform 会将您的代码上传到安全的加密编译环境 AWS，分析您的代码库，并确定移植应用程序所需的更新

在此分析过程中，Trans AWS form 会将您的.NET 解决方案或项目划分为多个代码组。代码组指一个项目及其所有依赖项的集合，它们共同构成一个可编译的代码单元，如动态链接库（DLL）或可执行文件。即使你没有选择所有要 AWS 转换的项目依赖关系，Transform 也会确定生成所选项目所需的依赖关系，并对它们进行转换，这样转换后的应用程序就可以构建并准备好使用。

分析您的代码后，Trans AWS form 会生成一份转换计划，其中概述了将要进行的拟议更改，包括将要转换的代码组及其依赖项的列表。

转换应用程序

要开始转 AWS 换，Transform 在安全的编译环境中再次构建您的代码，以验证其是否可以远程构建。AWS 然后，Transform 开始移植您的应用程序。转换采用“自下而上”的方式：从最低层级的依赖项开始处理。如果 T AWS ransform 在移植依赖项时遇到问题，它会停止转换并提供有关导致错误的原因的信息。

转换包含对应用程序的以下更新：

- 用 C# 版本替换过时的 Linux-compatible C# 版本的代码
- 将 .NET Framework 升级到跨平台 .NET，具体包括：
  - 识别并迭代替换包、库和 API
  - 升级和替换 NuGet 软件包和 API
  - 迁移到跨平台运行时
  - 配置中间件并更新运行时配置
  - 替换私有或第三方包
  - 处理 IIS 和 WCF 组件
  - 调试编译错误
- 重写代码以实现 Linux 兼容性，包括对已废弃、低效的代码进行重构和重写，以适配现有代码的移植需求

查看转换报告并接受更改

转换完成后，Transform 会提供一份 AWS 转换报告，其中包含有关其对应用程序所做的拟议更新的信息，包括更改的文件数量、更新的软件包数量和 API 更改的数量。它会标记所有未成功完成的转换（包括受影响的文件或文件片段、尝试编译时遇到的错误）。您还可查看包含编译日志的编译摘要，进一步了解已执行的变更。

转换报告还提供了 Linux 移植状态，表明是否需要额外的用户输入才能使应用程序 Linux 兼容。如果代码组中的任何项目需要您输入，则可以下载一份 Linux 就绪报告，其中包含 T AWS ransform 在构建时无法解决的 Windows-specific 注意事项。若任一代码组或文件需要人工干预，请查看报告以了解仍需执行的变更类型，以及（如适用）代码更新建议。这些变更必须手动完成，应用程序才能在 Linux 上运行。

您可以先在差异视图中查看 T AWS ransform 所做的拟议更改，然后再将其接受为文件的就地更新。完成文件更新并处理 Linux 就绪报告中的所有事项后，您的应用程序即可在跨平台 .NET 环境中运行。

你可以下载 Next Steps markdown 文件，其中包含使用 AWS 变换或 AI 代码配套继续转换的提示。要下载文件，请选择报告右上角的 “下载后续步骤” 按钮。

在 IDE 中排查 .NET 转换问题

使用以下各节来解决在 IDE 中使用转换进行.NET AWS 转换的常见问题。

如何判断任务是否在正常推进？

您应该在 “工作日志” 窗口中看到常规活动。如果 T AWS ransform 在 “AWS 转换作业计划” 窗口中的某个步骤上花费了很长时间，则可以在输出日志中检查该作业是否仍处于活动状态。若日志中持续生成诊断信息，则说明任务仍在正常执行。

要查看输出，请在中选择 “输出” 选项卡Visual Studio。在显示以下来源的输出:菜单中，选择 Amazon Q 语言客户端。

以下屏幕截图显示了 Transform 在 AWS 转换期间生成的输出示例。

为何部分项目未被选中进行转换？

AWS 转换只能转换支持的.NET 项目类型。有关支持的项目类型及 .NET 项目转换的其他先决条件，请参阅步骤 1：先决条件。

如果我的项目或解决方案没有转型，我该如何获得支持？

如果您无法自行解决问题，可以联系 支持 或您的 AWS 账户 团队提交支持案例。

要获得支持，请提供转换任务 ID， AWS 以便调查失败的作业。要查找转换任务 ID，请选择中的输出选项卡Visual Studio。在显示以下来源的输出:菜单中，选择 Amazon Q 语言客户端。

如何避免防火墙干扰转换作业？

如果您的组织使用防火墙，则可能会干扰中的Visual Studio转换。您可以暂时禁用安全检查 Node.js ，以排除故障或测试导致转换无法运行的原因。

环境变量 NODE_TLS_REJECT_UNAUTHORIZED 控制着重要的安全检查。设置NODE_TLS_REJECT_UNAUTHORIZED为 “0” 将禁用 Node.js拒绝未经授权 TLS/SSL 的证书。这意味着：

- Self-signed 证书将被接受
- 允许过期证书
- 允许主机名不匹配的证书
- 忽略其他所有证书验证错误

如果您的代理使用自签名证书，可设置以下环境变量（无需禁用 NODE_TLS_REJECT_UNAUTHORIZED）：

```
NODE_OPTIONS = –use-openssl-ca
NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs
```

否则，您必须指定代理使用的 CA 证书，才能禁用 NODE_TLS_REJECT_UNAUTHORIZED。

要在 Windows 上禁用 NODE_TLS_REJECT_AUNTHERIZED

1. 打开“开始”菜单，搜索环境变量。
2. 选择编辑系统环境变量。
3. 在系统属性窗口中，选择环境变量。

4. 在系统变量下，选择新建。
5. 设置变量名为 NODE_TLS_REJECT_UNAUTHORIZED，变量值为 0。
6. 选择确定，保存更改。
7. 重新启动 Visual Studio。

移植 UI 层代码

AWS Transform 可以将 ASP.NET 网站的用户界面层移植到与 ASP.NET Core 兼容的 UI 框架，该框架可以在 Linux 上运行。有以下转换可供选择：

- MVC Razor 用户界面移植
- 将 Web 表单移植到 Blazor 用户界面

MVC Razor 用户界面移植

ASP.NET 带有 Razor Views 用户界面的 MVC 项目可以移植到 C ASP.NET ore 上的 MVC Razor Views 中，保持在同一个用户界面框架上。虽然与 C ASP.NET ore 之间 ASP.NET 的 Razor 视图类似，但有一些差异需要更改移植代码：

- ASP.NET MVC Razor 视图使用 System.Web.Mvc 命名空间，并且与.NET 框架紧密相关。
- ASP.NET Core Razor Views 采用模块化构建 Microsoft.AspNetCore.Mvc，并改进了依赖注入。
- ASP.NET Core 具有新功能，包括标签助手和视图组件。

AWS Transform 会检测并移植 Razor Views 中常见的不兼容组件和结构。

将 Web 表单移植到 Blazor 用户界面

ASP.NET Web 表单用户界面在 C ASP.NET ore 上没有对应的界面。 AWS Transform 可以将 Web 表单用户界面层代码移植到 Core 上 ASP.NET 的 Blazor 服务器 为目标 UI 框架重写了 UI 层代码。

要启用或禁用 Web 表单到 Blazor 用户界面的移植，请选中或清除 “将用户界面 ASP.NET Web 表单转换为 Blazor” 作业设置。

转型细节

您的 Web 表单项目已转换为使用服务器端托管的 Blazor 项目。在转换过程中对项目和文件进行了以下更改：

文件转换映射

来源	目标	说明
.aspx、.ascx	*.razor	.aspx 页面和.ascx 自定义控件变为.razor 文件
Web.config	appsettings.json	Web.config 设置变成 appsettings.json
Global.asax	Program.cs	Global.asax 代码变成 Program.cs 代码
*.master	*layout.razor	主文件变为布局.razor 文件

Post-transformation 项目结构

转换后，转换后的文件位于以下项目位置：

- 组件文件夹：所有 razor 组件 (*.razor) 都放置在与项目.csproj 文件相同级别创建的组件文件夹中。
- 页面映射：Web 表单页面 (*.aspx) 转换为 Components/Pages 文件夹结构。
- 控件映射：Web 表单控件 (*.ascx) 直接放置在 “组件” 文件夹下。

限制和不支持的功能

目前不支持以下功能。如果您的工作负载使用这些功能，则需要手动移植该代码或在转换后与 AI 代码配套一起移植。

- .svc 文件（服务文件）
- .ashx 文件（通用处理程序文件）
- 服务参考和网络引用（reference.map、reference.cs、.wsdl 文件）
- .aspx（Web 表单）文件和.cshtml（Razor）文件混合在同一个项目中
- .NET AWS 转换尚不支持对项目类型的依赖关系
- Third-party 供应商用户界面 libraries/controls
- 网站项目

仅支持 Web 应用程序项目（包含.csproj 文件）。要将网站项目转换为 Web 应用程序项目，请参阅 Microsoft 指南将网站项目转换为 Web 应用程序项目。

转型报告

.NET 转换任务完成后，将提供以下转换报告：

- 转型摘要报告
- 转换详细信息报告

转型摘要报告

转换作业完成后，Web 控制台中将提供转换摘要报告。从 “控制面板” 选项卡下载转换摘要报告。选择 “下载转换摘要报告”，然后选择 “下载为 HTML” 或 “下载为 JSON”。

转换摘要报告概述了转换情况，并提供了每个已转换存储库的特定信息，包括：

- 作业详细信息
  - 转型工作概述
  - 转换结果概述
  - 文件概述
- 存储库列表，对于每个存储库：
  - 存储库名称概述
  - 解决方案转型摘要
  - 项目详细信息，包括状态、类型、.NET 版本、代码总行数、转换后的代码行和已更改的文件

转换详细信息报告

转换作业完成后，Web 控制台和 IDE 用户均可使用转换详细信息报告。

- Web 控制台用户：每个转换后的存储库都有一份详细报告。在 “控制面板” 选项卡上，使用存储库列表中的下载详细报告链接下载详细报告。
- IDE 用户：使用下载图标从 “转AWS 换 Job Plan” 窗口下载转换报告。

转换详细信息报告是一个交互式 HTML 报告。它包含有关转换的深入信息，包括文件更改的原因和可操作的错误详细信息。信息按以下层次结构排列：

- Job 信息
- 对于每种解决方案：

- 解决方案转型摘要
- 转型概述
- Projects
- 对于每个项目：
  - 项目摘要
  - 生成错误摘要
  - NuGet 包裹变更
  - 文件更改
  - 编译错误
- 单元测试结果
- Linux 就绪报告

有关带有示例的转换详细信息报告章节的演练，请参阅博客文章 “宣布为.NET 进行 AWS 转换” 详细的转换报告。

.NET 转换的最佳实践

遵循本指南，通过 T AWS ransform 获得更好的.NET 现代化成果。这些最佳做法适用于.NET 对话式 AI 助手，该助手目前可用于 Visual Studio IDE。

主题

在你变身之前

在开始.NET 转换作业之前，请查看以下建议。

使用.NET 对话式 AI 助手

使用新的.NET 代理以获得最佳转换结果。对话式人工智能助手可Visual Studio通过 Visual Studio 的 AWS Toolkit for Visual Studio 获得。通过 AWS 变换和转 AWS 换 MCP 代理的Kiro强大功能，它也可用于Kiro或其他 IDE。新的.NET 代理尚未在 Web 控制台中可用。

如果目标不是.NET 到.NET 的转换，请使用其他工具

AWS .NET 的转换适用于.NET Framework 到.NET 代码现代化以及.NET 升级到更高版本。它不适用于包含非.NET 语言（例如 Java）或非.NET 框架（例如 React）的转换。它也不提供应用程序架构重构。使用自定义AWS 转换或Kiro进行此类现代化改造。

使用稳定版的 Visual Studio，最好是 VS2026

使用 GA 版Visual Studio而不是预览版或 Insiders 版，以避免预览软件的复杂性。该 AWS 工具包可以与 Visual Studio 2026 年或 2022 年一起使用。推荐使用 VS2026，因为它的性能更好，内存消耗也更少。

使用最新的 AWS 的工具包 Visual Studio

请继续关注最新版本的 AWS Toolki Visual Studio t，了解错误修复和功能更新。你可以在 “扩展” > “管理扩展” > “已安装” 中查看工具包版本并进行升级。

在里面工作 Visual Studio 适用于中等或更高复杂度的项目的 IDE

IDE 体验为您提供了最深入的转换视图，在转换项目时，您可以与.NET 代理一起工作。对于中、高或关键复杂度的项目，请使用 IDE 而不是 Web 控制台。

制定验证计划

决定在应用程序转换后如何验证其正确性。 Post-transformation，你需要确认它在运行时行为和外观是否正确，并且安全控制、业务逻辑和数据存储完好无损。是否会 and/or 使用测试自动化手动进行验证？ 如果您的解决方案包含单元测试，Transfor AWS m 将为您移植它们并执行它们，结果将显示在转换报告中。

提供 NuGet 私有包依赖关系

如果您的解决方案依赖于私有包，请确保它们在本地计算机上可用，以便 IDE 和 Trans AWS form 可以找到它们。

指定更换包裹或询问代理建议

对于没有现代.NET 版本的软件包，您可以自定义转换计划以指定您想要的软件包替代方案，也可以向代理寻求建议。

在你确定不想再做任何改变之前，不要结束你的工作

转换完成后，如果您想进行其他更改，请不要立即结束工作。在你说完成之前，转型才会完成。在将任务标记为完成之前，您可以要求进行更改。

转换后，交给 AI 代码伴侣来完成您的应用程序

期望将 T AWS ransform 与 AI 代码配套组合，例如Kiro。一种常见的模式是先使用 Transform for .NET 进行 AWS 转换，然后交给 AI 代码伴侣来完成应用程序。最终确定工作可能包括识别和纠正运行时错误、行为问题和用户体验样式。

在现代化之旅中，可以 AWS 将 Transform 想象成带你实现目标的快速旅行，将 AI 代码伴侣想象成带你前往最终目的地的本地旅行。

为了帮助从 T AWS ransform 移交给 AI 代码伙伴，Transform 在 AWS 转换结束时提供了 HTML 转换报告和下一步降价文档。

评估和规划

开始 AWS 转换作业后，Transform 会分析您的代码并生成评估报告和转换计划。使用以下最佳实践来充分利用此阶段。

查看评估并提出问题以设定您的期望

仔细审查评估结果，以了解哪些项目难以转型，以及为什么。代理介绍具有复杂性级别（低、中、高、关键）的项目，并解释了为什么它们具有该等级。

提问以更多地了解具有挑战性的领域。例如：

- 询问代理对项目转型或用例的信心程度。
- 询问代理使用 AI 代码伴侣可能需要执行哪些转换后任务。

查看计划并与代理商讨论选项

代理提供转型计划供您审核。您可以讨论和修改此计划。首先要了解您的选择。询问代理商除了计划的任何部分之外还有哪些替代方案。

例如，转型计划可能提议将WCF服务转换为 ASP.NET Web API。但是，您的组织更愿意留在WCF。你向代理询问选项，然后得知另一种选择是将它们转换为CoreWCF。

上传指导文件，为您的组织量身定制计划

最初的转型计划是在不了解贵组织的要求和偏好的情况下制定的。您可以将组织惯例、应用程序规范、首选技术堆栈和首选编码模式示例告知代理人。

上传指导文件后，对其进行解释以向代理提供背景信息。利用指导文件中的其他信息，代理可以根据您的组织喜欢的工作方式准备一份量身定制的计划。

自由定制计划

.NET 代理非常灵活，您可以在.NET 到.NET 的转换域内自由自定义转换计划。你可以在聊天中要求更改计划，或者如果你愿意，也可以使用 markdown 文件。审查并完善计划，直至满意。

如果计划需要由多个利益相关者审核，则可以将该计划下载为降价文件，进行共享，然后再上传自定义计划。

例如，您可以查看转换计划，并决定要将类库项目转换为.NET Standard 而不是.NET 10。在聊天中，你说：“修改将所有类库转换为.NET Standard 2.0 的计划”，然后代理会向你提供修改后的计划。

以交互方式或自主方式转型

Visual StudioIDE 体验提供自主和交互模式，用于控制转换过程中的交互程度。

使用交互模式和自主模式来控制交互程度

你可以在开始转换时选择模式，也可以随时通过聊天窗口顶部的下拉菜单进行更改。

- 使用自主模式进行无人值守的转换，适用于夜间或长时间运行的工作。您仍然有机会查看结果，并在工作结束时要求进行更改。
- 在整个转型过程中，使用交互模式与代理一起聊天，制定可自定义的转型计划，对转型细节的高度可见性以及对每个项目的分步审查。您可以迭代以细化结果或改变方向，直到满意为止。

你可以组合模式。例如，从交互模式开始查看和调整转换计划，然后切换到自主模式以自动转换项目。

请代理解释代码更改

如果您看到不明白的代码更改，请让代理对其进行解释。

使用检查点在项目中停下来进行审查或更改

在交互模式下，批准计划后，您可以为每个项目设置或清除检查点。转换带有检查点的项目后，转换后的代码将应用于 IDE 中的项目，代理会暂停供您查看。您可以查看结果，如果您不喜欢它们，可以要求进行更多更改。

在检查站停下来时，你可以：

- 查看聊天中显示的结果，并在聊天中提问。例如：“你为什么要更改文件 X 中的加密 API？”
- 在 “ AWS 转换 Job Plan” 窗口中选择项目的 “查看结果” 按钮，即可查看代码更改。

- 通过要求进行其他更改来完善转换。例如：“将其更改为使用 logger X” 或 “将其更改为使用包 X 而不是包 Y”。
- 重试转换，按照不同的指令完成转换。例如：“将此类库更改为以.NET Standard 而不是.NET 10 为目标” 或 “重试此转换并将目标从Blazor更改为 MVC Razor Pages”。
- 在 IDE 中自行更改代码。
- 告诉代理继续进入下一个项目检查点。

迭代直到满意

现代化本质上是迭代的，你可以期望使用代理进行迭代。你可以在项目检查点进行更改，也可以在转换结束时进行更改。根据需要进行迭代，直到您满意为止。在你说完成之前，转型才会完成。

在检查点停下来时与代理一起编码

在使用代理时，您可以自己更改代码。当在检查点停下来时，可以在中编辑代码文件Visual Studio。当您指示代理继续操作时，您的更改将同步。

验证和定稿

转换完成后，验证转换后的应用程序并最终确定以供生产使用。

查看转型报告和后续步骤，以了解已完成的内容和剩余的内容

查看 HTML 转换报告以了解已完成的工作。查看后续步骤 markdown 文件，了解还有哪些任务还剩下。请代理人澄清任何不清楚的地方。

使用 AI 代码配套来验证、调试和完成您的应用程序

检查转换后的应用程序是否正确。使用 AI 代码配套工具（例如）Kiro来解决问题。

验证单元测试

如果您的解决方案包含单元测试项目（NUnitxUnit、或MSTest），Transfor AWS m 会将它们移植到现代.NET 并为您运行测试。查看 HTML 转换报告，了解单元测试结果。使用 AI 代码配套更正失败的测试。

验证应用程序功能

运行您的应用程序并确认其功能与原始功能相匹配。注意功能问题和运行时错误。使用 AI 代码伴侣更正。

验证应用程序 UI

运行您的应用程序并确认其外观和行为与原始应用程序相同，包括导航和路由。如果您的应用程序没有样式，则可能是.css 文件不在正确的位置。使用 AI 代码伴侣更正。

SQL 服务器现代化

AWS SQL Server 现代化转型是一项 AI-powered 服务，可自动将微软 SQL Server 数据库及其关联的.NET 应用程序的全栈现代化改造到亚马逊 Aurora PostgreSQL。该服务协调了从架构转换、数据迁移和修改应用程序代码以匹配新目标 PostgreSQL 的整个迁移过程，通过自动执行复杂和劳动密集型任务来提高团队的工作效率。

支持的区域

AWS SQL Server 转换已在美国东部（弗吉尼亚北部）推出-us-east-1

Cross-Region 用法：对于不支持区域的数据库，您可以将数据库克隆到支持的区域进行转换，然后将结果部署回目标区域。

功能和关键特性

数据库转换

- 架构转换：自动将 SQL Server 架构转换为 Aurora PostgreSQL，包括表、视图、索引、约束和关系
- 存储过程转换： AI-enhanced 准确地 PL/pgSQL 将 T-SQL 存储过程转换为
- 数据迁移：使用 AWS 数据库迁移服务 (DMS) 通过完整性验证迁移数据
- 数据库对象：支持触发器、函数、视图、计算列和标识列
- 验证：自动数据完整性验证和参照完整性检查

应用程序转型

- 实体框架转换：更新 PostgreSQL 的实体框架 6.3-6.5 和 EF Core 1.0-8.0 配置
- ADO.NET 转换：将 ADO.NET 数据访问代码从 SQL Server 转换为 PostgreSQL 提供程序。
- 连接字符串更新：自动将所有数据库连接字符串更新到新的目标 PostgreSQL 数据库
- 数据库提供程序变更：用 Npgsql（PostgreSQL 提供程序）替换 SQL Server 提供程序

- ORM 配置更新：修改数据类型映射、标识列和特定于数据库的配置

编排验证 &

- Wave-based 现代化：将大型房地产组织到合乎逻辑的迁移阶段
- 依赖关系映射：识别应用程序和数据库之间的关系
- Human-in-the-loop (HITL) 检查点：在关键阶段提供审查和批准大门
- 自动验证：测试架构兼容性、数据完整性和应用程序功能
- CI/CD 集成：与现有开发管道集成

部署

- Amazon ECS 和 Amazon EC2 部署：支持自动扩展的自动容器化部署
- Infrastructure-as-code 生成：创建 CloudFormation 或 AWS CDK 模板
- 自动部署验证：通过运行状况检查验证部署成功
- 回滚功能：在出现问题时支持回滚程序

支持的版本和项目类型

SQL Server 版本

AWS 转换支持以下 SQL Server 版本：

SQL Server 版本	支持状态
SQL Server 2022	支持
SQL Server 2019	支持
SQL Server 2017	支持
SQL Server 2016	支持
SQL Server 2014	支持
SQL Server 2012	支持

SQL Server 版本	支持状态
SQL Server 2008 R2	支持

> **Note**
>
> 支持所有 SQL Server 版本（快速、标准、企业版）。SQL Server 可以托管在 AWS（适用于 SQL Server 的 Amazon RDS 或亚马逊 EC2 上的 SQL Server）上，也可以托管在外部 AWS。

.NET 版本

.NET 版本	支持状态
.NET 10	支持
.NET 8	支持
.NET 7	支持
.NET 6（核心）	支持
.NET 框架 4.x 及更早版本	不支持

> **Important**
>
> 不支持旧版.NET 框架 4.x 及更早版本。如果您的应用程序使用.NET 框架，则在使用 SQL Server 转换功能之前，必须先使用 AWS 变换进行.NET 现代化升级到.NET Core 6+。

实体框架版本

框架	受支持的版本
实体框架 6	6.3、6.4、6.5

框架	受支持的版本
实体框架核心	1.0 到 8.0
ADO.NET	所有版本 (GA)

源代码存储库

AWS Transform 支持以下源代码平台：

- GitHub 和 GitHub 企业服务器
- GitLab.com 和 GitLab Self-Managed
- Bitbucket 云和比特桶数据中心
- 天蓝色 DevOps 和 Azure DevOps 服务器
- Amazon S3

目标数据库

AWS 转换目标亚马逊 Aurora PostgreSQL（兼容 PostgreSQL 15+），支持最新的 Aurora 功能和优化。

技术要求

数据库要求

- 微软 SQL Server 版本 2008 R2 到 2022
- SQL Server 托管在 AWS （适用于 SQL Server 的 Amazon RDS 或亚马逊 EC2 上的 SQL Server）上或托管在 AWS
- 对于 AWS托管的数据库，数据库和 T AWS ransform 必须位于同一 AWS 区域。
- 对于托管在外部的数据库 AWS，需要与 Trans AWS form 服务的网络连接。
- 具有 “查看定义” 和 “查看数据库状态” 权限的数据库用户
- 数据库密码仅使用可打印的 ASCII 字符（不包括 '/'、'@'、"" 和空格）
- 包含源 SQL Server 的 VPC 必须在至少 2 个不同的可用区中拥有子网（DMS 复制子网组是必需的）

申请要求

- .NET 酷睿 6、7 或 8 应用程序
- 实体框架 6.3-6.5 或实体框架核心 1.0-8.0，或 ADO.NET
- 可在源代码中发现数据库连接
- 应用程序成功构建并运行
- 支持的存储库平台中的源代码

AWS 账户要求

- AWS 具有管理员访问权限的账户
- 已启用 IAM 身份中心
- 已创建所需的服务角色（参见下面的设置说明）
- 具有适当网络配置的 VPC

数据处理和存储

处理地点

- 架构处理发生在您的 VPC 中的 DMS 实例中
- 数据迁移是可选的，如果需要，可以将其排除在外
- 转换对象存储在 AWS 转换服务区域中

存储的工件

以下项目存储在服务区域中：

- Agent 日志
- 评测结果
- SQL 架构文件
- DMS 输出伪影

> **Important**
>
> 对数据驻留很重要：即使选择退出数据迁移，元数据和处理工件也存储在服务区域中。这对于具有严格数据驻留要求的组织非常重要。

Artical 管理

- 客户可选择使用您自己的 KMS 密钥进行加密
- 为所有工件定义了 TTL（生存时间）周期
- 可以下载工件进行离线存储

SQL 服务器要求

数据库要求

外部托管的数据库

支持在外部托管的数据库。 AWS 要使用外部托管的数据库，必须确保数据库与 Transfor AWS m 服务之间的网络连接。

SSIS 工作负载

- 限制：不支持 SQL Server 集成服务 (SSIS) 转换。
- 解决办法：使用 AWS Glue 或其他 ETL 服务进行 SSIS 迁移。

链接服务器

- 限制：通过链接服务器连接外部数据库需要人工配置。
- 解决办法：迁移后重新配置链接服务器或使用其他方法，例如数据库链接或应用程序级集成。

复杂的 T-SQL 图案

- 局限性：某些高级 T-SQL 模式可能需要人为干预。
- 解决办法：使用 Amazon Kiro CLI 进行复杂的 SQL 转换。 AWS 转换会标记这些标记，以便在转换过程中进行审查。

申请要求

旧版.NET 框架

- 限制：不支持.NET Framework 4.x 及更早版本。
- 解决办法：先使用适用于.NET 的 AWS 转换升级到.NET Core 6+，然后使用 SQL Server 转换。

实体框架版本

- 限制：仅支持实体框架 6.3-6.5 和 EF Core 1.0-8.0。
- 解决办法：在转换之前升级到支持的实体框架版本。

VB.NET 应用程序

- 限制： VB.NET 不支持。
- 解决办法：转换为 C# 或使用自定义 AWS 转换从 C# 转换转换 VB.NET 为 C#。

Cross-database 依赖关系

- 局限性：数据库架构跨多个数据库进行交互时面临的挑战。
- 解决办法：在迁移之前查看并重构跨数据库查询。可以考虑整合数据库或使用 PostgreSQL 架构。
- 影响：复杂的跨数据库场景可能需要人工干预。

Repository-database 耦合

- 局限性：单个存储库为多个数据库提供服务时面临的挑战。
- 解决办法：考虑存储库重组或分阶段迁移方法。
- 影响：可能需要对基于波的迁移进行额外规划。

基础设施要求

account/region 每份工作仅限一人

- 局限性：每个转换任务都针对一个 AWS 账户和一个区域。

- 解决办法：为多账户或多区域部署创建多个转换任务。

部署目标

- 限制：支持 Amazon ECS 和 Amazon EC2 部署。

存储库要求

私人 NuGet 套餐

- 限制：私有 NuGet 软件包需要额外的配置。
- 解决办法：在开始作业之前 NuGet ，在转换设置中配置私有 Feed。

SQL 服务器安装

在您的 SQL Server 环境中执行以下步骤以启用 AWS 转换现代化。

数据库设置和配置

步骤 1：创建具有所需权限的数据库用户

创建具有必要权限的 T AWS ransform 专用数据库用户。如果您已经有 DMS 架构转换用户，则可以重复使用该用户。

连接到您的 SQL Server 实例并运行以下命令：

```
-- Create the login in master database
USE master;
CREATE LOGIN [atx_user] WITH PASSWORD = 'YourStrongPassword123!';

-- Switch to your application database
USE [YourDatabaseName];
CREATE USER [atx_user] FOR LOGIN [atx_user];

-- Grant required permissions
GRANT VIEW DEFINITION TO [atx_user];
GRANT VIEW DATABASE STATE TO [atx_user];
ALTER ROLE [db_datareader] ADD MEMBER [atx_user];

-- Grant master database permissions
```

```
USE master;
GRANT VIEW SERVER STATE TO [atx_user];
GRANT VIEW ANY DEFINITION TO [atx_user];
```

> **Note**
>
> 对要实现现代化的每个数据库重复特定于数据库的命令（USE、CREATE USER、GRANT）。

db_datareader 角色仅在数据迁移时是必需的，而不仅仅是架构转换所必需的。

- db_datareader 角色授予对数据库中所有表的读取权限
- 只有在执行数据迁移时才需要此角色。
- 仅适用于架构转换（不包括数据迁移），不需要 db_datareader 角色
- 其他权限（视图定义、查看数据库状态等）足以进行架构转换

第 2 步：将凭据存储在 AWS Secrets Manager

将您的数据库凭据安全地存储在 S AWS ecrets Manager 中。如果您已经为 DMS 创建了密钥，请跳过此步骤。

1. 在控制台中导航到 S AWS ecrets Manager
2. 选择 “存储新密钥”
3. 配置密钥：
   - 密钥类型：其他数据库的凭证
   - 数据库：微软 SQL Server
   - 用户名：atx_user（或您选择的用户名）
   - 密码：您创建的密码
   - 服务器名称：您的 SQL Server 端点
   - 数据库名称：您的数据库名称
   - 端口：1433（或您的自定义端口）
4. 选择下一步。
5. 输入秘密名称：atx-db-modernization-sqlserver
6. 添加必需的标签（这些标签是必填的）：

- 关键：项目，价值：atx-db-现代化
- 密钥：所有者，值：数据库连接器

7. 在剩余屏幕中选择 “下一步”
8. 选择商店
9. 记下秘密 ARN，以便在下一步中使用

> **Important**
>
> 数据库密码只能使用可打印的 ASCII 字符，不包括 '/'、'@'、"" 和空格。计划删除的密钥可能会导致转换失败。

步骤 3：创建所需的 DMS 角色

AWS 转换需要特定的 IAM 角色才能进行 DMS 操作。使用下面的 CloudFormation 模板部署这些角色。

> **Note**
>
> 如果您的 AWS 账户已有 DMS-related 角色，请修改此模板以重复使用这些资源，而不是创建重复的角色。

创建一个名为 dms-roles.yaml 的文件，其中包含以下内容：

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'DMS Service Roles for AWS Transform SQL Server Modernization'

Resources:
  DMSCloudWatchLogsRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-cloudwatch-logs-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
```

```
              - dms.amazonaws.com
              - schema-conversion.dms.amazonaws.com
          Action: sts:AssumeRole
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

DMSS3AccessRole:
  Type: AWS::IAM::Role
  Properties:
    RoleName: dms-s3-access-role
    AssumeRolePolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Principal:
            Service:
              - dms.amazonaws.com
              - schema-conversion.dms.amazonaws.com
          Action: sts:AssumeRole
    Policies:
      - PolicyName: S3TaggedAccess
        PolicyDocument:
          Version: '2012-10-17'
          Statement:
            - Effect: Allow
              Action:
                - s3:GetBucketLocation
                - s3:GetBucketVersioning
                - s3:PutObject
                - s3:PutBucketVersioning
                - s3:GetObject
                - s3:GetObjectVersion
                - s3:ListBucket
                - s3:DeleteObject
              Resource: arn:aws:s3:::atx-db-modernization-*
              Condition:
                StringEquals:
                  aws:ResourceAccount: !Ref AWS::AccountId

DMSSecretsManagerRole:
  Type: AWS::IAM::Role
  Properties:
    RoleName: dms-secrets-manager-role
    AssumeRolePolicyDocument:
```

```
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
            Action: sts:AssumeRole
      Policies:
        - PolicyName: SecretsManagerTaggedAccess
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action:
                  - secretsmanager:GetSecretValue
                  - secretsmanager:DescribeSecret
                Resource: '*'
                Condition:
                  StringEquals:
                    secretsmanager:ResourceTag/Project: atx-db-modernization
                    secretsmanager:ResourceTag/Owner: database-connector

  DMSVPCRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-vpc-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
            Action: sts:AssumeRole
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

  DMSServerlessRole:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: dms.amazonaws.com
      Description: 'Service Linked Role for AWS DMS Serverless'
```

```
Outputs:
  DMSCloudWatchLogsRoleArn:
    Description: ARN of the DMS CloudWatch Logs Role
    Value: !GetAtt DMSCloudWatchLogsRole.Arn
  DMSS3AccessRoleArn:
    Description: ARN of the DMS S3 Access Role
    Value: !GetAtt DMSS3AccessRole.Arn
  DMSSecretsManagerRoleArn:
    Description: ARN of the DMS Secrets Manager Role
    Value: !GetAtt DMSSecretsManagerRole.Arn
  DMSVPCRoleArn:
    Description: ARN of the DMS VPC Role
    Value: !GetAtt DMSVPCRole.Arn
    Export:
      Name: !Sub ${AWS::StackName}-VPCRole

  DMSServerlessRoleArn:
    Description: ARN of the DMS Serverless Role
    Value: !Sub 'arn:aws:iam::${AWS::AccountId}:role/aws-service-role/
dms.amazonaws.com/AWSServiceRoleForDMSServerless'
    Export:
      Name: !Sub ${AWS::StackName}-ServerlessRole
```

使用 AWS CLI 部署 CloudFormation 堆栈：

```
aws cloudformation create-stack \
  --stack-name dms-roles \
  --template-body file://dms-roles.yaml \
  --capabilities CAPABILITY_NAMED_IAM \
  --region us-east-1
```

或者使用 AWS 控制台进行部署：

1. 在 AWS 控制台 CloudFormation 中导航至
2. 选择创建堆栈
3. 选择上传模板文件
4. 上传 dms-roles.yaml 文件
5. 输入堆栈名称：dms-roles
6. 确认 IAM 功能

7. 选择创建堆栈

步骤 4：配置网络安全

确保 Transfor AWS m、您的 SQL Server 数据库和其他 AWS 服务之间的网络连接正确。

安全组配置（推荐方法）

推荐方法：使用基于安全组的访问控制而不是 IP-based 规则。这提供了更好的安全性，更易于管理，并且可以与Transform的 AWS 架构无缝协作。

为什么要进行安全 Group-Based 访问控制？

- DMS 架构转换在您的 VPC 中创建弹性网络接口 (ENI)
- 您的数据库不必是公开访问的
- AWS 转换不会暴露私有 IP 地址，这使得 IP-based 规则变得复杂
- 随着资源的扩展，安全组引用提供动态、自动的更新

配置你的 SQL Server 安全组

在转换中 AWS 配置 DMS 架构转换实例配置文件时，可以为 DMS SC 实例指定安全组。您的数据库安全组应允许来自此 DMS SC 安全组的入站流量。

Step-by-step 配置：

1. 确定 DMS 架构转换安全组：
   - 这是在 AWS 转换中创建实例配置文件时指定的
   - 记下安全组 ID（例如 sg-0123456789abcdef0）
2. 更新您的 SQL Server 安全组入站规则：
   - 类型：自定义 TCP
   - 端口：1433（或您的自定义 SQL 服务器端口）
   - 来源：DMS 架构转换安全组 ID
   - 描述：“允许 DMS 架构转换访问权限”
3. 对于 Aurora PostgreSQL 目标（创建后）：
   - 类型：P ostgreSQL
   - 端口：5432（或您的自定义 PostgreSQL 端口）

- 来源：DMS 架构转换安全组 ID
- 描述：“允许 DMS 架构转换访问权限”

> **Important**
>
> 对于权限最低的安全模型很重要：如果您的组织使用默认会阻止所有流量的 “最低权限” 安全模型，则必须明确允许从 DMS 架构转换安全组到您的数据库端口的入站流量。不要向所有源或 IP 范围开放端口 1433。

必填 AWS 服务连接

确保您的 VPC 可以与以下设备通信：

- AWS 转换服务端点
- AWS DMS 端点
- Aurora PostgreSQL 终端节点
- 用于对象存储的 S3 端点
- AWS Secrets Manager 端点
- AWS CodeConnections 端点

VPC 终端节点：对于私有网络，请为所需的 AWS 服务配置 VPC 终端节点，以避免依赖互联网网关。

外部托管数据库的要求

如果您的 SQL Server 数据库托管在外部 AWS，请确保满足以下先决条件，然后在开始现代化之前完成设置步骤。

先决条件

- 拥有 VPC 的 AWS 账户
- VPC 和外部数据库之间的网络连接。有关配置网络连接的信息，请参阅《 AWS DMS 用户指南》中的配置网络连接。

设置步骤

1. 使用外部数据库 AWS Secrets Manager 的连接详细信息在中创建密钥。有关更多信息，请参阅 the section called “第 2 步：将凭据存储在 AWS Secrets Manager”。
2. 出现提示时，请提供用于连接外部数据库的 VPC ID 和安全组 ID。 AWS Transform 会提示您输入此信息，因为密码中的数据库主机名无法在 AWS 账户中解析。

AWS 变换设置

访问 T AWS ransform 控制台并启动新的现代化项目，开始您的现代化之旅。此步骤将建立您的工作空间，并为您的全栈转换设置基础配置。

要完成的操作：

- 在 AWS 管理控制台中导航到 “ AWS 转换” 服务
- 从服务选项中选择 Microsoft 现代化
- 选择 “创建新的现代化项目”
- 提供项目名称和描述
- 选择您的目标 AWS 区域（必须与您的 SQL Server 位置相匹配）
- 查看并确认项目设置

> **Note**
>
> 最佳实践：使用包含应用程序名称和目标环境（例如 “CustomerPortal-Production-Modernization”）的描述性项目名称来轻松识别多波场景中的项目。

创建 SQL 服务器现代化任务

Connect 数据库和源代码存储库

配置数据库连接器

通过配置数据库连接器，建立与 SQL Server 数据库的安全连接。连接器执行环境分析、依赖关系发现，并允许 Tr AWS ansform 访问您的数据库架构和元数据以进行评估和转换。

要完成的操作：

- 从安装向导中选择 “配置数据库连接器”
- 选择连接方法：“新建连接” 或 “现有连接”
- 提供 SQL Server 连接详细信息（端点、端口、数据库名称）
- 配置身份验证并测试连通性
- 查看已发现的数据库并确认选择

> **Note**
>
> 网络连接：确保您的 SQL Server 安全组和 NACL 允许来自 AWS 转换服务端点的入站连接。

Connect 源代码存储库

启用 “ AWS 转换” 以访问您的.NET 应用程序源代码。 AWS Transform 支持三种提供源代码的方法：个人访问令牌 (PAT) 连接器（推荐）或 Amazon S3。 AWS CodeConnections这种集成允许该服务分析您的应用程序代码，识别数据库依赖关系，并执行自动代码转换以实现 PostgreSQL 兼容性。

要完成的操作：

- 导航到 “Connect 源代码存储库” 部分
- 选择您的身份验证方法：PAT 连接器（推荐）或 Amazon S3 AWS CodeConnections
- 选择包含.NET 应用程序的存储库
- 指定要分析的分支（通常 main/master 用于开发）
- 验证存储库访问权限和代码结构

> **Note**
>
> 存储库发现：T AWS ransform 会自动扫描您的存储库，以识别.NET 项目、实体框架配置、数据库连接字符串和 SQL 依赖关系。

> **Note**
>
> 安全注意事项：Trans AWS form 只需要对存储库具有读取权限，并为转换后的代码创建新的功能分支。你的主分支保持不变。

Human 在圈子里

AWS Transform 使用人性化 (HITL) 机制来确保质量，并允许您审查和批准关键的转型决策。以下检查点需要您注意：

波浪计划审查和批准

你回顾的内容：拟议的迁移浪潮，包括哪些数据库和应用程序被分组在一起以及迁移顺序。

你可以：

- 批准波浪计划
- 通过在波浪之间移动数据库来自定义波浪
- 修改波浪序列
- 分割或合并波浪

批准后， AWS 转换将继续进行架构转换。

架构转换审查

您查看的内容：转换后的数据库对象，包括表、存储过程、函数和触发器。操作项会突出显示需要注意的对象。

你可以：

- 接受转换后的代码
- 修改转换后的代码
- 转换后标记供人工审核
- 查看原始代码和转换后的代码的并排比较

批准后会发生什么： AWS 转换会将架构应用于 Aurora PostgreSQL，然后继续进行数据迁移（如果已配置）。

应用程序代码审查

您查看的内容：所有应用程序代码更改，包括实体框架配置、连接字符串、数据访问代码和存储过程调用。

你可以：

- 接受每个文件的更改
- 修改转换后的代码
- 拒绝更改（不推荐）
- 为你的团队添加评论
- 下载转换后的代码以供本地审阅

批准后会发生什么：T AWS ransform 会将更改提交到存储库中的新分支并继续进行验证。

验证结果审查

您查看的内容：自动验证结果，包括架构兼容性、数据完整性检查和应用程序构建状态。

你可以：

- 查看已通过的测试
- 调查失败的测试
- 地址警告
- 继续部署或返回修复问题

批准后会发生什么：T AWS ransform 为部署到目标环境做准备。

部署批准

您查看的内容：部署配置，包括基础架构即代码模板、ECS 服务配置和部署设置。

你可以：

- 查看和自定义部署设置
- 批准部署以继续
- 延迟部署以进行其他测试
- 下载基础设施代码以供审阅

获得批准后，Tr AWS ansform 会将您的现代化应用程序和数据库部署到目标环境。

评估和浪潮规划

设置着陆区

配置将部署现代化应用程序的目标基础架构环境。着陆区域设置包括 Aurora PostgreSQL 配置、网络配置和参考部署配置。

要完成的操作：

- 从配置菜单中选择 “设置着陆区”
- 配置 Aurora PostgreSQL 目标（版本、实例类等） Multi-AZ
- 配置网络和安全设置（VPC、子网、安全组）

> **Note**
>
> 成本注意事项：Aurora PostgreSQL 实例会持续产生成本。考虑在环境中使用 Aurora Serverless v2。 development/testing

评测

对您的数据库架构、应用程序代码和依赖关系进行全面分析。评估阶段提供转型复杂性评级，识别潜在挑战，并生成详细报告。

要完成的操作：

- 选择存储库分支进行代码分析
- 选择要转换的存储库和数据库
- 查看评估结果和复杂性评级
- 生成包含工作量预测的评估报告
- 供利益相关者审查和批准的出口报告

> **Note**
>
> 评估见解：评估提供对架构对象、存储过程、应用程序依赖关系的详细分析，并估计所需的人为干预级别。

波浪规划

根据转型的复杂性、业务优先级和应用程序依赖性，将您的现代化整理成可管理的浪潮。 AWS Transform 会生成您可以自定义的智能波浪建议。

要完成的操作：

- 查看 AI-Generated Wave 计划和建议
- 根据业务优先级自定义 Wave 配置
- 验证应用程序和数据库之间的依赖关系
- 使用对话界面敲定 Wave 计划
- 设定波次执行优先级并分配责任

> **Note**
>
> AI-Powered 建议：您可以通过自然语言与人工智能交互以调整建议：“将CustomerDB移至 Wave 1” 或 “将这两个应用程序合并成同一个浪潮”。

> **Note**
>
> 最佳实践：从包含 1-2 个低复杂度数据库的试点浪潮开始，以建立流程并建立团队信心。

每波数据迁移

每波的架构转换

使用 AI-enhanced 转换功能将 SQL Server 数据库架构转换为 PostgreSQL-compatible 等效架构。此过程转换表、存储过程、函数、触发器和其他数据库对象。

要完成的操作：

- 提供架构转换目标并配置首选项
- 使用 DMS 架构转换服务执行自动转换
- 查看转换结果并确定人为干预项目
- 通过 HITL 提示处理手动干预
- 验证人工更正并在需要时重新进行转换

> **Note**
>
> 常见的手动干预：链接的服务器、用户定义的类型、高级 T-SQL 模式和供应商特定的 SQL 功能通常需要人工检查和更正。

每波数据迁移

使用 () 集成将数据从 SQL Server 传输到 Aurora PostgreSQ AWS Database Migration Service L AWS DMS。在生产数据迁移或合成数据生成之间进行选择，以进行测试。

要完成的操作：

- 选择生产数据迁移或合成数据生成
- 配置 DMS 复制实例以进行数据传输
- 监控迁移进度并处理数据不一致问题
- 验证数据完整性和引用约束
- 确认成功完成后再继续

> **Note**
>
> 自动化 DMS 集成：Trans AWS form 抽象了 DMS 配置的复杂性，自动处理端点创建、任务配置和数据类型映射。

> **Note**
>
> 数据验证：该服务通过对源数据库和目标数据库运行相同的查询来执行实证测试，以确保数据一致性。

每波的代码迁移

转换.NET 应用程序代码以与 Aurora PostgreSQL 配合使用，包括实体框架配置更新、连接字符串修改、SQL 查询改编以及特定于框架的调整。

要完成的操作：

- 对 SQL Server 依赖项执行自动代码分析
- 执行框架转换（实体框架提供程序更新）
- 调整 SQL 查询语法以适应 PostgreSQL-compatible SQL
- 为转换后的代码配置目标分支管理
- 处理复杂模式的手动干预

SQL 服务器现代化工作流程

本节提供了使用 AWS 转换完成的 SQL Server 现代化过程的分步演练。

步骤 1：创建 SQL Server 现代化任务

在 Trans AWS form 控制台中创建新的转换任务，开始您的现代化之旅。

1. 登录 “ AWS 转换” 控制台
2. 选择创建现代化任务
3. 选择 Windows 现代化任务，然后选择 SQL Server 现代化
4. 输入职位详情：
   - Job nam e：项目的描述性名称
   - 描述：可选描述
   - 目标区域：要部署的 AWS 区域
5. 选择 Create job (创建作业）。

> **Important**
>
> 请勿在工作名称中包含个人身份信息 (PII)。

步骤 2：连接到 SQL Server 数据库

将 Trans AWS form 连接到 SQL Server 数据库以启用架构分析和转换。

创建数据库连接器

1. 在你的 SQL Server 现代化作业中，导航到 “连接资源”
2. 选择 “连接到 SQL Server 数据库”

3. 选择 “创建新连接器”
4. 输入连接器信息：
   - C 连接器名称：描述性名称
   - AWS 帐户 ID：托管 SQL Server 的帐户
5. 确认后，您将收到一个用于批准的链接。复制批准链接以获得 AWS 管理员对账户的批准。他们批准后，您就可以继续执行下一步了。
6. 管理员批准连接器请求后，单击 “提交” 继续进行源代码连接设置。

第 3 步：Connect 源代码存储库

AWS Transform 需要访问您的.NET 应用程序源代码，才能分析和转换与 SQL Server 数据库交互的代码。 AWS Transform 支持三种提供源代码的方法。

选择您的身份验证方法

个人访问令牌 (PAT) 连接器（推荐）

最适合需要自定义权限范围、自托管提供商支持或访问提供商特定的 API（例如 Secrets）的团队。 GitHub 您可以在源代码提供程序中创建具有自定义权限的 PAT，将其存储在中 AWS Secrets Manager，然后 Transfor AWS m 会在需要时对其进行检索。您负责管理代币的轮换和到期。

AWS CodeConnections

最适合想要自动凭证管理的团队。 AWS CodeConnections 使用托管提供商集成，通过 OAuth 2.0 授权流程处理身份验证。 AWS 管理整个凭证生命周期，包括自动令牌刷新和轮换。无需手动管理凭证。

Amazon S3

将您的源代码直接上传到 Amazon S3 存储桶。 AWS 在转换作业期间，Transform 会访问存储桶中的代码。

功能	PAT 连接器（推荐）	AWS CodeConnections
凭证管理	手动（客户管理）	自动（AWS托管）
代币生命周期	需要手动旋转	自动刷新
权限灵活性	完全可定制的瞄准镜	固定权限

功能	PAT 连接器（推荐）	AWS CodeConnections
Self-hosted 提供商支持	支持	不可用
设置复杂性	中等（手动创建和存储令牌）	低（一次性授权）
代币存储	客户的 AWS Secrets Manager	AWS托管式

设置 PAT 连接器（推荐）

使用 PAT 连接器，您可以在源代码提供程序中创建具有自定义权限的个人访问令牌，将其安全地存储在中 AWS Secrets Manager，然后 T AWS ransform 会在需要时对其进行检索。您负责管理代币生命周期，包括轮换和到期。 AWS Transform 会自动创建必要的 IAM 角色，该角色具有访问您的密钥的权限。

PAT 连接器支持以下提供商，包括自托管版本和自定义 DNS/URL 版本：

- GitHub 和 GitHub 企业服务器
- GitLab.com 和 GitLab Self-Managed
- Bitbucket 云和比特桶数据中心
- 天蓝色 DevOps 和 Azure DevOps 服务器

创建个人访问令牌

在您的源代码提供程序中创建 PAT。所需的权限因提供商而异。选择您的提供商对应的选项卡。

> **Important**
>
> 创建后立即复制令牌。您无法再次查看。设置转换任务持续时间的过期时间。不要将过期时间设置为永不过期。

> **Warning**
>
> 切勿将 PAT 令牌提交到代码存储库或通过不安全的渠道共享。一定要把它们存放在里面 AWS Secrets Manager。

GitHub

导航到 “设置”、“开发者设置”、“个人访问令牌”、“Fine-grained 令牌”。选择要转换的存储库并授予以下权限。

存储库权限

权限	访问	用途
内容	读和写	读取源代码并将转换后的代码写回存储库
元数据	Read-only	访问存储库的基本信息

组织权限（组织仓库必需）

权限	访问	用途
成员	Read-only	列出可使用令牌进行仓库发现的组织

GitLab

导航到 “编辑个人资料”、“访问令牌”。选择以下范围。

Scope	用途
`read_api`	读取仓库元数据、项目信息、用户详细信息以及列出群组和分支
`read_repository`	读取源代码文件和存储库结构以进行分析
`write_repository`	将转换后的代码写回存储库

Bitbucket

导航到 “账户设置”、“安全”、“创建和管理 API 令牌”。所需的范围取决于您的令牌类型。

Workspace/Repository 令牌（ATCT — 持有者身份验证，无需用户名）

权限	访问	用途
Repositories	读和写	通过 git push 列出存储库、读取分支并编写转换后的代码

账户 API 令牌（ATAT — 使用电子邮件进行基本身份验证）或应用程序密码（ATBB — 带用户名的基本身份验证）

Scope	用途
`read:account`	标识要解析存储库成员身份的经过身份验证的用户
`read:workspace:bitbucket`	列出令牌可以访问的工作空间，这样 Transfor AWS m 就可以枚举其存储库。如果您在密钥中指定工作区列表，则无需填写。
`read:repository:bitbucket`	列出存储库并读取元数据和分支信息
`write:repository:bitbucket`	通过 git push 将转换后的代码写回存储库

天蓝色 DevOps

导航到 “用户设置”、“个人访问令牌”。选择 “自定义范围”。对于组织范围，请选择所有可访问的组织（推荐）或指定单个组织。

Scope	访问	用途
代码	读和写	读取源代码，列出存储库和分支，并将转换后的代码写回来
用户个人资料	读取	验证令牌访问权限并发现用于组织查询的用户身份
会员权益管理	读取	列出可使用令牌进行仓库发现的组织

将 PAT 存放在里面 AWS Secrets Manager

1. 打开控制 AWS Secrets Manager 台。
2. 选择存储新密钥。
3. 对于密钥类型，请选择其他密钥类型。
4. 根据您的提供商和托管类型添加键值对：
   - Cloud-hosted 提供者-添加一个以您的 PAT 作为值命名的`token`密钥。
     - 对于 DevOps 具有特定组织的 Azure，还要添加一个以你的组织`organization`名称命名的密钥。
     - 对于 Bitbucket 应用程序密码 (ATBB)，还要添加一个以您的 Bitbucket 用户名命名的`username`密钥。对于 Bitbucket 账户 API 令牌 (ATAT)，请添加一个以您的 Bitbucket `email`电子邮件地址命名的密钥。
   - Self-hosted 和自定义 DNS/URL 提供商-添加以下密钥：`host`（例如您的服务器 URL`https://github.mycompany.com`）、`provider_type`（`github`、`gitlab`、`bitbucket`、或`ado`）和`token`（您的 PAT）。
     - 对于 DevOps 具有特定组织的 Azure，还要添加一个以你的组织`organization`名称命名的密钥。
     - 对于 Bitbucket 应用程序密码 (ATBB)，还要添加一个以您的 Bitbucket 用户名命名的`username`密钥。对于 Bitbucket 账户 API 令牌 (ATAT)，请添加一个以您的 Bitbucket `email`电子邮件地址命名的密钥。

以下示例显示了密钥如何查找 GitHub 云托管提供商： AWS Secrets Manager

```
{
  "token": "your-github-personal-access-token"
}
```

以下示例显示了 Bitbucket 应用程序密码 (ATBB)：

```
{
  "token": "your-bitbucket-app-password",
  "username": "my-bitbucket-username"
}
```

以下示例显示了一个自托管 GitLab 实例：

```
{
  "host": "https://gitlab.mycompany.com",
  "provider_type": "gitlab",
  "token": "your-gitlab-personal-access-token"
}
```

5. 选择下一步。
6. 例如，输入密钥名称`github-pat-myproject`。
7. （可选）选择客户管理的 KMS 密钥进行加密。
8. 完成向导并选择存储。
9. 复制秘密 ARN。配置 AWS 转换作业时需要此值。

如果您使用客户管理的 KMS 密钥来加密您的密钥（而不是默认的 AWS托管密钥），则必须更新 KMS 密钥策略以允许 Tr AWS ansform 解密密钥。将以下声明添加到您的客户管理的 KMS 密钥策略中：

```
{
  "Sid": "Allow AWS Transform to decrypt secrets",
  "Effect": "Allow",
  "Principal": {
    "Service": "transform.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "secretsmanager.REGION.amazonaws.com",
      "kms:EncryptionContext:SecretARN": "YOUR-SECRET-ARN"
    }
  }
}
```

*REGION*替换为您 AWS 所在的地区（例如`us-east-1`）和*YOUR-SECRET-ARN*您的密钥的 ARN。该`kms:ViaService`条件可确保 KMS 密钥只能通过 AWS Secrets Manager 服务使用。该`kms:EncryptionContext:SecretARN`条件将解密限制在您的特定机密范围内。

要更新 KMS 密钥策略，请执行以下操作：

1. 打开 AWS KMS 控制台，网址为`https://console.aws.amazon.com/kms`。
2. 在导航窗格中，选择客户托管密钥。
3. 选择您的 KMS 密钥。
4. 在密钥策略选项卡上，选择编辑。
5. 将政策声明添加到现有策略中。
6. 选择保存更改。

> **Note**
>
> 如果您使用默认的 AWS托管密钥 (`aws/secretsmanager`)，则无需修改任何 KMS 密钥策略。

配置 AWS 转换作业

1. 在 “ AWS 转换” 作业中，导航到 “Connect to 资源”。
2. 选择 Connect 源代码存储库。
3. 选择 PAT 连接器作为身份验证方法。
4. 输入步骤 2 中的秘密 ARN。
5. （可选）如果您使用客户管理的 KMS 密钥，请输入 KMS 密钥 ARN。
6. 选择您的存储库和分支。
7. 选择继续。

AWS Transform 会自动创建一个 IAM 角色，该角色具有访问您的密钥所需的权限。

代币轮换和维护

您有责任在 PAT 代币到期之前进行轮换。要轮换代币，请执行以下操作：

1. 在您的源代码提供程序中生成具有相同权限的新 PAT。
2. 更新中的密钥值 AWS Secrets Manager。
3. 验证您的 AWS 转换任务是否可以使用新令牌访问存储库。
4. 在源代码提供程序中撤消旧 PAT。

排除 PAT 连接器问题

访问被拒绝-PAT 无效

验证 PAT 是否未过期。确认 PAT 具有您的提供商所需的范围。检查 PAT 是否正确存储在中 AWS Secrets Manager。

无法检索密钥

验证密钥 ARN 是否正确。检查任务日志以确认 Trans AWS form 创建了 IAM 角色。如果您使用的是客户管理的 KMS 密钥，请验证密钥策略。

权限不足

PAT 可能缺少操作所需的瞄准镜。使用所需范围重新生成 PAT，并在中更新密钥值。 AWS Secrets Manager

设置 AWS CodeConnections

AWS CodeConnections 使用托管提供商集成，该集成可通过 OAuth 2.0 授权流程自动检索临时 OAuth 凭证。权限在提供商应用程序中配置并完全由管理 AWS。您只需对应用程序进行一次授权，即可 AWS 处理所有凭据管理。

1. 在 SQL Server 现代化作业中，导航到 “连接资源”。
2. 选择 Connect 源代码存储库。
3. 如果您没有现有连接，请选择创建连接。
4. 选择您的存储库提供商：
   - GitHub / GitHub 企业
   - GitLab.com
   - Bitbucket Cloud
   - Azure 存储
5. 按照您的提供商的授权流程进行操作。
6. 授权后，选择 Connect。

选择您的存储库和分支

1. 从列表中选择您的存储库。
2. 选择要转换的分支（通常是主分支、主分支或开发分支）。

3. （可选）如果您的.NET 应用程序不在存储库根目录中，请指定子目录。
4. 选择继续。

> **Note**
>
> AWS 转换为转换后的代码创建一个新分支。您可以通过正常的代码审查流程来查看和合并更改。

仓库访问批准

对于 GitHub 和其他一些平台，存储库管理员必须批准连接请求：

1. AWS “转换” 显示验证链接。
2. 与您的仓库管理员共享此链接。
3. 管理员在其存储库设置中查看并批准该请求。
4. 管理员批准请求后，连接状态更改为 “已批准”。

> **Important**
>
> 批准过程可能需要一些时间，具体取决于您所在组织的政策。相应地做好计划。

步骤 4：创建部署连接器（可选）

如果要将转换后的应用程序部署到您的 AWS 帐户，则可以选择部署连接器。

设置部署连接器

1. 如果要部署应用程序，请选择 “是”。选择 “否” 将跳过此步骤。
2. 将您的 AWS 账户添加到要部署转换后的应用程序的位置。
3. 添加一个可以帮助您轻松记住连接器的名称
4. 提交连接器请求以获得批准。

部署连接器批准

您的 AWS 账户管理员必须批准部署连接器的连接请求。

1. AWS “转换” 显示验证链接
2. 与您的 AWS 账户管理员共享此链接
3. 管理员在其存储库设置中查看并批准该请求
4. 获得批准后，连接状态将更改为 “已批准”

> **Important**
>
> 批准过程可能需要一些时间，具体取决于您所在组织的政策。相应地做好计划。

第 5 步：确认您的资源

连接到数据库和存储库后，T AWS ransform 会验证所有必需的资源是否均可访问并准备好进行转换。

内容 AWS 变换验证

- 数据库连接：连接处于活动状态，用户拥有所需权限，数据库可访问，版本支持
- 存储库访问权限：存储库可访问、分支存在、检测到.NET 项目文件、可发现数据库连接
- 环境就绪：VPC 配置支持 DMS，存在所需的 AWS 服务角色，已建立网络连接，确认区域兼容性

查看飞行前清单

1. 导航到在工作计划中确认您的资源
2. 查看清单项目：
   - # 数据库连接已验证
   - # 存储库访问权限已确认
   - # 支持.NET 版本
   - # 实体框架或 ADO.NET 检测到
   - # 网络配置有效
   - # 已授予所需权限
3. 如果所有项目都显示为已完成，请选择 “继续”
4. 如果有任何项目显示警告或错误，请在继续操作之前解决这些问题

第 6 步：发现和评估

AWS Transform 会分析您的 SQL Server 数据库和.NET 应用程序，以了解现代化的范围和复杂性。

发现了什么

- 数据库对象：表、视图、索引、存储过程、函数、触发器、约束、数据类型、计算列、标识列、外键关系
- 应用程序代码：.NET 项目结构、实体框架模型和配置、 ADO.NET 数据访问代码、数据库连接字符串、存储过程调用、代码中的 SQL 查询
- 依赖关系：哪些应用程序使用哪些数据库、跨数据库依赖关系、共享存储过程、常见的数据访问模式

发现过程

- AWS 资源确认后，转换会自动开始发现
- 发现通常需要 5-15 分钟，具体取决于数据库大小和应用程序复杂性
- 监控工作日志中的进度
- AWS 当发现对象时，变换会显示实时更新

查看发现结果

发现完成后，导航至 “发现和评估” 以查看：

数据库分析：

- 对象计数：表、视图、存储过程、函数、触发器的数量
- 复杂度分数：转换复杂度评估（低、中、高）
- 行动项目：可能需要人类注意的物体
- 支持的功能：将自动转换的数据库功能
- 不支持的功能：需要变通方法的功能

应用分析：

- 项目类型： ASP.NET 核心、控制台应用程序、类库等
- .NET 版本：已检测到.NET 核心版本

- 数据访问框架：实体框架版本或 ADO.NET
- 数据库连接：找到的连接字符串数
- 代码复杂性：评估转换复杂性

依赖关系图：

- 应用程序到数据库关系的可视化表示
- Cross-database 依赖关系
- 共享组件

了解复杂性评估

AWS Transform 将您的现代化改造分为三类：

复杂度	特性	预期结果
低（A 级）	标准 SQL 模式 (ANSI SQL)、简单存储过程、基本数据类型、带有标准配置的实体框架	预计人为干预最少，自动化成功率高
中型（B 级）	高级 T-SQL 模式、带有业务逻辑的复杂存储过程、用户定义的函数、计算列	专家评审建议，需要一些人为干预
高（C 级）	CLR 程序集、链接服务器、服务代理、复杂的全文搜索	需要大量的人工重构，请考虑分阶段的方法

评测报告

AWS Transform 会生成一份详细的评估报告，其中包括：

- 包含高级概述的执行摘要
- 完成数据库清单
- 应用程序清单
- 转型就绪百分比

- 工作量估算
- 风险评估和缓解策略
- 推荐方法

您可以下载评估报告，以便离线查看并与利益相关者共享。

第 7 步：生成并查看波浪计划

对于具有多个数据库和应用程序的大型房产，Trans AWS form会生成波浪计划，按逻辑组对现代化进行排序。

什么是波浪计划？

波浪计划将您的现代化改造分为几个阶段（波次），具体基于以下几点：

- 数据库和应用程序之间的依赖关系
- 业务优先事项
- 风险承受能力
- 资源可用性
- 技术复杂性

每个浪潮都包含一组数据库和应用程序，这些数据库和应用程序可以在不破坏依赖关系的情况下一起进行现代化改造。

查看浪潮计划

1. 导航到工作计划中的 Wave 计划
2. 查看提议的浪潮
3. 对于每波浪潮，请查看：
    - 包括数据库
    - 包含的应用程序
    - 对其他浪潮的依赖
    - 预计转换时间
    - 复杂性级别
    - 可部署的应用程序

自定义波浪计划

您可以通过两种方式自定义波浪计划以满足您的业务需求：

使用 JSON：

1. 选择 “下载所有波浪” 以获取包含所有波浪的 JSON 文件
2. 通过以下方式修改 JSON 中的波浪：
   - 在波浪之间移动数据库
   - 将波浪分成小组
   - 将波浪合并在一起
   - 改变波浪序列
   - 在作用域中添加或移除数据库
3. 选择 “上传波浪计划” 将 JSON 文件上传回控制台
4. AWS 转换会验证您的更改，并在违反依赖关系时发出警告
5. 选择确认波浪以更新波浪计划

使用聊天：

您可以通过与代理聊天并要求其将存储库和数据库移至特定波浪来修改波浪计划。如果你需要对波浪进行少量编辑，这种方法效果很好。

> **Important**
>
> 在自定义波浪时，请确保尊重依赖关系。在依赖应用程序的数据库之前对其进行转换可能会导致问题。

单一数据库现代化

如果您要对单个数据库和应用程序进行现代化 AWS 改造，Transform 会立即创建一个简单的计划。您可以直接进行转型，而无需进行波浪规划。

批准波浪计划

1. 查看和自定义（如果需要）后，选择批准波浪计划
2. AWS 变换锁定波浪计划并继续进行转换

3. 您仍然可以稍后通过选择 “编辑波浪计划” 来修改计划

步骤 8：架构转换

AWS Transform 会将你的 SQL Server 数据库架构转换为 Aurora PostgreSQL，包括表、视图、存储过程、函数和触发器。

架构转换的工作原理

AWS Transform 使用通过生成式 AI 增强的 AWS DMS 架构转换来：

- 分析 SQL 服务器架构和关系
- 将数据类型从 SQL Server 映射到 PostgreSQL 等效项
- 转换 T-SQL 为 PL/pgSQL
- 处理标识列、计算列和约束
- 验证转换和参照完整性
- 为需要人工审查的对象生成操作项目

支持的转换

自动转换：

- 表、视图和索引
- 主键和外键
- 检查约束条件和默认值
- 最常见的数据类型
- 简单的存储过程
- 基本功能和触发器
- 标识列（转换为 “序列” 或 “已生成”）
- 计算得最多的列

可能需要人工审查：

- 具有高级功能的复杂存储过程 T-SQL
- SQL Server-specific 函数（GETUTCDATE、SUSER_SNAME 等）

- 包含复杂表达式的计算列
- Full-text 搜索索引
- XML 数据类型操作
- HIERARCHYID 数据类型（需要 ltree 扩展名）

未自动转换：

- CLR 程序集
- 链接服务器
- 服务代理
- SQL Server Agent 作业

开始架构转换

1. 导航到作业计划中的架构转换
2. 查看转换设置：
   - 目标 PostgreSQL 版本
   - 扩展选项（ltree、PostGIS 等）
   - 命名规范
3. 选择 “开始转换”
4. 监控工作日志中的进度
5. 转换通常需要 10-30 分钟，具体取决于数据库对象的数量

查看转换结果

转换完成后，导航到 “查看架构转换”：

转换摘要：

- 已转换的对象：成功转换的对象计数
- 行动项目：需要人类注意的物体
- 警告：需要审查的潜在问题
- 错误：无法转换的对象

按对象类型查看：

- 表：数据类型映射、约束、索引
- 存储过程： T-SQL 转 PL/pgSQL 换
- 函数：函数签名和逻辑更改
- 触发器：触发语法和时间变更

查看行动项目

1. 选择 “查看操作项目”
2. 对于每个措施项，请查看：
   - 对象名称：数据库对象
   - 问题类型：需要注意什么
   - 严重性：严重、警告或信息
   - 建议：建议的解决方案
   - 原始代码：SQL Server 版本
   - 转换后的代码：PostgreSQL 版本
3. 对于每个措施项，您可以：
   - 接受：使用转换后的代码
   - 修改：编辑转换后的代码
   - 标记以备后用：转换后标记为人工审核

示例：存储过程转换

SQL 服务器 T-SQL：

```
CREATE PROCEDURE GetProductsByCategory
    @CategoryId INT,
    @PageSize INT = 10
AS
BEGIN
    SET NOCOUNT ON;

    SELECT TOP (@PageSize)
        ProductId,
        Name,
```

```
        Price,
        DATEDIFF(DAY, CreatedDate, GETUTCDATE()) AS DaysOld
    FROM Products
    WHERE CategoryId = @CategoryId
    ORDER BY Name
END
```

转换后的 PostgreSQL PL/pgSQL：

```
CREATE OR REPLACE FUNCTION get_products_by_category(
    p_category_id INTEGER,
    p_page_size INTEGER DEFAULT 10
)
RETURNS TABLE (
    product_id INTEGER,
    name VARCHAR(255),
    price NUMERIC(18,2),
    days_old INTEGER
) AS $$
BEGIN
    RETURN QUERY
    SELECT
        p.product_id,
        p.name,
        p.price,
        EXTRACT(DAY FROM (NOW() - p.created_date))::INTEGER AS days_old
    FROM products p
    WHERE p.category_id = p_category_id
    ORDER BY p.name
    LIMIT p_page_size;
END;
$$ LANGUAGE plpgsql;
```

所做的更改：

- 过程转换为函数返回 TABLE
- 以 p_ 为前缀的参数名
- TOP 转换为 LIMIT
- DATEDIFF 已转换为数据提取
- GETUTCDATE () 转换为 NOW ()
- 将列名转换为小写字母（PostgreSQL 惯例）

批准架构转换

1. 在查看了所有行动项目并进行了必要的修改之后
2. 选择批准架构转换
3. AWS Transform 为转换后的架构做好部署到 Aurora PostgreSQL 的准备

> **Note**
>
> 您可以将转换后的架构下载为 SQL 脚本，用于离线查看或版本控制。

步骤 9：数据迁移（可选）

AWS Transform 提供了将数据从 SQL Server 迁移到 Aurora PostgreSQL 的选项。数据迁移是可选的，如果您只需要架构和代码转换，则可以跳过。

数据迁移选项

选项 1：生产数据迁移

使用 AWS DMS 迁移您的实际生产数据：

- 所有数据的初始加载完毕
- 测试期间持续复制 (CDC)
- 最大限度减少停机时间切换
- 数据验证和完整性检查

选项 2：跳过数据迁移

仅转换架构和代码：

- 对 development/testing 环境很有用
- 何时将单独迁移数据
- 适用于概念验证项目

配置数据迁移

1. 导航到工作计划中的数据迁移

2. 选择您的迁移选项：
   - 迁移生产数据
   - 跳过数据迁移
3. 如果要迁移生产数据，请配置：
   - 迁移类型：满载或满载 + CDC
   - 验证：启用数据验证
   - 性能：DMS 实例大小
   - 选择 >开始迁移

生产数据迁移流程

如果您选择迁移生产数据：

1. 初始同步： AWS DMS 对所有表执行全量加载
2. 连续复制：（如果启用 CDC）保持数据同步
3. 验证：验证行数和数据完整性
4. 直接转换准备：为最终同步做准备

迁移时间表：

- 小型数据库 (< 10 GB)：30 分钟-2 小时
- 中型数据库 (10-100 GB)：2-8 小时
- 大型数据库 (> 100 GB)：8 小时以上

数据验证

AWS Transform 使用以下检查来验证迁移的数据：

- 行数比较（源与目标）
- 主键完整性
- 外键关系
- 数据类型兼容性
- 计算列结果
- 空值处理

步骤 10：应用程序代码转换

AWS Transform 会将你的.NET 应用程序代码转换为使用 Aurora PostgreSQL 而不是 SQL Server。它要求在仓库中输入目标分支名称来提交转换后的源代码。输入分支名称后，Trans AWS form 将创建一个新分支并启动转换以匹配 PostgreSQL 数据库。

什么会被改变

实体框架变更：

- 数据库提供商: UseSqlServer() → UseNpgsql ()
- 连接字符串：SQL Server 格式 → PostgreSQL 格式
- 数据类型映射：SQL Server 类型 → PostgreSQL 类型
- DbContext 配置：SQL Server-specific → PostgreSQL-specific
- 迁移文件：已针对兼容 PostgreSQL 而进行了更新

ADO.NET 变化：

- 连接类: SqlConnection → NpgsqlConnection
- 命令类: SqlCommand → NpgsqlCommand
- 数据读取器: SqlDataReader → NpgsqlDataReader
- 参数: SqlParameter → NpgsqlParameter
- S QL 语法： T-SQL → PostgreSQL SQL

配置更改：

- apsettings.json 中的连接字符串
- 数据库提供程序 NuGet 包
- 依赖注入配置
- Startup/Program.cs 配置

开始代码转换

1. 导航到工作计划中的 “应用程序转换”
2. 查看转换设置：

- 目标.NET 版本（如果正在升级）
- PostgreSQL 提供程序版本
- 代码样式偏好设置

3. 选择 “开始转换”
4. 监控工作日志中的进度
5. 转换通常需要 15-45 分钟，具体取决于代码库的大小

步骤 11：查看转换结果

在继续部署之前，请查看完整的转换结果，以确保一切准备就绪，可以进行测试。

您可以从存储库分支下载转换后的代码，用于：

- 本地测试和验证
- 在 IDE 中进行代码审查
- 与您的 CI/CD 管道集成
- 版本控制提交

您也可以下载转换摘要，以查看 Transform 在 AWS 转换过程中所做的自然语言更改。

转换摘要

1. 导航到工作计划中的转换摘要
2. 查看总体结果：
   - 架构转换：已转换的对象、措施项、警告
   - 数据迁移：已迁移的表、传输的行数、验证状态
   - 代码转换：文件已更改、行数已修改、问题已解决
   - 就绪性分数：总体部署就绪性

生成转换报告

AWS Transform 会生成一份全面的转换报告：

1. 选择 “生成报告”
2. 选择报告类型：

- 内容提要：利益相关者 High-level 概述
- 技术细节：完整的转换文档
- 操作项目：所需人工任务清单

3. 选择 “下载报告”

该报告包括：

- 转型范围和目标
- 对象和代码已转换
- 遇到的问题和解决方案
- 验证结果
- 部署准备情况评估
- 测试建议

第 12 步：验证和测试

在部署到生产环境之前，请验证转换后的应用程序是否可以与 Aurora PostgreSQL 一起正常运行。

验证类型

自动验证：T AWS ransform 执行自动检查：

- 对源数据库进行架构验证
- 数据完整性验证
- 查询等效性测试
- 连接字符串验证
- 配置验证

人工验证：您应该进行其他测试：

- 应用程序功能的功能测试
- 与其他系统的集成测试
- 性能测试和基准测试

- 用户验收测试
- 安全测试

运行自动验证

1. 导航到作业计划中的 “验证”
2. 选择 “运行验证”
3. AWS Transform 执行验证测试：
    - 数据库连接
    - 架构兼容性
    - 数据完整性
    - 应用程序构建
    - 基本功能
4. 查看验证结果：
    - 已通过：成功的测试
    - 失败：需要注意的测试
    - 警告：需要审查的潜在问题

测试清单

数据库功能：

- 所有桌子均可使用
- 存储过程可以正确执行
- 函数返回预期结果
- 触发器适当地触发
- 限制措施得到正确执行
- 索引可提高查询性能

应用程序功能：

- 应用程序成功启动
- 数据库连接已建立

- CRUD 操作可以正常运行
- 存储过程调用成功
- 交易 commit/rollback 正常
- 错误处理按预期工作

数据完整性：

- 行数与来源匹配
- 主键是唯一的
- 外键有效
- 计算列正确
- 适当处理空值
- 兼容的数据类型

性能：

- 查询响应时间可以接受
- 已配置连接池
- 索引已优化
- 没有 N+1 查询问题
- 高效的批量操作
- 资源利用率合理

步骤 13：部署

成功验证后，将现代化的应用程序和数据库部署到生产环境中。

部署选项

- 亚马逊 ECS 和亚马逊 EC2 Linux

Pre-deployment 清单

在部署到生产环境之前：

- 所有验证测试均已通过
- 性能测试已完成
- 安全审查已完成
- Backup 和回滚计划已记录在案
- 已配置监控和警报
- 团队接受了有关新环境的培训
- 向利益相关者通报了部署情况
- 已安排维护时段

部署到 Amazon ECS

1. 导航到作业计划中的 “部署”
2. 选择 “部署到 ECS”
3. 配置部署设置：
   - 集群：选择或创建 ECS 集群
   - 服务：配置 ECS 服务
   - 任务定义：查看生成的任务定义
   - 负载均衡器：配置 ALB/NLB
   - Auto-scaling: 设置扩展策略
4. 查看基础架构即代码（CloudFormation 模板或 CDK 代码） AWS
5. 选择部署

监控部署

AWS Transform 会部署您的应用程序：

1. 创建 Aurora PostgreSQL 集群
2. 应用数据库架构
3. 加载数据（如果适用）
4. 部署应用程序容器
5. 配置负载均衡器
6. 设置自动缩放

监控部署进度并验证：

- 基础设施预调配
- 数据库初始化
- 应用程序部署
- Health 检查通过
- 应用程序可访问
- 数据库连接正常
- 显示正常操作的日志

Post-deployment 验证

部署后：

烟雾测试：

- 验证关键功能
- 测试关键用户工作流程
- 检查集成点
- 监控错误率

性能监控：

- 追踪响应时间
- 监控数据库查询
- 检查资源利用率
- 查看应用程序日志

用户验证：

- 进行用户验收测试
- 收集反馈
- 解决任何问题
- 记录吸取的经验教训

回滚程序

如果部署后出现问题：

立即回滚：

- 恢复到以前的应用程序版本
- 切换回 SQL Server（如果仍然可用）
- 必要时从备份中恢复

部分回滚：

- 回滚特定组件
- 保留数据库更改
- 仅恢复应用程序代码

向前修复：

- 将修补程序应用于 Aurora PostgreSQL 版本
- 部署更新的应用程序代码
- 显示分辨率

> **Important**
>
> 在切换后保持 SQL Server 数据库可用一段时间，以便在需要时启用回滚功能。

Post-deployment 优化

成功部署后：

性能调整：

- 优化慢速查询
- 调整连接池设置
- Fine-tune Aurora PostgreSQL 参数
- 查看和优化索引

成本优化：

- Right-size Aurora 实例
- 适当地配置自动缩放
- 查看存储设置
- 优化备份保留期

监控设置：

- 配置 CloudWatch 仪表板
- 设置警报
- 启用增强监控
- 配置性能 Insights

文档：

- 更新运行手册
- 记录架构变更
- 列车运营组
- 创建疑难解答指南

转换后进行测试和部署

将转换后的应用程序部署到 landing zone，验证您的应用程序与转换后的数据库之间的连接，还可以选择设置 CI/CD 管道。生成示例 CI/CD 管道配置作为参考，以帮助您实现部署自动化。最后阶段验证了完整的现代化改造。

配置资源

您需要配置部署中使用的资源，例如 IAM 角色、实例配置文件和 S3 存储桶。 AWS Transform 无权创建 S3 存储桶或在您的 IAM 中进行更改。此操作需要由有权创建新角色的用户执行。通常是账户管理员。

为了简化流程，我们提供了一个安装脚本，该脚本可以自动：

- 执行必要的模板 CloudFormation

- 创建 ECS Service-Linked 角色
- 设置所有必需的 IAM 资源

> **Important**
>
> 按原样运行提供的安装脚本-请勿修改模板或脚本中的任何资源名称，因为这可能会影响部署过程。

对于 Linux：

```
./setup.sh --region <YOUR-Region>
```

对于 Windows：

```
./setup.ps1 -Region <YOUR-Region>
```

检查您的 VPC 中的安全组

AWS Transform 会将应用程序部署到与 Aurora PostgreSQL 实例相同的子网和相同的安全组。

要使应用程序连接到 Aurora 实例，请确保此安全组具有允许连接到相同安全组的出站规则和允许从同一安全组进行连接的入站规则。

选择和配置应用程序

T AWS ransform UI 显示了可以部署的应用程序列表。选择应用程序并单击 “配置并提交” 以打开配置窗口，您可以在其中指定：

- 应用程序的目标基础架构：选择 ECS 或其中一个 EC2 实例
- 应用程序或实例参数

完成并关闭配置窗口后， AWS 转换：

- 根据您的配置生成部署工件
- 将这些工件提交到您的存储库，包括：
  - 部署脚本

- CloudFormation 模板
- 示例 CI/CD 管道配置（您可以将其用作设置部署自动化的参考）

提交完成后，应用程序状态将更改为 “已配置并已提交”。然后，您可以选择应用程序并使用右上角的 “部署” 按钮启动部署。

云服务器部署

所有带有目标 ECS 的应用程序都部署到在您的账户中创建的新 ECS 集群中。每个应用程序都部署在自己的专用容器中，不支持每个容器有多个应用程序。您可以单独为每个应用程序配置容器参数，例如所需的 CPU 和内存。

EC2 部署

您可以选择一个建议的 EC2 实例，并可以配置其参数，例如实例类型。可以将多个应用程序部署到同一 EC2 实例：

- 要将多个应用程序部署到单个实例，请在配置期间为每个应用程序选择相同的目标 EC2 实例。
- 将相同实例选为目标的所有应用程序都将部署到该实例并分配不同的随机端口。
- 请注意，如果您编辑一个应用程序的实例参数，然后编辑另一个针对同一实例的应用程序，则更改会影响部署到该实例的所有应用程序。

部署成功

成功部署后，您的应用程序将在 Aurora PostgreSQL 上运行，从而降低许可成本、提高性能和云原生可扩展性。除非明确停止，否则任务将保持打开状态。这允许选择使用更新的部署参数进行可能的重新部署。

最佳实践和故障排除

现代化过程中的最佳实践、常见问题及其解决方案。

ECS 应用程序日志

CloudWatch 日志

- 所有 ECS 容器日志都会自动发送到 CloudWatch 日志
- 在 CloudWatch 控制台的 “日志组” 下访问日志

- 日志组命名格式：/aws/ecs/{应用程序名称}
- 每个容器实例都会在组内创建一个新的日志流

查看日志

通过 AWS 控制台：

- 导航到 CloudWatch > 日志组
- 选择您的应用程序的日志组
- 选择相关的日志流以查看容器日志

使用 AWS CLI：

```
aws logs get-log-events --log-group-name /aws/ecs/your-app-name --log-stream-name your-
stream-name
```

常见日志位置

- 应用程序日志： CloudWatch 日志
- ECS 服务事件：ECS 控制台 > 集群 > 服务 > 事件选项卡
- 容器 health/status：ECS 控制台 > 集群 > 服务 > 任务选项卡

数据库连接管理

应用程序使用环境变量进行数据库连接设置

如果您遇到连接问题：

- 验证环境变量中的当前连接设置
- 更新环境变量以根据需要修改数据库连接字符串
- 无需重新部署应用程序即可通过更新环境变量来更改连接字符串

数据库连接问题

问题：无法将 AWS 转换连接到 SQL Server

解决方案：

- 验证 AWS 转换和 SQL Server 之间的网络连接
- 检查安全组规则以获得正确的端口访问权限 (1433)
- 在 Secrets Manager 中确认数据库凭证
- 使用已创建的用户测试数据库权限
- 确保将 SQL Server 配置为使用混合模式身份验证
- 验证机密是否有必需的标签（项目：atx-db-moderation，所有者：数据库连接器）

防火墙和安全组问题

问题：连接超时或 “无法访问数据库” 错误

根本原因：安全组或网络 ACL 阻塞流量

解决方案：

1. 验证安全组配置：
   - 确认您的 SQL Server 安全组有允许来自 DMS 架构转换安全组的 1433 端口的入站规则
   - 检查来源是否是安全组 ID（例如 sg-0123456789abcdef0），而不是 IP 地址
   - 验证实例配置文件中是否正确指定了 DMS 架构转换安全组
   - 确保没有相互冲突的拒绝规则
2. 检查网络 ACL：
   - 验证子网级别的网络 ACL 是否允许端口 1433 上的入站流量
   - 确保网络 ACL 允许将出站临时端口用于返回流量
   - 检查数据库子网和 DMS 子网网络 ACL
3. 验证 VPC 配置：
   - 确认 DMS 架构转换实例和 SQL Server 在同一 VPC 中或者具有正确的 VPC 对等关系
   - 检查路由表是否允许子网之间的流量
   - 确认没有防火墙设备阻塞流量
4. 测试连接：
   - 在与 DMS 架构转换相同的子网中启动测试 EC2 实例
   - 附加与 DMS 架构转换相同的安全组
   - 使用 telnet 或 SQL 服务器管理工作室测试与 SQL Server 的连接
   - 如果测试成功，则问题出在 AWS 转换配置上；如果测试失败，则问题出在于 network/firewall

常见错误：将端口 1433 打开到 0.0.0。 0/0 （所有来源）存在安全风险。始终使用基于安全组的访问控制，将访问权限限制为 DMS 架构转换安全组。

架构转换问题

问题：架构转换显示了许多操作项

解决方案：

- 查看转化报告中的操作项目
- 根据影响确定优先级
- 使用 Amazon Q 开发人员进行复杂的 SQL 转换
- 请咨询 S AWS upport 以获取指导
- 考虑采用分阶段方法处理复杂的数据库

应用程序转换问题

问题：应用程序转换无法构建

解决方案：

- 查看转换报告中的构建错误
- 如有必 NuGet 要，配置私密订阅源
- 如有必要，更新软件包引用
- 检查 Windows-specific 依赖关系
- 查看转换日志以了解详细错误

数据迁移问题

问题：数据迁移验证失败

解决方案：

- 查看验证报告以了解具体故障
- 检查数据类型映射
- 验证身份列配置（默认生成与始终生成）
- 查看计算列表达式

- 如有复杂的数据问题，请联系 Su AWS pport

资源清理问题

问题：转换作业因资源错误而失败

解决方案：

- 检查现有的 DMS 资源（迁移项目、数据提供者、实例配置文件）
- 清理先前尝试中失败或不完整的资源
- 验证未计划删除密钥
- 查看 DMS 和 Aurora PostgreSQL 的服务配额
- 如果清理不能解决问题，请联系 AWS Support

部署问题

问题：转换后的应用程序无法连接到 Aurora PostgreSQL

解决方案：

- 验证 PostgreSQL 的连接字符串格式
- 查看安全组规则
- 在 Secrets Manager 中验证数据库凭证
- 确保配置 SSL/TLS 正确
- 使用 psql 或 pgadmin 测试连接

获得更多帮助

联系 Su AWS pport 时，请提供：

- 转换作业 ID
- AWS 账号
- Region
- 错误消息和屏幕截图
- 转换日志（可在 AWS 转换控制台中找到）

中的安全性 AWS 转换

云安全 AWS 是重中之重。作为 AWS 客户，您可以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。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。 Third-party 作为AWS 合规计划合规计划合规计划合的一部分，审计师定期测试和验证我们安全的有效性。要了解适用于 T AWS ransform 的合规计划，请参阅按合规计划划分的范围内的AWSAWS 服务按合规计划服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 Transform 时如何应用分担责任 AWS 模型。以下主题向您介绍如何配置 Trans AWS form 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Trans AWS form 资源。

主题

- 中的数据保护 AWS Transform
- 的身份和访问管理 AWS 转换
- 的合规性验证 AWS 转换
- 韧性在 AWS 转换
- AWS Transform 和接口端点 (AWS PrivateLink)
- 访问 AWS Transform 来自 VPC 的 Web 应用程序

中的数据保护 AWS Transform

分 AWS 担责任模型适用于中的数据保护 AWS Transform。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。您还要负责所使用的安全配置和管理任务。 AWS 服务 有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭据并使用 AWS Identity and Access Management (IAM) 设置个人用户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。建议使用 TLS 1.2 或更高版本。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务 Amazon Macie，例如，它有助于发现和保护存储在中的敏感数据 Amazon S3。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用 AWS Transform 或以其他 AWS 服务 方式使用 AWS Management Console、API、 AWS Command Line Interface (AWS CLI) 或 AWS 软件开发工具包的情况。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。有关如何 AWS Transform 使用内容的更多信息，请参阅AWS Transform 服务改进。

AWS Transform 在 IDE 中存储您的问题、答案和其他上下文（例如控制台元数据和代码），以生成对问题的回复。有关如何对数据进行加密的信息，请参阅 中的数据加密 AWS Transform。有关如何 AWS 使用您提出的某些问题 AWS Transform 及其回答来改善我们的服务的信息，请参阅AWS Transform 服务改进。

在中 AWS Transform，您的数据存储在创建您的 AWS Transform 个人资料的 AWS 区域。

通过交叉推理，您的请求 AWS Transform 可能会在存储数据的地理区域内的不同区域进行处理。有关更多信息，请参阅Cross-Region 推理。

主题

- Cross-region 正在处理 AWS Transform
- 中的数据加密 AWS Transform
- AWS Transform 服务改进

Cross-region 正在处理 AWS Transform

以下各节介绍如何使用跨区域推理和跨区域调用来提供服务。 AWS Transform

Cross-region 推断

AWS Transform 由 Amazon Bedrock 提供支持，使用跨区域推理在不同区域之间分配流量， AWS 区域 以增强大型语言模型 (LLM) 的推理性能和可靠性。通过跨区域推理，您可以：

- 在高需求时期提高吞吐量和弹性
- 提高性能
- 访问新推出的 AWS Transform 功能和功能，这些功能依赖于 Amazon Bedrock 上托管的最强大的 LLM

Cross-region 推理请求保存在数据最初所在的地理区域内。 AWS 区域 例如，根据美国 AWS Transform 配置发出的请求保存在美国境内。 AWS 区域 尽管跨区域推理不会更改存储数据的位置，但您的请求和输出结果可能会移出数据最初所在的区域。所有数据都将通过 Amazon 的安全网络加密传输。使用跨区域推理不会产生额外成本。

跨区域推理不会影响存储数据的位置。有关使用时数据存储位置的信息 AWS Transform，请参阅中的数据保护 AWS Transform。

支持的区域 AWS Transform 跨区域推理

您发出的某些请求 AWS Transform 可能需要跨区域调用。下表描述您的请求可能路由到哪些区域，具体取决于发出请求的地理位置。

源区域	目标区域
美国东部（弗吉尼亚州北部）（us-east-1）	美国东部（弗吉尼亚州北部）（us-east-1） 美国东部（俄亥俄州）(us-east-2) 美国西部（俄勒冈州）(us-west-2)
欧洲地区（法兰克福）(eu-central-1)	欧洲地区（法兰克福）(eu-central-1) 欧洲（斯德哥尔摩）(eu-north-1) 欧洲地区（米兰）(eu-south-1)

源区域	目标区域
	欧洲（西班牙）(eu-south-2) 欧洲地区（爱尔兰）(eu-west-1) 欧洲地区（巴黎）（eu-west-3）
亚太地区（孟买）(ap-south-1)	亚太地区（东京）(ap-northeast-1) 亚太地区（首尔）(ap-northeast-2) 亚太地区（大阪）(ap-northeast-3) 亚太地区（孟买）(ap-south-1) 亚太地区（海得拉巴）(ap-south-2) 亚太地区（新加坡）(ap-southeast-1) 亚太地区（悉尼）(ap-southeast-2) 亚太地区（墨尔本）(ap-southeast-4)
亚太地区（东京）(ap-northeast-1)	亚太地区（东京）(ap-northeast-1) 亚太地区（大阪）(ap-northeast-3)
亚太地区（首尔）(ap-northeast-2)	亚太地区（东京）(ap-northeast-1) 亚太地区（首尔）(ap-northeast-2) 亚太地区（大阪）(ap-northeast-3) 亚太地区（孟买）(ap-south-1) 亚太地区（海得拉巴）(ap-south-2) 亚太地区（新加坡）(ap-southeast-1) 亚太地区（悉尼）(ap-southeast-2) 亚太地区（墨尔本）（ap-southeast-4）

源区域	目标区域
亚太地区（悉尼）(ap-southeast-2)	亚太地区（悉尼）(ap-southeast-2) 亚太地区（墨尔本）(ap-southeast-4)
欧洲地区（伦敦）(eu-west-2)	欧洲地区（法兰克福）(eu-central-1) 欧洲（斯德哥尔摩）(eu-north-1) 欧洲地区（米兰）(eu-south-1) 欧洲（西班牙）(eu-south-2) 欧洲地区（爱尔兰）(eu-west-1) 欧洲地区（伦敦）(eu-west-2) 欧洲地区（巴黎）（eu-west-3）
加拿大（中部）(ca-central-1)	商业 AWS 区域 + 加拿大（中部）（ca-central-1）
南美洲（圣保罗）（sa-east-1）	商业 AWS 区域 + 南美洲（圣保罗）（sa-east-1）

有关可供使用的区域的完整列表 AWS Transform，请参阅支持的区域 AWS Transform。

Cross-Region 知识

当您询问有关 AWS Transform 服务、转换工作流程或相关 AWS 文档的一般问题时， AWS Transform 可能会向美国东部（弗吉尼亚）(us-east-1)（美国地区的 us-east-1）或向欧洲（法兰克福）（eu-central-1）提出跨区域请求，要求所有其他地区检索文档并满足您的请求。例如，当您询问有关如何使用其他 AWS 服务（例如 Lambda）的问题时， AWS Transform 可能会拨打跨区域调用以检索相关 AWS 文档来回答您的问题。下表描述您的请求可能路由到哪些区域，具体取决于发出请求的地理位置。

源区域	目标区域
美国东部（弗吉尼亚州北部）（us-east-1）	美国东部（弗吉尼亚州北部）（us-east-1）

源区域	目标区域
欧洲地区（法兰克福）(eu-central-1)	欧洲地区（法兰克福）(eu-central-1)
欧洲地区（伦敦）(eu-west-2)	欧洲地区（法兰克福）(eu-central-1)
亚太地区（东京）(ap-northeast-1)	欧洲地区（法兰克福）(eu-central-1)
亚太地区（悉尼）(ap-southeast-2)	欧洲地区（法兰克福）(eu-central-1)
亚太地区（首尔）(ap-northeast-2)	欧洲地区（法兰克福）(eu-central-1)
亚太地区（孟买）(ap-south-1)	欧洲地区（法兰克福）(eu-central-1)
加拿大（中部）(ca-central-1)	欧洲（法兰克福）(eu-central-1)
南美洲（圣保罗）（sa-east-1）	欧洲地区（法兰克福）(eu-central-1)

默认情况下，此设置处于启用状态。账户管理员可以修改此设置。禁用此功能会导致无法访问 AWS Transform 需要从其他区域检索知识的功能。这可能会导致回复的准确性降低。

要禁用通过以下方式 AWS Transform进行的跨区域呼叫：

1. 首次设置时 AWS Transform，导航到 “入门” 页面并完成配置。对于现有 AWS Transform 配置，请导航到 “设置” 页面。
2. 将启用跨区域呼叫以回答一般 AWS 相关问题切换到关闭位置。

AWS Transform 用于 Windows 跨区域推理

下表显示了您可以从中调用推理配置文件的源区域，以及可以将请求路由到的目标区域：

源区域	推理目标区域
美国东部（弗吉尼亚州北部）（us-east-1）	美国东部（弗吉尼亚州北部）（us-east-1） 美国东部（俄亥俄州）(us-east-2) 美国西部（俄勒冈州）(us-west-2)
欧洲地区（法兰克福）(eu-central-1)	欧洲地区（法兰克福）(eu-central-1)

源区域	推理目标区域
	欧洲（斯德哥尔摩）(eu-north-1) 欧洲地区（米兰）(eu-south-1) 欧洲（西班牙）(eu-south-2) 欧洲地区（爱尔兰）(eu-west-1) 欧洲地区（巴黎）（eu-west-3）
亚太地区（东京）(ap-northeast-1)	亚太地区（东京）(ap-northeast-1) 亚太地区（大阪）(ap-northeast-3)
亚太地区（悉尼）(ap-southeast-2)	亚太地区（悉尼）(ap-southeast-2) 亚太地区（墨尔本）(ap-southeast-4)
亚太地区（首尔）(ap-northeast-2)	所有商业区域
亚太地区（孟买）(ap-south-1)	所有商业区域
加拿大（中部）(ca-central-1)	所有商业区域

AWS Transform 用于跨区域迁移推断

下表显示了您可以从中调用推理配置文件的源区域，以及可以将请求路由到的目标区域：

源区域	推理目标区域
美国东部（弗吉尼亚州北部）（us-east-1）	所有商业区域
欧洲地区（法兰克福）(eu-central-1)	所有商业区域
欧洲地区（伦敦）(eu-west-2)	所有商业区域
亚太地区（东京）(ap-northeast-1)	亚太地区（东京）(ap-northeast-1) 亚太地区（大阪）(ap-northeast-3)

源区域	推理目标区域
亚太地区（悉尼）(ap-southeast-2)	亚太地区（悉尼）(ap-southeast-2) 亚太地区（墨尔本）(ap-southeast-4)
亚太地区（首尔）(ap-northeast-2)	所有商业区域
亚太地区（孟买）(ap-south-1)	所有商业区域
加拿大（中部）(ca-central-1)	所有商业区域

AWS Transform 用于大型机跨区域推理

AWS Transform 对于大型机，使用 Amazon Bedrock 地理跨区域推理。这意味着您的某些呼叫可能会被路由到源区域 AWS 区域 以外。下表显示了您可以从中调用推理配置文件的源区域，以及可以将请求路由到的目标区域：

源区域	推理目标区域
美国东部（弗吉尼亚州北部）（us-east-1）	美国东部（弗吉尼亚州北部）（us-east-1） 美国东部（俄亥俄州）(us-east-2) 美国西部（俄勒冈州）(us-west-2)
欧洲地区（法兰克福）(eu-central-1)	欧洲地区（法兰克福）(eu-central-1) 欧洲（斯德哥尔摩）(eu-north-1) 欧洲地区（米兰）(eu-south-1) 欧洲（西班牙）(eu-south-2) 欧洲地区（爱尔兰）(eu-west-1) 欧洲地区（巴黎）（eu-west-3）
欧洲地区（伦敦）(eu-west-2)	欧洲地区（法兰克福）(eu-central-1) 欧洲（斯德哥尔摩）(eu-north-1)

源区域	推理目标区域
	欧洲地区（米兰）(eu-south-1) 欧洲（西班牙）(eu-south-2) 欧洲地区（爱尔兰）(eu-west-1) 欧洲地区（伦敦）(eu-west-2) 欧洲地区（巴黎）（eu-west-3）
亚太地区（东京）(ap-northeast-1)	亚太地区（东京）(ap-northeast-1) 亚太地区（大阪）(ap-northeast-3)
亚太地区（悉尼）(ap-southeast-2)	亚太地区（悉尼）(ap-southeast-2) 亚太地区（墨尔本）(ap-southeast-4)
亚太地区（首尔）(ap-northeast-2)	所有商业区域
亚太地区（孟买）(ap-south-1)	所有商业区域
加拿大（中部）(ca-central-1)	加拿大（中部）(ca-central-1) 美国东部（弗吉尼亚州北部）（us-east-1） 美国东部（俄亥俄州）(us-east-2) 美国西部（俄勒冈州）(us-west-2)
南美洲（圣保罗）（sa-east-1）	所有商业区域

AWS Transform 自定义

AWS Transform custom 使用 Amazon Bedrock 地理跨区域推理。这意味着您的某些呼叫可能会被路由到源区域 AWS 区域 以外。下表显示了您可以从中调用推理配置文件的源区域，以及可以将请求路由到的目标区域：

源区域	推理目标区域
美国东部（弗吉尼亚州北部）（us-east-1）	美国东部（弗吉尼亚州北部）（us-east-1） 美国东部（俄亥俄州）(us-east-2) 美国西部（俄勒冈州）(us-west-2)
欧洲地区（法兰克福）(eu-central-1)	欧洲地区（法兰克福）(eu-central-1) 欧洲（斯德哥尔摩）(eu-north-1) 欧洲地区（米兰）(eu-south-1) 欧洲（西班牙）(eu-south-2) 欧洲地区（爱尔兰）(eu-west-1) 欧洲地区（巴黎）（eu-west-3）
欧洲地区（伦敦）(eu-west-2)	欧洲地区（法兰克福）(eu-central-1) 欧洲（斯德哥尔摩）(eu-north-1) 欧洲地区（米兰）(eu-south-1) 欧洲（西班牙）(eu-south-2) 欧洲地区（爱尔兰）(eu-west-1) 欧洲地区（伦敦）(eu-west-2) 欧洲地区（巴黎）（eu-west-3）
亚太地区（东京）(ap-northeast-1)	所有商业区域
亚太地区（悉尼）(ap-southeast-2)	亚太地区（悉尼）(ap-southeast-2) 亚太地区（墨尔本）(ap-southeast-4)
亚太地区（首尔）(ap-northeast-2)	所有商业区域

源区域	推理目标区域
亚太地区（孟买）(ap-south-1)	所有商业区域
加拿大（中部）(ca-central-1)	加拿大（中部）(ca-central-1) 美国东部（弗吉尼亚州北部）（us-east-1） 美国东部（俄亥俄州）(us-east-2) 美国西部（俄勒冈州）(us-west-2)

中的数据加密 AWS Transform

本主题提供有关传输中加密和静态加密的特定信息。 AWS Transform

AWS Transform 默认提供加密，使用 AWS 自有密钥进行加密，从而保护敏感的静态客户数据。

加密类型

传输中加密

使用 TLS 1.2 或更高版本的连接保护客户 AWS Transform 与其下游依赖关系之间的通信。 AWS Transform

> **Important**
>
> 当您连接发现账户时，T rans AWS form 会代表您在该账户中创建一个 Amazon S3 存储桶。默认情况下，该存储桶未`SecureTransport`启用。如果您希望存储桶策略包含安全传输，则必须更新该策略。有关更多信息，请参阅 Amazon S3 的安全最佳实践。

静态加密

AWS Transform 使用亚马逊 DynamoDB 和亚马逊简单存储服务 (Amazon S3) Service 存储静态数据。默认情况下，静态数据使用 AWS 加密解决方案进行加密。 AWS Transform 使用来自 AWS Key Management Service (AWS KMS) 的 AWS 自有密钥加密您的数据。您无需采取任何措施来保护加密数据的 AWS 托管密钥。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的 AWS 拥有密钥。

数据类型	AWS自有密钥加密	客户托管密钥加密（可选）
客户存储桶数据 客户输入和输出，例如存储在 Amazon S3 存储桶中的代码和文档	已启用	已启用
Artifact 作为代码转换一部分的中间工件存储在 S3 存储桶中	已启用	已启用
Job 目标 客户对任务的意图存储在 Amazon S3 存储桶中	已启用	已启用
聊天消息 客户之间的消息以及 AWS Transform 存储在 Amazon S3 存储桶中的消息	已启用	已启用
聊天知识库 与之相关的索引数据 AWS Transform 和客户聊天数据存储在亚马逊 OpenSearch 并通过 B AWS edrock 进行处理	已启用	已启用

注意：客户可以注册自己的客户管理密钥 (CMK)，用于加密上述所有数据类型。

客户托管密钥是您在 AWS 账户中创建、拥有和管理的 KMS 密钥，通过控制 KMS 密钥的访问权限来直接控制对数据的访问。仅支持对称密钥。有关创建自己的 KMS 密钥的信息，请参阅AWS Key Management Service 开发人员指南中的创建密钥。

使用客户托管密钥时， AWS Transform 使用 KMS 授权，允许授权用户、角色或应用程序使用 KMS 密钥。如果 AWS Transform 管理员选择在配置期间使用客户托管密钥进行加密，则会为他们创建授

权。此项授权可让最终用户使用加密密钥进行静态数据加密。有关授权的更多信息，请参阅 Grants in AWS KMS。

AWS 自有密钥（默认）

> **Note**
>
> AWS 自有密钥 — 默认 AWS Transform 使用这些密钥自动加密个人身份数据。您无法查看、管理或使用 AWS 自有密钥，也无法审核其使用情况。但是，无需采取任何措施或更改任何计划即可保护用于加密数据的密钥。有关更多信息，请参阅《密 AWS钥管理服务开发者指南》中的 AWS 自有密钥。

默认情况下，静态数据加密有助于降低保护敏感数据的操作开销和复杂性。同时，它还支持构建符合严格加密合规性和监管要求的安全应用程序。

虽然您无法禁用此加密层或选择其他加密类型，但您可以在创建转换时选择客户托管密钥，从而在现有 AWS 拥有的加密密钥上添加第二层加密：

客户管理的密钥（可选）

客户托管密钥 — AWS Transform 支持使用您创建、拥有和管理的对称客户托管密钥，在使用 AWS 自有密钥的现有加密基础上添加第二层加密。由于您可以完全控制这层加密，因此可以执行以下任务：

- 制定和维护关键策略
- 建立和维护 IAM 策略和授权
- 启用和禁用密钥策略
- 轮换加密材料
- 添加 标签
- 创建密钥别名
- 轮换加密材料
- 添加 标签
- 创建密钥别名
- 安排密钥删除
- 有关更多信息，请参阅《AWS Key Management Service Developer Guide》中的 customer managed key。

> **Note**
>
> AWS Transform 使用 AWS 自有密钥自动启用静态加密，以免费保护个人身份数据。但是，使用客户管理的密钥需要 AWS KMS 付费。有关定价的更多信息，请参阅 AWS Key Management Service 定价。

有关的更多信息 AWS KMS，请参阅什么是 AWS Key Management Service？

操作方法 AWS Transform 将补助金用于 AWS Key Management Service

AWS Transform 需要获得授权才能使用您的客户托管密钥。

当您创建使用客户托管密钥加密的 [资源名称] 时， AWS Transform 会通过向发送 CreateGrant 请求来代表您创建授权 AWS Key Management Service。中的授权 AWS Key Management Service 用于授予对客户账户中的 KMS 密钥的 AWS Transform 访问权限。

AWS Transform 需要获得授权才能使用您的客户托管密钥进行以下内部操作：

- 向发送 [KMS API] 请求， AWS KMS 以验证创建 [资源名称] 时输入的对称客户托管 KMS 密钥 ID 是否有效。
- 向发送 [KMS API] 请求 AWS KMS 以生成由您的客户托管密钥加密的数据密钥。
- 向发送 [KMS API] 请求 AWS KMS 以解密加密的数据密钥，以便这些密钥可用于加密您的数据。

您可以随时撤销授予访问权限，或删除服务对客户托管密钥的访问权限。如果这样做，将 AWS Transform 无法访问由客户托管密钥加密的任何数据，这会影响依赖该数据的操作。例如，如果您尝试从 AWS Transform 无法访问的加密 [资源名称] 中获取 [资源名称]，则该操作将返回 AccessDeniedException 错误。

创建客户托管密钥

您可以使用管理控制台或 AWS Key Management Service API 创建对称客户托管密钥。 AWS

要创建对称客户托管密钥，请按照《AWS Key Management Service 开发人员指南》中的创建对称客户托管密钥步骤进行操作。

要将客户托管密钥 AWS Transform 用于您的资源，必须在密钥策略中允许以下 API 操作：

kms: CreateGrant — 向客户托管密钥添加授权。授予对指定 KMS 密钥的控制访问权限，从而允许对授予操作 AWS Transform 所需的访问权限。有关使用授权的更多信息，请参阅《AWS Key Management Service 开发人员指南》。

这 AWS Transform 允许执行以下操作：

- 调用 [KMS API (GenerateDataKeyWithoutPlainText/GenerateDatakey) 生成加密的数据密钥并将其存储，因为数据密钥不会立即用于加密。
- 调用 [KMS API (Decrypt)] 使用存储的加密数据密钥访问加密数据。
- 设置停用主体，以允许服务 RetireGrant。
- kms: DescribeKey — 提供客户托管密钥详细信息以允许 [服务名称] 验证密钥。

用于 SQL 现代化的加密

在 SQL Server 现代化过程中，在您的账户中 AWS Transform 创建资源，例如 EC2 实例、ECS 集群、ECR 映像和 S3 对象。您可以选择提供客户管理的密钥来加密您账户中的数据。您需要使用密钥CreatedFor和值 a wstR ansForm 标记您的 KMS 密钥。如果您没有默认密钥策略，则此示例策略列出了密钥策略所需的最低权限。如果您有默认密钥策略，则除了默认密钥策略外，还需要手动更新 KMS 密钥以允许 ECS 使用您的密钥。

```
"Statement": [
   {
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::111122223333:root"
     },
     "Action": [
       "kms:Decrypt",
       "kms:GenerateDataKey"
     ],
     "Resource": "*",
     "Condition": {
       "StringLike": {
         "kms:ViaService": "s3.*.amazonaws.com",
         "kms:EncryptionContext:aws-transform": "*"
       },
       "ArnLike": {
         "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
       }
     }
```

```
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncrypt*"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        },
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:CreateGrant",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "ec2.*.amazonaws.com",
            "ecr.*.amazonaws.com"
          ]
        },
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        },
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::*:role/*AWSTransform*"
        }
      }
    },
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "fargate.amazonaws.com"
      },
      "Action": "kms:GenerateDataKeyWithoutPlaintext",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:ecs:clusterName": "AWSTransform*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "fargate.amazonaws.com"
      },
      "Action": "kms:CreateGrant",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:ecs:clusterName": "AWSTransform*"
        },
        "ForAllValues:StringEquals": {
          "kms:GrantOperations": "Decrypt"
        }
      }
    }
  ]
```

用于数据库迁移的加密

在数据库迁移过程中，AWS Transform 使用 AWS 数据库迁移服务 (DMS) 迁移您的数据库数据。您可以选择提供客户托管密钥，以便在迁移期间加密您的数据库数据。

以下策略包含三个声明。第一条语句授予根账户使用 AWS KMS 密钥的权限。第二条语句允许连接器角色在发现期间验证密钥。第三条语句允许连接器角色使用密钥进行 DMS 操作。

```
"Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
```

```
      "Principal": { "AWS": "arn:aws:iam::111122223333:root" },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow connector role to validate key during discovery",
      "Effect": "Allow",
      "Principal": { "AWS": "connector-role-arn" },
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "Allow connector role to use key via DMS",
      "Effect": "Allow",
      "Principal": { "AWS": "connector-role-arn" },
      "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:ReEncrypt*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "dms.us-east-1.amazonaws.com"
        }
      }
    }
  ]
```

使用客户自主管理型 KMS 密钥

创建客户托管的 KMS 密钥后，AWS Transform 管理员必须在 AWS Transform 控制台中提供密钥才能使用它来加密数据。

要设置用于加密数据的客户托管密钥 AWS Transform，管理员需要使用权限 AWS KMS。

要使用使用客户托管密钥加密的功能，用户需要获得 AWS Transform 访问客户托管密钥的权限。

如果您在使用时看到与 KMS 授权相关的错误 AWS Transform，则可能需要更新权限 AWS Transform 以允许创建授权。要自动配置所需的权限，请转到 AWS Transform 控制台并在页面顶部的横幅中选择“更新权限”。 AWS Transform 要允许创建授权，您需要更新 AWS Transform 控制台页面上的权限。

允许 AWS Transform 访问客户管理的密钥

以下示例政策声明通过允许用户访问使用客户托管密钥加密的密钥，向用户授予 AWS Transform 访问该密钥的权限。 AWS Transform 如果管理员设置了用于加密的客户托管密钥，则必须使用此策略。

> **Note**
>
> 此信息不适用于使用 CMK 的 SQL Server 现代化部署工作流程。

```
"Statement": [
   {
     "Sid": "QKMSDecryptGenerateDataKeyPermissions",
     "Effect": "Allow",
     "Action": [
       "kms:Decrypt",
       "kms:GenerateDataKey",
       "kms:GenerateDataKeyWithoutPlaintext",
       "kms:ReEncryptFrom",
       "kms:ReEncryptTo"
     ],
     "Resource": [
       "arn:aws:kms:arn:aws::111122223333:key/[[key_id]]"
     ],
     "Condition": {
       "StringLike": {
         "kms:ViaService": [
           "q.us-east-1.amazonaws.com"
         ]
       }
     }
   }
 ]
```

AWS Transform 服务改进

为了帮助 AWS Transform 提供最相关的信息，我们可能会使用来自 AWS Transform的某些内容（例如您提出的问题 AWS Transform 及其回答）来改进服务。本页说明了我们使用哪些内容以及您如何选择不授权。

AWS Transform 用于服务改进的内容

我们可能会使用来自 AWS Transform 的某些内容来改善服务。 AWS Transform 例如，可以使用此内容来更好地回答常见问题、修复 AWS Transform 操作问题、调试错误或进行模型训练。

例如， AWS 可用于改进服务的内容包括您提出的问题 AWS Transform 以及 AWS Transform 生成的回复和代码。

如何选择不授权

您选择不 AWS Transform 使用内容来改善服务的方式取决于您使用的环境 AWS Transform。

AWS Transform 要在中配置 AI 服务选择退出策略。 AWS Organizations有关更多信息，请参阅《AWS Organizations 用户指南》中的 AI 服务选择退出策略。

要选择不在 Visual Studio IDE 中共享您的内容，请按以下步骤操作。

前往工具 -> 选项 -> AWS Toolkit -> Amazon Q

将与 AWS共享 Amazon Q 内容切换为是或否。

要选择不在 T AWS oolkit 中共享您的遥测数据Visual Studio，请按以下步骤操作：

1. 在 Tools 下，选择 Options。
2. 在 Options 窗格中，选择 AWS Toolkit，然后选择 General。
3. 取消选择 “允许 AWS Toolkit 收集使用情况信息”。

的身份和访问管理 AWS 转换

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）来使用 Trans AWS form 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅问题排查 AWS 转变身份和访问权限）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅操作方法 AWS 转换与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅Identity-based 的策略示例 AWS 转换）

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问， AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 根用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

Identity-based 政策

Identity-based 策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

Identity-based 策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

Resource-based 政策

Resource-based 策略是您附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中指定主体。

Resource-based 策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略（SCP）– 指定 AWS Organizations中组织或组织单元的最大权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略（RCP）– 设置对账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略（RCP）。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

操作方法 AWS 转换与 IAM 配合使用

在使用 IAM 管理对 T AWS ransform 的访问权限之前，请先了解哪些可用于 T AWS ransform 的 IAM 功能。

IAM 功能	AWS 变换支持
Identity-based 政策	是
Resource-based 政策	否
策略操作	是
策略资源	是
策略条件键	是
ACL	否
ABAC（策略中的标签）	部分
临时凭证	是
主体权限	是
服务角色	是
Service-linked 角色	是

要全面了解 Trans AWS form 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

Identity-based 的政策 AWS 转换

支持基于身份的策略：是

Identity-based 策略是您可以附加到身份（例如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Identity-based 的策略示例 AWS 转换

要查看 AWS 转换基于身份的策略的示例，请参阅。Identity-based 的策略示例 AWS 转换

Resource-based 内部的政策 AWS 转换

支持基于资源的策略：否

Resource-based 策略是您附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

的政策行动 AWS 转换

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

要查看 AWS 转换操作列表，请参阅《服务授权参考》中的 “AWS 转换” 的操作、资源和条件键。

要查看 Trans AWS for m 自定义操作列表，请参阅《服务授权参考》中的 T AWS ransform custom 的操作、资源和条件键。

Transf AWS orm 中的策略操作在操作前使用以下前缀：

```
transform
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "transform:action1",
      "transform:action2"
         ]
```

要查看 AWS 转换基于身份的策略的示例，请参阅。Identity-based 的策略示例 AWS 转换

的政策资源 AWS 转换

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 AWS 转换资源类型及其 ARN 的列表，以及您可以使用哪些操作来指定每种资源的 ARN，请参阅《服务授权参考》中的 Transform AWS 的操作、资源和条件键。

要查看资源类型及其 ARN 的列表，以及您可以通过哪些操作 AWS 为转换自定义指定每种资源的 ARN，请参阅《服务授权参考》中的 Transform custom AWS 的操作、资源和条件键。

要查看 AWS 转换基于身份的策略的示例，请参阅。Identity-based 的策略示例 AWS 转换

的策略条件键 AWS 转换

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Condition 元素根据定义的条件指定语句何时执行。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 AWS 转换条件键的列表以及可以与哪些操作和资源一起使用条件键，请参阅《服务授权参考》中的 Trans AWS form 的操作、资源和条件键。

要查看条件键列表以及您可以使用哪些操作和资源进行 AWS 转换自定义，请参阅《服务授权参考》中的 Transf AWS orm custom 的操作、资源和条件键。

要查看 AWS 转换基于身份的策略的示例，请参阅。Identity-based 的策略示例 AWS 转换

输入的 ACL AWS 转换

支持 ACL：否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，但它们不使用 JSON 策略文档格式。

ABAC with AWS 转换

支持 ABAC（策略中的标签）：部分支持

Attribute-based 访问控制 (ABAC) 是一种授权策略，它根据称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`aws:RequestTag/*key-name* 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时证书与 AWS 转换

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

Cross-service 的委托人权限 AWS 转换

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

的服务角色 AWS 转换

支持服务角色：是

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 Trans AWS form 功能。只有在 Trans AWS form 提供相关指导时才编辑服务角色。

Service-linked 的角色 AWS 转换

支持服务关联角色：是

服务相关角色是一种链接到的服务角色。 AWS 服务该服务可以代替您执行操作。 Service-linked 角色出现在您的， AWS 账户 并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

有关创建或管理 Trans AWS form 服务相关角色的详细信息，请参阅将服务相关角色用于 AWS Transform。

Identity-based 的策略示例 AWS 转换

默认情况下，用户和角色无权创建或修改 Trans AWS form 资源。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 Tr AWS ansform 定义的操作和资源类型（包括每种资源类型的 ARN 格式）的详细信息，请参阅《服务授权参考》中的 “AWS 转换操作、资源和条件密钥”。

主题

策略最佳实践

Identity-based 策略决定了某人是否可以在您的账户中创建、访问或删除 T AWS ransform 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 AWS 改造控制台

要访问 T AWS ransform 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Trans AWS form 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

允许管理员接受账户发出的连接器请求 AWS 转换

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "transform:GetConnector",
                "transform:AssociateConnectorResource",
                "transform:RejectConnector"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketPublicAccessBlock",
                "s3:GetAccountPublicAccessBlock"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:AttachRolePolicy",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/service-role/
AWSTransform-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy"
```

```
            ],
            "Resource": "arn:aws:iam::111122223333:policy/service-role/
AWSTransform-*"
        }
    ]
}
```

允许管理员分配现有的 IAM Identity Center 用户并创建要分配给的新 IAM 身份中心用户 AWS 转换

以下策略授予管理员在 Trans AWS form 控制台中管理 IAM Identity Center 用户和群组所需的权限。通过此策略，管理员可以分配和删除用户和群组、查看显示名称、创建新的 IAM Identity Center 用户、管理应用程序分配以及配置应用程序会话设置。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSOApplicationAssignments",
      "Effect": "Allow",
      "Action": [
        "sso:ListApplicationAssignments",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
        "sso:ListInstances",
        "sso:DescribeInstance",
        "sso:ListDirectoryAssociations",
        "sso:GetApplicationGrant",
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationSessionConfiguration",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSODirectoryCreateUser",
      "Effect": "Allow",
      "Action": [
        "sso-directory:CreateUser"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "IdentityStoreAccess",
      "Effect": "Allow",
      "Action": [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListUsers",
        "identitystore:ListGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowKmsAccessViaIdentityCenter",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:*:sso:::instance/*"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowKmsAccessViaIdentityStore",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

允许管理员启用 AWS 转换

以下策略授予管理员通过 AWS 控制台启用和管理 Trans AWS form 所需的权限。这包括管理配置文件、配置代理和管理连接器。本政策仅适用于管理员，其范围应限于您账户中受信任的委托人。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSOEnableTransform",
      "Effect": "Allow",
      "Action": [
        "sso:ListInstances",
        "sso:CreateInstance",
        "sso:CreateApplication",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:ListApplications",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:PutApplicationAccessScope",
        "sso:DescribeApplication",
        "sso:DeleteApplication",
        "sso:UpdateApplication",
        "sso:DescribeRegisteredRegions",
        "sso:GetSSOStatus"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSODirectoryActions",
      "Effect": "Allow",
      "Action": [
        "sso-directory:GetUserPoolInfo",
        "sso-directory:DescribeUsers",
        "sso-directory:DescribeGroups",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso-directory:DescribeDirectory"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "KMSListAliases",
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Sid": "KMSActions",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey*",
        "kms:RetireGrant",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "transform.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "IAMServiceLinkedRole",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": [
        "arn:*:iam::*:role/aws-service-role/transform.amazonaws.com/
AWSServiceRoleForAWSTransform"
      ]
    },
    {
      "Sid": "TransformConsoleActions",
      "Effect": "Allow",
      "Action": [
```

```
        "transform:GetAccountSettings",
        "transform:UpdateAccountSettings",
        "transform:CreateProfile",
        "transform:UpdateProfile",
        "transform:DeleteProfile",
        "transform:ListProfiles",
        "transform:GetConnector",
        "transform:ListConnectors",
        "transform:DeleteConnector",
        "transform:AssociateConnectorResource",
        "transform:RejectConnector",
        "transform:ListAgents",
        "transform:GetAgent",
        "transform:GetAgentRuntimeConfiguration",
        "transform:PutAgentRuntimeConfiguration",
        "transform:UpdateAgentAccess",
        "transform:TagResource",
        "transform:UntagResource",
        "transform:ListTagsForResource",
        "transform:GetWebAppUrl"
      ],
      "Resource": "*"
    }
  ]
}
```

允许用户访问 AWS 使用 IAM 凭证进行转型

以下策略授予 IAM 委托人使用 IAM 证书访问 T AWS ransform Web 应用程序和 API 的访问权限。IAM-only 访问和与身份提供商一起启用 IAM 访问都需要此政策。

用您的值替换*regionaccount-id*、和*profile-id*。你可以在 Transf AWS orm 控制台的 “设置” 下找到配置文件 ID。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccess",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/profile-id"
    }
```

```
  ]
}
```

要授予对账户中所有个人资料的访问权限，请使用通配符作为配置文件 ID：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccessAllProfiles",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/*"
    }
  ]
}
```

> **Note**
>
> 该`transform:AccessTransformProfile`操作仅授予对 AWS 变换的访问权限。工作空间内的操作由 AWS 转换工作空间角色（管理员、贡献者、批准者 Read-only）控制，而不是 IAM 策略控制。工作空间角色决定了用户可以执行的操作，例如创建作业、管理协作者或批准任务。

问题排查 AWS 转变身份和访问权限

使用以下信息来帮助您诊断和修复在使用 Transf AWS orm 和 IAM 时可能遇到的常见问题。

主题

- 我无权在以下位置执行操作 AWS 转换
- 我无权执行 iam：PassRole
- 我想允许我以外的人进入 AWS 账户 访问我的 AWS 转换资源

我无权在以下位置执行操作 AWS 转换

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 AWS Transform:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: AWS
 Transform:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 AWS Transform:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到错误消息，提示您无权执行iam:PassRole操作，则必须更新您的策略以允许您将角色传递给 Trans AWS form。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户marymajor尝试使用控制台在 Trans AWS form 中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人进入 AWS 账户 访问我的 AWS 转换资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Trans AWS form 是否支持这些功能，请参阅操作方法 AWS 转换与 IAM 配合使用。

- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

将服务相关角色用于 AWS Transform

AWS Transform 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 AWS Transform Service-linked 角色由预定义 AWS Transform ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

将服务相关角色用于 AWS Transform

AWS Transform 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 AWS Transform Service-linked 角色由预定义 AWS Transform ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置变得 AWS Transform 更加容易，因为您不必手动添加必要的权限。 AWS Transform 定义其服务相关角色的权限，除非另有定义，否则 AWS Transform 只能担任其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务关联角色。这样可以保护您的 AWS Transform 资源，因为您不会无意中删除访问资源的权限。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的AWS 服务，并在Service-linked 角色列中查找带有 “是” 的服务。请选择是与查看该服务的服务关联角色文档的链接。

Service-linked 的角色权限 AWS Transform

AWS Transform 使用名为的服务相关角色 AWSServiceRoleForAWSTransform— 此 Service-Linked 角色为 T AWS ransform 提供了提供使用信息的能力。

AWSServiceRoleForAWSTransform 服务相关角色信任以下服务来代入该角色：

- `transform.amazonaws.com`

名为的角色权限策略 AWSServiceRoleForAWSTransform AWS Transform 允许对指定资源完成以下操作：

- 云观察：PutMetricData
  - 将自定义指标发送到以 CloudWatch 进行 AWS Transform 操作
  - 跟踪转型进度、成功率和绩效指标
  - 启用对转换工作流程的监控和警报
- sso：DescribeApplication
  - 在 Identity Center 中查看有关特定应用程序的详细信息
  - 获取应用程序元数据，例如名称、描述、状态和配置
- sso：GetApplicationAssignmentConfiguration
  - 检索应用程序的分配配置设置
  - 查看如何配置 users/groups 为分配给应用程序
- sso：ListApplicationAssignmentsForPrincipal
  - 列出分配给特定用户或组（主用户）的所有应用程序
  - 查看特定身份可以访问哪些应用程序
- 通过 IAM 身份中心访问时启用 KMS-encrypted 数据解密。仅当加密上下文包含有效的 IAM 身份中心实例 ARN 且必须通过 IAM 身份中心服务终端节点访问时才有效。
- 允许通过身份存储访问 KMS-encrypted 数据时解密数据。仅当加密上下文包含有效的身份存储 ARN 且必须通过身份存储服务端点访问时才有效。
- 秘密管理器：GetSecretValue
  - 访问用于存储外部身份提供商的客户机密的 AWS Transform 服务相关密钥
  - 资源：arn: aws: secretsmanager: *: *: secret: transform-preprod！ *
  - 条件：必须由 transform-preprod 服务拥有并可通过同一个账户进行访问
- 支持:CreateCase，支持：DescribeCases，支持：，支持：DescribeCommunications，支持：AddCommunicationToCase，支持：ResolveCase
  - 通过 AWS Transform Web 应用程序创建和管理高级支持案例
  - 查看案例详情和沟通
  - 添加沟通并解决支持案例

您必须配置使用户、组或角色能够创建、编辑或删除服务相关角色的权限。有关更多信息，请参阅 IAM 用户指南中的Service-linked 角色权限。

为 创建服务相关角色 AWS Transform

您无需手动创建服务关联角色。 AWS Transform 在中为创建配置文件时 AWS Management Console， AWS Transform 会为您创建服务相关角色。

如果您删除该服务关联角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。更新设置时， AWS Transform 会再次为您创建服务相关角色。

您也可以使用 IAM 控制台或 AWS CLI 创建具有服务名称的`transform.amazonaws.com`服务相关角色。有关更多信息，请参阅 IAM 用户指南 中的创建服务相关角色。如果您删除了此服务相关角色，可以使用同样的过程再次创建角色。

为 编辑服务相关角色 AWS Transform

AWS Transform 不允许您编辑 AWSServiceRoleForAWSTransform 服务相关角色。创建服务关联角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

删除 的服务相关角色 AWS Transform

如果您不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果您尝试删除资源时 AWS Transform 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

使用 IAM 手动删除服务关联角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForAWSTransform服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

支持的区域 AWS Transform 服务关联角色

AWS Transform 不支持在提供服务的每个区域中使用服务相关角色。您可以在以下区域使用该 AWSServiceRoleForAWSTransform 角色。有关更多信息，请参阅AWS 区域和端点。

区域名称	区域标识	Support in AWS Transform
美国东部（弗吉尼亚州北部）	us-east-1	是
欧洲地区（法兰克福）	eu-central-1	是

将服务相关角色用于 AWS 变换自定义

AWS Transform Custom 使用名AWSServiceRoleForAWSTransformCustom为的服务相关角色代表您向您的账户发布指标和日志。这些指标允许您直接在仪表板中监控转换计数、延迟和状态代码。通过日志，可以查看转换过程中遇到的问题。

此服务相关角色由 Tr AWS ansform Custom 预定义，仅包含服务所需的权限。您无需手动添加任何权限，该角色只能由 Transform Custom AWS 担任。有关服务相关角色的一般信息，请参阅 IAM 用户指南中的使用服务相关角色。

Service-linked 的角色权限 AWS 变换自定义

AWSServiceRoleForAWSTransformCustom 服务相关角色信任以下服务来代入该角色：

- `transform-custom.amazonaws.com`

名为的角色权限策略 AWSServiceRoleForAWSTransformCustom 允许 T AWS ransform Custom 对指定资源完成以下操作：

- `cloudwatch:PutMetricData`在所有 AWS 资源上
  - 将操作指标发布到`AWS/TransformCustom`命名空间下方
  - 跟踪转换计数、延迟和状态码
  - 通过`cloudwatch:namespace`条件键限定到`AWS/TransformCustom`命名空间
- `logs:CreateLogGroup`然后`logs:PutRetentionPolicy`在`/aws/TransformCustom`日志组上
  - 创建用于发布转换 CloudWatch 日志的日志日志组
  - 在日志组上设置日志保留策略
  - 范围设定为`arn:aws:logs:*:*:log-group:/aws/TransformCustom`，`aws:ResourceAccount`条件是确保只能在您的账户内进行访问

- `logs:CreateLogStream`logs:PutLogEvents并在日志组内的/aws/TransformCustom日志流上
  - 为转换操作创建日志流并发布日志事件
  - 范围设定为`arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*`，`aws:ResourceAccount`条件是确保只能在您的账户内进行访问

您必须配置使用户、组或角色能够创建、编辑或删除服务相关角色的权限。有关更多信息，请参阅 IAM 用户指南中的Service-linked 角色权限。

为 创建服务相关角色 AWS 变换自定义

您无需手动创建服务关联角色。当您使用转换自定义 CLI 运行 AWS 转换时，自定义 AWS 转换会为您创建服务相关角色。

如果您删除该服务关联角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您使用转换自定义 CLI 运行 AWS 转换时，自定义 AWS 转换会再次为您创建服务相关角色。

您也可以使用 IAM 控制台为 AWSServiceRoleForAWSTransformCustom 使用案例创建服务相关角色。在 AWS CLI 或 AWS API 中，使用服务名称创建服务相关角色。`transform-custom.amazonaws.com`有关更多信息，请参阅 IAM 用户指南 中的创建服务相关角色。如果您删除了此服务相关角色，可以使用同样的过程再次创建角色。

为 编辑服务相关角色 AWS 变换自定义

AWS 自定义转换不允许您编辑 AWSServiceRoleForAWSTransformCustom 服务相关角色。创建服务关联角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

删除 的服务相关角色 AWS 变换自定义

如果您不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。

AWSServiceRoleForAWSTransformCustom 服务相关角色不会在您的账户中创建永久资源。您可以直接将其删除，而无需清理任何资源。

如果您删除此角色，然后使用 AWS 转换自定义 CLI 运行转换，则会自动重新创建服务相关角色。

使用 IAM 手动删除服务关联角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForAWSTransformCustom服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

支持的区域 AWS 转换自定义服务相关角色

AWS Transform Custom 支持在所有可用 “自定义 AWS 转换” 的区域中使用服务相关角色。有关支持的区域列表，请参阅支持的区域。

AWS 的托管策略 AWS 转换

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 转换更新 AWS 托管策略

查看自 2021 年 3 月 1 日以来 AWS 转型 AWS 托管策略更新的详细信息。

更改	描述	日期
AWSTransformInfrastructureExecutorAccessBatch - 新策略	添加了一个新的 AWS 托管策略，该策略授予使用 B AWS atch 执行 AWS 转型持续现代化评估和转换所需的权限，包括上传源代码、检索结果、监控批处理作业状态、读取日志和管理转换计划。	2026年7月20日
AWSTransformInfrastructureExecutorAccessEC2：新策略	添加了一个新的 AWS 托管策略，该策略授予使用 Amazon EC2 执行 AWS 转型持续现代	2026年7月20日

更改	描述	日期
	化评估和转换所需的权限，包括上传源代码、检索结果、监控任务状态和管理转换计划。	
AWSTransformSecurityAgentExecutorAccess：新策略	添加了一个新的 AWS 托管策略，该策略授予 T AWS ransform Continue Moderation 调用 AWS 安全代理服务以进行自动代码安全审查和修复（包括上传扫描工件和检索结果）所需的权限。	2026 年 6 月 30 日
AWSServiceRoleForAWSTransformCustom - 更新的策略	添加了 CloudWatch 日志权限以允许 T AWS ransform custom 将`/aws/TransformCustom` 日志发布到您账户中的日志组。	2026 年 5 月 5 日
AWSTransformCustomExecuteTransformations - 更新的策略	添加了创建 Trans AWS form 自定义服务关联角色 (`AWSServiceRoleForAWSTransformCustom`) 的权限，以允许向客户账户发布 CloudWatch 指标。	2026 年 4 月 27 日
AWSTransformCustomManageTransformations - 更新的策略	添加了创建 Trans AWS form 自定义服务关联角色 (`AWSServiceRoleForAWSTransformCustom`) 的权限，以允许向客户账户发布 CloudWatch 指标。	2026 年 4 月 27 日

更改	描述	日期
AWSTransformCustomFullAccess - 更新的策略	添加了创建 Trans AWS form 自定义服务关联角色 (AWSServiceRoleForAWSTransformCustom) 的权限，以允许向客户账户发布 CloudWatch 指标。	2026 年 4 月 7 日
AWSServiceRoleForAWSTransformCustom：新策略	为 Trans AWS form 自定义服务相关角色添加了新的 AWS 托管策略。此政策允许 T AWS ransform custom 向您的账户发布 CloudWatch 指标。	2026 年 3 月 23 日
DBModProvisioningAndMigration：新策略	此策略授予数据库配置和迁移功能。	2026年3月24日
DBModDiscoveryAndAssessment：新策略	添加了新的 AWS 托管策略，该策略提供了全面的数据库现代化发现和评估功能。	2026年3月24日
AWSTransformCustomFullAccess：新策略	添加了一个新的 AWS 托管策略，该策略提供对 Trans AWS form 自定义的完全访问权限。	2025 年 12 月 5 日
AWSTransformCustomExecuteTransformations：新策略	添加了一个新的 AWS 托管策略，该策略提供在 Transform custo AWS m 中执行转换的权限。	2025 年 12 月 5 日
AWSTransformCustomManageTransformations：新策略	添加了一个新的 AWS 托管策略，该策略允许用户在 Transform custom 中创建、更新、读取和删除 AWS 转换资源以及执行转换。	2025 年 12 月 5 日

更改	描述	日期
AWSServiceRoleForAWSTransform - 更新的策略	增加了访问用于存储外部身份提供商 AWS 的客户端密钥的 Transform 服务相关密钥的权限。 添加了通过 T AWS ransform Web 应用程序创建高级支持案例的权限。	2025 年 12 月 1 日
AWSTransformApplicationECSDeploymentPolicy - 更新的策略	添加了 IAM 角色检查权限、ECS 服务相关角色创建以及支持 ECR 加密的 KMS 权限。	2025 年 11 月 22 日
AWSTransformApplicationDeploymentPolicy - 更新的策略	添加了 EC2 联网权限、IAM 角色检查权限、S3 存储桶列表权限和 KMS 加密支持，以增强部署功能。	2025 年 11 月 22 日
AWSServiceRoleForAWSTransform - 更新的策略	在 IAM 身份中心增加了对客户托管密钥的支持。	2025 年 9 月 17 日
AWSTransformApplicationDeploymentPolicy：新策略	添加了一个新的 AWS 托管策略，允许 Tr AWS ansform 通过创建和管理 Amazon EC2 实例、 CloudFormation 堆栈和相关资源来部署转换后的.NET 应用程序。	2025 年 8 月 28 日
AWSServiceRoleForAWSTransform - 更新的策略	添加了新的 策略。	2025 年 5 月 15 日

AWS 托管策略： AWSServiceRoleForAWSTransform

此策略附加到AWSServiceRoleForAWSTransform服务相关角色 (SLR)。

权限详细信息

要查看策略权限的详细信息，请参阅AWSServiceRoleForAWSTransform《 AWS 托管策略参考指南》。

AWS 托管策略： AWSServiceRoleForAWSTransformCustom

此策略附加到AWSServiceRoleForAWSTransformCustom服务相关角色 (SLR)。此角色允许 T AWS ransform custom 代表您向您的账户发布 CloudWatch 指标和日志。

描述

该策略包含以下权限：

- Amazon CloudWatch — 允许将指标发布到AWS/TransformCustom命名空间 CloudWatch 下。这样可以监控 CloudWatch 仪表板中的转换计数、延迟和状态代码。
- Amazon CloudWatch Logs-允许创建日志组、日志流、设置保留策略以及将日志事件发布到/aws/TransformCustom日志组。这样可以查看转换过程中遇到的问题。

AWS 托管策略： AWSTransformApplicationDeploymentPolicy

此策略允许 Tr AWS ansform 通过创建和管理 Amazon EC2 实例、 CloudFormation 堆栈和相关资源来部署转换后的.NET 应用程序。

描述

该策略包含以下权限：

- CloudFormation— 允许创建、更新、删除和描述名称以 aw CloudFormation stRansForm 开头的堆栈。堆栈操作仅限于标有 CreatedBy:awstRansForm 的资源，并且仅限于同一账户。 AWS
- Amazon EC2 — 允许描述 VPC、子网、安全组、映像、实例、路由表和互联网网关。允许运行、启动、停止、终止和修改 EC2 实例，但仅在通过 CloudFormation调用时才允许。标签创建仅限于允许的特定标签密钥，并且只能在 CloudFormation 操作期间创建。
- AWS Identity and Access Management (IAM) — 允许获取和传递 awstRansForm 部署实例的特定 IAM 角色。包括检查角色策略和附件的权限。访问权限仅限于同一个 AWS 账户。
- Amazon EC2 Systems Manager (SSM) — 允许从 AWS托管参数存储中检索 Amazon Linux AMI 参数并向实例发送命令。 AWSTransform-tagged
- Amazon S3 — 允许管理 awstRansForm 部署存储桶中的对象，包括列出存储桶和获取同一账户内的存储桶位置。 AWS

- AWS Key Management Service (KMS) — 允许使用标记为 awstRansForm 的 KMS 密钥进行加密和解密操作，但对 S3 和 EC2 服务的使用有限制。

该策略通过资源级权限、基于标签的条件、使用服务控制限制、账户级限制和显式拒绝声明来实现最低权限访问aws:CalledVia，以防止在操作之外进行未经授权的标签修改。 CloudFormation

权限详细信息

要查看策略权限的详细信息，请参阅AWSTransformApplicationDeploymentPolicy《 AWS 托管策略参考指南》。

AWS 托管策略： AWSTransformApplicationECSDeploymentPolicy

此策略允许 T AWS ransform 通过创建和管理 ECS 集群、服务、任务和关联资源，将转换后的应用程序部署到 Amazon ECS。

描述

该策略包含以下权限：

- CloudFormation— 允许创建、更新、删除和描述名称以 aw CloudFormation stRansForm 开头的堆栈。堆栈操作仅限于标有 CreatedBy:awstRansForm 的资源，并且仅限于同一账户。 AWS
- Amazon ECS — 允许创建、更新和删除 ECS 集群、服务和任务定义。允许运行任务、列出任务和描述任务状态。所有操作都仅限于名称以 awstRansForm 开头并标记为:awstRansForm 的 CreatedBy资源。
- AWS Identity and Access Management (IAM) — 允许获取和传递用于 ECS 任务的特定 IAM 角色（ AWSTransform-Deploy-ECS-Task-Role 和 AWSTransform-Deploy-ECS-Execution-Role ）。包括检查角色策略和在需要时创建 ECS 服务相关角色的权限。
- Amazon CloudWatch 日志 — 允许创建、删除和管理名称以 aws/ecs //awstransForm 开头的日志组。允许检索日志事件，以便对已部署的应用程序进行故障排除。
- Amazon ECR — 允许创建名称以 awstransform 开头的容器存储库，用于存储应用程序容器映像。
- AWS Key Management Service (KMS)-允许在使用客户管理的 KMS 密钥时为 ECR 加密创建授权和生成数据密钥。

该策略通过资源级权限、基于标签的条件和账户级别的限制来实现最低权限访问权限，以确保操作仅限于同一账户内的资源。 AWSTransform-managed AWS

权限详细信息

要查看策略权限的详细信息，请参阅AWSTransformApplicationECSDeploymentPolicy《 AWS 托管策略参考指南》。

AWS 托管策略： AWSTransformCustomFullAccess

此策略提供对 Trans AWS form 自定义的完全访问权限。

描述

该策略包含以下权限：

- AWS 转换自定义-允许对所有 AWS 转换自定义资源执行所有操作。这提供了对该服务的完全管理访问权限。
- AWS Identity and Access Management (IAM) — 允许创建 AWS 转换自定义服务相关角色 (`AWSServiceRoleForAWSTransformCustom`)。Transform c AWS ustom 需要此角色才能向您的账户发送 CloudWatch 指标和日志。权限的范围限定为仅允许创建此特定的服务相关角色。

权限详细信息

要查看策略权限的详细信息，请参阅AWSTransformCustomFullAccess《 AWS 托管策略参考指南》。

AWS 托管策略： AWSTransformCustomExecuteTransformations

此策略提供在自定义转换中执行 AWS 转换的权限。

描述

该策略包含以下权限：

- AWS 自定义转换-允许直播对话、执行转换和管理活动。包括获取活动详情、更新活动存储库状态和更新广告系列的权限。
- AWS Identity and Access Management (IAM) — 允许创建 AWS 转换自定义服务相关角色 (`AWSServiceRoleForAWSTransformCustom`)。Transform c AWS ustom 需要此角色才能向您的账户发送 CloudWatch 指标和日志。权限的范围限定为仅允许创建此特定的服务相关角色。

权限详细信息

要查看策略权限的详细信息，请参阅AWSTransformCustomExecuteTransformations《 AWS 托管策略参考指南》。

AWS 托管策略： AWSTransformCustomManageTransformations

此策略提供在自定义 AWS 转换中创建、更新、读取和删除转换资源以及执行转换的权限。

描述

该策略包含以下权限：

- AWS T@@ ransform Custom — 允许全面管理转换资源，包括直播对话、执行转换和管理转换包。允许创建、获取和删除转换包 URL 以及完成包上传。
- 知识管理-允许列出、获取、删除和更新知识项目及其配置和状态。
- 广告活动管理-允许获取活动详情、更新活动存储库状态和更新广告活动。
- 资源标记-允许列出、添加和移除 AWS 转换自定义资源的标签。
- AWS Identity and Access Management (IAM) — 允许创建 AWS 转换自定义服务相关角色 (`AWSServiceRoleForAWSTransformCustom`)。Transform c AWS ustom 需要此角色才能向您的账户发送 CloudWatch 指标和日志。权限的范围限定为仅允许创建此特定的服务相关角色。

权限详细信息

要查看策略权限的详细信息，请参阅AWSTransformCustomManageTransformations《 AWS 托管策略参考指南》。

AWS 托管策略： AWSTransformInfrastructureExecutorAccessBatch

此策略授予使用 B AWS atch 执行 AWS 转型持续现代化评估和转换所需的权限。将此策略附加到您账户中的 IAM 角色。Trans AWS form 持续现代化 CLI 和代理扮演此角色来上传源代码、检索结果、监控 Batch 作业状态、读取日志和管理转换计划。

描述

该策略包含以下权限：

- AWS Lambda — 允许调用和检索编排转换工作流程的带前缀的 `atx` Lambda 函数的配置。
- Amazon S3 — 允许将源代码上传到`atx-source-code-*`存储桶以及从`atx-custom-output-*`和`atx-ct-output-*`存储桶下载转换结果。
- AWS Key Management Service (KMS)-允许使用 AWS 转换加密密钥 (`alias/atx-encryption-key`) 对数据进行加密和解密。

- Amazon CloudWatch 日志 — 允许读取 Batch 作业和 Lambda 执行日志事件，以进行转换监控和调试。
- Amazon CloudWatch — 允许获取和列出 Trans AWS form CLI 控制面板以实现运营可见性。
- AWS Batch — 允许描述和列出计算环境、作业队列、作业定义和作业状态。
- CloudFormation— 允许描述和列出 T AWS ransform 基础架构堆栈以检查部署状态。
- R@@ esource Groups Tagging API — 允许检索已标记的资源以发现账户中的 Trans AWS form 基础架构。
- AWS Secrets Manager— 允许检索和描述存储在`atx/`前缀下的 Transf AWS orm 密钥。
- Amazon EventBridge 计划程序-允许管理计划组内的`atx-ct`计划转换任务。
- Amazon EC2 — 允许描述 Batch 计算环境联网的 VPC、子网、安全组、路由表和 NAT 网关配置。
- AWS Identity and Access Management (IAM) — 允许读取`ATX`前缀和`Atx`前缀的角色配置以验证基础设施设置，并将该配置传递给 `AtxSchedulerInvocationRole` Amazon S EventBridge cheduler，以便它可以调用计划任务。

该策略通过资源级权限、基于标签的条件、条件和服务范围`iam:PassedToService`的条件实现最低权限访问权限，以确保操作仅限于 AWS 同一账户内的转换资源。`aws:ResourceAccount` AWS

权限详细信息

要查看策略权限的详细信息，请参阅AWSTransformInfrastructureExecutorAccessBatch《 AWS 托管策略参考指南》。

AWS 托管策略： AWSTransformInfrastructureExecutorAccessEC2

该策略授予使用 Amazon EC2 执行 AWS 转型持续现代化评估和转型所需的权限。将此策略附加到您账户中的 IAM 角色。 AWS 转型持续现代化 CLI 和代理将扮演此角色来上传源代码、检索结果、监控作业状态和管理转换计划。

描述

该策略包含以下权限：

- CloudFormation— 允许描述 AWS 转换基础架构堆栈、堆栈事件、堆栈资源和偏差检测状态，列出堆栈，并在部署前验证 CloudFormation 模板。
- Amazon EC2 — 允许描述实例、AMI、VPC、子网、安全组、密钥对、路由表、NAT 网关和互联网网关。允许启动和停止标记为的 EC2 实例`atx-remote-infra: true`。

- Amazon EC2 Systems Manager (SSM) — 允许监控命令执行状态，并在 AWS Transform-tagged 实例上运行命令和会话，包括运行AWS-RunShellScript文档。
- Amazon S3 — 允许在 Tr AWS ansform 存储桶中管理源代码和输出项目，包括获取、放置和删除对象以及列出存储桶。
- AWS Key Management Service (KMS)-允许使用 AWS 转换加密密钥 (alias/atx-encryption-key) 对数据进行加密和解密。
- AWS Secrets Manager— 允许检索和描述存储在atx/前缀下的转换密钥，例如存储库凭据。
- Amazon EventBridge 计划程序-允许管理计划组内的atx-ct计划转换任务。
- R@@ esource Groups Tagging API — 允许检索已标记的资源以发现账户中的 Trans AWS form 基础架构。
- AWS Identity and Access Management (IAM) — 允许将atx-transform-role*角色传递给 Amazon EC2，将角色传递AtxSchedulerInvocationRole给 Amazon S EventBridge cheduler，以及读取 EC2 实例的角色和实例配置文件配置。

该策略通过资源级权限、基于标签的条件、条件和服务范围iam:PassedToService的条件实现最低权限访问权限，以确保操作仅限于 AWS 同一账户内的转换资源。aws:ResourceAccount AWS

权限详细信息

要查看策略权限的详细信息，请参阅AWSTransformInfrastructureExecutorAccessEC2《AWS 托管策略参考指南》。

AWS 托管策略： AWSTransformSecurityAgentExecutorAccess

此策略授予 T AWS ransform Continuation Moderiation 调用 AWS 安全代理服务以进行自动代码安全审查和修复所需的权限。将此策略附加到您账户中的 IAM 角色，Trans AWS form 持续现代化 CLI 和代理假设该角色用于上传扫描项目和检索结果。

描述

该策略包含以下权限：

- AWS 安全代理-允许列出代理空间、创建代码审查、启动代码审查作业、列出和检索发现结果以及启动代码修复。这些操作的范围仅限于您账户中的代理空间。
- Amazon S3 — 允许从kct-security-agent-*存储桶下载扫描结果和发现，并允许将用于安全扫描的源代码上传到该存储桶内的security-scans/*前缀。

- AWS Identity and Access Management (IAM)-允许将`security-agent-*`角色传递给 AWS 安全代理服务，使其可以执行扫描。

该策略通过资源级权限、S3 存储桶和密钥前缀、和条件以及服务范围`s3:ResourceAccount`和`iam:PassedToService`条件实现最低权限访问，以确保操作仅限于同一账户中的 AWS 安全代理资源。`aws:ResourceAccount` AWS

权限详细信息

要查看策略权限的详细信息，请参阅AWSTransformSecurityAgentExecutorAccess《 AWS 托管策略参考指南》。

AWS 托管策略： DBModDiscoveryAndAssessment

该策略为 T AWS ransform 提供了全面的数据库现代化发现和评估功能。

描述

该策略包含以下权限：

- Amazon EC2 — 允许描述基础设施组件，包括实例、VPC、子网、安全组、可用区、VPC 终端节点和互联网网关。
- Amazon RDS — 允许描述数据库实例、集群和子网组。允许修改同一 AWS 账户内的数据库子网组，以便为迁移做准备。
- Amazon RDS 数据 API — 允许启用和禁用 HTTP 终端节点，以及在标记为数据库现代化项目的数据库集群上执行 SQL 语句。
- AWS DMS— 允许描述终端节点、复制实例、任务、子网组和可订购实例。允许列出数据提供者、实例配置文件和迁移项目。允许描述表统计信息、评估运行和元数据模型操作。详细描述和元数据操作仅限于为数据库现代化项目标记的资源。
- — 允许列出用于发现数据库凭据的机密。
- AWS Identity and Access Management (IAM) — 允许检查特定的 AWS DMS 服务角色及其附加的策略。包括对读取 AWS托管 AWS DMS 策略的访问权限。
- AWS Key Management Service (KMS)-允许列出密钥别名和描述密钥。允许通过集成解密机密，仅限于同一 AWS 帐户。

该策略通过资源级权限、基于标签的条件和账户级限制实现最低权限访问权限，以确保操作仅限于同一账户内的数据库现代化项目资源。 AWS

权限详细信息

要查看策略权限的详细信息，请参阅DBModDiscoveryAndAssessment《 AWS 托管策略参考指南》。

AWS 托管策略： DBModProvisioningAndMigration

该策略为 T AWS ransform 数据库现代化项目提供数据库配置和迁移功能。它包括创建和管理迁移基础架构、配置目标数据库和存储迁移数据的权限。

描述

该策略包含以下权限：

- AWS DMS— 允许创建和管理复制子网组、实例配置文件、数据提供程序、迁移项目、端点、复制实例和复制任务。包括架构转换操作，例如元数据模型导入、转换、导出和评估。允许对复制实例（创建、删除、修改、重启）和复制任务（删除、启动、停止、评估）进行生命周期管理。所有写入操作仅限于为数据库现代化项目标记的资源。
- Amazon RDS — 允许创建数据库子网组、数据库集群和数据库实例。必须为数据库现代化项目的所有资源添加标签。
- — 允许使用数据库现代化命名前缀创建、更新和标记密钥。允许检索密钥值并描述已标记资源的密钥。
- Amazon S3 — 允许创建和管理 S3 存储桶和用于迁移数据存储的对象。包括存储桶标记、版本控制和对象生命周期操作。仅限于带有数据库现代化命名前缀的存储桶。
- AWS Identity and Access Management (IAM)-允许将特定的 AWS DMS 服务角色传递给 AWS DMS 架构转换服务。允许创建数据库操作所需的 Amazon RDS 服务相关角色。

该策略通过资源级权限、基于标签的条件和账户级限制实现最低权限访问权限，以确保操作仅限于同一账户内的数据库现代化项目资源。 AWS

权限详细信息

要查看策略权限的详细信息，请参阅DBModProvisioningAndMigration《 AWS 托管策略参考指南》。

AWS 转换权限参考

本节提供有关 Trans AWS form 使用的 API 及其用途的信息。

主题

- AWS 转换 API

AWS 转换 API

- 转换：BatchGetMessage
- 转换：BatchGetUserDetails
- 转换：CompleteArtifactUpload
- 转换：CreateArtifactDownloadUrl
- 转换：CreateArtifactUploadUrl
- 转换：CreateAssetDownloadUrl
- 转换：CreateConnector
- 转换：CreateFeedback
- 转换：CreateJob
- 转换：CreateSession
- 转换：CreateWorkspace
- 转换：DeleteConnector
- 转换：DeleteJob
- 转换：DeleteSelfRoleMappings
- 转换：DeleteUserRoleMappings
- 转换：DeleteWorkspace
- 转换：DetectIsAllowedForOperation
- 转换：GetConnector
- 转换：GetFeedbackQuestions
- 转换：GetHitlTask
- 转换：GetJob
- 转换：GetLoginRedirectUri
- 转换：GetUserDetails
- 转换：GetUserPreferences
- 转换：GetWebAppUrl
- 转换：GetWorkspace
- 转换：ListArtifacts

- 转换：ListConnectors
- 转换：ListHitlTasks
- 转换：ListJobPlanSteps
- 转换：ListJobs
- 转换：ListMessages
- 转换：ListPlanUpdates
- 转换：ListUserRoleMappings
- 转换：ListWorklogs
- 转换：ListWorkspaces
- 转换：PutUserPreferences
- 转换：PutUserRoleMappings
- 转换：RevokeSession
- 转换：SearchUsers
- 转换：SearchUsersTypeahead
- 转换：SendMessage
- 转换：StartJob
- 转换：StopJob
- 转换：SubmitCriticalHitlTask
- 转换：SubmitStandardHitlTask
- 转换：TestReleaseTraitPreProd
- 转换：TestReleaseTraitProd
- 转换：UpdateHitlTask
- 转换：UpdateJob
- 转换：UpdateWorkspace
- 转换：VerifySession

的合规性验证 AWS 转换

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。有关您在使用时的合规责任的更多信息 AWS 服务，请参阅AWS 安全文档。

韧性在 AWS 转换

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理分隔和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础架构外，Tr AWS ansform 还提供多项功能来帮助支持您的数据弹性和备份需求。

AWS Transform 和接口端点 (AWS PrivateLink)

您可以通过创建接口 VPC 终端节点在您 AWS Transform 的 VPC 和之间建立私有连接。接口端点由一项技术提供支持 AWS PrivateLink，该技术使您无需互联网网关、NAT 设备、VPN 连接或 Direct Connect 连接即可私密访问 AWS Transform 控制台。您的 VPC 和 VPC 之间的流量 AWS Transform 不会离开 Amazon 网络。

每个接口端点均由子网中的一个或多个弹性网络接口表示。

有关更多信息，请参阅《Amazon VPC 用户指南》中的接口 VPC 端点 (AWS PrivateLink)。

> **Note**
>
> 有关 AWS Transform 自定义 PrivateLink 文档，请参阅AWS Transform 自定义端点和接口端点 (AWS PrivateLink)。

的注意事项 AWS Transform VPC 端点

在为设置接口 VPC 终端节点之前 AWS Transform，请务必查看 Amazon VPC 用户指南中的接口终端节点属性和限制。

先决条件

在您开始下面的任何流程之前，请确保您满足以下条件：

- 具有创建和配置资源的适当权限的 AWS 账户。
- 已在您的 AWS 账户中创建了 VPC。
- 熟悉 AWS 服务，尤其是 Amazon VPC 和。 AWS Transform

为创建接口 VPC 终端节点 AWS Transform

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为 AWS Transform 服务创建 VPC 终端节点。有关更多信息，请参阅《Amazon VPC User Guide》中的 Creating an interface endpoint。

AWS Transform 支持以下 VPC 终端节点服务：

服务名称	端点	备注
控制面板	com.amazonaws. *region*.transform	
代理 API	com.amazonaws. *region*.transform-agents	
Web 应用程序	com.amazonaws. *region*.api.transform	对于 AWS Transform Web 应用程序来说是必需的。此终端节点必须启用私有 DNS（启用 DNS 名称选项），这样才能api.transform. *region*.on.aws解析到您的 VPC 中的私有 IP 地址。

*region*替换为安装您的 AWS Transform 个人资料的 AWS 区域，例如 com.amazonaws. us-east-1.transform。

> **Note**
>
> 如果您使用 AWS Transform Web 应用程序，则需要`api.transform`端点。有关完整的设置指南，请参阅访问 AWS Transform 来自 VPC 的 Web 应用程序。

有关更多信息，请参阅 支持的区域 AWS Transform Amazon VPC 用户指南中的通过接口终端节点访问服务。

使用本地计算机连接到 AWS Transform 端点

本节介绍使用本地计算机 AWS Transform 通过 AWS VPC 中的 AWS PrivateLink 终端节点进行连接的过程。

1. 在本地设备和 VPC 之间创建 VPN 连接。
2. 为创建接口 VPC 终端节点 AWS Transform。
3. 设置入站 Amazon Route 53 端点。这将使您能够在本地设备上使用 AWS Transform 终端节点的 DNS 名称。

访问 AWS Transform 来自 VPC 的 Web 应用程序

当您使用 AWS PrivateLink 从 VPC 私下访问 AWS Transform API 时，Web 应用程序需要额外的网络配置。它通过提供静态内容（HTML JavaScript、、CSS）CloudFront，这需要互联网连接。来自 Web 应用程序的 API 调用将通过您的 VPC 终端节点进行并保持完全私密状态。

本指南向您介绍如何配置来自您的 VPC 的受控互联网出口，这样 Web 应用程序就可以加载，同时将 VPC 锁定到所需的域。

工作原理

AWS Transform Web 应用程序使用两条网络路径：

- API 调用 — 当您与 Web 应用程序交互（启动作业、查看工作区等）时，浏览器会向发送 API 请求。`api.transform.`*`region`*`.on.aws`启用 `com.amazonaws.`*`region`*`.api.transform` VPC 终端节点和私有 DNS 后，这些请求将解析到您的 VPC 中的私有 IP 地址，并且永远不会离开 AWS 网络。

- 静态内容 — CloudFront 通过提供 Web 应用程序的 HTML 和 CSS 文件*tenant-id*.transform.*region*.on.aws。 JavaScript加载这些文件需要互联网连接，因为 CloudFront 内容交付只能通过公共互联网进行。
- 身份验证 — AWS IAM Identity Center 登录流程使用*region*.signin.aws，这也需要互联网连接。

要在维护安全的同时启用 Web 应用程序，您可以使用带有基于域的筛选的 Network Fire AWS wall 创建受控的出口路径。这允许您的 VPC 仅访问 Web 应用程序所需的特定域，同时阻止所有其他互联网流量。

架构

下图显示了 Web 应用程序流量的网络路径：

```
EC2 Instance / Workspace (Private Subnet)
    |
    | Route: 0.0.0.0/0 # Network Firewall Endpoint
    v
AWS Network Firewall (Firewall Subnet)
    | Allows: *.cloudfront.net, *.transform.<region>.on.aws,
    |         <region>.signin.aws, SSO domains, S3 presigned URLs
    | Blocks: everything else (TLS SNI inspection)
    |
    | Route: 0.0.0.0/0 # NAT Gateway
    v
NAT Gateway (Public Subnet)
    |
    | Route: 0.0.0.0/0 # Internet Gateway
    v
Internet Gateway # CloudFront Edge Locations
```

> **Important**
>
> Network Firewall 必须看到流量的两个方向（对称路由）才能执行 TLS SNI 检查。您必须在 NAT Gateway 子网中配置一条返回路由，以便通过防火墙将发往私有子网的流量发送回去。否则，基于域的过滤规则将无法运行。

先决条件

在开始之前，请确保您满足以下条件：

- 有权创建 VPC 资源、Network Firewall 和 NAT 网关的 AWS 账户。
- 带有私有子网的 VPC，您的实例或工作负载可以在其中运行。
- 连接到 VPC 的互联网网关（或创建网关的权限）。
- 启用了 AWS Transform 私有 DNS 的 `com.amazonaws.region.api.transform` VPC 终端节点。这是 Web 应用程序浏览器客户端使用的端点。有关创建端点的说明，请参阅AWS Transform 和接口端点 (AWS PrivateLink)。

配置 VPC 终端节点策略

如果您的 `com.amazonaws.region.api.transform` VPC 终端节点具有自定义终端节点策略，则必须添加允许 AWS Transform 操作的声明。否则，Web 应用程序将无法通过端点进行 API 调用。

将以下声明添加到您的 VPC 终端节点策略中。*AWS_TRANSFORM_PROFILE_ARN*替换为您的 AWS Transform 服务配置文件 ARN，您可以在 AWS Transform 控制台的 “设置” 页面上找到该配置文件。

```
{
    "Statement": [
        {
            "Sid": "AllowAWSTransform",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalArn": [
                        "AWS_TRANSFORM_PROFILE_ARN"
                    ]
                }
            }
        }
    ]
}
```

> **Note**
>
> 如果您的 VPC 终端节点使用默认策略（完全访问权限），则无需进行任何更改，您可以跳过此步骤。

设置受控的互联网出口

完成以下步骤，为 AWS Transform Web 应用程序配置 Network Firewall 使用基于域的筛选。

步骤 1：创建防火墙子网

创建一个专用 Network Firewall 端点的小型 /28 子网。该子网必须与您的私有子网位于同一个可用区。

```
aws ec2 create-subnet \
  --vpc-id your-vpc-id \
  --cidr-block firewall-subnet-cidr \
  --availability-zone your-az \
  --region region
```

步骤 2：为 NAT 网关创建公有子网

```
aws ec2 create-subnet \
  --vpc-id your-vpc-id \
  --cidr-block public-subnet-cidr \
  --availability-zone your-az \
  --region region
```

步骤 3：配置公有子网路由表

为将互联网流量路由到互联网网关的公有子网创建路由表。

```
# Create route table
PUB_RTB=$(aws ec2 create-route-table \
  --vpc-id your-vpc-id \
```

```
  --region region \
  --query 'RouteTable.RouteTableId' --output text)

# Add default route to internet gateway
aws ec2 create-route \
  --route-table-id $PUB_RTB \
  --destination-cidr-block 0.0.0.0/0 \
  --gateway-id your-igw-id \
  --region region

# Associate with public subnet
aws ec2 associate-route-table \
  --route-table-id $PUB_RTB \
  --subnet-id public-subnet-id \
  --region region
```

步骤 4：创建 NAT 网关

```
# Allocate an Elastic IP
EIP=$(aws ec2 allocate-address --domain vpc \
  --region region --query 'AllocationId' --output text)

# Create NAT Gateway in the public subnet
NAT_ID=$(aws ec2 create-nat-gateway \
  --subnet-id public-subnet-id \
  --allocation-id $EIP \
  --region region \
  --query 'NatGateway.NatGatewayId' --output text)

# Wait for NAT Gateway to become available (~2 minutes)
aws ec2 wait nat-gateway-available \
  --nat-gateway-ids $NAT_ID --region region
```

步骤 5：创建 Network Firewall 规则组

创建一个状态规则组，该组仅允许流向 AWS Transform Web 应用程序所需的域的流量。

```
aws network-firewall create-rule-group \
```

```
  --rule-group-name transform-webapp-domains \
  --type STATEFUL \
  --capacity 100 \
  --rule-group '{
    "StatefulRuleOptions": {
      "RuleOrder": "STRICT_ORDER"
    },
    "RulesSource": {
      "RulesSourceList": {
        "Targets": [
          ".cloudfront.net",
          ".transform.region.on.aws",
          "region.signin.aws",
          ".s3.region.amazonaws.com",
          "oidc.region.amazonaws.com",
          "portal.sso.region.amazonaws.com",
          "assets.sso-portal.region.amazonaws.com",
          "directory-id.awsapps.com"
        ],
        "TargetTypes": ["TLS_SNI", "HTTP_HOST"],
        "GeneratedRulesType": "ALLOWLIST"
      }
    }
  }' \
  --region region
```

*region*替换为安装您的 AWS Transform 配置文件的地 AWS 区（例如，us-east-1）。*directory-id*替换为您的 IAM 身份中心目录 ID（例如，d-1234567890）。您可以在 IAM 身份中心控制台中找到您的目录 ID。

下表说明了允许的域。

域：	用途
.cloudfront.net	CloudFront CDN — 提供 Web 应用程序静态资产（JavaScript、CSS、图像）
.transform. *region*.on.aws	Web 应用程序租户 URL — 浏览器通过以下方式从该域加载初始页面 CloudFront
region.signin.aws	SSO 登录重定向页面

域：	用途
.s3.*region*.amazonaws.com	S3 预签名 URL-工件上传和下载
oidc.*region*.amazonaws.com	用于 SSO 身份验证的 OIDC 令牌交换
portal.sso. *region*.amazonaws.com	SSO 门户登录页面
assets.sso-portal. *region*.amazonaws.com	SSO 门户网站静态资产 (CSS、 JavaScript)
directory-id .awsapps.com	适用于您的组织的 IAM 身份中心门户

> **Note**
>
> .cloudfront.net通配符允许任何 CloudFront分发的流量，而不仅仅是 AWS Transform Web 应用程序的流量。不可能使用更窄的域过滤器，因为 CloudFront 边缘 IP 是跨分布共享的，而且 TLS SNI 检查无法区分同一域下的各个分布。

> **Note**
>
> API 调用api.transform.*region*.on.aws可以通过 AWS PrivateLink ，不需要互联网出口。它们不受防火墙的影响。

步骤 6：创建防火墙策略

策略必须使用STRICT_ORDER规则评估drop_established作为默认操作。这样可以确保丢弃所有与许可名单不匹配的流量。

```
# Get the rule group ARN
RG_ARN=$(aws network-firewall describe-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL --region region \
  --query 'RuleGroupResponse.RuleGroupArn' --output text)
```

```
# Create the firewall policy
aws network-firewall create-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --firewall-policy "{
    \"StatelessDefaultActions\": [\"aws:forward_to_sfe\"],
    \"StatelessFragmentDefaultActions\": [\"aws:forward_to_sfe\"],
    \"StatefulRuleGroupReferences\": [
      {
        \"ResourceArn\": \"$RG_ARN\",
        \"Priority\": 1
      }
    ],
    \"StatefulEngineOptions\": {
      \"RuleOrder\": \"STRICT_ORDER\"
    },
    \"StatefulDefaultActions\": [\"aws:drop_established\", \"aws:alert_established\"]
  }" \
  --region region
```

步骤 7：创建 Network Firewall

```
# Get the policy ARN
FW_POLICY_ARN=$(aws network-firewall describe-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --region region \
  --query 'FirewallPolicyResponse.FirewallPolicyArn' --output text)

# Create the firewall
aws network-firewall create-firewall \
  --firewall-name transform-webapp-firewall \
  --firewall-policy-arn $FW_POLICY_ARN \
  --vpc-id your-vpc-id \
  --subnet-mappings SubnetId=firewall-subnet-id \
  --region region

# Wait for the firewall to become READY (3-5 minutes)
while true; do
  STATUS=$(aws network-firewall describe-firewall \
    --firewall-name transform-webapp-firewall \
    --region region \
    --query 'FirewallStatus.Status' --output text)
```

```
  echo "Status: $STATUS"
  if [ "$STATUS" = "READY" ]; then break; fi
  sleep 15
done
```

步骤 8：获取防火墙端点 ID

```
FW_ENDPOINT=$(aws network-firewall describe-firewall \
  --firewall-name transform-webapp-firewall \
  --region region \
  --query "FirewallStatus.SyncStates.\"your-az\".Attachment.EndpointId" \
  --output text)
echo "Firewall endpoint: $FW_ENDPOINT"
```

步骤 9：配置防火墙子网路由表

将互联网流量从防火墙子网路由到 NAT 网关。

```
FW_RTB=$(aws ec2 create-route-table \
  --vpc-id your-vpc-id \
  --region region \
  --query 'RouteTable.RouteTableId' --output text)

aws ec2 create-route \
  --route-table-id $FW_RTB \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id $NAT_ID \
  --region region

aws ec2 associate-route-table \
  --route-table-id $FW_RTB \
  --subnet-id firewall-subnet-id \
  --region region
```

步骤 10：更新私有子网路由表

将来自私有子网的所有互联网流量路由到防火墙。

```
aws ec2 create-route \
  --route-table-id private-subnet-route-table-id \
  --destination-cidr-block 0.0.0.0/0 \
  --vpc-endpoint-id $FW_ENDPOINT \
  --region region
```

如果已存在默认路由，请使用`replace-route`而不是`create-route`。

步骤 11：添加对称回程路由（必填）

> **Important**
>
> 这一步至关重要。Network Firewall 使用 TLS SNI 检查，并且必须看到 TCP 连接的两个方向。在 NAT Gateway 子网的路由表中添加一条路由，该路由将发往私有子网的返回流量通过防火墙发送回去。

```
aws ec2 create-route \
  --route-table-id $PUB_RTB \
  --destination-cidr-block private-subnet-cidr \
  --vpc-endpoint-id $FW_ENDPOINT \
  --region region
```

*`private-subnet-cidr`*替换为私有子网的 CIDR 块（例如`10.0.144.0/20`）。

如果没有对称路由，防火墙只能看到一个方向的流量。TLS 检查引擎无法从 TLS 握手中提取服务器名称指示 (SNI)，并且所有基于域的规则都将静默失败。

步骤 12：删除 IPv6 默认路由（如果存在）

如果私有子网路由表有直接指向互联网网关的 IPv6 默认路由 (`::/0`)，它将绕过防火墙 IPv6-capable 前往目的地。将其删除：

```
aws ec2 delete-route \
```

```
  --route-table-id private-subnet-route-table-id \
  --destination-ipv6-cidr-block ::/0 \
  --region region
```

验证

在私有子网中的实例中，验证配置：

```
# Should SUCCEED - web application content via CloudFront (allowed)
curl -vL --connect-timeout 15 \
  'https://tenant-id.transform.region.on.aws'

# Should SUCCEED - API via PrivateLink (does not use firewall)
curl -v --connect-timeout 15 \
  'https://api.transform.region.on.aws/'

# Should FAIL - non-allowlisted domain (blocked by firewall)
curl -v --connect-timeout 15 'https://www.example.com'
# Expected: TLS connection error (firewall drops after SNI inspection)
```

问题排查

你的防火墙阻止了对 api.transform 的 API 调用

该域api.transform.*region*.on.aws应通过 VPC 终端节点解析为私有 IP 地址，并且不应到达您的互联网防火墙。

- 确认您已创建com.amazonaws.*region*.api.transform终端节点。
- 验证终端节点上是否启用了私有 DNS：

```
aws ec2 describe-vpc-endpoints \
  --filters "Name=service-name,Values=com.amazonaws.region.api.transform" \
  --query 'VpcEndpoints[*].[State,PrivateDnsEnabled]' \
  --output table
```

预期输出：`available | True`

Web 应用程序无法加载（连接超时）

- 验证私有子网路由表中是否有指向防火墙端点的`0.0.0.0/0`路由。
- 验证防火墙子网路由表中是否有指向 NAT 网关的`0.0.0.0/0`路由。
- 验证 NAT 网关是否处于`available`状态。

Non-allowlisted 域名未被屏蔽

- 检查是否有指向互联网网关的 IPv6 `::/0` 路由。这会绕过防火墙。将其删除（步骤 12）。
- 验证是否配置了对称路由。NAT 网关子网路由表必须有穿过防火墙的私有子网 CIDR 的返回路由（步骤 11）。
- 验证防火墙策略是否`STRICT_ORDER`使用`drop_established`和`alert_established`作为默认操作。

成本注意事项

资源	大概成本
Network Firewall	~0 美元。 395/hr 每个可用区 (~$288/month)
NAT 网关	~0 美元。 045/hr (~$33/month) + 数据处理费
弹性 IP（公有 IPv4）	~0 美元。 005/hr （大约 3 美元。 60/month)
Network Firewall 数据处理	0 美元。 065/GB
NAT 网关数据处理	0 美元。 045/GB

单个可用区部署325/month 的估计基本成本约为 $。对于生产部署，请在存在私有子网的每个可用区中部署防火墙、NAT 网关和关联子网。

资源清理

要删除本指南创建的所有资源，请按相反顺序运行以下命令。将占位符替换为部署中的资源 ID。您可以在 AWS 管理控制台中找到这些值，也可以使用设置步骤中的`describe`命令来找到。

```
# Remove return route from NAT Gateway subnet
aws ec2 delete-route --route-table-id pub-rtb-id \
```

```
  --destination-cidr-block private-subnet-cidr \
  --region region

# Remove route from private subnet
aws ec2 delete-route \
  --route-table-id private-subnet-route-table-id \
  --destination-cidr-block 0.0.0.0/0 --region region

# Delete Network Firewall (takes ~5 minutes)
aws network-firewall delete-firewall \
  --firewall-name transform-webapp-firewall \
  --region region

# Delete firewall policy and rule group
aws network-firewall delete-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --region region
aws network-firewall delete-rule-group \
  --rule-group-name transform-webapp-domains \
  --type STATEFUL --region region

# Delete NAT Gateway (wait ~5 minutes for full deletion)
aws ec2 delete-nat-gateway --nat-gateway-id nat-gateway-id \
  --region region

# Release Elastic IP
aws ec2 release-address --allocation-id eip-allocation-id \
  --region region

# Delete subnets
aws ec2 delete-subnet --subnet-id firewall-subnet-id \
  --region region
aws ec2 delete-subnet --subnet-id public-subnet-id \
  --region region
```

监控 AWS 转换

监控是维护 Trans AWS form 和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS 提供了以下监视工具，用于监视 Trans AWS form、报告出现问题并在适当时自动采取措施：

- Amazon 会实时 CloudWatch监控您的 AWS 资源和您运行 AWS 的应用程序。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon CloudWatch Logs 允许您监控、存储和访问来自 Amazon EC2 实例和其他来源的日志文件。 CloudTrail CloudWatch 日志可以监视日志文件中的信息，并在达到特定阈值时通知您。您还可以在高持久性存储中检索您的日志数据。有关更多信息，请参阅 Amazon CloudWatch 日志用户指南。
- Amazon EventBridge 可用于实现 AWS 服务自动化，并自动响应系统事件，例如应用程序可用性问题或资源更改。来自 AWS 服务的事件几乎实时 EventBridge 地传送到。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。
- AWS CloudTrail捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 AWS CloudTrail 用户指南。

日志记录 AWS 使用转换 API 调用 AWS CloudTrail

AWS Transform 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 Trans AWS form 中执行的操作的记录。 CloudTrail AWS 将转换的所有 API 调用捕获为事件。捕获的调用包括来自 AWS 转换控制台的调用和对 AWS 转换 API 操作的代码调用。如果您创建跟踪，则可以将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括用于 AWS 转换的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 T AWS ransform 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅AWS CloudTrail 用户指南。

AWS 转换信息 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 Trans AWS form 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录中的事件 AWS 账户，包括 AWS 变换的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 AWS 转换日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序出现。

通知

AWS Transform 提供电子邮件通知，让您随时了解工作空间访问权限的更改、工作状态更新和待处理的协作者请求。

电子邮件通知

默认情况下，电子邮件通知处于启用状态，并发送给对作业具有只读或更高权限的用户。用户可以修改其通知首选项。电子邮件通知分为三类：

- 工作区访问权限更新

  当您被添加到新工作区时，以及在工作空间中更改角色时，您会收到通知。

- 每日摘要电子邮件

  太平洋时间上午 9:00，您会收到一封摘要电子邮件，其中汇总了您正在进行的工作，前提是一份或多份空缺的合作者申请。该电子邮件包含一个表格，显示工作空间名称、工作名称、工作状态、协作者请求详情和所需操作（限于 10 行）

  > **Note**
  >
  > 只有需要合作者请求的工作才会发送每日摘要电子邮件。可选的合作者请求不会触发摘要电子邮件。

- Job 状态更新

  当你有权访问的任务完成或失败时，你会收到一封电子邮件。

- 合作者请求更新

  每当任务需要您输入、审阅或批准时，您都会收到一封电子邮件。

管理电子邮件通知

您可以在 Web 应用程序中修改电子邮件通知首选项，方法是单击应用程序右上角的 “设置” 齿轮，然后选择 “通知设置”。

通知设置页面提供以下控件：

通知类型	说明	默认设置
工作区访问权限更新	添加到工作区或在工作空间中更改角色时接收电子邮件	已启用

通知类型	说明	默认设置
每日合作者请求摘要	每天收到一份摘要，了解合作者在无障碍工作空间中提出的职位空缺申请	已启用
Job 完成更新	任务完成或失败时接收电子邮件	已启用
合作者请求更新	在需要您输入或批准时接收电子邮件	已禁用

您可以使用常规设置来启用或禁用所有通知，也可以单独配置各个通知类型。

的配额 AWS 转换

您的 AWS 账户对每项 AWS 服务都有默认配额（以前称为限制）。除非另有说明，否则每个配额都是 Region-specific。您可以请求增加某些配额，但其他一些配额无法增加。

要查看 Trans AWS form 的配额，请打开 S ervice Quotas 控制台。在导航窗格中，选择AWS 服务，然后选择AWS 转换。

要请求提高配额，请参阅《Service Quotas 用户指南》中的请求提高配额。如果配额在 Service Quotas 中尚不可用，请使用提高限额表格。

您的 AWS 账户具有以下与 Trans AWS form 相关的配额。

工作负载	维度	配额	可调整	说明
平台	每个已启用的账户的 AWS 区域 每个 AWS Transform工作空间	每个支持的 100 个工作空间 AWS 区域	是	每个 AWS Transform启用账户的最大工作空间数量 AWS 区域
VMware	每波的服务器数量	每波：150 台服务器	否	一波中服务器的最大数量
大型机	每个 IAM 身份中心账户的并发任务	每个支持的地区有 10 个职位	是	IAM Identity Center 账户中的并发大型机作业的最大数量
	每项作业的代码行	每个支持的区域有 300 万行代码	否	每个作业的最大代码行数。
	分析每月的代码行	每个支持的区域有 1 亿行代码	是	一个日历月内 Analyze Code 作业目标的最大代码行数

工作负载	维度	配额	可调整	说明
	每月生成业务文档代码行	每个支持的区域有 50,000,000 行代码	是	一个日历月内 Business Documentation Generation 作业目标的最大代码行数
	每月生成技术文档代码行	每个支持的区域有 50,000,000 行代码	是	一个日历月内 Technical Documentation Generation 作业目标的最大代码行数
	转换代码行	每个支持的区域有 1000 万行代码	是	一个日历月内转换的最大代码行数
	分解每月的代码行数	每个支持的区域有 50,000,000 行代码	是	一个日历月内 Decomposition 作业目标的最大代码行数
	重塑每月的代码行	每个支持的区域有 50,000,000 行代码	是	一个日历月内 Reforge 作业目标的最大代码行数
	提取的业务逻辑每月代码行	每个支持的区域有 50,000,000 行代码	是	一个日历月内提取的 Business Logic 作业目标的最大代码行数

工作负载	维度	配额	可调整	说明
.NET	.NET 每月代码行（Web 和 IDE）	每个支持的区域有 1,000,000 行代码	是	在 IAM Identity Center 账户支持的每个账户中，在一个日历月内可以转换 AWS 区域 的.NET 应用程序代码的最大行数
	每个 IAM 身份中心账户使用微软 Visual Studio 扩展程序并发.NET 作业	每个支持的地区有 10 个职位	是	使用 Microsoft Visual Studio 扩展程序时，IAM 身份中心账户支持的 AWS 区域 每个账户中支持的最大并发.NET 转换作业数。
	每个 IAM 身份中心账户的并发 .NET 网络作业	每个支持的地区有 5 个职位	是	使用 Transfor AWS m Web 应用程序时，IAM Identity Center 账户支持的 AWS 区域 每个账户中并发.NET 转换任务的最大数量。
自定义转换	自定义转换定义	1000	是	自定义转换定义的最大数量
	自定义转换定义大小	10 MB	否	转换定义中包含的所有文件（包括文档引用）的最大总大小。

工作负载	维度	配额	可调整	说明
	自定义转换每月 CLI 对话请求	1000000	是	一个日历月内允许在 CLI 中提出的自定义转换对话请求的最大数量
评测	每次评估的服务器数量限制	每次评估：30,000 台服务器	否	单次评估任务中服务器的最大数量

支持的区域 AWS Transform

> **Note**
>
> 如果您提出的请求 AWS Transform 需要从未在此页面上列出的可选区域检索信息，则 AWS Transform 可以拨打该区域的电话。要管理对 AWS Transform 可以拨打电话的区域的访问权限，请参阅中的安全性 AWS 转换。

本主题介绍可在 AWS 区域 何处使用 AWS Transform。有关更多信息 AWS 区域，请参阅AWS 账户管理 参考指南中的指定 AWS 区域 您的账户可以使用。

您的数据可能在与您使用的区域不同的区域进行处理 AWS Transform。有关中跨区域处理的信息 AWS Transform，请参阅Cross-region 处理。有关处理期间数据存储位置的信息，请参阅数据保护。

支持 AWS 区域（默认启用）

你可以在下面 AWS 区域创建 AWS Transform 工作区。默认情况下，这些区域处于启用状态，您无需在使用前将其启用。有关更多信息，请参阅默认启用的区域。

- 美国东部（弗吉尼亚州北部）
- 欧洲地区（法兰克福）
- 亚太地区（孟买）
- 亚太地区（悉尼）
- 亚太地区（东京）
- 欧洲地区（伦敦）
- 亚太地区（首尔）
- 加拿大（中部）
- 南美洲（圣保罗）-仅限大型机现代化代理

您在其中创建作业的工作空间决定了该作业 AWS 区域 的范围。要在其他区域创建作业，您必须使用所需区域内的其他工作空间。

对于 VMware 项目，使用工作空间的区域进行发现。但是，您可以指定其他区域作为迁移目标。该目标区域是迁移完成后您的工作负载所在的区域。有关 VMware 迁移 AWS 区域 注意事项的更多信息，包括可能的目标区域列表，请参阅the section called “支持的目标区域”。

AWS 支持 AWS Transform

AWS Transform 允许您在转换工作中遇到问题时通过聊天创建和管理 AWS Support 案例。您的案例会自动充实工作背景，并发送给相应的支持团队。如果您是 Countdown Premium 的活跃客户，您的指定工程师将与您联系以管理问题的解决方案。在AWS 倒计时高级版中了解更多信息。否则，您的问题将由支持团队在其 AWS Transform 支持队列中进行调查。

先决条件

在使用支持案例管理之前，您需要：

- 有效的 S AWS upport 计划-商业 On-Ramp、企业或企业
- 现有 AWS Transform 应用程序

启用 Support 案例管理

1. 打开控制 AWS Transform 台。
2. 在导航窗格中，选择设置。
3. 在 “支持” 下，选择 “启用支持案例管理”。
4. 选择保存更改。

AWS Transform 使用服务相关角色 (SLR) 代表您创建和管理支持案例。不需要其他 IAM 权限。

创建 Support 案例

要创建支持案例，请使用聊天界面：

1. 要求创建支持案例。例如：
    - “为我失败的转型工作创建支持案例”
    - “我需要帮助解决工作错误，创建案例”
2. 聊天会提示您输入所需信息：
    - 您的问题的简要描述

- 详细描述

3. 出现提示时确认案例创建。

案例会自动填充您的转换作业中的上下文，包括：

- Job ID 和状态
- Job 元数据
- Job 执行日志（工作日志）
- Job 计划

案例将根据您的工作类型和问题类别自动分配。

查看 Support 案例

要查看您的支持案例，请提示聊天：

- “列出我的支持案例”
- “向我展示未解决的支持案例”
- “我的案件状况如何？”

聊天将显示：

- 案例 ID
- 主题
- 状态，例如 “打开”、“待处理”、“已解决” 或 “已关闭”
- 上次更新日期
- 关联的作业 ID

要查看特定案例的详细信息，请执行以下操作：

- “向我展示案例 [case-id] 的详情”
- “案例 [case-id] 的最新更新是什么？”

向案例添加通信

要向现有案例添加消息，请执行以下操作：

1. 询问聊天室：“在 case [case-id] 中添加一条消息”
2. 出现提示时提供您的消息。
3. 聊天将确认消息已添加。

当 Support 回复您的 AWS 问题时，您会收到通知。

解决案例

要解决支持案例，请执行以下操作：

1. 询问聊天室：“解决案例 [case-id]”
2. 出现提示时确认分辨率。

> **Note**
>
> 您只能解决由 AWS Support 解决的问题。

禁用 Support 案例管理

1. 打开控制 AWS Transform 台。
2. 在导航窗格中，选择设置。
3. 在 “支持” 下，选择 “禁用支持案例管理”。
4. 选择保存更改。

> **Note**
>
> 禁用 Support 案例管理会移除基于聊天的案例管理界面，但不会关闭现有案例。您仍然可以通过 Su AWS pport Center 访问您的案例。

用法遥测

默认情况下，在 AWS 转换执行期间，Tr AWS ansform IDE 插件、Transform Agent Skill 和 Transf AWS orm Kiro Power 遥测由不同的数据点组成，例如 IDE 名称（例如 VS Code 或 Kiro）、AI 代理名称（例如 Claude Code 或 OpenAI Codex）和执行模式（本地或远程）。Tr AWS ansform 使用这些数据来确定兼容性测试以及延迟和可靠性的优先级。

要禁用遥测，请在聊天会话中告诉代理您不想发射遥测功能。此选择退出仅适用于当前的聊天会话，并且必须为每个新会话重复此操作。如果您直接运行 AWS 转换 CLI，请设置`ATX_DISABLE_TELEMETRY=true`环境变量。

运营数据

我们可能会收集有关您使用 Tr AWS ansform 的操作信号，例如您使用了哪些功能、错误日志以及基于您的自然语言反馈（例如您是否批准继续执行转型计划或是否提供了迭代拟议计划的说明）的指标，以提供服务和评估服务性能。

更改日志

下表描述了 Transform 的重要版本和 AWS 更新。

日期	标题	说明	链接
2026-07-16	AWS “迁移转换” 添加了可下载的工作空间摘要报告	AWS “迁移转换” 现在允许您生成可下载的 PDF 格式的工作空间摘要报告。该报告整合了工作空间中所有迁移任务的数据，包括作业状态、工作流程步骤进度、波浪规划、网络迁移、landing zone 配置、重新托管进度和生成的构件。	下载工作空间摘要报告
2026-07-03	AWS 转换发现工具增加了 Oracle 数据库支持	Transfor AWS m 发现工具现在可以直接从 VMware 和裸机服务器上的数据库中收集详细的 Oracle 元数据。 Hyper-V您可以通过直接 SQL 连接发现 Oracle 实例。该工具收集容器 Database/Pluggable 数据库 (CDB/PDB) 枚举、组件清单和数据文件大小。它还捕获真实应用程序集群 (RAC)、Data Guard 和多租户架构的拓扑标志。如果您尚未配	甲骨文数据库发现

日期	标题	说明	链接
		置数据库凭据，则该工具会回退到 OS-level 检测模式。支持所有 Oracle 版本。	
2026-06-22	南美洲（圣保罗）地区对大型机现代化代理的支持	AWS 大型机现代化代理的转型现已在南美洲（圣保罗）地区（sa-east-1）推出。在支持的区域和跨区域推理表中添加了 sa-east-1。	支持的区域、Cross-region 推理
2026-06-22	AWS 针对 VMware 迁移的转型支持本地化	AWS 针对 VMware 迁移的转换现在支持本地化。在使用 VMware 迁移工作流程时，您可以通过选择 “设置” 图标并选择首选语言来更改 Web 应用程序的显示语言。	本地化设置
2026-06-18	AWS 迁移转型支持将所有 AWS 商业区域作为迁移目标	AWS VMware 迁移转型支持所有 AWS 商业区域作为迁移目标，不包括中东（巴林）和中东（阿联酋）。迁移目标区域是指部署迁移资源的 AWS 区域，包括着陆区、网络基础设施和服务器再托管。	支持的迁移目标区域

日期	标题	说明	链接
2026-06-18	AWS Transform for Migrations 允许您将现有 ENI 附加到启动模板中	AWS Transform 允许您将现有的弹性网络接口 (ENI) 附加到启动模板以进行迁移。AWS Transform 会显示在您的目标账户中找到的所有现有 ENI，您可以对其进行标记，以便在实例启动时可以通过启动配置使用它们。	用于迁移的 ENI 资源标记
2026-06-18	AWS “迁移转换” 允许您配置复制和启动设置	AWS Transform 允许您为迁移配置复制设置和启动设置。您可以根据目标账户或跨特定源服务器设置配置。	复制和启动设置

日期	标题	说明	链接
2026-06-17	Model-to-model 生成式 AI 工作负载的迁移评估	AWS Transform 现在提供模型到模型的迁移自定义转换。转型会评估您的生成式 AI 工作负载。它制定了从第三方提供商迁移到Amazon Bedrock的迁移计划。 AI-powered 代理会扫描您的代码库以识别正在使用的每个 AI SDK 和型号。代理通过交互式问题收集迁移需求。然后，它将模型映射到 Amazon Bedrock 等效模型，并进行透明的成本比较和生产就绪的代码更改。支持从 OpenAI、Google Gemini 迁移、直接使用 Anthropic SDK 以及通过 LiteLLM 或 Ollama 进行开源模型的迁移。处理直接 SDK 集成和框架封装模式 LangChain，包括、 LlamaIndex、Crewai 和多提供商 LangGraph路由层。除了标准的 Trans AWS form 定价外，无需支付额外费用。	新增内容帖子，自定义转换

日期	标题	说明	链接
2026-06-16	AWS 大型机转型提供可追溯的重新构想工作流程	AWS 大型机转型现在可提供从评估到代码生成的互联且可追溯的重新构想体验。运行 z/OS COBOL 和 PL/I 工作负载的企业可以评估其产品组合，以识别离散的业务功能，提取业务规则，生成开发就绪需求，并在单个互联工作流程中生成可追溯的云原生代码。每个要求都可以追溯到源代码，以实现全面的可审计性。	新增内容帖子，文档
2026-06-16	AWS Transform 现在支持适用于 NetApp ONTAP 的 Amazon FSx 作为目标存储（公共预览版）	现在，除了计算再托管的 Amazon EBS 之外，您还可以将块存储工作负载迁移到适用于 NetApp ONTAP 的 Amazon FSx。AWS 在处理计算和网络的同一迁移浪潮中，Transform 将块存储数据直接复制到 ONTAP 卷的 FSx。	新增内容帖子，文档

日期	标题	说明	链接
2026-06-05	适用于 SQL Server 的 Amazon RDS 总拥有成本评估支持	现在，您可以估算将本地 SQL Server 数据库迁移到 Amazon RDS for SQL Server 时的成本。使用 AI-powered Trans AWS form 中的 TCO 评估来分析您的环境并获得最佳的数据库实例建议。该评估支持 Database Savings Plans 中的 “自带媒体” (BYOM) 和 “含许可” (LI) 选项，最多可节省 20%。	新增内容帖子，文档
2026-06-04	AWS 现在支持将转换发现工具作为网络迁移输入源	现在，您可以 AWS 将转换发现工具与Modelizeit一起用作网络迁移的来源，从而为同时运行VMware和非VMware工作负载的环境实现混合网络迁移。	用户指南
2026-05-27	AWS Transform 自定义文档添加了客户端技能示例和最佳实践	客户端技能文档现在包括 Dockerfile 合规性、数据库迁移安全、Terraform 策略执行和 API 弃用帮助程序的实际示例，以及构建和共享技能的最佳实践。	文档

日期	标题	说明	链接
2026-05-22	Transform 现已推出新的代理迁移评估功能 AWS	AWS Transform 现在提供了高级迁移评估功能，包括假设情景、可自定义的假设、灵活的文件格式支持以及多种新的总拥有成本 (TCO) 评估功能。	新增内容帖子，文档
2026-05-20	AWS Transform 在网络迁移审查期间检测现有 VPC	AWS Transform 现在可以在网络迁移审查期间检测目标账户中的现有 VPC。您可以在映射的 VPC 旁边查看现有 VPC，识别 CIDR 冲突并在部署之前解决这些冲突。	文档
2026-05-14	AWS 变形代理现已在 Kiro、Claude、Cursor 和 Codex 中推出	AWS 现在可以通过 Kiro power、代理插件和 Trans AWS form MCP 服务器访问转换代理，让开发人员可以直接从他们首选的开发环境中使用转换功能。	最新消息帖子
2026-05-14	AWS Transform 引入了用于构建自定义转换代理的代理生成器工具包	合作伙伴和客户现在可以使用代理生成器工具包 Kiro power 构建、共享和注册专业的转换代理，将自定义工具和工作流程与 Tr AWS ansform 集成在一起。	最新消息帖子

日期	标题	说明	链接
2026-05-14	AWS Transform 在 Visual Studio 的 AWS Toolkit 中添加了代理人工智能助手	.NET 开发人员现在可以直接在 Visual Studio 中通过对话式的分步指导体验实现应用程序现代化，同时在 IDE 和 Web 控制台中保留完整的上下文。	最新消息帖子
2026-05-14	AWS Transform 现在支持客户拥有的神器商店	您可以配置自己的 Amazon S3 存储桶，也可以选择使用自己的 AWS KMS 密钥对项目进行加密，从而完全控制转换工件的存储位置。	新增内容帖子，《用户指南》
2026-05-14	AWS Transform 增加了迁移策略 (7R) 建议	借助 AWS Transform，您现在可以分析发现的清单，并获得针对每台服务器和应用程序的迁移策略建议。建议遵循行业标准的七种迁移策略 (7R)。每项建议都包括建议的 AWS 目标服务、置信度分数及其背后的原因。你可以生成交互式 HTML 仪表板、PDF 或 Microsoft PowerPoint 输出。	7R 建议

日期	标题	说明	链接
2026-05-11	AWS Transform 在迁移期间增加了容器化功能	AWS Transform 现在支持在迁移过程中将应用程序重塑为容器、自动生成 Dockerfile、使用 CVE 扫描构建容器映像以及部署到 Amazon ECS 或 Amazon EKS。	新增内容帖子，《用户指南》
2026-05-01	AWS Transform 现在为 Power BI 和 Tableau 提供商业智能迁移代理	Partner-built 来自 Wavicle Data Solutions 的代理在转换工作流程中将 Power BI 和 Tableau 仪表板转换为快速资产。 AWS	最新消息帖子
2026-04-21	AWS 自定义变身现已在另外六个 AWS 区域推出	AWS Transform custom 扩展到亚太地区、加拿大和欧洲（伦敦），共覆盖八个 AWS 地区。	最新消息帖子
2026-04-15	AWS Transform 在迁移工作流程中添加了着陆区创建功能	添加了直接在迁移工作流程中创建着陆区。 AWS 转换现有基金会的支票，推荐组织单位 (OU) 结构和目标客户，并提供全自动部署或基础设施即代码 (IaC) 输出（CloudFormation、AWS CDK 或着陆区加速器 (LZA) 格式）。	新增内容帖子，文档

日期	标题	说明	链接
2026-04-15	AWS Transform 添加了迁移规划图表和报告	现在，您可以在迁移计划期间生成交互式图表和分析报告。逻辑示意图类型包括网络拓扑图、应用程序依赖关系图、波浪甘特图和一般图表。报告类型包括风险评估、7R 建议和自定义分析报告。输出以交互式 HTML、PDF 或微软 PowerPoint (.pptx) 文件形式提供。	绘制图表和报告
2026-04-14	AWS 变换现已在 Kiro 和 VS Code 中可用	AWS 现在可以从 Kiro 和 VS Code 访问转换自定义转换，任务状态可在 IDE、CLI 和 Web 控制台界面上共享。	最新消息帖子
2026-04-10	AWS Transform 为网络迁移添加带有安全组映射的 DHC	在网络迁移期间添加了对带有安全组映射的 DHCP 的支持。如果您有 DHCP-enabled 迁移工作负载，现在可以确保您的安全规则在迁移后仍然有效。这适用于通过 Transit Gateway 进行的 VPC 内安全组引用以及跨VPC和跨账户出站规则。	文档

日期	标题	说明	链接
2026-03-31	AWS Transform custom 宣布自动代码库分析正式上线	全面的代码库分析转换已正式发布，可生成任何语言的架构文档、技术债务报告和现代化建议。	最新消息帖子
2026-03-31	AWS 自定义转换引入了新的托管转换，可大规模实现代码现代化	添加了七个新的托管转换，包括 Node.js 升级（正式上市）、Java 优化、Log4j 迁移 Angular-to-React、Angular 升级和 Vue 升级（抢先体验）。	最新消息帖子
2026-03-20	AWS Transform 为网络迁移添加了公共	添加了用于网络迁移的公共 API，使合作伙伴和编程人员能够访问网络迁移功能。	API 引用
2026-01-14	AWS Transform custom 增加了 AWS PrivateLink 支持并扩展到欧洲（法兰克	AWS Transform custom 现在支持通过 AWS PrivateLink 私有 VPC 访问，除美国东部（弗吉尼亚北部）外，欧洲（法兰克福）也可用。	最新消息帖子
2025-12-23	AWS Transform 支持混合数据中心迁移的网络转换	AWS Transform for VMware 可自动将混合数据中心网络配置（VLAN、IP 范围）转换为 AWS VPC、子网和安全组，无需手动映射。	最新消息帖子

日期	标题	说明	链接
2025-12-01	AWS 推出 T AWS ransform custom 以加快组织范围的	AWS Transform custom 已全面推出，使组织能够通过单个 CLI 命令大规模自动执行可重复的代码转换。	最新消息帖子
2025-12-01	AWS Transform 为企业 VMware 迁移添加了新的代理人工智能功能	AWS Transform 的 VMware 代理现在可以发现本地环境、映射依赖关系、生成迁移浪潮计划，以及在 HyperV、Nutanix、KVM 和裸机目标之间进行迁移。	最新消息帖子
2025-12-01	AWS Transform 推出用于全栈 Windows 现代化的 AI 代理	新的全栈式 Windows 代理可自动将.NET 应用程序和 SQL Server 数据库转换为 Aurora PostgreSQL，部署到亚马逊 ECS 或 EC2 Linux 上的容器中。	最新消息帖子
2025-12-01	AWS Transform 扩展.NET 转换功能并增强开发者体验	AWS Transform 在 Blazor 移植中添加了 .NET 10 支持、ASP.NET Web 表单以及通过 Visual Studio 的 AWS Toolkit for Visual Studio 增强	最新消息帖子

日期	标题	说明	链接
2025-12-01	AWS 大型机转型提供了新的测试自动化功能	AWS 大型机转型引入了自动测试计划生成、测试数据收集脚本和测试用例自动化，以加快大型机现代化测试。	最新消息帖子
2025-12-01	AWS 大型机转型现在支持应用程序重新构想	新的数据和活动分析以及业务逻辑提取功能可以将传统的大型机应用程序分解为云原生架构。	最新消息帖子
2025-11-13	AWS Transform 可自动执行着陆区加速器网络配置	AWS 适用于 VMware 的 Transform 会自动生成 LZA-compatible 网络 YAML 文件，从而简化 VMware 环境中的多账户云基础架构设置。	最新消息帖子
2025-07-16	AWS 大型机转型引入了增强的代码重构和业务逻辑功能	AWS 大型机转换增加了重构（代码重组）的普遍可用性，并扩展了应用程序级业务逻辑提取，以提高代码质量。	最新消息帖子
2025-05-15	AWS 针对 VMware 的转换现已正式推出	AWS VMware Transform 是一项代理人工智能服务，可自动执行从发现到部署的整个 VMware 现代化生命周期，现已正式上线。	最新消息帖子

日期	标题	说明	链接
2025-05-15	AWS 大型机转型现已正式推出	AWS Transform for mainframe 是第一个用于大规模实现 IBM z/OS 应用程序现代化的代理 AI 服务，它通过新的分析、分解和任务管理功能全面推出。	最新消息帖子

下载此数据。

的文档历史记录 AWS 变换用户指南

下表描述了《 AWS 转换用户指南》的文档历史记录。

变更	说明	日期
持续的现代化组合分析和修复	添加了新的章节，记录了用于自动代码分析和修复的 AWS 转换持续现代化功能（`atx ct`子命令）。查看持续现代化。	2026 年 6 月 3 日
棕地网络：现有 VPC 可见性	在网络迁移审查期间添加了现有 VPC 检测。 AWS Transform 会自动检测目标账户中已部署的 VPC，并标记与映射的 VPC 的 CIDR 冲突。查看目标账户中的现有 VPC。	2026 年 5 月 18 日
为 Transform 自定义添加了技能格式、客户端技能和子代理日志 AWS	转换定义现在使用技能格式（`SKILL.md`带有 YAML frontmatter 和可选`references/` 文件夹）。添加了用于使用其他功能扩展代理的客户端技能，以及用于改进调试的子代理日志。需要 CLI 版本 2.0 或更高版本。请参阅转换定义和Client-Side 技能。	2026 年 5 月 11 日
添加了源代码容器化	AWS Transform 现在可以使用生成式 AI 对您的应用程序进行容器化。提供来自 Git 存储库或 zip 上传的源代码，然后 Tr AWS ansform 对其进行分析，生成 Docker 工件，将容器映像发布到 Amazon ECR，生成基础设施即代码，然后部署到亚	2026 年 5 月 7 日

	马逊弹性容器服务或亚马逊弹性 Kubernetes 服务。请参阅源代码容器化。	
增加了网络优化操作和指导性建议	增加了第 5 步：查看和优化网络，包括 VPC 和子网操作（删除、排除、合并、拆分、调整大小、重命名、更改 IP 地址），以及命名标准化、范围审查、容量合理调整、安全审查和 VPC 整合的指导性建议。请参阅查看和优化网络。	2026 年 4 月 27 日
AWS 在 6 个新区域推出自定义转换	自定义变换中增加了对 ca-central-1、eu-west-2、ap-northeast-1、ap-northeast-2、ap-southeast-2 和 ap-southeast-2 和 ap-southeast-1 的支持。AWS	2026 年 4 月 21 日
更新了连接器权限文档	添加了目标 AWS 账户 连接器的详细权限细分，包括 S3、MGN、Migration Hub 权限、工作负载迁移和着陆区域基础设施配置。参见 Connec AWS 账户 t 目标。	2026年4月19日
更新了 VMware 迁移任务类型	添加了发现和迁移规划、着陆区和着陆区、网络和服务器迁移任务类型。仅将 “网络迁移” 重命名为 “网络迁移” 和 “迁移计划”，以制定迁移计划。请参阅 VMware 迁移任务类型。	2026年4月19日

重组后的 Connect 目标是 AWS 账户	将连接器设置重组为三个步骤：迁移类型选择、MAP 协议和连接器配置，包括支持的目标区域、账户角色、委派管理员指南和 IAM 角色。参见 Connec AWS 账户 t 目标。	2026年4月19日
添加了其他仅限服务器迁移的目标区域	记录了另外 14 个商业区域可用于服务器迁移作业，无需网络迁移，并且要求在 2026 年第三季度之前进入允许名单。请参阅支持的目标区域。	2026年4月19日
添加了 “迁移服务器” 章节	添加了新的 Migrate 服务器章节，涵盖了完整的重新托管工作流程，包括账户结构、IAM 角色、委派管理员设置、复制代理部署、测试和切换。	2026年4月19日
新增 “建造着陆区” 章节	添加了新的 B uild landing zon e 章节，其中包含着陆区域配置的连接器权限详细信息。	2026年4月19日
安全组映射和引用	为迁移网络添加了安全组映射策略（MAP、MAP_DHCP、SKIP）和安全组参考文档。	2026 年 4 月 13 日
Auto-conversion 对于不支持的网络文件类型	在 M igrat e 网络中添加了对自动转换不支持的网络配置文件类型的支持。	2026年4月6日
为数据库迁移添加了 KMS 密钥策略	添加了数据库迁移加密部分。	2026 年 3 月 26 日
记录在案的新 AWS 托管策略	添加了DBModProvisioningAndMigration章节。	2026年3月24日

记录在案的新 AWS 托管策略	添加了DBModDiscoveryAndAssessment章节。	2026年3月24日
生成网络图	为迁移网络添加了可选的网络逻辑示意图生成（Mermaid 和 PNG 格式）。	2026 年 3 月 18 日
防火墙和 SDN 配置文件支持	增加了对 Palo Alto Networks、Fortinet 和 Cisco ACI 配置文件的支持 FortiGate，用于在 Migrate 网络中进行网络迁移。	2026 年 2 月 11 日
网络资源的自定义标记	在 Migrate 网络中为网络迁移添加了作业级和 VPC-level 自定义标记支持。	2026 年 1 月 28 日
添加了支持文档	增加了对章节的AWS 支持。	2025 年 12 月 23 日
记录在案的新 AWS 托管策略	新增AWSTransformCustomFullAccessAWSTransformCustomExecuteTransformations、和AWSTransformCustomManageTransformations章节。	2025年12月7日
VMware	更新了 VMware 迁移部分。	2025 年 12 月 1 日
更新了 AWS 托管策略	更新了AWSServiceRoleForAWSTransform文档以反映新增的权限。	2025 年 12 月 1 日
支持的区域	更新了支持的区域主题。	2025 年 12 月 1 日
大型机现代化	更新了大型机现代化部分。	2025 年 12 月 1 日
入门指南	更新了入门主题。	2025 年 12 月 1 日

Full-stack Windows 现代化	添加了 Full-stack Windows 现代化主题，其中包括更新的 .NET 部分和新的 SQL Server 现代化部分。	2025 年 12 月 1 日
发现工具	添加了发现工具部分。	2025 年 12 月 1 日
更新了 AWS 托管策略	更新了AWSTransformApplicationECSDeploymentPolicy扩展的 IAM 角色检查权限、ECS 服务相关角色创建以及 ECR 加密支持的 KMS 权限。	2025 年 11 月 22 日
更新了 AWS 托管策略	AWSTransformApplicationDeploymentPolicy使用额外的 EC2 联网、IAM 角色检查、S3 存储桶管理和 KMS 加密权限进行了更新。	2025 年 11 月 22 日
发现收藏家	添加了AWS 变换发现工具> 文档。	2025 年 10 月 31 日
添加了 VMware 迁移架构图	在迁移网络中添加了 VMware 迁移架构图。	2025 年 10 月 23 日
VMware 迁移结果更新	更新了 M igrate 网络中的迁移结果信息。	2025年10月12日
VMware 迁移结果更新	更新了 M igrate 网络中的迁移结果信息。	2025年10月12日
S3 连接器文档	为.NET Web 应用程序添加了 S3 连接器文档。	2025 年 10 月 8 日
新的用户连接器主题	添加了用户连接器主题。	2025年9月21日
更新了 AWS 托管策略	更新了AWSServiceRoleForAWSTransform文档。	2025 年 9 月 17 日

存储评估支持	增加了对存储评估 NetApp 的数据基础设施见解 (DII) 文件支持。	2025 年 9 月 2 日
目标区域更新	添加了三个支持的目标区域。	2025 年 8 月 31 日
托管式策略更新	添加了供使用的 IAM 身份中心只读权限。AWSServiceRoleForAWSTransform	2025 年 8 月 29 日
记录在案的新 AWS 托管策略	添加了AWSTransformApplicationDeploymentPolicy章节。	2025 年 8 月 28 日
接口端点	添加了接口终端节点主题。	2025 年 7 月 9 日
初始版本	《 AWS 转换用户指南》的初始版本。	2025 年 5 月 15 日

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。