



Manual do usuário

AWS Transformação



AWS Transformação: Manual do usuário

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é AWS Transformar?	1
Terminologia	1
Introdução	4
Configurar	4
Antes de começar	4
Inscreva-se para um Conta da AWS	4
Começando com o IAM-only acesso	4
Usando credenciais do IAM	5
Conceitos básicos de AWS Organizations	6
Conceitos básicos de Centro de Identidade do AWS IAM	7
Usando provedores de identidade terceirizados	8
Onboarding	11
Usando seu próprio bucket S3	13
Enable (Habilitar) AWS Transformação	22
Início rápido: Experimentando AWS Transformação	23
Gerenciamento de usuários	24
Adicionar usuários no IAM Identity Center	24
Adicionando usuários ao AWS Transformação	25
Gerenciando usuários com IAM-only acesso	25
Entendendo as permissões dos colaboradores	25
AWS Transforme o ambiente	28
Configurações de idioma	30
Comece seu projeto	31
AWS Transforme o bate-papo	31
Ferramentas de desenvolvedor	34
Kiro Power	34
Plugin de agente	34
Plug-in IDE	35
Servidor MCP	35
Autenticação	36
Crie agentes personalizados para AWS Transformação	36
Avaliações de migração	38
Pré-requisitos	38
Como funcionam as avaliações de migração	38

Carregando dados de inventário	39
Analisando os resultados da descoberta	40
Gerenciando o escopo do inventário	40
Configurando cenários de avaliação	40
Capacidades de avaliação	41
Dimensionamento correto do Amazon EC2	41
Armazenamento Amazon EBS	41
Amazon FSx	42
Amazon RDS para SQL Server	42
Amazon EC2 SQL Server	43
On-premises preços	43
Sustentabilidade	43
Avaliação do valor comercial	43
Custos de rede	44
Custos de suporte	44
Computação de usuário final	44
Usando avaliações baseadas em bate-papo	44
Estimativa aproximada com dados limitados	44
Adicionar inventário por meio do chat	45
Modificando custos e adicionando serviços	45
Comparando cenários	45
Criação de cenários	45
Executando comparações	46
What-if análise	46
Geração de resultados	46
Tópicos relacionados	47
Personalizada	48
O que é AWS Transformar de forma personalizada?	48
Principais recursos	48
Padrões de transformação	48
Como AWS Transforma trabalhos personalizados	51
Compreender os conceitos principais do	52
Definições de transformação	52
Registro de transformação	53
Transformações preliminares versus transformações publicadas	53
Referências versus aulas	54

Comandos de compilação e validação	54
Aprendizagem contínua	55
Client-Side Habilidades	56
Conceitos básicos	56
Pré-requisitos	56
Instalar o AWS Transform CLI	57
Configuração da autenticação	58
Configurar AWS Região	60
Executando sua primeira transformação	63
Entendendo os resultados da transformação	64
Criando uma transformação personalizada	64
AWS Aplicativo Web Transform (opcional)	65
Introdução aos comandos de transformação personalizados	66
Fluxos de trabalho	67
Executando transformações	67
Aprendizagem contínua	72
Configuração avançada	73
Crie transformações personalizadas	87
Os comandos da Referência de comandos	91
Comandos interativos	91
Comandos de definição de transformação	91
Comandos da lição	95
Comandos de tag	96
Comandos de atualização	96
Comandos MCP	96
AWS-Transformações gerenciadas	97
Visão geral do	97
Available (Disponível) AWS-Transformações gerenciadas	97
Personalizar AWS-Transformações gerenciadas	114
Casos de uso comuns	114
Atualizações do Lambda Runtime	114
Endpoints da VPC (AWS PrivateLink)	116
Considerações para AWS Transform endpoints VPC personalizados	117
Pré-requisitos	117
Criação de uma interface VPC endpoint para AWS Transform personalizado	117
Criação de uma política de VPC endpoint para AWS Transform personalizado	118

Usando um computador local para se conectar a um AWS Transform endpoint personalizado	118
Solução de problemas	119
Localizações de registros	119
Problemas comuns	120
Como obter suporte	122
Problemas de acesso ao S3	122
Histórico de versões do CLI	123
Modernização contínua	133
O que é AWS Transformar a modernização contínua?	133
Capacidades gerais	133
Tipos de análise	134
Explicação sobre os principais conceitos	135
Fontes	135
Repositórios	135
Análises	136
Conclusões	136
Remediações	136
Definições de transformação	136
Como AWS Transforme os trabalhos de modernização contínua	136
Opções de computação	137
Configuração do agente de segurança	139
Introdução	140
Pré-requisitos	140
Início rápido	140
Trabalhando com modernização contínua	141
Gerenciamento de fontes	141
Descoberta e gerenciamento de repositórios	142
Análise em execução	143
Gerenciar descobertas	144
Criação de remediações	144
AWS Transformar aplicativo web (opcional)	145
Ferramentas de desenvolvedor	146
Habilidades do agente	146
Referência da CLI	147
Solução de problemas	149

Ferramenta de descoberta	151
Fluxo de trabalho	151
Configurar a ferramenta de descoberta	152
Pré-requisitos	152
Implemente no VMware	154
Implantar em Hyper-V	156
Implemente no Linux	156
Configurar a ferramenta de descoberta	159
Permissões obrigatórias	172
VMware vCenter	172
Hyper-V hospedeiros (Windows)	173
Servidores Linux (SSH)	173
Servidores Windows (WinRM) — métricas do sistema operacional	175
Servidores Windows (WinRM) — coleção SQL Server	177
Banco de dados Oracle (SQL)	178
Coleção de rede	178
Referência rápida: permissões mínimas por caso de uso	179
Coleta de dados	180
Cronograma de coleta	180
Inventário descoberto	182
OS-related dados	186
Considerações sobre segurança	206
Protegendo a ferramenta de descoberta VM	206
Protegendo credenciais	206
Armazenamento de credenciais	208
Usando o Auto-Connect recurso com cuidado	208
Segurança de importação de CSV	210
Considerações sobre a revogação do acesso	210
Solucionar problemas da ferramenta de descoberta	211
Verificando a conectividade da ferramenta de descoberta com o vCenter	211
Solução de problemas do WinRM	213
Solução de problemas do Kerberos	213
Solução de problemas do banco de dados	217
Solução de problemas de SNMP	219
Erros de coleta de rede	220
Erros de coleta de métricas do sistema operacional	221

Problemas de acesso no inventário descoberto	221
Solução de problemas de autenticação com chave SSH	221
Solução de problemas do instalador Linux	223
Mensagens de erro comuns	223
Notas da versão	224
Conectores	229
Rastreabilidade do usuário para operações de agentes	229
Gerenciando conectores	231
Migrações (incluindo VMware)	233
Capacidades e características principais	233
Arquitetura	233
Empregos de migração	234
Conseguir um espaço de trabalho	234
Tipos de emprego	235
Criando e começando um emprego	236
Baixando um relatório resumido do espaço de trabalho	236
Limitações	237
Descubra os dados de origem	237
Crie um plano de migração	238
Fluxo de trabalho	240
Recomendações 7Rs	242
Diagramas e relatórios	244
Conecte o alvo Conta da AWS s e regiões	245
Etapa 1: Seleção do tipo de migração	245
Etapa 2: contrato MAP	245
Etapa 3: configuração do conector	246
Construa uma landing zone	252
Configuração do conector	252
Configuração da fundação	254
Design da conta de carga de trabalho	257
Formatos IaC	259
Processo de aprovação de implantação	260
Tag: recursos da zona de pouso	260
Revertendo mudanças	261
Recursos relacionados	261
Migre sua rede para AWS	262

Etapa 1: mapeamento da rede de origem	262
Etapa 2: arquivos de configuração adicionais	264
Etapa 3: topologias de rede	264
Etapa 4: mapeamento de grupos de segurança	267
Etapa 5: Revise e otimize sua rede	270
Etapa 6: diagrama de rede	274
Etapa 7: configurar a marcação de recursos	274
Etapa 8: implantar sua rede	276
Excluir recursos de rede implantados	277
Extração do arquivo de configuração	278
Migrar servidores	279
Pré-requisitos e configuração de padrões de migração	280
Etapa 1: configurar a onda de migração	282
Etapa 2: validar e confirmar o inventário	286
Etapa 3: implantar agentes de replicação	287
Etapa 4: replicação de dados	294
Etapa 5: Teste	296
Etapa 5b: Marcar os aplicativos como prontos para a transição	296
Etapa 6: transição	296
Estados do ciclo de vida do servidor	297
Aprovações de implantação	298
Notas da versão	299
Junho de 2026	299
Maio de 2026	299
Abril de 2026	300
Março de 2026	300
Fevereiro de 2026	300
Janeiro de 2026	300
Dezembro de 2025	300
Outubro de 2025	301
Setembro de 2025	301
Agosto de 2025	301
Maio de 2025	301
Containerização do código-fonte	303
Capacidades e características-chave	303
Como funciona a containerização	304

Pré-requisitos	304
Fluxo de trabalho de containerização	305
Iniciando um trabalho de containerização	305
Permissões	306
Política básica	306
Política de rede	307
Política de armazenamento	307
AWS KMS política	307
Política do Amazon ECS	308
Política do Amazon EKS	308
Etapa 1: isenção de responsabilidade de segurança	308
O que a isenção de responsabilidade cobre	308
O que você precisa fazer	309
Etapa 2: clonar o código-fonte	309
Opção 1: repositórios Git	310
Opção 2: upload de arquivo zip	311
Opcional: configurar dependências privadas	311
Confirmando as preferências de containerização	311
Etapa 3: Containerizar	312
O que acontece durante a containerização	312
Tipos de aplicação compatíveis	313
O que você precisa fazer	313
Etapa 4: revisar os artefatos	313
Revisando as alterações dos repositórios Git	313
Analisando as alterações dos uploads de zip	314
Solicitando alterações	314
Etapa 5: publicar imagens	314
O que acontece durante a publicação	314
O que você precisa fazer	315
Etapa 6: Gerar IaC	315
Amazon Elastic Kubernetes Service (Kubernetes)	315
Amazon Elastic Container Service (Terraform)	316
Validação automatizada e verificação de segurança	316
Gerando IaC sem imagens publicadas	317
O que você precisa fazer	317
Etapa 7: implantar a infraestrutura de teste	317

O que acontece durante a implantação de teste	318
O que você precisa fazer	318
Iterando na infraestrutura	318
Recuperação da sessão	319
Etapa 8: Limpar a infraestrutura de teste	319
O que você precisa fazer	319
Etapa 9: implantar a infraestrutura de transição	319
O que você precisa fazer	320
Recuperação da sessão	320
Mainframe Modernization	321
Capacidades e características-chave	321
High-level passo a passo	322
Human in the loop (HITL)	322
Tipos de arquivo compatíveis para transformação de aplicativos de mainframe	323
Regiões suportadas e cotas para AWS Transforme o mainframe	324
Jornada de modernização	324
Fase 1: Avaliar	324
Fase 2: Mobilizar	325
Fase 3: Migrar e modernizar	326
Fase 4: operar, otimizar e inovar	328
Transformação do fluxo de trabalho de aplicativos de mainframe	329
Pré-requisito: preparar as entradas do projeto no S3	329
Coleção de artefatos de origem de mainframe	330
Sign-in e criar um emprego	339
Acompanhando o progresso da transformação	340
Configurar um conector	340
Avalie e reinvente o plano de trabalho	345
Reinvente o plano de trabalho	351
Plano de trabalho personalizado	351
Crie e implante aplicativos modernizados	383
Pré-requisitos	383
Etapa 1: recuperar o código modernizado	384
Etapa 2: criar o aplicativo modernizado	384
Etapa 3: Configurar o ambiente de teste	385
Etapa 4: implantar o aplicativo modernizado	386
Etapa 5: testar o aplicativo modernizado	387

Exemplo adicional	387
Full-stack Modernização do Windows	388
.NET	388
Experiências	388
Capacidades e características-chave	389
Versões e tipos de projeto compatíveis	389
Limitações	390
Intervenção humana	391
Mais informações	391
Aplicativo web.NET	391
IDEO.NET	408
Portando o código da camada de UI	417
Relatórios de transformação	419
Práticas recomendadas	421
Modernização do SQL Server	427
Regiões compatíveis	427
Capacidades e características principais	427
Versões e tipos de projeto compatíveis	429
Requisitos do SQL Server	433
Requisitos de aplicação	433
Requisitos de infraestrutura	434
Requisitos do repositório	435
Configuração do SQL Server	435
AWS Configuração de transformação	443
Crie um trabalho de modernização do SQL Server	444
Fluxo de trabalho de modernização do SQL Server	451
Teste e implante após a transformação	483
Práticas recomendadas e solução de problemas	486
Segurança	491
Proteção de dados	492
Cross-region processamento	493
Criptografia de dados	502
Melhoria do serviço	512
Gerenciamento de identidade e acesso	513
Público	514
Autenticação com identidades	514

Gerenciar o acesso usando políticas	516
Como AWS O Transform funciona com o IAM	517
Identity-based exemplos de políticas	523
Solução de problemas	533
Uso de perfis vinculados ao serviço	535
AWS políticas gerenciadas	541
AWS Referência de permissões de transformação	557
Validação de conformidade	559
Resiliência	559
Endpoints da VPC (AWS PrivateLink)	560
Considerações para AWS Transform Endpoints da VPC	560
Pré-requisitos	560
Criação de uma interface VPC endpoint para AWS Transform	561
Usando um computador local para se conectar a um AWS Transform endpoint	562
Acesso VPC ao aplicativo Web	562
Como funciona	562
Arquitetura	563
Pré-requisitos	564
Configurando a política de VPC endpoint	564
Configurando a saída controlada da Internet	565
Verificação	572
Solução de problemas	573
Considerações sobre custos	574
Limpeza	574
Monitoramento	576
CloudTrail troncos	576
AWS Transform informações em CloudTrail	577
Noções básicas AWS Transformar entradas do arquivo de log	578
Notificações	578
Notificações por e-mail	578
Cotas	581
Regiões aceitas	587
Compatível Regiões da AWS (ativado por padrão)	587
Suporte	589
Pré-requisitos	589
Habilitando o Support Case Management	589

Criando um Support Case	589
Exibindo Support Cases	590
Adicionando comunicações a um caso	591
Resolvendo um caso	591
Desativando o Support Case Management	591
Telemetria de uso	592
Dados operacionais	593
Log de alterações	594
Histórico do documento	619
.....	dcxxviii

O que é AWS Transformar?

AWS O Transform é um serviço que ajuda você a acelerar e simplificar a transformação da infraestrutura, dos aplicativos e do código com uma experiência de IA agente. Ele fornece ferramentas especializadas para agilizar os esforços de modernização e migração em várias cargas de trabalho.

Com o AWS Transform, você pode:

- Modernize e migre a IBM z/OS e a Fujitsu GS21 para AWS
- Migre cargas de trabalho da VMware para o Amazon EC2
- Modernize aplicativos.NET para Linux-ready transformar.NET multiplataforma
- Avalie as cargas de trabalho quanto à prontidão para a migração

AWS O Transform ajuda você a transferir tarefas de transformação complexas e trabalhosas nas fases de descoberta, planejamento e execução para agentes de IA com experiência em linguagens, estruturas e infraestrutura. Essa abordagem permite que suas equipes se concentrem na inovação enquanto transforma com eficiência projetos complexos e de grande escala por meio de uma experiência web unificada.

Não há custo adicional para usar o AWS Transform.

Terminologia

Nesta seção, o *itálico* indica um termo oficial dentro da definição de um termo diferente.

Conexão de conta

Nesse contexto, a conta é uma referência generalizada a um contêiner de propriedade do cliente ou limite de segurança para recursos em um serviço remoto, por exemplo, uma conta AWS ou *Conta da AWS GitHub*.

Artifato

Um produto de saída produzido pela AWS Transform.

Administrador

Os administradores podem ler e alterar tudo no espaço de trabalho. Eles podem iniciar bate-papos com o AWS Transform, iniciar e interromper trabalhos e upload/download artefatos. Os

administradores podem interagir com trabalhos em execução para ações human-in-the-loop (HITL) e aprovar ações críticas de HITL, como mesclar com o principal, realizar decomposição gráfica ou implantar código em ambientes de produção. Os administradores podem transformar [espaços de trabalho](#), [conectores](#) e usuários.

Agente

Um serviço específico de tarefa que executa um tipo de transformação específico. Por exemplo, migrações da VMware.

Aprovador

Os aprovadores têm permissões semelhantes às dos administradores, exceto pelo fato de não terem permissões para alterar espaços de trabalho, conectores ou usuários. Os aprovadores não podem alterar [espaços de trabalho](#), [conectores](#) ou usuários.

Ativo

Entrada para um [trabalho](#) de transformação. Por exemplo, código-fonte, servidor, banco de dados e rede do cliente. Os ativos são acessados por meio de um [conector](#).

Solicitação de colaborador

Uma tarefa na qual AWS Transform está pedindo a um humano que faça alguma coisa.

Conector

Os conectores são fornecedores de ativos que permitem o acesso a recursos de propriedade do cliente em um sistema externo ao Transform. AWS

Quando você configura um conector, o administrador da conta à qual você está se conectando deve aceitar a conexão. Para aceitar a conexão, eles devem ter permissões fornecidas na [política de aceitadores de conectores](#).

As duas contas a seguir devem ser idênticas ou pertencer à mesma AWS Organizations organização:

- A conta a partir da qual o administrador do AWS Transform ativa o serviço.
- A conta que receberá sua transformação. Essa conta deve ter uma função do IAM que permita o uso de um [conector](#).

Colaborador

Os colaboradores podem ler tudo no espaço de trabalho. Eles podem iniciar bate-papos com o AWS Transform, iniciar e interromper trabalhos, carregar ou baixar artefatos e interagir com

[trabalhos](#) em execução para ações do HITL. No entanto, eles não podem realizar ações críticas de HITL, como mesclar com o principal, realizar a decomposição de gráficos ou implantar código em ambientes de produção. Os colaboradores também não podem alterar [espaços de trabalho](#), [conectores](#) ou usuários.

Objetivo

Um estado final definido pelo usuário que o AWS Transform trabalha para alcançar. Os usuários escrevem isso e, em seguida, o AWS Transform converte o objetivo em uma série de tarefas que ele executa em conjunto com os usuários quando necessário.

Job

Um processo de longa duração (weeks/months+) no qual o AWS Transform está trabalhando para cumprir um [objetivo](#) definido por um usuário. Composto por várias [tarefas](#) e [solicitações de colaboradores](#).

Plano

[Uma lista de tarefas que o AWS Transform realiza \(com a ajuda de usuários humanos\) em busca de um objetivo.](#)

Leitor

Os leitores podem ver o status e os resultados dos trabalhos do AWS Transform, mas não podem fazer nenhuma alteração. Eles podem ler tudo no [espaço de trabalho](#), baixar artefatos, visualizar [trabalhos](#) e visualizar ações do human-in-the-loop (HITL). No entanto, os leitores não podem realizar ações mutantes no AWS Transform.

Tarefa

Uma unidade individual de trabalho que faz parte de um [trabalho](#).

Registro de trabalho

Um registro das ações que o AWS Transform e os usuários realizaram como parte de um [trabalho](#).

Espaço de trabalho

Um recurso de AWS transformação que contém outros recursos, como [conectores](#) e [tarefas](#). Um [espaço de trabalho](#) serve como limite de permissões.

Conceitos básicos de AWS Transformação

Tópicos

- [Configurar AWS Transformação](#)
- [Enable \(Habilitar\) AWS Transformação](#)
- [Início rápido: Experimentando AWS Transformação](#)
- [Gerenciamento de usuários](#)
- [AWS Transforme o ambiente](#)

Configurar AWS Transformação

Antes de começar

Antes de configurar o AWS Transform, verifique se você tem uma AWS conta com acesso de administrador.

Note

Se você quiser experimentar o AWS Transform como prova de conceito ou para ambientes de teste, consulte [Início rápido: Experimentando o Transform. AWS](#)

Inscreva-se para um Conta da AWS

Para começar AWS, você precisa de um Conta da AWS. Para obter informações sobre como criar um Conta da AWS, consulte [Introdução a um Conta da AWS](#) no Guia de AWS Gerenciamento de contas referência.

Começando com o IAM-only acesso

Com o IAM-only acesso, os usuários se autenticam com suas AWS credenciais existentes.

Para configurar o IAM-only acesso:

1. No AWS console, navegue até AWS Transformar e escolha Começar.

2. Conclua a configuração das configurações da conta.
3. Em Acesso do usuário, selecione IAM-only acesso.
4. Escolha Ativar para criar seu perfil.

Os usuários fazem login no aplicativo web AWS Transform por meio de [AWS Sign-In](#). Seu identificador de usuário no aplicativo web é baseado em seu IAM principal.

Important

Você não pode adicionar um provedor de identidade após a conclusão da configuração. Para gerenciar usuários com o IAM Identity Center ou um provedor de identidade existente, escolha uma dessas opções durante a configuração inicial.

Com o IAM-only acesso, qualquer diretor do IAM com a `transform:AccessTransformProfile` permissão no recurso de perfil pode acessar o AWS Transform. Você gerencia o acesso do usuário por meio de políticas do IAM e não por meio de atribuições de usuários do provedor de identidade.

A `transform:AccessTransformProfile` ação só concede acesso ao AWS Transform. Uma vez dentro do AWS Transform, as funções do espaço de trabalho controlam quais ações um usuário pode realizar. Essas funções incluem Administrador, Colaborador, Aprovador e Read-only. As funções do espaço de trabalho se aplicam independentemente de como o usuário se autenticou.

Usando credenciais do IAM

Tratamento de informações do usuário

Quando os diretores do IAM acessam o AWS Transform, o serviço trata a identidade do usuário de forma diferente do que com o acesso baseado no provedor de identidade.

Identidade do usuário

Os usuários do IAM são identificados pelo [diretor do IAM](#).

Identidade dupla

Um usuário que tem uma identidade de provedor de identidade (como o IAM Identity Center) e uma sessão do IAM aparece como dois usuários separados no AWS Transform. O trabalho deles não está vinculado entre as duas identidades.

Notificações por e-mail

As notificações por e-mail só estão habilitadas para usuários de SSO. Os diretores do IAM ainda podem ser adicionados aos espaços de trabalho, mas não receberão notificações por e-mail.

Auditoria

As chamadas da API IAM são registradas AWS CloudTrail com a identidade IAM do chamador. As ações realizadas por usuários do IAM em um trabalho também podem ser rastreadas nos registros de trabalho do AWS Transform.

Habilitando o acesso ao IAM junto com um provedor de identidade

Se você configurar o AWS Transform com o IAM Identity Center ou um provedor de identidade terceirizado, também poderá ativar o acesso ao IAM como uma forma adicional de autenticação. Isso permite que os diretores do IAM acessem o AWS Transform junto com seus usuários atuais do provedor de identidade.

O acesso ao IAM é ativado por padrão quando você cria um perfil com o IAM Identity Center ou um provedor de identidade terceirizado. Para ativar ou desativar o acesso ao IAM a qualquer momento:

1. No console do AWS Transform, navegue até Configurações.
2. Em AWS Transformação de acesso com credenciais do IAM, ative ou desative a opção Ativar acesso ao IAM.

Quando o acesso ao IAM está ativado, tanto os usuários do provedor de identidade quanto os principais do IAM podem usar o AWS Transform. Os usuários do IAM e os usuários do provedor de identidade podem colaborar no mesmo espaço de trabalho.

Conceitos básicos de AWS Organizations

Siga estas etapas para configurar o AWS Transform:

1. Faça login na sua conta de gerenciamento do AWS Organizations.
2. Navegue até o serviço AWS Transform.
3. Escolha Habilitar serviço para sua organização usar o AWS Transform.
4. Configure as permissões necessárias para contas de membros organizacionais.

5. Acesse a experiência web do AWS Transform a partir de suas contas de membros.

 Note

Para usar a AWS solução Landing Zone Accelerator (LZA) ou para criar sua zona de pouso junto com o AWS Transform para recursos de migração, sua conta do AWS Transform e a instalação do LZA devem estar na mesma organização. AWS Não há suporte para o uso de Organizations IDs separadas para implantações de LZA e AWS Transform, pois isso pode causar inconsistências no gerenciamento organizacional e nas implantações de recursos. Para saber como configurar sua instalação do LZA usando Organizations, consulte [Implementar uma base em nuvem para suportar cargas de trabalho altamente regulamentadas e requisitos complexos de conformidade](#) no guia do usuário do Landing Zone Accelerator on AWS Implementation Guide.

Conceitos básicos de Centro de Identidade do AWS IAM

Siga estas etapas para usar o IAM Identity Center for AWS Transform e adicionar usuários e grupos.

Por padrão, nenhum usuário tem acesso ao AWS Transform quando você o ativa pela primeira vez.

 Note

O IAM Identity Center não está limitado à região em que está configurado. Se você já configurou o IAM Identity Center em uma região que não é compatível com o AWS Transform, você pode usá-lo para o AWS Transform.

1. Configure o IAM Identity Center seguindo as instruções em [Para habilitar uma instância do IAM Identity Center](#).

Configure o IAM Identity Center para usar um provedor de identidade empresarial externo e replicar suas informações de usuário e grupo no IAM Identity Center.

2. No AWS console, selecione AWS Transformar e escolha Começar.
3. Escolha Habilitar serviço para sua organização usar o AWS Transform.
4. Selecione uma chave de criptografia. A seleção padrão é uma chave AWS gerenciada. Para usar uma chave personalizada:

- a. Em Chave de criptografia, escolha Personalizar configurações de criptografia.
- b. Selecione Usar uma chave AWS KMS.
- c. Escolha uma chave existente ou crie uma nova.
- d. Escolha Enviar para aplicar suas alterações e, em seguida, escolha Ativar AWS transformação.

Escolha Exibir perfil para ver a configuração. O URL do aplicativo Web é usado por seus usuários para acessar a experiência web unificada do AWS Transform.

5. Selecione Usuários no painel de navegação e selecione Atribuir usuários ou grupos.
6. Pesquise o nome do usuário ou dos grupos que você deseja autorizar a usar o AWS Transform. A pesquisa faz referência a usuários e grupos propagados pelo seu provedor de identidade.
7. Selecione um grupo ou usuário, selecione Concluído e, em seguida, Atribuir. Esses usuários estão autorizados a usar a interface web unificada do AWS Transform.

Usando provedores de identidade terceirizados

AWS O Transform oferece suporte à integração com provedores de identidade de terceiros (IdPs), como Azure Active Directory (Entra ID) e Okta Workforce Identity. Isso permite que você use seu sistema de gerenciamento de identidade existente para autenticação do usuário.

Pré-requisitos

Antes de configurar a integração de provedores de identidade de terceiros, certifique-se de que os usuários do seu provedor de identidade tenham atributos de nome, e-mail e nome de usuário configurados

Informações armazenadas

Quando você usa o AWS Transform with IdPs, AWS armazena o mínimo de informações do usuário que são criptografadas e protegidas:

Informações armazenadas do usuário

AWS O Transform armazena informações básicas do perfil do usuário no primeiro login, incluindo nome de exibição, endereço de e-mail, nome de usuário (preferred_username) e um identificador

de usuário exclusivo. Essas informações são criptografadas usando uma chave KMS de propriedade do cliente ou uma chave de propriedade do serviço, dependendo da configuração do perfil Transform do cliente. AWS Os dados são armazenados no banco de dados de autenticação do AWS Transform e são coletados somente durante a sessão inicial de login. Isso preenche os resultados da pesquisa ao convidar outros usuários para um espaço de trabalho.

Ciclo de vida dos dados

As informações do usuário são armazenadas somente para usuários que fizeram login no aplicativo web AWS Transform pelo menos uma vez e podem ficar obsoletas se os usuários atualizarem suas informações no provedor de identidade sem fazer login AWS novamente no Transform. Todas as informações armazenadas do usuário são excluídas quando o perfil AWS Transform é excluído.

Armazenamento secreto do cliente

O segredo do cliente fornecido durante a configuração é armazenado AWS Secrets Manager usando um Segredo Vinculado ao Serviço (SLS) em sua conta.

Tratamento de identificadores de usuário

Entra

Usa a declaração “oid” (identificador de objeto) como identificador de usuário exclusivo, que é imutável e identifica de forma exclusiva os usuários em todo o locatário da Microsoft. Esse valor é visível para os clientes no console do Entra e aparece nos CloudTrail registros.

Identidade da força de trabalho da Okta

Usa declarações diferentes para identificação do usuário, dependendo do tipo de token: a declaração “sub” nos tokens de ID e a declaração “uid” nos tokens do Access. AWS A transformação valida que ambas as declarações contêm o mesmo valor durante a autenticação. Esse valor é visível para os clientes no console do Okta e aparece nos CloudTrail registros.

Configurando o Azure Active Directory (Inserir ID)

Para configurar a integração do Azure Active Directory com o AWS Transform:

1. Navegue até o portal do Azure e selecione Azure Active Directory.
2. No painel de navegação esquerdo, escolha Gerenciar > Registros de aplicativos.

3. Escolha + Novo registro.
4. Insira o nome do aplicativo, escolha o tipo de conta compatível, deixe o URI de redirecionamento em branco e escolha Registrar.
5. No painel de navegação à esquerda, escolha Gerenciar > Manifesto.
6. Atualize `requestedAccessTokenVersion` de `null` para 2 e escolha Salvar.
7. Escolha Gerenciar > Expor uma API e escolha Adicionar um escopo.
8. Crie um URI de ID do aplicativo usando a estrutura padrão `api://<client-id>`.
9. Adicione o escopo `transform:read_write`.
10. Escolha Adicionar um certificado ou segredo e crie um novo segredo de cliente. Salve esse valor conforme necessário para a criação do perfil.
11. Encontre o URL do emissor escolhendo Endpoints e selecionando o documento de metadados do OpenID Connect. O campo “emissor” nos metadados é o URL do emissor.
12. Crie um perfil no console do AWS Transform usando o ID do cliente, o segredo do cliente e o URL do emissor.
13. Após a criação do perfil, adicione um URI de redirecionamento escolhendo Adicionar uma plataforma, selecionando Web e inserindo `<web-application-url>/login/callback`.

Configurando o Okta Workforce Identity

Para configurar a integração do Okta Workforce Identity com AWS o Transform:

1. Navegue até o console do Okta Workforce Identity.
2. Escolha Aplicativos > Aplicativos e selecione Criar integração de aplicativos.
3. Selecione OIDC - OpenID Connect and Web Application e escolha Avançar.
4. Nomeie seu aplicativo, deixe o Tipo de concessão como código de autorização, deixe os URIs de redirecionamento em branco, configure as atribuições do usuário e escolha Salvar.
5. Navegue até a guia Login e defina o Emissor como URL Okta em vez de Dinâmico.
6. Copie o ID do cliente e configure-o como o público do seu servidor de autorização acessando Segurança > API e adicionando um servidor de autorização.
7. No Servidor de Autorização, adicione o escopo na `transform:read_write` guia Escopos.
8. Adicione uma política de acesso que permita que o aplicativo OIDC use esse servidor de autorização e configure uma regra para a política.

9. Na página Configurações do servidor de autorização, observe a URL do emissor para a criação do perfil no AWS Transform.
10. Crie um perfil no AWS Transform usando o URL do emissor, o ID do cliente e o segredo do cliente nas configurações do aplicativo.
11. Após a criação do perfil, adicione `<web-application-url>/login/callback` como URL de redirecionamento na guia Geral do aplicativo.

Note

Se você quiser ser redirecionado de volta para o aplicativo web AWS Transform após o logout, você precisará configurar o URL do seu aplicativo web como uma origem confiável em Segurança > API.

Integração de usuários

Esta seção descreve a experiência dos usuários que receberam acesso ao AWS Transform.

Aceitando o convite

Quando um usuário é adicionado ao AWS Transform, ele recebe um convite por e-mail contendo:

- Uma saudação e informações sobre o convite
- O URL do aplicativo web AWS Transform
- Seu nome de usuário
- Um link para aceitar o convite e configurar sua senha

Para configurar a conta deles:

1. O usuário clica no link “Aceitar convite” no e-mail.
2. Na página “Registro de novo usuário”, eles inserem e confirmam uma senha.
3. A senha deve atender aos requisitos de segurança, incluindo:
 - Pelo menos 8 caracteres
 - Pelo menos uma letra maiúscula
 - Pelo menos uma letra minúscula

- Pelo menos um número
 - Pelo menos um caractere especial
4. Depois de criar uma senha, eles recebem uma confirmação de que a conta foi criada com sucesso.

Fazendo login em AWS Transformação

Para fazer login no AWS Transform:

1. Navegue até o URL do aplicativo web AWS Transform fornecido no e-mail de convite.
2. Insira o nome de usuário.
3. Escolha Próximo.
4. Digite a senha.
5. Escolha Logon.

Experiência bem-vinda

No primeiro login, os usuários veem a página de boas-vindas do AWS Transform com:

- Uma saudação personalizada
- Capacidades de transformação disponíveis
- Opção para criar um espaço de trabalho

A página de boas-vindas fornece informações sobre os recursos de transformação disponíveis no AWS Transform, incluindo:

- Modernize as z/OS migrações da IBM para AWS
- Migre cargas de trabalho da VMware para o Amazon EC2
- Modernize aplicativos.NET para Linux-ready transformar.NET multiplataforma
- Avalie as cargas de trabalho quanto à prontidão para a migração

Os usuários podem começar criando um espaço de trabalho ou pedindo à equipe que o adicione a um espaço de trabalho existente.

Usando seu próprio bucket Amazon S3

Por padrão, o AWS Transform usa um bucket Amazon S3 gerenciado por serviços para armazenar artefatos de transformação. Em vez disso, você pode optar por usar seu próprio bucket do Amazon S3 para ter maior controle sobre armazenamento de dados, criptografia e políticas de acesso.

Note

Se você tiver um bucket Amazon S3 para transformações de mainframe, poderá continuar usando esse conector S3 e não precisará usar essa funcionalidade.

Note

Seu bucket do Amazon S3 armazena somente os uploads e artefatos de transformação com os quais você interage. Artefatos internos gerados pelo sistema não são armazenados em seu bucket. Além disso, o AWS Transform indexa os artefatos em seu bucket. Ele armazena os dados indexados em uma base de conhecimento gerenciada por serviços que é usada para fornecer a você uma experiência de bate-papo enriquecida.

Pré-requisitos

Antes de configurar seu próprio bucket do Amazon S3, certifique-se de que os seguintes requisitos sejam atendidos:

- O bucket deve estar na mesma AWS região em que a AWS transformação está ativada.
- A política de bucket necessária deve ser aplicada ao seu bucket. Para obter mais informações, consulte [the section called “Política de bucket necessária”](#).
- Se você usa o aplicativo web AWS Transform, o CORS deve ser configurado em seu bucket. Para obter mais informações, consulte [the section called “Configuração CORS necessária”](#).
- Se você usar uma chave AWS KMS personalizada, a política de chaves necessária deverá ser aplicada. Para obter mais informações, consulte [the section called “Política de chaves do KMS \(opcional\)”](#).

Configurações de criptografia suportadas

Seu bucket deve usar uma das seguintes configurações de criptografia:

- SSE-S3 (AES256) — Deixe o campo da chave KMS vazio. AWS O Transform grava objetos sem especificar um cabeçalho de criptografia, e o Amazon S3 aplica a criptografia S3-managed padrão do bucket com chaves. Para obter mais informações, consulte [Uso da criptografia do lado do servidor com chaves gerenciadas do Amazon S3 \(\) SSE-S3 no Guia do usuário do Amazon S3](#).
- SSE-KMS com uma chave KMS gerenciada pelo cliente — forneça o ARN da chave KMS. AWS O Transform grava objetos `x-amz-server-side-encryption: aws:kms` usando a chave fornecida. Confira [the section called “Política de chaves do KMS \(opcional\)”](#).

Não há suporte para o seguinte:

- SSE-KMS com uma chave KMS AWS gerenciada (por exemplo,) `aws/s3`
- SSE-C
- DSSE-KMS
- Chaves KMS assimétricas ou chaves KMS com uma especificação de chave diferente de `SYMMETRIC_DEFAULT`

 Warning

AWS- as chaves KMS gerenciadas não são suportadas. Se seu bucket estiver criptografado com `aws/s3`, migre para uma chave gerenciada pelo cliente ou SSE-S3 antes de usar o bucket com o Transform. AWS

Configurando seu bucket Amazon S3

Você pode configurar o AWS Transform para usar seu próprio bucket do Amazon S3 a partir do console do AWS Transform.

Para usar seu próprio bucket Amazon S3

1. No console do AWS Transform, escolha Configurações.
2. Em Armazenamento de artefatos, escolha Usar meu próprio bucket do S3. Você pode usar um bucket na sua conta atual Conta da AWS ou em outra conta.
3. Para Bucket, insira o URI do Amazon S3.
4. (Opcional) Em Chave KMS, insira um ARN da chave AWS KMS para criptografar objetos no bucket. Se você deixar esse campo vazio, o AWS Transform grava objetos sem um cabeçalho

de criptografia, e o Amazon S3 aplica as configurações de criptografia padrão do bucket. Para obter mais informações, consulte [Definir o comportamento padrão da criptografia para os buckets do Amazon S3](#) no Guia do usuário do Amazon S3.

Se a criptografia padrão do seu bucket for SSE-KMS, insira o ARN da chave KMS gerenciada pelo cliente nesse campo e atualize sua política de chaves. Para obter mais informações, consulte [the section called “Política de chaves do KMS \(opcional\)”](#).

5. Escolha Salvar. AWS O Transform valida a configuração e as permissões do bucket antes de aplicar a configuração.

Depois de salvar a configuração, o AWS Transform usa seu bucket para armazenar artefatos de transformação.

Note

AWS O Transform valida sua configuração somente quando você salva. Se você alterar posteriormente a política de bucket, a configuração do CORS ou a política de chaves do KMS, salve novamente suas configurações de perfil para revalidá-las.

Política de bucket necessária

Você deve configurar a política do bucket para conceder acesso ao AWS Transform. Adicione a seguinte política de bucket ao seu bucket do Amazon S3 para permitir que o responsável pelo serviço AWS Transform leia, grave, exclua e liste artefatos de transformação.

```
{
  "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"
        }
    }
}
]
}

```

Substitua os valores a seguir:

- *bucket-name*— O nome do seu bucket Amazon S3.
- *profile-account-id*— O Conta da AWS ID associado ao seu perfil do AWS Transform.
- *profile-arn*— O ARN do seu perfil AWS Transform.

Configuração CORS necessária

Se você usa o aplicativo web AWS Transform, deve configurar o compartilhamento de Cross-Origin recursos (CORS) no seu bucket do Amazon S3. Você pode encontrar o domínio do aplicativo web depois de ativar o AWS Transform. Para obter mais informações, consulte [Introdução](#).

```
[
  {
    "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
  }
]
```

Substitua os valores a seguir:

- **webapp-domain**— O URL de origem do seu aplicativo web (por exemplo, `https://1a2b3c4d5e6f7a8b9.transform.us-east-1.on.aws`), que pode ser encontrado na página de configurações do AWS Transform. Não inclua a barra final.

Política de chaves do KMS (opcional)

Esta seção se aplica somente quando seu bucket é criptografado com uma chave KMS gerenciada pelo cliente. Se o seu bucket usa SSE-S3, pule esta seção.

Se você especificar sua própria chave AWS KMS para criptografia de bucket, adicione a seguinte declaração à sua política de chaves. AWS A Transform conta com o Forward Access Sessions (FAS) para criar subsídios para seu diretor de serviço. Essas concessões são usadas para validar sua chave e acessar artefatos em seu bucket do Amazon S3.

```
{
  "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"
    }
  }
}
```

Substitua os valores a seguir:

- **key-owner-account-id**— O Conta da AWS ID que possui a chave KMS.
- **region**— A AWS região em que a AWS transformação está ativada (por exemplo, `us-east-1`).

Voltando ao bucket padrão

Você pode voltar para o bucket gerenciado por serviços a qualquer momento.

Para mudar para AWS Transforme o armazenamento gerenciado

1. No console do AWS Transform, escolha Configurações.
2. Em Armazenamento de artefatos, escolha Editar.
3. Escolha AWS Transformar armazenamento gerenciado.
4. Escolha Salvar.

Warning

Se você alternar as configurações de armazenamento enquanto os trabalhos de transformação estão em andamento, esses trabalhos falharão. Todos os artefatos que já foram gerados por esses trabalhos em andamento também não estariam acessíveis.

Important

Quando você volta para o bucket gerenciado pelo serviço:

- Os artefatos em seu bucket não são migrados automaticamente. Para reter quaisquer artefatos, baixe-os do seu bucket do Amazon S3 e recarregue-os por meio AWS do aplicativo web Transform para o armazenamento de artefatos para o espaço de trabalho e o trabalho correspondentes.
- AWS O Transform retira sua concessão em sua chave KMS. Os objetos gravados no seu bucket permanecem no seu bucket; exclua-os manualmente se não forem mais necessários.

Fazer upload de arquivos diretamente para o seu bucket

Você pode fazer upload de arquivos diretamente para seu bucket do Amazon S3 sem usar o aplicativo web AWS Transform. Para disponibilizar os arquivos enviados aos agentes de transformação, carregue-os User Uploads na pasta do trabalho. O caminho do diretório para essa pasta usa o seguinte formato:

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

Substitua os valores a seguir:

- *workspace-id*— O ID do seu espaço de trabalho AWS Transform.
- *job-id*— O ID do trabalho de transformação.

Cada trabalho no AWS Transform tem sua própria User Uploads pasta. Os arquivos que você carrega para esse caminho aparecem no aplicativo web e estão disponíveis para os agentes de transformação enquanto eles concluem o trabalho.

Os caminhos dos arquivos não devem conter . . espaços à esquerda ou à direita — os arquivos que violam essas restrições não são visíveis para os agentes. //

Important

Se seu bucket usar SSE-KMS, inclua os seguintes cabeçalhos em cada upload direto:

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

Os objetos devem ser criptografados com a chave KMS registrada em seu perfil do AWS Transform. Objetos criptografados com qualquer outra chave não estão acessíveis ao AWS Transform.

Matriz de compatibilidade

A tabela a seguir resume a compatibilidade do AWS Transform com recursos comuns de bucket do Amazon S3.

Recurso	Compatibilidade	Observações
Bucket versioning	Compatível	Gerencie versões não atuais com uma regra de ciclo de vida.
Propriedade de Objeto	Obrigatório: obrigatório pelo proprietário do bucket	O proprietário do bucket preferencial e o gravador de objetos não são compatíveis.
ACL	Não compatível	As ACLs devem estar desativadas no bucket.

Recurso	Compatibilidade	Observações
Bloqueio de objetos (modo de governança)	Suporte parcial	As exclusões podem ser bloqueadas pelas configurações de retenção.
Bloqueio de objetos (modo de conformidade)	Não compatível	—
Bloqueio de Acesso Público	Compatível	—
Requester Pays (Pagamento pelo solicitante)	Não compatível	—
Pontos de acesso do S3	Não compatível	Use o nome do bucket.
Pontos de Acesso do S3 Object Lambda	Não compatível	Use o nome do bucket.
S3 on Outposts	Não compatível	—
S3 Express One Zone (buckets de diretório)	Não compatível	—
Cross-Region baldes	Não compatível	—
Cross-account baldes	Compatível	—
Cross-account Chaves KMS	Não compatível	—
Regras de ciclo de vida	Compatível	—
CloudTrail eventos de dados	Compatível	—

Enable (Habilitar) AWS Transformação

Para ativar o AWS Transform:

1. Faça login no AWS Management Console.
2. Na barra de pesquisa na parte superior do console, pesquise por AWS Transform.
3. Selecione AWS Transformar nos resultados da pesquisa.
4. Escolha Começar para ativar o serviço na sua região atual.
5. Opcional: configure o IAM Identity Center. Você também poderá optar por usar um [provedor de identidade terceirizado \(IdP\)](#) em uma etapa posterior.
6. Selecione uma chave de criptografia: chave AWS gerenciada padrão ou Personalize as configurações de criptografia.
7. Opcional: use seu próprio bucket do Amazon S3. Por padrão, o AWS Transform usa um bucket Amazon S3 gerenciado por serviços para armazenar artefatos de transformação. Em vez disso, você pode optar por usar seu próprio bucket. Para obter mais informações, consulte [Usando seu próprio bucket Amazon S3](#).
8. Escolha quais recursos do AWS Transform você deseja ativar:
 - Interface de linha de comando (CLI), necessária para criar e executar transformações [personalizadas](#). Para habilitar a CLI, veja e siga as instruções de download.
 - Aplicativo web, a interface de usuário agente para modernização. Escolha Habilitar aplicativo web para usá-lo.
9. Escolha Ativar AWS transformação.
10. Opcional: escolha Ativar perfil de exibição para acessar as guias AWS Transformar usuários, configurações e conectores ou Gerenciar usuários para gerenciar usuários.

Você pode acessar as guias Usuários, Configurações e Conectores a qualquer momento escolhendo o ícone do menu no canto superior esquerdo do console.
11. Configure o acesso do usuário escolhendo uma das seguintes opções:
 - Centro de Identidade do IAM
 - Um [provedor de identidade terceirizado \(IdP\)](#)
 - [IAM-only access](#)

 Note

Essa opção é finalizada e não pode ser alterada quando você ativa a AWS Transformação.

12. Escolha Ativar aplicativo web.
13. O sistema exibe “Ativando a AWS transformação” enquanto cria os recursos necessários.

Depois que a AWS Transformação estiver ativada, a guia Configurações exibirá as seguintes informações:

- URL do aplicativo Web - O URL para acessar o aplicativo web AWS Transform
- URL inicial do IDE - A URL para acessar o AWS Transform em ambientes de desenvolvimento integrados
- Região - A AWS região em que o AWS Transform está ativado

Início rápido: Experimentando AWS Transformação

A maneira mais fácil de experimentar o AWS Transform é com uma AWS conta independente. Talvez você queira fazer isso como prova de conceito ou para ambientes de teste. Use este procedimento:

1. Faça login no AWS Management Console.
2. Navegue até o serviço AWS Transform.
3. Escolha Começar para ativar o serviço.
4. Selecione e configure seu provedor de identidade.
5. Atribua usuários ao serviço AWS Transform.
6. Depois que o serviço for ativado, você verá a URL do aplicativo web AWS Transform.
7. Abra esse URL em uma nova janela do navegador para acessar a experiência web do AWS Transform.

Agora você está pronto para configurar seu espaço de trabalho.

Gerenciamento de usuários

A forma como você gerencia o acesso do usuário ao AWS Transform depende do modelo de acesso escolhido durante a configuração. Se você configurou o IAM Identity Center, você adiciona usuários por meio do IAM Identity Center. Se você configurou um provedor de identidade terceirizado, gerencia os usuários desse provedor. Se você escolher o IAM-only acesso, o acesso do usuário será gerenciado por meio de políticas do IAM.

Adicionar usuários no IAM Identity Center

Para adicionar usuários no IAM Identity Center:

1. Navegue até o console do Centro de identidade do IAM.
2. No painel de navegação, escolha Users (Usuários).
3. Escolha Add user (Adicionar usuário).
4. Insira as informações necessárias:
 - Nome de usuário - Um identificador exclusivo para o usuário (não pode ser alterado posteriormente)
 - Endereço de e-mail - O endereço de e-mail do usuário
 - Nome e sobrenome - O nome do usuário
 - Nome de exibição - O nome que aparece na lista de usuários
5. Em Senha, escolha como o usuário receberá sua senha:
 - Envie um e-mail - Envie instruções de configuração por e-mail
 - Gere uma senha de uso único - Crie uma senha para compartilhar manualmente
6. Escolha Avançar para revisar as informações do usuário.
7. Revise os detalhes e escolha Adicionar usuário.

Depois que o usuário for adicionado, ele receberá um convite por e-mail para configurar sua conta do IAM Identity Center. O link do convite é válido por 7 dias.

Você também pode aprender sobre como trabalhar com o IAM Identity Center and AWS Transform neste vídeo:

[VideoTitle](#)

Adicionando usuários ao AWS Transformação

Depois de adicionar usuários ao IAM Identity Center, você pode conceder a eles acesso ao AWS Transform:

1. Retorne ao console do AWS Transform.
2. No painel de navegação, escolha Usuários e grupos.
3. Selecione a guia Usuários ou a guia Grupos.
4. Pesquise e selecione os usuários ou grupos que você deseja adicionar do IAM Identity Center.
5. Escolha Atribuir usuários e grupos para conceder aos usuários ou grupos selecionados acesso ao AWS Transform.

Depois de adicionar usuários, eles aparecem na lista de Usuários com o status “Pendente” até aceitarem o convite e entrarem.

Gerenciando usuários com IAM-only acesso

Se você configurou o AWS Transform com IAM-only acesso, o acesso do usuário é gerenciado por meio de políticas do IAM. Qualquer diretor do IAM com a `transform:AccessTransformProfile` permissão no recurso de perfil pode acessar o AWS Transform.

Para conceder a um usuário ou função acesso ao AWS Transform:

1. Navegue até o console do IAM.
2. Anexe uma política que inclua a `transform:AccessTransformProfile` ação ao usuário ou função do IAM. Para ver um exemplo de política, consulte [Permitir que os usuários acessem o AWS Transform com credenciais do IAM](#).

Para revogar o acesso, remova a política do usuário ou da função do IAM.

Entendendo as permissões dos colaboradores

AWS O Transform usa um modelo de permissão baseado em espaço de trabalho para controlar o acesso a recursos e ações. Cada usuário recebe uma função específica em um espaço de trabalho, que determina quais ações eles podem realizar. Um usuário pode ter funções diferentes em diferentes espaços de trabalho.

Perfis de usuário

AWS O Transform oferece suporte a cinco funções de usuário em cada espaço de trabalho. Essas funções se aplicam ao contexto de um espaço de trabalho, e um usuário receberá funções em cada espaço de trabalho do qual for membro. As permissões de acesso definidas para cada função são independentes do espaço de trabalho, portanto, o usuário A com a função Administrador no espaço de trabalho A tem as mesmas permissões que o usuário B com a função Administrador no espaço de trabalho B.

Permissões de perfil

Permissões detalhadas para cada função:

Ação	ResourceType	Administrador	Aprovador	Colaborador	ReadOnly
Criar	Espaço de trabalho	✓	✓	✓	✓
Lista	Espaço de trabalho	✓	✓	✓	✓
Obtenção	Espaço de trabalho	✓	✓	✓	✓
Atualizar	Espaço de trabalho	✓	✗	✗	✗
Delete	Espaço de trabalho	✓	✗	✗	✗
Criar	ChatMessage	✓	✓	✓	✗
Ler	ChatMessage	✓	✓	✓	✓
Criar	RoleAssociation	✓	✗	✗	✗
Ler	RoleAssociation	✓	✓	✓	✓
Atualizar	RoleAssociation	✓	✗	✗	✗
Delete	RoleAssociation	✓	✗	✗	✗
Ler	Tarefa crítica de HITL	✓	✓	✓	✓
Atualizar	Tarefa crítica de HITL	✓	✓	✗	✗

Ação	ResourceType	Administrador	Aprovador	Colaborador	ReadOnly
Delete	Tarefa crítica de HITL	✓	✓	✗	✗
Ler	Tarefa HITL	✓	✓	✓	✓
Atualizar	Tarefa HITL	✓	✓	✓	✗
Delete	Tarefa HITL	✓	✓	✓	✗
Criar	Trabalho	✓	✓	✓	✗
Ler	Trabalho	✓	✓	✓	✓
Atualizar	Trabalho	✓	✓	✓	✗
Delete	Trabalho	✓	✓	✓	✗
Ler	Log de trabalho	✓	✓	✓	✓
Criar	Artifact	✓	✓	✓	✗
Ler	Artifact	✓	✓	✓	✓
Atualizar	Artifact	✓	✓	✓	✗
Delete	Artifact	✓	✓	✓	✗
Criar	Conector	✓	✓	✓	✗
Ler	Conector	✓	✓	✓	✓
Atualizar	Conector	✓	✓	✓	✗
Delete	Conector	✓	✓	✓	✗

Human-in-the-loop ações (HITL)

AWS O Transform fornece dois tipos de ações de HITL: padrão e crítica:

Ações padrão do HITL

Essas são ações rotineiras que podem ser executadas por usuários com funções de Colaborador, Aprovador ou Administrador.

Ações críticas do HITL

Essas são ações com impacto significativo e, portanto, exigem níveis de permissão mais altos. Os exemplos incluem:

- Mesclando código com as filiais principais
- Executando a decomposição do gráfico
- Implantação de código em ambientes de produção

As ações críticas do HITL só podem ser executadas por usuários com funções de Aprovador ou Administrador.

Para garantir que haja uma diferenciação entre as ações de HITL padrão e de HITL crítico nas políticas do AuthZ, o AWS Transform fornece duas APIs de HITL separadas, uma para concluir uma ação padrão de HITL e outra para concluir uma ação crítica de HITL.

AWS Transforme o ambiente

AWS O Transform é um serviço agente que usa processamento de linguagem natural para ajudá-lo a planejar e executar suas transformações de carga de trabalho. Você interage com o AWS Transform principalmente por meio de uma interface conversacional, na qual o serviço se adapta e responde com base no contexto de sua discussão. Por exemplo, você pode começar descrevendo sua arquitetura atual e suas metas de transformação usando uma linguagem comum, como “Preciso migrar minhas VMs locais para o EC2”.

Conforme você conversa com o AWS Transform, o serviço cria um plano de trabalho personalizado que se alinha às suas necessidades específicas. O fluxo da conversa é dinâmico e conduzido por você, permitindo que você refine seu plano de transformação de forma iterativa. Você pode modificar o plano de trabalho durante a conversa fazendo solicitações como “adicionar uma fase de teste antes da transição da produção” ou “remover a etapa de backup, pois já temos uma solução”. Você também pode voltar para uma tarefa anterior e executá-la novamente. AWS O Transform atualiza continuamente o plano com base em suas informações, garantindo que a estratégia final de transformação atenda às suas necessidades técnicas e comerciais.

Veja o que você vê ao abrir o AWS Transform.

- Exibir painel de controle: esse é o painel estreito à esquerda do AWS Transform. Você pode escolher um dos ícones para escolher qual exibição será mostrada à direita do painel de controle de exibição. Passe o mouse sobre cada ícone para ver uma dica de ferramenta explicando a exibição. As visualizações padrão fornecidas, de cima para baixo, são:
 - Plano de trabalho
 - Painel
 - Aprovações
 - Artefatos
 - Registro de trabalho

Alguns fluxos de trabalho oferecem visualizações adicionais.

Quando você está trabalhando em um plano de trabalho, as visualizações são:

- Chat
- Aprovações
- Loja de artefatos
- Registro de trabalho

Quando você está em um espaço de trabalho, as visualizações estão na parte superior:

- Trabalhos
- Artefatos
- Colaboradores (Usuários)
- Conectores
- Configurações
- O painel Exibir fica ao lado dos controles de exibição.
- O painel Chat está no centro. É aqui que você conduz sua conversa com o AWS Transform.

 Note

Usuários com permissões somente de leitura não conseguem enviar mensagens no chat.

- À direita está o painel Colaboração. Isso aparece quando atividades humanas no circuito (HITL) são realizadas, como:

- Carregando arquivos de dados
- Analisando as informações e os planos fornecidos pela Transform AWS

Configurações de idioma

AWS O Transform oferece suporte à localização para fluxos de trabalho selecionados. Você pode alterar o idioma de exibição do aplicativo web escolhendo o ícone Configurações no canto superior direito e selecionando seu idioma preferido no menu Idioma.

Há suporte para os seguintes idiomas:

- Inglês (EUA)
- Inglês (Reino Unido)
- Deutsch (Alemão)
- Español (Espanhol)
- Français (Francês)
- 394 (Japonês)
- Bahasa Indonesia (indonésio)
- Italiano (Italiano)
- Português (Português)
- (Coreano)
- () (Chinês simplificado)
- () (Chinês tradicional)
- Türkçe (Turco)

Os fluxos de trabalho a seguir oferecem suporte à localização:

- [Migrações \(incluindo VMware\)](#)

 Note

No momento, outros fluxos de trabalho do AWS Transform estão disponíveis somente em inglês. O suporte de localização para fluxos de trabalho adicionais pode ser adicionado em futuras atualizações.

Comece seu projeto

AWS O Transform orienta você em seus projetos de modernização e migração. Para começar:

1. Crie um espaço de trabalho para hospedar seu projeto. Na página Espaços de trabalho, escolha Criar espaço de trabalho. Siga as instruções e abra o espaço de trabalho.
2. No painel Chat, digite “criar um trabalho”
3. Escolha um trabalho e siga as instruções fornecidas pelo AWS Transform. Se sua entrada for necessária, o painel Colaboração será exibido e explica o que é necessário.

flexibilidade do fluxo de trabalho

O ambiente de fluxo de trabalho AWS Transform oferece flexibilidade na progressão de seus projetos de modernização. Usando a linguagem natural no painel de bate-papo, você pode:

- Tente novamente uma tarefa que o AWS Transform já tenha concluído, fornecendo diferentes informações humanas no circuito ao longo do caminho.
- Execute novamente um trabalho, por exemplo, se houver mudanças em suas fontes de modernização.

Conversando com AWS Transformação

AWS O bate-papo do Transform está disponível em todas as etapas do seu projeto. Para abrir o bate-papo, clique no ícone hexagonal roxo no canto inferior direito do console web.

O chat está aí para você perguntar qualquer coisa. Por exemplo, você pode pedir ao chat que explique conceitos, oriente você em um processo, explique uma solicitação ou resposta do AWS Transform ou explique um relatório do AWS Transform.

 Note

Usuários com permissões somente de leitura não conseguem enviar mensagens no chat.

AWS Transforme as integrações de bate-papo

AWS O Transform chat está integrado com:

Experience-Based Aceleração

Experience-Based O [Acceleration \(EBA\)](#) é oferecido por meio do chat do AWS Transform. Ele permite que você realize uma avaliação do EBA para cargas de trabalho do Windows e gere um plano. Você pode começar importando os resultados da avaliação do CAST. Ele ajuda você a descobrir seu portfólio de aplicativos. Depois disso, você pode usar o chat do AWS Transform para selecionar aplicativos que atendam às suas necessidades comerciais (por exemplo, filtrar aplicativos com base na complexidade ou nas linhas de código). Em seguida, você pode realizar uma avaliação mais profunda do aplicativo selecionado e gerar um plano de modernização.

AWS Contagem regressiva Premium

AWS O [Countdown Premium](#) (CDP) integrado ao AWS Transform fornece orientação sustentada e especializada com suporte de engenharia designado AWS . Seu engenheiro de CDP designado mergulha profundamente em sua pilha de tecnologia, fornecendo suporte personalizado e contextual quando surgem problemas. Os usuários podem aproveitar o AWS Transform para registrar um ticket de suporte diretamente de sua interface de bate-papo. O ticket de suporte incorpora detalhes do registro de trabalho e do plano de trabalho para ajudar o suporte a entender o contexto do cliente. Se um cliente ou parceiro fizer parte do Programa CDP, o ticket de suporte será automaticamente encaminhado para o engenheiro designado do CDP, que pode ajudar a depurar problemas, interpretar os resultados da transformação e impulsionar o progresso para a resolução rápida de problemas. Por exemplo:

- Para cargas de trabalho do .NET, o CDP pode ajudar com problemas de conectores de repositórios, resolução de dependências e implantação pós-transformação.
- Em cenários de mainframe, o CDP pode ajudar a solucionar problemas de código Java refatorado, configurar ferramentas de migração de banco de dados e criar pipelines. CI/CD
- Nas migrações da VMware, o CDP pode acelerar a configuração da rede, a configuração da MGN e a instalação do agente.

AWS Construtor de habilidades

AWS O [Skill Builder](#) fornece módulos de aprendizagem relevantes por meio do chat. Você pode perguntar ao AWS Transform chat sobre suas necessidades de aprendizado e ele apresentará um catálogo de cursos relevante. O Skill Builder oferece experiências contextuais de microaprendizagem enquanto você trabalha nos estágios de transformação.

Ferramentas de desenvolvedor

Você pode acessar os agentes do AWS Transform a partir de IDEs agentes, plug-ins de agentes e do servidor MCP. Escolha a superfície que se adapta ao seu fluxo de trabalho.

Note

Os plug-ins Kiro Power e do agente instalam automaticamente o servidor MCP. Você só precisa instalar o servidor MCP manualmente se quiser usá-lo sem um plug-in Kiro Power ou agente.

Kiro Power

O [AWS Transform Kiro Power](#) fornece acesso total aos agentes AWS Transform a partir do Kiro IDE.

Para instalar o AWS Transform e o poder de Kiro

1. Abra o Kiro IDE e navegue até o painel Powers.
2. Encontre o AWS Transform na lista e instale-o.
3. Abra o Kiro Chat, clique em Power e selecione Try power.

Como alternativa, no painel Powers, escolha Adicionar energia personalizada > Importar energia de GitHub e cole: `https://github.com/kirodotdev/powers/tree/main/aws-transform`

Plugin de agente

O plug-in do agente AWS Transform está disponível em [awslabs/agent-plugins](#) on GitHub, no `plugins/aws-transform` diretório. O plugin suporta Claude Code, Codex e Cursor.

O plug-in inclui `.claude-plugin`, `.codex-plugin`, e `.mcp.json` configurações. Ele fornece acesso a todos os agentes do AWS Transform, como .NET, mainframe, VMware, SQL Server e transformações personalizadas.

Para instalar no Claude Code

Execute os seguintes comandos :


```
/plugin marketplace add awslabs/agent-plugins  
/plugin install aws-transform@agent-plugins-for-aws
```

Para instalar no Codex ou Cursor

Siga as instruções no repositório de plug-ins de agentes (README).

Plug-in IDE

O plug-in AWS Transform IDE está disponível nos editores compatíveis com VS Code e Open VSX. Ele expõe os recursos personalizados do AWS Transform, incluindo a criação e execução de definições de transformação. Também expõe os recursos do mainframe, incluindo a rastreabilidade entre os requisitos de modernização, as regras de negócios e o código-fonte, bem como a capacidade de gerar documentação técnica sob demanda. Para começar, instale usando um dos seguintes métodos:

- VS Code: instale a partir do [VS Code Marketplace](#).
- Abra o VSX: instale a partir do registro do [Open VSX](#).

Servidor MCP

Use o servidor MCP para integrar o AWS Transform programaticamente a qualquer cliente. MCP-compatible Você pode instalar o servidor MCP do PyPI como. `awslabs.aws-transform-mcp-server` Ele fornece 19 ferramentas para gerenciamento de espaço de trabalho, gerenciamento de tarefas, tarefas humanas-in-the-loop (HITL), manuseio de artefatos, gerenciamento de conectores, bate-papo e navegação de recursos.

Pré-requisitos

- Python 3.10 ou posterior

Instalação

Código Claude

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

Kiro

Adicionar a `~/.kiro/settings/mcp.json`:

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

Para obter detalhes de configuração para seu cliente MCP específico, consulte o README [aws-transform-mcp-server](#) em GitHub

Autenticação

AWS O Transform é compatível com SSO (AWS Identity and Access Management Identity Center) e autenticação baseada em funções do IAM.

SSO (Central de Identidade do IAM)

Peça ao seu assistente de IA para “Configurar o AWS Transform with SSO”. O assistente fornece uma URL inicial e abre seu navegador para login.

Perfil do IAM

Seu ambiente fornece AWS credenciais automaticamente. Defina `AWS_PROFILE` no env bloco de configuração do cliente MCP para selecionar um perfil específico.

Para obter informações sobre como configurar a autenticação para o AWS Transform, consulte [Conceitos básicos de AWS Transformação](#).

Crie agentes personalizados para AWS Transformação

O [kit de ferramentas do Agent Builder](#) permite que AWS parceiros e clientes criem agentes personalizados para suas necessidades específicas de modernização que funcionem no AWS Transform.

Para instalar o kit de ferramentas do Agent Builder

1. Abra o Kiro IDE e navegue até o painel Powers.
2. Encontre o AWS Transform Agent Toolkit na lista e instale-o.

Como alternativa, no painel Powers, escolha Adicionar energia personalizada > Importar energia de GitHub e cole: `https://github.com/kirodotdev/powers/tree/main/aws-transform-agent-toolkit`

O kit de ferramentas do Agent Builder permite que parceiros de competência em migração e modernização, ISVs ou clientes criem soluções de transformação para casos de uso específicos. Você pode integrar agentes, ferramentas, bases de conhecimento e fluxos de trabalho especializados com os recursos de IA do AWS Transform Agentic.

Ciclo de vida do agente

Criar

Use o Kiro Power para combinar o agente base e o SDK para criar seu próprio agente personalizado.

Compartilhar

Distribua agentes com equipes ou entre redes de parceiros.

Inscreva-se

Registre agentes no AWS Transform para serem descobertos por outros usuários.

Avaliações de migração

AWS As avaliações de transformação ajudam você a avaliar o custo, a viabilidade e o valor comercial da migração da infraestrutura local para o. AWS As avaliações fornecem recomendações automatizadas de dimensionamento correto, comparação de vários cenários e refinamento interativo por meio do chat.

Você pode usar as avaliações de migração para:

- Obtenha estimativas de custo do Amazon RDS for SQL Server, Amazon EC2, Amazon EBS, Amazon S3 e Amazon FSx
- Receba recomendações automatizadas de dimensionamento correto
- Avalie o valor comercial e o impacto na sustentabilidade
- Compare vários cenários de migração lado a lado
- Refine as avaliações de forma interativa por meio do chat
- Gere apresentações executivas e relatórios detalhados

Pré-requisitos

Antes de criar uma avaliação de migração, confirme se você tem o seguinte:

- Um espaço de trabalho AWS Transform
- Dados de inventário em um formato compatível, ou você pode usar uma estimativa aproximada por meio do chat
- Permissões apropriadas para criar e executar avaliações

Como funcionam as avaliações de migração

As avaliações de migração seguem um fluxo de trabalho estruturado que orienta você desde o carregamento inicial dos dados até a geração final do material de entrega.

Para concluir uma avaliação de migração

1. Crie um trabalho de avaliação de migração em seu espaço de trabalho do AWS Transform.
2. Carregue seus dados de inventário local.

3. Analise os resultados da descoberta que o AWS Transform gera a partir de seus dados.
4. Gerencie o escopo do inventário excluindo servidores ou ajustando agrupamentos.
5. Configure seu cenário de avaliação com premissas de preços e infraestrutura.
6. Execute a avaliação.
7. Analise e refine os resultados por meio do chat.

Depois de analisar os resultados, você pode criar cenários adicionais, comparar cenários e gerar resultados, como apresentações e relatórios.

Carregando dados de inventário

AWS O Transform aceita dados de inventário de várias fontes. A tabela a seguir lista os formatos de dados compatíveis.

Fonte de dados	Description
AWS Exportação da Transform Discovery	Inventário automatizado de servidores descoberto pela ferramenta de descoberta AWS Transform
Ferramentas de RV	Exporta de ambientes VMware em formato Excel ZIP/CSV ou Excel. Tanto as exportações completas quanto Info-only as exportações v são suportadas.
Dados do CMDB	Exportações do banco de dados de gerenciamento de
Ferramentas de descoberta de parceiros	Dados das ferramentas de descoberta de AWS parceiros
Avaliador de migração	Arquivo Quick Insights do console do Migration Evaluator
Formato MPA	Arquivo de importação da avaliação do portfólio de migração
AWS Transformar modelo de dados	Arquivo do Microsoft Excel criado a partir do modelo AWS Transform Assessment Data

AWS O Transform identifica automaticamente o formato do arquivo durante a ingestão. O processo de ingestão valida seus dados, aceita dados parciais quando alguns campos estão ausentes e

oferece suporte a carregamentos incrementais. Você pode fazer upload de arquivos adicionais a qualquer momento para complementar seu inventário.

Analizando os resultados da descoberta

Depois que o AWS Transform processa seus dados de inventário, ele gera um resumo da descoberta. O resumo inclui as seguintes informações:

- Contagem de servidores por sistema operacional
- Avaria do servidor físico e virtual
- Detecção do SQL Server
- Resumos de armazenamento
- Avisos de qualidade de dados

Analise os resultados da descoberta para confirmar se o AWS Transform identificou corretamente sua infraestrutura antes de prosseguir com a avaliação.

Gerenciando o escopo do inventário

Depois de analisar os resultados da descoberta, você pode refinar o escopo da sua avaliação. Use as seguintes ações para gerenciar o escopo do seu inventário:

- Consulte o inventário para servidores ou cargas de trabalho específicos
- Excluir servidores do escopo da avaliação
- Analise os agrupamentos de servidores e as dependências de aplicativos
- Identifique cargas de trabalho do SQL Server para avaliação especializada

Configurando cenários de avaliação

Antes de executar uma avaliação, configure as suposições que o AWS Transform usa para gerar recomendações. Você pode modificar essas suposições a qualquer momento e executar novos cenários com configurações diferentes.

A tabela a seguir lista as categorias de suposições disponíveis.

Suposição	Description
Modelo de definição de preços	Database Savings Plans (para Amazon RDS for SQL Server) ou On-Demand Instâncias Reservadas
Alvo Região da AWS	O Região da AWS local onde você planeja hospedar as cargas de trabalho migradas
Exclusões de tipos de instância	Famílias ou tipos de instâncias do Amazon EC2 a serem excluídos das recomendações
Configuração do Amazon EBS	Tipo de volume e configurações de desempenho para armazenamento
Licenciamento do SQL Server	Traga sua própria mídia (BYOM) ou licença incluída (LI) para Amazon RDS for SQL Server; Licença incluída (LI) ou traga sua própria licença (BYOL) para SQL Server no EC2

Capacidades de avaliação

AWS As avaliações do Transform abrangem várias dimensões de sua migração. As seções a seguir descrevem cada capacidade de avaliação.

Dimensionamento correto do Amazon EC2

AWS O Transform analisa as especificações do seu servidor local e recomenda instâncias do Amazon EC2 de tamanho adequado. As recomendações levam em conta os requisitos de CPU, memória e desempenho.

Armazenamento Amazon EBS

AWS A Transform recomenda os tipos e configurações de volume do Amazon EBS com base em seus requisitos atuais de uso e desempenho de armazenamento.

Amazon FSx

AWS O Transform avalia as cargas de trabalho de armazenamento de arquivos e fornece recomendações para a migração do Amazon FSx, incluindo estimativas de custo para os tipos de sistema de arquivos Amazon FSx compatíveis.

Amazon RDS para SQL Server

AWS O Transform avalia o custo da migração de bancos de dados SQL Server locais para o Amazon RDS for SQL Server. Usando AI-powered agentes, o AWS Transform analisa seu ambiente SQL Server local e fornece um caso de negócios de migração completo em minutos, com recomendações de computação e memória compatíveis com seus requisitos de carga de trabalho, para que você evite o excesso de provisionamento e pague apenas pelo que precisa.

A avaliação do RDS para SQL Server inclui os seguintes recursos:

- Licenciamento Bring Your Own Media (BYOM), permitindo que você use suas licenças existentes do SQL Server
- Opções de licenciamento com licença incluída (LI)
- Otimização de custos usando Database Savings Plans, que oferecem até 20% de economia em comparação com os On-Demand preços
- Avaliação de elegibilidade para o AWS Migration Acceleration Program (MAP), que fornece créditos e suporte para compensar os custos de migração

Você pode iniciar sua avaliação do RDS for SQL Server com qualquer formato de dados compatível, incluindo exportações do RVTools, dados do banco de dados de gerenciamento de configuração (CMDB), exportações da ferramenta de descoberta AWS Transform e outras ferramentas de descoberta de terceiros. Crie cenários hipotéticos para comparar vários modelos de custo com suposições personalizadas, incluindo região, utilização de recursos e termos de preços.

Exemplos de prompts:

- “Estimar o custo da migração dos meus bancos de dados do SQL Server para o RDS for SQL Server”
- “Compare o preço do BYOM com o preço da licença incluída para o RDS para SQL Server”
- “Mostre-me as opções do Database Savings Plans para minhas cargas de trabalho do RDS”

Amazon EC2 SQL Server

AWS O Transform avalia as cargas de trabalho do SQL Server e fornece recomendações para executar o SQL Server no Amazon EC2, incluindo análise de licenciamento e mapeamentos de host dedicados.

On-premises preços

AWS O Transform estima seus custos locais atuais para fornecer uma linha de base para comparação com AWS os preços. Você pode fazer ajustes gerais de custo por meio do chat. On-premises os ajustes de custo são refletidos no relatório em PDF e nas respostas do bate-papo, mas não na exportação PPTX.

Exemplos de prompts:

- “Atualize o custo do servidor local para 500 USD por servidor por mês”
- “Adicione custos anuais de instalação de data center de \$50.000”

Sustentabilidade

AWS A Transform estima a redução da pegada de carbono resultante da migração para o AWS. Você pode explorar as métricas de sustentabilidade por meio do chat.

Experimente instruções como:

- “Mostre-me a redução estimada de carbono para essa migração”
- “Qual é a melhoria na eficiência energética das minhas cargas de trabalho AWS?”

Avaliação do valor comercial

AWS O Transform avalia o valor comercial mais amplo da migração, além da economia de custos de infraestrutura. A avaliação abrange a produtividade, resiliência e agilidade comercial da equipe.

Aqui estão alguns exemplos de solicitações:

- “Estime os ganhos de produtividade da equipe com a migração para AWS”
- “Quais melhorias de resiliência posso esperar após a migração?”

- “Mostre-me os benefícios da agilidade comercial dessa migração”

Custos de rede

AWS O Transform estima os custos relacionados à rede para sua migração, incluindo requisitos de transferência de dados e conectividade.

Custos de suporte

AWS O Transform inclui os custos do plano AWS Support na avaliação com base no nível de suporte selecionado.

Computação de usuário final

AWS O Transform avalia as cargas de trabalho de computação do usuário final e fornece recomendações para os serviços de computação do usuário AWS final.

Usando avaliações baseadas em bate-papo

Você pode interagir com o AWS Transform por meio do chat para criar e refinar avaliações. O chat suporta três modos de interação.

Você pode refinar sua avaliação de forma iterativa continuando a conversa. AWS O Transform mantém o contexto em todas as mensagens e atualiza os resultados da avaliação com base em sua opinião.

Estimativa aproximada com dados limitados

Você pode obter uma estimativa aproximada de custo descrevendo seu ambiente no chat sem fazer upload de arquivos de inventário detalhados. A estimativa aproximada é um recurso independente e não pode ser combinada com dados de inventário enviados ou enriquecimento de dados por meio do chat.

Você pode usar prompts como estes:

- “Tenho 200 servidores Windows e 150 servidores Linux, estime meus AWS custos”
- “Forneça uma estimativa aproximada da migração de 500 VMs para” AWS

- “Estime os custos de 50 servidores com uma média de 8 CPUs e 32 GB de RAM”

Adicionar inventário por meio do chat

Você pode fornecer detalhes do inventário diretamente pelo chat para complementar ou substituir os arquivos enviados.

Use prompts como os seguintes:

- “Inclua um servidor de banco de dados executando Oracle em 4 CPUs com 128 GB de RAM”
- “Adicione 20 servidores web executando Linux com 4 CPUs e 16 GB de RAM”

Modificando custos e adicionando serviços

Você pode ajustar os custos locais e adicionar AWS serviços à sua avaliação por meio do chat.

Exemplos de solicitações para ajustes locais:

- “Aumente os custos locais em 15% para contabilizar a próxima atualização de hardware”
- “Adicione custos anuais de manutenção de USD 100.000 à linha de base local”

Você também pode adicionar estimativas aproximadas de custo para AWS serviços que não são totalmente suportados pelas avaliações do AWS Transform. Isso fornece uma análise mais completa, mas essas estimativas são menos precisas do que as recomendações automatizadas.

- “Adicione custos AWS de Backup para todos os servidores migrados”
- “Inclua os custos de CloudWatch monitoramento da Amazon na estimativa”
- “Adicione os custos do AWS Direct Connect para uma conexão de 10 Gbps”

Comparando cenários

Você pode criar vários cenários de avaliação com diferentes suposições e compará-los para identificar a estratégia de migração ideal.

Criação de cenários

Experimente instruções como:

- “Crie um cenário BYOM para migrar bancos de dados do SQL Server para o RDS for SQL Server”
- “Crie um cenário com Database Savings Plans for RDS for SQL Server”
- “Crie um cenário de LI para todas as cargas de trabalho do SQL Server no EC2”
- “Crie um cenário com todas as cargas de trabalho em us-west-2”

Executando comparações

Aqui estão alguns exemplos de solicitações:

- “Mostre-me uma comparação de custos em todos os cenários”
- “Qual cenário tem o menor custo total de propriedade?”

What-if análise

Modele o impacto de mudanças específicas sem criar um cenário totalmente novo.

Exemplos de prompts:

- “E se eu mover minhas cargas de trabalho do SQL Server para o RDS for SQL Server em vez do EC2?”
- “Qual é a diferença de custo entre o BYOM e a licença incluída para o RDS para SQL Server?”
- “E se eu excluir os 50 menores servidores da migração?”
- “E se eu usar apenas instâncias otimizadas para armazenamento?”
- “Qual é o impacto da migração dos volumes gp3 para io2?”

Geração de resultados

Depois de concluir sua avaliação, você pode gerar resultados em vários formatos. A tabela a seguir descreve os formatos de saída disponíveis.

Formato	Description	Personalização
PPTX () PowerPoint	Apresentação executiva com resultados resumidos e recomendações	Estrutura fixa

Formato	Description	Personalização
XLSX (Excel)	Exportação detalhada de dados com recomendações em nível de servidor e detalhamento de custos	Estrutura fixa
PDF	Documento de relatório	Personalizável por meio do chat

Tópicos relacionados

- [Conceitos básicos](#)
- [Trabalhos personalizados](#)
- [Ferramenta de descoberta](#)

Personalizada

O que é AWS Transformar de forma personalizada?

AWS O Transform Custom usa IA agente para realizar a modernização em grande escala de software, código, bibliotecas e estruturas para reduzir a dívida técnica. Ele lida com diversos cenários, incluindo atualizações de versões de idiomas, migrações de API e serviços, atualizações e migrações de estruturas, refatoração de código e transformações específicas da organização.

Por meio do aprendizado contínuo, o agente melhora a cada execução e feedback do desenvolvedor, oferecendo transformações repetíveis e de alta qualidade sem exigir conhecimento especializado em automação.

Principais recursos

AWS O Transform custom fornece os seguintes recursos:

- Definição de transformação baseada em linguagem natural - Crie transformações personalizadas usando linguagem natural, documentação e exemplos de código
- Execução da transformação - aplique transformações de forma consistente e confiável em várias bases de código
- Aprendizado contínuo - Melhore automaticamente a qualidade da transformação em cada execução
- AWS-transformações gerenciadas - Use transformações aprovadas e prontas para uso em cenários AWS comuns

Padrões de transformação

AWS O Transform custom oferece suporte a diversos padrões de transformação para atender às suas necessidades de modernização. Cada padrão tem características de complexidade diferentes com base no escopo e na natureza das mudanças necessárias.

Padrão	Description	Complexidade	Exemplos
Migrações de API e serviços	Migração entre versões de API ou	Médio	AWS SDK v1→v2 (Java, Python,)

Padrão	Description	Complexidade	Exemplos
	serviços equivalentes, mantendo a funcionalidade		Boto2→Boto3, JUnit 4→5, JavaScript javax→jacarta
Atualizações de versão de idioma	Atualização para versões mais recentes da mesma linguagem de programação, adoção de novos recursos e substituição de funcionalidades obsoletas	Low-Medium	Java 8→17, Python 3.9→3.13, 12→22, atualizações de versão Node.js TypeScript
Atualizações da estrutura	Atualização para versões mais recentes da mesma estrutura, abordando mudanças significativas	Médio	Spring Boot 2.x→3.x, React 17→18, atualizações Angular, atualizações do Django
Migrações de estrutura	Migração para estruturas totalmente diferentes que atendem a propósitos semelhantes	Alto	Angular→React, Redux→Zustand, →React Vue.js
Atualizações de bibliotecas e dependências	Atualizando bibliotecas de terceiros para versões mais recentes, mantendo a mesma linguagem e estrutura	Low-Medium	Pandas 1.x→2.x, atualizações, atualizações de bibliotecas, NumPy atualizações do Lodash Hadoop/HBase/Hive

Padrão	Description	Complexidade	Exemplos
Refatoração de código e modernização de padrões	Modernizando padrões de código e adotando as melhores práticas sem alterar a funcionalidade externa	Low-Medium	Imprimir→Estruturas de registro, concatenação de strings→f-strings, adoção de dicas de tipo, instrumentação de observabilidade
Roteiro e File-by-File traduções	Traduzindo scripts independentes ou arquivos de configuração em que os arquivos são, em sua maioria, independentes	Low-Medium	AWS CDK → Terraform, Terraform →, Excel → notebooks Python, Bash CloudFormation → PowerShell
Migrações de arquitetura	Migração entre arquiteturas de hardware ou ambientes de execução com o mínimo de alterações de código	Medium-High	x86 →AWS Graviton (ARM), no local → Lambda, servidor tradicional → contêineres
Language-to-Language Migrações	Traduzindo bases de código de uma linguagem de programação para outra	Muito alto	Java→Python, →, C→Rust, JavaScript Python→Go TypeScript

Padrão	Description	Complexidade	Exemplos
Personalização e Organization-Specific transformações	Requisitos organizacionais exclusivos e necessidades especializadas de modernização	Varia	Migrações personalizadas de bibliotecas internas, padrões de codificação específicos da organização, migrações de estruturas proprietárias

 Note

Para COBOL/mainframe idiomas, use AWS Transform for Mainframe. Para atualizações do.NET Framework para o.NET Core, considere o AWS Transform for Windows. Para migrações da VMware para AWS, considere o AWS Transform for VMware.

Como AWS Transforme trabalhos personalizados

AWS O Transform custom geralmente é usado em projetos de grande escala em que várias bases de código ou módulos são transformados. As equipes normalmente seguem um fluxo de trabalho de quatro fases:

Definir transformação - Forneça instruções em linguagem natural, documentação e exemplos de código para o agente, o que gera uma definição inicial de transformação. Essa definição pode ser refinada iterativamente por meio de bate-papo ou edições diretas. Essa fase pode ser ignorada ao usar transformações AWS gerenciadas.

Pilote ou Proof-of-Concept - Teste a transformação em bases de código de amostra e refine com base nos resultados. Essa fase de validação ajuda a estimar o custo e o esforço da transformação completa. O aprendizado contínuo melhora a qualidade durante essa fase.

Execução escalonada - Configure a execução em massa automatizada usando a CLI, com os desenvolvedores revisando e validando os resultados. Monitore o progresso usando o aplicativo web e acompanhe as transformações em vários repositórios.

Monitore e revise - O aprendizado contínuo melhora automaticamente a qualidade da transformação. Analise as lições que foram extraídas de séries anteriores para garantir que atendam aos padrões de qualidade e archive as que não forem úteis.

Compreender os conceitos principais do

Esta seção explica os principais conceitos para trabalhar com o AWS Transform custom.

Definições de transformação

Uma definição de transformação contém as instruções e o conhecimento necessários para realizar uma transformação de código específica. É representado como uma habilidade e consiste em:

- `SKILL.md`(obrigatório) - Instruções no Markdown com o frontmatter (`name` e `description` campos) do YAML que contém a lógica de transformação principal e as instruções de execução
- `references/`pasta (opcional) - Documentação carregada conforme necessário durante a execução da transformação
- `scripts/`pasta (opcional) - Scripts que a transformação baixa e executa durante a execução

AWS O Transform CLI baixa automaticamente as definições de transformação para o diretório atual quando necessário para execução, inspeção ou modificação.

Important

Ao publicar uma transformação, o diretório deve conter somente `SKILL.md` e, opcionalmente, a `references/` pasta, a `scripts/` pasta ou ambas. Nenhum outro arquivo ou subdiretório é permitido.

Note

A CLI versão 2.0 e posterior usa o formato de habilidades. As definições de transformação existentes são tratadas automaticamente pela CLI.

Registro de transformação

O registro de transformação é o repositório centralizado da sua AWS conta para armazenar e gerenciar as definições de transformação. As transformações no registro podem ser:

- Listado usando `atx custom def list`
- Executado em várias bases de código
- Compartilhado com outros usuários em sua AWS conta
- Version-controlled

Important

As definições de transformação são específicas da conta. Se quiser usar uma transformação em uma AWS conta diferente, você deve publicá-la separadamente nessa conta.

Transformações preliminares versus transformações publicadas

AWS O Transform custom oferece suporte a dois estados para transformações no registro:

As transformações preliminares são definições de transformação em andamento ou não testadas. Eles são salvos como versões específicas e podem ser recuperados, atualizados e executados por usuários que se referem a essa versão específica. Os rascunhos são úteis para desenvolvimento, teste e refinamento iterativos antes que a transformação esteja pronta para ser compartilhada com sua equipe. Os rascunhos também estão associados a uma conversa específica. Se você reiniciar a CLI, poderá usá-la `atx --conversation-id {id}` para restaurar uma anterior.

As transformações publicadas estão disponíveis no registro de transformação da sua conta para execução por outros usuários com as permissões necessárias do IAM. As transformações publicadas podem ser descobertas usando `atx custom def list`.

O fluxo de trabalho típico é:

1. Crie transformação localmente
2. Salvar como rascunho para teste (`atx custom def save-draft`)
3. Refine e valide
4. Publique para compartilhar com sua equipe (`atx custom def publish`)

Você também pode publicar uma transformação diretamente sem salvá-la como rascunho.

Referências versus aulas

AWS O Transform custom usa dois tipos de conhecimento para melhorar a qualidade da transformação:

As referências são documentação fornecida pelo usuário armazenada na `references/` pasta de uma definição de transformação. As referências oferecem suporte somente a arquivos de texto (máximo de 10 MB no total para todos os arquivos) e geralmente contêm documentação, especificações de API, guias de migração e exemplos de código. As referências são carregadas conforme necessário durante a execução da transformação. Você adiciona referências ao criar ou atualizar uma definição de transformação no modo interativo.

As aulas são extraídas automaticamente de execuções anteriores de uma transformação. O sistema de aprendizado contínuo os gera a partir de trajetórias de execução, feedback do desenvolvedor e correções de código encontradas durante as transformações. Ele agrupa as aulas relacionadas em categorias para que vocês possam analisá-las em conjunto. Ao contrário das referências, que você fornece antecipadamente, as aulas se acumulam ao longo do tempo à medida que você executa a transformação em diferentes bases de código, e o sistema as aplica automaticamente para melhorar futuras execuções. Você revisa e gerencia as aulas de forma interativa com `atx custom def learnings`.

Comandos de compilação e validação

O comando de compilação ou validação é um parâmetro opcional que especifica como validar seu código durante o processo de transformação. Esse comando é executado em vários pontos durante a transformação para garantir a integridade do código.

Fornecer um comando que valide os resultados e retorne os problemas se a validação falhar é muito importante para melhorar a qualidade da transformação por meio do aprendizado contínuo. Se nenhuma compilação ou validação for necessária, omita da sua entrada.

Para obter exemplos e orientações detalhadas, consulte Comandos de criação e validação na seção Fluxos de trabalho.

Aprendizagem contínua

O aprendizado contínuo é o sistema que captura automaticamente o feedback de cada execução da transformação e melhora a qualidade da transformação ao longo do tempo. O sistema coleta informações por meio de:

- Feedback explícito - Comentários e correções de código fornecidos no modo interativo
- Observações implícitas - Problemas que o agente encontra ao transformar e depurar o código

O sistema de aprendizado contínuo processa essas informações para criar lições que são adicionadas à definição de transformação para melhorar as transformações futuras. O sistema executa o processo de aprendizado automaticamente após a conclusão das transformações, sem exigir nenhuma entrada adicional de você.

Important

As aulas são específicas para cada transformação e não são compartilhadas entre diferentes transformações ou diferentes contas de clientes.

Gerenciando aulas

O sistema gera aulas automaticamente, mas você mantém o controle de quais serão aplicadas às futuras corridas. O `atx custom def learnings` comando abre uma sessão de terminal interativa para revisar e organizar as lições que uma transformação acumulou.

Nesta sessão, você pode:

- Procure aulas agrupadas em categorias e veja quantas aulas ativas cada categoria contém.
- Abra uma aula para ler todos os detalhes, incluindo o corpo da aula, seu impacto e quantas edições anteriores a consultaram.
- Arquive uma lição para evitar que o sistema a aplique em futuras execuções e restaure-a posteriormente, se necessário.
- Exclua permanentemente uma lição arquivada que não é mais útil.

Para obter instruções detalhadas, consulte [the section called “Aprendizagem contínua”](#).

Client-Side Habilidades

Client-side habilidades são recursos adicionais que ampliam o agente durante as execuções de transformação. Diferentemente das definições de transformação que definem qual transformação realizar, as habilidades do lado do cliente fornecem ferramentas, scripts e instruções complementares que o agente pode usar junto com seus recursos integrados durante qualquer transformação.

Client-side as habilidades são descobertas nos diretórios no nível do projeto e no nível do usuário. Coloque as habilidades no nível do projeto quando elas aplicam padrões específicos para um repositório e no nível do usuário quando elas se aplicam a todos os seus projetos. Project-level as habilidades só estão disponíveis quando um caminho de repositório de código é fornecido. Para configuração e uso detalhados, consulte [the section called “Client-Side Habilidades”](#).

Conceitos básicos

Esta seção descreve como configurar o AWS Transform custom e executar sua primeira transformação.

Pré-requisitos

Antes de instalar o AWS Transform custom, verifique se você tem o seguinte:

Plataformas com suporte

AWS O Transform custom é compatível com os seguintes sistemas operacionais:

- Linux - Suporte completo para todas as distribuições Linux
- macOS - Suporte total para sistemas macOS
- Windows - Suporte completo para Windows nativo usando o Windows Terminal e PowerShell (Os `atx` `ct` comandos ainda não são suportados no Windows)
- Subsistema Windows para Linux (WSL) - Compatível quando executado em WSL

Software necessário

- Node.js 22 ou posterior - Faça o download em <https://nodejs.org/en/download>

- Git - Deve estar instalado e o diretório de trabalho precisa ser um repositório Git válido para executar uma transformação. Execute `git init; git add .; git commit -m "Initial commit"` para inicializar um repositório Git em seu diretório de trabalho.

Requisitos de rede

É necessária uma conexão com a Internet com acesso aos seguintes endpoints:

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

Se você estiver trabalhando em um ambiente restrito à Internet, atualize as regras de firewall para permitir esses URLs.

Instalar o AWS Transform CLI

O método de instalação recomendado é usar o script de instalação. Escolha a guia do seu sistema operacional.

Para instalar a CLI do AWS Transform

1. Execute o script de instalação:

Linux and macOS

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

Windows (PowerShell)

No Windows nativo, execute o script de instalação no Terminal do Windows usando PowerShell.

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

2. Verifique a instalação:

```
atx --version
```

O comando deve exibir a versão instalada da CLI do AWS Transform.

Configuração da autenticação

AWS O Transform custom exige AWS credenciais para se autenticar com o serviço. Configure a autenticação usando um dos métodos a seguir.

Variáveis de ambiente

Defina as seguintes variáveis de ambiente.

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"
```

Você também pode especificar um perfil usando a variável de AWS_PROFILE ambiente.

Linux and macOS

```
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

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


 Note

As variáveis de ambiente definidas com `$env:` in PowerShell se aplicam somente à sessão atual. Para mantê-los em todas as sessões, defina-os em Propriedades do sistema > Variáveis de ambiente ou use `[System.Environment]::SetEnvironmentVariable()`.

AWS Arquivo de credenciais

Configure as credenciais no arquivo de AWS credenciais, localizado no Linux e `~/.aws/credentials` no macOS, ou no Windows: `%USERPROFILE%\aws\credentials`

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

Permissões do IAM

Suas AWS credenciais devem ter permissões para chamar o serviço personalizado AWS Transform. Recomendamos anexar a política [AWSTransformCustomFullAccess](#) AWS gerenciada ao seu usuário ou função do IAM. Essa política fornece acesso total ao AWS Transform custom, incluindo a permissão para criar a [função vinculada ao serviço](#) necessária para a emissão de CloudWatch métricas para sua conta.

Para um controle mais granular, o AWS Transform custom também fornece as seguintes políticas AWS gerenciadas:

- [AWSTransformCustomExecuteTransformations](#)— Fornece acesso para executar transformações.
- [AWSTransformCustomManageTransformations](#)— fornece acesso para criar, atualizar, ler e excluir recursos de transformação, bem como executar transformações.

Para obter mais informações sobre essas políticas, consulte [políticas AWS gerenciadas do AWS Transform](#). Para políticas personalizadas do IAM com permissões em nível de recurso, consulte o Guia de referência de [autorização do serviço AWS Transform Custom IAM](#).

 Note

- As definições de transformação são AWS recursos com ARNs (Amazon Resource Names). Você pode usar políticas do IAM para controlar o acesso a transformações específicas ou grupos de transformações especificando o ARN da transformação nas declarações de recursos da política do IAM. As tags podem ser usadas para controle de acesso agrupado.
- AWS O IAM Identity Center é necessário para acessar o AWS Transform, mas não é necessário usar a CLI.

Configurar AWS Região

AWS O Transform custom está disponível em AWS regiões específicas e detecta automaticamente sua configuração de região usando a precedência padrão da AWS CLI.

Regiões aceitas

AWS O Transform custom está disponível nas seguintes AWS regiões:

- `us-east-1`(Leste dos EUA - Norte da Virgínia)
- `eu-central-1`(Europa - Frankfurt)
- `eu-west-2`(Europa - Londres)
- `ca-central-1`(Canadá - Central)
- `ap-northeast-1`(Ásia-Pacífico - Tóquio)
- `ap-northeast-2`(Ásia-Pacífico - Seul)
- `ap-southeast-2`(Ásia-Pacífico - Sydney)
- `ap-south-1`(Ásia-Pacífico - Mumbai)

Como a região é determinada

A CLI verifica essas fontes em ordem prioritária para determinar qual região usar:

1. `AWS_REGION` variável de ambiente (prioridade mais alta)
2. `AWS_DEFAULT_REGION` variável de ambiente
3. Perfil selecionado no arquivo de AWS configuração (via variável de `AWS_PROFILE` ambiente)

4. Perfil padrão no AWS arquivo de configuração
5. Retorno padrão para us-east-1 se nenhuma configuração for encontrada

 Note

O arquivo de AWS configuração está localizado no Linux e ~/.aws/config no macOS %USERPROFILE%\aws\config ou no Windows.

 Note

Se ATX_CUSTOM_ENDPOINT estiver definida, a região será extraída da URL do endpoint e substituirá todas as outras configurações.

Definindo sua região

Escolha um desses métodos para configurar sua região:

Opção 1: Variável de ambiente (recomendada para uso temporário):

Linux and macOS

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

Windows (PowerShell)

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

Opção 2: configuração da AWS CLI (recomendada para configuração permanente):

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

Opção 3: Profile-specific configuração:

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"
```

Opção 4: edição direta de arquivos:

Edite o arquivo de AWS configuração diretamente (~/.aws/config no Linux e no macOS %USERPROFILE%\ .aws\config ou no Windows):

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

Verificando a configuração da sua região

Para verificar qual região o AWS Transform custom usará:

Verifique a configuração atual da região:

```
aws configure get region
```

Verifique as variáveis de ambiente:

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"
```

Veja a resolução detalhada da região nos registros de depuração:

Linux and macOS

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

Windows (PowerShell)

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

Exemplo de saída de log mostrando a origem da região:

```
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"
}
```

O `regionSource` campo mostra de onde a região foi derivada (por exemplo, “aws-config (profile: default)”, “AWS_REGION”, “default”).

Important

Se a configuração da sua região apontar para uma região sem suporte, a CLI exibirá uma mensagem de erro clara com instruções para atualizar sua configuração para uma região compatível.

Executando sua primeira transformação

A maneira mais rápida de começar é usar uma transformação AWS gerenciada. AWS-transformações gerenciadas são transformações pré-criadas e AWS aprovadas que estão prontas para uso sem qualquer configuração.

Para executar uma transformação AWS gerenciada de forma interativa:

```
atx
```

Em seguida, peça ao agente que execute uma transformação:

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

Para executar uma transformação de forma não interativa:

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

Para obter informações detalhadas sobre modos de execução, opções de configuração e sinalizadores de comando, consulte [the section called “Os comandos da Referência de comandos”](#).

Entendendo os resultados da transformação

Quando uma transformação é concluída, o AWS Transform custom fornece um relatório descrevendo os resultados. Se a transformação não foi validada (por exemplo, construção bem-sucedida para aplicativos Java), o relatório fornece recomendações para ações futuras.

A maioria das transformações é realizada em várias etapas, usando o Git para confirmar as intermediárias. Você pode revisar as alterações feitas pela transformação usando os comandos padrão do Git:

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

Criando uma transformação personalizada

Quando as transformações AWS gerenciadas não atendem às suas necessidades, você pode criar transformações personalizadas sob medida para seus requisitos específicos.

Para criar uma transformação personalizada

1. Inicie a CLI do AWS Transform no modo interativo:

```
atx
```

2. Diga ao agente que você deseja criar uma nova transformação e descreva seus requisitos.

3. Forneça materiais de referência, como documentação e exemplos de código, para melhorar a qualidade.
4. Teste e refine a transformação de forma iterativa.
5. Publique-o no registro de transformação da sua organização.

Para obter instruções detalhadas sobre como criar transformações personalizadas, consulte [the section called “Fluxos de trabalho”](#).

AWS Aplicativo Web Transform (opcional)

O aplicativo web AWS Transform é uma interface opcional para monitorar campanhas de transformação em grande escala em vários repositórios. Antes de usar o aplicativo web AWS Transform, você precisa ter uma identidade de usuário habilitada para acessar o AWS Transform em sua organização. Para obter informações sobre como ativar o AWS Transform, consulte [Configurando o AWS Transform](#).

Para usar o aplicativo web AWS Transform:

1. Visite <https://aws.amazon.com/transform/> e faça login usando as credenciais AWS do IAM Identity Center.
2. Selecione o tipo de tarefa “Custom/code” no aplicativo web AWS Transform.
3. Diga ao agente o nome da definição de transformação que você gostaria de usar.
4. O aplicativo web fornece um comando AWS Transform CLI que pode ser compartilhado com sua equipe. Esse comando invoca a definição da transformação e registra os resultados da execução no aplicativo web.
5. Depois que os resultados da transformação forem capturados, visualize estatísticas, medições de economia de tempo e faça perguntas sobre o progresso do seu trabalho no Painel.

O aplicativo web foi projetado para operações em escala empresarial, nas quais você precisa de monitoramento centralizado das transformações em várias bases de código.

Note

AWS O IAM Identity Center é necessário para acessar o aplicativo web AWS Transform. A CLI não exige o IAM Identity Center — somente AWS credenciais padrão são necessárias.

Introdução aos comandos de transformação personalizados

Aqui estão alguns dos comandos que você pode usar com transformações personalizadas. A lista completa de comandos está na [referência de comandos AWS Transformar transformações personalizadas](#).

- `atx custom`
 - Executa uma experiência interativa de transformação personalizada, permitindo a criação, descoberta, execução e refinamento das transformações.
 - Esse é o comando padrão para `atx`.
 - `--trust-all-tools(-t)` é opcional e permite implicitamente todas as solicitações de ferramentas solicitadas pelo agente. Use com cuidado, especialmente em ambientes de produção. Você pode configurar a confiança da ferramenta para ferramentas e comandos específicos usando o [arquivo de configurações de confiança](#).
- `atx custom --help` | `atx custom -h`
 - Mostra o menu de ajuda.
 - Cada comando também inclui um menu de ajuda, por exemplo, `atx custom def exec --help`.
- `atx --version` | `atx -v`
 - Mostra a versão.
 - O número da versão muda a cada lançamento.
- `atx custom def list`
 - Imprime a lista de transformações disponíveis no registro de transformação.
- `atx custom def exec`
 - Executa uma transformação
- `atx custom def learnings`
 - Abre uma sessão interativa para visualizar e gerenciar as lições que uma transformação aprendeu em execuções anteriores
- `atx mcp`
 - Usado para gerenciar as configurações do servidor MCP

Fluxos de trabalho

Executando transformações

Esta seção descreve as diferentes formas de executar transformações e as opções para controlar o comportamento da execução.

Modos de execução

AWS O Transform custom oferece suporte a três modos de execução para acomodar diferentes fluxos de trabalho.

Modo conversacional interativo

Inicie a CLI com `atx` e peça ao agente que execute uma transformação por meio da linguagem natural. Esse modo permite que você tenha uma conversa completa com o agente, interrompa a execução a qualquer momento e forneça feedback durante o processo de transformação.

Use esse modo quando quiser o máximo controle e a capacidade de guiar o agente em cenários complexos.

Execução direta interativa

Use `atx custom def exec -n <transformation-name> -p <path>` para iniciar uma transformação específica de forma interativa. Esse modo permite que você revise e interaja com o agente no início, durante ou no final da execução. O agente fará uma pausa nos principais pontos de decisão e pedirá sua opinião.

Isso é ideal para testar e refinar transformações antes de executá-las de forma autônoma.

Você pode executar transformações no modo não interativo ou no modo headless. Non-interactive o modo suprime as solicitações durante uma transformação nomeada. O modo headless permite que você execute o agente com um prompt de texto sem formatação, ignorando totalmente a interface interativa.

Non-interactive modo

Use `atx custom def exec -n <transformation-name> -p <path> -x -t` para automação total. Adicione `-x` para executar no modo não interativo e `-t` para confiar em todas as ferramentas automaticamente sem aviso prévio.

Esse modo foi projetado para integração de CI/CD tubulações e execução em massa, onde nenhuma intervenção humana está disponível ou é desejada.

Modo sem cabeça

Para concluir tarefas sem interagir com o agente, execute `atx -x "<prompt>" -t` e forneça suas instruções em texto simples.

Execução de transformação sem interrupções

Use esse modo para aplicar uma definição de transformação existente à sua base de código. A transformação executa cada etapa automaticamente sem exigir sua aprovação.

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

Desenvolvimento de transformação sem cabeça

Crie ou modifique definições de transformação.

Para converter uma definição de transformação antiga para o novo formato de habilidade (SKILL.md + referências/), execute o seguinte comando:

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

Para criar uma nova definição de transformação, execute o seguinte comando:

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

Sinalizadores de comando comuns

Ao executar transformações com `atx custom def exec`, os seguintes sinalizadores são comumente usados:

- `-nou --transformation-name` - Especifica o nome da transformação a ser executada
- `-pou --code-repository-path` - Especifica o caminho para sua base de código (use "." para o diretório atual)

- `-cou --build-command` - Especifica o comando de compilação ou validação a ser executado
- `-xou --non-interactive` - Ativa o modo não interativo (sem solicitações do usuário)
- `-tou --trust-all-tools` - Confia automaticamente em todas as ferramentas sem aviso prévio
- `-dou --do-not-learn` - Impede a extração da lição dessa execução
- `--tvou --transformation-version` - Especifica uma versão específica da transformação
- `-gou --configuration` - Fornece um arquivo de configuração ou configuração embutida

Important

O `--trust-all-tools` sinalizador `-t` aprova automaticamente todas as execuções de ferramentas sem aviso prévio e ignora a maioria das barreiras de segurança (os comandos que correspondem à sua `alwaysPromptCommands` lista ainda exigem permissão explícita, a menos que sejam substituídos por). `trustedShellCommands` É necessário aprovar `--non-interactive` e `--trust-all-tools` é necessário para uma experiência totalmente autônoma, mas não é necessário para executar a transformação. Use com cautela em ambientes de produção.

Usando arquivos de configuração

AWS O Transform custom oferece suporte a arquivos de configuração opcionais no formato YAML ou JSON. Os arquivos de configuração permitem que você especifique parâmetros de execução e forneça contexto adicional ao agente.

Para usar um arquivo de configuração:

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

Você também pode fornecer a configuração como pares de valores-chave em linha:

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

Exemplo de arquivo de configuração (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
```

O `additionalPlanContext` parâmetro fornece contexto adicional para o plano de execução do agente. Isso é especialmente útil com transformações AWS gerenciadas para personalizar seu comportamento de acordo com suas necessidades específicas.

Comandos de compilação e validação

O comando de compilação ou validação é um parâmetro opcional que especifica como validar seu código durante o processo de transformação. AWS O Transform custom tentará inferir o melhor comando de construção com base na transformação, se não for especificado, embora seja recomendado que seja específico em termos de qualidade.

Exemplos de comandos de compilação e validação:

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

Mesmo para linguagens ou transformações que não exigem construção, fornecer um comando que valide os resultados e retorne problemas se a validação falhar é muito importante para melhorar a qualidade da transformação.

Se nenhuma compilação ou validação for necessária, omita da sua entrada.

Controlando o comportamento de aprendizagem

Por padrão, o AWS Transform custom extrai lições de cada execução de transformação. Você pode evitar o aprendizado para execuções específicas.

Para evitar o aprendizado com uma execução:

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

O `--do-not-learn` sinalizador `-d` or opta por não permitir a extração da lição da execução atual.

Retomando conversas

AWS O Transform custom permite que você retome conversas anteriores dentro de 30 dias após a criação.

Para retomar a conversa mais recente:

```
atx --resume
```

Para retomar uma conversa específica:

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

Important

As conversas só podem ser retomadas dentro de 30 dias após a criação. Após 30 dias, a conversa não poderá mais ser retomada.

Minutos do agente de rastreamento

AWS O Transform custom rastreia os [minutos do agente](#) consumidos durante uma sessão de transformação. Os minutos do agente se acumulam durante todo o ciclo de vida da conversa e são exibidos quando a conversa termina:

```
Agent minutes used: 12.50
```

Os minutos do agente persistem em todas as interrupções. Se você interromper uma sessão com `Ctrl+C` e retomá-la posteriormente, os minutos acumulados anteriormente serão transferidos e continuarão sendo acumulados na sessão retomada.

Para verificar os minutos do agente durante uma sessão interativa:

Digite `/usage` no prompt de entrada para exibir os minutos atuais acumulados do agente sem encerrar a conversa.

Para definir um limite de orçamento de minutos do agente:

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

A `--limit` opção define um orçamento máximo de [minutos do agente](#) para a sessão. Os minutos do agente refletem o tempo de trabalho do agente ativo, não o horário do relógio de parede. Quando o limite é atingido, a CLI exibe uma mensagem e sai com instruções para continuar:

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

Você pode retomar a conversa mais tarde com um limite maior:

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

Aprendizagem contínua

Esta seção descreve como revisar e gerenciar as aulas criadas pelo aprendizado contínuo.

Entendendo as lições

O sistema de aprendizado contínuo extrai automaticamente as lições de execuções anteriores de uma transformação. O sistema os cria de forma assíncrona com base em:

- Feedback do desenvolvedor fornecido no modo interativo
- Problemas de código encontrados durante as transformações

As aulas se acumulam com o tempo à medida que você executa a transformação em diferentes bases de código. O sistema os aplica automaticamente para melhorar as execuções futuras. Cada lição pertence a uma categoria que contém todas as lições de um domínio similar para que vocês possam revisar as lições relacionadas em conjunto. Para aulas que você não gostaria de usar, você pode arquivar ou excluir totalmente a lição.

Visualizando e gerenciando aulas

Use o `learnings` comando para abrir uma sessão interativa para navegar e gerenciar as lições de uma definição de transformação.

Para abrir o visualizador de aulas:

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

O visualizador abre uma lista de categorias de aulas, cada uma mostrando quantas aulas ativas ela contém. Selecione uma categoria para ver suas aulas e, em seguida, selecione uma lição para ver todos os detalhes, incluindo o corpo da aula, seu impacto e quantas edições anteriores a consultaram.

Aulas de arquivamento e restauração

O sistema aplica as aulas automaticamente. Se você não quiser que o sistema aplique uma lição, você pode arquivá-la. O sistema retém as aulas arquivadas, mas não as aplica a futuras execuções. Todas as aulas arquivadas são agrupadas para que você possa revisá-las e restaurá-las para uso ativo.

Excluindo aulas

Remova permanentemente uma lição que não seja útil. A exclusão não pode ser desfeita e o sistema pode reaprender uma lição excluída em futuras execuções.

Uma lição deve ser arquivada antes de ser excluída.

Configuração avançada

Esta seção descreve os recursos avançados e as opções de configuração do AWS Transform custom.

Variáveis de ambiente

Você pode personalizar o comportamento da CLI usando variáveis de ambiente.

Note

Os exemplos a seguir mostram a sintaxe do Linux e do macOS (`()`). `export` No Windows, defina as variáveis de ambiente PowerShell usando `$env:NAME="value"`. Consulte as guias Windows (PowerShell) para obter os comandos equivalentes.

ATX_SHELL_TIMEOUT

Substitua o tempo limite padrão para comandos do shell (900 seconds/15 minutos).

Linux and macOS

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

Windows (PowerShell)

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

Isso é útil para grandes bases de código ou processos de compilação de longa duração.

ATX_DISABLE_UPDATE_CHECK

Desative as verificações automáticas de versão e as notificações de atualização durante a execução do comando.

Linux and macOS

```
export ATX_DISABLE_UPDATE_CHECK=true
```

Windows (PowerShell)

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

ATX_GIT_COMMITTER_NAME e ATX_GIT_COMMITTER_EMAIL

Configure a identidade do autor usada para os commits do ponto de verificação que o AWS Transform custom cria em seu repositório à medida que aplica as alterações durante uma transformação. Quando essas variáveis não são definidas, as confirmações do ponto de verificação são atribuídas a uma identidade padrão ()ATX Bot <checkpoint@atx.bot>. Defina as duas variáveis para atribuir pontos de verificação a um autor específico.

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"
```

Configurações de confiança

As configurações de confiança permitem que você pré-aprove ferramentas e comandos específicos para execução sem solicitações. Você também pode exigir permissão explícita para comandos específicos do shell, independentemente do nível de confiança. Essas configurações são definidas no arquivo `~/.aws/atx/trust-settings.yaml`.

O arquivo contém três listas:

- `trustedTools`- Ferramentas que podem ser executadas sem aviso
- `trustedShellCommands`- Comandos de shell que podem ser executados sem aviso
- `alwaysPromptCommands`- Padrões de comando do Shell que exigem permissão explícita, a menos que sejam substituídos por `trustedShellCommands`, independentemente do `-t` sinalizador ou da confiança da sessão. Esses padrões não são aplicados no modo não interativo `()-x`.

Ferramentas confiáveis padrão:

- `file_read`
- `get_transformation_from_registry`
- `list_available_transformations_from_registry`

Editando configurações de confiança:

Você pode editar manualmente o arquivo `trust-settings.yaml` para adicionar ou remover ferramentas e comandos confiáveis. Ambos `trustedShellCommands` e `alwaysPromptCommands` suportam padrões globais de curingas usando `*`.

Note

Se um comando corresponder às duas listas, `trustedShellCommands` terá prioridade.

O seguinte descreve cada lista de comandos e fornece exemplos:

- `trustedShellCommands`- Os comandos que correspondem a esses padrões são executados sem aviso prévio, ignorando todas as outras grades de proteção. Os padrões são comparados com a cadeia de comando completa.

Exemplos:

- `cd *`- Combina comandos compostos começando com `cd`
- `*&&*`- Confia em todos os comandos com operadores `&&`
- `alwaysPromptCommands`- Os comandos que correspondem a esses padrões exigem permissão explícita, a menos que sejam substituídos por `trustedShellCommands`, independentemente do -t sinalizador ou da confiança da sessão. Esses padrões não são aplicados no modo não interativo `()-x`. Os padrões são comparados com cada subcomando em expressões compostas `(&&, | |`, substituições de comandos).

Exemplos:

- `rm -rf *`- Sempre solicita comandos recursivos de exclusão forçada
- `sudo *`- Sempre solicita comandos executados com `sudo`
- `find * -exec *`- Sempre solicita comandos de localização com `-exec`

Session-level confiança:

Durante os prompts interativos, você pode escolher:

- `(y)es`- Execute uma vez
- `(n)o`- Negar
- `(t)rust`- Confie somente na sessão atual

Session-level as configurações de confiança são temporárias e são redefinidas quando a CLI é reiniciada, fornecendo aprovação temporária sem modificar permanentemente `trust-settings.yaml`.

Note

A confiança da sessão não está disponível para comandos que correspondam à sua `alwaysPromptCommands` lista.

Servidores do Model Context Protocol (MCP)

O AWS Transform CLI oferece suporte a servidores Model Context Protocol (MCP), que ampliam sua funcionalidade com ferramentas adicionais.

Configuração:

Configure os servidores MCP no `~/.aws/atx/mcp.json` arquivo. O AWS Transform CLI suporta dois tipos de servidores MCP: servidores locais baseados em comandos e servidores HTTP remotos.

Servidores locais baseados em comandos:

Os servidores locais são executados como processos secundários em sua máquina. Configure-os com a `command` propriedade:

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

Servidores HTTP remotos:

Os servidores remotos se conectam aos servidores MCP hospedados em uma URL HTTP ou HTTPS. Configure-os com a `url` propriedade:

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

A `headers` propriedade é opcional e oferece suporte à expansão de variáveis de ambiente usando a `${VAR_NAME}` sintaxe. Isso permite que você armazene valores confidenciais, como tokens de API, em variáveis de ambiente e não no arquivo de configuração.

Propriedades de configuração:

Os servidores locais baseados em comandos oferecem suporte às seguintes propriedades:

- `command`(obrigatório) - O comando para executar o servidor
- `args`(opcional) - Matriz de argumentos de linha de comando
- `env`(opcional) - Variáveis de ambiente a serem passadas para o processo do servidor

Os servidores HTTP remotos oferecem suporte às seguintes propriedades:

- `url`(obrigatório) - O URL HTTP ou HTTPS do servidor MCP remoto
- `headers`(opcional) - cabeçalhos HTTP a serem incluídos nas solicitações, com suporte para expansão de variáveis de `${VAR_NAME}` ambiente

Gerenciando servidores MCP:

Veja a lista de servidores MCP configurados:

```
atx mcp tools
```

Liste as ferramentas disponíveis oferecidas por um servidor MCP específico:

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

Rastreamento de uso:

A CLI rastreia automaticamente o uso da ferramenta MCP durante as execuções de transformação. As estatísticas de uso são mantidas, como `mcp_usage.json` no diretório de conversas ao lado `metadata.json`. O arquivo registra métricas por ferramenta para cada execução, incluindo:

- Número de invocações por ferramenta
- Número de erros por ferramenta
- Tempo total de execução por ferramenta
- Detalhes do último erro (se houver)

Client-Side Habilidades

Client-side habilidades são recursos adicionais que ampliam o agente durante as execuções de transformação. Eles permitem que você forneça ferramentas, scripts e instruções personalizados que o agente pode usar junto com seus recursos integrados.

Diretórios de descoberta de habilidades:

As habilidades são descobertas em quatro diretórios em ordem de precedência. Se uma habilidade com o mesmo nome existir em vários diretórios, o primeiro diretório na lista terá prioridade:

1. <project>/.`aws/atx/skills/`- Project-level, AWS Transformar CLI-specific
2. <project>/.`agents/skills/`- Project-level, multicliente (disponível para qualquer ferramenta de agente compatível)
3. ~/.`aws/atx/skills/`- User-level, AWS Transformar CLI-specific
4. ~/.`agents/skills/`- User-level, multicliente (disponível para qualquer ferramenta de agente compatível)

Os `.aws/atx/skills/` diretórios são específicos da CLI do AWS Transform. Os `.agents/skills/` diretórios são multiclientes, o que significa que as habilidades colocadas lá estão disponíveis para qualquer ferramenta de agente compatível além da CLI do Transform AWS .

Estrutura do diretório de habilidades:

Cada habilidade é um diretório contendo um `SKILL.md` arquivo com o frontmatter YAML:

```
~/.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 formato:

```
---  
name: my-skill  
description: When to use this skill
```

```
---  
# Skill Title  
  
Instructions for the agent...
```

O nome campo deve corresponder ao nome do diretório principal.

Desativando uma habilidade:

Para evitar que uma habilidade seja carregada sem remover seus arquivos, adicione `disable-model-invocation: true` ao `frontmatter`:

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

Quando essa propriedade é definida, a CLI ignora a habilidade durante a descoberta. O agente não pode ver nem usar a habilidade, a menos que uma definição de transformação o instrua explicitamente a ler o arquivo de habilidade. Use isso para desativar temporariamente uma habilidade, marcá-la como trabalho em andamento ou manter o material de referência destinado somente a leitores humanos.

Note

Os arquivos de uma habilidade desativada permanecem no disco. Se uma definição de transformação instruir o agente a ler um caminho de arquivo específico, o agente ainda poderá acessar o conteúdo. A `disable-model-invocation` propriedade impede a descoberta automática e a injeção de contexto, não o acesso ao sistema de arquivos.

Disponibilidade de habilidades por modo de execução:

- Modo executivo (`atx custom def execcom--code-repository-path`) - descobre habilidades dos diretórios em nível de usuário e de projeto.
- Modo interativo (`atx`) - Somente habilidades em nível de usuário são descobertas inicialmente. Quando você fornece um caminho de repositório de código durante a sessão, as habilidades em nível de projeto também são carregadas.

Verificando a descoberta de habilidades:

Verifique o registro de depuração da CLI após uma execução para verificar quais habilidades foram descobertas:

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
```

As habilidades que falham na validação são ignoradas com um aviso nos registros de depuração.

Note

Client-side as habilidades exigem CLI versão 2.0 ou posterior.

Escolhendo entre Project-Level e User-Level habilidades

O local onde você coloca uma habilidade determina quem se beneficia dela e quando ela é ativada.

Project-level habilidades (<project>/~/.aws/atx/skills/):

Comprometa-os ao controle de versão para que cada membro da equipe que executa transformações no repositório os descubra automaticamente. Use habilidades em nível de projeto para:

- Repository-specific verificações de conformidade (regras do Dockerfile, políticas do Terraform, validadores de segurança de migração)
- Padrões de codificação da organização que se aplicam a essa base de código (padrões de observabilidade, tratamento de erros, convenções de nomenclatura)
- Crie ou teste scripts exclusivos para o projeto (impressoras personalizadas, funções de condicionamento físico de arquitetura)
- Guias de migração de API para bibliotecas internas usadas neste repositório

User-level habilidades (~/.aws/atx/skills/):

Eles permanecem na sua máquina e são ativados durante todas as transformações, independentemente do repositório de destino. Use habilidades em nível de usuário para:

- Ferramentas pessoais de fluxo de trabalho (geradores de changelog, formatadores de mensagens de confirmação)
- Cross-project preferências (padrões de teste preferidos, lembretes de estilo de documentação)
- Verificações de conformidade de licenças que sua organização exige em todos os repositórios
- Limites de cobertura ou barreiras de qualidade que você impõe em cada base de código com a qual trabalha

Dicas para habilidades eficazes:

- Escreva `description` campos claros em seu `SKILL.md` frontmatter. O agente usa esse campo para decidir quando uma habilidade é relevante.
- Saia dos scripts de validação com código 0 em caso de sucesso e diferente de zero em caso de falha. O agente interpreta os códigos de saída para determinar a conformidade.
- Imprima mensagens de erro claras e acionáveis em scripts. O agente lê a saída para entender o que corrigir.
- Coloque as habilidades no diretório entre clientes (`.agents/skills/`) em qualquer nível para compartilhá-las com outras ferramentas de desenvolvimento de IA além da CLI do AWS Transform.

Client-Side Exemplos de habilidades

Esses exemplos mostram dois padrões comuns: uma habilidade de validação baseada em script e uma habilidade somente de referência.

Exemplo: Dockerfile Compliance Checker () Script-Based

Essa habilidade valida os Dockerfiles em relação às melhores práticas operacionais e de segurança. Ele usa um script de validação que o agente executa antes e depois de fazer as alterações.

Estrutura de diretórios:

```
.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.
```

O script de validação verifica se há tags de imagem base não fixadas, executadas como raiz, segredos codificados em ENV diretivas e definições ausentes. HEALTHCHECK O agente executa o script, corrige violações usando padrões do arquivo de referência e executa novamente o script para confirmar a conformidade.

Exemplo: Auxiliar de depreciação da API () Reference-Only

Essa habilidade orienta o agente na substituição de chamadas de API obsoletas durante as transformações de upgrade. Ele usa somente arquivos de referência sem scripts.

Estrutura de diretórios:

```
.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
```

Os arquivos de referência contêm exemplos de código de antes e depois. Por exemplo, `aws-sdk-v2-to-v3.md` mapeia padrões como `s3.putObject(params).promise()` o equivalente modular v3 usando `S3Client` e `PutObjectCommand`

Tags e organização

Você pode organizar transformações com tags para controle de acesso e categorização.

 Note

Alguns desses comandos exigem a especificação do Amazon Resource Name (ARN) para uma definição de transformação. A estrutura do ARN é: `arn:aws:transform-custom:<region>:<account-id>:package/<td-name>`

Para listar tags para uma transformação:

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

Para adicionar tags a uma transformação:

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

Para remover tags de uma transformação:

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

As tags podem ser usadas para controle de acesso agrupado nas políticas do IAM. Você pode criar políticas que concedam permissões para todas as transformações com tags específicas (por exemplo, todas as transformações marcadas com `team:frontend` ou `environment:production`).

Logs

AWS O Transform CLI mantém três tipos de registros para solução de problemas e depuração.

Registros de conversas:

Linux and macOS

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

Windows

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

Esses registros contêm o histórico completo de conversas de uma sessão específica.

Registros do subagente:

Linux and macOS

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

Windows

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

Esses registros contêm saídas de subagentes que o agente principal gera durante as transformações. Você não precisa gerenciar subagentes diretamente.

Registros de depuração do desenvolvedor:

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
```

Esses registros fornecem informações avançadas de solução de problemas para a própria CLI.

Note

Pode haver vários arquivos de log de depuração no diretório de logs (ou seja, debug1.log, debug2.log). Revise e forneça todos os registros relevantes, por exemplo, `~/.aws/atx/custom/<conversation-id>/*` e `~/.aws/atx/logs/*`, ao abrir tickets de suporte para uma resolução mais rápida.

Atualizações da CLI

Mantenha sua CLI atualizada para acessar novos recursos e melhorias.

Para verificar se há atualizações:

```
atx update --check
```

Para atualizar para a versão mais recente:

```
atx update
```

Para atualizar para uma versão específica:

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

Crie transformações personalizadas

Esta seção descreve como criar, modificar e gerenciar definições de transformação personalizadas.

Criando uma nova transformação

Use a CLI interativa para criar uma nova definição de transformação.

Para criar uma definição de transformação

1. Inicie a CLI do AWS Transform:

```
atx
```

2. Diga ao agente que você deseja criar uma nova transformação.
3. Forneça uma descrição clara e detalhada do objetivo da transformação. Inclusão:
 - O estado de origem e de destino (por exemplo, “atualização da versão X para a versão Y”)
 - Mudanças específicas necessárias (por exemplo, “atualizar instruções de importação, substituir métodos obsoletos”)
 - Quaisquer considerações ou restrições especiais
4. Quando o agente solicitar esclarecimentos ou informações adicionais, forneça exemplos específicos e materiais de referência.
5. Revise a definição de transformação inicial criada pelo agente.
6. Teste a transformação em uma base de código de amostra.

7. Faça iterações fornecendo feedback, correções de código ou exemplos adicionais.
8. Salve a transformação localmente ou publique-a no registro.

Práticas recomendadas para criar transformações:

- Comece com transformações simples e bem definidas antes de tentar transformações complexas
- Forneça materiais de referência abrangentes, incluindo guias de migração e amostras de código
- Teste em várias bases de código de amostra antes de publicar
- Use comandos determinísticos de construção ou validação para permitir o aprendizado contínuo
- Considere dividir transformações complexas em várias etapas menores
- Marque as informações cruciais com “CRÍTICO:” ou “IMPORTANTE:” em suas definições de transformação para garantir que o agente priorize esses requisitos
- Quando você precisar que os requisitos exatos sejam seguidos (como usar um comando específico ou um valor de string), especifique explicitamente a string completa em suas definições de transformação. Você pode colocá-los em aspas bash para indicar claramente que são comandos de terminal ou strings literais, o que reduz a variabilidade e garante uma execução consistente

Fornecimento de materiais de referência

Você pode fornecer arquivos de referência ao AWS Transform custom especificando os caminhos dos arquivos durante a conversa. Esses arquivos são armazenados na `references/` pasta da definição de transformação.

Tipos recomendados de arquivos de referência:

- Before/after código de exemplo
- Documentação para APIs, bibliotecas ou recursos envolvidos
- Human-readable guias de migração

Para fornecer um arquivo de referência:

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

Você também pode fornecer um diretório contendo vários arquivos de referência:

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

Note

Somente arquivos baseados em texto (.md, .html, .txt, arquivos de código) são suportados. No momento, não há suporte para arquivos binários, imagens e arquivos de rich text (por exemplo, .pdf, .png, .docx). Muitas vezes, é possível extrair o conteúdo do texto e usá-lo como referência. Se você tiver muitos arquivos de texto pequenos, considere concatená-los em alguns arquivos com nomes descritivos. Há um limite total de 10 MB para todos os arquivos.

Modificando uma transformação existente

Você pode modificar as transformações personalizadas antes e depois de salvá-las como rascunhos ou publicá-las. Você não pode modificar AWS transformações gerenciadas. Se precisar personalizá-los, você pode fornecer contexto adicional usando o arquivo de configuração.

Para modificar uma transformação existente

1. Inicie a CLI do AWS Transform:

```
atx
```

2. Diga ao agente que você deseja modificar uma transformação existente.
3. Escolha se deseja:
 - Forneça um caminho de arquivo para uma transformação armazenada localmente (ou seja, não um rascunho salvo ou publicado)
 - Solicite a lista de transformações do registro
4. Se escolher no registro, selecione a transformação que você deseja modificar.
5. Trabalhe com o agente para descrever as alterações que você deseja fazer.
6. Teste a transformação atualizada em uma base de código de amostra.
7. Publique suas atualizações no registro, se desejar.

Publicando e gerenciando transformações

Você pode publicar e gerenciar suas transformações usando a experiência interativa ou com os seguintes comandos.

Para salvar uma transformação como rascunho:

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

Para publicar uma transformação:

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

Para listar as transformações disponíveis:

```
atx custom def list
```

Para baixar uma definição de transformação:

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

Isso baixa a definição de transformação para seu diretório de trabalho atual. Você pode especificar um diretório de destino com o `--td` sinalizador e uma versão com o `--tv` sinalizador.

Para excluir uma definição de transformação:

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

Important

Isso exclui permanentemente a definição de transformação especificada da sua conta.

Gerenciando versões de transformação

AWS O Transform custom mantém versões de suas definições de transformação. Você pode especificar uma versão ao executar ou baixar uma transformação.

Para executar uma versão específica:

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

Para baixar uma versão específica:

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

Se nenhuma versão for especificada, a versão mais recente será usada.

Os comandos da Referência de comandos

Esta seção fornece uma referência abrangente de todos os comandos personalizados da CLI do AWS Transform.

Comandos interativos

imposto

Inicie uma conversa interativa com a CLI do AWS Transform.

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

Comandos de sessão interativos

Os comandos a seguir podem ser digitados no prompt de entrada durante uma sessão interativa:

- /usage- Exibir os [minutos acumulados do agente](#) para a sessão atual

Comandos de definição de transformação

atx custom def exec

Execute uma definição de transformação em um repositório de código.

Opção	Forma longa	Parâmetro	Description
-p	--code-repository-path	<path>	Caminho para o repositório de código a ser transformado. Para o diretório atual, use “.”
-c	--build-command	<command>	Comando a ser executado ao criar o repositório
-n	--transformation-name	<name>	Nome da definição de transformação no registro
-x	--non-interactive	-	Executa a transformação sem assistência do usuário
-t	--trust-all-tools	-	Confia em todas as ferramentas (sem instruções de ferramentas)
-d	--do-not-learn	-	Opte por não permitir a extração da lição desta execução
-g	--configuration	<config>	Caminho para o arquivo de configuração (JSON ou YAML) ou pares chave=valor
--tv	--transformation-version	<version>	Versão da definição de transformação a ser usada

Opção	Forma longa	Parâmetro	Description
<code>--limit</code>	<code>--limit</code>	<code><limit></code>	Defina o limite de orçamento de minutos do agente . A transformação sai quando o limite é atingido e pode ser retomada com um limite aumentado
<code>-h</code>	<code>--help</code>	<code>-</code>	Exibir ajuda para o comando

lista de definição personalizada atx

Listar as definições de transformação disponíveis.

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

atx custom def get

Obtenha detalhes de uma definição de transformação específica.

Opção	Forma longa	Parâmetro	Description
<code>-n</code>	<code>--transformation-name</code>	<code><name></code>	O nome da definição de transformação a ser recuperada
<code>--tv</code>	<code>--transformation-version</code>	<code><version></code>	A versão da definição de transformação a ser recuperada
<code>--td</code>	<code>--target-directory</code>	<code><directory></code>	O diretório de destino no qual salvar a

Opção	Forma longa	Parâmetro	Description
			definição de transform ação (padrão: ".")
--json	--json	-	Resposta de saída no formato JSON
-h	--help	-	Exibir ajuda para o comando

atx custom def delete

Exclua uma definição de transformação permanentemente.

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

atx custom def publish

Publique uma definição de transformação no registro.

Opção	Forma longa	Parâmetro	Description
-n	--transfo rmation-name	<name>	O nome da definição de transformação a ser publicada
--tv	--transfo rmation-v ersion	<version>	A versão da definição de transformação a ser usada (não aplicável com --description ou --source-directory)
--sd	--source- directory	<directory>	O diretório de origem a partir do qual ler os arquivos de definição de transformação

Opção	Forma longa	Parâmetro	Description
			local (não aplicável com --transformation-version)
--description	--description	<description>	Uma descrição para a definição de transformação (não aplicável com --transformation-version)
--json	--json	-	Resposta de saída no formato JSON
-h	--help	-	Exibir ajuda para o comando

atx custom def save-draft

Salve uma definição de transformação como rascunho no registro. Os rascunhos expiram após 30 dias e não aparecem no registro. Esse comando retorna o número da versão do rascunho. Você deve executar e recuperar rascunhos explicitamente usando o nome da transformação e o número da versão.

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

Comandos da lição

aprendências de definição personalizada de impostos

Abra uma sessão interativa para ver e gerenciar as lições que uma definição de transformação aprendeu em execuções anteriores. Procure aulas por categoria, veja os detalhes das aulas e archive, restaure ou exclua aulas.

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

Comandos de tag

tags de lista de definição personalizada atx

Listar tags para uma definição de transformação.

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

tag de definição personalizada atx

Adicione tags a uma definição de transformação.

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

atx custom def untag

Remova as tags de uma definição de transformação.

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

Comandos de atualização

atualização fiscal

Atualize a CLI do AWS Transform.

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

Comandos MCP

ferramentas atx mcp

Permite que os clientes façam view/confirm suas configurações de ferramentas MCP. As atualizações nas configurações devem ser gerenciadas diretamente por meio do arquivo `~/.aws/atx/mcp.json`

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

AWS-Transformações gerenciadas

AWS-transformações gerenciadas são transformações pré-criadas e AWS aprovadas para casos de uso comuns que estão prontas para uso sem nenhuma configuração adicional.

Visão geral do

AWS- as transformações gerenciadas têm as seguintes características:

- Validado por AWS - Essas transformações são avaliadas por AWS serem de alta qualidade
- Pronto para usar - Nenhuma configuração adicional é necessária
- Crescendo continuamente - transformações adicionais estão sendo adicionadas continuamente
- Personalizável — Pre-built as transformações podem ser personalizadas fornecendo orientações adicionais ou requisitos específicos às necessidades da sua organização usando o `additionalPlanContext` parâmetro de configuração
- Suporte de acesso antecipado - Algumas transformações podem ser marcadas como acesso antecipado à medida que passam por testes e refinamentos adicionais

Available (Disponível) AWS-Transformações gerenciadas

O catálogo a seguir lista as transformações AWS gerenciadas que estão disponíveis atualmente, agrupadas por caso de uso. Cada tabela mostra o nome da transformação, o idioma ou a pilha à qual ela se aplica e seu status. Para encontrar uma transformação rapidamente, use a caixa de pesquisa na parte superior desta página para pesquisar por nome, idioma ou caso de uso.

Este catálogo é a lista canônica de transformações AWS gerenciadas. O Kiro Power, o plug-in do agente, o plug-in VS Code e a CLI executam as mesmas transformações. Para listar as transformações disponíveis em seu registro, execute `atx custom def list`.

Note

As transformações marcadas como Acesso antecipado são funcionais, mas podem ser atualizadas com frequência com base no feedback do cliente.

Atualizações de tempo de execução

Atualize um idioma ou tempo de execução para uma versão mais recente ou altere a distribuição do tempo de execução.

Transformação	Idioma/pilha	Status	Description
AWS/java-version-upgrade	Java	Disponível ao público	Atualize aplicativos Java usando qualquer sistema de compilação de qualquer versão do JDK de origem para qualquer versão do JDK de destino, com modernização de dependências, incluindo migração para o Jakarta EE, drivers de banco de dados, estruturas ORM e atualizações do ecossistema Spring. Especifique a versão de destino do JDK no chat ou com o additionalPlanContext parâmetro.
AWS/python-version-upgrade	Python	Disponível ao público	Migre projetos Python do Python 3.8 ou 3.9 para o Python 3.11, 3.12 ou 3.13 enquanto mantém a funcionalidade e o desempenho. Especifique a

Transformação	Idioma/pilha	Status	Description
			versão de destino do Python no chat ou com o additionalPlanContext parâmetro.
AWS/nodejs-version-upgrade	Node.js	Disponível ao público	Atualize Node.js aplicativos de qualquer Node.js versão de origem para qualquer Node.js versão de destino. Especifique a versão de destino no chat ou com o additionalPlanContext parâmetro.
AWS/lambda-nodejs-runtime-upgrade	Node.js (Lambda)	Acesso antecipado	Atualize as funções do AWS Lambda de Node.js tempos de execução mais antigos (nodejs4.3 a nodejs22.x) para nodejs24.x, abordando alterações significativas no Lambda Runtime Interface Client (RIC) e no tempo de execução de 24 linguagens. Node.js

Transformação	Idioma/pilha	Status	Description
AWS/oracle-java-to-corretto	Java (distribuição JDK)	Acesso antecipado	Migre projetos Java do Oracle JDK para o Amazon Corretto. Substitui as APIs Oracle-specific internas por equivalentes Java padrão, atualiza as configurações de compilação (Maven e Gradle) e imagens de base de contêineres, remove sinalizadores comerciais da JVM e gera um relatório de licenciamento.

Transformação	Idioma/pilha	Status	Description
AWS/ruby-upgrade	Ruby	Acesso antecipado	Atualize os aplicativos Ruby do Ruby 2.x para o Ruby 4.0 e suas estruturas para o Rails 8.0 ou Sinatra 4.1. Você pode usar essa transformação com Rails e ActiveRecord aplicativos, aplicativos Sinatra e gems autônomas. A transformação combina cada versão do Ruby com a atualização da estrutura correspondente e executa a suíte de testes. Em seguida, ele isola as falhas antes de avançar para a próxima versão.

Migrações de SDK

Migre entre as versões principais de um AWS SDK.

Transformação	Idioma/pilha	Status	Description
AWS/java-aws-sdk-v1-to-v2	Java	Disponível ao público	Atualize o AWS SDK da v1 para a v2 para projetos Java usando o Maven ou o Gradle.

Transformação	Idioma/pilha	Status	Description
AWS/python-boto2-to-boto3	Python	Disponível ao público	Migre aplicativos Python do boto2 para o boto3, com base na documentação oficial de migração. AWS
AWS/nodejs-aws-sdk-v2-to-v3	Node.js	Disponível ao público	Atualize os Node.js aplicativos do AWS SDK para JavaScript v2 para v3 para obter arquitetura modular, TypeScript suporte de primeira classe e desempenho aprimorado, sem alterar a versão. Node.js

Atualizações e migrações de estruturas

Atualize uma estrutura para uma versão mais recente ou migre para uma estrutura diferente.

Transformação	Idioma/pilha	Status	Description
AWS/spring-boot-version-upgrade	Java/Spring Boot	Disponível ao público	Atualize um aplicativo Spring Boot antigo para uma versão de destino do Spring Boot, incluindo arquivos de compilação e iniciadores, propriedades, pacotes Jackson 3, Spring Security 7 DSL, infraestrutura de teste

Transformação	Idioma/pilha	Status	Description
			e dependências de observabilidade.
AWS/JBoss-to-Spring-Boot	Java (JBoss ou WildFly para Spring Boot)	Acesso antecipado	Migre aplicativos corporativos Java EE ou Jakarta EE executados no JBoss EAP ou WildFly no Spring Boot, eliminando as dependências do servidor de aplicativos para um modelo de implantação em contêiner nativo da nuvem.
AWS/early-access-angular-to-react-migration	Angular para React	Acesso antecipado	Transforme um aplicativo Angular em React.
AWS/angular-version-upgrade	Angular	Acesso antecipado	Atualize um aplicativo Angular mais antigo para uma versão Angular de destino, incluindo componentes, serviços, modelos e roteamento.

Transformação	Idioma/pilha	Status	Description
AWS/vue.js-version-upgrade	Vue.js	Acesso antecipado	Execute uma atualização de versão principal de Vue.js 2 para Vue.js 3, modernizando componentes, gerenciamento de estado, roteamento e APIs globais. Atualizações secundárias e de patch estão fora do escopo.

GenAI e migrações de modelos

Migre cargas de trabalho generativas de IA para o.

Transformação	Idioma/pilha	Status	Description
AWS/GenAI-to-Bedrock-Migration-Assessment	Cargas de trabalho generativas de IA	Acesso antecipado	Avalie cargas de trabalho generativas de IA para migração de fornecedores terceirizados (OpenAI, Google Gemini, Anthropic direct e modelos de código aberto) para o. Descubra o uso e os modelos do SDK, esclarece os requisitos, projeta um mapeamento

Transformação	Idioma/pilha	Status	Description
			de modelos, estima custos e riscos e gera artefatos de avaliação. Assessment-only; não modifica o código-fonte. Também abrange estruturas agênticas, como CrewAI e Strands. LangGraph

Language-to-language migrações

Traduza uma base de código de uma linguagem de programação para outra.

Transformação	Idioma/pilha	Status	Description
AWS/vba-to-python-migration	VBA para Python	Acesso antecipado	Migre macros, UserForms módulos e lógica incorporada do Excel VBA para scripts e módulos Python equivalentes, usando openpyxl, pandas, tkinter ou 6 e bibliotecas padrão. PyQt O idioma de destino é o Python 3.8 ou posterior. Use ao converter código VBA incorporado em .bas, .cls, .frm ou .xlsm.

Migrações de banco de dados

Nenhuma transformação AWS gerenciada específica do banco de dados está disponível no momento. Para modernizar os bancos de dados Microsoft SQL Server e seus aplicativos.NET associados ao Amazon Aurora PostgreSQL, consulte. [the section called “Modernização do SQL Server”](#)

Observabilidade

Modernize o registro e o monitoramento para AWS serviços nativos.

Transformação	Idioma/pilha	Status	Description
AWS/early-access-log4j-to-slf4j-migration	Java (registro em log)	Acesso antecipado	Migre aplicativos Java do Log4j (1.x ou 2.x) para o SLF4J com um back-end Logback. Lida com código-fonte, gerenciamento de dependências (Maven e Gradle) e registra arquivos de configuração, além de validar por compilação, teste e verificação de importação residual.
AWS/datadog-monitors-to-cloudwatch-alarms	Infraestrutura como código/monitoramento	Acesso antecipado	Migre monitores DataDog métricas que rastreiam métricas de AWS serviço e métricas personalizadas para CloudWatch alarmes nativos como infraestrutura como código. Gera CloudForm

Transformação	Idioma/pilha	Status	Description
			ation YAML, CDK TypeScript e Terraform HCL.

Arquitetura

Re-architect, reformule a plataforma ou otimize aplicativos para AWS.

Transformação	Idioma/pilha	Status	Description
AWS/java-performance-optimization	Java (desempenho)	Disponível ao público	Otimize o desempenho do aplicativo Java analisando os dados de criação de perfil do JFR para detectar pontos de acesso e antipadrões de CPU e memória e, em seguida, aplicando correções de código direcionadas. Para obter instruções sobre como coletar dados do JFR, consulte o guia de tempo de execução do JFR .
AWS/early-access-java-x86-to-graviton	Java (Arm64/Graviton)	Acesso antecipado	Valide a compatibilidade do aplicativo Java com a arquitetura Arm64 para processadores AWS Graviton e resolva incompatibilidades atualizan

Transformação	Idioma/pilha	Status	Description
			do dependências, detectando padrões de código específicos da arquitetura e recompilando bibliotecas nativas quando o código-fonte estiver disponível. Muitos aplicativos Java modernos já existem Arm64-compatible.
AWS/oracle-service-bus-to-aws	Java//integração com a tecnologia sem servidor	Acesso antecipado	Migre as configurações do processo Oracle Service Bus (OSB) e BPEL para uma arquitetura sem servidor AWS nativa, gerando um projeto CDK implantável com TypeScript Amazon API Gateway, Lambda e Step Functions. AWS AWS

Transformação	Idioma/pilha	Status	Description
AWS/mulesoft-to-aws-native	Java/ MuleSoft para sem servidor	Acesso antecipado	Transforme os aplicativos MuleSoft Mule 3.x e 4.x em arquiteturas AWS sem servidor (Amazon API Gateway, AWS Lambda e AWS Step Functions) direcionadas ao Java 17 no Lambda com. AWS SnapStart A transformação mapeia acionadores de fluxo para fontes de AWS eventos, converte DataWeave expressões MEL (MuleSoft Expression Language) em AWS equivalentes e substitui conectores por chamadas do SDK for AWS Java v2. Ela produz modelos de SAM, manipuladores AWS Lambda e testes JUnit 5.

Transformação	Idioma/pilha	Status	Description
AWS/payshield-hsm-to-aws-payment-cryptography	Java (HSM para criptografia AWS de pagamento)	Disponível ao público	Migre aplicativos Java do protocolo do módulo de segurança de PayShield hardware (HSM) da Thales para o AWS Payment Cryptography SDK v2. A migração inclui mapeamento de comandos, migração de chaves, configuração de dependências e testes de paridade.

Análise de base de código

Analise bases de código e portfólios para planejar a modernização. Essas transformações produzem relatórios e não modificam seu código.

Transformação	Idioma/pilha	Status	Description
AWS/comprehensive-codebase-analysis	Vários idiomas	Disponível ao público	Realize uma análise estática profunda de uma base de código para gerar documentação hierárquica com referências cruzadas que combine análise comportamental, documentação arquitetônica e inteligência comercial, com ênfase em

Transformação	Idioma/pilha	Status	Description
			insights técnicos sobre dívidas.
AWS/agenti- c-readiness-analy- sis	Vários idiomas	Acesso antecipado	Avalie se os sistemas estão prontos para serem chamados com segurança por agentes de IA, abrangendo APIs, identidade, gerenciamento de estado, humanos no circuito e observabilidade.
AWS/moder- nization- readiness- analysis	Vários idiomas	Acesso antecipado	Examine os portfólios em busca de lacunas de maturidade nativas na nuvem e mapeie as descobertas para AWS os caminhos de modernização.
AWS/portfolio- agenti- c-readi- ness-analysis	Portfólio	Acesso antecipado	Agregue relatórios individuais de análise de prontidão do agente em um portfólio de aplicativos para identificar obstáculos transversais, padrões de remediação compartilhados e recomendações prioritizadas.

Transformação	Idioma/pilha	Status	Description
AWS/portfolio-modernization-readiness-analysis	Portfólio	Acesso antecipado	Agregue relatórios individuais de análise de modernização em um portfólio em um roteiro consolidado com ondas de migração priorizadas e caminhos de modernização recomendados.

Transformação	Idioma/pilha	Status	Description
AWS/business-rules-extraction	Vários idiomas	Acesso antecipado	Essa transformação analisa estaticamente uma base de código monolítica para produzir documentação pronta para reescrita sem exigir uma construção, execução ou modificações no código-fonte. Ele decompõe o sistema em domínios limitados e extrai regras de negócios, fluxos de trabalho, questões transversais e estrutura de banco de dados por domínio. O resultado inclui um manifesto legível por máquina, um painel interativo e especificações de implementação de linguagem neutra por domínio para orientar a modernização ou a regravação completa.

Personalizar AWS-Transformações gerenciadas

Você pode personalizar as transformações AWS gerenciadas para atender às necessidades específicas da sua organização fornecendo contexto adicional por meio do parâmetro de `additionalPlanContext` configuração.

Exemplo: personalização da atualização da versão Java

```
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.
```

Exemplo: personalização da migração do AWS SDK

```
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.
```

Casos de uso comuns

Esta seção fornece orientação passo a passo para cenários de transformação comuns usando a CLI do Transform AWS .

Atualizações do Lambda Runtime

O Lambda suspende periodicamente os tempos de execução de linguagens mais antigas, exigindo que as equipes atualizem suas funções do Lambda para versões compatíveis. AWS O Transform custom pode automatizar essas atualizações usando as transformações de atualização de versão AWS de linguagem gerenciada. Por exemplo, para atualizar uma função Lambda escrita em Python 3.9 para Python 3.13, você usaria a transformação. `AWS/python-version-upgrade` Transformações semelhantes estão disponíveis para Java (`AWS/java-version-upgrade`) e

Node.js (AWS/nodejs-version-upgrade), abrangendo as linguagens de tempo de execução Lambda mais comuns.

Para atualizar uma única função do Lambda de forma interativa, navegue até a raiz do repositório de origem da sua função e inicie a CLI do Transform AWS com. `atx` Na sessão interativa, descreva a atualização de que você precisa — por exemplo, “Atualize esta função Lambda do Python 3.9 para o Python 3.13”. O agente selecionará a transformação AWS gerenciada apropriada, analisará seu código, atualizará a sintaxe da linguagem, ajustará as dependências e modernizará as chamadas de API obsoletas. Você pode fornecer um comando de compilação ou validação `python -m py_compile *.py` para que o agente possa verificar se o código transformado compila e passa nos testes. `pytest` Durante a sessão interativa, você pode revisar as alterações propostas pelo agente, fornecer feedback e solicitar ajustes antes de aceitar o resultado final.

Quando precisar atualizar os tempos de execução do Lambda em vários repositórios, use o modo não interativo para executar transformações em grande escala. Para cada repositório, invoque a CLI com os sinalizadores apropriados para execução sem a entrada do usuário. Por exemplo, para atualizar uma função Lambda Node.js 16 para Node.js 22:

```
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
```

O `-x` sinalizador executa a transformação de forma não interativa e `-t` confia em todas as execuções de ferramentas, portanto, nenhuma solicitação é necessária. Você pode programar esse comando em dezenas ou centenas de repositórios usando um simples loop de shell. Depois que cada transformação for concluída, revise o Git diff para verificar as alterações e execute sua suíte de testes para confirmar se a função atualizada funciona corretamente. Você também pode integrar o AWS Transform custom em seu CI/CD pipeline para identificar continuamente funções obsoletas do Lambda. Essa abordagem não apenas aborda o problema imediato de tempos de execução obsoletos, mas também estabelece um processo contínuo para detectar e atualizar funções antes que elas atinjam o status de fim do suporte.

As equipes da plataforma central podem criar campanhas por meio do [aplicativo web AWS Transform](#) para definir a transformação, especificar repositórios Lambda de destino e acompanhar o progresso em toda a organização. Para uma explicação detalhada da criação de uma solução de

implantação em escala de nível de produção usando o AWS Batch, [consulte Criando uma solução escalável](#) de modernização de código com o Transform custom. AWS

AWS Transform endpoints personalizados e de interface (AWS PrivateLink)

Você pode estabelecer uma conexão privada entre sua VPC e a AWS Transform personalização criando uma interface VPC endpoint. Os endpoints de interface são alimentados por [AWS PrivateLink](#) uma tecnologia que permite acessar serviços AWS Transform personalizados de forma privada sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão. Direct Connect O tráfego entre sua VPC e o AWS Transform personalizado não sai da rede Amazon.

Cada endpoint de interface é representado por uma ou mais [Interfaces de Rede Elástica](#) nas sub-redes.

Para obter mais informações, consulte [Endpoints da VPC da interface \(AWS PrivateLink\)](#) no Manual do Usuário do Amazon VPC.

Note

- Você deve habilitar a AWS PrivateLink integração para o Amazon S3, pois o cliente faz chamadas AWS Transform de API do S3. Para obter instruções detalhadas, consulte a [AWS PrivateLink documentação do Amazon S3](#). Se você encontrar problemas de acesso ao S3 ao usar o AWS Transform personalizado, consulte nosso [guia de solução de problemas](#).
- Se você não estiver usando o recurso DNS AWS PrivateLink privado (consulte [DNS privado](#)), você deve:
 - Configurar o roteamento para endpoints da interface VPC (consulte a documentação do [roteamento para endpoints da interface VPC](#))
 - Defina a variável de ATX_CUSTOM_ENDPOINT ambiente para especificar seu domínio personalizado, por exemplo:

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

Considerações para AWS Transform endpoints VPC personalizados

Antes de configurar uma interface VPC endpoint para AWS Transform personalização, certifique-se de revisar as [propriedades e limitações do endpoint da interface no](#) Guia do usuário da Amazon VPC.

AWS Transform suporte personalizado para fazer chamadas para todas as suas ações de API por meio do endpoint da interface.

Pré-requisitos

Antes de começar, verifique se você tem:

- Uma AWS conta com as permissões apropriadas para criar e configurar recursos.
- Uma VPC já criada em sua AWS conta.
- Familiaridade com AWS serviços, especialmente Amazon VPC AWS Transform e personalizados.

Criação de uma interface VPC endpoint para AWS Transform personalizado

Você pode criar um VPC endpoint para o serviço AWS Transform personalizado usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte [Criar um endpoint de interface](#) no Guia do usuário da Amazon VPC.

Crie os seguintes VPC endpoints AWS Transform personalizados usando esse nome de serviço:

- com.amazonaws. *region*.transform-custom

region Substitua pela AWS região em que você deseja usar a CLI AWS Transform personalizada, por exemplo, com.amazonaws.us-east-1.transform-custom.

Para mais informações, consulte [Acessar um serviço por um endpoint de interface](#) no Guia do usuário da Amazon VPC.

Criação de uma política de VPC endpoint para AWS Transform personalizado

Você pode anexar uma política de endpoint ao seu VPC endpoint que controla o acesso à personalização. AWS Transform Essa política especifica as seguintes informações:

- A entidade principal que pode realizar ações.
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para mais informações, consulte [Controlar o acesso a serviços com VPC endpoints](#) no Guia do usuário da Amazon VPC.

Exemplo: política de VPC endpoint para AWS Transform personalizar ações

Veja a seguir um exemplo de uma política de endpoint AWS Transform personalizada. Quando anexada a um endpoint, essa política concede acesso às ações AWS Transform personalizadas listadas para todos os diretores em todos os recursos.

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

Usando um computador local para se conectar a um AWS Transform endpoint personalizado

Esta seção descreve o processo de usar um computador local para se conectar ao AWS Transform personalizado por meio de um AWS PrivateLink endpoint em sua AWS VPC.

1. [Crie uma conexão VPN entre seu dispositivo on-premises e sua VPC.](#)

2. [Crie uma interface VPC endpoint personalizada. AWS Transform](#)
3. [Configure um endpoint de entrada do Amazon Route 53](#). Isso permitirá que você use o nome DNS do seu endpoint AWS Transform personalizado a partir do seu dispositivo local.

Solução de problemas

Esta seção fornece orientação para solucionar problemas comuns com o AWS Transform custom.

Localizações de registros

AWS O Transform CLI mantém registros nos seguintes locais:

Registros de conversas:

Linux and macOS

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

Windows

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

Esses registros contêm o histórico completo de conversas para depurar execuções de transformação específicas.

Registros do subagente:

Linux and macOS

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

Windows

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

Esses registros contêm saídas de subagentes que o agente principal gera durante as transformações. Você não precisa gerenciar subagentes diretamente.

Registros de depuração do desenvolvedor:

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
```

Esses registros fornecem informações detalhadas sobre operações e erros da CLI. Cada arquivo de log tem um limite de 5 MB antes de ser transferido. Pode haver vários registros de depuração nesse diretório, como debug1.log e debug2.log.

Problemas comuns

Problemas de instalação:

Se a instalação falhar, verifique se você tem o Node.js 22 ou posterior instalado:

```
node --version
```

Faça o Node.js download, <https://nodejs.org/en/download> se necessário.

Problemas de autenticação:

Verifique se suas AWS credenciais estão configuradas corretamente:

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

Certifique-se de que seu usuário ou função do IAM tenha as `transform-custom:*` permissões necessárias.

Problemas de conectividade de rede:

Se você encontrar erros de conexão, verifique o acesso à rede aos endpoints necessários:

- `transform-cli.awsstatic.com`

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

Se estiver trabalhando em um ambiente restrito à Internet, atualize as regras de firewall para permitir esses URLs.

Problemas de configuração da região:

Se você encontrar erros relacionados à região:

- Verifique se sua região é suportada
- Verifique as variáveis de ambiente que podem substituir sua configuração: `echo $AWS_REGION $AWS_DEFAULT_REGION`
- Verifique a configuração da sua região: `aws configure get region`
- Atualize sua região, se necessário: `aws configure set region <your-region>`
- Verifique os registros de depuração para obter detalhes sobre a resolução da região

Problemas com o Git:

Certifique-se de que o Git esteja instalado e que seu repositório esteja sob controle de origem do git:

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

AWS O Transform custom exige que os repositórios estejam sob controle de origem do git.

Problemas de execução da transformação:

Se uma transformação falhar:

1. Revise os registros de conversas em `~/.aws/atx/custom/<conversation_id>/logs/`
2. Verifique se há falhas de construção ou teste na saída da transformação
3. Verifique se o comando build está correto para seu projeto
4. Tente executar a transformação no modo interativo para fornecer feedback

Problemas de retomada da conversa:

Se você não conseguir retomar uma conversa:

- Verifique se a conversa tem menos de 30 dias
- Verifique se o ID da conversa está correto
- Verifique se você tem conectividade de rede

Como obter suporte

Para obter assistência adicional, acesse AWS Support por meio do [AWS console](#).

Ao abrir um ticket de suporte, inclua:

- Registros de conversas de `~/.aws/atx/custom/<conversation_id>/logs/`
- Registros de subagentes de `~/.aws/atx/custom/<conversation_id>/logs/subagents/`
- Registros de depuração de `~/.aws/atx/logs/`
- Etapas para reproduzir o problema
- AWS Transformar versão CLI () `atx --version`

Problemas de acesso ao S3

O serviço personalizado AWS Transform vende URLs pré-assinados do S3 para facilitar o upload e o download de máquinas clientes de arquivos de transformação potencialmente grandes. to/from Isso significa que a CLI não apenas interage com os endpoints do serviço AWS Transform, mas também interage com os endpoints do serviço S3. Essas interações usam URLs pré-assinadas para que as credenciais do IAM do seu cliente não exijam nenhuma permissão do S3, mas às vezes as configurações do servidor proxy da sua máquina local e as políticas de VPC Endpoint do S3 da sua rede podem restringir esse tráfego.

Examine as mensagens de erro mais detalhadas [the section called “Localizações de registros”](#) para ajudar a raiz a causar qualquer falha na ferramenta ou o acesso ao S3 negado relacionado ao download e upload de arquivos de transformação.

Se você estiver usando um VPN/Proxy servidor que utiliza as variáveis de `no_proxy` ambiente `https_proxy` e, considere adicionar os seguintes valores ao valor da variável de `no_proxy` ambiente para ignorar o proxy dos endpoints de serviço personalizados do S3 e do AWS Transform, por exemplo:

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"
```

Se você estiver usando um [AWS PrivateLink para o Amazon S3](#) em sua VPC, isso pode ter uma política definida para restringir o tráfego do S3. Certifique-se de que sua política de endpoint VPC do S3 GetObject permita PutObject e opere os buckets de propriedade AWS do serviço personalizado Transform. Isso pode ser feito adicionando a seguinte declaração à sua política de VPC endpoint:

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

DenyDeclarações explícitas em políticas têm precedência sobre Allow declarações. Analise as políticas do S3 VPC Endpoint Deny para ver declarações que possam estar restringindo o acesso.

AWS Histórico de versões do Transform CLI

Consulte a tabela a seguir para obter detalhes sobre as versões atuais e anteriores da CLI do AWS Transform. A tabela inclui a versão, a data de lançamento e as notas de lançamento de cada versão.

Versão	Data de lançamento	Notas da versão
3.6.0 (mais recente)	17 de julho de 2026	Foi adicionado o <code>atx custom def learnings</code> subcomando, que abre uma sessão interativa de TUI para visualizar e gerenciar os aprendizados gerados automaticamente para uma definição de transformação com base em execuções anteriores.

Versão	Data de lançamento	Notas da versão
		• Foi adicionada a coleta de telemetria de uso durante a execução da transformação. Para desativar a telemetria, defina a variável de <code>ATX_DISABLE_TELEMETRY=true</code> ambiente. Para obter mais informações, consulte Telemetria de uso. • Corrigido um problema no Windows em que as operações de arquivo usando caminhos ~ (diretório inicial) eram resolvidas para um diretório inesperado. Isso causou read/write falhas no arquivo durante uma sessão. • Corrigido um problema em que nomes de servidores e ferramentas MCP contendo caracteres especiais podiam causar falhas de conexão. A CLI agora limpa automaticamente os nomes para usar somente caracteres válidos.

Versão	Data de lançamento	Notas da versão
3.5.0	8 de julho de 2026	- Foi adicionado suporte nativo ao Windows. Agora você pode executar os comandos AWS Transform Custom diretamente no Windows. (Os atx ct comandos ainda não são suportados no Windows) - Foram adicionadas entradas de direção para atx ct analysis run que as análises de prontidão e modernização do agente reflitam suas preferências. Use --context para enquadramento estratégico, --agent-scope para definir o acesso do agente para garantir a prontidão do agente --prefer e/ou para --avoid direcionar as recomendações de modernização para ou para longe de tecnologias específicas. - As definições de transformação no formato de habilidade agora podem incluir uma scripts/ pasta, permitindo que você agrupe scripts auxiliares ao lado dos seus SKILL.md e das referências. - Adicionado --wait aatx ct remediation create , que aguarda até que a remediação seja concluída. - Foi adicionado o modo headless para execução única. Execute atx -x "prompt" -t para passar uma solicitação, obter uma resposta e saia sem solicitações interativas. O modo sem cabeça requer confiar em todas as ferramentas.
3.4.1	2 de julho de 2026	Corrigido um problema de sessão interativa introduzido pela versão 3.4.0. Depois que o agente terminar de responder, a CLI poderá permanecer no prompt “Pensando” (mostrado com reticências na interface do usuário) em vez de retornar ao prompt de entrada. A CLI agora retorna você ao prompt de entrada após cada resposta.

Versão	Data de lançamento	Notas da versão
3.4.0 (não recomenda do)	29 de junho de 2026	 Problema conhecido Em sessões interativas, a CLI pode permanecer no prompt “Pensando” (mostrado com uma elipse na interface do usuário) depois que o agente terminar de responder. Isso impede que você insira sua próxima mensagem. Para resolver esse problema, atualize para a versão 3.4.1 ou posterior executando <code>atx update</code>. • Foi adicionado <code>atx ct schema</code> um manifesto legível por máquina de toda a superfície de <code>atx ct</code> comando para criação de scripts e automação. • Foi adicionada a validação do escopo do token quando você adiciona ou atualiza uma fonte, revelando problemas de credenciais ou permissões imediatamente, em vez de falhar posteriormente durante a análise. • As pull requests de correção automática aprimoradas para incluir a localização de contexto e o modo de rascunho de suporte para PRs mais revisáveis. • Feedback aprimorado do progresso da CLI com contexto em tempo real sobre a atividade atual, minutos estimados do agente e atividade do subagente. • Foi adicionada a identidade configurável do autor do commit do ponto de verificação por meio das variáveis de <code>ATX_GIT_COMMITTER_EMAIL</code> ambiente <code>ATX_GIT_COMMITTER_NAME</code> e. • Várias pequenas correções de bugs e melhorias.

Versão	Data de lançamento	Notas da versão
3.3.0	18 de junho de 2026	• Foi adicionada consistência <code>--json</code> e <code>--help</code> suporte em todos <code>atx ct</code> os comandos. • A configuração do agente de segurança foi corrigida para que o espaço do agente fosse criado durante a configuração e removido na desmontagem. • Várias pequenas correções de bugs e melhorias.
3.2.0	15 de junho de 2026	• Foram adicionados comandos de modernização contínua (<code>atx ct</code>) à distribuição padrão da CLI para todos os usuários. • Execução aprimorada de subagentes para mostrar um botão giratório “Pensando...” enquanto aguarda as respostas do servidor, fornecendo um feedback visual claro de que o trabalho está em andamento. • O botão giratório foi aprimorado para reiniciar automaticamente com “Working on it...” após 3 segundos de silêncio após a saída do agente, para que o terminal nunca pareça congelado entre as etapas de processamento. • Girador de pensamento aprimorado com uma animação sutil de brilho para uma aparência visual mais polida.

Versão	Data de lançamento	Notas da versão
3.1.0	3 de junho de 2026	• Variável de <code>ATX_MAX_VALIDATION_LOOPS</code> ambiente adicionada para configurar o máximo de loops de validação. • A verificação de atualização corrigida não mostra mais falsos avisos de “atualização disponível” quando a versão instalada já é mais recente que a versão do registro. • Corrigido <code>delete --transformation-name ""</code> não mostra mais uma solicitação de confirmação sem sentido; valores vazios agora são rejeitados com um claro erro de validação. • Os subcomandos não reconhecidos corrigidos agora mostram “comando desconhecido” em vez de uma mensagem de erro interna confusa. • Comparação de versões corrigida para usar comparação numérica em vez de desigualdade de string para verificações de atualização.
3.0.0	21 de maio de 2026	• Foi adicionada a validação de nome de transformação pré-voos que sugere nomes semelhantes do seu registro quando um nome não é encontrado, ajudando a detectar erros de digitação sem precisar de um comando de lista separado. • Foram adicionadas explicações opcionais para comandos shell, mostrando o que eles fazem e por quê. • Banner de configurações de confiança aprimorado para incluir mais informações sobre as permissões da ferramenta. • Foi adicionado um banner de desativação de aprendizagem ao usar o sinalizador de não aprender, dando visibilidade ao recurso de aprendizado e como ativá-lo. • Alteração significativa: Node.js 22 ou posterior agora é necessária. Faça o upgrade https://nodejs.org/ se você estiver usando uma versão mais antiga.

Versão	Data de lançamento	Notas da versão
2.0.0	14 de maio de 2026	• Suporte de servidor MCP remoto adicionado — conecte-se a servidores MCP HTTP e HTTPS com fallback automático de SSE, autenticação de token Bearer com expansão variável de ambiente nos cabeçalhos e suporte a proxy (). HTTP_PROXY/HTTPS_PROXY • Adicionado <code>atx resume</code> subcomando como alias para <code>atx --resume</code> • <code>grep</code> Ferramenta adicionada para pesquisa de texto em vários arquivos com controle de saída — suporta padrões de regex, filtragem global de arquivos, pesquisa sem distinção entre maiúsculas e minúsculas, limites configuráveis e truncamento de saída. <code>depth/result</code> • Implementação aprimorada do MCP para usar o SDK MCP padrão para um comportamento mais consistente e suporte mais fácil para recursos futuros do MCP. • Manipulação aprimorada da saída do shell — a saída agora é normalmente truncada em 30 mil caracteres por fluxo, em vez de causar um erro grave, preservando o início e o fim da saída para o contexto. • Corrigido um problema em que Ctrl+C durante uma sessão interativa podia sair prematuramente da CLI ativada Linux/macOS em vez de abortar a operação atual e retornar ao prompt. • Mensagem de rejeição de confiança corrigida para mostrar um motivo específico pelo qual a confiança não está disponível, além do motivo pelo qual o comando precisava de autorização. • O aviso de comando perigoso corrigido não menciona mais a confiança quando o comando está ativado. <code>alwaysPromptCommands</code>

Versão	Data de lançamento	Notas da versão
1.10.0	29 de abril de 2026	• Descrições aprimoradas das ferramentas com orientação entre ferramentas, ajudando o agente a escolher a melhor ferramenta para cada tarefa e reduzindo o uso desnecessário do shell. • <code>alwaysPromptCommands</code> Adicionado <code>trust-settings.yaml</code> — configure padrões de comando do shell que sempre exigem permissão explícita, independentemente das configurações de confiança. Suporta curingas globais e corresponde a cada subcomando em expressões compostas. <code>trustedShellCommands</code> pode anular esses padrões. Não aplicado no modo não interativo para evitar a interrupção de tubulações automatizadas. • Caminhos relativos fixos que não estão sendo resolvidos em caminhos absolutos.
1.9.0	23 de abril de 2026	• Solicitações aprimoradas de aprovação da ferramenta — cada opção agora mostra o que ela faz em linha, uma mensagem “Por quê” explica por que a aprovação é necessária e a confirmação de confiança inclui uma dica sobre <code>trust-settings.yaml</code> a confiança permanente.
1.8.0	16 de abril de 2026	• O prefixo de saída do agente foi alterado de <code>ATX:</code> para <code>></code> para uma distinção visual mais clara entre a entrada do usuário e a saída do agente. • Exibição fixa do comando resume quando as novas tentativas da CLI estão esgotadas. • Currículo fixo de um diretório de trabalho diferente. No modo interativo, solicita o caminho corrigido; no modo não interativo, falha rapidamente com um erro descritivo.

Versão	Data de lançamento	Notas da versão
1.7.1	9 de abril de 2026	- Falha de login de SSO corrigida (“Token de sessão não encontrado ou inválido”) quando a região do provedor de credenciais é diferente da do perfil. <code>sso_region</code> - O cache de credenciais foi corrigido para que sessões de longa duração não falhem mais quando as credenciais são giradas no disco.
1.7.0	2 de abril de 2026	<code>execComando</code> fixo para sair com o código 1 em erros de validação de entrada, tornando a CLI confiável em scripts e CI/CD pipelines. - Foi adicionada a exibição de mensagens de aviso do serviço. - Foi adicionado suporte imediato de MFA para perfis de AWS credenciais. - Chamadas de credenciais STS fixas para respeitar as configurações de proxy HTTP (S).
1.6.0	18 de março de 2026	<code>--limit <minutes></code> Opção adicionada para definir um orçamento de minutos do agente <code>exec</code> e <code>interactive</code> comandos. Quando o limite é atingido, a CLI exibe o uso e sai com as instruções de retomada. - Registro fixo da mensagem inicial do usuário nos registros de conversas.
1.5.0	11 de março de 2026	- Foi adicionado suporte para execução simultânea de tarefas, permitindo transformações mais rápidas. - Foi adicionada a exibição de uso dos Minutos do Agente no final de cada conversa e o <code>/usage</code> comando no modo interativo para verificar o uso a qualquer momento.

Versão	Data de lançamento	Notas da versão
1.4.0	2 de março de 2026	• Mensagens de erro aprimoradas ao salvar definições de transformação com arquivos não suportados. • Foi adicionado tempo limite às chamadas de serviço para evitar que a CLI seja interrompida quando a conexão for interrompida. • O processo de CLI foi corrigido após a conclusão bem-sucedida. • Validação de região fixa ao retomar conversas.
1.3.0	19 de fevereiro de 2026	• Restrição removida para caminhos do servidor MCP — os usuários agora podem especificar qualquer caminho para a command propriedade na configuração do MCP. • Estabilidade aprimorada das conexões do servidor MCP.
1.2.0	9 de fevereiro de 2026	• Foi adicionado suporte para configuração de proxy por meio de variáveis de ambiente (<code>https_proxy</code> <code>no_proxy</code>, etc.). • Melhorias gerais de estabilidade e correções de bugs.
1.1.1	16 de janeiro de 2026	Correções de erros e melhorias na estabilidade.
1.1.0	13 de janeiro de 2026	Foi adicionado suporte à configuração de região da AWS CLI, verificações antecipadas de validação de credenciais e funcionalidade fixa de currículo de campanha.
1.0.1	18 de dezembro de 2025	Desligamentos simples, registros de erros mais limpos e melhorias gerais.
1.0.0	1 de dezembro de 2025	Versão inicial do AWS Transform CLI.

AWS Transforme a modernização contínua

O que é AWS Transformar a modernização contínua?

AWS A modernização contínua do Transform fornece análise e remediação para seus repositórios de código-fonte. Você pode conectar GitHub organizações, GitLab grupos, espaços de trabalho do Bitbucket e repositórios locais e, em seguida, executar análises automatizadas para identificar débitos técnicos, vulnerabilidades de segurança, oportunidades de modernização e prontidão do agente em toda a sua base de código.

Todas as análises e correções são executadas Conta da AWS usando suas credenciais. Seu código-fonte permanece sob seu controle.

Note

Recomendamos começar com o plug-in Kiro Power ou agente. A habilidade do agente coordena a configuração, a integração e o uso contínuo da modernização contínua, incluindo provisionamento de infraestrutura, configuração da fonte, execução de análises, triagem de descobertas e remediação. Para obter instruções de instalação, consulte [Ferramentas de desenvolvedor](#).

Capacidades gerais

AWS A modernização contínua do Transform fornece os seguintes recursos:

- **Análise da dívida técnica** — Examine os repositórios em busca de dependências desatualizadas, vulnerabilidades de segurança, problemas de qualidade de código e oportunidades de modernização. Execute varreduras rápidas de metadados em manifestos de pacotes ou uma análise abrangente em nível de código. Defina critérios de análise personalizados usando definições de transformação adaptadas ao seu ambiente.
- **Remediação autônoma** — gere pull requests validados em grande escala. Cada descoberta pode ser corrigida automaticamente usando sua definição de transformação associada. A remediação cria ramificações e abre PRs/MRs automaticamente no Bitbucket GitHub e no Bitbucket. GitLab
- **Relatórios** — Gere relatórios em HTML mostrando as descobertas por gravidade, repositório e tipo de análise. Acompanhe o progresso da remediação e encontre uma solução ao longo do tempo.

- Monitoramento contínuo — Programe análises recorrentes usando o Amazon EventBridge Scheduler. Configure programações cron diárias, semanais ou personalizadas para monitorar continuamente seu portfólio em busca de novos problemas.

Tipos de análise

AWS A modernização contínua do Transform oferece suporte aos seguintes tipos de análise para atender às suas necessidades de modernização.

Tipo	Description
<code>rapid-techdebt-analysis</code>	Análise rápida somente de metadados dos manifestos de pacotes (<code>pom.xml</code> , <code>package.json</code> , <code>requirements.txt</code>) para identificar versões obsoletas e dependências desatualizadas. Não analisa o código-fonte.
<code>tech-debt-comprehensive</code>	Análise técnica profunda da dívida em nível de código usando o agente AWS Transform. Examina o código-fonte para identificar padrões de dívida, problemas de qualidade do código, preocupações com a arquitetura e oportunidades de melhoria.
<code>security</code>	Vulnerabilidade de segurança e detecção de CVE usando o AWS Security Agent. Verifica o código-fonte e as dependências em busca de vulnerabilidades conhecidas, padrões de codificação inseguros e fraquezas exploráveis. Requer configuração única da infraestrutura.
<code>agentic-readiness</code>	Avaliação da prontidão para integração de agentes e IA. Classifica 56 critérios em cinco categorias: infraestrutura e plataforma, arquitetura de aplicativos Identity/Security/Governance, fundamentos de dados e operações e observabilidade.

Tipo	Description
modernization-readiness	Avaliação da oportunidade de modernização da nuvem. Avalia a prontidão nas dimensões de infraestrutura, aplicativos, dados, segurança e operações. Identifica candidatos para containerização, migração sem servidor e atualizações de plataforma.
custom	Execute qualquer definição de transformação (TD) como uma análise. Use esse tipo para definir seus próprios critérios de análise ou para executar transformações AWS gerenciadas não cobertas pelos tipos incorporados.

Explicação sobre os principais conceitos

Fontes

Uma fonte informa à modernização contínua onde estão seus repositórios. Tipos de origem com suporte:

- GitHub— Organizações com tokens de acesso pessoal (clássico)
- GitLab— Grupos ou usuários, incluindo instâncias auto-hospedadas
- Bitbucket — Espaços de trabalho (nuvem) ou projetos (data center)
- Local — Diretórios principais contendo repositórios git

Repositórios

Os repositórios são descobertos pelas fontes de varredura. Após a descoberta, você pode filtrar por origem, rótulos ou outros critérios; aplicar rótulos para organização (equipe, prioridade, onda de migração); e direcionar repositórios específicos para análise ou remediação.

Análises

Uma análise é uma verificação de um ou mais repositórios usando um tipo de análise específico. Cada análise produz descobertas que identificam problemas em seu código. Você pode executar análises sob demanda ou programá-las para serem executadas automaticamente. Os tipos de análise incluem análise rápida da dívida tecnológica, abrangente da dívida técnica, segurança, prontidão para agentes, prontidão para modernização e personalização. Cada análise rastreia seu status (pendente, em execução, concluído, cancelado ou com falha) e os repositórios que ela examinou.

Conclusões

As descobertas são os resultados da análise. Cada descoberta inclui severidade (alta, média ou baixa), status (aberta, rejeitada ou obsoleta) e a transformação de correção que pode remediá-la (se for corrigida automaticamente). Novas descobertas começam como abertas. Os usuários podem descartar as descobertas por um motivo. Re-analysis marca automaticamente as descobertas resolvidas como obsoletas.

Remediações

As remediações aplicam definições de transformação para corrigir as descobertas. Três modos: baseado em descobertas (cada descoberta usa sua própria transformação fixa), substituição de TD (substituir a definição de transformação para descobertas especificadas) e TD direto (executar uma transformação em um repositório sem descobertas). A saída depende do provedor de origem (GitHub PR, GitLab MR, Bitbucket PR ou filial local).

Definições de transformação

Uma definição de transformação contém as instruções e o conhecimento necessários para realizar uma transformação de código específica. A modernização contínua usa definições de transformação para análise personalizada (`--type custom --transformation-name name`) e remediação (`--transformation-name name`). Liste as definições de transformação disponíveis com `atx custom def list`.

Como AWS Transforme os trabalhos de modernização contínua

AWS A modernização contínua do Transform é normalmente usada em projetos de grande escala em que várias bases de código precisam de análise e remediação contínuas. Normalmente, as equipes seguem esse fluxo de trabalho:

1. **Connect Sources** — Adicione GitHub organizações, GitLab grupos, espaços de trabalho do Bitbucket ou diretórios locais como fontes. Forneça tokens de autenticação com escopos apropriados.
2. **Descubra repositórios** — Execute escaneamentos de descoberta para enumerar todos os repositórios em suas fontes. Use rótulos para organizar repositórios por equipe, prioridade ou onda de migração.
3. **Execute análises** — Execute análises em todo o seu portfólio. Escolha escaneamentos rápidos para resultados rápidos ou análises abrangentes para descobertas detalhadas. A análise de segurança requer uma configuração única da infraestrutura.
4. **Descobertas de triagem** — Analise as descobertas por gravidade, repositório ou tipo de análise. Ignore os falsos positivos com motivos documentados. Re-runanálise para marcar problemas resolvidos como obsoletos.
5. **Remediar** — crie correções para corrigir as descobertas. A modernização contínua cria filiais automaticamente e abre pull/merge solicitações com as correções. Acompanhe o status da remediação e repita as falhas.
6. **Configurar a análise contínua** — Programe análises recorrentes usando o Amazon EventBridge Scheduler. Configure a cadência de análise (diária, semanal ou cron personalizado) para monitorar continuamente seu portfólio em busca de novos problemas. Combine com a remediação automatizada para manter a integridade do código ao longo do tempo.

Opções de computação

A modernização contínua oferece suporte a três opções de computação para executar análises e remediações. As habilidades do agente no Kiro Power e no plug-in do agente ajudam você a configurar a infraestrutura para cada opção.

Note

Independentemente da opção de computação, todas as análises e correções acontecem quando você Conta da AWS usa suas credenciais. Seu código-fonte permanece sob seu controle.

Local (padrão)

Por padrão, as análises são executadas em sua máquina local. Essa opção não requer infraestrutura adicional. O servidor é executado localmente e executa análises usando recursos computacionais locais. Bom para testar a ferramenta, pequenos repositórios ou uso individual.

Amazon EC2

Execute análises em uma instância persistente do Amazon EC2 em seu. Conta da AWS Essa opção descarrega a computação de sua máquina local, suporta análises maiores e permite análises programadas recorrentes. A instância permanece em execução entre os envios.

A habilidade do agente fornece uma AWS CloudFormation pilha que inclui:

- Uma instância do Amazon EC2 (Amazon Linux 2023) com Docker e o contêiner de modernização contínua
- Uma função do IAM com permissões para AWS Transform, Amazon S3, AWS KMS, Secrets Manager e o agente de segurança
- AmazonSSMManagedInstanceCore para acesso ao shell via SSM (não é necessário par de chaves SSH ou portas de entrada)
- Um grupo de segurança sem regras de entrada

Seu usuário ou função do IAM precisa de permissões para o gerenciamento do ciclo de vida do Amazon EC2, operações de AWS CloudFormation pilha, criação de funções do IAM, operações de bucket do Amazon S3, gerenciamento de segredos do Secrets Manager e comandos SSM.

Para configurar a execução do EC2, instale o plug-in Kiro Power ou agente (consulte [Ferramentas de desenvolvedor](#)) e pergunte ao agente: “Configurar uma instância do EC2 para análise de modernização contínua”. O agente provisiona a infraestrutura, verifica se o contêiner está íntegro e envia suas análises via SSM, sem a necessidade de SSH.

AWS Batch (Fargate)

Execute análises como trabalhos isolados no AWS Batch com o Fargate para computação sem servidor. Cada análise é executada em seu próprio contêiner sem gerenciar a infraestrutura persistente. Bom para análise paralela de várias fontes ou tipos de análise.

Essa opção reutiliza a pilha de infraestrutura do AWS Transform CDK. A habilidade do agente implanta a infraestrutura necessária, incluindo:

- AWS Fila de trabalhos em lote e ambiente de computação
- Definição do trabalho com a imagem do contêiner de modernização contínua
- Funções do IAM para execução de trabalhos em lote
- Uma função Lambda para envio de trabalhos

Para configurar a execução em lote, instale o plug-in Kiro Power ou agente (consulte [Ferramentas de desenvolvedor](#)) e pergunte ao agente: “Executar minha análise no Fargate” ou “Configurar a execução em lote para modernização contínua”. O agente implanta a pilha CDK, armazena suas credenciais de origem no Secrets Manager e envia trabalhos de análise para o Batch. AWS

Configuração do agente de segurança

O tipo de security análise usa o serviço AWS Security Agent para detecção de vulnerabilidades e CVE. Ao contrário de outros tipos de análise, ela requer uma configuração única de infraestrutura em seu Conta da AWS.

O comando setup provisiona uma AWS CloudFormation pilha que inclui:

- Um bucket Amazon S3 para upload de código-fonte
- Uma função do IAM assumida por `securityagent.amazonaws.com`
- Uma política gerenciada para a função de agente de segurança

Seu usuário ou função do IAM deve ter as seguintes permissões adicionais para executar a configuração:

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

Use os comandos a seguir para gerenciar a infraestrutura do agente de segurança:

```
# 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
```

Após a conclusão da configuração, você pode executar análises de segurança da mesma forma que outros tipos de análise.

Introdução

Pré-requisitos

Para usar a modernização contínua de forma eficaz, você deve ter uma compreensão básica do controle de versão do Git, familiaridade com sua plataforma de código-fonte GitHub (GitLab,, ou Bitbucket), conhecimento prático das permissões AWS do IAM e experiência com ferramentas de linha de comando.

Antes de usar a modernização contínua, verifique se você tem o seguinte:

- AWS Transforme a CLI instalada:

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

- Node.js 22 ou mais tarde
- AWS Credenciais válidas (AWS_PROFILE ou variáveis de ambiente)
- A política AWS AWSTransformCustomFullAccess gerenciada anexada ao seu usuário ou função do IAM

Início rápido

1. Inicie o servidor de modernização contínua:

```
atx ct server &
```

2. Adicione uma fonte:

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

Onde *name* está um identificador descritivo para sua fonte, *provider* é a plataforma (github,,gitlab, oulocal)bitbucket, *org-or-group* é o nome da sua organização ou grupo e *token* é o seu token de autenticação.

3. Descubra os repositórios:

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

4. Execute uma análise:

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

5. Explore as descobertas:

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

6. Corrija as descobertas:

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

Trabalhando com modernização contínua

Gerenciamento de fontes

Use `atx ct source` comandos para conectar repositórios. Provedores compatíveis: GitHub, GitLab, Bitbucket, local.

GitHub organizações

Token: token de acesso pessoal (clássico) com repo escopo. Read-only para análise, repositório completo para remediação.

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

GitLab grupos e usuários

Token: token de acesso pessoal com api escopo.

```
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
```

Espaços de trabalho e projetos do Bitbucket

Bitbucket Cloud —

escopos:read:repository:bitbucket,,write:repository:bitbucket,read:pullrequest:bitb
write:pullrequest:bitbucket Também precisa --email --username e.

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

Centro de dados Bitbucket:

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

Repositórios locais

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

Important

--path deve apontar para um diretório pai contendo repositórios git como subdiretórios, não para um único repositório.

Gerenciando fontes

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

Descoberta e gerenciamento de repositórios

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

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

Após a descoberta:

```
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"
```

Análise em execução

O `--type` sinalizador especifica o tipo de análise a ser executada:

- `rapid-techdebt-analysis`— Dependências desatualizadas e vitórias fáceis.
- `tech-debt-comprehensive`— AI-powered Análise mais profunda abrangendo descobertas sobre dependência, segurança, padrões, desempenho, capacidade de manutenção, arquitetura, qualidade de código e infraestrutura.
- `security`— Vulnerabilidades e exposições de segurança.
- `agentic-readiness`— Preparação de seus repositórios para agentes de IA (estruturas, APIs, documentação).
- `modernization-readiness`— oportunidades de modernização em suas dimensões de infraestrutura, aplicativos, dados, segurança e operações.

```
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]
```

Análise personalizada

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

Configuração com -g sinalizador: valor-chave, JSON ou caminho do arquivo.

Listar TDs: `atx custom def list`

Gerenciar descobertas

```
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
```

Encontrando status

- open— Ativo
- dismissed— Dispensado manualmente (requer motivo)
- obsolete— System-set quando a reanálise não produz mais a descoberta

```
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
```

Encontrando a obsolescência

Re-analysis marca as descobertas resolvidas como obsoletas. Não pode ser reaberto. Retido para auditoria.

Criação de remediações

Três modos: baseado em descobertas, substituição de TD, TD direto.

```
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
```

Saída por provedor: GitHub PR, GitLab MR, Bitbucket PR, filial local.

 Note

O token deve ter acesso de gravação para PR/MR criação.

Execução local com `--local` bandeira.

```
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 Transformar aplicativo web (opcional)

O aplicativo web AWS Transform é uma interface opcional para monitorar análises, descobertas e correções de modernização contínua em todo o seu portfólio de fontes de código.

Antes de usar o aplicativo web AWS Transform, você precisa ter uma identidade de usuário habilitada para acessar o AWS Transform em sua organização. Para obter informações sobre como ativar o AWS Transform, consulte [Configurando o AWS Transform](#).

Para usar o aplicativo web AWS Transform:

1. Visite <https://aws.amazon.com/transform/> e faça login usando as credenciais AWS do IAM Identity Center.
2. Se a modernização contínua não aparecer após o login, faça login com as credenciais do IAM. Para ativar o login com as credenciais do IAM:
 - a. No AWS Management Console, abra AWS Transformar e escolha Configurações.
 - b. Na seção AWS Transformação de acesso com credenciais do IAM, ative o acesso às credenciais do IAM.
 - c. Na mesma página de configurações, copie o link de login mostrado em URL do aplicativo Web (com IAM).
 - d. Cole o URL de login na mesma janela do navegador em que o AWS Management Console está aberto. Isso garante que o aplicativo web use as AWS credenciais dessa conta.

3. Abra o menu de navegação à esquerda e escolha a modernização contínua. O painel exibe estatísticas resumidas, incluindo fontes, repositórios, resultados totais por gravidade e tipos de análise.
4. Use as guias Análises, Descobertas e Remediações para visualizar resultados detalhados.
5. AWS Converse com o Transform diretamente do aplicativo web para fazer perguntas sobre suas análises, descobertas ou correções.

O aplicativo web foi projetado para operações em escala empresarial em que você precisa de visibilidade centralizada das análises e correções contínuas de modernização em várias bases de código.

Ferramentas de desenvolvedor

Você pode acessar a modernização contínua a partir de IDEs agentes usando o plug-in AWS Transform Power e agente. O agente coordena a configuração, a integração e o uso contínuo da modernização contínua por meio da interação conversacional.

- Kiro IDE — Instale o [AWS Transform Kiro Power](#). Abra o Kiro Chat e peça ajuda ao agente nos fluxos de trabalho de modernização contínua.
- Claude Code, Codex, Cursor — Instale o [awslabs/agent-plugins \(diretório\)](#)plugins/aws-transform. O plug-in do agente fornece os mesmos recursos do Kiro Power.

Habilidades do agente

O plug-in Kiro Power and agent inclui habilidades que orquestram fluxos de trabalho de modernização contínua por meio de interação conversacional:

Habilidade	Description
Guia	Integração interativa que orienta você em todo o fluxo de trabalho, passo a passo
Fonte	Adicionar, listar e remover conexões de origem
Descoberta	Escaneie fontes para descobrir repositórios
Análise	Execute e gerencie análises em todos os tipos

Habilidade	Description
Conclusões	Consulte, filtre e gerencie os resultados da análise
Correção	Crie e gerencie correções para corrigir descobertas
Execução do EC2	Provisione e gerencie uma instância do Amazon EC2 para análise remota
Execução em lote	Envie trabalhos de análise para o AWS Batch with Fargate
Agendamento	Configure análises recorrentes em uma programação cron usando o Amazon Scheduler EventBridge
Relatórios	Gere relatórios HTML independentes com gráficos que mostram as descobertas, a distribuição da gravidade e o progresso da remediação

Referência da CLI

A tabela a seguir resume todos os `atx` `ct` subcomandos.

Subcomando	Description
<code>atx ct server</code>	Inicie o servidor de modernização contínua
<code>atx ct status</code>	Visualize o status do sistema, incluindo fontes, repositórios, análises, descobertas e remediações
<code>atx ct source add</code>	Adicionar uma fonte (GitHub GitLab, Bitbucket ou local)

Subcomando	Description
<code>atx ct source list</code>	Listar fontes configuradas
<code>atx ct source remove</code>	Remover uma fonte
<code>atx ct discovery scan</code>	Descubra repositórios a partir de uma fonte
<code>atx ct discovery status</code>	Verifique o status do escaneamento de descoberta
<code>atx ct repository list</code>	Listar repositórios com filtros opcionais
<code>atx ct repository get</code>	Obtenha um único repositório
<code>atx ct repository update</code>	Atualizar rótulos do repositório
<code>atx ct repository delete</code>	Excluir um repositório
<code>atx ct analysis run</code>	Execute uma análise nos repositórios
<code>atx ct analysis get</code>	Obtenha detalhes da análise
<code>atx ct analysis list</code>	Análises de listas com filtros opcionais de status e tipo
<code>atx ct analysis cancel</code>	Cancelar uma análise em execução
<code>atx ct analysis delete</code>	Excluir uma análise
<code>atx ct findings list</code>	Liste as descobertas com filtros para repositório, fonte, gravidade, tipo, status e análise
<code>atx ct findings get</code>	Obtenha uma única descoberta
<code>atx ct findings update</code>	Atualizar o status da descoberta (aberta ou rejeitada)
<code>atx ct findings batch-update</code>	Atualização em lote de várias descobertas
<code>atx ct findings delete</code>	Excluir uma descoberta descartada ou obsoleta

Subcomando	Description
<code>atx ct remediation create</code>	Crie uma remediação a partir das descobertas ou de uma definição de transformação
<code>atx ct remediation list</code>	Listar todas as remediações
<code>atx ct remediation status</code>	Verifique o status da remediação e visualize os links PR/MR
<code>atx ct remediation retry</code>	Tente novamente uma correção que falhou
<code>atx ct remediation delete</code>	Excluir uma remediação
<code>atx ct setup security-agent</code>	Provisione ou gerencie a infraestrutura do agente de segurança
<code>atx ct schema</code>	Imprima um manifesto JSON legível por máquina de toda a superfície de <code>atx ct</code> comando — cada comando, opção e argumento — para que os agentes e a automação possam descobrir a CLI sem analisar o texto de ajuda

Solução de problemas

Conexão recusada ou servidor não funcionando

A CLI de modernização contínua requer um servidor em execução. Comece com `atx ct server &` e verifique com `atx ct status --health`.

O Discovery scan retorna zero repositórios

Para fontes locais, verifique se isso `--path` aponta para um diretório principal que contém repositórios como subdiretórios (por exemplo, `/home/user/repos`), não diretamente para um repositório (por exemplo, `/home/user/repos/my-app`). O scanner procura diretórios secundários que contenham uma `.git` pasta.

erro SETUP_REQUIRED

A fonte existe na sua conta, mas as credenciais não estão configuradas nesta máquina. Execute `atx ct source add --name name` para configurar as credenciais localmente.

erro AUTH_REQUIRED

Nenhum token válido encontrado para a fonte. Verifique se seu token está correto e tem os escopos necessários. Para GitHub, certifique-se de que o token tenha `repo` escopo. Para GitLab, garanta o `api` escopo.

erro INVALID_INPUT

Verifique se você está usando o nome correto do tipo de análise. Os valores válidos são: `rapid-techdebt-analysis`, `tech-debt-comprehensive`, `security`, `agentic-readiness`, `modernization-readiness`, `custom`.

Erros de permissão durante a remediação

A remediação cria ramificações e pull/merge solicitações, o que requer acesso de gravação ao repositório. Atualize seu token com permissões de gravação. Pois GitHub, garanta o `repo` escopo completo. Para GitLab, garanta o `api` escopo. Para o Bitbucket, garanta `write:repository:bitbucket` e `write:pullrequest:bitbucket` escopo.

Falha na configuração do agente de segurança

Verifique se seu usuário ou função do IAM tem as permissões necessárias AWS CloudFormation, IAM e Amazon S3 listadas na seção de configuração do agente de segurança do. [Como AWS Transforme os trabalhos de modernização contínua](#) Verifique o status com `atx ct setup security-agent --status`.

Modernização contínua não visível no aplicativo web

Se a modernização contínua não aparecer depois que você fizer login no aplicativo web AWS Transform, faça login com as credenciais do IAM do Conta da AWS local em que o AWS Transform está habilitado, em vez do AWS IAM Identity Center. Para obter as etapas, consulte [AWS Transformar aplicativo web \(opcional\)](#).

Ferramenta de descoberta

A ferramenta de AWS Transform descoberta ajuda você a descobrir automaticamente o inventário de servidores em sua organização para se preparar para a migração. A ferramenta é compatível com VMware vCenter, Hyper-V Microsoft e servidores importados. Para usar a ferramenta de descoberta, você configura uma ou mais fontes de descoberta, deixa a ferramenta funcionar e, em seguida, analisa os resultados no painel Inventário descoberto.

Depois de configurar uma fonte de descoberta, a ferramenta de descoberta começa a coletar informações. O tempo que a ferramenta de descoberta precisa para analisar completamente sua rede depende do tamanho do seu ambiente. Para um caso comercial de migração direcional, você pode usar os arquivos de Avaliação do Portfólio de Migração (MPA) que a ferramenta gera após a conclusão da coleta do servidor.

Workflow da ferramenta Discovery

O fluxo de trabalho da ferramenta de descoberta consiste em dois tipos de atividades:

- Atividades de configuração
- Análise e uso de dados

As etapas a seguir descrevem como instalar e usar a ferramenta de descoberta e trabalhar com os dados coletados:

1. Instale a ferramenta de descoberta.
2. Configure as fontes de descoberta. Você pode configurar um ou mais dos seguintes: VMware vCenter, hosts ou servidores da Hyper-V Microsoft por meio de uma importação de arquivo CSV. A descoberta de dados começa depois que você configura qualquer fonte.
3. Configure o acesso ao sistema operacional e, em seguida, revise o status da coleção de servidores, bancos de dados e conexões de rede.
 - Ajuste as credenciais do sistema operacional conforme necessário.
4. (Opcional) Configure as credenciais do Oracle para ativar a coleta direta de SQL ou use a detecção de OS-level fallback por meio de SSH ou WinRM.
5. Para gerar um caso comercial de migração, faça upload do arquivo.zip para a [avaliação de migração](#) ou descompacte-o e faça upload dos arquivos MPA do diretório mpa_exports. A

exportação inclui dados de todas as fontes configuradas e contém arquivos MPA para servidores VMware e Hyper-V importados.

A ferramenta de descoberta oferece suporte aos seguintes caminhos de descoberta:

- Descoberta automática do VMware vCenter — descubra automaticamente servidores gerenciados pelo VMware vCenter.
- Hyper-V descoberta automática — Descubra automaticamente servidores gerenciados por Hyper-V hosts da Microsoft.
- Importação do servidor — importe manualmente o inventário do servidor por meio de um arquivo CSV.

Configurando a ferramenta de descoberta

Pré-requisitos

A seguir estão os pré-requisitos para usar a ferramenta de descoberta: AWS Transform

Pré-requisitos gerais

- A ferramenta requer 4 vCPUs, 16 GB de RAM e um disco rígido de 35 GB.
- O DHCP deve estar disponível na rede para a ferramenta de descoberta VM.
- A ferramenta coleta dados usando uma abordagem centralizada. Os servidores no escopo devem permitir conectividade de entrada da VM da ferramenta de descoberta (portas padrão, há suporte para configuração de porta personalizada):
 - Linux — SSH TCP/22
 - Windows — TCP/5985 para HTTP, TCP/5986 para HTTPS
 - SNMP — UDP/161 (usado somente para coleta de rede, não para métricas do sistema operacional)
- Para Linux, contas de usuário que podem usar SSH para se conectar ao servidor. A ferramenta de descoberta executa comandos via SSH para coleta de rede e métricas do sistema operacional. A maioria dos comandos é executada como um usuário comum. Um pequeno número de comandos tenta sudo e retorna automaticamente se o sudo não estiver disponível: dmidecode (UUID do servidor e fabricante), (detecção de LVM) ss e/ou lvsdisplay netstat (conexões de rede com informações do processo). Sem o sudo, a ferramenta de descoberta ainda coleta a maioria

dos dados, mas faltarão detalhes de UUID, LVM e rede em nível de processo. Recomendamos configurar o sudo sem senha para o usuário SSH para garantir a coleta completa dos dados. Para obter uma análise completa, consulte [the section called “Permissões obrigatórias”](#).

Pré-requisitos da VMware

- VMware vCenter Server versão 6.5, 6.7, 7.0 ou 8.0.
- Permissões para implantar um OVA em seu VMware vCenter.
- Para a configuração do VMware vCenter Server, um usuário do vCenter com a Read-Only função atribuída no nível do datacenter raiz. Para obter detalhes, consulte [the section called “Permissões obrigatórias”](#).

Hyper-V Pré-requisitos

- Windows Server com a Hyper-V função ativada.
- WinRM habilitado em hosts. Hyper-V
- Uma conta de usuário que é membro dos grupos Usuários de Gerenciamento Remoto, Hyper-V Administradores e Usuários do Monitor de Desempenho em cada Hyper-V host, com acesso de leitura WMI ao root\cimv2 namespace. Para obter detalhes, consulte [the section called “Permissões obrigatórias”](#).
- Autenticação suportada: NTLM (somente HTTPS) e Kerberos (HTTP ou HTTPS).

Pré-requisitos de importação do servidor

- Um arquivo CSV com nomes de host ou endereços IP do servidor e os nomes das credenciais (opcionais) que são mapeados para os nomes amigáveis das credenciais do sistema operacional configuradas ou a serem configuradas na ferramenta de descoberta. O CSV deve usar os seguintes cabeçalhos:

```
hostname_or_ip,os_credential_name,oracle_credential_name
```

- Os servidores devem estar acessíveis a partir da ferramenta de descoberta VM. Portas padrão: porta SSH 22 para Linux, porta 5985/5986 WinRM para Windows. Portas personalizadas são suportadas.

Pré-requisitos do instalador Linux

- Uma distribuição Linux compatível: Amazon Linux 2, Amazon Linux 2023, RHEL 8—9, Rocky Linux 8—9, 9, Ubuntu 20.04—24.04, Debian 10—12 ou SLES 15 AlmaLinux SP5.
- Mínimo de 4 vCPUs, 16 GB de RAM, 35 GB de espaço em disco disponível.
- A porta 5000 deve estar disponível (não em uso por outro serviço).
- O systemd é necessário para o gerenciamento de serviços.
- A ferramenta de descoberta VM deve ter acesso à rede à sua infraestrutura de destino. Portas padrão: vCenter na porta 443, Hyper-V hosts na porta 5985/5986, servidores na porta 22. Portas personalizadas são suportadas para SSH, WinRM e SNMP.

Pré-requisitos do banco de dados Oracle

- Acesso à rede da ferramenta de descoberta aos hosts Oracle na porta 1521 (ou porta personalizada).
- Versões Oracle suportadas: você pode coletar o Oracle Database 12c Release 1 (12.1) e posterior por meio de conexões SQL diretas. OS-level a detecção de fallback funciona com todas as versões do Oracle.
- Uma conta de serviço Oracle somente para leitura com concessão SELECT_CATALOG_ROLE. Para obter detalhes, consulte [the section called “Banco de dados Oracle \(SQL\)”](#).
- Para detecção de OS-level fallback: acesso SSH ou WinRM ao host Oracle (usa credenciais de sistema operacional existentes).

Implemente no VMware

Especificações da máquina virtual VMware

- Sistema operacional — Amazon Linux 2023
- RAM — 16 GB
- CPU — 4 núcleos
- Discos — 35 GB
- Requisitos do VMware — Veja os requisitos de [host do VMware para executar](#) o AL2023 no VMware

Implante o VMware OVA

1. Faça o download do arquivo OVA a partir deste URL: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.ova>
2. Faça login no vCenter como um administrador VMware.
3. Use uma das seguintes formas de instalar o arquivo OVA:
 - a. Use a interface do usuário: escolha Arquivo, escolha Implantar modelo OVF, selecione o arquivo OVA da ferramenta de descoberta que você baixou na etapa 1 e, em seguida, conclua o assistente. Verifique se as configurações de proxy no painel de gerenciamento do servidor estão configuradas corretamente.
 - b. Use a linha de comando: Para instalar o arquivo OVA da ferramenta de descoberta a partir da linha de comando, baixe e use a VMware Open Virtualization Format Tool (ovftool). Para baixar o ovftool, selecione uma versão na página de [documentação da ferramenta OVF](#). Este é um exemplo de uso da ferramenta de linha de comando ovftool para instalar o arquivo OVA da ferramenta de descoberta.

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

Descrições dos valores substituíveis no exemplo:

- O nome é o nome que você deseja usar para sua ferramenta de descoberta VM.
 - O armazenamento de dados é o nome do armazenamento de dados em seu vCenter.
 - O nome do arquivo OVA é o nome do arquivo OVA da ferramenta de descoberta baixado.
 - Essas username/password são suas credenciais do vCenter.
 - O vcenterurl é o URL do seu vCenter.
 - O caminho vi é o caminho para seu host VMware ESXi.
4. Localize a ferramenta de descoberta implantada em seu vCenter. Right-click a VM e, em seguida, escolha Power, Power On.
 5. Depois de alguns minutos, o endereço IP da ferramenta de descoberta é exibido no vCenter. Você usa esse endereço IP para se conectar à ferramenta de descoberta.

Implantar em Hyper-V

Hyper-V especificações da máquina virtual

- Sistema operacional — Amazon Linux 2023
- RAM — Recomendamos alocar pelo menos 16 GB
- CPU — Recomendamos alocar pelo menos 4 núcleos
- Discos — 35 GB (incluídos no VHD)
- Hyper-V requisitos — Veja os [requisitos de Hyper-V host para executar o AL2023 em Hyper-V](#)

Implemente o Hyper-V VHD

1. Baixe o arquivo VHD a partir deste URL: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.vhd>
2. Copie o arquivo VHD para a máquina Windows Server que tem a Hyper-V função ativada.
3. Hyper-V Gerenciador aberto.
4. Escolha Novo e, em seguida, escolha Máquina Virtual.
5. Conclua o assistente de configuração. Na página Especificar geração, selecione Geração 1. As máquinas virtuais de segunda geração não oferecem suporte ao formato VHD. Na página Atribuir memória, aloque pelo menos 16384 MB. Na página Conectar disco rígido virtual, escolha Usar um disco rígido virtual existente e selecione o arquivo VHD que você copiou.
6. Inicie a VM. Depois de alguns minutos, verifique a guia Rede da VM no Hyper-V Manager para encontrar o endereço IP ou conecte-se ao console da VM e execute. `ip addr` Você usa esse endereço IP para se conectar à ferramenta de descoberta.

Implemente no Linux

A ferramenta de descoberta está disponível como um instalador Linux autônomo para implantação em distribuições Linux suportadas. Use essa opção quando quiser instalar a ferramenta de descoberta diretamente em um servidor Linux existente em vez de implantar uma máquina virtual.

Especificações do servidor Linux

- RAM — Recomendamos alocar pelo menos 16 GB
- CPU — Recomendamos alocar pelo menos 4 núcleos

- Discos — 35 GB

Distribuições Linux compatíveis

- Amazon Linux — Amazon Linux 2, Amazon Linux 2023
- Red Hat Enterprise Linux e derivados — RHEL 8—9, Rocky Linux 8—9, 9 AlmaLinux
- Ubuntu — 20.04, 22.04, 24.04
- Debian — 10, 11, 12
- SUSE — SLES 15 SP5

Instale a ferramenta de descoberta

Baixe o script do instalador a partir deste URL: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh>

Para instalar a ferramenta de descoberta no Linux

1. Baixe o script do instalador no seu servidor Linux.

```
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. (Opcional) Execute a verificação de compatibilidade para verificar se o sistema atende aos requisitos.

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

3. Instale a ferramenta de descoberta. Escolha uma das seguintes opções:

Opção 1: instalar com instalação automática de dependência (recomendado)

Essa opção instala automaticamente todas as dependências ausentes do sistema antes de instalar o serviço.

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

Opção 2: instalar sem instalação automática de dependências

Essa opção verifica se há dependências ausentes e exibe erros com instruções de instalação manual se dependências críticas estiverem ausentes. Use essa opção se sua organização restringir a instalação automática de pacotes e você preferir gerenciar pacotes do sistema manualmente.

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

4. Inicie o serviço de ferramentas de descoberta.

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

5. Acesse a ferramenta de descoberta em `https://ip_address:5000`.

Para desinstalar a ferramenta de descoberta, execute `sudo ./AWS-Transform-discovery-tool.sh uninstall`.

Você também pode usar os seguintes comandos para gerenciar o serviço:

- `sudo ./AWS-Transform-discovery-tool.sh status`— Verifique se o serviço está em execução.
- `sudo ./AWS-Transform-discovery-tool.sh stop`— Pare o serviço.
- `sudo ./AWS-Transform-discovery-tool.sh logs`— Visualize os registros do serviço.

Dependências do sistema

O instalador verifica as seguintes dependências do sistema:

Dependência	Gravidade	Finalidade
OpenSSL	Crítico	Gera a chave de criptografia do banco de dados
libcrypt	Crítico	Exigido pelo tempo de execução do Python
Bibliotecas Kerberos	Aviso	Necessário para a autenticação Kerberos em servidores Windows. Sem isso, o NTLM e a autenticação básica ainda funcionam.

Dependências críticas são necessárias para que a ferramenta de descoberta seja iniciada. Se eles estiverem ausentes e você escolher a Opção 2 (sem `--install-deps`), o instalador exibirá um erro com instruções para instalá-los manualmente. Warning-level dependências são opcionais — o instalador avisa você, mas prossegue com a instalação.

Note

O instalador verifica a compatibilidade do sistema, incluindo a versão glibc e a disponibilidade do systemd. Em sistemas com systemd 250 ou posterior (Amazon Linux 2023, RHEL 9, Rocky 9, 9, Ubuntu 24.04+, AlmaLinux Debian 12+), a chave de criptografia do banco de dados é criptografada em repouso usando systemd-creds. Em sistemas mais antigos, a chave de criptografia é armazenada como um arquivo protegido por permissão.

Configurar a ferramenta de descoberta

Acesse o console da ferramenta de descoberta

1. Em um navegador da web, acesse: `https://ip_address:5000`, onde `ip_address` está o endereço IP da ferramenta de descoberta do Deploy Discovery Tool. A ferramenta de descoberta usa um certificado autoassinado para conexão HTTPS, o que resulta em um aviso de segurança. Escolha Aceitar o risco e continue até o console da ferramenta de descoberta.
2. Se você estiver acessando o console da ferramenta de descoberta pela primeira vez, crie uma senha de login da ferramenta de descoberta. Crie uma senha, que você usará para futuros logins.

Important

Lembre-se dessa senha - não há mecanismo de recuperação de senha.

Acessando a ferramenta de descoberta VM

- A ferramenta de descoberta VM vem por padrão com um nome de usuário e senha (“descoberta”, “senha”). Para uma segurança forte, recomendamos que você atualize a senha usando `sudo passwd discovery` depois de fazer login na VM por meio do console do seu hipervisor (por exemplo, vSphere Client for VMware ou Manager for). Hyper-V Hyper-V

- O acesso SSH está desativado por padrão. Os usuários podem usar `disablessh` aliases `enablessh` e pré-configurados para acessar por `enable/disable` SSH a ferramenta de descoberta VM. Os usuários podem entrar via SSH na VM `ssh discovery@<VM-IP>` após habilitar o acesso SSH. Os usuários são incentivados a manter o acesso SSH desativado na maioria das vezes e ativá-lo somente quando necessário. A alteração da senha é imposta durante a execução `enablessh`.
- Para acessar o diretório de dados da ferramenta de descoberta em `/home/ec2-user/.local/share/DiscoveryTool`, recomendamos mudar para `ec2-user` executando `sudo su ec2-user`.

Configurar a autenticação Kerberos

A autenticação Kerberos é o método recomendado para se conectar aos servidores Windows a partir da ferramenta de descoberta. A ferramenta de descoberta VM usa bibliotecas Kerberos nativas do Amazon Linux 2023 para se autenticar em seu domínio do Active Directory.

A seguir estão os principais pontos sobre a autenticação Kerberos na ferramenta de descoberta VM:

- Use o `kinit` comando para obter um tíquete Kerberos e `klist` verificar o tíquete.
- O arquivo de configuração do Kerberos está localizado em `/etc/krb5.conf`
- Antes de configurar a ferramenta de descoberta, verifique se a CLI é `kinit` bem-sucedida na VM da ferramenta de descoberta.

Pré-requisitos do Kerberos

Antes de configurar a autenticação Kerberos, verifique se você tem as seguintes informações e conectividade de rede.

1. Obtenha as seguintes informações do administrador do Active Directory:

- O nome do território Kerberos (normalmente seu nome de domínio em maiúsculas, por exemplo). `EXAMPLE.COM`
- O nome do host ou endereço IP do Centro de Distribuição de Chaves (KDC), que normalmente é um controlador de domínio (por exemplo, `dc01.example.com`).
- Uma conta de serviço com permissões para autenticação nos servidores Windows de destino.

2. Verifique se a VM da ferramenta de descoberta tem conectividade de rede com o seguinte:

- O KDC na porta 88 (TCP e UDP) para autenticação Kerberos.

- Os servidores Windows de destino nas portas WinRM (5985 para HTTP, 5986 para HTTPS).

Configurar o Kerberos

Conclua as etapas a seguir para configurar a autenticação Kerberos na VM da ferramenta de descoberta.

1. SSH para a ferramenta de descoberta VM.

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

2. Edite o arquivo de configuração do Kerberos em. `/etc/krb5.conf`

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

Adicione a configuração a seguir, substituindo os valores do espaço reservado pelos detalhes do seu ambiente.

```
[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

O Kerberos diferencia maiúsculas de minúsculas. O nome do território deve estar em maiúsculas (por exemplo `EXAMPLE.COM`, não). `example.com` O nome do domínio na `[domain_realm]` seção deve estar em letras minúsculas.

Vários domínios do Active Directory

A ferramenta de descoberta oferece suporte a várias credenciais Kerberos para diferentes domínios do Active Directory. Cada credencial é autenticada de forma independente, então você pode configurar várias credenciais normalmente e o isolamento é automático.

Se você tiver servidores em vários domínios, adicione entradas para cada região em seu `/etc/krb5.conf` arquivo:

```
[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. Verifique se você pode obter um tíquete Kerberos executando o `kinit` comando.

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

Digite a senha quando solicitado. Se o comando for concluído sem erros, a autenticação será bem-sucedida.

4. Verifique o ticket executando o `klist` comando.

```
klist
```

A saída esperada é semelhante à seguinte.


```
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. Configure a ferramenta de descoberta com o mesmo princípio de distinção entre maiúsculas e minúsculas que você usou com kinit (por exemplo,username@REALM.COM).

Uma krb5.conf configuração explícita pode não ser necessária se seu ambiente tiver registros DNS SRV configurados para descoberta de serviços Kerberos. [Para obter mais informações sobre as opções de configuração do Kerberos, consulte a documentação krb5.conf do MIT Kerberos e o arquivo krb5.conf de amostra.](#)

Encontre a configuração do Kerberos em máquinas associadas ao domínio

Se você não tiver os detalhes da configuração do Kerberos, poderá recuperá-los de uma máquina Windows associada ao domínio. Execute os comandos a seguir em um prompt de comando na máquina associada ao domínio.

Para encontrar o nome do domínio, execute o comando a seguir.

```
echo %USERDNSDOMAIN%
```

Resultado do exemplo:

```
EXAMPLE.COM
```

Para encontrar o nome do host do controlador de domínio, execute o comando a seguir.

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

Resultado do exemplo:

```
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
```

Mapeie a saída para sua `krb5.conf` configuração da seguinte forma:

- Região — Use o valor de `%USERDNSDOMAIN%` em maiúsculas (por exemplo,). `EXAMPLE.COM`
- KDC — Use o nome do host DC da `nltest` saída (por exemplo, `dc01.example.com`).

Configurar o acesso ao vCenter

1. Na página da ferramenta Discovery, na Etapa 1. Configure as fontes de descoberta, escolha Configurar fontes.
2. Na página Configurar fontes de descoberta, forneça o nome amigável, o vCenter FQDN/IP, o nome de usuário e a senha.
3. Escolha Save configuration.

A ferramenta de descoberta começa a coletar informações do vCenter, conforme descrito em Inventário [descoberto](#).

Após a configuração inicial, escolha Editar acesso ao vCenter no quadro de status da ferramenta Discovery para alterar suas configurações de acesso ao vCenter.

A ferramenta de descoberta coleta dados de todos os servidores vCenter configurados em paralelo. Se um servidor vCenter estiver inacessível durante a coleta, a ferramenta relatará um sucesso parcial e continuará coletando dos demais servidores vCenter.

Se uma VM aparecer em vários servidores vCenter (por exemplo, devido a hosts ESXi compartilhados ou entre vCenter vMotion), a ferramenta de descoberta desduplica automaticamente as VMs. Cada VM exclusiva aparece apenas uma vez no inventário.

Configurar o Hyper-V acesso

1. Na página da ferramenta Discovery, na Etapa 1. Configure as fontes de descoberta, escolha Configurar fontes.

2. Na página Configurar fontes de descoberta, forneça um nome amigável, o FQDN ou endereço IP do host, o tipo de autenticação (NTLM ou Kerberos), o nome de usuário do WinRM e a senha do WinRM.
3. Escolha Save configuration.

A ferramenta de descoberta começa a coletar Hyper-V informações, conforme descrito em [Inventário descoberto](#).

A coleta começa automaticamente depois que você salva as credenciais.

Para clusters Hyper-V de failover, você pode adicionar vários hosts no mesmo cluster. A ferramenta desduplica automaticamente as VMs que aparecem em mais de um host.

Servidores de importação

1. Navegue até a página Importar servidores na página inicial da ferramenta Discovery.
2. Prepare um arquivo CSV com as seguintes colunas: `hostname_or_ip` (obrigatório), `os_credential_name` (opcional) e `oracle_credential_name` (opcional).
 - O `hostname_or_ip` valor deve ser um endereço IPv4 válido ou um nome de domínio totalmente qualificado (FQDN).
 - O `os_credential_name` valor, se fornecido, deve corresponder ao nome amigável de uma credencial do sistema operacional que você já configurou (SSH, WinRM ou SNMP). Deixe em branco para servidores nos quais você ainda não configurou uma credencial de sistema operacional.
 - O `oracle_credential_name` valor, se fornecido, deve corresponder ao nome amigável de uma credencial Oracle que você já configurou.
3. Faça upload do arquivo CSV. A ferramenta valida todas as linhas e rejeita o arquivo se alguma linha for inválida.

Após uma importação bem-sucedida, a ferramenta inicia automaticamente a coleta de métricas de banco de dados, rede e sistema operacional para os servidores importados, se as credenciais do sistema operacional estiverem configuradas. Se você fizer upload de outro arquivo CSV, os registros existentes serão atualizados sem criar duplicatas e os novos registros serão mesclados ao inventário.

Importe uma autoridade de certificação autoassinada para a ferramenta de descoberta (opcional)

Isso é necessário quando você usa o WinRM em HTTPS e servidores de destino usando certificados WinRM HTTPS assinados por uma Autoridade de Certificação (CA) autoassinada e deseja ativar a opção “Validar certificado SSL do servidor” na ferramenta de descoberta.

Pré-requisitos

1. Self-signed Certificado CA que foi usado para assinar os certificados HTTPS do WinRM nos servidores de destino
2. Certificado em formato PEM (extensão.pem ou .crt)

Para importar uma autoridade de certificação autoassinada na ferramenta de descoberta VM:

1. VM da ferramenta Ssh to Discovery
2. Coloque os certificados de CA que assinaram os certificados WinRM de seus servidores de destino no diretório `/etc/pki/ca-trust/source/anchors/` de armazenamento confiável na VM da ferramenta de descoberta. Por exemplo: `sudo cp winrm-ca.pem /etc/pki/ca-trust/source/anchors/winrm-ca.pem`. Nota: Se seus servidores de destino usarem certificados assinados por CAs diferentes, copie todos os certificados de CA relevantes para esse diretório.
3. Atualize o repositório confiável de certificados: `sudo update-ca-trust`
4. Reinicialize a VM
5. (Opcional) Para verificar se os certificados foram importados com êxito, você pode executar o comando a seguir. `sudo trust list --filter=ca-anchors | grep -A 5 "<certificate_name>"`

Consulte [Instalação e configuração do Gerenciamento Remoto do Windows](#)

Configurar a ferramenta de descoberta para acesso ao sistema operacional

Configure o acesso ao sistema operacional para que a ferramenta de descoberta possa:

- Descubra bancos de dados para realizar a avaliação do banco de dados e auxiliar na migração da VM,

- Rastreie as conexões de rede entre os servidores em seu inventário, incluindo o processo associado a cada conexão, para auxiliar no mapeamento de dependências de aplicativos e no planejamento de ondas. Somente conexões em que os dois endpoints estão no inventário da ferramenta de descoberta são incluídas.

Habilite a ferramenta de descoberta OS Access

1. Navegue até a página Configurar acesso ao sistema operacional para fornecer as credenciais do Windows e do Linux.
2. Escolha um protocolo para o qual você deseja adicionar credenciais.
3. Forneça as credenciais necessárias para o protocolo selecionado.
4. Selecione Auto-connect para ativar a ferramenta de descoberta para testar todas as credenciais fornecidas nos servidores descobertos até que as credenciais correspondentes sejam encontradas para cada servidor.

Consulte [the section called “Usando o Auto-Connect recurso com cuidado”](#) para obter recomendações de segurança importantes sobre o recurso de conexão automática.

5. Escolha Configurar e conectar.

Quando o processo de correspondência do sistema operacional for concluído, você verá uma mensagem informando que a coleta de dados está em andamento e um erro em relação aos servidores para os quais não foi encontrada uma correspondência de credenciais.

Configuração de protocolos suportados

Você deve configurar os protocolos WinRM, SSH e SNMP nos servidores de destino para que a ferramenta de descoberta se comunique com eles.

Configurar WinRM e WMI

O WinRM é instalado automaticamente com todas as versões atualmente suportadas do sistema operacional Windows.

Para verificar ou editar a configuração do WinRM, use `winrm` a ferramenta de linha de comando:

- Verifique os ouvintes WinRM instalados: `winrm enumerate winrm/config/listener`
- Verifique as configurações do WinRM: `winrm get winrm/config`
- Exemplo de comando para configurar o WinRM: `winrm quickconfig -transport:https`

Portas de ouvinte

A porta HTTP padrão é 5985; HTTPS é 5986. Você pode usar outras portas conforme necessário. As portas devem estar abertas entre a ferramenta de descoberta e os servidores de destino.

Criptografia

A ferramenta de descoberta usa comunicação WinRM criptografada. Recomendamos que os ouvintes do WinRM nos servidores de destino também usem criptografia: `winrm set winrm/config/service '@{AllowUnencrypted="false"}'`

NTLM x Kerberos

Os protocolos de autenticação WinRM Kerberos e NTLM são suportados pela ferramenta de descoberta. O NTLM pode ser usado somente com HTTPS e o Kerberos pode ser usado com HTTP ou HTTPS.

Requisitos do WMI

A ferramenta de descoberta consulta os seguintes namespaces WMI. A conta WinRM precisa de acesso de leitura a cada namespace relevante para seus módulos de coleção:

Namespace WMI	Used by (Usado por)
<code>root\cimv2</code>	Métricas do sistema operacional, metadados do Hyper-V host, coleção do SQL Server
<code>root\virtualization\v2</code>	Hyper-V Inventário da VM
<code>root\StandardCIMV2</code>	Coleção de rede
<code>root\Microsoft\SqlServer\ComputerManagement*</code>	Coleção SQL Server
<code>root\Microsoft\SqlServer\ReportServer*</code>	Coleção SQL Server (SSRS)

Para coleta de rede, certifique-se de que estas condições sejam atendidas:

- Permitir conectividade de rede via ICMP

- Permitir conectividade de rede via porta TCP 135 + intervalo de portas TCP efêmeras (49152 - 65535)
- Desativar o UAC
- As permissões remotas do DCOM estão configuradas
- Crie uma conta de serviço dedicada com o mínimo de permissões necessárias
- As permissões de namespace WMI são configuradas para contas do Windows com namespaces:,
class \\root\\standardcimv2 MSFT_NetTCPConnection

Para a coleção do SQL Server, é necessária uma conta do Windows (local ou domínio) pertencente ao Grupo de Administradores Locais devido aos requisitos complexos de permissão de objetos WMI.

Configurar o SSH

- A porta padrão é 22. Portas personalizadas são suportadas. A porta configurada deve estar aberta entre a ferramenta de descoberta e os servidores de destino.
- Para que a coleta de rede SSH funcione corretamente, forneça um usuário configurado para sudo sem senha.
- Certifique-se de que os seguintes comandos estejam disponíveis nos servidores Linux de destino (instalados por padrão na maioria das distribuições): ss ou netstat para coleta de rede e,lsblk,,iostat,dmidecode,smartctl,, top ps freeip, e df para coleta de métricas do sistema operacional.

A ferramenta de descoberta oferece suporte a dois métodos de autenticação para SSH:

Opção 1: nome de usuário e senha

Forneça o nome de usuário e a senha do SSH. Esse é o método de autenticação padrão.

Opção 2: chave privada SSH

Forneça o nome de usuário SSH e uma chave privada no formato PEM. Para usar essa opção, escolha Chave SSH no menu suspenso Tipo de autenticação ao configurar as credenciais SSH. Se a chave privada estiver criptografada com uma frase secreta, insira a frase secreta no campo opcional Senha da chave.

Os seguintes formatos de chave são suportados:

- RSA

- ECDSA
- Ed 25519
- Formato OpenSSH
- Formato PKCS #8

Ambos os métodos de autenticação oferecem suporte à conexão automática. As credenciais são armazenadas criptografadas em repouso.

Configurar o SNMP

- A porta padrão é 161/UDP. Portas personalizadas são suportadas. A porta configurada deve estar aberta entre a ferramenta de descoberta e os servidores de destino.
- Para SNMP v2: forneça uma string de comunidade somente para leitura que possa acessar OIDs de conexão TCP.
- Para SNMP v3: forneça username/password auth/privacy detalhes com permissão somente para leitura que possa acessar OIDs de conexão TCP

A ferramenta de descoberta requer acesso a:

- "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)

Configurar o acesso ao banco de dados Oracle

Configure o acesso ao banco de dados Oracle para coletar metadados detalhados do banco de dados Oracle diretamente por meio de conexões SQL. Os metadados coletados incluem topologia de CDB e PDB, uso de recursos e opções instaladas. Esses dados ajudam você a planejar as migrações de bancos de dados Oracle com mais precisão. Você pode coletar o Oracle Database 12c Release 1 (12.1) e posterior por meio de conexões SQL diretas. OS-level a detecção de fallback funciona com todas as versões do Oracle.

Configure as credenciais da Oracle na ferramenta de descoberta

1. Na página da ferramenta Discovery, na barra lateral, escolha Acesso ao banco de dados.
2. Escolha Adicionar credencial Oracle.

3. Forneça as informações a seguir:

- Nome amigável — Um nome descritivo para essa credencial (por exemplo, `Oracle Production`).
 - Porta — A porta do ouvinte Oracle (padrão 1521).
 - Nome do serviço — O nome do serviço Oracle para o banco de dados de destino.
 - Nome de usuário — O nome de usuário da conta de serviço Oracle.
 - Senha — A senha da conta de serviço Oracle.
 - Auto-connect— Ative essa opção para testar a credencial em todos os servidores do seu inventário. Desative essa opção para atribuir manualmente a credencial a servidores específicos.
4. Para adicionar mais credenciais (por exemplo, para diferentes ambientes Oracle), escolha Adicionar credencial Oracle novamente.
5. Escolha Salvar.

Modos de credencial

Ao configurar as credenciais da Oracle, você pode escolher entre dois modos:

- Manual — Fixe uma credencial em um servidor específico. A ferramenta de descoberta usa essa credencial exclusivamente para esse servidor. Se a conexão falhar, nenhum retorno ocorrerá. Corrija a configuração da credencial para resolver o problema.
- Auto-connect— A ferramenta de descoberta testa cada credencial de conexão automática em cada servidor em seu inventário. Quando uma credencial é bem-sucedida para um servidor, a ferramenta de descoberta usa essa credencial para todas as rodadas de coleta subsequentes.

Fluxo de detecção

Quando você configura as credenciais do Oracle, a ferramenta de descoberta primeiro tenta uma conexão SQL direta. Se todas as credenciais do banco de dados falharem, a ferramenta voltará à OS-level detecção por meio de SSH ou WinRM, para que você ainda possa descobrir instalações Oracle sem acesso ao banco de dados.

Atualizando a ferramenta de descoberta

A ferramenta de descoberta não tem um recurso de atualizações automáticas, mas você receberá uma notificação de lembrete após 30 dias da instalação para atualizar. É recomendável manter o aplicativo atualizado para receber os recursos e os patches de segurança mais recentes.

Para atualizar manualmente a ferramenta

1. Baixe o arquivo de imagem mais recente da ferramenta de descoberta (OVA para VMware ou VHD para Hyper-V) no link fornecido.
2. (Opcional) Recomendamos que você exclua o arquivo de imagem anterior da ferramenta de descoberta antes de implantar o mais recente.
3. Siga as etapas na seção Implantar a ferramenta de descoberta para implantar a versão atualizada.

Revogar acesso

Você pode revogar o acesso de cada fonte de descoberta de forma independente. Quando você revoga o acesso a uma fonte, os dados de outras fontes não são afetados.

- Revogando o acesso ao vCenter — Exclui credenciais e dados do vCenter. VMware-collected Não exclui Hyper-V dados, dados importados do servidor ou credenciais do sistema operacional.
- Revogando o Hyper-V acesso — Exclui somente Hyper-V credenciais e Hyper-V-collected dados.
- Excluindo servidores importados — Remove os servidores importados do inventário. Os dados de coleta downstream (rede, banco de dados) que foram coletados desses servidores são retidos.

Permissões necessárias para a ferramenta de descoberta

A ferramenta de descoberta se conecta à sua infraestrutura usando vários protocolos. Cada protocolo e módulo de coleção exige permissões de conta específicas. Esta seção descreve as permissões mínimas necessárias para a coleta completa de dados e quais dados você perde se determinadas permissões não estiverem disponíveis.

VMware vCenter

A ferramenta de descoberta se conecta ao VMware vCenter Server na porta 443 (HTTPS) e executa operações somente de leitura. Nenhuma alteração é feita em seu ambiente vCenter.

Função mínima exigida: Read-Only, atribuída no nível raiz do vCenter.

A Read-Only função fornece todo o acesso que a ferramenta de descoberta precisa para coletar o inventário da VM (nome, UUID, CPU, memória, disco, rede, estado de energia, sistema operacional convidado) e métricas de desempenho (utilização da CPU, utilização da memória, IOPS do disco e taxa de transferência).

Recomendação: crie um usuário dedicado do vCenter com a Read-Only função integrada no nível do datacenter raiz.

Hyper-V hospedeiros (Windows)

A ferramenta de descoberta se conecta aos Hyper-V hosts via WinRM (porta 5985 para HTTP, porta 5986 para HTTPS) e PowerShell executa comandos para coletar o inventário da VM, os metadados do host e o desempenho do armazenamento.

Número mínimo de associações de grupo exigidas para cada Hyper-V anfitrião:

Grupo Windows	Por que é necessário
Usuários de gerenciamento remoto	Acesso remoto WinRM de linha de base
Hyper-V Administradores	Coleção de inventário de VMs (lista de VMs, disco, rede, memória, sistema operacional convidado)
Usuários do Monitor de Desempenho	Contadores de I/O desempenho de armazenamento (read/write IOPS e taxa de transferência por VM)

A conta também precisa de acesso de leitura WMI ao `root\cimv2` namespace para a versão do sistema operacional host e o UUID do hardware. Esse acesso é concedido por padrão para administradores locais, mas deve ser configurado explicitamente para contas não administrativas.

Recomendação: Crie uma conta de serviço de domínio dedicada e adicione-a aos grupos Usuários de Gerenciamento Remoto, Hyper-V Administradores e Usuários do Monitor de Desempenho em cada Hyper-V host. Evite usar contas de administrador de domínio.

Servidores Linux (SSH)

A ferramenta de descoberta se conecta a servidores Linux via SSH (porta 22) para coletar métricas do sistema operacional, conexões de rede e inventário de servidores. A maior parte da coleta

de dados é executada como um usuário comum. Um pequeno número de comandos tenta sudo retornar automaticamente se o sudo não estiver disponível.

Acesso mínimo necessário: uma conta de usuário SSH que pode fazer login no servidor de destino.

Acesso recomendado: O mesmo usuário SSH configurado com sudo sem senha para coleta completa de dados.

O que requer sudo e o que acontece sem ele:

Dados coletados	Sudo é necessário?	O que você perde sem sudo
Nome do servidor, sistema operacional, CPU, memória, IP, contagem de discos	Não	Nada — coletado como usuário regular
Utilização de CPU, memória e rede	Não	Nada — coletado como usuário regular
IOPS, taxa de transferência e espaço em disco	Não	Nada — coletado como usuário regular
Configuração da interface de rede	Não	Nada — coletado como usuário regular
Processos em execução (nome, PID, comando)	Não	Nada — coletado como usuário regular
UUID do servidor e SMBIOS UUID	Sim	Os campos UUID estão vazios na exportação
Fabricante de hardware (detecção física versus detecção virtual)	Sim	A detecção do tipo de recurso é menos precisa em distribuições mais antigas
Detecção de volume lógico LVM	Sim	Volumes LVM não detectados; o tipo de volume pode aparecer como “Desconhecido”
Conexões de rede com nome do processo e PID	Sim	As conexões ainda são coletadas, mas sem atribuição de processo (as colunas PID e nome do processo estão vazias)

Dados coletados	Sudo é necessário?	O que você perde sem sudo
OS-level Detecção do banco de dados Oracle (alternativa quando as credenciais do Oracle não estão configuradas)	Sim	A detecção básica de presença do Oracle (oratab, monitor de processo) funciona sem sudo. A coleta detalhada (opatch, lsnrctl, ASM, Grid Infrastructure) requer acesso sem senha <code>sudo -u oracle</code> aos binários do Oracle home.

Note

A ferramenta de descoberta nunca falha totalmente devido à falta de sudo. Ele coleta o que pode e relata resultados parciais. No entanto, para obter os dados mais completos, especialmente o mapeamento de dependências de rede com nomes de processos, recomendamos o sudo sem senha.

Utilitários necessários nos servidores de destino: os seguintes comandos devem estar disponíveis (instalados por padrão na maioria das distribuições Linux): `ss` ou `netstat`, `lsblk`, `top`, `ps`, `free`, `ip`, `df`, `hostname`, `catnproc`, e. `grep` Opcional para dados adicionais: `iostat` (I/O detalhes do disco), `dmidecode` (UUID de hardware), `smartctl` (tipo de interface de disco), `lvdisplay` (detecção de LVM).

Servidores Windows (WinRM) — métricas do sistema operacional

A ferramenta de descoberta se conecta aos servidores Windows pelo WinRM para coletar métricas do sistema operacional (inventário do servidor, desempenho, armazenamento, interfaces de rede e processos em execução).

Acesso mínimo necessário: uma conta de WinRM-enabled usuário com acesso remoto ao servidor de destino.

Acesso recomendado: um usuário no grupo Administradores local para a coleta completa de dados.

Nível de permissão	O que isso permite	O que você perde sem isso
Usuários de gerenciamento remoto (acesso WinRM)	Toda a coleta de dados do Windows	Nenhum dado coletado do servidor
Acesso de leitura WMI a root\cimv2	Nome do servidor, versão do sistema operacional, memória, UUID, série do BIOS, espaço em disco	Os campos de inventário do servidor estão vazios
Usuários do Monitor de Desempenho	Utilização da CPU, taxa de transferência de rede, IOPS de disco e taxa de transferência	Métricas de desempenho não coletadas
Administrador local	Nomes do proprietário do processo em execução	Lista de processos coletada, mas a user/owner coluna está vazia

Note

A associação ao administrador local concede implicitamente aos usuários do Monitor de Desempenho acesso e acesso de leitura ao WMI, portanto, satisfaz todos os requisitos acima.

Note

A detecção de OS-level fallback do Oracle Database no Windows usa consultas Get-Service e Get-Process comandos de registro quando as credenciais do Oracle não estão configuradas. Esses comandos exigem somente o acesso padrão dos Usuários de Gerenciamento Remoto. Nenhuma permissão adicional além dos requisitos de métricas do sistema operacional é necessária.

Servidores Windows (WinRM) — coleção SQL Server

A coleção do SQL Server descobre instâncias do SQL Server, Reporting Services (SSRS) e Integration Services (SSIS) em servidores Windows.

Acesso recomendado: Um usuário no grupo Administradores local em cada servidor Windows de destino.

O administrador local é recomendado porque a descoberta do SQL Server consulta vários namespaces WMI e requer acesso elevado para algumas operações:

O que é descoberto	Permissão necessária	O que você perde sem isso
Instâncias do SQL Server Database Engine (versão, edição, status)	Acesso de leitura WMI aos namespaces <code>root\Microsoft\SqlServer\ComputerManagement*</code>	Instâncias do SQL Server não descobertas
SQL Server Reporting Services (SSRS)	Acesso de leitura WMI aos namespaces <code>root\Microsoft\SqlServer\ReportServer</code>	Componentes do SSRS não descobertos
Configuração de URL e porta do SSRS	Privilegios elevados (administrador local)	Detalhes da reserva de URL do SSRS ausentes
SQL Server Integration Services (SSIS)	Acesso de leitura do registro (HKLM)	Versão e edição do SSIS ausentes
Port-to-service associação	Acesso à enumeração de ouvintes TCP	Não é possível associar portas de escuta aos serviços do SQL Server

Note

A coleção do SQL Server é Windows-only. A ferramenta de descoberta ignora servidores Linux para descoberta do SQL Server.

Banco de dados Oracle (SQL)

A coleção do Oracle Database se conecta diretamente às instâncias Oracle na porta 1521 (ou em uma porta personalizada) para coletar metadados do banco de dados. A ferramenta de descoberta não exige privilégios de DBA ou SYSDBA.

Acesso mínimo necessário: uma conta de serviço Oracle somente para leitura com a concessão `SELECT_CATALOG_ROLE`.

A ferramenta de descoberta não acessa as visualizações do Diagnostics Pack ou do Tuning Pack, portanto, nenhuma licença adicional da Oracle é necessária para a coleta de dados.

SQL para criar a conta:

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

OS-level fallback: Se as credenciais do banco de dados não estiverem configuradas ou a conexão falhar, a ferramenta de descoberta usará as credenciais existentes do sistema operacional SSH ou WinRM para detectar instalações Oracle. Nenhuma permissão adicional do Oracle-specific sistema operacional é necessária além do que o módulo de métricas do sistema operacional exige.

Coleção de rede

A coleta de rede usa protocolos diferentes, dependendo do sistema operacional do servidor:

Sistema operacional do servidor	Protocolo	Permissões necessárias
Linux	SSH	Usuário comum para dados de conexão. Sudo sem senha recomendado para detalhes em nível de processo (PID e nome do processo).
Linux	SNMP v2	Uma string de comunidade somente para leitura com acesso ao TCP MIB (tcpConnState, tcpConnectionProcess) e ao Host Resources MIB (hr). SWRunName

Sistema operacional do servidor	Protocolo	Permissões necessárias
Linux	SNMP v3	Um usuário do USM com acesso de leitura aos mesmos MIBs do SNMPv2. Suporta os níveis de segurança no AuthNoPriv, vNoPriv, auth e authPriv.
Windows	WinRM	Acesso de leitura WMI ao root\StandardCIMV2 namespace (classe MSFT_NetTcpConnection).

Referência rápida: permissões mínimas por caso de uso

Caso de uso	Account type (Tipo de conta)	Permissões mínimas
Descoberta de VMs da VMware	Usuário do vCenter	Read-Only função no nível do datacenter raiz
Hyper-V Descoberta da VM	Domínio do Windows ou conta local	Usuários de gerenciamento remoto + Hyper-V Administradores + Usuários do Monitor de Desempenho em cada host
Métricas do sistema operacional Linux — dados completos	Usuário SSH	Sudo sem senha
Métricas do sistema operacional Linux — dados parciais	Usuário SSH	Usuário comum (sem sudo). Faltarão informações sobre UUID, fabricante, LVM e processo de rede.
Métricas do sistema operacional Windows — dados completos	Usuário WinRM	Administrador local

Caso de uso	Account type (Tipo de conta)	Permissões mínimas
Métricas do sistema operacional Windows — dados básicos	Usuário WinRM	Usuários de gerenciamento remoto + acesso de leitura WMI a root\cimv2
Descoberta do banco de dados do SQL Server	Usuário WinRM	Administrador local
Descoberta de banco de dados Oracle (SQL)	Conta de serviço Oracle	SELECT_CATALOG_ROLE (somente leitura, sem DBA ou SYSDBA)
Coleção de rede — Linux (SSH)	Usuário SSH	Sudo sem senha para dados em nível de processo; usuário comum somente para dados de conexão
Coleção de rede — Linux (SNMP)	Cadeia de caracteres da comunidade SNMP ou usuário USM	Acesso de leitura aos MIBs de recursos de TCP e host
Coleção de rede — Windows	Usuário WinRM	Acesso de leitura WMI a root\StandardCIMV2

Coleta de dados

Agenda de coleta da ferramenta Discovery

Após sua coleta inicial de descobertas, a ferramenta de descoberta continua sendo executada em um cronograma escalonado para evitar a contenção de recursos:

- Descoberta da VMware — a cada hora (às :00 UTC)
- Hyper-V descoberta — a cada hora (às :20 UTC)

A ferramenta de descoberta também coleta métricas do sistema operacional por meio dos seguintes módulos independentes, cada um com seu próprio cronograma escalonado:

- Métricas de rede — a cada 15 segundos, podem ser menos frequentes em ambientes grandes
- Métricas de desempenho do servidor — a cada 10 minutos (às :03, :13, :23, :33, :43, :53 UTC)
- Métricas de desempenho de armazenamento — a cada 10 minutos (às :07, :17, :27, :37, :47, :57 UTC)
- Processos em execução — de hora em hora (às :40 UTC)
- Dados de provisionamento do servidor — diariamente (às 00:05 UTC)
- Dados de provisionamento de armazenamento — diariamente (às 00:35 UTC)
- Interfaces de rede — diariamente (às 01:05 UTC)
- Descoberta do SQL Server — diariamente (às 03:05 UTC)
- Descoberta do banco de dados Oracle — diariamente (às 05:05 UTC)

Você pode iniciar, interromper ou acionar de forma independente cada módulo de métricas do sistema operacional usando Coletar dados agora.

Para executar manualmente uma coleção, no menu Ações, escolha:

- Iniciar — ativa o módulo de descoberta.
- Parar — Desativa o módulo de descoberta.
- Colete dados agora — inicia a descoberta imediatamente. Use essa opção, por exemplo, depois de fazer uma alteração na sua rede.

Essas ações se aplicam por módulo. Você pode controlar os módulos de métricas do sistema operacional individualmente.

Tentativas de coleta de dados do SO

Quando um novo servidor é descoberto, a ferramenta de descoberta tenta cada credencial configurada para cada endereço IP e nome do host. Depois que a ferramenta de descoberta encontra uma credencial válida, ela continua usando essa credencial, a menos que você adicione uma nova credencial.

Após uma falha na coleta, a ferramenta de descoberta tenta coletar dados de rede para um servidor após 3 minutos, 30 minutos, 2 horas e depois 6 horas. Após 4 tentativas malsucedidas, a ferramenta de descoberta continua testando todas as credenciais configuradas uma vez a cada 6 horas.

Inventário descoberto

Depois de configurar uma fonte de descoberta, o valor do Número de servidores descobertos no quadro de status da ferramenta Discovery começa a aumentar. O status de descoberta da fonte configurada muda para Ativado no quadro do módulo Coleção. A página de inventário mostra servidores de todas as fontes configuradas: VMs VMware, Hyper-V VMs e servidores importados. Cada servidor mostra seu status de origem e coleção por módulo.

Navegue até a página Inventário descoberto para ver os servidores que a ferramenta de descoberta encontrou. Nessa página, escolha Baixar inventário para baixar um arquivo ZIP (`discovery_tool_export.zip`) que contém até 30 dias de dados coletados, incluindo arquivos MPA para todas as fontes configuradas, dados de utilização de desempenho, informações do banco de dados e informações de comunicação entre servidores.

Você pode baixar o arquivo ZIP enquanto a ferramenta de descoberta continua funcionando e obter resultados parciais. Faça o upload desse arquivo para a [avaliação de migração](#) para obter um caso de negócios para migração.

Opções de exportação

Ao exportar dados, você pode personalizar a exportação com as seguintes opções:

Intervalo de datas

Selecione uma data de início e uma data de término para exportar somente os dados coletados dentro desse período. Ambas as datas são inclusivas. O intervalo máximo de datas é de 30 dias.

Note

A ferramenta de descoberta armazena até 30 dias dos dados coletados. Se você precisar de dados que abranjam mais de 30 dias, execute exportações incrementais a cada 30 dias para capturar todos os dados.

Seleção do módulo

Escolha quais módulos de dados incluir na exportação. Você pode exportar todos os módulos ou selecionar alguns específicos:

Módulo	Description
Dados da VMware	Inventário de máquinas virtuais a partir de servidores vCenter
Hyper-V dados	Inventário de máquinas virtuais a partir de Hyper-V hosts
Dados de rede	Conexões de rede entre servidores
Inventário do servidor	Informações sobre hardware e sistema operacional do servidor
Métricas de desempenho do servidor	Utilização de CPU, memória e rede
Desempenho de armazenamento do servidor	IOPS e taxa de transferência de disco
Configuração de armazenamento	Configuração de disco e volume
Interfaces de rede	Detalhes do adaptador de rede
Métricas de processo	Processos em execução
Dados do SQL Server	Inventário do banco de dados SQL Server
Dados do banco de dados Oracle	Inventário do banco de dados Oracle — CDBs, PDBs, recursos, opções e componentes

Se você não selecionar nenhum módulo, a ferramenta de descoberta exportará todos os dados disponíveis.

Pontos de dados coletados

A ferramenta de descoberta reúne dados abrangentes sobre VMware, métricas de sistema operacional Hyper-V, banco de dados e componentes de rede. As seções a seguir detalham os pontos de dados específicos coletados para cada componente.

Coleta de dados da VMware

Esta tabela descreve as informações da máquina virtual VMware coletadas pela ferramenta de descoberta:

Nome	Tipo	Categoria	Valor de exemplo
nome_vm	String	Informações sobre a VM	"w2k22-snmpd-v2-pt-br-mssql-2022-testcase4-1"
vm_id	String	Informações sobre a VM	"vm-30920"
vm_uuid	String	Informações sobre a VM	"4201ecf8-cc44-ee7e-01da-34dfb2acf6c0"
estado de potência	String	Informações sobre a VM	"Ligado"
host	String	Informações sobre a VM	"esxi-70-node1.testlab.local"
endereço_IP primário	String	Informações sobre a VM	"192.168.0.52"
xícaras	Inteiro	Informações sobre a VM	2
memória	Inteiro	Informações sobre a VM	4096
capacidade total do disco mib	Inteiro	Informações sobre a VM	32768
os_according_to_the_configuration_file	String	Informações sobre a VM	"Microsoft Windows Server 2016 ou posterior (64 bits)"
max_cpu_usage_pct_dec	Float	Desempenho da VM	79,33

Nome	Tipo	Categoria	Valor de exemplo
avg_cpu_usage_pct_dec	Float	Desempenho da VM	45,06
max_ram_usage_pct_dec	Float	Desempenho da VM	63,99
avg_ram_util_pct_dec	Float	Desempenho da VM	29,27

Hyper-V coleta de dados

Esta tabela descreve as informações da máquina Hyper-V virtual coletadas pela ferramenta de descoberta:

Nome	Tipo	Categoria	Valor de exemplo
nome_vm	String	Informações sobre a VM	"win2022-hyperv-test-01"
vm_id	String	Informações sobre a VM	"a1b2c3d4-e5f6-7890-abcd-ef1234567890"
estado de potência	String	Informações sobre a VM	"Correndo"
xícaras	Inteiro	Informações sobre a VM	4
memória_mb	Inteiro	Informações sobre a VM	8192
caminhos_de_disco	String	Disk	"C:\\ VMs\\ disk1.vhdx"
tamanho_do_gb do disco	Float	Disk	127,0
adaptadores de rede	String	Rede	"00:15:5D:01:02:03"

Nome	Tipo	Categoria	Valor de exemplo
endereços_IP	String	Rede	"10.0.1.50"
host_name	String	Host	"hyperv-host-01.example.com"
versão host_os	String	Host	"Centro de dados do Windows Server 2022"
cluster_name	String	Host	"FailoverCluster01"
hypervisor	String	Informações sobre a VM	"Hyper-V"

Dados importados do servidor

Os servidores importados não são descobertos automaticamente. Eles são importados por meio de um arquivo CSV. A ferramenta de descoberta não coleta dados em nível de hipervisor para servidores importados. Em vez disso, ele coleta dados de métricas de banco de dados, rede e sistema operacional usando as credenciais do sistema operacional associadas a cada servidor durante a importação.

OS-related Dados da ferramenta Discovery

A ferramenta de descoberta coleta dados de inventário, desempenho, armazenamento, interface de rede e processo do servidor por meio de SSH (Linux) e WinRM (Windows). As tabelas a seguir descrevem os pontos de dados coletados.

Inventário do servidor (server_inventory.csv)

Combina o provisionamento de servidores (configuração de hardware e sistema operacional) com desempenho de armazenamento agregado. Coletado a cada 24 horas.

Nome	Tipo	Categoria	Valor de exemplo
id_do_servidor	String	Informações do servidor	"vm-web-servidor-01"

Nome	Tipo	Categoria	Valor de exemplo
server_name	String	Informações do servidor	“servidor web-01”
resource_type	String	Informações do servidor	“máquina virtual”
estado_de_potência	String	Informações do servidor	“Correndo”
tipo de sistema operacional	String	Informações do servidor	“Linux”
nome_do_sistema operacional	String	Informações do servidor	“Amazon Linux”
os_version	String	Informações do servidor	“2023”
nome_do_host primário	String	Informações do servidor	“servidor web-01.example.com”
endereço_IP primário	String	Informações do servidor	“10.0.2.101”
máscara de rede	String	Informações do servidor	“255.255.255.0”
número total de cartões de rede	Inteiro	Informações do servidor	2
número total de discos	Inteiro	Informações do servidor	1
contagem_de_CPU	Inteiro	Informações do servidor	4
memória_total_gb	Float	Informações do servidor	15,88

Nome	Tipo	Categoria	Valor de exemplo
server_uuid	String	Informações do servidor	"4201ecf8-cc44-ee7e-01da-34dfb2acf6c0"
smbios_uuid	String	Informações do servidor	"4201ecf8-cc44-ee7e-01da-34dfb2acf6c0"
cluster_name	String	Informações do servidor	"cluster de produção-01"
id_de_objeto_hipervisor	String	Informações do servidor	"vm-30920"
tipo_de_hipervisor	String	Informações do servidor	"VMware"
versão_hipervisor	String	Informações do servidor	"8.0.0"
nome_do_host do hipervisor	String	Informações do servidor	"esxi-node1.example.com"
hypervisor_host_id	String	Informações do servidor	"host-1234"
id_de-hipervisor	String	Informações do servidor	"4201ecf8-cc44-ee7e-01da-34dfb2acf6c0"
disk_read_iops_avg	Float	Desempenho de Armazenamento	12,5
disk_read_iops_peak	Float	Desempenho de Armazenamento	245,0

Nome	Tipo	Categoria	Valor de exemplo
disk_write_iops_avg	Float	Desempenh o de Armazenam ento	8.3
disk_write_iops_peak	Float	Desempenh o de Armazenam ento	180,0
disco_total_iops_avg	Float	Desempenh o de Armazenam ento	20,8
pico total de iops do disco	Float	Desempenh o de Armazenam ento	425,0
taxa de transferência de leitura de disco avg_mbps	Float	Desempenh o de Armazenam ento	1.2
taxa de transferência de leitura de disco com pico de mbps	Float	Desempenh o de Armazenam ento	24,5
taxa de transferência de gravação em disco avg_mbps	Float	Desempenh o de Armazenam ento	0.8

Nome	Tipo	Categoria	Valor de exemplo
taxa de transferência de gravação em disco com pico de mbps	Float	Desempenho de Armazenamento	18,0
taxa de transferência total do disco avg_mbps	Float	Desempenho de Armazenamento	2,0
pico de taxa de transferência total do disco	Float	Desempenho de Armazenamento	42,5

Métricas de desempenho do servidor (server_performance_metrics.csv)

Utilização de CPU, memória e taxa de transferência de rede. Amostradas a cada 10 minutos, agregadas em 30 dias.

Nome	Tipo	Categoria	Valor de exemplo
id_do_servidor	String	Informações do servidor	"vm-web-servidor-01"
data_source	String	Informações do servidor	"NÓS"
utilização_de_cpu_avg_pct	Float	CPU	45,06
pico de utilização_pct da CPU	Float	CPU	79,33
contagem_de_CPU	Inteiro	CPU	4
memória_total_gb	Float	Memória	15,88

Nome	Tipo	Categoria	Valor de exemplo
utilização_de_memória_avg_pct	Float	Memória	29,27
peak_pct de utilização de memória	Float	Memória	63,99
network_in_avg_mbps	Float	Rede	0,52
network_in_peak_mbps	Float	Rede	12.3
network_out_avg_mbps	Float	Rede	0,31
network_out_peak_mbps	Float	Rede	8.7
network_total_avg_mbps	Float	Rede	0,83
peak_mbps de pico total da rede	Float	Rede	21,0

Desempenho de armazenamento (server_storage_performance.csv)

Per-volume utilização de disco I/O e espaço. Amostras a cada 10 minutos, agregadas em 30 dias.

Nome	Tipo	Categoria	Valor de exemplo
id_do_servidor	String	Informações do servidor	"vm-web-servidor-01"
data_source	String	Informações do servidor	"NÓS"
id_volume_de_disco	String	Informações sobre o volume	"/dev/nvme0n1p1"

Nome	Tipo	Categoria	Valor de exemplo
ponto_de_montagem do disco	String	Informações sobre o volume	"/"
sistema_de_arquivos	String	Informações sobre o volume	"xfs"
disco_total_gb	Float	Espaço em disco	30.0
disco usado_gb	Float	Espaço em disco	12,5
disco livre_gb	Float	Espaço em disco	17,5
disk_read_iops_avg	Float	Disco I/O	12,5
disk_read_iops_peak	Float	Disco I/O	245,0
disk_write_iops_avg	Float	Disco I/O	8.3
disk_write_iops_peak	Float	Disco I/O	180,0
disco_total_iops_avg	Float	Disco I/O	20,8
pico total de iops do disco	Float	Disco I/O	425,0
taxa de transferência de leitura de disco avg_mbps	Float	Taxa de transferência de disco	1.2
taxa de transferência de leitura de disco com pico de mbps	Float	Taxa de transferência de disco	24,5

Nome	Tipo	Categoria	Valor de exemplo
taxa de transferência de gravação em disco avg_mbps	Float	Taxa de transferência de disco	0,8
taxa de transferência de gravação em disco com pico de mbps	Float	Taxa de transferência de disco	18,0
taxa de transferência total do disco avg_mbps	Float	Taxa de transferência de disco	2,0
pico de taxa de transferência total do disco	Float	Taxa de transferência de disco	42,5

Configuração de armazenamento (storage_config.csv)

Detalhes do hardware do disco físico. Coletado a cada 24 horas.

Nome	Tipo	Categoria	Valor de exemplo
id_do_servidor	String	Informações do servidor	"vm-web-servidor-01"
id_do_controlador de disco	String	Informações do disco	"/dev/sda"
vmdk_vhd_nome_do_arquivo	String	Informações do disco	"servidor web-01.vmdk"
tipo_volume_de_disco	String	Informações do disco	"Virtual"
disco provisionado_gb	Float	Informações do disco	30.0

Nome	Tipo	Categoria	Valor de exemplo
tipo_do_dispositivo_disco	String	Informações do disco	“DISCO RÍGIDO SCI”
tipo de interface de disco	String	Informações do disco	“SCI”
protocolo_de_disco	String	Informações do disco	“LSI Logic SAS”

Interfaces de rede (network_interfaces.csv)

Configuração do adaptador de rede. Coletado a cada 24 horas.

Nome	Tipo	Categoria	Valor de exemplo
id_do_servidor	String	Informações do servidor	“vm-web-servidor-01”
nome_de_interface	String	Informações da interface	“eth0”
índice de interface	Inteiro	Informações da interface	2
endereço_mac	String	Informações da interface	“A:1B:2C:3D:4E:5F0”
tipo_adaptador	String	Informações da interface	“vmxnet3”
nome_de_rede virtual	String	Informações da interface	“Rede VM”
id_de_rede virtual	String	Informações da interface	“dvportgroup-1234”

Nome	Tipo	Categoria	Valor de exemplo
interruptor_virtual	String	Informações da interface	"vSwitch 0"
endereço_ipv4	String	Configuração de IP	"10.0.2.101"
máscara de subrede ipv4	String	Configuração de IP	"255.255.255.0"
gateway ipv4	String	Configuração de IP	"10.0.2.1"
endereço_ipv6	String	Configuração de IP	"fe80: :a1b:2cff: fe3d:4e5f"
comprimento do prefixo ipv6	Inteiro	Configuração de IP	64
gateway ipv6	String	Configuração de IP	"fe80: :1"
servidores dns_	String	Configuração de IP	"10.0.0.2"
dhcp_enabled	Booleano	Configuração de IP	false
status da interface	String	Informações da interface	"Para cima"
id_vlan	Inteiro	Informações da interface	100
é_primário	Booleano	Informações da interface	true

Processos em execução (process_metrics.csv)

Instantâneo dos processos em execução. Coletado a cada hora, deduplicado em 30 dias.

Nome	Tipo	Categoria	Valor de exemplo
id_do_servidor	String	Informações do servidor	"vm-web-servidor-01"
process_name	String	Informações do processo	"sshd"
process_id	Inteiro	Informações do processo	1234
linha de comando do processo	String	Informações do processo	"/usr/sbin/sshd-D"
usuário_de_processo	String	Informações do processo	"raiz"

Coleção de rede

O módulo de coleta de rede ajuda você a descobrir dependências entre servidores em seu data center local. Esses dados de rede aceleram seu planejamento de migração, fornecendo visibilidade sobre como os aplicativos se comunicam entre os servidores.

Esse módulo coleta dados de rede para servidores de todas as fontes configuradas, incluindo VMware e servidores Hyper-V importados. Ele usa o WinRM para coletar dados de servidores Windows e usa SSH, SNMPv2 e SNMPv3 para coletar dados de servidores Linux.

Coleta de dados de rede

O módulo de coleta de rede captura conexões TCP IPv4 no estado ESTABELECIDO ou TIME_WAIT entre servidores em seu inventário descoberto. Uma conexão aparece na saída somente quando os endereços IP de origem e de destino pertencem aos servidores que a ferramenta de descoberta descobriu ou que você importou. As conexões de ou para endereços IP fora do seu inventário, como serviços externos, endpoints de nuvem ou servidores que ainda não foram adicionados à ferramenta de descoberta, não estão incluídas.

Esse design concentra os dados da rede nas dependências de servidor para servidor em seu ambiente, que são as informações necessárias para o mapeamento de dependências de aplicativos e o planejamento da onda de migração.

Esses pontos de dados são coletados para cada conexão:

Nome	Tipo	Categoria	Valor de exemplo
IP de origem	String	Conexão	"192.168.1.10"
Porta de origem	Inteiro	Conexão	49152
ID do processo de origem	Inteiro	Processo	1234
Nome do processo de origem	String	Processo	"java"
IP de destino	String	Conexão	"192.168.1.20"
Porta de destino	Inteiro	Conexão	5432
ID do processo de destino	Inteiro	Processo	5678
Nome do processo de destino	String	Processo	"postgres"
Estado	String	Conexão	"ESTABELECIDO"
Protocolo de transporte	String	Conexão	"TCP"
Versão IP	String	Conexão	"IPv4"
Contagem	Inteiro	Conexão	42

Tip

Para maximizar a integridade do seu mapa de dependência de rede, configure todas as fontes de descoberta (VMware e importação de CSV do servidor) e adicione as credenciais

do sistema operacional antes de revisar os dados da rede. Hyper-V Quanto mais servidores em seu inventário, mais conexões o módulo de rede pode capturar.

Coleção de rede de endereços privados

Por padrão, o módulo de coleta de rede captura somente conexões em que ambos os endpoints são servidores em seu inventário descoberto. Você pode habilitar a coleta de endereços privados para também capturar conexões de e para endereços IP privados da RFC 1918 (10.0.0. 0/8, 172.16.0. 0/12, 192.168.0. 0/16) que não estão em seu inventário.

Para iniciar a coleta de endereços privados

1. Na página de configuração do coletor, localize a seção Módulos de coleção.
2. Encontre Descoberta de conexões de rede em Descoberta de aplicativos.
3. Abra o menu suspenso Ações.
4. Escolha Iniciar coleta de endereços particulares.
5. Se o status do módulo estiver Ativado, você poderá vê-lo mudar para Ativado · Endereço privado ativado.

Para interromper a coleta de endereços particulares, abra a lista suspensa Ações e escolha Parar coleta de endereços particulares. Os dados de endereço privado coletados anteriormente são retidos mesmo após a interrupção.

As conexões de endereço privado aparecem somente na exportação CSV completa (dentro do arquivo ZIP), não nos arquivos MPA CSV. Se um endereço IP pertencer a um servidor que já está em seu inventário, ele sempre será identificado pelo ID do servidor descoberto, independentemente dessa configuração.

Essa configuração persiste nas reinicializações. Você pode iniciar ou interromper a coleta de endereços particulares a qualquer momento. Os dados de endereço privado coletados anteriormente são exportados independentemente da configuração atual.

Coleção SQL Server

O módulo de coleção do SQL Server reúne informações do SQL Server de servidores Windows em todas as fontes configuradas, incluindo VMware e servidores Hyper-V importados. O módulo usa o WinRM para se conectar remotamente a cada servidor Windows e executar consultas. PowerShell

Ele coleta informações sobre todos os serviços (componentes) instalados do SQL Server usando namespaces, registro e propriedades de arquivo WMI.

Um componente do SQL Server é uma instância específica de serviço ou recurso instalada como parte de uma implantação do SQL Server em um servidor Windows. A ferramenta de descoberta reúne o Database Engine, o Analysis Services, o Reporting Services e o Integration Services.

Coleta de dados do SQL Server

O módulo de coleção do SQL Server reúne informações sobre os componentes do SQL Server. Esta tabela descreve os principais pontos de dados coletados:

Nome	Tipo	Categoria	Valor de exemplo
Tipo de mecanismo	String	Componente	servidor_sql
É componente do motor	Booleano	Componente	S
Status	String	Serviço	Correndo, parado, StartPending
Versão	String	Serviço	2015.131.5026.0
Edição	String	Serviço	Edição Developer (64 bits)
Nome do serviço SQL	String	Serviço	MsDtsServer130, MSQL
Tipo de serviço SQL	String	Serviço	Serviço SQL Server, serviço Integration Services
Nome da instância	String	Instância	SERVIDOR MSSQL
Nome de exibição	String	Serviço	SQL Server (MSSQLSERVER2017)
Modo de início	String	Serviço	Automático, manual, desativado
Nome da conta de serviço	String	Serviço	NT Service/MsDtsServer130
Está agrupado	Booleano	Configuração	N

 Note

O formato completo inclui todos os tipos de serviço. O formato MPA inclui somente componentes do mecanismo de banco de dados. Nem todos os campos estão disponíveis, dependendo do tipo e da configuração do serviço SQL.

Coleção de banco de dados Oracle

Com o Oracle Database Collection, você pode descobrir instâncias do banco de dados Oracle em todas as fontes configuradas, incluindo VMware e Hyper-V servidores importados. O módulo coleta os seguintes dados:

- Enumeração de banco de dados de contêiner (CDB) e banco de dados conectável (PDB)
- Versão e edição
- Opções instaladas
- Estatísticas de uso do recurso
- Inventário de componentes (DBA_REGISTRY)
- Dimensionamento do arquivo de dados
- Sinalizadores de topologia (RAC, Data Guard e arquitetura multilocatária)

Database-connected (SQL)

Quando você configura as credenciais da Oracle, a ferramenta de descoberta se conecta diretamente ao banco de dados Oracle usando a conta de serviço somente para leitura. Isso fornece uma SQL-level coleção completa, incluindo detalhes do PDB, uso de recursos e opções instaladas. Todos os arquivos CSV contêm dados completos.

OS-level recuar

Se você não configurou as credenciais do banco de dados ou se a conexão falhar, a ferramenta de descoberta usa SSH ou WinRM para detectar instalações Oracle. Ele descobre endereços, ouvintes, patches, versões e edições do Oracle sem acesso ao banco de dados. Para OS-detected hosts, o CSV CDB exportado contém nome da instância, nome do host, versão e edição. Os arquivos CSV do PDB, dos recursos, das opções e dos componentes não contêm linhas.

A coleção Oracle produz os seguintes arquivos CSV no ZIP de exportação. Cada tabela descreve os pontos de dados coletados por arquivo.

Dados do CDB (oracle_data_cdb_full.csv)

Uma linha por instância de CDB. Esta tabela descreve os pontos de dados do CDB coletados:

Nome	Tipo	Categoria	Valor de exemplo	Fonte
Nome da instância	String	Identidade	“ORCO”	SQL, SISTEMA OPERACIONAL
Nome do host	String	Identidade	“oracledb01.example.com”	SQL, SISTEMA OPERACIONAL
Nome do banco de dados	String	Identidade	“ORCO”	Somente SQL
Nome exclusivo do banco de dados	String	Identidade	“ORCL_PRIMARY”	Somente SQL
DBID	Inteiro	Identidade	1234567890	Somente SQL
Versão	String	Versão	“19.0.0.0”	SQL, SISTEMA OPERACIONAL
Versão completa	String	Versão	“19.21.0.0.0”	Somente SQL
Edição	String	Versão	“Edição Empresarial”	SQL, SISTEMA OPERACIONAL
Tipo de banco de dados	String	Configuração	“SOLTEIRO”	Somente SQL

Nome	Tipo	Categoria	Valor de exemplo	Fonte
Perfil de banco de dados	String	Configuração	“PRIMÁRIO”	Somente SQL
Modo aberto	String	Configuração	“LER ESCREVER”	Somente SQL
Modo de registro	String	Configuração	“REGISTRO DE ARQUIVAMENTO”	Somente SQL
Plataforma	String	Configuração	“Linux x86 de 64 bits”	Somente SQL
Bandeira CDB	String	Configuração	“SIM”	Somente SQL
É RAC	String	Topologia	“SIM” ou “NÃO”	Somente SQL
O Data Guard está em espera?	String	Topologia	“SIM” ou “NÃO”	Somente SQL
Modo de proteção	String	Topologia	“DESEMPENHO MÁXIMO”	Somente SQL
Corretor do Data Guard	String	Topologia	“ATIVADO”	Somente SQL
Conjunto de caracteres NLS	String	Configuração	“AL32UTF8”	Somente SQL
Contagem de PDB	Inteiro	Dimensionamento	3	Somente SQL
Flashback ativado	String	Configuração	“SIM”	Somente SQL
Caminho de detecção	String	Metadados	“phase2” ou “phase1b”	SQL, SISTEMA OPERACIONAL

Dados do PDB (oracle_data_pdb_full.csv)

Uma linha por PDB (banco de dados conectável). Esta tabela descreve os pontos de dados do PDB coletados:

 Note

Os dados do PDB exigem credenciais do banco de dados Oracle (conexão SQL). OS-level fallback não preenche esse CSV.

Nome	Tipo	Categoria	Valor de exemplo	Fonte
Nome da instância do CDB	String	Identidade	"ORCO"	Somente SQL
Nome do PDB	String	Identidade	"APPDB1"	Somente SQL
Modo aberto	String	Status	"LER ESCREVER"	Somente SQL
Status do ciclo de vida	String	Status	"NORMAL"	Somente SQL
Contagem de tablespaces	Inteiro	Dimensionamento	5	Somente SQL
Contagem de arquivos de dados	Inteiro	Dimensionamento	12	Somente SQL
Tamanho total de bytes	Inteiro	Dimensionamento	5368709120	Somente SQL
Contagem de esquemas do usuário	Inteiro	Dimensionamento	8	Somente SQL
Contagem de links do DB	Inteiro	Conectividade	2	Somente SQL

Nome	Tipo	Categoria	Valor de exemplo	Fonte
Componentes instalados	String	Configuração	“ÁPICE; JVM; XML”	Somente SQL
Contagem de tablespaces criptografados	Inteiro	Segurança	1	Somente SQL

Dados de uso do recurso (oracle_data_features_full.csv)

Uma linha por entrada de uso do recurso de DBA_FEATURE_USAGE_STATISTICS. Esta tabela descreve os pontos de dados de uso do recurso coletados:

 Note

Os dados de uso do recurso exigem credenciais do banco de dados Oracle (conexão SQL). OS-level fallback não preenche esse CSV.

Nome	Tipo	Categoria	Valor de exemplo	Fonte
Nome da instância do CDB	String	Identidade	“ORCO”	Somente SQL
Nome	String	Recurso	“Particionamento (usuário)”	Somente SQL
Usos detectados	Inteiro	Usage	42	Somente SQL
Usado atualmente	String	Usage	“VERDADEIRO”	Somente SQL
Data da primeira utilização	DateTime	Usage	“2024-01-15T00:00:00”	Somente SQL
Data da última utilização	DateTime	Usage	“2026-06-01T00:00:00”	Somente SQL

Dados de opções (oracle_data_options_full.csv)

Uma linha por entrada V\$OPTION por CDB. Esta tabela descreve os pontos de dados das opções instaladas coletados:

Note

Os dados de opções exigem credenciais do banco de dados Oracle (conexão SQL). OS-level fallback não preenche esse CSV.

Nome	Tipo	Categoria	Valor de exemplo	Fonte
Nome da instância do CDB	String	Identidade	“ORCO”	Somente SQL
Nome da opção	String	Opção	“Análise avançada”	Somente SQL
Está instalado	String	Opção	“VERDADEIRO”	Somente SQL
ID do contêiner	Inteiro	Opção	0	Somente SQL

Dados de componentes (oracle_data_components_full.csv)

Uma linha por componente DBA_REGISTRY. Esta tabela descreve os pontos de dados do componente coletados:

Note

Os dados dos componentes exigem credenciais do banco de dados Oracle (conexão SQL). OS-level fallback não preenche esse CSV.

Nome	Tipo	Categoria	Valor de exemplo	Fonte
Nome da instância do CDB	String	Identidade	“ORCO”	Somente SQL

Nome	Tipo	Categoria	Valor de exemplo	Fonte
Nome do PDB	String	Identidade	"APPDB1"	Somente SQL
ID do componente	String	Componente	"ÁPICE"	Somente SQL
Nome do componente	String	Componente	"Oracle Application Express"	Somente SQL
Versão	String	Componente	"22.1.0.15.0"	Somente SQL
Status	String	Componente	"VÁLIDO"	Somente SQL
Schema	String	Componente	"APEX_220100"	Somente SQL

Considerações sobre segurança

Protegendo a ferramenta de descoberta VM

A segurança da VM da ferramenta de descoberta é crucial porque a ferramenta de descoberta armazena todas as credenciais, registros e dados do cliente na VM da ferramenta de descoberta.

A ferramenta de descoberta VM tem acesso ssh desabilitado por padrão e só pode ser acessada a partir do cliente. `vCenter UI -> "Launch Web Console"`

A ferramenta de descoberta VM vem com uma senha de login padrão "senha" para a "descoberta" do usuário.

- Recomendamos que você atualize essa senha imediatamente após a implantação.
- Exigimos que você atualize a senha se quiser habilitar o ssh usando o comando `enablessh` depois de fazer login usando o `vCenterLaunch Web Console`. Observe que toda vez que esse comando é chamado, você precisa redefini-lo.

Protegendo credenciais

Melhores práticas gerais para gerenciamento de credenciais

- Armazene credenciais com segurança

- Alterne regularmente todas as credenciais
- Use gerenciadores de senhas ou cofres seguros
- Monitore o uso de credenciais
- Siga o princípio do privilégio mínimo e conceda apenas as permissões mínimas necessárias

Credenciais SNMP v2

- Use cadeias de caracteres de comunidade complexas e não padrão
- Evite cadeias de caracteres comuns, como “pública” ou “privada”
- Trate as cadeias de caracteres da comunidade como senhas

Credenciais SNMP v3

- Ative a autenticação e a privacidade
- Use protocolos de autenticação fortes (SHA preferido em vez de MD5)
- Use protocolos de criptografia fortes (AES preferido em vez de DES)
- Use senhas complexas para autenticação e privacidade
- Use nomes de usuário exclusivos (evite nomes comuns)

Credenciais WinRM

- Evite desativar a verificação do certificado WinRM.
- Recomendamos que você crie uma conta de serviço dedicada com o mínimo de permissões necessárias.
- Evite usar contas de administrador de domínio ou administrador local, a menos que você precise da coleção do SQL Server. A coleção do SQL Server requer acesso de administrador local porque consulta vários namespaces WMI e usa comandos elevados. Para métricas do sistema operacional sem a descoberta do SQL Server, uma conta não administrativa com usuários de gerenciamento remoto, usuários do monitor de desempenho e acesso de leitura ao WMI `root\cimv2` é suficiente. Consulte [the section called “Permissões obrigatórias”](#) para obter detalhes por módulo.

Hyper-V credenciais

- Use contas de serviço dedicadas com permissões mínimas Hyper-V de gerenciamento.
- Evite usar contas de administrador de domínio.
- Hyper-V as credenciais oferecem suporte à autenticação NTLM (somente HTTPS) e Kerberos.
- A ferramenta de descoberta armazena credenciais criptografadas em repouso usando SQLCipher.

Credenciais da Oracle

- Use uma conta de serviço dedicada somente para leitura com apenas `SELECT_CATALOG_ROLE`. Não use privilégios de `DBA`, `SYSDBA` ou `SYSOPER`.
- A ferramenta de descoberta executa somente operações de leitura e nunca grava no banco de dados Oracle.
- A ferramenta de descoberta não acessa as visualizações do Diagnostics Pack ou do Tuning Pack, portanto, nenhuma licença adicional da Oracle é necessária.
- Alterne a senha da conta de serviço Oracle regularmente e atualize a credencial na ferramenta de descoberta.

Armazenamento de credenciais

A ferramenta de descoberta criptografa as credenciais armazenadas em repouso usando uma chave de criptografia de banco de dados. Em sistemas com `systemd 250` ou posterior, essa chave é criptografada usando `systemd-creds`. Em sistemas mais antigos, a chave é armazenada como um arquivo protegido por permissão. Em ambos os casos, um invasor com acesso `root` ao host da ferramenta de descoberta poderia acessar a chave de criptografia e descriptografar as credenciais armazenadas. Restrinja o acesso ao host da ferramenta de descoberta e trate-o como um sistema privilegiado em seu ambiente.

Usando o Auto-Connect recurso com cuidado

A ferramenta de descoberta usa dois mecanismos para atribuir credenciais aos servidores durante a OS-level coleta: conexão automática e manual. OS-level A coleção inclui os módulos de métricas de rede, SQL Server, banco de dados Oracle e sistema operacional. Esses módulos se conectam a servidores individuais de todas as fontes, incluindo VMs VMware, Hyper-V VMs e servidores importados.

Manual: um servidor pode ser associado manualmente a uma credencial específica. Nesse caso, a ferramenta de descoberta usa somente essa credencial, independentemente do sucesso ou do fracasso. Você deve monitorar manualmente o status da coleta desse servidor e fazer ajustes.

Auto-connect: se nenhuma credencial for associada manualmente ao servidor, a ferramenta de descoberta usará o mecanismo de conexão automática desse servidor. Isso significa:

- No início de cada rodada de coleta, a ferramenta de descoberta obtém uma lista de credenciais disponíveis para esse servidor (com base nos tipos de sistema operacional) e também configurada para ser “conectável automaticamente”.
- Em seguida, a ferramenta de descoberta testa todas as credenciais no servidor em um loop.
 - Se uma credencial ativa for encontrada, a rodada de coleta para o servidor será bem-sucedida. A ferramenta de descoberta se lembra disso e o experimenta primeiro na próxima vez.
 - Se nenhuma credencial ativa for encontrada, a rodada de coleta do servidor falhou.
 - Módulo de rede: o servidor usa um cronograma de recuo, iniciando a próxima rodada de coleta em 3 minutos, 30 minutos, 2 horas e 6 horas após cada falha (semelhante ao recuo exponencial).
 - Coleção do SQL Server: a ferramenta de descoberta não tenta novamente. Ele faz uma tentativa por servidor por dia.

Impacts/Risks:

Use a conexão automática somente quando tiver certeza de que os riscos são mitigados em seu sistema:

Risco 1: Com a conexão automática configurada em várias credenciais erradas, testá-las automaticamente em servidores pode desencadear bloqueios de contas em ambientes de produção em que as políticas de bloqueio estão configuradas. Por exemplo, um data center pode configurar suas VMs para serem bloqueadas após três tentativas malsucedidas de login SSH. Nesse caso, se a conexão automática for configurada para 3 credenciais SSH erradas, ocorrerão bloqueios legítimos da conta. Se ocorrerem bloqueios em vários sistemas, processos comerciais críticos poderão ser afetados, causando potencialmente falhas em cascata nos sistemas dependentes. Além disso, os Centros de Operações de Segurança podem sofrer tempestades de alertas de eventos de falha de autenticação em massa, criando incidentes de segurança falsos positivos que drenam recursos e podem mascarar ataques reais.

Risco 2: O ator com acesso à ferramenta de descoberta (conhece a senha da ferramenta de descoberta) pode forçar as credenciais do sistema operacional em todos os servidores, configurando um grande número de credenciais de teste e usando a conexão automática para encontrar as bem-sucedidas.

Mitigações:

Siga estas diretrizes:

- Certifique-se de que a senha da ferramenta de descoberta esteja devidamente protegida e seja conhecida somente por agentes autorizados
- Certifique-se de que as credenciais adequadas sejam inseridas para o ambiente se as políticas de bloqueio estiverem em vigor. Recomendamos configurar somente credenciais de trabalho conhecidas, mesmo que as políticas de bloqueio de conta estejam ausentes, para garantir uma carga operacional mínima em VMs individuais.
- “Auto-connect” é um recurso opcional. Não a selecione e use a atribuição manual de credenciais se o bloqueio da conta for uma preocupação para o meio ambiente.

Segurança de importação de CSV

Ao importar servidores usando um arquivo CSV, considere as seguintes implicações de segurança:

- O arquivo CSV pode conter nomes de host ou endereços IP de servidores internos. Trate-os como dados confidenciais.
- As `oracle_credential_name` e `os_credential_name` colunas os fazem referência às credenciais pré-configuradas por nome amigável. O CSV não contém segredos.
- All-or-nothing validação: se alguma linha no CSV for inválida, todo o upload será rejeitado. Isso evita importações parciais que podem criar um estado confuso.
- Os servidores importados ficam imediatamente visíveis no inventário e são elegíveis para coleta. Certifique-se de que as credenciais do sistema operacional e do Oracle tenham o escopo correto antes de importar.

Considerações sobre a revogação do acesso

Quando você revoga o acesso, a exclusão tem como escopo a fonte específica:

- A revogação do acesso ao vCenter exclui somente os dados do vCenter. Ela não afeta Hyper-V nem importa os dados do servidor.
- A revogação do Hyper-V acesso exclui somente Hyper-V os dados. Isso não afeta o VMware nem os dados importados do servidor.
- A exclusão dos servidores importados os remove do inventário, mas os dados da coleta posterior (rede, banco de dados, métricas do sistema operacional) são retidos.
- Para remover todos os dados de inventário específicos da fonte, você deve revogar ou excluir cada fonte de forma independente. Os dados de coleta downstream (rede, banco de dados, métricas do sistema operacional) são retidos mesmo após a revogação de todas as fontes.

Solução de problemas

Verificando a conectividade da ferramenta de descoberta com o vCenter

Quando você encontrar erros de configuração do módulo VMware, siga estas etapas para verificar a conectividade:

Acesse a ferramenta de descoberta VM

- Log-in para a ferramenta de descoberta VM, abra o console remoto no vCenter
 - Nome de usuário: discovery
 - Senha: senha

Teste a conectividade do vCenter

1. Teste o acesso à API vCenter:

```
curl -v --insecure -u <username>:<password> https://<vcenter-ip-or-hostname>:443/mob
```

2. Resultado de sucesso esperado:

```
[ec2-user@discoverytool ~]$ curl -v --insecure -u <user>:<password> https://vcsa/mob > tmp.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %    0     0    0         0      0      0     0
           %    0     0    0         0      0      0     0
```

```

0 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

```

Teste o certificado SSL

1. Execute este comando:

```
openssl s_client -showcerts -servername <hostname> -connect <hostname>:443
```

2. Resultado de sucesso esperado:

- Deve mostrar detalhes do certificado vSphere
- Verifica a SSL/TLS conectividade na porta 443

```

[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

```

Solução de problemas do WinRM

Se você estiver enfrentando problemas de conectividade com o WinRM, siga estas etapas para testar a conexão. Essas etapas também se aplicam a problemas de Hyper-V conectividade, porque a ferramenta de descoberta usa o WinRM para se comunicar com os hosts. Hyper-V

Teste a conectividade básica do WinRM usando as portas 5985 (HTTP) e 5986 (HTTPS).

Precisamos garantir que a conectividade funcione na porta 5986 (HTTPS)

```
# 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
```

Se os testes acima falharem, tente estabelecer uma PowerShell sessão com a validação do certificado desativada:

```
$cred = Get-Credential
$so = New-PsSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
Enter-PSsession -ComputerName <HOST> -Credential $cred -Port 5985 -SessionOption $so
```

Solução de problemas do Kerberos

Se você tiver falhas de autenticação Kerberos ao coletar dados de servidores Windows, use as seções a seguir para diagnosticar e resolver problemas comuns.

Verifique os requisitos de rede

Antes de solucionar problemas de autenticação Kerberos, verifique se a ferramenta de descoberta pode alcançar os endpoints de rede necessários.

Para verificar os requisitos de rede para Kerberos

1. Verifique a resolução de DNS para o controlador de domínio. Execute o seguinte comando na ferramenta de descoberta VM:

```
nslookup dc01.example.com
```

Você também pode usar dig:

```
dig dc01.example.com
```

Se a resolução de DNS falhar, verifique se a VM da ferramenta de descoberta está configurada para usar um servidor DNS que possa resolver seu domínio do Active Directory. Verifique `/etc/resolv.conf` e confirme se as entradas do servidor de nomes apontam para os servidores DNS do seu domínio.

2. Verifique a conectividade com o Centro de Distribuição de Chaves (KDC) na porta 88. Execute este comando: .

```
nc -zv dc01.example.com 88
```

Saída esperada:

```
Connection to dc01.example.com 88 port [tcp/kerberos] succeeded!
```

Se a conexão falhar, verifique se nenhuma regra de firewall bloqueia o tráfego da VM da ferramenta de descoberta para o controlador de domínio na porta 88.

3. Verifique a conectividade com os servidores Windows de destino nas portas WinRM. Execute os seguintes comandos :

```
nc -zv <windows-server> 5985  
nc -zv <windows-server> 5986
```

Se a conexão falhar, verifique se o WinRM está habilitado no servidor de destino e se as regras de firewall permitem tráfego de entrada nas portas 5985 e 5986.

Problemas comuns do Kerberos

A seguir estão os problemas comuns do Kerberos e suas soluções.

Erros de distinção entre maiúsculas

Sintoma: Você recebe um erro “Servidor não encontrado no banco de dados Kerberos” durante a autenticação.

Esse erro geralmente ocorre quando o nome do território Kerberos não está em maiúsculas.

As regiões Kerberos devem ser especificadas em maiúsculas em seu arquivo. `krb5.conf` Por exemplo, use `EXAMPLE.COM` em vez de `example.com`.

Prevenção de bloqueio de conta

A ferramenta de descoberta usa um mecanismo de recuo para evitar bloqueios de contas devido a repetidas tentativas de autenticação malsucedidas. Se sua conta de serviço for bloqueada, você poderá redefinir o processo de coleta interrompendo e iniciando o módulo de coleta por meio da interface web da ferramenta de descoberta em `https://<discovery-tool-vm-ip>:5000`.

kinit falha na CLI

A tabela a seguir lista `kinit` os erros comuns e suas soluções.

Erro	Causa	Solução
Não é possível encontrar o KDC para o reino	O nome do host ou endereço IP do KDC não está acessível ou o território não está configurado em <code>krb5.conf</code>	Verifique se o <code>krb5.conf</code> arquivo contém o nome de host e o território KDC corretos. Confirme a resolução do DNS e a conectividade de rede com o KDC na porta 88.
Falha na pré-autenticação	A senha da conta de serviço está incorreta.	Verifique a senha e tente novamente. Se a conta estiver bloqueada, desbloqueie-a no Active Directory antes de tentar novamente.
Cliente não encontrado no banco de dados Kerberos	O nome principal não corresponde a nenhuma conta no Active Directory.	Verifique se o nome principal corresponde exatamente ao nome da conta, incluindo maiúsculas e minúsculas. Use

Erro	Causa	Solução
		o formato <code>username@REALM</code> com o reino em maiúsculas.
Não é possível resolver o endereço de rede do KDC	O DNS não pode resolver o nome do host KDC.	Verifique a configuração do DNS em <code>/etc/resolv.conf</code> . Confirme se o servidor DNS pode resolver o nome do host KDC. Teste com <code>nslookup</code> ou <code>dig</code> .

A coleta falha apesar do sucesso da triagem

Se for `kinit` bem-sucedido, mas a coleta de dados ainda falhar, verifique o seguinte:

1. Verifique se o nome principal usado para a coleta corresponde `kinit` exatamente ao caso usado durante.
2. Verifique se a conta de serviço tem as permissões necessárias nos servidores de destino.
3. Verifique se o WinRM está habilitado nos servidores de destino.
4. Verifique se o nome do host usado para a coleta corresponde ao nome do host registrado no Active Directory.

O Kerberos funciona para alguns servidores, mas não para outros

Se a autenticação Kerberos for bem-sucedida em alguns servidores, mas falhar em outros, investigue as seguintes áreas:

Se seus servidores abrangem vários domínios do Active Directory, configure uma credencial Kerberos separada para cada domínio. Certifique-se de que seu `/etc/krb5.conf` arquivo inclua entradas para todos os reinos. Cada domínio exige sua própria credencial com o `username@REALM` principal correto.

Compare a configuração do WinRM em um servidor em funcionamento com um servidor com falha. Execute o seguinte comando em cada servidor:

```
winrm get winrm/config
```

Teste a conectividade com a Área de Trabalho Remota para isolar o problema. A ferramenta de descoberta usa o `formatousername@DOMAIN`, enquanto a Área de Trabalho Remota usa o `formatoDOMAIN\username`.

Verifique se a conta de serviço é membro do grupo local de administradores no servidor com falha. Execute o seguinte comando no servidor de destino:

```
net localgroup Administrators
```

O WMI exige privilégios de administrador local para acessar as informações do sistema operacional. A coleção do SQL Server também exige que a conta de serviço tenha acesso de administrador local no servidor de destino.

Lista de verificação de configuração do Kerberos

Use a lista de verificação a seguir para verificar a configuração do Kerberos antes de iniciar a coleta de dados.

- O `krb5.conf` arquivo existe na ferramenta de descoberta VM.
- O nome do reino está em maiúsculas em `krb5.conf`
- A execução `kinit` com a conta de serviço é bem-sucedida sem erros.
- `klistA` corrida mostra um tíquete válido e não expirado.
- O nome principal corresponde exatamente ao nome da conta do Active Directory.
- A resolução de DNS funciona para o nome do host KDC.
- A conectividade de rede com o KDC na porta 88 está confirmada.
- A conectividade de rede para servidores Windows de destino nas portas 5985 e 5986 está confirmada.
- (Multi-domain) Cada domínio do Active Directory tem sua própria credencial configurada na ferramenta de descoberta `[realms]` e `krb5.conf` contém `[domain_realm]` entradas para todos os domínios.

Solução de problemas do banco de dados

Para diagnosticar problemas de coleta do Oracle Database, como dados ausentes ou erros, verifique o seguinte.

Conexão recusada ou tempo limite

Sintoma: O status da coleta do Oracle mostra um erro de conexão para um servidor.

Para solucionar esse problema, verifique o seguinte:

- Verifique se o ouvinte Oracle está sendo executado no host de destino: `lsnrctl status`
- Verifique a conectividade de rede da ferramenta de descoberta com o host Oracle na porta 1521 (ou sua porta personalizada): `nc -zv <oracle-host> 1521`
- Verifique se as regras de firewall permitem conexões de entrada na porta do ouvinte Oracle.
- Verifique o nome do serviço executando `lsnrctl services` no host Oracle. Se o nome do serviço estiver incorreto, o ouvinte Oracle rejeitará a conexão.

Falhas de autenticação (ORA-01017)

Sintoma: falha na coleta com um erro de nome de usuário ou senha inválidos.

Para solucionar esse problema, verifique o seguinte:

- Verifique se a conta de serviço Oracle existe e não está bloqueada: `SELECT account_status FROM dba_users WHERE username = 'DISCOVERY_USER';`
- Verifique se a senha está correta conectando-se manualmente: `sqlplus discovery_user/<password>@<host>:1521/<service_name>`
- Se a conta estiver bloqueada, desbloqueie-a: `ALTER USER discovery_user ACCOUNT UNLOCK;`

Privilégios insuficientes () ORA-01031

Sintoma: a conexão é bem-sucedida, mas a coleta retorna dados incompletos.

Para solucionar esse problema, verifique o seguinte:

- Verifique se `SELECT_CATALOG_ROLE` foi concedido: `SELECT * FROM dba_role_privs WHERE grantee = 'DISCOVERY_USER';`
- Conceda a função necessária se estiver faltando: `GRANT SELECT_CATALOG_ROLE TO discovery_user;`

A credencial manual mostra erro, mas a conexão automática funciona

Quando você fixa uma credencial manualmente em um servidor, a ferramenta de descoberta não retrocede se a conexão falhar. Verifique se a porta e o nome do serviço que você configurou na credencial correspondem ao ouvinte Oracle nesse servidor específico. Se o servidor tiver uma porta ou nome de serviço não padrão, atualize a configuração da credencial adequadamente.

OS-level fallback não detectando o Oracle

Se nenhuma credencial do banco de dados estiver configurada e o OS-level fallback não detectar o Oracle:

- Verifique se as credenciais SSH ou WinRM OS estão configuradas e funcionando para o servidor (verifique o status da coleta de métricas do sistema operacional).
- Para hosts Linux, verifique se `/etc/oratab` existe ou se os processos do Oracle process monitor (pmon) estão em execução.
- Para hosts Windows, verifique se as entradas do registro Oracle existem `HKLM\SOFTWARE\Oracle` ou se os `oracle.exe` processos estão sendo executados.

Solução de problemas de SNMP

Acesse a ferramenta de descoberta VM

- Log-in para a ferramenta de descoberta VM, abra o console remoto no vCenter
 - Nome de usuário: discovery
 - Senha: senha

Instale as ferramentas SNMP (se necessário)

- `sudo yum install net-snmp-utils -y`

Teste a conexão SNMP com servidores Linux

1. `snmptable -v 2c -c <COMMUNITY_STRING>
<REMOTE_SERVER_IP> .1.3.6.1.2.1.6.13.1`
2. Exemplo:

```
#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
```

Erros de coleta de rede

é necessário um terminal para ler a senha

Erro:

```
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
```

O comando `ss` está solicitando a senha do usuário. O usuário `ssh` configurado deve estar no grupo `sudoers` e estar configurado com `sudo` sem senha para o comando. `ss/netstat` Para configurar o `sudo` sem senha:

1. Crie um novo arquivo `sudoers`:

```
sudo vi -f /etc/sudoers.d/<username>
```

2. Adicione a linha:

```
<username> ALL=(ALL) NOPASSWD: /usr/sbin/ss, /usr/bin/netstat
```

3. Após essa alteração, em execução `sudo ss -tnap` e `sudo netstat -tnap` deve ser executado sem solicitar uma senha

A coleção de rede foi executada sem sudo

Se você ver o seguinte aviso na página Inventário descoberto:

```
Network collection ran without sudo. Process-level connection data may be missing.
```

Esse aviso indica que a conta de usuário SSH não tem acesso sudo no servidor de destino. Sem o sudo, a ferramenta de descoberta ainda pode coletar dados de conexão de rede, mas não pode determinar qual processo possui cada conexão. Para coletar dados completos de conexão em nível de processo, certifique-se de que o usuário SSH tenha acesso sudo no servidor de destino.

Erros de coleta de métricas do sistema operacional

UUID de servidor ausente para servidores Linux

Se a ferramenta de descoberta não conseguir coletar o UUID do servidor (exibido como vazio ou ausente) para servidores Linux, verifique se as credenciais SSH configuradas para esses servidores têm privilégios sudo. A ferramenta usa dmidecode para ler o UUID do servidor. Se não dmidecode estiver instalada, a ferramenta volta à leitura `/sys/class/dmi/id/product_uuid`, o que também requer acesso sudo. Sem o sudo, nenhum método pode recuperar o UUID.

Resolução: Certifique-se de que a conta de usuário SSH fornecida à ferramenta de descoberta tenha acesso sudo nos servidores Linux de destino.

Problemas de acesso no inventário descoberto

Se você ver uma mensagem no status da coleção do servidor, como Credenciais ausentes ou Acesso negado:

1. Selecione o servidor na tabela de servidores descobertos.
2. Escolha Gerenciar credencial de acesso. Você pode optar por:
 - a. Selecione credenciais alternativas no menu suspenso Selecionar credenciais.
 - b. Selecione Usar novas credenciais e fornecer novas credenciais.
3. Save (Salvar).

A ferramenta de descoberta tenta novamente a conexão depois que você salva suas alterações.

Solução de problemas de autenticação com chave SSH

Testando a conectividade da chave SSH a partir da ferramenta de descoberta

Se a autenticação da chave SSH falhar, verifique a conectividade da ferramenta de descoberta com o servidor de destino:

1. Faça login na ferramenta de descoberta (via console vSphere ou SSH no host Linux).
2. Teste a conectividade SSH usando sua chave privada:

```
ssh -i /path/to/private_key -o StrictHostKeyChecking=no <username>@<target_ip>
```

3. Se a conexão for bem-sucedida, o problema é como a chave foi carregada na ferramenta de descoberta. Re-upload insira a chave e verifique se o nome de usuário corresponde.
4. Se a conexão falhar, verifique a mensagem de erro na tabela a seguir.

Mensagem de erro	Causa	Resolução
Permission denied (publickey)	A chave pública não está no <code>authorized_keys</code> arquivo do servidor de destino ou o nome de usuário está errado.	Adicione a chave pública ao <code>~/.ssh/authorized_keys</code> servidor de destino para o usuário correto. Verifique as permissões do arquivo: <code>chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys</code> .
Connection timed out after 20s	A porta 22 não pode ser acessada pela ferramenta de descoberta.	Verifique se a porta 22 está aberta entre a ferramenta de descoberta e o servidor de destino. Verifique firewalls e grupos de segurança.
Connection refused	O serviço SSH não está sendo executado no servidor de destino.	Inicie o serviço SSH: <code>sudo systemctl start sshd</code> .
Invalid SSH key for credential ' <i>name</i> '	O formato da chave não é suportado, os dados da chave estão corrompidos ou a frase secreta está ausente ou está incorreta.	Verifique se o formato da chave é RSA, ECDSA ou Ed25519 no formato PEM, OpenSSH ou PKCS #8. Se a chave estiver criptografada, verifique se a senha está correta.

Solução de problemas do instalador Linux

A porta 5000 já está em uso

Sintoma: O serviço da ferramenta de descoberta falha ao iniciar após a instalação.

Resolução: identifique e interrompa o processo usando a porta 5000:

```
sudo ss -tlnp | grep :5000
```

Pare o processo conflitante e reinicie a ferramenta de descoberta:

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

Mensagens de erro comuns

Esta tabela descreve mensagens de erro comuns e suas explicações:

Mensagem	Local	Explicação
Uma senha já foi criada	Criar página de senha	Condição de corrida quando dois usuários criam senhas ao mesmo tempo; atualizar
Falha na exportação	Página de inventário	Tente novamente ou envie registros
Uma coleta sob demanda já está em andamento	Página de inventário	Condição de corrida quando dois usuários iniciam as coletas manuais ao mesmo tempo; tente novamente após a conclusão da coleta manual atual
Command timed out after 60s	Status da coleção do servidor	Um comando no servidor de destino não foi concluído em 60 segundos. Isso pode ocorrer em servidores muito carregados. Repita a coleta ou investigue a carga do servidor de destino.
Uma ou mais credenciais contêm UUIDs desconhecidos	Página de acesso ao sistema operacional	Condição de corrida quando dois usuários editam as credenciais do

Mensagem	Local	Explicação
		sistema operacional ao mesmo tempo; tente novamente
Senha inválida	Sign-in página	Senha incorreta para fazer login; entre em contato com o administrador ou entre em contato
Sua sessão expirou. Por favor, faça login novamente.	Sign-in página	A sessão expirou, é necessário fazer login novamente
Ocorreu um erro interno	Várias páginas	Tente novamente ou envie registros

Notas da versão

Esta seção descreve os recursos, aprimoramentos e correções de erros da ferramenta de AWS Transform descoberta, organizados por data de lançamento.

Data	Versão	Notas de versão
30 de junho de 2026	1.0.1646	Novos recursos - Foi adicionada a descoberta do Oracle Database. A ferramenta coleta topologia de CDB e PDB, versão, edição, opções instaladas, uso de recursos e inventário de componentes. A ferramenta de descoberta oferece suporte a conexões SQL diretas (usando SELECT_CATALOG_ROLE) e OS-level detecção de fallback por meio de SSH ou WinRM. - Foi adicionado suporte para várias credenciais Kerberos em diferentes domínios do Active Directory. Cada credencial é autenticada de forma independente, permitindo a coleta de servidores Windows em vários domínios sem conflitos de autenticação. Melhorias

Data	Versão	Notas de versão
		• Coleção aprimorada de métricas de sistema operacional para hosts legados. Foi adicionada a coleta de dados alternativos para sistemas operacionais mais antigos (RHEL 5, SLES 11, Windows Server 2008 R2) em que os comandos modernos não estão disponíveis. Os dados de armazenamento, desempenho e interface de rede agora são coletados usando interfaces de sistema alternativas. Correções de bugs • Falhas de autenticação Kerberos corrigidas para servidores descobertas por meio de. Hyper-V A ferramenta de descoberta agora resolve corretamente o nome do host do servidor (FQDN) dos metadados do Hyper-V convidado, necessários para a correspondência do SPN do Kerberos.

Data	Versão	Notas de versão
14 de maio de 2026	1.0.1363	Novos recursos • Instalador Linux adicionado para implantar a ferramenta de descoberta em distribuições Linux compatíveis (Amazon Linux 2, Amazon Linux 2023, RHEL 8—9, Rocky Linux 8—9, 9, Ubuntu 20.04—24.04, Debian 10—12, AlmaLinux SLES 15 SP5). • Foi adicionado suporte para configurar vários servidores VMware vCenter com deduplicação automática de VM em todos os vCenters. • Foi adicionada a autenticação de chave privada SSH como alternativa ao nome de usuário e senha para acesso ao sistema operacional Linux. Os formatos de chave suportados incluem RSA, ECDSA, Ed25519, OpenSSH e PKCS #8. • Foi adicionada uma coleção de rede de endereços privados para capturar conexões de e para endereços IP privados da RFC 1918 que não estão em seu inventário descoberto. • Opções de exportação adicionadas para selecionar um intervalo de datas personalizado e escolher quais módulos de dados incluir na exportação. Melhorias • Maior confiabilidade da coleta programada ao escalonar os cronogramas dos coletores. • Melhor desempenho da coleta de métricas do sistema operacional por meio de lotes de comandos SSH. • As alterações de credenciais agora repetem imediatamente os servidores que falharam anteriormente. • A coleção de métricas do sistema operacional agora relata um status parcial quando alguns comandos retornam resultados vazios.

Data	Versão	Notas de versão
		• Melhor visibilidade de erros para problemas de conexão do vCenter no painel.
7 de abril de 2026	1.0.1074	Novos recursos • Suporte adicional para Hyper-V descoberta da Microsoft, incluindo descoberta automática de VMs de Hyper-V hosts com deduplicação de clusters de failover. • Foi adicionado suporte para importação de servidores por meio do upload de arquivos CSV. • Coleção de métricas de sistema operacional adicionada com seis módulos independentes: desempenho do servidor, desempenho do armazenamento, provisionamento do servidor, provisionamento do armazenamento, interfaces de rede e processos em execução. • Opção Hyper-V de implantação adicionada usando um arquivo de imagem VHD. • Melhorou o fortalecimento da segurança local removendo EC2-specific serviços e bloqueando o acesso ao endpoint de metadados da instância.
26 de março de 2026	1.0.1014	Correções de erros e melhorias • Moveu a validação de capitalização de domínio Kerberos do back-end para o front-end. • Mudou de Python-kerberos para Python-pykerberos e tornou o cache baseado em arquivos o padrão. • Corrigiu a validação da ID do servidor de edição em massa sem distinção entre maiúsculas e minúsculas • Nome do arquivo ZIP de exportação fixo (agoradiscovery_tool_export.zip). • Verificação de execução do serviço corrigido e registros de depuração adicionados para credenciais do sistema. • Script de configuração de rede adicionado para criar artefato.

Data	Versão	Notas de versão
16 de dezembro de 2025	1.0.718	Novos recursos e melhorias • Foi adicionado suporte ao SMBIOS UUID para evitar a duplicação de VMs em serviços downstream. • Introduziu o Min/Max/Avg rastreamento e expandiu as métricas de armazenamento para melhorar o monitoramento de recursos. • Foram adicionadas melhorias na validação da API. • Foi adicionada a funcionalidade do painel de ajuda com orientação contextual. • Terminologia atualizada de “coletor” para “ferramenta” em toda a interface.
31 de outubro de 2025	1.0.0	Lançamento inicial Lançamento inicial da ferramenta de AWS Transform descoberta. Essa versão inclui: • Coleção offline (sem dependência de uma AWS conta ou do Application Discovery Service). • Detecção e monitoramento da VMware. • Descoberta do banco de dados do SQL Server. • Server-to-server coleta de comunicação por meio de SSH, WMI e SNMP.

AWS Conectores de transformação

AWS Os conectores Transform permitem que você acesse com segurança os recursos em todos os limites da conta para fluxos de trabalho de migração e modernização. Isso permite que você acesse e gerencie recursos em todos os limites da conta, mantendo os controles e as permissões de segurança. Um conector representa uma conexão entre sua conta de AWS Transform-enabled origem e recursos externos nas contas de AWS destino ou em sistemas de terceiros.

Os conectores exigem solicitações de acesso do conector de origem e aprovação do proprietário da conta de destino. Você faz essa solicitação ao configurar um conector de origem. Da mesma forma, você pode receber solicitações para aprovar conectores de destino para permitir que outras contas acessem sua conta.

- Criação de conectores: crie conectores em sua conta de AWS Transform-enabled origem, especificando a conta de destino e as permissões necessárias
- Configuração de permissão: o AWS Transform exige funções e permissões específicas do IAM na conta de destino para realizar ações de migração, incluindo:
 - Gerenciando dados de migração com AWS KMS
 - Fazendo chamadas de API entre regiões
 - Instalação de agentes de replicação em servidores VMware
 - Criação de infraestrutura de rede (VPCs, sub-redes, roteamento)
 - Lançamento de instâncias do Amazon EC2 e implantação de pilhas CloudFormation
 - Executando fluxos de trabalho de migração por meio do Migration Hub
- Processo de aprovação: você deve aprovar as solicitações do conector de destino antes que o AWS Transform possa acessar seus recursos.
- Conexão ativa: depois de aprovar um conector, ele permite que os trabalhos do AWS Transform acessem e gerenciem com segurança os recursos na conta de destino.

Rastreabilidade do usuário para operações de agentes

Por padrão, AWS CloudTrail registra as ações do agente em seus AWS recursos sob a identidade do serviço AWS Transform. A rastreabilidade do usuário atribui essas ações ao usuário específico do AWS IAM Identity Center que iniciou ou interagiu com o trabalho, permitindo a auditoria de segurança e a investigação de incidentes no nível do usuário individual.

 Note

A rastreabilidade de usuários é compatível somente com usuários do IAM Identity Center (IDC).

Para ativar a rastreabilidade do usuário, ative a sessão em segundo plano nas configurações do seu perfil do AWS Transform. Quando ativado, o AWS Transform cria automaticamente uma [sessão em segundo plano](#) do IAM Identity Center quando você interage com um trabalho e a usa para produzir sessões de função do IAM com identidade aprimorada para operações de conectores. Essas sessões incorporam sua identidade de usuário em chamadas e AWS CloudTrail eventos AWS de serviço downstream. Quando as sessões em segundo plano são desativadas, o AWS Transform volta às sessões padrão de função assumida sem contexto de identidade do usuário.

Novos conectores são configurados automaticamente para oferecer suporte à rastreabilidade do usuário. Para conectores existentes, você deve adicionar manualmente `sts:SetContext` à política de confiança da função de conector:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": ["transform.amazonaws.com"] },
      "Action": ["sts:AssumeRole", "sts:SetContext"],
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "your-account-id" }
      }
    }
  ]
}
```

Você pode visualizar e revogar suas sessões ativas em segundo plano na guia Sessões em segundo plano na página do trabalho. Revogar uma sessão imediatamente a invalida e qualquer sessão de conector derivada dela.

Para saber mais, consulte [Visão geral da propagação de identidades de confiança](#) no AWS Guia do usuário do IAM Identity Center.

Gerenciando conectores

Na página Conectores, você pode ver:

- **Aba Conectores de origem:** lista todos os conectores que você criou para se conectar a outras contas, mostrando as contas de destino e o status do conector
- **Guia Conectores de destino:** mostra as solicitações de conectores recebidas de outras contas que desejam acessar seus recursos e exigem sua aprovação ou rejeição

AWS O Transform exige confirmação de ações críticas, como aprovação, rejeição ou exclusão de conectores, para evitar alterações acidentais que possam interromper seus fluxos de trabalho de migração ativos.

Para criar um conector

1. Navegue até a guia Conectores de origem.
2. Especifique a conta de destino e o tipo de recurso.
3. Configure as permissões e o escopo de acesso necessários.

Configurar permissões

1. Escolha criar uma nova função do IAM com as permissões necessárias ou
2. Selecione uma função existente que você criou anteriormente para conectores.
3. Certifique-se de que a função tenha todas as permissões necessárias para as operações de AWS transformação.

Para gerenciar solicitações recebidas

1. Analise as solicitações de conectores na guia Conectores de destino.
2. Aprove solicitações legítimas para permitir o acesso entre contas.
3. Rejeite tentativas de conexão não autorizadas ou desnecessárias.

Para gerenciar seus conectores

1. Monitore seus conectores ativos para garantir a segurança e a conformidade.

2. Exclua os conectores quando não precisar mais deles. Observe que isso fará com que os trabalhos em execução usando o conector falhem.
3. Atualize as permissões à medida que seus requisitos mudarem.

Migrações (incluindo VMware)

AWS O Transform pode ajudá-lo a migrar seus ambientes de servidores virtuais e bare metal para o Amazon EC2 usando IA generativa, incluindo Hyper-V VMware e outras fontes. Este capítulo fornece uma visão geral dos recursos de migração do AWS Transform e do fluxo de trabalho do processo de migração.

Capacidades e características principais

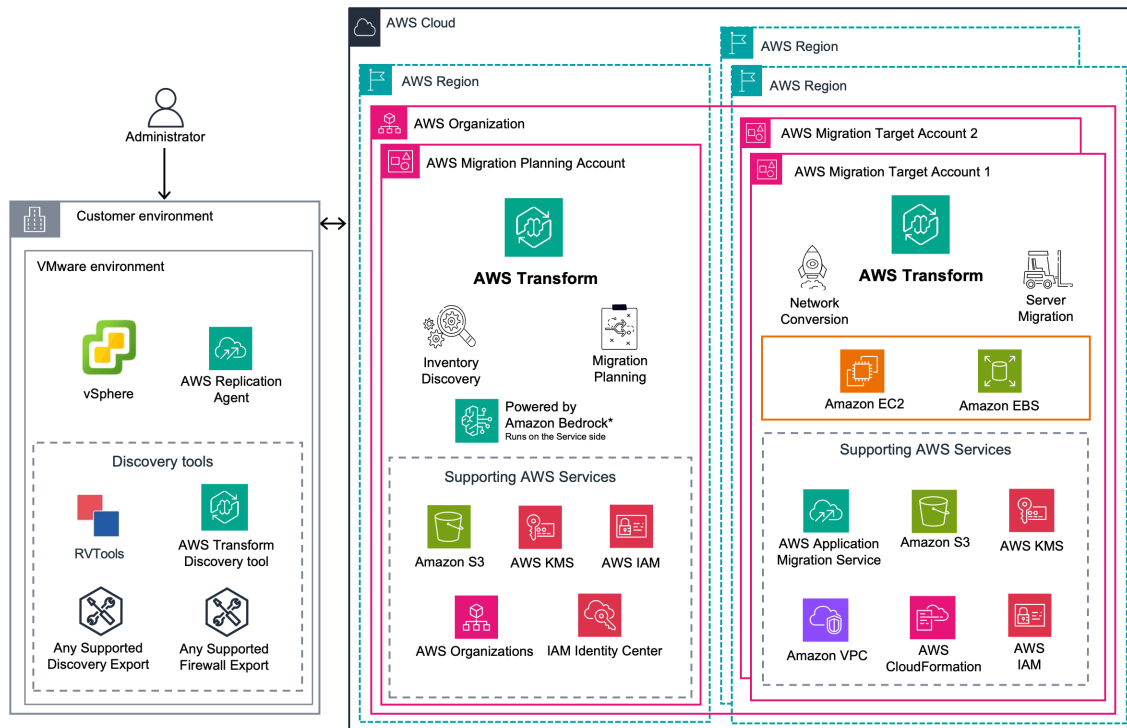
AWS O Transform oferece os seguintes recursos e os principais recursos para migrar seus ambientes de servidor para o AWS

- Várias opções de descoberta:
 - Descoberta assistida de seu ambiente VMware usando coletores de. AWS Application Discovery Service
 - Use a ferramenta de código aberto [Export for vCenter](#) (ambientes VMware).
 - Importação de dados de descoberta coletados de forma independente (qualquer ambiente de origem).
- AI-driven conversão da configuração de sua rede de origem em uma arquitetura de rede Amazon VPC.
- AI-driven geração de planos de migração, incluindo agrupamento de aplicativos e ondas de migração sugeridas.
- Hospedando novamente seus servidores para serem executados de forma nativa no Amazon EC2.
- Interface de aplicativo web localizada, permitindo que você use o AWS Transform para migrações em seu idioma preferido. Para obter mais informações, consulte [Configurações de idioma](#).

AWS O Transform oferece suporte à migração de servidores Windows e Linux de sistemas operacionais compatíveis. Para obter a lista completa dos sistemas operacionais compatíveis, consulte [Sistemas operacionais compatíveis](#) no Guia do AWS Transform MGN usuário.

AWS Transforme a arquitetura de migração

Este diagrama mostra uma visão geral da arquitetura de migração do AWS Transform.



Empregos de migração

Para usar o AWS Transform para migrações, primeiro você precisa de um espaço de trabalho, que é um contêiner lógico no qual você pode criar uma ou mais tarefas de transformação. As seções deste tópico descrevem como obter um espaço de trabalho e como criar e iniciar um trabalho de migração nele.

Conseguir um espaço de trabalho

Para obter informações sobre como obter um espaço de trabalho, consulte [Introdução](#).

O espaço de trabalho que você usa determina Região da AWS onde você pode criar trabalhos de transformação. É Região da AWS aí que seus empregos residirão. Seus dados de descoberta e recomendações do AWS Transform também residirão nisso Região da AWS. Para criar espaços de trabalho e trabalhos em um local diferente Região da AWS, peça ao administrador que crie um espaço de trabalho diferente para você. Para obter informações sobre o suporte Regiões da AWS, consulte [Regiões aceitas](#).

Embora o Região da AWS local onde você pode criar trabalhos e armazenar dados e recomendações de descoberta seja determinado pelo administrador do AWS Transform, você pode

especificar um diferente Região da AWS como destino para a migração. Em outras palavras, você pode executar a descoberta e receber recomendações do AWS Transform em um Região da AWS, mas depois criar seu ambiente de destino em outro Região da AWS. Se você fizer isso, estará transferindo seus dados. Regiões da AWS Para obter mais informações, consulte [the section called “Conecte o alvo Conta da AWS s e regiões”](#).

Tipos de emprego

AWS O Transform oferece os seguintes tipos de trabalhos de migração que você pode escolher de acordo com suas necessidades de migração. Além dessas opções predefinidas, você pode adicionar ou remover dinamicamente qualquer etapa do seu trabalho a qualquer momento para personalizar seu fluxo de trabalho de migração.

End-to-end migração

1. Execute a descoberta
2. Crie um plano de migração
3. Conecte contas de destino
4. Construa uma landing zone
5. Migrar rede
6. Migrar servidores

Planejamento de descoberta e migração

1. Execute a descoberta
2. Crie um plano de migração

Migração de rede

1. Conecte contas de destino
2. Migrar rede

Zona de pouso

1. Conecte contas de destino
2. Construa uma landing zone

Migração de zona de aterrissagem, rede e servidor

1. Conecte contas de destino
2. Construa uma landing zone
3. Migrar rede
4. Migrar servidores

Planejamento de migração e migração de servidores

Inclui descoberta, plano de ondas e rehostedagem.

1. Execute a descoberta
2. Crie um plano de migração
3. Conecte contas de destino
4. Migrar servidores

Criando e começando um emprego

A primeira etapa de um projeto de migração é criar uma tarefa AWS Transform. Para projetos de migração, você pode escolher diferentes tipos de trabalho, dependendo de suas metas. O procedimento a seguir descreve como criar e iniciar um novo trabalho de migração de qualquer tipo. Para obter informações sobre os diferentes tipos de trabalho, consulte [the section called “Tipos de emprego”](#).

Para criar e iniciar um novo trabalho de migração

1. Na página inicial do seu espaço de trabalho, escolha Criar um trabalho.
2. Escolha a opção de migração e, em seguida, especifique o tipo de trabalho de migração que você deseja criar. Para obter informações sobre as etapas incluídas em cada um dos tipos de trabalho de migração, consulte [the section called “Tipos de emprego”](#).
3. Depois de responder a todas as perguntas do chat, escolha Criar emprego.

Baixando um relatório resumido do espaço de trabalho

Você pode gerar um relatório resumido do espaço de trabalho como um PDF para download a qualquer momento durante a migração. O relatório fornece uma visão consolidada de todas as

tarefas de migração em seu espaço de trabalho, incluindo status de tarefas e etapas atuais do fluxo de trabalho, ações e aprovações do usuário, detalhes do planejamento de ondas, topologia de migração de rede, configuração da zona de pouso, progresso da rehostedagem, decisões de containerização e principais artefatos produzidos. Para gerar um relatório, peça ao agente no chat um resumo do espaço de trabalho — por exemplo, “Dê-me um resumo do espaço de trabalho do progresso da minha migração em todos os trabalhos”. O agente compila dados de todos os trabalhos e entrega o PDF diretamente no chat como um arquivo para download. Você pode usar esse relatório para acompanhar o progresso geral da migração ou compartilhar o status com as partes interessadas.

Limitações

AWS O Transform tem as seguintes limitações:

- Se você interromper a execução de um trabalho de migração e, em seguida, solicitar que o agente o reinicie, o trabalho será reiniciado do início e você perderá qualquer progresso feito no trabalho. No entanto, os artefatos criados na tarefa antes de reiniciá-la ainda estarão disponíveis.
- Você pode especificar um destino Região da AWS por trabalho de migração. Para migrar aplicativos para diferentes regiões de destino, crie vários trabalhos de migração.
- Multi-account migração — Somente uma única região — Você pode migrar para várias contas em uma única Região da AWS. Para migrações multirregionais, você deve criar projetos separados para cada região de destino.
- Multi-account migração — Uma conta por onda — Cada onda de migração pode atingir apenas uma conta. Os aplicativos que exigem contas-alvo diferentes devem ser colocados em ondas separadas.
- Multi-account migração — AWS Organizações necessárias — Todas as contas de destino devem fazer parte de uma AWS organização.

Descubra os dados de origem

Para descobrir e coletar dados locais, você pode usar a [ferramenta de descoberta AWS Transform](#), o coletor AWS Migration Evaluator ou fazer upload de exportações do RVTools e do ModelizeIt, bem como exportações no formato AWS Migration Portfolio Assessment (MPA) geradas por ferramentas como o Cloudamize. AWS O Transform pode processar as exportações da ferramenta de descoberta AWS Transform como arquivos CSV e JSON em um formato de arquivo ZIP, as exportações do RVTools como um arquivo Excel ou um arquivo ZIP contendo arquivos CSV e as exportações CSV

do Modelizelt em um arquivo ZIP. Para cada fonte de dados, o AWS Transform aceita o arquivo do servidor primário individualmente. No entanto, arquivos suplementares, como conexões, só serão processados quando incluídos em um arquivo ZIP com os arquivos do servidor ou em um arquivo do Excel com a planilha do servidor.

Recomendamos que você faça o upload dos dados mais detalhados disponíveis e revise seus arquivos de exportação antes de fazer o upload para garantir a integridade e a precisão dos dados. Verifique se todos os arquivos necessários estão incluídos no upload e confirme se os dados refletem o estado atual do seu ambiente. Essa análise preliminar ajuda a minimizar a necessidade de recarregamentos e garante que o AWS Transform possa capturar com mais precisão seu ambiente local e oferecer melhor suporte ao planejamento de migração, incluindo agrupamento de aplicativos e planejamento de ondas. Você também pode adicionar dados de forma incremental à medida que obtém dados melhores.

AWS O Transform detecta automaticamente o formato e a estrutura do arquivo, analisa e extrai registros estruturados de entidades, remove duplicatas em vários arquivos, valida a qualidade dos dados e relata problemas e, em seguida, prepara um resumo pronto para o planejamento da migração posterior.

Depois de compartilhar e confirmar seus dados locais, você pode revisar os dados de descoberta expandindo Discover on-premises data no Job Plan e escolhendo Resumo da disponibilidade do inventário. Você também pode fazer perguntas sobre os dados que você enviou para verificar se o AWS Transform ingeriu tudo corretamente ou para identificar e corrigir quaisquer erros no processamento de dados. Por exemplo, você pode perguntar sobre o sistema operacional e as versões. Se precisar corrigir erros, você pode recarregar seus dados de inventário a partir da ferramenta de descoberta que você usou, e o AWS Transform processará, deduplicará e mesclará automaticamente os registros atualizados. Você também pode remover um arquivo carregado anteriormente se não quiser mais usar esses dados de inventário.

Crie um plano de migração

A etapa do trabalho de planejamento da migração no AWS Transform for VMware é uma experiência colaborativa baseada em bate-papo para planejar grandes migrações. AWS Os agentes de transformação aplicam a orientação AWS prescritiva para orientar os clientes desde a análise de dados locais até os planos finalizados da onda de migração.

Depois que o trabalho de dados locais do Discover for concluído com êxito, o AWS Transform usa os dados de descoberta para agrupar aplicativos em ondas de migração. AWS O Transform orienta você nas etapas para analisar e definir o escopo de seus servidores, agrupá-los em aplicativos, gerar

grupos de movimentação e criar ondas de migração. Ao analisar seu ambiente local, você pode fazer perguntas para entender melhor como o AWS Transform analisou seu software instalado, por exemplo, dependências de servidor e arquitetura de rede.

AWS O Transform suporta ajustes de escopo em grupos e ondas de aplicativos. Você pode recarregar os dados de descoberta a qualquer momento, e o AWS Transform processará, desduplicará e mesclará automaticamente novos registros com os dados existentes. Quando mudanças são detectadas, como dependências recém-descobertas ou adições de infraestrutura, o AWS Transform sinalizará os grupos de dependências afetados e fornecerá recomendações para ajustes no plano de ondas. O planejamento da migração também pode usar dados de texto não estruturados para enriquecer o processo de planejamento.

Há quatro estágios de planejamento da migração:

- Em Escopo e análise, você pode revisar seus dados de descoberta, fazer perguntas sobre seu ambiente de software e rede e determinar os recursos no escopo da migração.
- Nos aplicativos de grupo, você pode fornecer uma combinação de regras comerciais e técnicas relacionadas, por exemplo, à análise de nomes de host, dependências de rede e regras de negócios, para que o planejamento da migração possa agrupar sua infraestrutura em aplicativos. Se você já tem um inventário de seus aplicativos, o planejamento de migração pode usá-lo em vez disso.
- Em Gerar grupos de movimentação, você pode fornecer ao planejamento de migração seus requisitos técnicos e comerciais para que ele possa determinar quais aplicativos devem ser movidos juntos. As dependências técnicas incluem bancos de dados, filas de mensagens ou outros recursos compartilhados entre vários aplicativos. As dependências comerciais e operacionais incluem importância comercial, RPO e RTO, localização do data center e proprietários de aplicativos.
- Por fim, em Build waves, você pode fornecer um contexto de planejamento de migração sobre seus cronogramas e prioridades para que ele possa criar um plano de ondas que você possa migrar. Você pode selecionar grupos de movimentação para inclusão em uma onda com base em fatores como pontuação de prioridade, tamanho do grupo de movimentação, contagem de usuários e complexidade do aplicativo.

Terminologia de planejamento de migração:

- As ondas de migração são grupos lógicos que são migrados juntos. As ondas de migração são compostas por um ou mais grupos de movimento.

- Um grupo de movimentação é um conjunto de aplicativos codependentes que devem ser movidos juntos. Eles podem ter dependências técnicas, como um banco de dados compartilhado, ou dependências comerciais, como suporte a uma função comercial compartilhada.
- Uma dependência é uma relação entre sistemas. Há vários tipos de dependências, incluindo:
 - Dependências críticas ou difíceis, nas quais os sistemas não podem operar sem a dependência. Exemplos comuns disso são aplicativos que dependem de bancos de dados, outros aplicativos ou serviços.
 - Dependências flexíveis, que não são críticas para a operação do sistema. Exemplos comuns disso incluem dependências insensíveis à latência que podem ser migradas de forma independente.
 - Non-technical as dependências incluem dependências comerciais, organizacionais, operacionais e de conformidade. Essas são dependências relacionadas à sua organização e suas prioridades. Exemplos disso incluem função comercial compartilhada e propriedade organizacional.

Fluxo de trabalho

O planejamento da migração é um fluxo de trabalho interativo e iterativo. Você pode voltar e fazer alterações nas etapas anteriores a qualquer momento. Um fluxo de trabalho típico de planejamento de migração é:

1. O planejamento da migração começa resumindo os dados de descoberta que estão disponíveis. Analise os dados disponíveis e retorne à etapa de descoberta a qualquer momento para fornecer dados adicionais.
2. Na etapa de escopo e análise, você pode fazer perguntas sobre seu ambiente local para validar os dados coletados. Exemplos de perguntas incluem:
 - a. Listar meus servidores por sistema operacional
 - b. Resumir minha topologia de rede local
 - c. Listar as tecnologias mais comuns em execução no meu ambiente.
3. Ao analisar seu ambiente, se você identificar servidores que não deveriam estar no escopo da migração, você pode pedir ao AWS Transform que exclua esses recursos. Exemplos incluem:
 - a. Remova todos os servidores que têm um legado em seu nome de host
 - b. Remova todos os servidores na versão 10.0.2. 0/24 sub-rede
 - c. Remova todos os servidores que executam versões do Windows anteriores a 2022

4. Depois de explorar suficientemente seu ambiente e determinar seu escopo de migração, você pode pedir ao AWS Transform que passe para a próxima etapa de planejamento da migração.
5. A próxima etapa é o agrupamento de aplicativos. Se você já tem seus servidores mapeados para aplicativos, você pode dizer ao AWS Transform para usar esse mapeamento e pular esta etapa. Se você não tiver seus aplicativos predefinidos, poderá fornecer a lógica técnica e comercial que define seus aplicativos. O AWS Transform o guiará pelo processo de agrupamento de aplicativos e sugerirá os pontos de dados que você pode fornecer para agrupar efetivamente seus servidores em aplicativos. Quanto mais informações você puder fornecer sobre seus aplicativos locais, mais eficientemente o AWS Transform poderá agrupar seus servidores em aplicativos. Depois de fornecer informações suficientes, você poderá instruir o AWS Transform a realizar o agrupamento de aplicativos.
6. Depois que o agrupamento de aplicativos for realizado, revise os grupos de aplicativos. Você pode instruir o AWS Transform a fazer as alterações necessárias, por exemplo:
 - a. Mova o servidor exemplo-servidor para o aplicativo-5
 - b. Renomear o aplicativo-5 para “Ambiente de teste de aplicativos de RH”
 - c. Remova todos os servidores Linux do IIS Dev Farm
7. Depois que seus aplicativos estiverem agrupados, instrua o AWS Transform a passar para a próxima etapa
8. A próxima etapa é mover o agrupamento. Na etapa de agrupamento de movimentação, você identifica os aplicativos que devem ser movidos juntos. Forneça contexto sobre suas dependências técnicas e não técnicas. O AWS Transform guiará você pelo processo e sugerirá pontos de dados que você pode fornecer para agrupar seus aplicativos. Há várias considerações a serem feitas nesse estágio, incluindo:
 - a. Qual deve ser o tamanho alvo do grupo de movimentação?
 - b. Você quer combinar ambientes, por exemplo, desenvolvimento, teste e produção, para cada aplicativo ou dividi-los?
 - c. Como você deseja considerar as dependências de rede? Todas as dependências são críticas ou algumas dependências podem ser consideradas dependências flexíveis e divididas entre grupos de movimentação?
9. Depois de fornecer suas regras para o agrupamento de movimentos, instrua o AWS Transform a executar sua estratégia de agrupamento de movimentos. Em seguida, você pode revisar e modificar seus grupos de movimentação. Depois de analisar seus grupos de mudança, você pode instruir o AWS Transform a passar para a etapa final de planejamento da migração.

- 10.O planejamento de ondas é a etapa final do planejamento da migração. Nesta etapa, você agrupa seus grupos de mudança em ondas de migração e prioriza essas ondas. Na etapa de planejamento de ondas, o AWS Transform orientará você a fornecer a priorização de negócios necessária para agrupar seus grupos de mudança em ondas e, em seguida, priorizar essas ondas. As considerações no planejamento de ondas incluem:
- a. A importância comercial de cada um dos seus grupos de mudança
 - b. Os cronogramas de migração e os cronogramas de cada grupo de mudança
 - c. Os riscos associados a cada grupo de movimento
 - d. O número de servidores a serem migrados por onda
- 11.Depois de fornecer orientação suficiente sobre como se agrupar em ondas, instrua o AWS Transform a executar o planejamento das ondas. Você pode então revisar suas ondas e modificá-las.
- 12.Depois de finalizar seu plano de ondas, você pode concluir o planejamento da migração e passar para a execução. Você pode retornar ao planejamento da migração a qualquer momento para refinar e iterar seu plano.
- 13Para cada onda, você pode atribuir uma estratégia de migração: rehostedar (migrar servidores para o Amazon EC2) e containerizar (containerizar o código-fonte e implantar no Amazon Elastic Container Service ou no Amazon Elastic Kubernetes Service). Quando você atribui a uma onda a estratégia containerize, o AWS Transform executa o fluxo de trabalho de containerização do código-fonte dessa onda durante a execução da migração. Para obter mais informações, consulte [Containerização do código-fonte](#). Para obter estratégias AWS recomendadas em toda a estrutura 7Rs antes de atribuí-las, consulte [the section called “Recomendações 7Rs”](#)

Recomendações de estratégia de migração (7Rs)

Durante o planejamento da migração, a AWS Transform pode analisar seu inventário descoberto e recomendar uma estratégia de migração — uma das 7Rs padrão do setor — para cada servidor e aplicativo. Cada recomendação inclui um serviço AWS alvo sugerido, uma pontuação de confiança e o raciocínio por trás disso. Isso fornece um ponto de partida defensável para seu plano de ondas e apresenta oportunidades de modernização que, de outra forma, você poderia perder.

As sete estratégias são rehostedar, reformatar, refatorar, recomprar, aposentar, reter e realocar. AWS Transform analisa seus dados, como sistema operacional, utilização e tipo de carga de trabalho, para fazer recomendações explicáveis. Por exemplo, pode recomendar a desativação de servidores ociosos ou em fim de vida útil, a migração do SQL Server ou bancos

de dados de código aberto para o Amazon RDS, a transferência de cargas de trabalho de e-mail e colaboração para o Microsoft 365, a manutenção de sistemas legados especializados e a rehostagem das cargas de trabalho restantes no Amazon EC2. As recomendações abrangem desde servidores individuais até aplicativos e em todo o seu portfólio, com uma visão crítica por estratégia e resumos em nível de onda.

Para gerar um relatório de estratégia de migração (7Rs):

1. Conclua a etapa de descoberta de dados locais e agrupe seus servidores em aplicativos. Ambos são necessários para que o AWS Transform possa fornecer recomendações por servidor e por aplicativo.
2. No chat de planejamento de migração, peça ao AWS Transform um relatório de estratégia de migração (7Rs), por exemplo, Gerar um relatório. R-strategy Após a conclusão do agrupamento de aplicativos, o AWS Transform também se oferece para gerar o relatório para você.
3. AWS O Transform analisa seu inventário, aplica a estrutura 7Rs e gera o relatório. Você pode fornecer detalhes como o nome da sua organização e quaisquer filtros para definir o escopo da análise.
4. Revise as recomendações. Para ajustar uma recomendação, diga ao AWS Transform in the chat: altere um único servidor ou aplicativo ou aplique uma alteração em massa (por exemplo, por sistema operacional, ambiente, onda ou prioridade). AWS O Transform atualiza o relatório com suas alterações.

Por padrão, o AWS Transform produz um painel HTML interativo que você pode filtrar e explorar. Mediante solicitação, você também pode gerar um documento PDF para compartilhar com as partes interessadas ou um conjunto de slides da Microsoft PowerPoint (PPTX) para apresentar; o PDF e as PowerPoint saídas são instantâneos pontuais da mesma análise. O relatório inclui uma estratégia recomendada e um serviço AWS alvo para cada servidor e aplicativo, pontuações de confiança e raciocínio, oportunidades de modernização destacadas, uma visão crítica por estratégia, resumos em nível de onda e indicadores de risco.

A estratégia recomendada neste relatório complementa a estratégia por onda que você atribui durante o planejamento da onda. Para a containerização do código-fonte, consulte. [Containerização do código-fonte](#)

Diagramação e geração de relatórios

Durante o planejamento da migração, o AWS Transform transforma o inventário descoberto e os resultados do planejamento em diagramas visuais e relatórios analíticos. Você os gera conversacionalmente no bate-papo de planejamento — por exemplo, “Mostre-me um diagrama de topologia de rede” ou “Gere um relatório de risco”. AWS O Transform os cria a partir dos dados que você já forneceu, sem necessidade de configuração.

Os diagramas são interativos e permitem que você explore seu ambiente visualmente. Os diagramas disponíveis incluem:

- Topologia de rede — Um mapa interativo de seus servidores e seus relacionamentos de rede, projetado para escalar para grandes ambientes de milhares de nós.
- Dependência de aplicativos — relacionamentos direcionados entre aplicativos derivados de suas conexões de rede observadas.
- Gráfico de Gantt do Wave — Uma visão cronológica de suas ondas de migração mostrando cronogramas, dependências, marcos e progresso (disponível após o planejamento da onda).
- Gráficos gerais — gráficos circulares, gráficos de barras, histogramas, mapas de árvores e tabelas de resumo sobre as dimensões dos dados que você escolher.

Os relatórios fornecem análises narrativas e recomendações sobre seus dados de migração. Os relatórios disponíveis incluem:

- Avaliação de risco — avalia cada aplicativo em termos de complexidade técnica, risco de dependência, prontidão para migração e risco operacional, com resumos por aplicativo, por onda e em todo o portfólio.
- Estratégia de migração (7Rs) — Per-server e recomendações de estratégia por aplicativo. Para obter mais informações, consulte [the section called “Recomendações 7Rs”](#).
- Relatórios gerais e personalizados — relatórios analíticos para solicitações, como resumos de prontidão executiva, compensações entre custo e risco e avaliações de candidatos à containerização.

Alguns resultados dependem de até que ponto você está planejando. Por exemplo, os diagramas de dependência de aplicativos usam seus dados de conexão de rede. O gráfico de Gantt da onda e os resumos dos relatórios em nível de onda ficam disponíveis após a conclusão do planejamento

da onda. Se faltar um pré-requisito, o AWS Transform informa o que é necessário e pode executar a etapa necessária primeiro.

AWS O Transform fornece diagramas como HTML interativo que você pode filtrar e explorar. Por padrão, o AWS Transform entrega relatórios como um arquivo HTML independente. Mediante solicitação, o AWS Transform também pode gerar um documento PDF para compartilhar com as partes interessadas ou um conjunto de slides da Microsoft PowerPoint (PPTX) para apresentar. O PDF e PowerPoint as saídas são instantâneos pontuais da mesma análise.

Conecte o alvo Conta da AWS s e regiões

Configure seu Conta da AWS conector de destino para migração de rede, criação de landing zone e migração de servidor. Isso envolve três etapas: selecione seu tipo de migração, forneça os detalhes do contrato MAP (se aplicável) e configure o conector. Essas configurações se aplicam a todos os estágios de migração: migração de rede, landing zone e rehostedagem do servidor.

Etapa 1: Seleção do tipo de migração

Escolha se você está realizando uma migração de conta única ou de várias contas:

- Single-account migração — todas as cargas de trabalho migram para um destino. Conta da AWS A conta de destino do conector e a conta de destino são iguais.
- Multi-account migração — As cargas de trabalho migram para diferentes contas de destino. O conector deve estar conectado à conta de gerenciamento da organização ou a uma conta de Administrador Delegado (DA) registrada para AWS Transform MGN e CloudFormation StackSets

Etapa 2: contrato MAP

Se sua migração fizer parte do AWS Migration Acceleration Program (MAP 2.0), forneça sua ID do Migration Portfolio Experience (MPE) — um código de 10 caracteres usando letras maiúsculas e dígitos (por exemplo, ABCDE12345). Quando você fornece seu MPE ID, a tag MAP é aplicada a todos os recursos criados nos estágios de migração de rede, landing zone e rehostedagem do servidor. O formato da tag é:

- Key (Chave): map-migrated Value (Valor): migMPE_ID

Você deve aplicar as tags MAP para receber crédito MAP. Para obter mais informações sobre o MAP, consulte [AWS Migration Acceleration Program](#).

Etapa 3: configuração do conector

Você usa o conector da conta de destino para conectar sua tarefa de migração ao AWS ambiente em que suas cargas de trabalho residirão após a migração. Antes de começar, verifique se seu destino Conta da AWS tem as permissões, cotas e configurações necessárias para dar suporte à sua infraestrutura migrada.

Ao aprovar a solicitação do conector, você concede permissões de AWS transformação para:

- Gerencie as operações de bucket do Amazon S3 (read/write) para migração do VMware, junto com o acesso ao Migration Hub e ao AWS Application Migration Service (MGN). Isso inclui permissões para os seguintes itens, todos restritos aos recursos da conta de destino que estão marcados com `CreatedBy:AWSTransform` ou `CreatedFor:AWSTransform`:
 - Gerencie as ondas de migração.
 - Gerencie configurações de rede (Amazon EC2, VPC, Transit Gateway, Direct Connect, Load Balancers, Network Firewall).
 - Gerencie implantações CloudFormation de pilhas.
 - Execute instalações automatizadas de agentes por meio do Systems Manager.
- Migre suas cargas de trabalho locais para o destino Conta da AWS e a região usando as informações armazenadas na região de descoberta.
- Provisione e gerencie a infraestrutura da landing zone no destino Conta da AWS e na região. Isso inclui permissões para os seguintes itens, restritos aos recursos marcados com, `CreatedBy:AWSTransform` quando aplicável:
 - Execute operações de bucket do Amazon S3 (criar, ler, gravar, excluir) para buckets que começam com `transform-vmware-landing-zone-`
 - Gerencie implantações de CloudFormation pilhas e conjuntos de alterações para pilhas de landing zone.
 - Execute as operações da AWS Control Tower. Você pode gerenciar zonas de pouso, ativar linhas de base e ativar controles.
 - Gerenciar AWS organizações. Você pode criar e gerenciar unidades organizacionais, criar contas e mover contas.
 - Gerencie políticas de controle de serviço (SCPs) por meio da AWS Control Tower.
 - Gerencie AWS artefatos de provisionamento do Service Catalog.

 Note

Os tipos de conectores podem ser atualizados quando novos recursos exigem alterações de permissão. A versão atual do tipo de conector da conta de destino é 2.0. Quando você cria um novo conector, ele usa a versão mais recente.

Antes de configurar o conector, entenda as funções da conta envolvidas na sua migração:

Conta	Description
AWS Transformar conta	Qualquer conta de membro em sua AWS organização em que você configurou o AWS Transform. É aqui que seu espaço de trabalho do AWS Transform é executado. Não precisa ser a conta de gerenciamento.
Conta de destino do conector	A conta para a qual seu conector AWS Transform está configurado. Isso depende do seu tipo de migração: • Single-account migração — Conecte-se à conta para a qual você está migrando cargas de trabalho. A conta de destino do conector e a conta de destino são iguais. • Multi-account migração — Conecte-se à conta de gerenciamento da organização ou a uma conta de Administrador Delegado (DA). A conta DA deve ser registrada como administrador delegado tanto para a MGN quanto para a sua CloudFormation StackSets AWS organização. AWS O Transform verifica se a conta conectada é a conta de gerenciamento ou uma conta DA e ajusta seu comportamento de acordo.
Conta de destino	O Conta da AWS local para onde suas cargas de trabalho são migradas. Em uma migração de conta única, isso é o mesmo que a conta de destino do conector. Em uma migração de várias contas, essas são as contas individuais dos membros que recebem as cargas de trabalho migradas.

Usando uma conta de administrador delegado

Para migrações de várias contas, AWS recomenda que você use uma conta de Administrador Delegado (DA) em vez da conta de gerenciamento da organização diretamente. Uma conta DA segue o princípio do menor privilégio ao limitar o escopo das permissões necessárias para as operações de migração. A conta DA deve ser registrada como administrador delegado tanto para a MGN quanto para a sua CloudFormation StackSets AWS organização.

A principal diferença entre as duas opções é:

- Conta de gerenciamento — Pode permitir acesso confiável para a MGN e para CloudFormation StackSets toda a organização. AWS Transforme as CloudFormation StackSets APIs de chamadas com `CallAs: SELF`.
- Conta de administrador delegado — Não é possível habilitar o acesso confiável diretamente (isso deve ser feito a partir da conta de gerenciamento), mas pode gerenciar servidores de origem da MGN, iniciar instâncias e implantar CloudFormation StackSets em todas as contas dos membros. AWS Transforme as CloudFormation StackSets APIs de chamadas com `CallAs: DELEGATED_ADMIN`.

Para obter mais informações, consulte [Administrador delegado do MGN](#) no Guia do usuário do MGN.

Funções do IAM criadas durante a configuração do conector

Durante a configuração do conector, o AWS Transform cria a seguinte função do IAM em sua conta de destino:

- `AWSTransform-Connector-role` — Criado quando você configura o conector da conta de destino, na conta de gerenciamento ou na conta de administrador delegado da sua AWS organização. Essa função permite que o AWS Transform se conecte à sua conta de destino e aja em seu nome para executar operações de migração.

Configuração do conector da conta de destino

Important

Durante a configuração do conector, um bucket Amazon S3 é criado em seu destino. Conta da AWS Esse bucket não aplicará HTTPS-only access (SecureTransport) por padrão. Se você quiser que a política de bucket inclua transporte seguro, você mesmo deverá atualizar

a política. Para obter mais informações, consulte [Melhores práticas de segurança para o Amazon S3](#).

Para usar um conector de conta de destino existente

1. No painel Job Plan, expanda Escolher conta de destino e, em seguida, escolha Criar ou selecionar conectores.
2. Na guia Colaboração, selecione um conector existente e escolha Usar conector. Se um conector não estiver disponível, sua versão não é compatível com o tipo de tarefa que você selecionou.

 Important

Se você especificar um conector com um destino Região da AWS diferente da região de AWS transformação, o AWS Transform transferirá seus dados Regiões da AWS.

3. Escolha Continuar.

Para criar um novo conector

1. No painel Job Plan, expanda Connect target account e escolha Create ou select connectors.
2. Especifique Conta da AWS e Região da AWS para seu alvo e escolha Avançar.

 Important

Se o alvo Região da AWS for diferente da descoberta Região da AWS, o AWS Transform transferirá seus dados Regiões da AWS.

3. Escolha se deseja usar as chaves gerenciadas do Amazon S3 para criptografia. Se você especificar sua própria chave KMS, poderá usar a política de chaves padrão ou uma menos permissiva. Para obter informações sobre como criar e configurar uma chave KMS, consulte [Criar uma chave KMS](#) no Guia do desenvolvedor do AWS Key Management Service .

AWS O Transform usa a `kms:DescribeKey` permissão para verificar se a chave existe e `kms:Decrypt` para criptografar `kms:GenerateDataKey` e descriptografar os dados do trabalho no bucket do Amazon S3. Para obter mais informações, consulte [Redução do custo SSE-KMS com as chaves de bucket do Amazon S3](#).

4. Escolha Continuar.

5. Copie o link de verificação, compartilhe-o com um administrador do alvo Conta da AWS e peça que ele aprove a solicitação de conexão.
6. Depois que o administrador aprovar a solicitação, selecione o conector recém-criado na lista e escolha Usar conector.
7. Escolha Enviar para AWS transformar.

Se você planeja modificar o AWS Transform MGN modelo para permitir ações pós-lançamento, adicione a seguinte permissão à função do conector de destino. Essa declaração de política JSON concede a `iam:PassRole` permissão para a função de ações pós-lançamento. Você pode encontrar o nome da função na guia Colaboração após a criação do conector. Para obter informações sobre como adicionar permissões a uma função, consulte [Atualizar permissões para uma função](#) no Guia do usuário do IAM.

```
{
  "Sid": "MGNPostLaunchActions",
  "Effect": "Allow",
  "Action": [
    "iam:PassRole"
  ],
  "Resource": "arn:aws:iam::target-account-ID:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
}
```

Regiões-alvo suportadas

Uma região de destino de migração é Região da AWS onde os recursos migrados são implantados, incluindo zonas de aterrissagem, infraestrutura de rede e rehostedagem de servidores. Ao criar o conector, especifique um destino Região da AWS. Você pode usar qualquer um dos seguintes Regiões da AWS:

- Leste dos EUA (Norte da Virgínia)
- Leste dos EUA (Ohio)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)
- África (Cidade do Cabo)
- Ásia Pacífico (Hong Kong)
- Ásia-Pacífico (Taipei)

- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Hyderabad)
- Ásia-Pacífico (Tóquio)
- Ásia-Pacífico (Seul)
- Asia Pacific (Osaka)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Melbourne)
- Ásia-Pacífico (Malásia)
- Ásia-Pacífico (Nova Zelândia)
- Ásia-Pacífico (Tailândia)
- Canadá (Central)
- Oeste do Canadá (Calgary)
- Europa (Frankfurt)
- Europa (Zurique)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Paris)
- Europa (Estocolmo)
- Europa (Milão)
- Europa (Espanha)
- Israel (Tel Aviv)
- México (Centro)
- América do Sul (São Paulo)

 Important

Se você especificar um destino Região da AWS diferente do AWS Transform Região da AWS, alguns dos seus dados serão transferidos Regiões da AWS.

Observe que os dados de replicação do servidor vão diretamente do ambiente de origem para a conta e região de destino.

Construa uma landing zone

AWS O Transform orienta você no projeto e na implantação de um AWS landing zone como parte do seu projeto de migração. Uma landing zone é um AWS ambiente de várias contas que serve como base para suas cargas de trabalho com limites organizacionais, controles de governança e estrutura de contas estabelecidos antes que qualquer carga de trabalho chegue. AWS O Transform analisa seu inventário de migração e os requisitos de negócios para recomendar uma unidade organizacional (OU) e uma estrutura de contas, aplicar políticas de controle de serviços (SCPs) recomendadas e gerar a and/or implantação da infraestrutura como código (IaC).

O agente do landing zone orienta você em duas fases:

- Configuração da base — Estabeleça a estrutura principal da landing zone: AWS Control Tower, OUs fundamentais e contas principais.
- Design da conta de carga de trabalho — Projete e crie OUs e contas de carga de trabalho com base em suas ondas de migração, unidades de negócios e requisitos de separação de ambientes.

AWS O Transform suporta ambientes novos (sem landing zone existente) e ambientes abandonados (OUs existentes e contas já implantadas). Em cenários abandonados, o AWS Transform detecta sua estrutura organizacional existente e recomenda somente as mudanças necessárias para preencher as lacunas em relação AWS às melhores práticas.

Configuração do conector

O agente da landing zone requer um Conta da AWS conector de destino para provisionar recursos na conta de gerenciamento da sua organização. O conector tem permissões para:

- Configurar a [AWS Control Tower](#)
- Crie [unidades organizacionais e contas](#)
- Configurar [políticas de controle de serviço \(SCPs\)](#)

Ao aprovar a solicitação do conector, você concede permissões de AWS transformação para:

- Provisione e gerencie a infraestrutura da landing zone no destino Conta da AWS e na região. Isso inclui permissões para os seguintes itens, restritos aos recursos marcados com `CreatedBy:AWSTransform` e por, `ATWorkspace:{workspace-id}` quando aplicável:
 - Operações de bucket do S3 (criar, ler, gravar, excluir) para buckets começando com `transform-vmware-landing-zone-`
 - CloudFormation implantações de pilhas e gerenciamento de conjuntos de alterações para pilhas de landing zone
 - AWS Operações da Control Tower (gerenciamento de zonas de pouso, habilitação de linhas de base e controles)
 - AWS Gerenciamento de [organizações](#) (criação e gerenciamento de unidades organizacionais, criação de contas e movimentação de contas)
 - Gerenciamento da política de controle de serviços (SCP) via AWS Control Tower
 - [AWS Gerenciamento de artefatos de provisionamento do Service Catalog](#)

Ao criar o conector, você especifica um destino Região da AWS. Essa região deve ser igual à região da Control Tower de sua casa. Para obter mais informações sobre as regiões da Control Tower, consulte [Como Regiões da AWS trabalhar com a AWS Control Tower](#).

No início da configuração da landing zone, o AWS Transform recupera a configuração do conector e apresenta o ID da conta de gerenciamento AWS da organização e a região de destino para confirmação. Para obter mais informações, consulte [Conectores](#).

Important

Dependência da região do IAM Identity Center — O AWS Transform requer o AWS IAM Identity Center (IAM Identity Center), o que significa que a região do conector deve corresponder tanto à região de origem da AWS Control Tower quanto à região do IAM Identity Center. Se o IAM Identity Center já estiver configurado em sua organização, a inicialização do AWS Control Tower falhará se o conector for direcionado a uma região diferente. Para obter mais informações, consulte [Considerações para clientes do IAM Identity Center](#) no Guia do usuário do AWS Control Tower.

Configuração da fundação

A fase de configuração da fundação estabelece a infraestrutura central da landing zone usando a [AWS Control Tower](#). Quando a AWS Control Tower configura uma landing zone, ela provisiona automaticamente um conjunto de recursos gerenciados em sua conta de gerenciamento que formam a base de governança para toda a sua AWS organização:

- Root — O pai de nível superior que contém todas as OUs em sua landing zone.
- OU de segurança — criada automaticamente pela Control Tower. Contém duas contas compartilhadas: a conta Log Archive (registro centralizado e imutável de todas as atividades de AWS API e alterações de recursos em sua organização) e a conta Audit (acesso somente leitura a todas as contas para análise de segurança e conformidade). Essas contas não podem ser renomeadas nem substituídas após a configuração inicial.
- Controles obrigatórios (grades de proteção) — A Control Tower aplica automaticamente controles preventivos e de detetive em toda a organização para aplicar políticas básicas de governança. Eles não podem ser desativados.
- Diretório do IAM Identity Center — O Control Tower cria um diretório nativo da nuvem com grupos pré-configurados e acesso de login único para os usuários da landing zone. Para obter mais informações, consulte [AWS IAM Identity Center](#).

A Control Tower usa [CloudFormation StackSets](#) para implantar e gerenciar esses recursos de forma consistente em todas as contas e regiões da sua organização. Você não deve modificar ou excluir recursos gerenciados da Control Tower fora dos métodos suportados, pois isso pode fazer com que sua landing zone entre em um estado desconhecido.

Convenção de e-mail da conta

AWS requer um endereço de e-mail exclusivo para cada conta. Esses e-mails recebem notificações importantes para a conta. AWS O Transform usa mais endereçamento para gerar e-mails de conta exclusivos a partir de uma única caixa de correio.

Formato: `prefix+account-name@domain`.

Você fornece um prefixo (por exemplo, `aws-admin`) e um domínio (por exemplo, `acme.com`), e o AWS Transform obtém todos os e-mails da conta automaticamente. Por exemplo:

- Conta de auditoria: `aws-admin+audit@acme.com`

- Conta do Log Archive: `aws-admin+log-archive@acme.com`
- Conta Sandbox: `aws-admin+sandbox@acme.com`

Em cenários abandonados, o AWS Transform inspeciona os e-mails existentes da conta para inferir a convenção de endereçamento adicional já em uso e oferece a possibilidade de continuar com o mesmo padrão.

Estrutura de fundação recomendada

Com base nas AWS melhores práticas, a AWS Transform recomenda a seguinte estrutura básica de OU. Você pode personalizá-lo antes da criação.

UO	Finalidade	Contas
Segurança	Registro e monitoramento de auditoria centralizados. O isolamento desses serviços em contas dedicadas foi projetado para ajudar a manter sua trilha de auditoria separada das equipes de carga de trabalho.	Auditoria, arquivamento de registros
Infraestrutura	Rede compartilhada (Transit Gateway, VPN), DNS e serviços comuns. É recomendável centralizá-los para ajudar a reduzir a duplicação e dar à sua equipe de rede um único local para gerenciar a conectividade.	Nenhum (criado vazio)
Sandbox	Experimentação para desenvolvedores com limites de gastos e acesso restrito. Recomenda-se para dar aos desenvolvedores um espaço para experimentar sem arriscar os recursos de produção.	Sandbox
Workloads	Contém produção e Non-Production, opcionalmente, sub-OU's regulamentados. As contas de carga de trabalho são projetadas na próxima fase com base em seus requisitos de migração.	Nenhum (criado vazio)

 Note

A OU de segurança com [contas de Audit e Log Archive](#) é criada como parte da configuração básica da Control Tower. As OUs de infraestrutura, sandbox e cargas de trabalho são criadas separadamente após a confirmação da estrutura.

Em cenários abandonados, o AWS Transform compara sua base existente com essa estrutura recomendada e relata apenas as lacunas. Por exemplo: “Sua fundação tem OUs de segurança e infraestrutura, mas nenhuma unidade organizacional de sandbox”.

Políticas de controle de serviço (SCPs)

Os SCPs são [barreiras de permissão em nível organizacional](#) que definem o máximo de permissões para todas as contas em sua organização. AWS Eles não concedem acesso. Em vez disso, eles definem limites que ninguém na conta pode ultrapassar, nem mesmo os administradores da conta.

Como parte da implantação da Control Tower, as grades de proteção básicas são aplicadas automaticamente. AWS A Transform também recomenda SCPs adicionais projetados para ajudar a fortalecer a postura da sua organização. Eles são baseados nas AWS melhores práticas para uma zona de pouso mínima viável.

Os SCPs podem ser aplicados às OUs de infraestrutura, sandbox e cargas de trabalho. A OU de segurança é gerenciada pela Control Tower e não pode ser alvo de SCPs por meio dessa ferramenta.

 Important

A Security OU é uma OU básica gerenciada pela Control Tower. Você não pode adicionar contas, SCPs ou quaisquer recursos a ele por meio do agente landing zone.

Em cenários abandonados, o AWS Transform verifica quais SCPs já foram aplicados e recomenda apenas aqueles que preencheriam lacunas.

Implantação da Fundação

Depois que o design da base estiver concluído, você escolhe como implantar:

- Implante para mim — O AWS Transform implanta as OUs, contas e SCPs básicos em sua AWS organização.
- Vou implantar sozinho — o AWS Transform gera artefatos de infraestrutura como código (IaC) para download em seu formato preferido (consulte [the section called “Formatos IaC”](#)).
- Projete contas de carga de trabalho primeiro — ignore a implantação e continue com a fase de design da conta de carga de trabalho. Você pode implantar tudo junto mais tarde.

Inicialização da Control Tower

Se o AWS Transform detectar que o AWS Control Tower ainda não foi inicializado em sua organização, ele fornecerá ao usuário um link para a página do console do AWS Transform. A geração da operação no link criará uma CloudFormation pilha para inicializar o Control Tower. O processo criará essa pilha no CloudFormation console para sua região de destino. Depois que a criação da pilha for concluída, o AWS Transform continua com a implantação.

Design da conta de carga de trabalho

Na fase de design da conta de carga de trabalho, o AWS Transform projeta a OU e a estrutura de contas para suas cargas de trabalho de aplicativos com base em seu inventário de migração, requisitos de negócios e preferências de separação de ambientes.

Contexto de planejamento de migração

AWS O Transform recupera dados de sua fase de planejamento de migração, incluindo planos de ondas, mapeamentos de servidor para aplicativo e contexto compartilhado. Se os dados de planejamento de migração estiverem disponíveis, o AWS Transform exibirá um resumo e solicitará que você o confirme ou ajuste. Se nenhum dado de planejamento de migração estiver disponível, o AWS Transform fará perguntas de descoberta diretamente.

Descoberta

AWS O Transform faz perguntas para entender seus requisitos de carga de trabalho. Você pode pular qualquer pergunta. Os tópicos incluem:

- Número de unidades de negócios ou equipes usando AWS
- Setor e qualquer estrutura aplicável (HIPAA, SOC2 PCI-DSS, FedRAMP)
- Se as cargas de trabalho lidam com dados confidenciais (PII, PHI, financeiros)

- Preferências de separação de ambiente (dev/test/staging/prod como contas separadas ou compartilhadas)
- Requisitos de isolamento da carga de trabalho
- Aplicativos de negócios e suas finalidades
- Agrupamento de servidores em aplicativos
- Necessidades de rastreamento e alocação de custos (por unidade de negócios, projeto, ambiente)
- Crescimento esperado nos próximos 12 a 24 meses
- Preferência de estratégia de conta (aplicativo único por conta, agrupado ou baseado no ambiente)

Estrutura de carga de trabalho proposta

Com base em suas respostas e dados de planejamento de migração, o AWS Transform propõe uma OU e uma estrutura de contas sob a OU Workloads. A proposta inclui o raciocínio por trás de cada decisão de design.

AWS O Transform segue esses princípios de design:

- Todos os servidores em uma onda de migração vão para a mesma conta — as ondas não podem ser divididas entre contas. Essa é uma limitação de rehosting durante a execução da onda.
- Se você solicitar ambientes isolados, o AWS Transform cria uma Workloads/Production Workloads/Non-Production sub-OU.
- Se as estruturas aplicáveis forem identificadas, o AWS Transform cria uma Workloads/Regulated Workloads/Standard sub-OU.
- Se várias unidades de negócios precisarem de governança diferente, o AWS Transform cria OUs específicas para cada unidade de negócios em Cargas de trabalho.
- Aplicativos de dados críticos ou confidenciais recebem um único aplicativo por conta. Nesse caso, você pode ser solicitado a iterar seu plano de ondas.
- Aplicativos fortemente acoplados com dependências compartilhadas são agrupados em uma conta.

Cada conta proposta inclui: nome, finalidade, UO alvo e unidade de negócios. AWS Transform mostra a convenção de nomenclatura que está sendo usada (por exemplo, <business-unit>-<environment>-<workload>).

Você pode revisar e modificar a estrutura proposta antes que o AWS Transform aplique as alterações. Depois de se inscrever, você pode iterar — fazendo alterações adicionais até ficar satisfeito.

Configuração do SCP da carga de trabalho

Depois que a estrutura da carga de trabalho é criada, o AWS Transform apresenta as SCPs disponíveis e pergunta se você deseja aplicar alguma às suas OUs de carga de trabalho. Você seleciona quais SCPs aplicar e a quais OUs. O AWS Transform aplica os SCPs e mostra a árvore organizacional atualizada com uma tabela de resumo do SCP.

Implantação da carga de trabalho

Depois que o design da carga de trabalho estiver concluído, você escolhe como implantar:

- **Implante para mim** — O AWS Transform implanta a carga de trabalho OUs, contas e SCPs em sua organização. AWS
- **Vou implantar sozinho** — o AWS Transform gera artefatos IaC para download em seu formato preferido (consulte [the section called “Formatos IaC”](#)).

Formatos IaC

Quando você escolhe a autoimplantação, o AWS Transform gera artefatos de infraestrutura como código nos seguintes formatos:

- [AWS Cloud Development Kit \(AWS CDK\)](#) — TypeScript projeto para implantação de infraestrutura programática.
- HashiCorp Terraform — Gera modelos HashiCorp de linguagem de configuração (HCL) para gerenciar recursos da zona de pouso.
- Landing Zone Accelerator (LZA) — Arquivos YAML de configuração com base na configuração universal LZA versão 1.1.0. Esses modelos prontos para empresas funcionam com o Landing Zone Accelerator AWS para estabelecer ambientes com várias contas. Os arquivos gerados incluem configurações pré-definidas para governança, estrutura organizacional e rede que se alinham às AWS melhores práticas. Para saber mais, consulte [Configuração universal do LZA](#).

Note

Ao implantar por meio do pipeline Landing Zone Accelerator (LZA), sua conta AWS Transform e a instalação do LZA devem estar na mesma organização. A implantação falhará se houver uma incompatibilidade entre os IDs de Organizations usados no AWS Transform e no LZA. Para saber como configurar sua instalação do LZA usando Organizations, consulte [Instalação baseada em AWS Organizations](#).

Depois de selecionar um formato, o AWS Transform gera os artefatos e os disponibiliza para download.

Para verificar se o arquivo baixado não foi corrompido ou adulterado, gere e baixe uma soma de verificação e, em seguida, compare-a com um hash gerado localmente usando:

```
openssl dgst -sha256 -binary <file.zip> | base64
```

Processo de aprovação de implantação

As solicitações de implantação da zona de aterrissagem exigem aprovação explícita antes da execução. Quando você envia uma solicitação de implantação, ela é encaminhada automaticamente para aprovadores autorizados por meio da guia AWS Transformar aprovações.

Os aprovadores revisam os CloudFormation modelos e as configurações da zona de pouso. Somente usuários com a função de administrador no AWS Transform podem aprovar solicitações de implantação. Cada envio aciona um novo ciclo de revisão, e as implantações prosseguem somente após o recebimento da confirmação.

Se um aprovador negar sua solicitação, entre em contato diretamente com ele para discutir as modificações necessárias. O sistema rastreia todas as decisões de aprovação para fins de auditoria e mantém o histórico de implantação.

Tag: recursos da zona de pouso

AWS O Transform marca automaticamente todos os recursos gerados "CreatedBy": "AWSTransform" junto com os IDs de definição e execução para fins de rastreamento.

Etiquetas automáticas

Todos os recursos da landing zone recebem as seguintes tags:

- CreatedBy— AWS Transform
- ATWorkspace— Identificador do espaço de trabalho

Note

Se sua migração fizer parte do AWS Migration Acceleration Program (MAP 2.0), você poderá incluir a tag MAP necessária: Key: map-migrated Value: migMPE_ID (onde MPE_ID é seu identificador de avaliação do portfólio de migração). A tag MAP é solicitada durante a fase de configuração do conector. AWS O Transform aplica essas tags durante a implantação da landing zone.

Revertendo mudanças

Somente elementos não implantados podem ser removidos. Depois que uma OU ou conta é implantada, ela não pode ser removida por meio do agente landing zone.

Ao remover elementos, a ordem é importante — você deve remover os filhos antes dos pais:

1. Remova as contas primeiro (por e-mail).
2. Remova SCPs das OUs.
3. Remover OUs secundárias — uma OU não pode ser removida se ainda tiver contas ou OUs aninhadas.

Recursos relacionados

- [the section called “Conecte o alvo Conta da AWS s e regiões”](#)
- [the section called “Migre sua rede para AWS”](#)
- [AWS Guia do usuário da Control Tower](#)
- [AWS Guia do usuário do Organizations](#)
- [AWS Usuários do IAM Identity Center](#)
- [CloudFormation Guia do usuário](#)
- [Acelerador de zona de pouso ativado AWS](#)
- [AWS Well-Architected Framework](#)
- [AWS Orientação prescritiva: Construindo zonas de pouso](#)

Migre sua rede para AWS

Com o AWS Transform, você pode migrar sua rede para o AWS. O AWS Transform traduz a configuração do seu ambiente de origem em recursos de rede AWS equivalentes — VPCs, sub-redes, grupos de segurança, gateways NAT, gateways de trânsito, IPs elásticos, rotas e tabelas de rotas, conforme necessário. Você pode revisar e modificar a configuração de rede gerada antes da implantação. Você pode implantar a configuração com o AWS Transform e analisar a conectividade da rede. Como alternativa, você pode escolher a autoimplantação e receber Infrastructure as Code (IaC) no formato de sua preferência: AWS Cloud Development Kit (AWS CDK) Landing Zone Accelerator (LZA) ou Terraform. HashiCorp

Para migrar sua rede, siga estas etapas:

1. Carregue seu arquivo de rede de origem.
2. Carregue arquivos de configuração adicionais (opcional, para ambientes RVTools).
3. Selecione uma topologia de rede.
4. Selecione uma estratégia de mapeamento de grupos de segurança.
5. Revise e otimize sua rede.
6. Gere um diagrama de rede (opcional).
7. Configure a marcação de recursos.
8. Implante sua rede.

Note

Para implantações com várias contas, você deve configurar funções do IAM entre contas e acesso confiável para AWS Organizations antes de iniciar a migração da rede. Para obter mais informações sobre os tipos de migração, consulte [the section called “Etapa 1: Seleção do tipo de migração”](#).

Etapa 1: mapeamento da rede de origem

O processo de mapeamento de rede exige que você carregue um arquivo de configuração do seu ambiente de origem. A ferramenta escolhida depende do tipo de rede de origem:

- Redes definidas por software (SDN): Import/Export para virtualização de rede VMware NSX ou configuração Cisco ACI para Cisco Application Centric Infrastructure.
- [Redes VMware vSphere: RVTools](#). Quando você usa arquivos RVTools, o AWS Transform gera somente configurações da Amazon VPC. As configurações do grupo de segurança exigem entrada adicional do firewall ou dos arquivos de rede definidos por software. Para obter mais informações sobre a geração de grupos de segurança a partir de arquivos [adicionais, consulte Arquivos de configuração adicionais](#).
- Redes baseadas em dados de configuração de firewall: Exporte arquivos do Palo Alto Networks Firewall, Fortinet FortiGate Firewall ou Cisco ACI. Para obter mais informações sobre as versões suportadas e as instruções de extração, consulte Extração [do arquivo de configuração](#).
- Redes híbridas que executam cargas de trabalho VMware e não VMware: AWS [ferramenta de descoberta Transform ou ModelizeIt](#).
- Outros tipos de arquivo: se o arquivo de configuração não for um dos formatos compatíveis listados acima, o arquivo será convertido automaticamente em um formato compatível. Essa conversão pode levar até duas horas com base no tamanho e na complexidade do arquivo.

 Note

O tamanho máximo do arquivo de rede de origem suportado é 70 MB.

 Warning

Baixe o RVTools somente do site oficial da Dell em: <https://www.dell.com/en-us/shop/vmware/sl/rvtools> Não baixe o RVTools de fontes não oficiais.

Cada segmento de rede de origem é mapeado para sua própria VPC distinta. A segmentação da rede varia de acordo com o tipo de fonte:

- vNetwork: AWS transforme grupos de VMs por vSwitch e LAN virtual (VLAN). As VLANs podem aparecer em vários vSwitches (exceto a VLAN 0).
- Redes NSX: AWS transforme segmentos da rede com base em Tier-1 roteadores, agrupando os roteadores e coletando seus segmentos.

Etapa 2: arquivos de configuração adicionais

Para ambientes de origem do RVTools, você pode, opcionalmente, carregar arquivos de configuração adicionais para permitir a geração de grupos de segurança. Se você não fizer upload de arquivos de configuração adicionais, nenhum grupo de segurança será gerado para sua RVTools-based migração.

AWS O Transform oferece suporte aos seguintes tipos de arquivo de configuração adicionais. Você pode carregar somente um arquivo de configuração de uma plataforma.

- A Cisco Application Centric Infrastructure (ACI) fornece configurações de políticas de rede.
- A Palo Alto Networks fornece políticas de segurança de firewall.
- A Fortinet FortiGate fornece políticas de segurança de firewall.

Quando você carrega um firewall ou um arquivo Cisco ACI, o AWS Transform gera infraestrutura de rede e grupos de segurança. Quando você carrega um arquivo RVTools sozinho, o AWS Transform gera somente infraestrutura de rede.

Para obter mais informações sobre as versões suportadas e as instruções de extração, consulte Extração [do arquivo de configuração](#).

Etapa 3: topologias de rede

Durante a etapa de definição da rede, você seleciona uma topologia de rede. Você pode escolher a topologia de VPCs isoladas ou a topologia Hub and Spoke.

VPCs isoladas

O que é implantado

As VPCs isoladas são ambientes de rede independentes que operam como unidades separadas em seu interior AWS. Suas VPCs estão completamente isoladas, sem caminhos de comunicação integrados entre elas. Essa separação fornece o nível mais alto de proteção dos limites da rede.

AWS O Transform cria os seguintes recursos:

- Uma VPC dedicada para cada segmento de rede de origem detectado.
- Sub-redes privadas com base na configuração da rede de origem.
- Grupos de segurança (se você forneceu arquivos de configuração de firewall ou SDN).

Conclua sua configuração

AWS O Transform implanta a infraestrutura de rede, mas deixa o acesso à Internet e a conectividade entre VPCs para você, para que você possa escolher a configuração que atenda aos requisitos da sua organização.

Para habilitar o acesso à Internet para uma VPC isolada, conclua as seguintes etapas:

1. Crie um [gateway de internet](#) e conecte-o à VPC.
2. Crie sub-redes públicas em cada zona de disponibilidade em que você precisa de acesso à Internet. Adicione uma rota para `0.0.0.0/0` apontar para o gateway da Internet. Para obter mais informações sobre a configuração de sub-rede, consulte [Sub-redes para sua VPC](#).
3. Crie [gateways NAT](#) nas sub-redes públicas (um por AZ para alta disponibilidade). Aloque um IP elástico para cada gateway NAT.
4. Atualize suas [tabelas de rotas](#) de sub-rede privada — adicione uma rota para `0.0.0.0/0` apontar para o gateway NAT na mesma AZ.
5. Revise suas [regras de grupo de segurança](#) — garanta que as regras de saída permitam o tráfego de que suas cargas de trabalho precisam (HTTPS, DNS etc.).

Para VPC-to-VPC comunicação, configure o [emparelhamento de VPC](#) ou um [Transit Gateway](#) e atualize as tabelas de rotas em cada VPC para rotear o tráfego para a conexão de emparelhamento ou anexo TGW.

Hub e Spoke

Nesse modelo, um [AWS Transit Gateway](#) atua como o hub central que conecta várias VPCs de carga de trabalho (os spokes).

O que é implantado

AWS O Transform cria os seguintes recursos:

- VPCs Spoke: uma VPC por segmento de rede de origem detectado, com sub-redes privadas e um anexo do Transit Gateway.
- VPC de inspeção: hospeda seu dispositivo de firewall para inspeção de tráfego. Todo o tráfego entre VPC é roteado por essa VPC. O anexo do Transit Gateway usa o [modo de dispositivo](#), uma configuração que garante que o tráfego flua simetricamente pelo mesmo dispositivo nas duas direções de uma conexão.

- VPC de entrada: gerencia o tráfego que entra na sua rede a partir da Internet pública (entrada norte-sul). Inclui um [gateway de internet](#) e sub-redes públicas em várias zonas de disponibilidade.
- VPC de saída: gerencia o tráfego que sai da sua rede para a Internet pública (saída norte-sul). Inclui um gateway de internet, [gateways NAT](#) com [endereços IP elásticos](#) em cada zona de disponibilidade para alta disponibilidade e sub-redes privadas para o anexo do Transit Gateway.
- Tabelas de rotas do Transit Gateway: duas tabelas de rotas direcionam o tráfego pela VPC de inspeção. A tabela não inspecionada está associada a VPCs spoke, VPC de entrada e VPC de saída — ela roteia todo o tráfego (0.0.0). 0/0) ao anexo VPC de inspeção e é a tabela de rotas de associação padrão. A tabela inspecionada está associada à VPC de inspeção — ela contém rotas propagadas de todas as VPCs spoke e é a tabela de rotas de propagação padrão.

Para implantações com várias contas, o Transit Gateway é compartilhado entre contas por meio do [AWS Resource Access Manager \(RAM\)](#).

Fluxo de tráfego

Todo o tráfego entre VPCs segue esse caminho:

1. O tráfego de uma VPC spoke é enviado para o Transit Gateway (rota padrão 0.0.0). 0/0).
2. A tabela de rotas não inspecionadas direciona o tráfego para a VPC de inspeção.
3. Seu firewall na VPC de inspeção inspeciona o tráfego e o encaminha de volta para o Transit Gateway.
4. A tabela de rotas inspecionadas encaminha o tráfego para a VPC de destino usando rotas propagadas.

Para tráfego de saída da Internet, a tabela de rotas inspecionada roteia o tráfego para a VPC de saída. Os gateways NAT traduzem endereços IP privados antes que o tráfego seja encaminhado para o gateway da Internet. A tabela de rotas públicas de saída da VPC inclui rotas específicas para cada intervalo de roteamento Inter-Domain sem classe (CIDR) da VPC até o Transit Gateway. Essas rotas permitem que o tráfego de retorno alcance a VPC de fala correta.

O tráfego de entrada da Internet entra pelo gateway de Internet da VPC de entrada e segue o mesmo caminho de inspeção para alcançar as VPCs spoke.

Conclua sua configuração

AWS O Transform implanta a infraestrutura de rede, mas deixa a configuração do firewall e do serviço de entrada para você, para que você possa escolher os dispositivos e políticas de segurança que atendam aos requisitos da sua organização.

Note

Por padrão, o tráfego entre VPCs passa pela VPC de inspeção sem inspeção. Você deve implantar um firewall para permitir a inspeção de tráfego.

Implante um firewall: crie sub-redes adicionais na VPC de inspeção para os endpoints do firewall. AWS O Transform cria sub-redes somente para o anexo do Transit Gateway. Roteie o tráfego das sub-redes de anexo do TGW para os endpoints do firewall e das sub-redes do firewall de volta para o Transit Gateway. Você pode implantar o [AWS Network Firewall](#) ou um dispositivo de terceiros. Para obter mais informações sobre como implantar um firewall com um Transit Gateway, consulte [Criando um firewall com um Transit Gateway](#).

Verifique a conectividade: depois de implantar o firewall, teste o acesso de saída à Internet a partir de uma instância de VPC spoke (por exemplo `curl https://aws.amazon.com`). Você pode usar o [Reachability Analyzer para solucionar problemas de conectividade](#).

Configurar serviços de entrada: para hospedar serviços voltados para o público, implante um [Application Load Balancer ou Network Load Balancer](#) nas sub-redes públicas da VPC de entrada. Configure grupos-alvo que apontam para instâncias em suas VPCs spoke por meio do Transit Gateway e verifique se a tabela de rotas inspecionadas tem rotas de retorno para a VPC de entrada.

Se você quiser um controle refinado sobre a comunicação entre as VPCs, escolha a opção VPCs isoladas e modifique a rede gerada para criar os caminhos de comunicação específicos necessários.

Etapa 4: mapeamento de grupos de segurança

Escolha como suas políticas de segurança de origem se traduzem em grupos AWS de segurança. AWS O Transform cria grupos de segurança com base nas configurações do seu ambiente de origem. Políticas de segurança, regras de política de segurança, políticas de gateway e regras de política de gateway são convertidas em grupos de segurança.

⚠ Important

AWS O Transform cria grupos de segurança com base no melhor esforço possível para corresponder ao seu ambiente de origem. Analise e modifique os grupos de segurança gerados para garantir que eles atendam às necessidades e às políticas de segurança da sua empresa.

Referenciamento de grupo de segurança

Quando grupos de segurança são gerados, o AWS Transform usa referências de grupos de segurança quando há suporte. A referência de grupos de segurança define regras de segurança com base em outro ID de grupo de segurança em vez de intervalos de endereços IP específicos (blocos CIDR). Essa abordagem fornece configurações de segurança mais flexíveis e fáceis de manter.

Suas regras de grupo de segurança só podem fazer referência a outros grupos de segurança dentro da mesma VPC ou em uma VPC conectada na mesma região. Cross-account referências também são suportadas. Você não pode referenciar um grupo de segurança em uma VPC não conectada ou entre regiões. Para VPCs conectadas, somente as regras de entrada oferecem suporte a referências de grupos de segurança entre VPCs — as regras de saída devem usar regras CIDR-based. A forma como o AWS Transform cria regras de grupos de segurança depende da topologia de rede escolhida:

- **Hub and Spoke:** o Transit Gateway fornece conectividade de rede entre VPCs. AWS O Transform usa referências para regras dentro da VPC e de entrada cruzada. VPC/cross-account Cross-VPC/cross-account As regras de saída (de saída) usam CIDR-based regras.
- **VPCs isoladas:** suas VPCs não têm conectividade de rede entre elas. AWS O Transform usa referências somente para regras dentro da VPC. Todas as regras entre VPCs e contas cruzadas usam regras CIDR-based

CIDR-based as regras também são usadas quando as configurações de origem não são simétricas.

Escolha uma das seguintes estratégias de mapeamento de grupos de segurança:

- **MAP:** traduz as regras de segurança do seu ambiente de origem em grupos e regras de AWS segurança. Use essa opção para migrações usando endereçamento IP estático.
- **MAP_DHCP** (Traduzir com suporte a DHCP): traduz as regras de segurança do seu ambiente de origem com compatibilidade com DHCP. O DHCP atribui endereços IP dinamicamente do

intervalo CIDR da sub-rede. Como resultado, as regras de saída entre VPCs são ampliadas para corresponder ao CIDR completo da sub-rede de destino. Um CIDR mais restrito bloquearia DHCP-assigned IPs que estão fora dessa faixa — revise essas regras após a migração.

Use essa opção para suporte a DHCP com comunicação entre VPC Transit Gateway. Também funciona com IPs estáticos, mas pode produzir regras mais amplas do que o MAP.

- **IGNORAR:** Não traduz regras de segurança. Configure grupos AWS de segurança manualmente após a migração. Funciona com ambientes IP estáticos e DHCP. Para ambientes de origem do RVTools sem arquivos de configuração adicionais, o AWS Transform usa automaticamente o SKIP.

Note

Sua estratégia de mapeamento determina suas opções de atribuição de IP. O MAP suporta somente IP estático. O MAP_DHCP e o SKIP suportam tanto a estática quanto a DHCP.

Abordagens de migração de IP

Você tem duas opções de configuração de rede para sua migração:

Seleção de alcance de rede

- **Manter intervalos existentes (retenção de intervalos de endereços IP):** mantenha intervalos de endereços IP originais durante a migração. Ideal para migrações para as quais você move aplicativos AWS sem modificação (lift-and-shift), especialmente com aplicativos legados que têm dependências IP codificadas ou regras de firewall existentes.
- **Atualização para novos intervalos de IP (atualização CIDR):** você pode modificar cada intervalo de CIDR da VPC durante a migração, AWS e o Transform propaga automaticamente as alterações para sub-redes, tabelas de rotas e grupos de segurança.

Atribuição de endereço IP

- **Endereços IP fixos (estáticos):** o AWS Transform atribui IPs estáticos com base no CIDR. Isso é melhor para aplicativos que exigem comportamento de rede previsível, gerenciamento de DNS ou controle de IP-based acesso. Os IPs persistem nas reinicializações de instâncias por meio de Elastic Network Interfaces (ENIs), que são placas de rede virtuais conectadas às suas instâncias.

- **Atribuição dinâmica de IP (AWS DHCP):** atribua automaticamente IPs de pools de sub-rede na inicialização da instância. Ideal para aplicativos projetados para serem executados na nuvem e cargas de trabalho com escalonamento automático. Reduz a sobrecarga operacional, mas exige que os aplicativos usem o DNS ou a descoberta de serviços.

Você pode combinar qualquer seleção de intervalo com qualquer método de atribuição de IP.

Note

A estratégia de atribuição de endereço IP é definida no nível da onda. Você pode atribuir estratégias diferentes a servidores específicos personalizando o arquivo wave. Por exemplo, se você escolheu uma abordagem de endereço IP estático para o wave, mas deseja atribuir uma abordagem dinâmica a um servidor específico, você usaria [RESET_VALUE] conforme descrito em [Editando sua configuração](#) no guia do usuário do MGN.

Etapa 5: Revise e otimize sua rede

Depois que o AWS Transform gerar sua configuração de rede de destino, você poderá revisar os segmentos de rede locais convergidos para a AWS infraestrutura. Use a interface visual para analisar sua rede e a interface de bate-papo para fazer alterações e receber recomendações guiadas. AWS O Transform realiza análises de impacto em cascata e implementa as mudanças necessárias para manter a consistência da rede e a conformidade com as melhores práticas. Você também pode pedir à AWS Transform que analise sua rede e sugira otimizações — consulte as recomendações [guiadas](#).

VPCs existentes em sua conta de destino

Se sua conta de destino já contém VPCs — de fases anteriores de migração ou projetos de infraestrutura paralelos — o AWS Transform as detecta automaticamente e as exibe junto com suas VPCs mapeadas durante o processo de análise. Para migrações de várias contas, o AWS Transform detecta VPCs existentes em todas as contas da sua organização. AWS

Essa visibilidade ajuda você a entender como sua rede planejada se relaciona com sua infraestrutura existente, identificar possíveis conflitos de CIDR e tomar decisões informadas antes da implantação.

Note

AWS O Transform detecta somente VPCs existentes (não sub-redes ou outros recursos). A detecção é somente para leitura — o AWS Transform não modifica suas VPCs existentes.

Otimize sua rede

Note

Essas operações se aplicam somente às VPCs de carga de trabalho. Para VPCs de dispositivos na topologia Hub and Spoke (inspeção, entrada, saída), somente a alteração do endereço IP é suportada.

Você não pode desfazer as operações de exclusão, mesclagem e divisão. Revise sua configuração cuidadosamente antes de aplicar essas alterações.

As seguintes operações estão disponíveis para VPCs:

- Excluir: remova permanentemente uma VPC da configuração. Use isso para segmentos de rede obsoletos que não devem migrar para o AWS
- Excluir: remova temporariamente uma VPC da migração para estratégias de migração em fases. As VPCs excluídas não são implantadas, mas podem ser reincluídas posteriormente.
- Incluir: adicione uma VPC excluída anteriormente de volta à migração.
- Mesclar: combine duas VPCs em uma. A primeira VPC mantém sua identidade e absorve todas as sub-redes da segunda VPC. Os grupos de segurança são movidos para a VPC mesclada e suas associações são reconstruídas adequadamente. O CIDR da primeira VPC se expande para o menor intervalo de CIDR que contém os dois CIDRs originais, e o roteamento é atualizado automaticamente. A segunda VPC é removida da configuração.

Requisitos de mesclagem:

- Os CIDRs de sub-rede não devem se sobrepor entre as duas VPCs.
- O CIDR mesclado não deve exceder /16.
- Para implantações com várias contas, as duas VPCs devem ser atribuídas à mesma conta.
- Alterar endereço IP: altere o endereço IP base de um CIDR de VPC mantendo o mesmo tamanho de prefixo. AWS O Transform traduz automaticamente todos os CIDRs de sub-rede pelo mesmo

deslocamento. Por exemplo, alterar uma VPC de 10.0.0.0/16 para 10.20.0.0/16 desloca uma sub-rede de para. 10.0.1.0/24 10.20.1.0/24

As regras do grupo de segurança que correspondem exatamente ao antigo CIDR da VPC são atualizadas automaticamente. As regras que se sobrepõem parcialmente ou não correspondem ao CIDR antigo não são alteradas — revise essas regras após a alteração.

- Renomear: altere o nome de uma VPC para se alinhar às convenções de nomenclatura da sua organização para alocação de custos, controle de conformidade e padrões operacionais.
- Redimensionar: altere o comprimento do prefixo de um CIDR de VPC para expandir ou reduzir o intervalo de endereços IP.
 - Diminuição do comprimento do prefixo (mais IPs, por exemplo, /20 a /16): as sub-redes ainda se encaixam na faixa maior. Nenhuma alteração na sub-rede é necessária.
 - Aumento do comprimento do prefixo (menos IPs, por exemplo, /16 a /20): as sub-redes que estão fora do novo intervalo devem ser redimensionadas primeiro usando a operação de redimensionamento da sub-rede.

As regras do grupo de segurança que correspondem exatamente ao antigo CIDR da VPC são atualizadas automaticamente. As regras que se sobrepõem parcialmente ou não correspondem ao CIDR antigo não são alteradas — revise essas regras após o redimensionamento.

Requisitos de redimensionamento:

- O novo CIDR deve estar entre /16 e /28.
- O novo CIDR não deve se sobrepor a outras VPCs na rede (topologia Hub and Spoke).
- Ao reduzir o CIDR, todas as sub-redes existentes devem caber no novo CIDR. Redimensione as sub-redes primeiro, se necessário.
- Dividir: divida uma VPC em duas VPCs com base nos limites de CIDR que você fornece. As sub-redes são atribuídas à nova VPC cujo CIDR as contém. Os grupos de segurança são clonados nas duas novas VPCs, mas os CIDRs das regras do grupo de segurança não são atualizados automaticamente. Revise suas regras após a divisão para garantir que a comunicação entre VPCs funcione conforme o esperado. A VPC original é substituída pelas duas novas VPCs.

Requisitos divididos:

- Você deve fornecer exatamente dois intervalos de CIDR.
- Os dois CIDRs não devem se sobrepor.
- Cada CIDR deve estar entre /16 e /28.

- Cada sub-rede deve caber exatamente em um dos dois CIDRs. Se alguma sub-rede não couber, a operação será rejeitada.

As seguintes operações estão disponíveis para sub-redes:

- Alterar endereço IP: altere o endereço IP base de um CIDR de sub-rede, mantendo o mesmo tamanho de prefixo.
- Excluir: remova permanentemente uma sub-rede da configuração sem afetar a VPC principal.
- Redimensionar: altere o comprimento do prefixo de um CIDR de sub-rede para expandir ou reduzir o intervalo de endereços IP.

Requisitos de redimensionamento da sub-rede:

- O novo CIDR deve estar entre /16 e /28.
- O novo CIDR não deve se sobrepor a outras sub-redes na mesma VPC.
- O novo CIDR deve estar dentro do CIDR da VPC principal.

Depois de cada operação, o AWS Transform reavalia a referência de grupos de segurança, o que pode converter CIDR-based regras em referências de grupos de segurança ou vice-versa. Revise as regras do grupo de segurança depois de fazer alterações para verificar se elas atendem aos seus requisitos.

Recomendações de rede guiadas

AWS O Transform analisa sua rede mapeada e fornece recomendações priorizadas por meio da interface de bate-papo. As recomendações são baseadas nos dados da sua rede e exigem sua confirmação antes que qualquer alteração seja aplicada.

AWS A Transform pode recomendar as seguintes otimizações:

- Resolução de conflitos de CIDR: sinaliza intervalos CIDR sobrepostos entre suas VPCs mapeadas e VPCs existentes em todas as contas da sua organização. AWS VPCs conflitantes são mostradas primeiro. Você pode resolver conflitos reendereçando a VPC mapeada, excluindo-a ou excluindo-a, ou reconhecendo o conflito e resolvendo-o você mesmo após a implantação.
- Padronização de nomenclatura: sinaliza nomes de VPC que não seguem um padrão consistente (por exemplo, nomes contendo referências de hardware). AWS O Transform solicita sua convenção de nomenclatura de nuvem antes de propor substituições.

- **Análise do escopo:** identifica segmentos de rede para os quais talvez não seja necessário migrar AWS, como sistemas legados ou construções pendentes de desativação. AWS O Transform solicita sua confirmação antes de excluir qualquer construção.
- **Dimensionamento correto da capacidade de VPC:** mostra VPCs em que o CIDR parece superdimensionado ou subdimensionado para as sub-redes que ele contém. AWS O Transform apresenta os dados de capacidade atuais e permite que você decida se deseja redimensionar.
- **Análise de segurança:** sinaliza as regras do grupo de segurança que permitem tráfego de entrada irrestrito (0.0.0.0/0) para sua avaliação.
- **Consolidação de VPC:** identifica VPCs fragmentadas que parecem separadas por limites de infraestrutura física em vez de requisitos de isolamento lógico, e sugere mesclá-las.

Note

Todas as recomendações exigem sua confirmação explícita antes que o AWS Transform aplique qualquer alteração. AWS O Transform apresenta vantagens quando uma recomendação afeta vários aspectos da sua rede.

Etapa 6: diagrama de rede

Depois de analisar as configurações de VPC geradas, você pode, opcionalmente, gerar um diagrama de rede para visualizar sua topologia de rede. AWS O Transform é compatível com os seguintes formatos de diagrama:

- **Código sereia (.mmd):** esse formato produz um arquivo de definição de diagrama baseado em texto que você pode renderizar com ferramentas. Mermaid-compatible
- **Imagem (.png):** esse formato produz uma imagem renderizada da topologia da rede.

Etapa 7: configurar a marcação de recursos

Seus recursos de rede são marcados para lançamento e replicação. Você também pode adicionar tags personalizadas e tags do AWS Migration Acceleration Program (MAP).

Etiquetas automáticas para lançamento e replicação

AWS O Transform marca automaticamente seus recursos de rede migrados (VPCs, sub-redes, grupos de segurança e tabelas de rotas) com as seguintes tags:

- Key (Chave): CreatedBy Value (Valor): AWSApplicationMigrationService
- Key (Chave): ATWorkspace Value (Valor): *workspace-id*

Essas tags permitem usar a VPC e a sub-rede para iniciar instâncias de teste e transição em. AWS

 Note

Suas VPCs e sub-redes migradas não incluem conectividade com a Internet por padrão, portanto, não são adequadas como áreas de preparação para replicação.

Para também usar a VPC e a sub-rede como área de armazenamento (replicação), adicione manualmente as seguintes tags:

- Key (Chave): CreatedFor Value (Valor): AWSTransform
- Key (Chave): ATWorkspace Value (Valor): *workspace-id*

Você também pode aplicar essas tags a qualquer recurso de AWS rede existente para disponibilizá-lo para replicação.

Encontre o ID do seu espaço de trabalho na URL do aplicativo web AWS Transform: [https://... /workspace//workspace-id-id/job/job](https://.../workspace//workspace-id-id/job/job)

Tags personalizadas

Além das tags aplicadas automaticamente pelo AWS Transform, você pode, opcionalmente, adicionar tags personalizadas para organizar, rastrear custos e gerenciar a conformidade dos recursos de rede migrados. Você pode aplicar tags personalizadas em dois níveis:

- Job-level tags: aplicam-se a todos os recursos criados por esse trabalho, incluindo todas as VPCs, sub-redes, grupos de segurança e tabelas de rotas.
- VPC-level tags: aplicam-se a uma VPC específica e se propagam automaticamente a todos os recursos associados (sub-redes, grupos de segurança, tabelas de rotas).

 Note

Máximo de 40 tags por solicitação. Cada tag exige uma chave e um valor. AWS as convenções de marcação se aplicam.

AWS O Transform aplica essas tags ao gerar os modelos de Infraestrutura como Código.

AWS Programa de Aceleração da Migração

Se sua migração fizer parte do AWS Migration Acceleration Program (MAP 2.0), o AWS Transform aplicará uma tag MAP aos seus recursos. Se você forneceu sua ID MPE no início do processo de migração, a tag será aplicada automaticamente. Caso contrário, depois de concluir a análise das configurações de VPC geradas AWS, o Transform pergunta se você tem um contrato de MAP e solicita que você forneça seu ID MPE — um código de 10 caracteres usando letras e dígitos maiúsculos (por exemplo, ABCDE12345). A tag aplicada usa o formato:

- Key (Chave): map-migrated Value (Valor): mig`MPE_ID`

Etapa 8: implantar sua rede

Depois de marcar, selecione sua estratégia de implantação:

- AWS Transform-managed implantação: o AWS Transform usa CloudFormation modelos para implantar sua rede e executa o Reachability Analyzer para verificar a conectividade entre sub-redes em várias VPCs e dentro da mesma VPC.

 Note

Você deve obter aprovação explícita antes que sua solicitação de implantação de rede seja executada. Consulte o [processo de aprovação de implantação](#).

- Self-deployment: o AWS Transform gera modelos de infraestrutura como código (IaC). CloudFormation os modelos são gerados por padrão. Você também pode selecionar formatos de saída adicionais:
 - AWS CDK gera um TypeScript projeto para implantação de infraestrutura programática.
 - HashiCorp O Terraform gera modelos HashiCorp de Linguagem de Configuração (HCL) para gerenciar recursos de rede.

- O Landing Zone Accelerator (LZA) gera um arquivo `network-config.yaml` para a configuração da rede LZA.

Note

Quando você implanta por meio do pipeline Landing Zone Accelerator (LZA), sua conta AWS Transform e a instalação do LZA devem estar na mesma organização. A implantação falhará se houver uma incompatibilidade entre as IDs da organização.

Para implantação automática, use o link fornecido para baixar um arquivo zip contendo os modelos gerados. A pasta zip inclui um `README.md` arquivo que explica como usar os modelos gerados.

Para verificar se o arquivo baixado não foi corrompido ou adulterado, gere e baixe uma soma de verificação e, em seguida, compare-a com um hash gerado localmente usando o comando. `openssl dgst -sha256 -binary <file.zip> | base64`

Processo de aprovações de implantação

Para garantir que as mudanças na rede estejam em conformidade com os padrões de segurança e os requisitos de arquitetura da sua organização, todas as solicitações de implantação passam por um fluxo de trabalho de aprovação. Você deve obter aprovação explícita antes que sua solicitação de implantação de rede seja executada. Quando você envia uma solicitação de implantação, ela é encaminhada automaticamente para aprovadores autorizados por meio da guia AWS Transformar aprovações. Os aprovadores validam os CloudFormation modelos e as configurações de rede para garantir a conformidade com os padrões de segurança e os requisitos de arquitetura. Cada envio aciona um novo ciclo de revisão, e as implantações prosseguem somente após o recebimento da confirmação. Se um aprovador negar sua solicitação, entre em contato diretamente com ele para discutir as modificações necessárias. AWS O Transform rastreia todas as decisões de aprovação para fins de auditoria e mantém o histórico de implantação.

Excluir recursos de rede implantados

Se precisar reverter uma implantação, você pode excluir os recursos de rede que o AWS Transform implantou. Você pode excluir recursos imediatamente após a conclusão da implantação. Se você modificar os recursos de rede implantados após a implantação, os recursos não poderão ser excluídos automaticamente.

- AWS Transform-managed implantações: o AWS Transform remove todas as CloudFormation pilhas que foram criadas durante a implantação. Essa ação requer aprovação por meio da guia AWS Transformar aprovações.
- Self-deployments: você deve excluir manualmente os recursos implantados por meio do AWS Management Console ou da AWS CLI.

Extração do arquivo de configuração

Se seu ambiente de origem usa Cisco ACI, Palo Alto Networks ou Fortinet FortiGate, você precisa extrair um arquivo de configuração para fornecer ao Transform. AWS Você pode usar esses arquivos como arquivos de origem autônomos para gerar infraestrutura de rede e grupos de segurança, ou como arquivos complementares junto com um upload do RVTools para adicionar a geração de grupos de segurança. O processo de extração é o mesmo nos dois casos.

Para extrair arquivos de configuração do firewall e dos ambientes de rede, siga estes procedimentos. Consulte a documentação do fornecedor para obter as informações mais recentes.

Fortinet FortiGate

- A versão do firmware deve ser v7.0 ou posterior.
- Você precisa de `super_admin` e `super_admin_readonly` privilégios em nível global.
- Etapas:
 1. Conecte-se ao firewall via SSH ou cliente CLI integrado
 2. Executar: `show | grep ""` (| `grep ""` desativa a paginação)
 3. Salve toda a saída em um arquivo a partir do `show` comando

Palo Alto Networks

- A versão do firmware deve ser 10.1 ou posterior.
- Você precisa da função de superadministrador.
- Conecte-se ao firewall por meio de SSH, execute os comandos a seguir para desativar a paginação, definir o formato de saída, entrar no modo de configuração e exportar a configuração e os objetos predefinidos. Salve as saídas:

```
set cli pager off
set cli config-output-format set
```

```
configure
show                # Save as palo-conf.txt
show predefined     # Save as palo-default.txt
```

Cisco ACI

- A versão do firmware deve ser 6.0 ou posterior.
- Você precisa da função de administrador com todos os privilégios e um destino configurado para Secure Copy Protocol (SCP), SSH File Transfer Protocol (SFTP) ou File Transfer Protocol (FTP).
- Etapas:
 1. Conecte-se ao Application Policy Infrastructure Controller (APIC) por meio do seu navegador
 2. Abra o menu Admin e escolha Config Rollbacks
 3. Na caixa de diálogo Tirar um instantâneo, selecione a opção de localização remota e escolha Criar um instantâneo agora.
 4. Depois de receber a mensagem “Transferência bem-sucedida”, conecte-se ao servidor de localização remota e recupere o arquivo de instantâneo mais recente (arquivo.gz)

Migrar servidores

AWS O Transform usa AWS Transform MGN (MGN) para rehostar seus servidores no Amazon EC2. O fluxo de trabalho de migração de servidores orienta você na configuração de cada onda de migração, na validação do inventário de servidores, na implantação de agentes de replicação, no monitoramento da replicação de dados, no teste de instâncias migradas e na execução da transição final. Para ler mais sobre isso, consulte [O que é AWS Transform MGN?](#) no Guia do usuário do MGN.

A migração do servidor é organizada por ondas. Cada onda representa um grupo de servidores que são migrados juntos. Para cada onda, você conclui as seguintes fases:

Para ondas com uma estratégia de migração de contêineres, o AWS Transform executa o fluxo de trabalho de containerização do código-fonte em vez das etapas de rehostagem descritas abaixo. O fluxo de trabalho de containerização orienta você na clonagem do código-fonte, na geração de artefatos do Docker, na publicação de imagens de contêineres e na implantação no Amazon Elastic Container Service ou no Amazon Elastic Kubernetes Service. Para ver o fluxo de trabalho completo de containerização, consulte. [Containerização do código-fonte](#)

1. Pré-requisitos e configuração de padrões de migração

2. Etapa 1: configurar a onda de migração
3. Etapa 2: validar e confirmar o inventário
4. Etapa 3: implantar agentes de replicação
5. Etapa 4: replicação de dados
6. Etapa 5: Teste
7. Etapa 6: transição

Pré-requisitos e configuração de padrões de migração

Pré-requisitos

Antes de iniciar a migração de rehosting, verifique se você tem o seguinte:

Note

Se você concluiu todas as etapas de um trabalho de migração de ponta a ponta no AWS Transform, suas contas de destino e arquivo de inventário já estão preparados — o arquivo de inventário terá sido gerado para você durante a etapa de planejamento da migração. A infraestrutura de rede configurada por meio da migração de rede AWS Transform também está pronta. Se você não criou sua infraestrutura de rede por meio do AWS Transform, certifique-se de que ela esteja configurada com antecedência antes de iniciar a migração de rehosting.

Antes de iniciar a migração de rehosting, verifique se você tem os recursos de rede e a infraestrutura para hospedar seus servidores. Você pode usar os recursos de migração de landing zone e rede do AWS Transform ou qualquer outra ferramenta para isso.

- Sistemas operacionais compatíveis — os servidores de origem devem executar um sistema operacional compatível. Para ver a lista completa, consulte [Sistemas operacionais compatíveis](#) no Guia do usuário do MGN.
- Contas de destino para migração — as Contas da AWS IDs para os quais você precisa que seus servidores sejam migrados. Você pode usar o AWS Transform landing zone ou qualquer outra ferramenta para configurar sua infraestrutura.
- Infraestrutura de rede instalada — VPCs, sub-redes e grupos de segurança implantados e configurados. Você pode usar a migração de rede do AWS Transform ou qualquer outra ferramenta para configurar sua infraestrutura de rede.

- Arquivo de inventário — Preparado com detalhes do servidor, atribuições de ondas, informações da conta-alvo e preferências de tipo de instância do Amazon EC2. Você pode usar o planejamento de migração do AWS Transform para gerar esse arquivo.

Configurar padrões de migração

Antes de iniciar a execução da migração de várias contas, você deve definir as configurações padrão que se aplicam a todas as suas contas de destino. Esses padrões definem como suas instâncias do Amazon EC2 são iniciadas e como a migração geral é configurada. Você pode substituir esses padrões no nível da onda durante a configuração da onda.

Preferências de recomendação do Amazon EC2

AWS O Transform fornece recomendações de tipo de instância do Amazon EC2 com base na especificação de utilização de suas VMs de origem. Você pode configurar suas preferências de recomendação do Amazon EC2 para controlar como os tipos de instância são selecionados para seus servidores migrados.

Para obter mais informações sobre como gerar recomendações do Amazon EC2, consulte [Geração de recomendações do Amazon EC2](#) em AWS Migration Hub

Note

Você pode modificar os tipos de instância sugeridos do Amazon EC2 para incluir recomendações do [Migration Evaluator](#), [AWS Optimization and Licensing Assessment \(OLA\)](#) ou de um [AWS trabalho de avaliação](#) do Transform.

Inicialização da migração

Para iniciar a migração, o AWS Transform inicializa o MGN para todas as Região da AWS quais você planeja migrar, bem como para todas as contas de destino nas quais o serviço será usado. Durante o processo de inicialização:

- As funções e políticas necessárias do IAM são criadas.
- Os modelos padrão necessários estão configurados.

Para obter informações sobre o processo de inicialização, consulte [Inicializando AWS Transform MGN com o console no Guia do usuário](#) do MGN.

Modelo de inicialização do Amazon EC2

As configurações de lançamento incluem duas partes: as configurações gerais de lançamento e o modelo de execução do Amazon EC2, que determina como uma instância de teste ou substituição é iniciada para cada servidor de origem em AWS.

As configurações de lançamento, incluindo o modelo de lançamento do Amazon EC2, podem ser definidas no nível da conta e, em seguida, aplicadas automaticamente a cada servidor de origem sempre que você adiciona um servidor de origem ao AWS Transform MGN. Os padrões das configurações de lançamento definidos nesta seção podem ser aplicados automaticamente a todas as suas contas de destino.

AWS O Transform apresenta a lista de configurações disponíveis do modelo de lançamento. Você pode optar por continuar com os padrões ou configurar seu modelo de lançamento. Se você optar por configurar, o AWS Transform fornecerá um link para uma análise human-in-the-loop (HITL) que contém todos os parâmetros das configurações do modelo de lançamento. Você também pode fazer modificações diretamente por meio da interface de bate-papo para quaisquer parâmetros que desejar.

Os [servidores de origem](#) são criados com as configurações do modelo de lançamento da conta. Depois que os servidores de origem forem criados com essas configurações padrão, você poderá alterá-las no nível das configurações de inicialização do servidor de origem. Você pode alterar as configurações do servidor de origem em qualquer parâmetro usando a interface de bate-papo ou para operações em massa usando o arquivo Excel de inventário durante [Etapa 2: validar e confirmar o inventário](#).

Para revisar a lista completa de configurações e detalhes do modelo de lançamento, consulte [Configurações gerais do Launch](#) no Guia do usuário do MGN.

Alterações adicionais no modelo de lançamento do Amazon EC2

Para alterações adicionais no modelo de lançamento do Amazon EC2, você deve executá-las no ID do modelo de cada conta de destino. Essa opção está disponível dentro da configuração de onda. AWS O Transform orienta você e fornece o link apropriado.

Etapa 1: configurar a onda de migração

Nessa fase, o AWS Transform prepara a onda de migração configurando a conta de destino, verificando as permissões do serviço, configurando etiquetas de recursos, adicionando dados de rede ao seu inventário e definindo as configurações de replicação e lançamento.

Modo de migração e configuração da conta

AWS O Transform oferece suporte a dois modos de migração:

- Single-account migração — Todos os servidores do wave migram para a mesma conta de destino configurada em seu conector.
- Multi-account migração — Os servidores migram para diferentes contas de destino especificadas em seu arquivo de inventário. Para migrações de várias contas, seu arquivo de inventário deve incluir uma `mgn:account-id` coluna com o ID da conta de destino para cada servidor.

AWS O Transform confirma a configuração da conta de destino e verifica se o MGN foi inicializado em cada conta de destino. Se o MGN ainda não tiver sido inicializado, o AWS Transform fornecerá instruções para concluir a inicialização. Durante a inicialização, o MGN cria as seguintes funções de serviço do IAM para operações de replicação e lançamento:

- `AWSApplicationMigrationReplicationServerRole`
- `AWSApplicationMigrationConversionServerRole`
- `AWSApplicationMigrationMGHRole`
- `AWSApplicationMigrationLaunchInstanceWithDrsRole`
- `AWSApplicationMigrationLaunchInstanceWithSsmRole`
- `AWSApplicationMigrationAgentRole`

Para saber mais sobre essas funções, consulte [Iniciando o MGN com o console ou Iniciando o MGN com a API no Guia do usuário do MGN](#).

Para migrações de várias contas, o AWS Transform também cria a seguinte função durante a etapa de inicialização: `AWSTransformRehostSharingRole_<management-or-delegated-admin-account-id>` Essa função é implantada em todas as contas de destino da migração.

Verificação da marcação de recursos

Depois que as permissões do serviço são confirmadas, o AWS Transform verifica se todos os recursos necessários estão devidamente marcados para que a migração seja operada pelo agente com sucesso. Se algum recurso não tiver as tags necessárias, o AWS Transform fornecerá um link para a página de marcação, onde você poderá aplicar as tags ausentes antes de continuar. As seguintes tags são obrigatórias:

- Os servidores de origem existentes devem ter tags `CreatedBy: AWSTransform` `ATWorkspace: <workspace_id>` e. Se você já iniciou a replicação nos servidores de origem e os criou no serviço AWS Transform MGN, precisará marcar esses servidores para que o AWS Transform possa correlacioná-los com os servidores de origem descobertos em seu ambiente local e evitar a criação desnecessária de servidores de origem duplicados. O AWS Transform correlaciona automaticamente entre eles usando as chaves de ID, FQDN ou nome de host fornecidas pelo usuário.
- Os recursos de rede devem ser etiquetados adequadamente tanto para as instâncias de replicação (área de preparação) quanto para as instâncias de inicialização. O AWS Transform exibe a lista completa de recursos de rede em sua conta de destino, com uma indicação de se cada recurso já está marcado ou não. Você pode revisar a lista e selecionar quaisquer recursos não marcados que você queira adicionar. Para cada recurso selecionado, o AWS Transform aplica a tag relevante:
 - `CreatedBy: AWSTransform``CreatedFor: AWSTransform`, dependendo do tipo de recurso.
 - `ATWorkspace: <workspace_id>` é aplicado a todos os recursos selecionados.

VPCs e sub-redes criadas pelo agente de migração de rede AWS Transform são automaticamente marcadas.

- Além de VPCs e sub-redes, o AWS Transform também exibe todas as interfaces de rede elástica (ENIs) existentes na sua conta de destino. Se você quiser que o AWS Transform os use como parte da execução da sua instância, eles devem ser marcados com `CreatedFor: AWSTransform` `ATWorkspace: <workspace_id>` e. Para obter mais informações sobre como anexar ou adicionar ENIs ao modelo de lançamento do Amazon EC2, [consulte Considerações detalhadas](#) no Guia do usuário do MGN.

Adicione dados de rede ao inventário

O AWS Transform adiciona informações de rede da sua migração de rede ao arquivo de inventário. Essa etapa mapeia seus servidores para as sub-redes e grupos de segurança de destino apropriados com base na configuração de rede gerada durante a fase de migração da rede.

Configurações de replicação e inicialização

Configuração das configurações de replicação

As configurações de replicação determinam como os dados são replicados de seus servidores de origem para o AWS Defina as configurações de replicação no modelo de replicação antes de adicionar servidores de origem ao AWS Transform MGN. AWS O Transform mostra todos os parâmetros das configurações de replicação — você pode configurá-los por meio de um HITL dedicado ou por meio da interface de bate-papo.

Para obter mais detalhes sobre os parâmetros das configurações de replicação, consulte o [modelo de configurações de replicação no Guia](#) do usuário do MGN.

Configurações do modelo de lançamento

O modelo de execução permite que você controle a forma como o AWS Transform MGN inicia instâncias em AWS. A configuração padrão definida no modelo é aplicada automaticamente a cada servidor recém-adicionado. Você pode definir as configurações do modelo de lançamento por meio de um HITL dedicado ou por meio da interface de bate-papo.

Para obter mais detalhes sobre os parâmetros de configuração do modelo de lançamento, consulte [Modelo de lançamento](#) no Guia do usuário do MGN.

AWS O Transform também fornece um link para o ID do modelo de lançamento do Amazon EC2 associado ao modelo de lançamento, permitindo que você altere atributos adicionais do modelo de lançamento do Amazon EC2. Para editar o modelo de lançamento do Amazon EC2, siga as instruções no modelo de [lançamento no Guia do usuário](#) do MGN.

Estratégia de atribuição de IP

Você escolhe como os endereços IP são atribuídos aos seus servidores migrados:

- IP estático — O endereço IP do servidor de origem é mantido. Se a transformação do CIDR for necessária, o AWS Transform converterá automaticamente o endereço IP para corresponder ao novo CIDR.
- IP dinâmico (DHCP) — Cada servidor recebe um novo endereço IP do pool IP da sub-rede.

 Note

Se você selecionou a estratégia de mapeamento de grupos de segurança do MAP durante a migração da rede, somente a atribuição de IP estático estará disponível. Para obter mais detalhes, consulte [Mapeamento de grupos de segurança](#).

Etapa 2: validar e confirmar o inventário

Antes de carregar os dados do servidor no MGN, o AWS Transform prepara o arquivo de inventário para sua análise. Você pode baixar o arquivo no formato CSV ou XLSX, revisar as configurações do servidor e fazer alterações, se necessário.

O arquivo de inventário inclui detalhes como nomes de servidores, sistemas operacionais, recomendações de tipo de instância do Amazon EC2, sub-redes de destino, grupos de segurança, atribuições de IP e opções de licenciamento. Os campos obrigatórios incluem:

- Informações do servidor — nome do servidor, VMID e especificações da fonte.
- Atribuição de ondas — agrupamento de ondas de migração.
- Agrupamento de aplicativos — Associações lógicas de aplicativos.
- Configuração de destino — Conta de destino, região e tipo de instância do Amazon EC2.
- Configuração de rede — Sub-rede de destino e grupos de segurança.

Você pode modificar o arquivo para ajustar as configurações do Amazon EC2, alterar as opções de licenciamento do sistema operacional (BYOL ou Licença incluída) e atualizar as configurações de localização.

Depois de revisar o inventário, você pode aceitá-lo conforme mostrado ou fazer upload de uma versão modificada. AWS Em seguida, o Transform carrega os dados no MGN, que cria registros do servidor de origem para cada servidor na onda.

 Note

Não remova as colunas nem altere os cabeçalhos das colunas no arquivo de inventário. AWS O Transform exige que a estrutura original do arquivo processe os dados corretamente.

Note

AWS A transformação permite uma importação para um determinado alvo Conta da AWS e um alvo por Região da AWS vez. Se você trabalha em mais de uma onda simultaneamente, ou se há mais de uma tarefa de migração em execução com a mesma conta de destino, você deve aguardar a conclusão de uma importação antes de poder realizar outra importação em uma onda ou tarefa diferente.

Você pode controlar as opções de licenciamento do sistema operacional (BYOL ou Licença incluída) e a locação especificando a configuração nas colunas do arquivo de inventário e. `mgn:launch:placement:operating-system-licensing`
`mgn:launch:placement:tenancy` Para obter mais informações, consulte [Importar parâmetros](#) no Guia do usuário do MGN.

Etapa 3: implantar agentes de replicação

Para começar a replicar dados de seus servidores de origem para AWS, você instala o Agente de AWS Replicação em cada servidor de origem. AWS O Transform oferece três métodos de instalação:

- Ferramentas organizacionais — Use as ferramentas de implantação existentes da sua organização (como SCCM, Ansible ou Chef) para instalar agentes em seus servidores. AWS O Transform fornece aos comandos de instalação parâmetros adicionais para instalação silenciosa `--no-prompt` `--aws-access-key-id`, incluindo `--aws-secret-access-key`, `--aws-session-token` e.
- Conector MGN — Use um conector MGN para automatizar a instalação do agente. O conector se conecta às máquinas de origem via SSH (Linux) ou WinRM (Windows) e instala o agente de replicação automaticamente. Uma vez configurado, um conector pode ser reutilizado em várias ondas e alvos Contas da AWS diferentes. Para obter mais informações sobre o conector MGN, consulte [Configurar o conector MGN](#) no Guia do usuário do MGN.

Note

Antes de usar o conector MGN com o AWS Transform, você deve marcar a instância gerenciada do conector no AWS Systems Manager Fleet Manager com as seguintes tags:

- Chave: `CreatedFor` Valor: `AWSTransform`
- Chave: `ATWorkspace` Valor: *workspace-id*

Para marcar a instância gerenciada, abra o AWS Systems Manager console, navegue até o Fleet Manager em Node Tools, escolha a instância gerenciada do seu conector MGN e aplique as tags acima. Encontre o ID do seu espaço de trabalho na URL do aplicativo web AWS Transform: `https://.../workspace/workspace-id/job/job-id`.

- Instalação manual — Instale o agente diretamente em cada servidor de origem. Esse método requer acesso direto a cada servidor, mas oferece controle total sobre o processo de instalação.

AWS Configuração do conector Transform MGN

O conector AWS Transform MGN automatiza a implantação de agentes de replicação em seus servidores de origem. O conector é um cliente leve implantado em uma máquina Linux dedicada em seu ambiente local. Ele se conecta aos servidores de origem via SSH (Linux) ou WinRM (Windows) para instalar e configurar agentes de replicação, eliminando a necessidade de coordenar manualmente vários serviços. AWS

Como o conector funciona

O conector opera por meio dos seguintes componentes:

- Cliente Connector — Implantado em uma máquina Linux dedicada em seu ambiente.
- Agente SSM — Instalado na mesma máquina para permitir a comunicação segura com AWS.
- Ativação híbrida SSM — vincula a máquina conectora ao AWS Systems Manager para execução segura de comandos.
- Gerenciamento de credenciais — Recupera as credenciais do servidor de origem do Secrets Manager AWS .

Quando você implanta agentes, o AWS Transform envia um documento SSM para a máquina conectora. Em seguida, o conector recupera as credenciais do servidor de origem do AWS Secrets Manager, estabelece uma conexão com cada servidor de origem, valida se o servidor de origem atende aos pré-requisitos, instala e configura o agente de replicação e verifica se a instalação foi bem-sucedida.

Requisitos da máquina conectora

Requisito	Detalhes
Sistema operacional	Sistema operacional Linux compatível. Para ver a lista completa, consulte os pré-requisitos do conector MGN no Guia do usuário do MGN.
Acesso à rede	Deve alcançar todos os servidores de origem (Linux sobre SSH, Windows sobre WinRM)
Conectividade com a Internet	HTTPS (443) de saída para AWS endpoints (Systems Manager, Secrets Manager, MGN)
Espaço em disco	Mínimo de 200 MB grátis
Permissões	Acesso root ou sudo

Note

O conector deve estar instalado em uma máquina Linux, mas pode implantar agentes nos servidores de origem Linux e Windows.

Processo de configuração

AWS O Transform orienta você nas seguintes etapas para configurar o conector:

Etapas 1: configuração do conector

Forneça um nome para seu conector ou use o nome padrão gerado automaticamente. O conector pode ser instalado na conta de gerenciamento ou em uma conta de administrador delegado no MGN. Para migrações de várias contas, o conector pode implantar agentes em servidores em todas as contas dos membros.

Etapas 2: configuração do AWS recurso

AWS O Transform abre uma página de configuração que é executada no seu navegador usando suas AWS credenciais. Você deve estar conectado ao AWS Management Console com sua conta de

gerenciamento ou sua conta de administrador delegado. Essa deve ser a mesma conta à qual seu conector de destino do AWS Transform está conectado.

A página de configuração cria automaticamente os seguintes recursos:

- Funções do IAM (criadas de forma idêntica — ignoradas se já existirem):
 - `AWSApplicationMigrationConnectorManagementRole`— Usado durante a instalação do agente para acessar as credenciais.
 - `AWSApplicationMigrationConnectorSharingRole_<ACCOUNT-ID>`— Contém permissões para instalação do agente.
- Ativação híbrida SSM — período de expiração de 30 dias. Vincula a máquina conectora ao AWS Systems Manager e gera credenciais de ativação seguras.

Como alternativa, você pode baixar um CloudFormation modelo da página de configuração para implantar você mesmo as funções do IAM.

A página de configuração gera um comando de instalação de uma linha com todas as credenciais e configurações necessárias.

Important

Mantenha a página de configuração aberta até que a instalação seja concluída. Fechá-lo exigirá a reinicialização do processo. Todas as credenciais existem somente no seu navegador e não são armazenadas pelo AWS Transform.

Etapa 3: instalação do conector

Instale o conector em uma máquina Linux em seu ambiente:

1. Copie o link de instalação da página de configuração.
2. SSH na máquina Linux escolhida.
3. Cole e execute o comando de instalação.
4. Aguarde a conclusão da instalação (normalmente de 2 a 3 minutos).

Etapa 4: conectar servidores de origem

Após a instalação, o AWS Transform identifica todos os servidores de origem que pertencem à onda atual e os conecta automaticamente ao conector MGN.

Etapa 5: configurar as credenciais

Forneça ARNs do AWS Secrets Manager para suas credenciais do servidor de origem. AWS O Transform oferece três opções de configuração de credenciais:

- Segredo único para servidores Linux — Um segredo compartilhado contendo chaves SSH ou username/password para todos os servidores de origem Linux.
- Segredo único para servidores Windows — Um segredo compartilhado contendo nome de usuário e senha para todos os servidores de origem do Windows.
- Vários segredos por servidor — Segredos diferentes por servidor ou grupo de servidores. Use isso quando os servidores tiverem credenciais diferentes. AWS O Transform gera um arquivo CSV pré-preenchido com sua lista de servidores. Você preenche a `secret_arn` coluna de cada servidor e carrega o arquivo completo.

Note

Você pode combinar as opções de segredo único do Linux e do Windows se tiver os dois tipos de servidor com um segredo compartilhado cada. A opção de segredos por servidor é mutuamente exclusiva com as opções de segredo único.

Formato secreto da credencial. Para ler mais sobre isso, consulte as [credenciais do conector MGN no Guia](#) do usuário do MGN:

```
{
  "WinConnectionProtocol": "HTTPS",
  "WinUserName": "windows_username",
  "WinPassword": "windows_password",
  "LinuxUserName": "linux_username",
  "LinuxPrivateKey": "linux_private_key",
  "LinuxHostKeyValidation": false
}
```

Implantação do agente

Depois que as credenciais são configuradas e verificadas, o AWS Transform implanta agentes de replicação em seus servidores de origem. Você pode implantar em todos os servidores na onda atual ou selecionar servidores específicos.

O processo de implantação de cada servidor:

1. AWS O Transform envia comandos de implantação para o conector via SSM.
2. O conector recupera as credenciais do AWS Secrets Manager.
3. O conector se conecta ao servidor de origem usando as credenciais configuradas.
4. O conector valida se o servidor de origem atende a todos os pré-requisitos necessários para executar o agente de replicação.
5. O conector instala e configura o agente de replicação.
6. O conector verifica se a instalação e a conectividade foram bem-sucedidas.

Você pode monitorar o progresso da implantação em tempo real com o rastreamento do status por servidor, incluindo a etapa atual da instalação, o tempo decorrido e o tempo restante estimado. Se algum servidor falhar, o AWS Transform exibirá o motivo da falha e oferecerá opções de repetição por servidor. Os servidores implantados com sucesso podem prosseguir de forma independente enquanto os servidores com falha são testados novamente.

Reutilização e ciclo de vida do conector

Ao implantar agentes para ondas subsequentes, você pode reutilizar um conector existente ou criar um novo. AWS O Transform lista todos os conectores configurados em sua conta, mostrando o nome do conector, o status (ativo ou expirado), a contagem de servidores conectados e a data de expiração da ativação híbrida.

- Conector ativo — A ativação híbrida ainda é válida. AWS O Transform verifica as funções do IAM para a nova onda e prossegue com a configuração das credenciais. Nenhuma nova ativação híbrida é necessária.
- Conector expirado — A ativação híbrida do SSM expirou. As ativações expiradas não podem ser renovadas. Você deve selecionar um conector diferente ou criar um novo.

As ativações híbridas do SSM expiram após 30 dias. A ativação é necessária somente para instalar o conector na máquina Linux. Depois que o conector estiver instalado, você poderá continuar a usá-lo

para instalar agentes de replicação nos servidores de origem mesmo após a expiração da ativação. Se precisar instalar o conector em uma nova máquina após a expiração da ativação, você precisará criar um novo conector por meio do processo de configuração.

Instalação manual do agente

Para a instalação manual, primeiro você gera AWS as credenciais (temporárias ou permanentes) e depois instala o agente em cada servidor de origem.

Opções de credencial:

- Credenciais temporárias (recomendado) — Crie uma função do IAM com a política `AWSApplicationMigrationAgentInstallationPolicy` gerenciada e use-a `aws sts assume-role` para gerar credenciais temporárias. Para ler mais sobre isso, consulte [Permissões de instalação do agente](#) no Guia do usuário do MGN.
- Credenciais permanentes — Crie um usuário do IAM com a política `AWSApplicationMigrationAgentInstallationPolicy` gerenciada e gere uma chave de acesso.

Etapas de instalação:

Para servidores Linux, baixe e execute o instalador:

```
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
```

Para servidores Windows, baixe e execute o instalador apropriado usando PowerShell como administrador:

```
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

O parâmetro `--user-provided-id` é obrigatório. *server-identifier* Substitua pelo valor exato da `mgn:server:user-provided-id` coluna em seu arquivo de inventário. Esse identificador vincula o servidor físico ao registro do servidor de origem MGN.

Para obter mais informações sobre a instalação do agente, consulte o [agente Linux](#) e o [agente do Windows](#) no Guia do usuário do MGN.

Após a instalação, o AWS Transform verifica se todos os agentes estão conectados com êxito, verificando se os servidores mostram um estado de replicação de `INITIATING` ou `INITIAL_SYNC`.

 Note

AWS O Transform não oferece suporte à replicação sem agente do MGN. Para obter informações sobre replicação sem agente, consulte [Visão geral da replicação sem agente no Guia do usuário do MGN](#).

 Note

Você deve instalar o agente de replicação em todos os servidores em uma onda. Desconecte e archive servidores nos quais você não instala o agente de replicação. Você pode usar o `disconnect-from-service` comando para desconectar servidores e o `mark-as-archived` comando para arquivar servidores desconectados. O comando de arquivamento só funciona para servidores de origem cujo estado do ciclo de vida é `DISCONNECTED`.

Para cotas relacionadas à replicação, consulte os [limites de cota de serviço do MGN](#) no Guia do usuário do MGN.

Etapa 4: replicação de dados

Depois que os agentes de replicação são instalados, a replicação de dados começa automaticamente. AWS O Transform usa replicação contínua em nível de bloco para sincronizar dados dos servidores de origem com o AWS

O processo de replicação consiste em duas fases:

- Sincronização inicial — Uma cópia completa dos dados do servidor de origem para AWS o. Os dados são armazenados como snapshots do Amazon Elastic Block Store (Amazon EBS) ou em volumes do Amazon FSx NetApp for ONTAP (FSx for ONTAP) na conta de destino, dependendo do tipo de armazenamento de destino configurado. Para obter mais informações, consulte [Tipo de armazenamento de destino](#) no Guia do usuário do MGN. A duração depende do volume de dados e da largura de banda da rede.
- Replicação contínua — sincronização contínua dos blocos alterados com impacto mínimo no desempenho do servidor de origem. Mantém uma cópia atualizada em AWS.

Os servidores de replicação são instâncias temporárias do Amazon EC2 implantadas na sub-rede da área de armazenamento. Eles recebem dados replicados dos servidores de origem e são gerenciados automaticamente pela MGN. Para ler mais sobre isso, consulte [Configurações do servidor de replicação no Guia](#) do usuário do MGN.

AWS O Transform monitora o progresso da replicação e fornece atualizações de status, incluindo status da replicação, atraso na replicação (a diferença de tempo entre os dados de origem e replicados) e o uso da largura de banda.

Durante a replicação, cada servidor passa pelos seguintes estados:

- Não está pronto — O servidor está passando pelo processo de sincronização inicial e ainda não está pronto para o teste.
- Pronto para o teste — o servidor foi adicionado com sucesso e a replicação de dados foi iniciada. Agora, instâncias de teste ou transição podem ser iniciadas.

Depois que todos os servidores da onda tiverem progredido além do NOT_READY estado, a fase de replicação de dados estará concluída e você poderá prosseguir com os testes.

Você pode controlar a replicação de servidores individuais ou de toda a onda a qualquer momento:

- Pausar a replicação — Pausa temporariamente a replicação para servidores específicos ou para toda a onda.
- Retomar a replicação — retoma a replicação pausada anteriormente.
- Interrompa a replicação — interrompa permanentemente a replicação. A replicação interrompida pode ser reiniciada, mas começa na sincronização inicial.

Etapa 5: Teste

Depois que a replicação de dados for concluída, você poderá iniciar instâncias de teste para validar seus servidores migrados antes de realizar a transição final. Para ler mais sobre isso, consulte [Iniciar instâncias de teste](#) no Guia do usuário do MGN. AWS O Transform oferece suporte a duas opções de teste:

- Teste de onda completa — Inicie instâncias de teste para todos os servidores da onda.
- Teste seletivo — Inicie instâncias de teste para servidores específicos que você seleciona fornecendo suas IDs fornecidas pelo usuário a partir do arquivo de inventário.

AWS O Transform inicia instâncias do Amazon EC2 a partir dos dados replicados e fornece os IDs das instâncias para que você possa se conectar e validar as instâncias de teste. Após o teste, você pode:

- Prossiga com a transição se o teste for bem-sucedido.
- Inicie novas instâncias de teste para testar novamente.
- Encerre as instâncias de teste e resolva quaisquer problemas antes de testar novamente.

Etapa 5b: Marcar os aplicativos como prontos para a transição

Depois que o teste estiver concluído e você estiver satisfeito com os resultados, marque seus aplicativos como prontos para transferência. AWS O Transform analisa o status de replicação de cada aplicativo e resolve todos os alertas de replicação antes de permitir que você continue. Somente aplicativos com um status de replicação limpo podem ser marcados para substituição.

Etapa 6: transição

A transição é a etapa final da migração para a qual suas cargas de trabalho de produção são movidas. Para ler mais sobre isso, consulte [Iniciar instâncias de transição no Guia](#) do usuário do MGN. Semelhante aos testes, o AWS Transform oferece suporte à transição de onda completa ou à transferência seletiva para servidores específicos.

Durante a transição, o AWS Transform inicia instâncias do Amazon EC2 a partir dos dados replicados mais recentes e fornece os IDs de instância para cada servidor. Depois de verificar as instâncias de transição, você finaliza a transição, o que interrompe a replicação contínua da máquina de origem.

O processo de transição inclui as seguintes etapas:

1. Inicie instâncias de transição — O AWS Transform inicia instâncias do Amazon EC2 para os servidores selecionados. Você pode escolher a transição de onda completa ou a transição seletiva.
2. Verifique as instâncias de transição — Conecte-se às instâncias iniciadas e verifique se elas estão funcionando corretamente.
3. Finalizar a transição — Confirme a transição para interromper a replicação da máquina de origem. Você pode finalizar todos os servidores da onda ou selecionar servidores específicos. A finalização impede que os agentes de replicação enviem dados, remove os agentes de replicação dos servidores de origem e bloqueia o estado do ciclo de vida do servidor. Essa ação não pode ser facilmente desfeita. Para ler mais sobre isso, consulte [Finalizar a transição no Guia do usuário do MGN](#).
4. Servidores de origem de arquivamento (opcional) — Após a finalização, você pode marcar os servidores de origem como arquivados para liberar a cota do servidor de origem em sua conta.

 Important

A finalização da transição interrompe a replicação contínua da máquina de origem. Verifique se você verificou suas instâncias de transição antes de finalizar.

 Note

O tempo de inatividade ocorre entre o desligamento da origem e a disponibilidade da instância de transição. Planeje sua janela de transição adequadamente.

Estados do ciclo de vida do servidor

Durante a migração, cada servidor passa pelos seguintes estados do ciclo de vida. Para ler mais sobre isso, consulte o [ciclo de vida do servidor de origem no Guia do usuário do MGN](#).

- Não está pronto — O servidor está passando pelo processo de sincronização inicial e ainda não está pronto para o teste.

- Pronto para o teste — a replicação de dados foi iniciada e as instâncias de teste ou transferência podem ser iniciadas.
- Teste em andamento — Uma instância de teste está sendo iniciada no momento.
- Pronto para transferência — O servidor foi testado e está pronto para transferência.
- Transferência em andamento — Uma instância de transição está sendo executada no momento.
- Transição concluída — O servidor foi transferido. Todos os dados foram migrados para a instância de AWS transferência.
- Desconectado — O servidor foi desconectado do MGN.

Você pode perguntar ao AWS Transform sobre o status dos seus servidores a qualquer momento durante a migração. O AWS Transform fornece uma tabela interativa de status do wave que exibe todas as informações relevantes do servidor, incluindo o ciclo de vida da migração, o status da replicação e as próximas etapas recomendadas. Você também pode perguntar em linguagem natural, por exemplo:

- Qual é o status dos meus servidores?
- Qual é o status da minha onda?
- Qual é o status da etapa em que estou atualmente?

Durante a migração do Wave, você pode pedir ao AWS Transform que atualize ou altere o status de servidores individuais. Por exemplo, se 9 em cada 10 servidores em seu wave passaram na fase de teste, mas um falhou, você pode permitir que o AWS Transform continue movendo os 9 servidores para a próxima fase enquanto executa novamente o teste no servidor com falha.

Aprovações de implantação

Algumas operações de migração exigem aprovação explícita antes da execução. Quando uma operação exige aprovação, o AWS Transform encaminha a solicitação para aprovadores autorizados por meio da guia Aprovações. Somente usuários com a função de administrador no AWS Transform podem aprovar solicitações de implantação. As implantações prosseguem somente após o recebimento da confirmação.

Notas da versão

As notas de versão a seguir abrangem as alterações mais recentes do [Migrações \(incluindo VMware\)](#). Para regiões de AWS transformação compatíveis, consulte [Regiões suportadas](#). Para regiões de destino compatíveis, consulte a [página de configuração do conector de conta](#).

Junho de 2026

- AWS O Transform for migrations agora oferece suporte à localização. Você pode alterar o idioma de exibição do aplicativo Web ao trabalhar com fluxos de trabalho de migração. [Saiba mais sobre as configurações de idioma](#).
- AWS O Transform agora permite que você defina suas configurações de replicação e de inicialização para sua migração. Você pode definir a configuração de acordo com sua conta de destino ou em servidores de origem específicos. [Saiba mais sobre as configurações de replicação e inicialização](#).
- AWS O Transform agora permite que você anexe interfaces de rede elásticas (ENIs) existentes ao seu modelo de lançamento. Você pode marcar ENIs em sua conta de destino para que estejam disponíveis para uso quando as instâncias forem lançadas. [Saiba mais sobre a marcação de recursos de rede](#).
- AWS O Transform for migrations agora oferece suporte a todas as regiões AWS comerciais como alvos de migração, exceto Oriente Médio (Bahrein) e Oriente Médio (Emirados Árabes Unidos). [Saiba mais sobre as regiões-alvo suportadas](#).

Maio de 2026

- AWS O Transform agora detecta VPCs existentes em sua conta de destino durante a análise da migração da rede. Você pode ver as VPCs existentes junto com as VPCs mapeadas, identificar conflitos de CIDR e resolvê-los antes da implantação. [Saiba mais sobre a detecção de VPC existente](#).
- AWS O Transform oferece suporte à replataforma de repositórios de código-fonte em contêineres durante a migração para o. AWS [Saiba mais sobre containerização](#).

Abril de 2026

- Foi adicionada a criação de landing zone diretamente nos fluxos de trabalho de migração. AWS O Transform verifica uma base existente, recomenda estruturas de unidades organizacionais (OU) e contas de destino e oferece implantação automatizada ou saída de infraestrutura como código (IaC) (formatos CloudFormation, AWS CDK, ou Landing Zone Accelerator (LZA)). [Saiba mais sobre a criação de landing zone](#).
- Foi adicionado suporte para DHCP com mapeamento de grupos de segurança durante a migração da rede. [Saiba mais sobre a criação de grupos de segurança](#).

Março de 2026

- Foram adicionadas APIs públicas para migração de rede, permitindo o acesso programático e de parceiros aos recursos de migração de rede. Veja a [referência da API de migração de rede](#).

Fevereiro de 2026

- A migração de rede agora suporta a ingestão de [arquivos de configuração de firewall ou Software-Defined rede \(SDN\)](#) sem exigir dados de descoberta do [RVTools](#). Você pode usar arquivos de configuração de firewall ou SDN de forma independente ou combiná-los com as exportações do RVTools.

Janeiro de 2026

- Foi adicionado suporte à marcação do [Migration Acceleration Program \(MAP\)](#) e à [marcação definida pelo usuário](#) em elementos de migração de rede, permitindo que você acompanhe os recursos de migração para fins organizacionais e de crédito do MAP.

Dezembro de 2025

- Foi adicionada uma nova [experiência de migração](#) com fluxo de trabalho redesenhado e usabilidade aprimorada. Para obter mais informações, consulte [Acelerando a migração da VMware: a nova experiência da AWS Transform](#).
- Foi adicionada a configuração de [rede Landing Zone Accelerator \(LZA\) para configuração automática da zona de pouso](#).

- Foi adicionado suporte para [várias AWS contas de destino](#) na execução da migração, permitindo que você migre cargas de trabalho entre contas.
- Foi adicionado suporte à migração de rede para os formatos de origem [Cisco ACI, Palo Alto e ModelizeIT](#). FortiGate

Outubro de 2025

- Expandiu a execução da migração para [16 regiões-alvo](#) com a adição da Ásia-Pacífico (Osaka).

Setembro de 2025

- Foi adicionado suporte para configuração de licenciamento em [ondas de rehostagem](#), permitindo que você especifique opções de Bring Your Own License (BYOL) ou opções de licença incluída por onda.
- Foi adicionado suporte ao [Terraform na migração de rede](#), permitindo que você implante a infraestrutura de rede usando modelos do Terraform.
- Foi adicionado suporte para atualizar a configuração da sub-rede de replicação, removendo a necessidade de uma VPC padrão na conta de destino.

Agosto de 2025

- Expandiu a execução da migração (migração de rede e rehostagem) para [15 regiões-alvo](#) com a adição do Leste dos EUA (Ohio), Europa (Estocolmo) e Europa (Irlanda).
- Foram adicionados [recursos flexíveis de intervalo CIDR](#) para migração de rede, permitindo que você personalize intervalos de endereços IP durante a implantação da rede.

Maio de 2025

- Lançamento inicial do serviço [Migrações \(incluindo VMware\)](#), fornecendo recursos de migração de ponta a ponta, incluindo [descoberta](#), avaliação, [planejamento de migração](#), [migração](#) de rede e rehostagem do servidor.
- Suportou a execução da migração em 12 [regiões-alvo](#): Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Canadá (Central), América do Sul (São Paulo), Europa (Frankfurt), Europa

(Londres), Europa (Paris), Ásia-Pacífico (Mumbai), Ásia-Pacífico (Seul), Ásia-Pacífico (Tóquio), Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Sydney).

Containerização do código-fonte

AWS O Transform oferece suporte à replataforma de aplicativos em contêineres durante a migração para o. AWS Este capítulo descreve os recursos de IA agente do AWS Transform para automatizar a containerização do seu código-fonte. Você pode migrar e modernizar paralelamente, reduzindo o tempo e a complexidade da migração de arquiteturas locais para arquiteturas nativas em nuvem. Você pode containerizar o código-fonte de GitHub arquivos Bitbucket ou.zip GitLab, gerar imagens do Docker, publicar no Amazon Elastic Container Registry (Amazon ECR) e implantar no Amazon Elastic Container Service (Amazon ECS) ou no Amazon Elastic Kubernetes Service (Amazon EKS). Isso coloca a containerização no mesmo fluxo de trabalho que você usa para planejar e executar migrações de rehostagem.

Note

A containerização do código-fonte foi projetada para aplicativos que ainda não estão em contêineres. Ele exige acesso ao código-fonte do seu aplicativo e não oferece suporte à migração de cargas de trabalho em contêineres existentes. Para migrar contêineres existentes para AWS, use métodos de implantação padrão para o Amazon Elastic Container Service ou o Amazon Elastic Kubernetes Service.

Capacidades e características-chave

AWS O Transform oferece os seguintes recursos para armazenar seus aplicativos em contêineres.

- AI-driven análise de código-fonte — analisa o código-fonte do aplicativo e gera automaticamente artefatos do Docker, incluindo Dockerfiles e arquivos de configuração relacionados.
- Criação e publicação de imagens de contêineres — Cria e testa imagens de contêineres usando compilações do AI-driven Docker e as publica no Amazon Elastic Container Registry com verificação automática de vulnerabilidades.
- Infraestrutura como geração de código — Gera infraestrutura de implantação para o Amazon Elastic Kubernetes Service (Helm charts) ou o Amazon Elastic Container Service (módulos Terraform), com validação automatizada e verificação de segurança.
- Suporte a dependências privadas — Opcionalmente, você pode configurar AWS CodeArtifact repositórios (Maven, PyPI, npm) e imagens básicas privadas do Amazon ECR como fontes de dependência para suas compilações.

- Teste iterativo e implantação de transição — implanta a infraestrutura de teste para validação e, em seguida, implanta a infraestrutura finalizada para transição da produção.

Como funciona a containerização

AWS O Transform usa um AI-powered agente para guiá-lo pelo processo de containerização em um fluxo de trabalho baseado em bate-papo. AWS O Transform coordena tarefas especializadas, como análise de código-fonte, geração de imagens do Docker e criação de infraestrutura. Em pontos-chave do fluxo de trabalho, você revisa e aprova a saída antes de continuar.

Você acessa a containerização do código-fonte criando um trabalho de migração do VMware. Dentro do trabalho, você pode executar a containerização como um fluxo de trabalho independente ou como parte de uma migração de ponta a ponta quando a estratégia de migração de uma onda está definida para ser containerizada. Para obter mais informações sobre a migração do VMware, consulte [Migrações \(incluindo VMware\)](#)

Pré-requisitos

Antes de começar, verifique se você tem:

- Um espaço de trabalho AWS Transform. Para obter informações sobre como obter um espaço de trabalho, consulte [Introdução](#).
- O código-fonte do seu aplicativo em um repositório Git acessível por meio AWS CodeConnections de ou empacotado como arquivos zip para upload. Arquivos individuais não devem exceder 1 GB e o tamanho total de todo o código-fonte não deve exceder 8 GB.
- (Opcional) Um repositório Amazon ECR para publicação de imagens de contêineres. Você pode configurar o acesso ao Amazon ECR posteriormente no fluxo de trabalho quando estiver pronto para publicar.
- Para implantações do Amazon EKS: um cluster existente do Amazon EKS ou permissões para criar a infraestrutura necessária.
- Para implantações do Amazon ECS: Permissões para criar clusters, serviços e recursos relacionados do Amazon ECS usando o Terraform,, ou. AWS CloudFormation AWS Cloud Development Kit (AWS CDK)

Fluxo de trabalho de containerização

O fluxo de trabalho de containerização consiste nas seguintes etapas. O agente AWS Transform orienta você em cada etapa da interface de bate-papo.

1. [the section called “Etapa 1: isenção de responsabilidade de segurança”](#)— Revise e aceite a isenção de responsabilidade de segurança.
2. [the section called “Etapa 2: clonar o código-fonte”](#)— Forneça o código-fonte do seu aplicativo.
3. [the section called “Etapa 3: Containerizar”](#)— O agente de IA analisa seu código e gera artefatos do Docker.
4. [the section called “Etapa 4: revisar os artefatos”](#)— Analise os artefatos gerados e aprove as alterações no código.
5. [the section called “Etapa 5: publicar imagens”](#)— Publique imagens de contêineres no Amazon ECR.
6. [the section called “Etapa 6: Gerar IaC”](#)— Gere modelos de implantação do Amazon EKS ou do Amazon ECS.
7. [the section called “Etapa 7: implantar a infraestrutura de teste”](#)— Implemente e valide a infraestrutura de teste.
8. [the section called “Etapa 8: Limpar a infraestrutura de teste”](#)— Elimine os recursos de teste.
9. [the section called “Etapa 9: implantar a infraestrutura de transição”](#)— Implantar infraestrutura de produção.

Iniciando um trabalho de containerização

Para colocar seus aplicativos em contêineres, primeiro você cria um trabalho de migração do VMware em seu espaço de trabalho Transform. AWS De dentro do trabalho, você pode optar por executar um fluxo de trabalho autônomo de containerização ou um fluxo de migração de ponta a ponta que inclua containerização.

- Containerização autônoma — Containerize seu código-fonte sem realizar uma migração completa do VMware. Escolha essa opção quando quiser colocar aplicativos em contêineres independentemente de qualquer migração de infraestrutura.
- End-to-end migração com containerização — execute todo o fluxo de trabalho de migração da VMware com uma estratégia de migração de contêineres atribuída a uma ou mais ondas. O fluxo

de trabalho de containerização é executado como parte da migração dessas ondas. Para obter mais informações sobre a migração do VMware, consulte [Migrações \(incluindo VMware\)](#)

Para iniciar um trabalho de containerização

1. Na página inicial do seu espaço de trabalho, escolha Criar um trabalho.
2. Escolha a migração do VMware.
3. Escolha se deseja executar um fluxo de trabalho de containerização autônomo ou um fluxo de migração de ponta a ponta que inclua containerização.
4. AWS O Transform orienta você pelas etapas do fluxo de trabalho, começando por [the section called “Etapa 1: isenção de responsabilidade de segurança”](#).

Permissões de containerização

Durante o fluxo de trabalho de containerização, o AWS Transform implanta uma função do IAM em você Conta da AWS que usa para criar imagens de contêiner e implantar infraestrutura. Você deverá revisar e aprovar a criação dessa função antes que o fluxo de trabalho continue.

A função é nomeada `AWSTransformCodeBuildExecutionRole` e implantada por meio de uma AWS CloudFormation pilha. Ela inclui as seguintes políticas gerenciadas.

Política básica

Fornece permissões básicas para o fluxo de trabalho de containerização:

- Amazon S3 — Leia e grave objetos em buckets `aws-transform-*`
- Amazon ECR — Autenticar, extrair imagens (marcadas com `Project: atx-migration`) e enviar imagens para repositórios marcados com `CreatedBy: AWSTransform`
- AWS CodeArtifact — Leia os repositórios marcados com `Project: atx-migration`, liste repositórios, obtenha tokens de autorização e leia os endpoints do repositório. Essas permissões oferecem suporte à resolução de dependências públicas e às fontes de dependência privadas configuradas durante o fluxo de trabalho.
- Amazon CloudWatch Logs — Crie grupos e streams de log e grave eventos de log para grupos de log do Amazon ECS
- AWS KMS — Descrever e descriptografar chaves (com escopo para o Amazon S3 por meio da condição de serviço)

- Amazon EC2 — Crie e gerencie interfaces de rede para projetos VPC-enabled
- AWS CodeConnections — Use conexões para acessar repositórios de código-fonte por meio do ARN configurado CodeConnections

Política de rede

Gerencia recursos de rede para aplicativos implantados:

- Elastic Load Balancing — Crie, descreva e gerencie balanceadores de carga, grupos-alvo, ouvintes e regras (marcados com) `CreatedBy: AWSTransform`
- Route 53 — Crie e gerencie zonas hospedadas e registros DNS
- AWS Cloud Map — Crie e gerencie namespaces e serviços para descoberta de serviços (marcado com) `CreatedBy: AWSTransform`

Política de armazenamento

Gerencia recursos de armazenamento para aplicativos implantados:

- Amazon S3 — Crie e gerencie buckets, incluindo criptografia, controle de versão, ciclo de vida e políticas de acesso
- Amazon EFS — Crie e gerencie sistemas de arquivos, alvos de montagem e pontos de acesso (marcados com `CreatedBy: AWSTransform`)
- Amazon EBS — Crie e gerencie volumes e snapshots (marcados com) `CreatedBy: AWSTransform`

AWS KMS política

Gerencia as operações da chave de criptografia:

- Descreva chaves, liste aliases e leia políticas de chaves
- Criptografe, descriptografe e gere chaves de dados (com escopo para Amazon Logs, Amazon EFS, CloudWatch Amazon EC2 e Amazon S3 por meio de condições de serviço)

Política do Amazon ECS

Gerencia os recursos do Amazon Elastic Container Service para implantações de contêineres:

- Crie e gerencie clusters, serviços e definições de tarefas (marcados com `CreatedBy: AWSTransform`)
- Registre e cancele o registro de definições de tarefas, execute tarefas
- Passe funções do IAM para tarefas e serviços do Amazon ECS
- Leia as informações da função do IAM e os certificados do ACM
- Descreva VPCs, sub-redes, grupos de segurança e interfaces de rede do Amazon EC2

Política do Amazon EKS

Gerencia os recursos do Amazon Elastic Kubernetes Service para implantações do Kubernetes:

- Acesse a API Kubernetes, descreva clusters e liste complementos
- Passe funções do IAM para o Amazon EKS

Note

Todas as permissões são atribuídas ao seu Conta da AWS e. Região da AWS Os recursos criados pelo AWS Transform são marcados com `CreatedBy: AWSTransform`, e as operações de gravação são restritas a recursos com essa tag, quando aplicável.

Etapa 1: revisar a isenção de responsabilidade de segurança

Antes do início do fluxo de trabalho de containerização, o AWS Transform apresenta um aviso de segurança que você deve revisar e aceitar.

O que a isenção de responsabilidade cobre

O processo de containerização requer acesso à Internet para baixar as dependências do aplicativo (como pacotes de registros públicos como npm, PyPI ou Maven Central). A isenção de responsabilidade de segurança informa que:

- Os ambientes de compilação terão acesso de saída à Internet para resolver e baixar as dependências especificadas na configuração de compilação do seu aplicativo.
- Você é responsável por analisar as dependências que seu aplicativo exige e garantir que elas atendam às políticas de segurança da sua organização.
- Opcionalmente, você pode configurar fontes de dependência privadas (como AWS CodeArtifact repositórios ou imagens básicas privadas do Amazon ECR) em uma etapa posterior para evitar o download de registros públicos.

O que você precisa fazer

Para revisar e aceitar a isenção de responsabilidade de segurança

1. Leia o aviso de segurança que o AWS Transform apresenta.
2. Aceite a isenção de responsabilidade para continuar com o fluxo de trabalho de containerização.

Depois de aceitar a isenção de responsabilidade, o AWS Transform prossegue para a próxima etapa, na qual você fornece seu código-fonte.

Note

A configuração do conector para AWS CodeConnections o Amazon ECR não é mais necessária antecipadamente. AWS O Transform solicita que você configure o acesso a esses serviços posteriormente no fluxo de trabalho, somente quando necessário. Por exemplo, você configura CodeConnections quando escolhe clonar a partir de repositórios Git e configura o acesso ao Amazon ECR quando estiver pronto para publicar imagens de contêineres.

Etapa 2: clonar o código-fonte

Nesta etapa, você fornece o código-fonte do seu aplicativo para AWS Transform. Você pode fornecer o código-fonte dos repositórios Git ou fazer o upload de arquivos zip.

Opção 1: repositórios Git

Você pode fornecer seu código-fonte dos repositórios Git. Se você ainda não configurou AWS CodeConnections, o AWS Transform solicitará que você forneça seu CodeConnections ARN neste momento. Você tem duas maneiras de especificar seus repositórios:

- Carregar um arquivo CSV — Prepare um arquivo CSV com colunas `repo_name` e `branch`. Eles `repo_name` devem estar em `owner/repo-name` formato. A `branch` coluna é opcional; deixe-a vazia para usar a ramificação padrão do repositório. Exemplo:

```
repo_name,branch
owner/my-app,main
owner/api-service,develop
owner/another-repo,
```

- Forneça detalhes do repositório no bate-papo — Informe ao AWS Transform o (s) nome (s) e ramificação (s) do repositório diretamente no bate-papo, em vez de fazer o upload de um CSV.

AWS O Transform valida se cada repositório existe e está acessível por meio de sua CodeConnections configuração e, em seguida, clona os repositórios.

Note

Arquivos individuais não devem exceder 1 GB e o tamanho total de todos os repositórios não deve exceder 8 GB. AWS Transform clona vários repositórios simultaneamente para acelerar o processamento.

Important

Aplicativos que abrangem vários repositórios não são compatíveis com a opção de clonagem do Git. Se seu aplicativo exigir código-fonte de vários repositórios, empacote-os como um arquivo zip e use a opção de upload zip em vez disso.

Opção 2: upload de arquivo zip

Se você não CodeConnections configurou ou prefere carregar seu código-fonte diretamente, você pode fazer upload de arquivos zip.

Para carregar o código-fonte como arquivos zip

1. Quando solicitado, faça upload de um arquivo zip por aplicativo. Você pode arrastar arquivos para o bate-papo ou usar o botão de anexo.
2. Cada arquivo zip deve conter o código-fonte de um aplicativo.
3. Arquivos individuais não devem exceder 1 GB e o tamanho total de todos os uploads não deve exceder 8 GB.

Opcional: configurar dependências privadas

Se seu aplicativo depender de pacotes de registros privados, você poderá configurar fontes de dependência privadas durante esta etapa. AWS O Transform é compatível com os seguintes tipos de dependência privada:

- AWS CodeArtifact repositórios — Configure repositórios Maven, PyPI ou npm hospedados em. AWS CodeArtifact AWS O Transform apresenta uma lista de repositórios disponíveis em sua conta para você selecionar.
- Imagens básicas privadas do Amazon ECR — Se seus Dockerfiles usarem imagens básicas de um repositório privado do Amazon ECR, forneça os detalhes do repositório para que o ambiente de criação possa extrair essas imagens.

Quando você configura dependências privadas, o AWS Transform solicita que você se conecte ao Conta da AWS local onde esses recursos estão hospedados. Essa configuração de conector só é necessária se você usar dependências privadas.

Confirmando as preferências de containerização

Depois que seu código-fonte estiver disponível, o AWS Transform pergunta se você tem instruções específicas sobre como a containerização deve ser feita. Opcionalmente, você pode especificar:

- Seja para gerar um novo Dockerfile ou reutilizar um existente.
- Seja para processar um serviço específico em um monorepo ou todos os serviços.

- Quaisquer outras preferências para o processo de containerização.

Os padrões são:

1. Use a imagem base do Amazon Linux 2023 (`public.ecr.aws/amazonlinux/amazonlinux:latest`).
2. Processe todos os aplicativos no repositório.
3. Reutilize um Dockerfile existente, se presente, com pequenas modificações, se necessário.

Você pode confirmar para continuar com os padrões ou fornecer instruções específicas.

Etapa 3: Containerizar

Nesta etapa, o agente AWS Transform AI analisa o código-fonte do seu aplicativo e gera artefatos do Docker. AWS O Transform examina a estrutura, as dependências e os requisitos de tempo de execução do seu aplicativo para produzir Dockerfiles apropriados e arquivos de configuração relacionados.

O que acontece durante a containerização

O agente de containerização executa as seguintes tarefas:

1. **Análise do código-fonte** — O AWS Transform examina os arquivos de projeto, as dependências, a configuração de compilação e os requisitos de tempo de execução do seu aplicativo. AWS O Transform também substitui valores codificados (como endereços IP do banco de dados ou nomes DNS), identifica variáveis de ambiente, detecta volumes e tenta redirecionar os registros para a saída padrão.
2. **Geração de Dockerfile** — Com base na análise, o AWS Transform gera um Dockerfile personalizado para seu aplicativo.
3. **Criação e teste da imagem do contêiner** — O AWS Transform cria a imagem do contêiner e executa um teste para verificar se o Dockerfile produz uma imagem funcional. Se a compilação falhar, o AWS Transform itera automaticamente no Dockerfile.
4. **Análise de segurança** — O AWS Transform verifica os artefatos gerados em busca de valores codificados, como credenciais, chaves de API ou outros dados confidenciais, e sinaliza quaisquer descobertas para sua análise.

Se você forneceu vários repositórios ou um monorepo com vários serviços, eles processarão cada serviço em paralelo.

Tipos de aplicação compatíveis

AWS O Transform oferece suporte à containerização dos seguintes tipos de aplicativos:

- .NET 7 e versões posteriores — containerização otimizada para aplicativos .NET executados na versão 7 ou posterior.
- Aplicativos gerais — Containerização para aplicativos criados com qualquer linguagem ou estrutura, incluindo Java, Python Node.js, Go e outros.
- Aplicativos sem suporte — Windows, Xcode ou qualquer ambiente de compilação proprietário não é suportado.

O que você precisa fazer

Essa etapa é executada automaticamente. AWS O Transform exibe atualizações de progresso à medida que analisa e armazena cada aplicativo em contêineres. Se o AWS Transform encontrar problemas, ele poderá solicitar esclarecimentos ou informações adicionais.

Quando a containerização estiver concluída, o AWS Transform passa para a próxima etapa, na qual você revisa os artefatos gerados. As saídas são salvas no Artifact Store.

Etapa 4: revisar artefatos do Docker e alterações de código

Nesta etapa, você revisa os artefatos do Docker e as alterações de código que o AWS Transform gerou durante a containerização.

Revisando as alterações dos repositórios Git

Se você forneceu o código-fonte dos repositórios Git, o AWS Transform confirma as alterações de containerização em uma nova ramificação em cada repositório. Se você tiver vários repositórios, o AWS Transform apresentará todas as alterações em um lote para análise consolidada.

Para revisar e aprovar alterações

1. Analise os links de comparação de código fornecidos pelo AWS Transform. Cada diff mostra todos os arquivos que foram adicionados ou modificados, incluindo Dockerfiles, arquivos de configuração e quaisquer alterações no código-fonte.

2. Quando o AWS Transform apresentar a caixa de diálogo de aprovação, aprove ou rejeite as alterações. Para vários repositórios, você aprova todas as alterações em uma única operação em lote.
3. Se você aprovar, o AWS Transform enviará as alterações para as novas ramificações em seus repositórios.
4. Confirme se você está pronto para prosseguir para a próxima etapa.

Analizando as alterações dos uploads de zip

Se você fez upload do código-fonte como arquivos zip, o AWS Transform fornece links de download para os artefatos em contêineres. Baixe e revise os artefatos, que incluem os Dockerfiles gerados e quaisquer modificações no código-fonte.

Solicitando alterações

Se os artefatos gerados precisarem de modificações, você pode fornecer feedback para que o AWS Transform reinicie a etapa de containerização com suas instruções atualizadas e gere novos artefatos para sua análise.

Etapa 5: publicar imagens

Nesta etapa, o AWS Transform publica suas imagens de contêiner no Amazon Elastic Container Registry. Se você ainda não configurou o acesso ao Amazon ECR, o AWS Transform solicitará que você forneça os detalhes do seu repositório Amazon ECR neste momento.

O que acontece durante a publicação

AWS O Transform executa as seguintes tarefas para cada imagem de contêiner:

1. Configuração do conector — Se você ainda não configurou o acesso ao Amazon ECR, o AWS Transform apresenta um formulário de conector em que você fornece o ARN do seu repositório Amazon ECR e se conecta ao seu. Conta da AWS
2. Solicitação de aprovação — O AWS Transform apresenta a lista de imagens a serem publicadas e solicita sua aprovação. Você pode aprovar ou rejeitar a operação de publicação.
3. Envio de imagem — Após a aprovação, o AWS Transform publica as imagens do contêiner no seu repositório Amazon ECR usando. Se você tiver vários serviços, o AWS Transform publica todas as imagens em uma única operação em lote.

4. **Análise de vulnerabilidades** — O Amazon ECR verifica automaticamente as imagens publicadas em busca de vulnerabilidades conhecidas. AWS O Transform relata os resultados do escaneamento. Para uma análise mais abrangente, habilite o escaneamento aprimorado AWS do ECR e o monitoramento AWS GuardDuty de tempo de execução.

 Note

A publicação de imagens é executada de forma assíncrona usando. Se sua sessão for interrompida durante a publicação, o AWS Transform recuperará automaticamente a operação quando você se reconectar.

O que você precisa fazer

- Revise a lista de imagens a serem publicadas.
- Aprovar ou rejeitar a operação de publicação. Se você rejeitar, o AWS Transform ignorará a publicação de imagens e você poderá prosseguir para a próxima etapa sem as imagens publicadas.
- Analise os resultados da verificação de vulnerabilidade após a conclusão da publicação.

Após a publicação, o AWS Transform fornece os URIs de imagem que são usados nas etapas de implantação da infraestrutura.

Etapa 6: gerar infraestrutura como código

Nesta etapa, o AWS Transform gera modelos de AWS infraestrutura para implantar seu aplicativo em contêineres. Você escolhe entre o Amazon Elastic Kubernetes Service e o Amazon Elastic Container Service como sua plataforma de destino.

Amazon Elastic Kubernetes Service (Kubernetes)

Se você escolher o Amazon EKS, o AWS Transform gera gráficos do Helm com manifestos do Kubernetes para seu aplicativo. Os modelos gerados incluem:

- Implantações e serviços
- Regras de entrada

- ConfigMaps e SecretProviderClass recursos
- Contas de serviço
- Reivindicações de volume persistentes (EBS e EFS)
- Registros DNS do Route 53
- Configurações de verificação de saúde

Opcional: CloudWatch registro

AWS O Transform pergunta se você deseja incluir o CloudWatch registro em sua implantação do Amazon EKS. Se você optar por participar, o AWS Transform gera uma DaemonSet configuração de bits fluentes que coleta os registros do pod e os envia para CloudWatch o Logs.

Se você escolher o CloudWatch registro, o administrador do cluster deverá preencher os seguintes pré-requisitos antes da implantação:

1. Crie o `amazon-cloudwatch` namespace no cluster.
2. Crie uma função do IAM para a conta de serviço do Fluent Bit com permissões de gravação de CloudWatch registros. Você é solicitado a fornecer o ARN da função durante a implantação.

Amazon Elastic Container Service (Terraform)

Se você escolher o Amazon ECS, o AWS Transform gera módulos do Terraform para implantar seu aplicativo. Os modelos gerados incluem:

- Cluster do ECS
- Serviço ECS com definições de tarefas
- Application Load Balancer com registro de acesso
- Amazon EFS para armazenamento persistente
- Zonas hospedadas privadas para descoberta de serviços
- Configurações de verificação de saúde

Validação automatizada e verificação de segurança

AWS O Transform valida automaticamente os modelos de infraestrutura gerados antes de apresentá-los a você. A validação inclui:

- Para Terraform: `terraform fmt` e para verificar `terraform validate` a exatidão da sintaxe e da configuração.
- Para Helm: validação de gráficos para verificar se os manifestos gerados estão bem formados.
- Escaneamento de segurança usando o Checkov para identificar possíveis erros de configuração de segurança no código de infraestrutura gerado.

AWS O Transform relata quaisquer problemas de validação e os resolve antes de continuar.

Gerando IaC sem imagens publicadas

Você pode gerar modelos de infraestrutura mesmo que não tenha publicado imagens de contêiner na etapa anterior. Os modelos gerados usam URIs de imagem de espaço reservado que você pode atualizar posteriormente com a localização real da imagem.

O que você precisa fazer

Para gerar modelos de infraestrutura

1. Quando solicitado, escolha sua plataforma de destino: Amazon EKS ou Amazon ECS.
2. Se você escolheu o Amazon EKS, o AWS Transform pergunta se deseja incluir o CloudWatch registro. Responda sim ou não.
3. Se solicitado, forneça detalhes do endpoint de verificação de integridade do seu aplicativo (como um `/health` caminho).
4. AWS O Transform gera e valida os modelos de infraestrutura. Essa etapa é executada automaticamente e o AWS Transform exibe atualizações de progresso, incluindo quaisquer resultados de validação ou verificação de segurança.
5. Revise os modelos gerados quando o AWS Transform os apresentar.

Etapa 7: implantar a infraestrutura de teste

Nesta etapa, o AWS Transform implanta a infraestrutura de teste para que você possa validar seu aplicativo em contêineres antes da transição da produção.

O que acontece durante a implantação de teste

AWS O Transform implanta os modelos de infraestrutura gerados na etapa anterior em seu Conta da AWS. Para implantações do Amazon EKS, isso usa o Helm. Para implantações do Amazon ECS, isso usa o Terraform.

Antes da implantação, o AWS Transform apresenta um formulário de valores de infraestrutura em que você pode configurar parâmetros de implantação, como nomes de recursos, contagens de réplicas e configurações específicas do ambiente. AWS O Transform também gera uma prévia da implantação que mostra quais recursos serão criados, para que você possa revisar as alterações antes de aprovar.

O que você precisa fazer

Para implantar e validar a infraestrutura de teste

1. Preencha o formulário de valores de infraestrutura com sua configuração de implantação. O formulário inclui parâmetros como nomes de clusters, namespaces, contagens de réplicas e outras configurações específicas do ambiente.
2. Analise a pré-visualização da implantação que mostra os recursos que serão criados ou modificados.
3. Aprove a implantação da infraestrutura quando o AWS Transform a solicitar.
4. Aguarde a conclusão da implantação. AWS O Transform exibe os resultados da implantação.
5. Teste seu aplicativo implantado para verificar se ele é executado corretamente em um contêiner e se a infraestrutura atende aos seus requisitos.
6. Diga ao AWS Transform se você está satisfeito com a implantação ou se deseja modificar a infraestrutura e reimplantá-la.

Iterando na infraestrutura

Se precisar modificar os modelos de infraestrutura, você pode carregar modelos atualizados e reimplantar:

1. Diga ao AWS Transform que você deseja modificar o IaC.
2. Faça upload de um arquivo zip contendo seus modelos de infraestrutura modificados.
3. AWS O Transform substitui os modelos e executa uma atualização incremental (aplicação do Terraform ou atualização do Helm).

4. Analise os resultados atualizados da implantação.

Você pode repetir esse ciclo até ficar satisfeito com a implantação.

Recuperação da sessão

As implantações de infraestrutura são executadas de forma assíncrona usando. Se sua sessão for interrompida durante uma implantação, o AWS Transform recuperará automaticamente a operação quando você se reconectar e exibirá os resultados da implantação.

Etapa 8: Limpar a infraestrutura de teste

Depois de concluir a validação, o AWS Transform derruba a infraestrutura de teste para evitar custos desnecessários.

O que você precisa fazer

Para limpar a infraestrutura de teste

1. AWS O Transform informa que a infraestrutura de teste será demolida.
2. Aprove a operação de destruição quando o AWS Transform a solicitar.
3. Aguarde a conclusão da limpeza. AWS O Transform exibe os resultados quando todos os recursos de teste foram removidos.

Para implantações do Amazon ECS, essa etapa remove todos os recursos que foram criados durante a implantação de teste, incluindo recursos computacionais, balanceadores de carga, armazenamento e componentes de rede.

Para implantações do Amazon EKS, a limpeza tem como escopo o rótulo do seu projeto específico. Somente os recursos marcados para esse fluxo de trabalho de containerização são removidos. Outras cargas de trabalho em execução no mesmo cluster do Amazon EKS não são afetadas.

Etapa 9: implantar a infraestrutura de transição

Nesta etapa final, o AWS Transform implanta a infraestrutura finalizada para uso em produção. A implantação por transferência usa os mesmos modelos de infraestrutura que você validou durante a etapa de implantação de teste.

O que você precisa fazer

Para implantar a infraestrutura de transição

1. Preencha o formulário de valores de infraestrutura com sua configuração de implantação de produção. Você pode ajustar os parâmetros da implantação de teste ou usar os mesmos valores.
2. Analise a pré-visualização da implantação que mostra os recursos de produção que serão criados.
3. Aprove a implantação de produção quando o AWS Transform a solicitar.
4. Aguarde a conclusão da implantação. AWS O Transform exibe os resultados da implantação por transferência.
5. Verifique se seu aplicativo está sendo executado corretamente no ambiente de produção.

Important

Analise as configurações de infraestrutura geradas com sua equipe para garantir que elas atendam aos requisitos de segurança, conformidade e negócios de sua organização. Embora o AWS Transform forneça recomendações de configuração automatizadas, você é responsável por validar e ajustar as configurações de acordo com suas necessidades antes de prosseguir com a implantação por transferência.

Recuperação da sessão

As implantações de produção são executadas de forma assíncrona usando. Se sua sessão for interrompida durante a implantação, o AWS Transform recuperará automaticamente a operação quando você se reconectar e exibirá os resultados da implantação.

Modernização de aplicativos de mainframe

AWS O Transform foi projetado para acelerar a modernização de aplicativos antigos de mainframe. Ele orquestra a análise das bases de código do mainframe, gera documentação, extrai a lógica de negócios, decompõe estruturas monolíticas, transforma o código legado e gerencia a jornada geral com entradas humanas (HITL) quando necessário. Os recursos de transformação do AWS Transform para modernizar e migrar aplicativos de mainframe permitem que você modernize seu aplicativo crítico de mainframe com mais rapidez, preservando sua lógica crítica de negócios durante todo o processo de transformação.

Tópicos

- [Capacidades e características-chave](#)
- [High-level passo a passo](#)
- [Human in the loop \(HITL\)](#)
- [Tipos de arquivo compatíveis para transformação de aplicativos de mainframe](#)
- [Regiões suportadas e cotas para AWS Transform o mainframe](#)
- [High-level visão geral da jornada de modernização do mainframe](#)
- [Transformação de aplicativos de mainframe](#)
- [Crie e implante seu aplicativo modernizado após a refatoração](#)

Capacidades e características-chave

AWS O Transform fornece os seguintes recursos para a modernização do mainframe:

- Oferece suporte à modernização de aplicativos de z/OS mainframe escritos em COBOL (Common Business-Oriented Language) e PL/I (Programming Language One) com transações associadas de JCL (Job Control Language), CICS (Customer Information Control System), telas BMS (Basic Mapping Support), bancos de dados Db2 e arquivos de dados VSAM (Virtual Storage Access Method).
- Suporta a refatoração de aplicativos de mainframe Fujitsu GS21 com PSAM (Presentation Service Access Method), conjuntos de caracteres japoneses e arquivos de dados NDB (Network Data Base).
- Executa raciocínio, análise, decomposição, planejamento, geração de documentação e refatoração de código orientados por metas.

- Refatora automaticamente as cargas de trabalho do COBOL-based mainframe em aplicativos Java modernos e otimizados para a nuvem.
- Orquestra e se integra perfeitamente às ferramentas subjacentes que executam análise, documentação, decomposição, planejamento e refatoração de código.
- Ajuda você a configurar ambientes de nuvem para aplicativos de mainframe modernizados, fornecendo modelos de infraestrutura como código (IaC) prontos para uso.

High-level passo a passo

Aqui está um passo a passo de alto nível do AWS Transform para modernizar e migrar aplicativos de mainframe.

1. Inicie um bate-papo com o AWS Transform e insira um objetivo.
2. Com base em seu objetivo, o AWS Transform propõe um plano de modernização, dividindo a meta de alto nível em etapas intermediárias.
3. Dependendo da meta que você forneceu, o AWS Transform pode:
 - Avalie e reimagine a base de código
 - Crie um trabalho personalizado com base no objetivo

Ao longo do caminho, o AWS Transform pode solicitar informações de você para executar as tarefas.

Note

Para obter mais informações sobre os recursos de refatoração do AWS Transform for mainframe, consulte [Criar um projeto na documentação](#) do AWS Transform for mainframe refactor.

Human in the loop (HITL)

Durante a transformação dos aplicativos de mainframe, você pode monitorar o progresso e o status das tarefas de transformação por meio da experiência web do AWS Transform.

AWS O Transform coletará informações adicionais de você nos seguintes cenários:

- Quando informações adicionais são necessárias para executar tarefas.

- Quando a aprovação é necessária para artefatos intermediários (por exemplo, decomposição de domínios ou planejamento de ondas).
- Quando surgem problemas que o AWS Transform não consegue resolver automaticamente.

Tipos de arquivo compatíveis para transformação de aplicativos de mainframe

Os tipos de arquivo compatíveis z/OS incluem:

- Artefatos COBOL e CPY (cadernos) relacionados
- PL/I arquivos de origem
- JCL (Job Control Language) e JCL Procedure (PROC)
- Definição do sistema CICS (CSD)
- BMS (Basic Mapping Support)
- Bancos de dados Db2
- VSAM (método de acesso ao armazenamento virtual)
- IMS TM (Gerenciador de Transações)

Os tipos de arquivo suportados pelo Fujitsu GS21 incluem:

- PSAM (método de acesso ao serviço de apresentação)
- ADL (linguagem de definição AIM)
- NDB (base de dados de rede)

Para obter mais informações sobre o Fujitsu GS21, consulte estes tópicos no guia de migração do AWS Transform for mainframe:

- [GS21](#)
- [Captura e reprodução - Terminais GS21](#)
- [Mainframe, AS400, Open VMS e GS21](#)

Regiões suportadas e cotas para AWS Transforme o mainframe

Para obter uma lista das regiões suportadas, consulte [Regiões suportadas para AWS Transform](#).

Note

Seus dados podem ser processados em uma região diferente da região em que você usa o AWS Transform. Para obter informações sobre processamento entre regiões, consulte [the section called “Cross-region processamento”](#).

Para os limites da cota, consulte [Cotas](#).

High-level visão geral da jornada de modernização do mainframe

A modernização dos aplicativos de mainframe geralmente AWS é realizada em quatro fases: (a) avaliar, (b) mobilizar, (c) migrar e modernizar e (d) operar, otimizar e inovar. Cada uma dessas fases é descrita detalhadamente com metas e atividades associadas para apoiar sua jornada de modernização.

Fases

- [Fase 1: Avaliar](#)
- [Fase 2: Mobilizar](#)
- [Fase 3: Migrar e modernizar](#)
- [Fase 4: operar, otimizar e inovar](#)

Fase 1: Avaliar

Objetivo: compreender sua prontidão para a modernização e desenvolver planos iniciais de modernização.

Com o AWS Transform, você pode avaliar seus aplicativos, infraestrutura e operações de mainframe para determinar a abordagem de modernização correta para suas necessidades comerciais.

 Note

Cada fase contém uma lista de todas as atividades possíveis que você pode realizar ao modernizar seu aplicativo de mainframe. Você pode pular algumas das atividades que não estão alinhadas com seu caso de uso ou suas metas.

Atividades

- Comece com uma conversa informal sobre a modernização e trabalhe na qualificação de oportunidades, reunindo as pessoas certas na sala
- Determine a qualificação da oportunidade
- Faça uma apresentação na primeira chamada com o plano de mapeamento de dependências de aplicativos e a arquitetura do aplicativo
- Determine a ROM (ordem aproximada de magnitude) que inclui custo de infraestrutura durante a migração, mão de obra de migração, custos de pós-produção e duração do projeto
- Detecção rápida de portfólio:
 - Execute a avaliação da orientação de padrões e ferramentas
 - Faça uma análise do código-fonte
 - Identifique candidatos à prova de conceito (POC)
- Crie um treinamento de capacitação técnica:
 - Dias de imersão
 - Workshops com tópicos gerais
- Crie um relatório de avaliação de prontidão de migração (MRA) para grandes projetos de modernização de mainframe ou novos clientes AWS
- Crie uma declaração de trabalho para a fase Mobilize

Fase 2: Mobilizar

Objetivo: criar uma base e validar a abordagem por meio de provas de conceito bem-sucedidas ou modernizações piloto.

Com a fase de mobilização, você pode estabelecer as estruturas, as ferramentas e os processos necessários para apoiar a modernização do mainframe em grande escala.

Atividades

- Inicie o plano de modernização com um piloto e o POC identificado:
 - Analise o piloto e configure o código para modernização
 - Crie e teste os dados modernizados do piloto
 - Forneça resultados e analise o piloto para criar uma solução detalhada para uma maior modernização de dados
- Para plataforma:
 - Crie um plano de segurança, conformidade e monitoramento
 - Configure ambientes de zona de pouso com a zona de pouso do AWS mainframe e a estrutura da conta
 - Determine a arquitetura, a infraestrutura, o aplicativo, a integração e muito mais
- Pense nas pessoas e nos processos:
 - O Cloud Center of Excellence é um bom recurso
 - Modelo de operação
- Crie uma análise abrangente do portfólio para diferentes cenários de aplicação:
 - Descoberta abrangente que inclui documentação de alto nível
 - Plano de decomposição (para todas as aplicações)
 - Orientação de padrões e ferramentas para todas as aplicações
 - Elabore um plano inicial de modernização e migração
- Crie uma solução detalhada considerando o piloto, a plataforma, as pessoas e os processos e uma análise abrangente do portfólio
- Determine o caso de negócios
- Piloto completo de sucesso com solução para a declaração de trabalho para a próxima fase

Fase 3: Migrar e modernizar

Meta: concluir a modernização e a migração dentro do cronograma e do orçamento planejados.

Durante essa fase, você pode migrar e modernizar seus aplicativos e dados de mainframe para o AWS

Atividades

- Aloque recursos para o código do aplicativo pronto para produção
- Revise e analise o design usando a documentação existente ou entrevistando especialistas no assunto (PMEs)
- Defina cenários de teste
- Configure ambientes de modernização com tempo de execução, bancos de dados e software de terceiros adequados
- Migre e modernize o código-fonte e os dados:
 - Você pode modernizar seu aplicativo de forma iterativa com base nos domínios de negócios na base de código do aplicativo.
 - Dimensione os ambientes de modernização conforme necessário para dar suporte às suas cargas de trabalho de modernização
- Estabeleça um pipeline CI/CD (integração contínua, entrega contínua)
- Migre cargas de trabalho selecionadas para iniciar sua modernização.
- Transfira programas de aplicativos e ajuste o dimensionamento do ambiente conforme necessário:
 - Você pode escalar os ambientes para cima ou para baixo, dependendo de sua necessidade
 - Modernize os pacotes de trabalho executando testes de integridade do código
 - Ressincronize com o código-fonte conforme necessário
- Execute testes abrangentes e verifique sua migração:
 - Colete dados do estado inicial
 - Registre cenários de teste no mainframe
 - Ambiente de palco, aplicativo e dados
 - Execute cenários de teste na nuvem
 - Compare os resultados dos testes de origem e destino
 - Crie pipelines automatizados de execução de cenários de teste
 - Gere KPIs e relatórios
- Valide seus dados para configuração de produção
- Valide seu progresso fazendo o seguinte:
 - Executando a integração e o teste do sistema

- Executando testes de aceitação do usuário
- HA/DR Executando testes
- Defina um plano de implantação com o proprietário do aplicativo e crie um plano para treinamento e transferência de conhecimento
- Considere a transição e execute as transições de produção
- Estabeleça suporte sustentado para atividades de pós-produção, como operações, monitoramento, planejamento de capacidades e garantia para funções de aplicativos

Fase 4: operar, otimizar e inovar

Objetivo: Oferecer suporte à excelência operacional e à melhoria contínua de aplicativos modernizados.

Após a modernização, você pode otimizar o desempenho, a segurança e os custos de seus aplicativos enquanto aproveita AWS os serviços para inovação.

Atividades

- Aplicativo de monitoramento para:
 - Métricas de performance
 - Práticas de segurança
 - Diretrizes de conformidade
 - Custos
- Detalhes de registro
- Gerencie as operações do aplicativo:
 - Gerenciamento de infraestrutura
 - Transações e gerenciamento de tarefas
 - Suporte ao ambiente de execução
- Otimização e modernização de aplicativos
- Desenvolvimento e manutenção de aplicativos:
 - IDE de codificação
 - Criar
 - Integração

- Teste
- Implantação

Transformação de aplicativos de mainframe

AWS O Transform acelera a transformação de seus aplicativos de modernização de mainframe. Este tópico descreve os recursos disponíveis.

Tópicos

- [Pré-requisito: preparar as entradas do projeto no S3](#)
- [Coleção de artefatos de origem de mainframe](#)
- [Sign-in e criar um emprego](#)
- [Acompanhando o progresso da transformação](#)
- [Configurar um conector](#)
- [Avalie e reinvente o plano de trabalho](#)
- [Reinvente o plano de trabalho](#)
- [Plano de trabalho personalizado](#)

Pré-requisito: preparar as entradas do projeto no S3

AWS O Transform é capaz de lidar com bases de código complexas de mainframe. Para usar a base de código, verifique se você tem todos os ativos em sua localização do S3.

Principais insumos do projeto:

- **Código-fonte:** você deve fazer o upload dos arquivos de código-fonte do mainframe para o S3. Isso inclui programas COBOL, scripts JCL, cadernos e quaisquer outros arquivos de origem relevantes.
- **Arquivos de dados:** se você tiver arquivos VSAM ou outros arquivos de dados que seus aplicativos de mainframe usam, eles precisam ser enviados para o S3.
- **Arquivos de configuração:** inclua arquivos de configuração específicos para seu ambiente de mainframe.

Outros insumos do projeto

- **Registros do System Management Facility (SMF):** se aplicável, carregue os registros SMF em uma nova pasta no bucket do S3 em que o código-fonte está armazenado. Esses registros devem estar em formato de arquivo.zip.
- **Formatação:** para geração de documentação técnica, você pode aproveitar um arquivo de configuração opcional para gerar documentos PDF alinhados aos formatos e padrões necessários, incluindo cabeçalhos, rodapés, logotipos e informações personalizadas.
- **Glossário:** O AWS AWS Transform Transform aproveita a automação com IA generativa para geração de documentação e extração de regras de negócios. Incluir um arquivo CSV de glossário com informações sobre abreviações e terminologias importantes no diretório raiz do arquivo zip ajudará a melhorar a qualidade da documentação gerada.
- **Dados de teste:** se disponíveis, faça upload de conjuntos de dados de teste que possam ser usados para validar o aplicativo modernizado. Esses dados devem ser armazenados em uma nova pasta no bucket do S3 em que o código-fonte está armazenado.

Detalhes sobre as contribuições do projeto podem ser encontrados [aqui](#).

Coleção de artefatos de origem de mainframe

Este tópico descreve o processo de coleta do código-fonte do mainframe e artefatos relacionados para apoiar as iniciativas de modernização do mainframe usando o Transform. AWS A coleta e a preparação adequadas dos artefatos de origem são essenciais para uma análise, planejamento de migração e implementação bem-sucedidos.

Inventário de código fonte

Tipos de código-fonte do aplicativo

Os seguintes tipos de código-fonte do aplicativo são compatíveis:

- Programas COBOL
- Scripts de JCL
- Programas Assembler
- PL/I programas
- Transações do CICS
- Programas naturais
- Scripts REXX

- Programas Easytrieve
- Cadernos e inclui
- Bibliotecas Proc

Recursos do banco de dados

Os seguintes ativos de banco de dados são compatíveis:

- Scripts DB2 DCLGEN e DDL
- Definições de banco de dados IMS (PSBs e DBDs)
- Definições de arquivo VSAM
- Esquemas de banco de dados físicos e lógicos
- Procedimentos e gatilhos do banco de dados

Extensões de arquivo de código-fonte

Se você não tiver certeza da extensão, deixe-a em branco ou em.txt e o AWS Transform a classificará para você.

A tabela a seguir lista extensões de arquivo comuns para artefatos de origem de mainframe.

Extensões de arquivo de código-fonte de mainframe

Language/Type	Extensões comuns	Description
COBOL	.cbl, .cob, .cobol	Programas de origem COBOL
JCL	.jcl	Scripts da Job Control Language
Assembler	.asm	Programas de linguagem Assembler
PL/I	.pl1	PL/I programas de idiomas
Definição do CICS	.csd	Definição do sistema CICS (CSD)
Natural	.nat	Programas naturais
REXX	.rex, .rexX	Scripts REXX

Language/Type	Extensões comuns	Description
Easytrieve	.ezt	Programas de relatórios Easytrieve
Livros cadernos	.copiar	cadernos COBOL
BMS	.bms	Basic Mapping Support (BMS)
PL/I cadernos	.pl1_copy	PL/I cadernos
DB2 DCLGEN	.dcl	Gerador de declarações Db2
Definição do Db2	.sql, .ddl	Definições do banco de dados Db2
Definição de IMS	.ims	Conjunto de dados de definição de recursos do IMS (IMS Stage 1)
MFS	.mfs	IMS MFS (serviço de formato de mensagem)
PSB	.psb	IMS PSB (bloco de especificação do programa)
DBD	.dbd	Definições do banco de dados IMS
Processo JCL	.prc, .proc	Bibliotecas de procedimentos JCL
O JCL inclui	.inc	JCL Incluir arquivos
Macros	.mac	Macros do Assembler
Cartões de controle	.ctl	Cartões de controle JCL Utility

Métodos de coleta

Extração do código-fonte

Use clientes FTP seguros (WinSCP/FileZilla) para extração interativa de código-fonte de bibliotecas PDS de mainframe.

Extração do esquema DB2

O software cliente DB2 LUW (Linux, UNIX e Windows) inclui o db2look utilitário como parte de seu pacote de instalação. O db2look utilitário extrai instruções DDL (Data Definition Language) de um banco de dados DB2.

Execute este comando: .

```
db2look -d DATABASE_NAME -i userid -w password -a -e -m -l -x -f -createdb -printdbcfg  
-o DATABASE_NAME.sql
```

A lista a seguir descreve os parâmetros:

- -d *DATABASE_NAME*: especifica o nome do banco de dados do qual extrair o esquema
- -i *userid*: ID do usuário para autenticação do banco de dados
- -w *password*: Senha para autenticação do banco de dados
- -a: Extrai informações de autorização (concessões)
- -e: extrai todos os objetos do banco de dados (tabelas, visualizações, índices etc.)
- -m: Extrai estatísticas e características físicas
- -l: extrai comentários de tabelas e colunas
- -x: Extratos explicam tabelas
- -f: formata a saída para melhor legibilidade
- -createdb: inclui instruções de criação de banco de dados
- -printdbcfg: inclui parâmetros de configuração do banco de dados
- -o *DATABASE_NAME*.sql: especifica o nome do arquivo de saída

Extraindo informações do catálogo do mainframe

O comando LISTCAT no IDCAMS é um utilitário para recuperar informações do catálogo sobre conjuntos de dados no mainframe. Isso é útil durante projetos de modernização do mainframe para inventariar conjuntos de dados e entender suas características.

```
//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.CARDDMO.*') ALL
  LISTCAT ENT('SYS1.*') ALL
/*
```

Extraindo definições do CICS

O utilitário IBM-provided DFHCSDUP pode extrair definições de recursos CICS do arquivo CICS System Definition (CSD).

Use o seguinte JCL para descarregar as definições existentes do DFHCSD:

```
//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
/*
```

Extraindo definições do IMS

Para extrair as definições do IMS, você pode gerar o arquivo de transação do IMS usando o utilitário DFSURDD0. Esse utilitário cria instruções de macro de estágio 1 que você pode usar para fins de migração. Somente o IMS Stage 1 é suportado atualmente.

Use o seguinte JCL para extrair as definições do IMS:

```
//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
/*

```

Extraindo informações do CA-7 agendador

CA-7 as informações do cronograma de trabalho são incluídas nos relatórios do LJOB. Use o utilitário LJOB com o LIST=N0DD parâmetro para gerar os relatórios no mainframe. Os relatórios devem ter uma .ca7 extensão. Cada relatório deve ter caracteres ANSI de controle de transporte na coluna 1. Você pode criar um relatório com caracteres de controle de transporte na coluna 1 especificando DCB=RECFM=FBA (ou FA) no JCL usado para executar o utilitário LJOB.

Por exemplo: LJOB, JOB=ZBN*, LIST=ALL

Para obter mais informações, consulte a [documentação da Broadcom](#).

Extraindo dados SMF

Os registros do System Management Facility (SMF) fornecem métricas de atividade usadas pelo AWS Transform para analisar o trabalho em lote e o uso de transações do CICS. Os seguintes tipos de registro SMF são suportados: 14, 15, 30 (subtipo 5), 64, 102, 110 (subtipo 1 com classes de dados 1, 3 e 4).

Requisitos de formato para registros SMF:

- Deve incluir os tipos de registro 30 e 110 (no mínimo)
- Deve estar no formato EBCDIC binário bruto com bytes RDW (palavra descritora de registro) incluídos
- Deve ser fornecido como um dos seguintes:

- Um arquivo de até 600 MB compactado no formato.zip
- Um arquivo de até 5 GB compactado no formato.tar.gz ou .gz
- Deve ser armazenado em uma pasta separada do seu código-fonte no Amazon S3

Forneça um mínimo de 13 meses de registros SMF para capturar ciclos de lotes anuais e padrões sazonais que prazos mais curtos podem perder.

Opção 1: extrair e classificar registros SMF

Use o exemplo de JCL a seguir para extrair e classificar registros SMF:

```
//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
/*

```

Personalize os seguintes valores no JCL anterior:

1. Cartão de trabalho: Atualizar conta, classe e msgclass
2. DUMPIN: aponte para seus conjuntos de dados SMF
3. DUMPOUT: especifique o nome do conjunto de dados de saída e o HLQ
4. TIPO: Selecione os tipos de registro (14, 15, 30, 110 ou outros)
5. DATA: Formato yyyy/ddd (por exemplo, 2026/055,2026/056)
6. ESPAÇO: ajuste com base no volume de dados esperado
7. Remova a etapa SORT se não for necessário

Opção 2: extrair dados SMF com o DFSORT

Você pode usar o DFSORT para consolidar e relatar dados históricos do SMF. Isso é útil se você armazenar seus registros SMF em um GDG por dia ou semana. A tarefa a seguir usa o DFSORT para consolidar registros SMF do arquivo SORTIN e filtrar com base nos registros especificados no parâmetro INCLUDE COND.

```
//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')
```

Para baixar os dados enquanto mantém os dados RDW, você pode usar um servidor FTP para receber o arquivo extraído. Certifique-se de que os dados sejam transferidos em formato binário e que a opção RDW seja usada para que o RDW seja incluído na transferência de dados. O trabalho a seguir mostra um exemplo de trabalho de FTP para transferir esse arquivo.

```
//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
```


Carregando relatório SCRT

Você também pode carregar um Sub-Capacity relatório da Ferramenta de Relatórios (SCRT) no AWS Transform.

Upload do inventário do

Depois de coletar todos os artefatos, conclua as seguintes etapas:

1. Organize arquivos em subpastas por tipo de artefato (por exemplo, /cobol, /jcl, /copybooks, /db2, /ims, /cics, /ca7).
2. Comprima a pasta de nível superior em um único arquivo.zip.
3. Faça o upload do arquivo.zip para o bucket do Amazon S3 conectado ao AWS seu espaço de trabalho Transform.

Note

Os registros SMF devem ser colocados em uma pasta separada do seu código-fonte no bucket do Amazon S3 e devem estar no formato .tar.gz ou .gz.

Para obter instruções detalhadas sobre como conectar seu bucket do Amazon S3 ao AWS Transform, consulte [the section called “Configurar um conector”](#)

Sign-in e criar um emprego

Para entrar na experiência web do AWS Transform, siga todas as instruções na [Conceitos básicos de AWS Transformação](#) seção da documentação.

Para criar e iniciar um trabalho: siga as etapas em [Iniciar seu projeto](#).

Crie um espaço de trabalho: nomeie e descreva seu espaço de trabalho onde trabalhos, colaboradores e artefatos associados serão armazenados.

Criar trabalho: crie um trabalho selecionando planos de trabalho pré-configurados ou personalize o plano de trabalho com base em seu objetivo selecionando na lista de recursos suportados.

⚠ Important

AWS O Transform recusará suas operações se você não tiver as permissões adequadas. Por exemplo, um colaborador não pode cancelar a transformação de uma tarefa de aplicativos de mainframe nem excluir uma tarefa. Somente um administrador pode executar essas funções.

Ao criar seu trabalho, você pode selecionar entre os recursos abaixo, mas a etapa inicial é sempre necessária, pois é onde está localizada a localização do código-fonte do projeto. No primeiro trabalho configurado em um espaço de trabalho, você deve configurar um conector para seu bucket Amazon S3.

Acompanhando o progresso da transformação

Você pode acompanhar o progresso da transformação em todo o processo de duas maneiras:

- Registro de trabalho — fornece um registro detalhado das ações que o AWS Transform realiza, junto com as solicitações de entrada humana e suas respostas a essas solicitações.
- Painel — fornece um resumo de alto nível da transformação do aplicativo de mainframe. Ele mostra métricas sobre o número de trabalhos transformados, a transformação aplicada e o tempo estimado para concluir a transformação dos aplicativos de mainframe. Você também pode ver detalhes de cada etapa, incluindo linhas de código por tipo de arquivo, documentação gerada por cada tipo de arquivo, código decomposto e plano de migração.

Configurar um conector

AWS O Transform usa um conector para acessar os recursos em sua conta necessários para as funções de modernização do mainframe. Seu conector é configurado automaticamente com a primeira tarefa que você executa no espaço de trabalho. Dependendo do plano de trabalho escolhido, o AWS Transform orienta você na criação do seu conector.

Conector de reimaginação de mainframe

O conector de reimaginação do mainframe é para trabalhos que executam os fluxos de trabalho de avaliação e reimaginação. Ele usa um bucket S3 para acessar e armazenar recursos de transformação, bem como um cluster Amazon Neptune para armazenar artefatos extraídos. O cluster Neptune serve como o gráfico de conhecimento unificado que armazena todos os artefatos extraídos

sobre seu trabalho, e o gráfico de conhecimento responde a todas as perguntas na interface de bate-papo do Transform. AWS

Implante o cluster Amazon Neptune em uma VPC em AWS que o Transform possa criar interfaces de rede elásticas (ENIs). Essas são as conexões de rede que permitem que o AWS Transform se comunique com segurança com o Neptune em sua VPC para carregar dados e consultar seu gráfico de conhecimento.

AWS CloudFormation

Recomendamos usar o CloudFormation modelo a seguir para criar os recursos necessários para seu mainframe reimagine o conector. Use o mesmo bucket do S3 que você planeja usar para o conector ao executar o CloudFormation modelo. Para obter mais informações sobre o uso CloudFormation de modelos, consulte Como [trabalhar com modelos](#).

Para baixar o CloudFormation modelo, escolha [neptune-kg-setup.yaml](#).

O modelo aceita os seguintes parâmetros:

- BucketName – obrigatório. Nome do bucket S3 para acesso ao carregador em massa Neptune. Você deve usar o mesmo bucket S3 que planeja usar no seu conector AWS Transform.
- KmsKeyId: opcional. Chave KMS para criptografia Neptune. Aceita ID da chave, ARN, nome do alias ou ARN do alias. O padrão é a chave AWS gerenciada, se omitida.

Forneça os seguintes detalhes ao configurar seu conector:

- ARN do bucket do S3
- ARN do cluster Neptune
- ID do recurso do cluster Neptune
- IDs de sub-rede do aplicativo
- ID do grupo de segurança do aplicativo
- Função ARN do carregador em massa Neptune S3

Important

A guia Saídas do CloudFormation modelo inclui os detalhes que você precisa fornecer ao AWS Transform ao configurar o conector.

Configuração personalizada

Se você preferir usar uma VPC existente ou outras ferramentas para criar a infraestrutura necessária, seu ambiente deve atender aos seguintes requisitos:

Aglomerado de Netuno

- Amazon Neptune Serverless com motor versão 1.4.5.1 ou posterior
 - Autenticação IAM ativada
 - Criptografia de armazenamento ativada (chave AWS gerenciada ou chave KMS gerenciada pelo cliente)
- Configuração de escalabilidade sem servidor (recomendada: 1—128 NCUs)
- (Recomendado) Leia a réplica em uma segunda zona de disponibilidade para alta disponibilidade e melhor desempenho de leitura

Redes

- Uma VPC com suporte a DNS e nomes de host DNS habilitados
- Pelo menos duas sub-redes em zonas de disponibilidade separadas. AWS O Transform cria ENIs nessas sub-redes para acessar o cluster Neptune, que pode residir nas mesmas sub-redes ou em sub-redes dedicadas. Dimensione as sub-redes em /20 para acomodar ENIs de aplicativos e endpoints de VPC.
- Conectividade de rede das sub-redes com os seguintes AWS serviços por meio de endpoints () da interface VPC:AWS PrivateLink
 - AWS API Transform Agents — coordena os trabalhos de modernização do mainframe
 - Amazon Bedrock Runtime — invoca modelos básicos para análise e raciocínio
 - Amazon Relational Database Service (Amazon RDS) — Gerenciamento de clusters do Neptune
 - Amazon Elastic Compute Cloud (Amazon EC2) — Gerenciamento de ENIs
 - Amazon CloudWatch — Métricas para a observabilidade do AWS Transform
- Um endpoint do gateway S3 conectado às tabelas de rotas associadas às suas sub-redes. AWS O Transform usa esse endpoint para carregar dados do bucket do S3 para o cluster Neptune.

Grupos de segurança

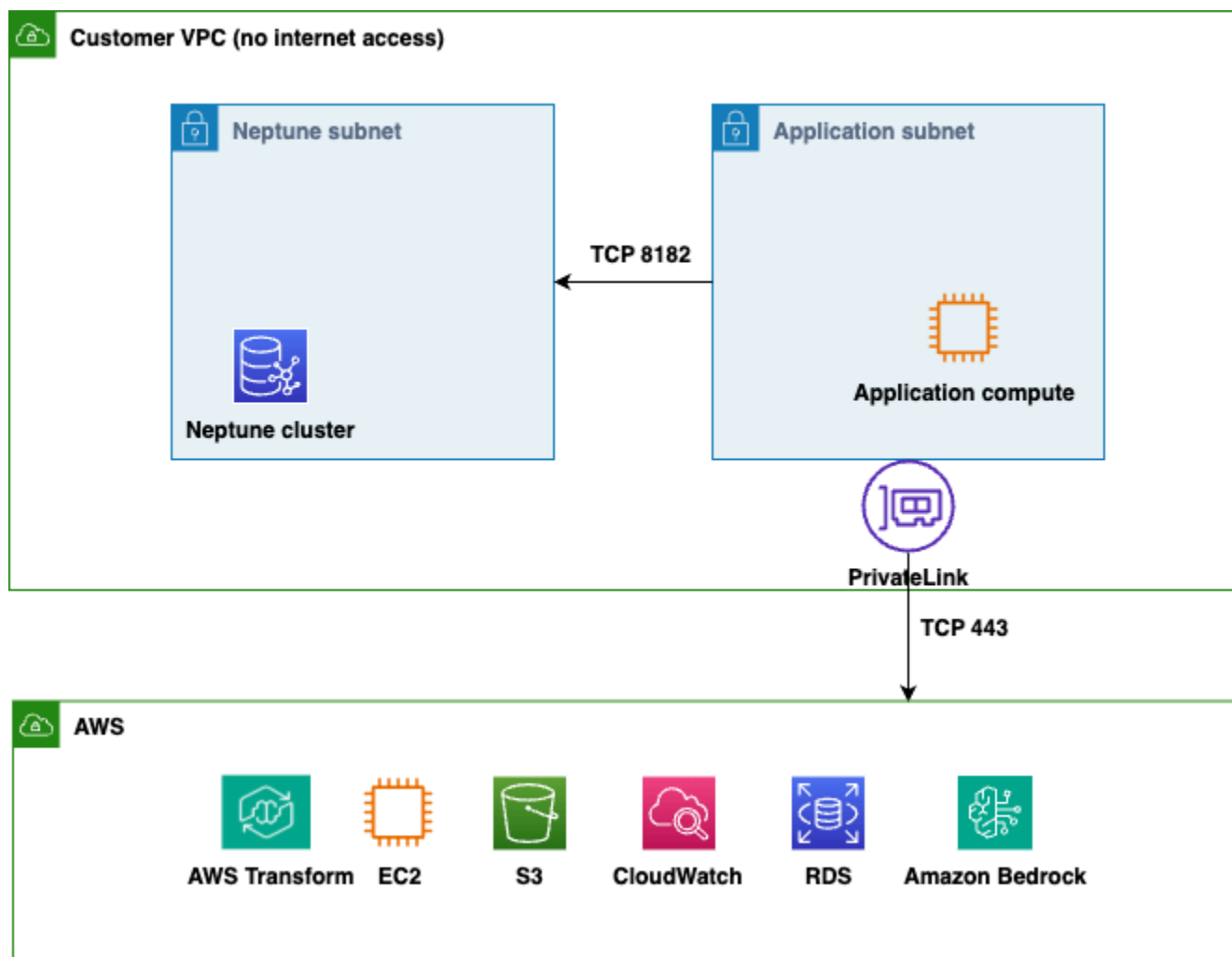
Os grupos de segurança são anexados às ENIs, não às sub-redes. Mesmo quando o AWS Transform ENIs e o Neptune residem na mesma sub-rede, grupos de segurança separados controlam o acesso entre eles.

- Um grupo de segurança (anexado aos ENIs criados pelo AWS Transform) que permite:
 - TCP 8182 de saída para o grupo de segurança Neptune
 - TCP 443 de saída para alcançar endpoints de VPC
- Um grupo de segurança (anexado ao cluster Neptune) que permite:
 - TCP 8182 de entrada do grupo de segurança do aplicativo
- Um grupo de segurança de endpoint VPC (anexado ao endpoint de interface ENiS) que permite:
 - TCP 443 de entrada do grupo de segurança do aplicativo

IAM

- Uma função do IAM com uma política de confiança para `ids.amazonaws.com` com essas concessões `s3:GetObject` e `s3:GetBucketLocation` em seu bucket do S3 `s3:ListBucket`
- Essa função deve estar associada ao cluster Neptune para carregamento em massa de dados do gráfico de conhecimento

O diagrama a seguir mostra a arquitetura recomendada.



Conector S3

Para trabalhos com um plano personalizado, o AWS Transform pode usar um conector S3. O conector S3 usa um bucket S3 para acessar e armazenar recursos de transformação e um bucket vetorial S3 para saída indexada.

Important

Seus dados são armazenados e persistem no armazenamento de artefatos AWS Transform em seu espaço de trabalho e são usados somente para executar o trabalho.

Configuração opcional do bucket vetorial S3.

Nas regiões em que os compartimentos vetoriais do S3 estão disponíveis, o AWS Transform armazenará codificações vetoriais pesquisáveis da saída do trabalho nesse intervalo vetorial do S3 em sua conta para fornecer uma experiência de pesquisa e bate-papo com inteligência artificial. Os dados não são usados fora desse trabalho e não são usados para treinar modelos. Para habilitar isso, você deve criar e fornecer um bucket vetorial S3. AWS O Transform cria e anexa automaticamente uma função com as permissões necessárias para gravar nesse bucket.

Permissões CORS do bucket S3

Depois que seu conector estiver configurado, adicione a seguinte política de CORS ao seu bucket do S3 para que você possa visualizar e comparar artefatos diretamente no console do AWS Transform. Se essa política não estiver configurada corretamente, talvez você não consiga usar as funcionalidades de visualização em linha ou comparação de arquivos do AWS Transform.

```
[
  {
    "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
  }
]
```

Avalie e reinvente o plano de trabalho

O plano de trabalho Avaliar e reimaginar é um fluxo de trabalho predefinido para modernizar aplicativos de mainframe. Ele orienta você em duas fases: avaliar sua base de código para identificar

funções de negócios e reimaginar as funções que você seleciona. Para escolher capacidades individuais em vez disso, use o plano de trabalho personalizado.

Avaliar

As jornadas de modernização do mainframe geralmente começam com a avaliação da base de código para identificar conteúdos e entender relacionamentos e dependências. Após essa avaliação, você pode começar a decompor e selecionar partes do código-fonte para modernizar. Os limites da decomposição são determinados com base nas funções de negócios.

O catálogo de funções de negócios decompõe sua base de código em funções comerciais distintas, que são construídas sobre uma base de caminhos de dados determinísticos que mapeiam cada função comercial do início ao fim. Um caminho de dados é a rota que os dados seguem, começando com um gatilho de negócios até a gravação final no código do mainframe. Em vez de limitar a análise a um único ponto de entrada, o sistema abrange trabalhos em lote, transações do CICS e seus armazenamentos de dados compartilhados para identificar unidades coerentes de trabalho comercial.

Uma função comercial é um conjunto de trabalho que começa com um gatilho comercial e termina com um resultado comercial mensurável. AWS O Transform fornece um catálogo de funções de negócios nas quais uma linha de negócios pode atuar, permitindo decisões informadas sobre o que modernizar primeiro.

Benefícios de avaliar sua base de código para se modernizar usando funções de negócios:

- Full-estate visibilidade — entenda como seus trabalhos em lotes, transações on-line e armazenamentos de dados se conectam a funções significativas para sua empresa.
- Limites acionáveis — Cada função comercial identificada é uma unidade independente que as partes interessadas da linha de negócios podem revisar e priorizar para o esforço de modernização.
- Consistência do código à especificação — Os mesmos blocos de código que definem uma função de negócios são usados para gerar suas especificações, sem camada de tradução e sem necessidade de reconciliação.
- Tempo de descoberta reduzido — A detecção automatizada substitui meses de entrevistas manuais de conhecimento tribal por análises sistemáticas e repetíveis.

Resultados da avaliação fornecidos por meio do chat

Os resultados da avaliação fornecidos pelo chat incluem uma lista de funções de negócios, incluindo o número de caminhos de dados, o que cada função abrange em termos de transações em lote e do CICS e uma descrição da empresa. Você recebe um link para os artefatos gerados no bucket do Amazon S3 e também pode acessá-los por meio do chat. Dois artefatos são fornecidos: detalhes da função comercial e resumo da função comercial.

- **Resumo da função comercial** — fornece uma lista das funções de negócios e uma descrição em linguagem natural das funções que os elementos do código estão executando.
- **Detalhes da função comercial** — fornece um gráfico interativo que mostra as relações entre o código-fonte.

Para interagir com o gráfico, selecione um elemento para mostrar detalhes adicionais sobre ele ou abra um elemento para interrogar seus detalhes. Em cada página, há um resumo de todos os elementos desse nível e uma interface gráfica para interagir e aprender mais sobre cada componente, incluindo o seguinte:

- **Função comercial** — Descreve quais funções de negócios estão conectadas entre si e fornece uma visão geral de cada função comercial. Quando você seleciona uma função comercial, as seguintes informações são fornecidas:
 - Número de caminhos de dados
 - Número de linhas de código
 - Descrição da empresa: uma visão geral da função comercial que descreve, em linguagem natural, quais funções os elementos do código estão executando.
 - Interfaces: detalha como os elementos de dados dentro da função de negócios se relacionam (por exemplo, troca ou gravação).
- **Detalhes da função comercial** — descreve as conexões entre os caminhos de dados em uma única função comercial, permitindo que você se aprofunde na composição da função comercial. Ao selecionar um elemento, você vê como esse elemento se conecta à função comercial, junto com os seguintes detalhes:
 - Datastore: escritores e leitores para o armazenamento de dados.
 - Outros elementos: uma visão geral do caminho de dados relacionado que descreve, em linguagem natural, as ações e os resultados tratados no caminho de dados, uma lista de programas e leitores e escritores.

- Caminhos de dados — descreve os detalhes de um caminho de dados e como os elementos dentro do caminho de dados se relacionam entre si.
- Descrição: uma visão geral do caminho de dados que descreve, em linguagem natural, as ações e os resultados tratados dentro do caminho de dados.
- Conteúdo do caminho de dados:
 - Ponto de entrada
 - Leituras
 - Gravações
 - Programas

Por meio do bate-papo, você pode interrogar os resultados para entender os elementos contidos em cada função comercial e explorar os limites por meio do gráfico da função comercial.

Depois de identificar os limites de sua modernização, o chat solicita que você selecione as funções de negócios que você deseja reimaginar. Você pode selecionar uma única função comercial ou várias funções comerciais. AWS O Transform envia os limites selecionados e os resultados de avaliação necessários para o fluxo reimaginado para continuar a jornada de modernização.

Depois de concluir sua primeira modernização, você pode usar o chat para selecionar um conjunto adicional de funções de negócios para modernizar.

Reimagine

Na fase de reimaginação, você pode selecionar uma ou todas as funções de negócios que a avaliação identificou e prepará-las para a modernização. Isso aciona a extração da lógica de negócios seguida pela geração de requisitos para as funções comerciais selecionadas. Os requisitos gerados são a principal entrada para a engenharia avançada, traduzindo a compreensão do sistema legado em uma especificação precisa do que o aplicativo modernizado deve oferecer.

Extraia a lógica de negócios

Depois de selecionar uma ou mais funções comerciais, o AWS Transform começa a gerar a lógica de negócios para as funções comerciais selecionadas. Após a conclusão da extração, o AWS Transform armazena os resultados em um bucket do Amazon S3 no formato JSON para uso posterior. Você pode monitorar o progresso da extração e analisar quaisquer problemas diretamente no console do AWS Transform.

Para revisar os resultados da extração da lógica de negócios

1. No painel de navegação esquerdo, escolha a etapa Extrair lógica comercial para expandi-la.
2. Veja o seguinte nos detalhes da etapa:
 - Link do bucket S3: o local em que os resultados da lógica de negócios extraídos são armazenados no formato JSON.
 - Problemas: uma lista de todos os problemas encontrados durante o processo de extração da lógica de negócios.

Se algum arquivo tiver problemas durante a extração, os seguintes detalhes serão exibidos para cada arquivo afetado:

- Nome do arquivo: o nome do arquivo que encontrou um problema.
- Tipo de arquivo: o tipo do arquivo (por exemplo, COBOL ou JCL).
- Caminho do arquivo: a localização do arquivo em seu aplicativo.
- Status: O status atual da extração do arquivo.
- Detalhes: uma descrição do problema encontrado.

 Note

Após a conclusão da etapa de extração, o AWS Transform começa automaticamente a gerar requisitos. Você não será solicitado a fornecer nenhuma entrada adicional antes do início desse processo.

Gere requisitos

Após a conclusão da extração da lógica de negócios, o agente Generate Requirements consome os artefatos extraídos (análise de código, análise de dados, regras de negócios) e produz requisitos de modernização. Esses requisitos são especificações funcionais formais que são independentes de tecnologia e incluem critérios de aceitação testáveis. AWS O Transform produz um `requirements.md` arquivo para cada função comercial que você seleciona e armazena a saída em um bucket do Amazon S3. Para visualizar a localização da saída no Amazon S3, escolha a etapa Gerar requisitos.

Cada `requirements.md` arquivo é organizado nas seguintes partes:

- **Título** — Nomeia a função comercial e o fluxo de trabalho que ela representa.
- **Condições prévias globais** — condições que devem ser válidas em todo o fluxo de trabalho antes e durante o processamento. Os valores configuráveis aparecem como espaços reservados para parâmetros.
- **Seções numeradas do fluxo de trabalho** — Cada seção representa um estágio distinto da função comercial. Cada seção contém o seguinte:
 - Uma história de usuário que declara a meta como uma função, a ação que a função deseja realizar e o resultado resultante.
 - Uma lista de requisitos no formato EARS (Easy Approach to Requirements Syntax), cada um com um identificador exclusivo.

Note

A seleção de um segundo conjunto de funções de negócios reinicia a etapa de reimaginação das funções recém-selecionadas. O console então mostra os resultados somente para a nova seleção, portanto, quaisquer problemas com as regras de negócios de suas funções comerciais anteriores e os links do Amazon S3 que armazenam as saídas para a lógica e os requisitos de negócios não são mais exibidos. Suas saídas anteriores não foram perdidas. Você ainda pode acessá-los na guia Artifacts ou em seu bucket do Amazon S3.

Rastreabilidade entre artefatos de transformação

AWS O Transform mantém a rastreabilidade entre os artefatos que gera em todo o fluxo de trabalho de avaliação e reimaginação. A rastreabilidade permite rastrear cada requisito de acordo com as regras de negócios extraídas ou diretamente com o código-fonte original que produziu o requisito.

Você pode visualizar todos os detalhes de rastreabilidade de cada função comercial usando o `traceability.yaml` arquivo. Ela descreve como cada regra de negócios se relaciona com um requisito.

Para rastreabilidade interativa, você pode usar o plug-in IDE nos editores compatíveis com VS Code e Open VSX. Para obter mais informações, consulte [Ferramentas para desenvolvedores](#).

Reinvente o plano de trabalho

Para aplicativos que você tem como escopo a modernização e está pronto para reimaginar, você pode executar um trabalho de reimaginação independente. O trabalho analisa seu código e dados, extrai a lógica de negócios, identifica domínios de negócios e gera requisitos de modernização para cada domínio comercial.

Plano de trabalho personalizado

Um plano de trabalho personalizado permite que você crie seu próprio fluxo de trabalho de modernização selecionando os recursos que você deseja executar. Ele oferece controle total sobre quais recursos estão incluídos. Escolha entre os seguintes recursos com base em seu objetivo de modernização. Alguns recursos dependem de outros serem executados primeiro. Por exemplo, a análise de código é necessária para a maioria dos outros recursos.

Analise o código

Depois de compartilhar o caminho do bucket do Amazon S3 com o AWS Transform, ele analisará o código de cada arquivo com detalhes como nome do arquivo, tipo de arquivo, linhas de código e seus caminhos.

Note

Você pode baixar os resultados do código Análise por meio da guia de artefatos no nível do trabalho ou do espaço de trabalho. No nível do trabalho, vá até a opção 'Artefatos' no menu de navegação esquerdo e abra a pasta 'resultados' ou, no nível do espaço de trabalho, encontre o nome do trabalho e abra a pasta 'resultados'. Isso fará o download de um arquivo zip que contém o arquivo de classificação para o fluxo de trabalho de classificação manual, a lista de ativos, o arquivo JSON de dependências e a lista de arquivos ausentes.

No plano de trabalho, selecione Analisar código no painel de navegação esquerdo para ver seus resultados. Você pode visualizar os resultados da análise de código de várias maneiras:

- Visualização em lista — Todos os arquivos no bucket do Amazon S3 que você deseja transformar para mainframe
- Visualização do tipo de arquivo — Todos os arquivos no bucket do Amazon S3 exibidos por tipo de arquivo. Para obter uma lista dos tipos de arquivo compatíveis, consulte [Arquivos compatíveis](#).

- Visualização de pastas — Todos os arquivos no bucket do Amazon S3 exibidos na estrutura de pastas.

Nos resultados do arquivo, o AWS Transform fornece as seguintes informações, dependendo da visualização de arquivo escolhida:

- Nome
- Tipo de arquivo
- Total de linhas de código
- Caminho do arquivo
- Linhas de comentários
- Linhas vazias
- Linhas de código eficazes
- Número de arquivos
- Complexidade ciclomática - A complexidade ciclomática representa o número de caminhos linearmente independentes através do código-fonte de um programa. AWS A transformação mostrará uma complexidade ciclomática para cada um dos arquivos.

Arquivos ausentes — Arquivos ausentes da análise do código de modernização do mainframe. Idealmente, esses arquivos devem ser adicionados como parte da entrada de origem no bucket do Amazon S3, e a etapa de análise deve ser executada novamente para obter resultados melhores e coesos.

Nome idêntico — AWS Transform fornece uma lista de arquivos que compartilham o mesmo nome e, possivelmente, as mesmas características (por exemplo, número de linhas de código). Ele não poderá comparar a diferença entre o conteúdo de dois arquivos ao mesmo tempo.

IDs duplicados — Com o programa Cobol, o campo ID do programa serve como o identificador exclusivo do arquivo. Esse ID deve ser exclusivo porque é usado para chamar o programa em todo o projeto. No entanto, alguns projetos podem ter arquivos COBOL com nomes diferentes, mas com o mesmo ID do programa. Obter a lista desses arquivos durante a avaliação pode ajudar a entender as dependências entre todos os programas.

 Note

Isso é específico para códigos e arquivos COBOL.

Quando você tem programas com IDs duplicados, é recomendável alterar os IDs de programa desses arquivos para ter um identificador exclusivo para cada um deles no código COBOL. Em seguida, você pode executar novamente seu trabalho para obter resultados de análise de código mais precisos e abrangentes.

Ao resolver IDs de programa duplicados, você pode:

- Melhore a clareza e a capacidade de manutenção do código
- Reduza possíveis conflitos nas chamadas do programa
- Melhore a precisão do mapeamento de dependências
- Simplifique os esforços futuros de modernização

Problemas na base de código — Possíveis problemas detectados na base de código que você deve resolver antes de continuar com o projeto de modernização. Esses problemas podem incluir referências ausentes com declarações associadas ou links sem suporte no código.

Classificação de atualização — Com a reclassificação manual, você pode reclassificar arquivos usando o recurso de atualização em massa fazendo o upload do arquivo JSON com a nova classificação.

 Important

Isso só está disponível para TXT arquivos UNKNOWN e.

Após a reclassificação, AWS o Transform irá:

1. Atualiza os resultados da classificação
2. Re-runs análise de dependências com os novos tipos de arquivo
3. Atualiza todos os resultados de análise afetados

 Note

Você pode reclassificar arquivos somente após a conclusão do ciclo de análise inicial.

Visualizador embutido e comparação de arquivos

O visualizador embutido é um recurso do AWS Transform for mainframe que fornece dois recursos principais de visualização:

- Visualização do arquivo: visualize o conteúdo dos arquivos herdados selecionados das tarefas
- Comparação de arquivos: compare o conteúdo de dois arquivos legados lado a lado

Visualização do arquivo de entrada

Para visualizar seus arquivos no Analise o código step (etapa)

- Em Exibir resultados da análise de código, selecione um arquivo usando a caixa de seleção na lista.

Escolha o botão Exibir ação (ativado quando 1 item é selecionado).

O conteúdo do arquivo será renderizado na tela no componente Exibição de arquivo.

Comparação de arquivos

Para comparar arquivos no Analise o código step (etapa)

1. Em Exibir resultados da análise de código, selecione dois arquivos usando as caixas de seleção na lista.
2. Escolha o botão de ação Comparar (ativado somente quando 2 itens são selecionados).
3. Os arquivos serão exibidos lado a lado no componente de comparação de arquivos.

 Note

Você não pode selecionar mais de dois arquivos para comparar arquivos.

 Important

Se você estiver tendo problemas com o visualizador embutido ou com a comparação de arquivos, verifique se o bucket do S3 está configurado corretamente. Para obter mais informações sobre a política CORS do bucket S3, consulte [the section called “Permissões CORS do bucket S3”](#)

Análise de dados

AWS O Transform fornece análise de dados para ajudar a entender o impacto das relações e dos elementos de dados no projeto de modernização do mainframe. As duas saídas fornecidas são:

- Linhagem de dados: rastreia o ciclo de vida dos dados mapeando as relações entre fontes de dados, trabalhos e programas
- Dicionário de dados: serve como um repositório que documenta os metadados estruturais dos elementos de dados legados

Após a conclusão da análise, haverá duas guias presentes para cada saída e, em seguida, várias visualizações disponíveis descritas abaixo para a linhagem de dados e o dicionário.

 Note

Quando você solicita a análise de dados, AWS O Transform realiza a análise de código, necessária para realizar a análise de dados.

Linhagem de dados

AWS O Transform fornece várias visualizações com base nas relações de dados que precisam ser entendidas em toda a base de código que está sendo modernizada. As quatro visualizações de tabela disponíveis na linhagem de dados incluem:

- Conjuntos de dados: essa visualização fornece uma análise de impacto abrangente, incluindo rastreamento de operações para ajudar a distinguir entre leitura, gravação, atualização e exclusão
- Tabelas do Db2: forneça a análise de impacto relacionada às tabelas e às operações do Db2
- Program-to-data: identifique quais programas COBOL fazem referência a cada conjunto de dados

- JCL-to-data relacionamentos: identifique quais scripts JCL fazem referência a cada conjunto de dados

O resumo fornece uma visão geral das fontes de dados e suas relações com programas e JCLs, bem como informações resumidas sobre como as fontes de dados são aproveitadas e o total de operações encontradas na base de código.

Dicionário de dados

Compreender os elementos de dados nas fontes de dados presentes na base de código é a próxima etapa para perceber como as várias fontes de dados são dependentes. O dicionário de dados é um catálogo de dados que fornece metadados em nível de campo com descrições de linguagem comercial para um mapeamento preciso da transformação.

- Estrutura de dados COBOL: fornece informações de campo em cadernos COBOL e referências INLINE presentes na base de código, incluindo propriedades de campo e definição de negócios
- Tabelas Db2: Fornece propriedades de colunas e tabelas em todas as tabelas Db2 presentes na base de código, incluindo chaves primárias e estrangeiras, informações de esquema e índice e tipos de dados

A relação entre a linhagem de dados e o dicionário está disponível selecionando a fonte de dados e, em seguida, utilizando o botão de linhagem de dados ou dicionário de dados para aprofundar a relação entre a fonte de dados e os elementos de dados. A navegação entre a linhagem de dados e o dicionário fornece visibilidade de dados integrada com a linhagem de dados fornecendo o “quê” - estrutura e significado, juntamente com o “onde” - uso e relacionamento.

Análise de métricas de atividade

A análise de métricas de atividade permite analisar registros do System Management Facility (SMF) do tipo 14, 15, 30, 64, 102 e 110. A análise fornece informações sobre como os elementos são usados em seu aplicativo de mainframe. Ele pode ajudar na remoção de código não utilizado ou na tomada de decisões sobre a arquitetura de destino do aplicativo modernizado. Se você incluir a análise de métricas de atividade em seu trabalho, concluir primeiro a etapa de análise de código fornecerá resultados SMF mais ricos, embora isso não seja obrigatório.

 Note

Quando você negocia o plano de trabalho para a modernização do mainframe, concluir primeiro as etapas de análise e decomposição do código fornece resultados mais ricos.

Registros SMF integrados para análise

Você deve fornecer a localização do registro SMF em seu bucket do Amazon S3 como a etapa inicial para a análise SMF. Forneça um mínimo de 13 meses de registros para capturar ocorrências anuais que prazos mais curtos possam perder. Embora 13 meses sejam recomendados, qualquer período de tempo com registros SMF detectáveis produz resultados de análise.

Sua extração SMF deve atender aos seguintes requisitos de formato:

- Inclua os tipos 14, 15, 30 (subtipo 5), 64, 102 e 110.
- Use um arquivo binário bruto no formato EBCDIC.
- Inclua bytes RDW.

Forneça um link para os registros SMF em seu bucket do Amazon S3, garantindo que os registros estejam em uma pasta separada do seu código-fonte. As opções de formato incluem .zip (até 600 MB) ou .tar.gz (até 5 GB) compactado. Se você fornecer um link para uma pasta na qual os registros SMF não foram detectados, você receberá uma mensagem de erro e nenhuma análise será concluída.

Saída de análise

A saída da análise contém dois componentes, dependendo do tipo de registro: uma visualização tabular e uma saída.csv (disponível em seu bucket do Amazon S3). Em AWS Transform, as saídas são exibidas para os tipos 30 e 110. Por meio dos artefatos em seu bucket do Amazon S3, você pode explorar a análise em outros tipos de registros. Na interface do usuário, o cabeçalho exibe o intervalo de tempo dos registros fornecidos para que você possa identificar as datas-chave ausentes. Por exemplo, se seus registros abrangem 1º de maio a 31 de outubro, mas excluem o dia movimentado após o Dia de Ação de Graças, você pode ver que faltam os principais registros. Os carimbos de data/hora no aplicativo web refletem o fuso horário do seu sistema e os registros SMF.

Os artefatos disponíveis no Amazon S3 fornecem análises para qualquer tipo de registro encontrado nos registros fornecidos.

Visualização tabular

A exibição tabular, disponível somente para SMF 30 e 110, contém até três componentes principais para trabalhos em lotes e transações do CICS:

- **Resumo** — Fornece os principais trabalhos e transações.
- **Análise de job/CICS transações em lote** — fornece análise agregada entre trabalhos e transações.
- **Comparação de análise de código (somente em lote)** — Fornece dados de comparação quando a etapa de análise de código é executada antes da análise SMF.

O resumo da descoberta fornece três grupos de trabalhos e transações que ajudam você a identificar rapidamente os itens para uma análise mais profunda.

A análise de tarefas em lotes e transações do CICS fornece análises agregadas entre trabalhos e transações. Algumas colunas nos resultados da análise estão ocultas por padrão. Escolha o ícone de engrenagem para exibir campos adicionais.

A chave de transação gera uma agregação de dados exclusiva para transações do CICS, combinando quatro campos em um único valor de chave:

- ID da transação
- Nome do programa
- SysPlex ID
- SysID

Você pode pesquisar pela chave completa ou por qualquer componente da chave na saída da análise.

A comparação da análise de código destaca as tarefas encontradas nos registros SMF ou na etapa de análise do código, mas não estão presentes em ambas. Isso mostra trabalhos que não foram executados durante o período de registro do SMF ou que não estavam presentes na etapa de análise do código. Essa saída está disponível somente quando você executa a etapa de análise de código antes da análise SMF em seu trabalho.

Práticas recomendadas

Para obter resultados abrangentes para trabalhos em lote (tipo 30), certifique-se de que o nome do arquivo JCL corresponda ao nome do trabalho para obter resultados significativos na comparação da análise de código.

Gere documentação técnica

Você pode gerar documentação técnica para seus aplicativos de mainframe que estão passando por modernização. Ao analisar seu código, o AWS Transform pode criar automaticamente uma documentação detalhada de seus programas de aplicativos, incluindo descrições da lógica, fluxos, integrações e dependências do programa presentes em seus sistemas legados. Esse recurso de documentação ajuda a preencher a lacuna de conhecimento, permitindo que você tome decisões informadas ao fazer a transição de seus aplicativos para arquiteturas de nuvem modernas.

Note

Quando você solicita a geração da documentação técnica, o AWS Transform realiza a análise do código, incluindo a análise de dependência do código, que é necessária para gerar a documentação.

Para gerar documentação técnica

1. No painel de navegação esquerdo, em Generate technical documentation, escolha Select files and configure settings.
2. Selecione os arquivos no bucket do Amazon S3 para os quais você deseja gerar documentação e defina as configurações na guia Colaboração.

Note

Os arquivos selecionados devem ter o mesmo tipo de codificação (ou seja, todos no mesmo CCSID - UTF8 ou ASCII). Caso contrário, a documentação técnica gerada pode ter campos ou seções vazios.

3. Escolha o nível de detalhes da documentação:
 - Summary: fornece uma visão geral de alto nível de cada arquivo no escopo. Além disso, fornece um resumo de uma linha de cada arquivo.

- Detailed functional specification: fornece detalhes abrangentes de cada arquivo no escopo de transformação da aplicação de mainframe. Alguns detalhes incluem lógica e fluxo, dependências, processamento de entrada e saída e vários detalhes da transação.

 Note

A documentação só pode ser gerada para arquivos COBOL e JCL.

4. Escolha Continuar.
5. Depois que o AWS Transform gerar a documentação, revise os resultados da documentação seguindo o caminho do bucket do Amazon S3 no console, onde os resultados são gerados e armazenados.
6. Depois que a documentação for gerada, você também poderá usar o bate-papo do AWS Transform para fazer perguntas sobre a documentação gerada e decidir as próximas etapas.

Adicione informações do usuário à documentação

```
ARTIFACT_ID.zip
### app/
    ### File1.CBL
    ### File2.JCL
    ### subFolder/
        # # File3.CBL
### glossary.csv
### pdf_config.json
### header-logo.png
### footer-logo.png
# ...
```

Arquivos opcionais podem ser adicionados ao arquivo zip para ajudar a melhorar a qualidade da documentação gerada e fornecer uma capa personalizada em PDF. Alguns deles podem ser:

- arquivo glossary.csv: você pode optar por fornecer e carregar um glossário opcional no arquivo zip no bucket do S3. O glossário está no formato CSV. Esse glossário ajuda a criar documentação com descrições relevantes de acordo com o vocabulário do cliente. Um glossary.csv arquivo de amostra se parece com:

```
LOL, Laugh out loud
```

ASAP, As soon as possible
WIP, Work in progress
SWOT, "Strengths, Weaknesses, Opportunities and Threats"

- `pdf_config.json`: você pode aproveitar esse arquivo de configuração opcional para gerar documentos PDF alinhados aos formatos e padrões da empresa, incluindo cabeçalhos, rodapés, logotipos e informações personalizadas. Uma amostra `pdf_config.json` se parece com:

```
{
  "header": {
    "text": "Acme Corporation Documentation",
    "logo": "header-logo.png"
  },
  "customSection": {
    "variables": [
      {
        "key": "business Unit",
        "value": "XYZ"
      },
      {
        "key": "application Name",
        "value": "ABC"
      },
      {
        "key": "xxxxxxxxxxx",
        "value": "yyyyyyyyyyyyyy"
      },
      {
        "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  
}  
}
```

- Cabeçalho:
 - Para o arquivo PDF da capa, o texto padrão será o nome do projeto.
 - Para cada arquivo PDF do programa, o texto padrão será o nome do programa.
 - Não há logotipo padrão. Se um logotipo de cabeçalho não estiver configurado, nenhum logotipo será exibido.
 - O tamanho da fonte e o tamanho do logotipo devem ser alterados dinamicamente com base no número de palavras ou no tamanho do arquivo do logotipo.
- Seção personalizada:
 - Se a seção personalizada não estiver configurada, ela será omitida do PDF.
 - O link deve ser clicável.
- Rodapé:
 - Não há texto ou logotipo padrão para o rodapé.
 - O número da página será exibido no rodapé por padrão, a menos que seja explicitamente configurado de outra forma.
 - O tamanho da fonte e o tamanho do logotipo devem ser alterados dinamicamente com base no número de palavras ou no tamanho do arquivo do logotipo.

Gere um visualizador embutido de documentação

Você pode visualizar os arquivos PDF na etapa de geração da documentação técnica.

Para visualizar os arquivos PDF

1. Navegue até a guia Revisar resultados da documentação.
2. Localize o PDF na tabela que lista os PDFs gerados.
3. Selecione o arquivo e, em seguida, selecione Exibir ou selecione o elemento de link sobreposto ao nome do arquivo.

O PDF é aberto no AWS Transform, com a opção de expandir a tela no canto superior direito.

 Note

AWS O Transform também permite baixar uma versão em XML ou PDF da documentação técnica gerada.

 Important

Se você estiver tendo problemas com o visualizador embutido da documentação, verifique se o bucket do S3 está configurado corretamente. Para obter mais informações sobre a política CORS do bucket S3, consulte [the section called “Permissões CORS do bucket S3”](#)

Extraia a lógica de negócios

Você pode extrair a lógica comercial essencial de seus aplicativos de mainframe que estão passando por modernização. AWS O Transform analisa automaticamente seu código para identificar e documentar elementos comerciais essenciais, incluindo fluxos de processo detalhados e lógica de negócios incorporada em seus aplicativos. Esse recurso atende a várias partes interessadas em sua jornada de modernização. Os analistas de negócios podem aproveitar a lógica extraída para criar requisitos comerciais precisos e identificar lacunas ou inconsistências nas implementações atuais. Os desenvolvedores ganham a capacidade de compreender rapidamente a funcionalidade complexa do sistema legado sem ampla experiência em mainframe.

 Note

Quando você solicita a extração da lógica de negócios, AWS O Transform realiza a análise do código, incluindo a dependência do código e a análise do ponto de entrada, que são necessárias para realizar a extração da lógica de negócios.

Para extrair a lógica de negócios

1. No painel de navegação esquerdo, em Extrair lógica comercial, escolha Definir configurações.
2. Na guia Colaboração, selecione como você deseja extrair a lógica de negócios:

- Nível do aplicativo: gera documentos comerciais para todas as funções comerciais, transações, trabalhos em lotes e arquivos. Isso seleciona todos os arquivos no aplicativo.
- Nível do arquivo: gera documentos comerciais somente para arquivos selecionados na tabela de arquivos.

 Note

- Para qualquer uma das opções, você pode selecionar Incluir especificação funcional detalhada para que o AWS Transform inclua fluxo de controle e regras de negócios abrangentes para os arquivos selecionados.
- Os arquivos selecionados devem ter o mesmo tipo de codificação (ou seja, todos no mesmo CCSID - UTF8 ou ASCII). Caso contrário, a documentação gerada pode ter campos ou seções vazios.
- A documentação só pode ser gerada para arquivos COBOL e JCL.
- No nível do aplicativo, os programas usados por transações do CICS e trabalhos em lotes são agrupados, enquanto todos os outros programas são categorizados como Não atribuídos.

3. Escolha Continuar.
4. Depois que o AWS Transform extrai a lógica de negócios, ele armazena os resultados em um bucket do Amazon S3 no formato JSON para que você possa visualizá-los on-line.

 Note

O número de arquivos de regras de negócios gerados pode ser maior do que sua seleção inicial. Alguns arquivos selecionados podem acionar a extração de regras de negócios para incluir arquivos dependentes adicionais, que também aparecerão na tabela de resultados.

Veja a documentação comercial extraída em linha

Você pode visualizar a lógica de negócios na etapa Extrair regra de negócios. Para fazer isso,

1. Navegue até Revisar os resultados da extração da lógica de negócios.
2. Selecione o documento que você deseja visualizar na tabela e clique no botão Exibir resultado.

A página de documentação comercial é aberta em uma nova guia do navegador.

Decomposição

Você pode decompor seu código em domínios que contabilizam as dependências entre programas e componentes. Isso ajuda os arquivos e programas relacionados a serem agrupados adequadamente no mesmo domínio. Também ajuda a manter a integridade da lógica do aplicativo durante o processo de decomposição.

Note

Quando você solicita a decomposição, o AWS Transform realiza análises de código, incluindo análises de dependência de código, que são necessárias para realizar a decomposição. Também recomendamos que você execute a extração da lógica de negócios antes da decomposição para obter melhores resultados.

Para começar a decompor seu aplicativo:

1. Selecione Decompor código no painel de navegação esquerdo.

Note

Um domínio, Não atribuído, é criado automaticamente para todos os arquivos não associados a um domínio. Na navegação inicial, todos os arquivos devem ser associados a Não atribuído, a menos que os domínios tenham sido propostos a partir da extração da lógica de negócios no nível do aplicativo.

2. Crie um novo domínio por meio do menu Ações e escolha Criar domínio.
3. Em Criar domínio, forneça o nome do domínio, a descrição opcional e marque alguns arquivos como sementes.
 - Os arquivos configurados pelo CICS (CSD) e os arquivos configurados pelo agendador (SCL) podem ser usados para detecção automática de sementes.
 - Você também pode definir um domínio somente como um componente comum. Os arquivos nesse domínio são comuns a vários domínios.
4. Escolha Criar.

 Note

Você pode criar vários domínios com arquivos diferentes como sementes.

5. Depois de confirmar todos os domínios e sementes, escolha Decompor.
6. AWS O Transform verificará os arquivos do código-fonte e depois se decomporá em domínios com programas e conjuntos de dados com casos de uso semelhantes e altas dependências de programação.

AWS O Transform oferece uma visualização tabular e gráfica dos domínios decompostos como dependências. A visualização gráfica tem três opções:

- Visualização de domínio — Pode ver como diferentes domínios estão relacionados entre si em formato visual.
- Visualização de dependências — Pode visualizar todos os arquivos em cada domínio como um gráfico complexo de dependências. Se um nó que foi adicionado a um domínio não recebeu informações de uma semente no mesmo domínio, esse nó será previsto como não atribuído (o nó não recebeu nenhuma informação), desconectado (em um subgráfico que não recebeu informações iniciais) ou em outro domínio (o nó recebeu informações de pelo menos esse domínio).
- Visualização do subgráfico - O usuário pode criar subgráficos para visualizar um subconjunto de nós para entender mais claramente o impacto relacional e os limites dessa coleção de nós.
 - Para criar um subgráfico, selecione um grupo de nós e selecione a opção Extrair subgráfico na barra de ferramentas.
 - A mesclagem de subgráficos está disponível quando um novo terceiro subgráfico é criado, além dos dois subgráficos que você está mesclando.

 Note

Repita essas etapas para adicionar mais domínios ou reconfigurar seus domínios já criados com um conjunto diferente de sementes se você não gostar da estrutura de domínio atual.

7. Ao concluir, escolha Continuar.

Sementes

As sementes são as entradas fundamentais para a fase de decomposição do código. Cada componente ou arquivo (por exemplo, JCL, COBOL, tabelas Db2, CSD e arquivos do agendador) pode ser atribuído como semente a apenas um domínio, garantindo limites e alinhamento claros durante o processo de decomposição.

A identificação das sementes depende da estrutura da aplicação ou do portfólio. No caso de um aplicativo legado típico de mainframe, as sementes geralmente podem ser determinadas aderindo às convenções de nomenclatura estabelecidas, ao agrupamento em nível de lote no agendador e ao agrupamento em nível de transação definido no sistema CICS. Além disso, as tabelas do banco de dados também podem servir como sementes, fornecendo outra camada de estrutura para decomposição.

Importar arquivos de dependências de and/or atualização

Durante a decomposição, você pode carregar um arquivo JSON para as dependências que substitui os arquivos existentes gerados pela análise de dependências que o Transform executa. AWS

A função de exportação de dependências permite que você baixe o arquivo json de dependências gerado na etapa de decomposição. Após o download, você pode modificar o arquivo de acordo com sua necessidade. Em seguida, você pode importar dependências usando a funcionalidade de upload do AWS Transform, que permite carregar o novo arquivo JSON das dependências que substitui o arquivo gerado pela análise de dependências. Depois disso, o gráfico na etapa de decomposição será atualizado.

Para exportar, modificar e importar dependências

1. Na página Exibir resultados de decomposição, escolha Ações.
2. Na lista suspensa, escolha a opção Atualizar arquivo de dependências em Outras ações.
3. No modal Atualizar dependências do arquivo,
 - a. Baixe o arquivo de dependência AWS Transform criado a partir dos resultados da análise existente.
 - b. No arquivo baixado, modifique as dependências com base no que você deseja alcançar.
 - c. Depois de modificar, salve e carregue esse arquivo usando o botão Carregar arquivo de dependência.

 Note

O único formato de arquivo aceito é o arquivo JSON.

4. Em seguida, escolha Importar.

AWS O Transform importará o arquivo de dependências e criará um novo gráfico de dependências com base na sua entrada.

Importar domínios de and/or atualização

Para clientes que têm domínios, sementes e relacionamentos de and/or arquivos mapeados antes da etapa de decomposição, você pode carregar essa definição de domínio por meio da função Importar arquivo de domínios, disponível no menu Ações. Alguns exemplos de quando essa função pode ser utilizada:

- Antecipe a decomposição de outro trabalho
- Especialistas no assunto que fornecem esse mapeamento

Depois que o arquivo do domínio for importado, o usuário poderá executar a decomposição na definição do domínio ou, se estiver satisfeito, pode salvar e enviar a definição do domínio.

Parent/child/neighbor arquivos

Em um gráfico de dependências, os programas se relacionam entre si por meio de diferentes tipos de conexões. A compreensão dessas relações ajuda você a analisar as dependências do programa durante a transformação de seus aplicativos de mainframe. Também ajuda a entender os limites de um domínio. Por exemplo, se você selecionar um domínio e, em seguida, selecionar um nível principal, ele mostrará os nós conectados.

Relacionamentos com os pais — Um arquivo principal chama ou controla outros programas. Os pais estão acima dos programas dependentes na hierarquia. Você pode selecionar o pai em um nível ou em todos os níveis.

Relacionamentos com filhos — Um arquivo secundário é chamado ou controlado pelo programa principal. Os filhos estão abaixo dos pais na hierarquia de arquivos.

Relações entre vizinhos — Vizinhos são arquivos no mesmo nível hierárquico. Eles compartilham o mesmo programa principal e podem interagir diretamente uns com os outros.

Reforge o código

O Reforge usa modelos de linguagem grande (LLMs) para melhorar a qualidade do código refatorado. A COBOL-to-Java transformação inicial preserva a equivalência funcional enquanto retém estruturas de COBOL-influenced dados e nomes de variáveis do sistema legado. O Reforge reestrutura esse código para seguir práticas e expressões modernas de Java, substituindo COBOL-style construções por coleções Java nativas e convenções de nomenclatura. Isso torna o código mais legível e fácil de manter para desenvolvedores Java.

Note

As cotas para reforma são:

- 3.000.000 de linhas de código por trabalho
- 50.000.000 de linhas de código por usuário por mês

Reforje seu código após a refatoração seguindo estas etapas:

1. Escolha Reforge código java no painel de navegação esquerdo e selecione Configurar código reforge.
2. Forneça a localização do S3 para seu projeto de código-fonte compilável compactado e escolha Continuar. Use essa estrutura de zíper:

```
input.zip
  ### PROJECT-pom
  ### PROJECT-entities
  ### PROJECT-service
  ### PROJECT-tools
  ### PROJECT-web (optional)
  ### pom.xml
```

AWS O Transform analisa seu pacote zip para localizar arquivos dentro do PROJECT-service diretório para que ele possa fornecer uma lista selecionável de classes que você pode reformar. Essas classes têm o sufixo `ProcessImpl.java`.

3. Complete a página Selecionar classes a serem reforjadas e escolha Continuar. Acompanhe o status da reforma na guia Registro de trabalho.

4. Veja os resultados de sua reforma concluída na página Exibir resultados, que exibe o status da reforma por classe. Ele também especifica onde encontrar o resultado do Reforge em seu bucket do S3.

Depois que o AWS Transform recebe essa entrada de você, ele fornece um arquivo para download com os resultados do Reforge.

Esta é a estrutura zip resultante de uma reforma bem-sucedida:

```
reforge.zip
### maven_project
### reforge.log
###tokenizer_map.json
```

- maven_project contém o código-fonte reforjado.
 - Os arquivos que foram refatorados, mas cuja compilação não foi finalizada com êxito, estão localizados em e são nomeados. /src/main/resources/reforge/originalClassName.java.incomplete originalClassName.java.incomplete Compare-os com as versões originais dos arquivos para escolher as funções reforjadas que você deseja salvar.
 - Os arquivos de origem fornecidos ao AWS Transform que foram refatorados com sucesso são copiados src/main/resources/reforge/originalClassName.java.original e nomeados. originalClassName.java.original As versões refatoradas dos arquivos substituem os arquivos de origem fornecidos ao Transform. AWS

 Note

Os originalClassName.java arquivos são substituídos pelos arquivos reforjados somente se o processo de reformulação for bem-sucedido. Caso contrário, eles retêm o conteúdo original.

- O reforge.log contém registros que você pode usar para diagnosticar falhas de trabalho ou fornecer AWS suporte em caso de problema.
- tokenizer_map.json contém um mapeamento de IDs de token para seus dados, como caminhos e class/method nomes de arquivos, que são tokenizados nos registros para proteção de privacidade. Você pode fornecer esse arquivo para AWS suporte em caso de problema.

Planeje seus testes de aplicativos modernizados

Você pode criar e gerenciar planos de teste para seus aplicativos modernizados de mainframe com base nos atributos de código extraídos, na complexidade do trabalho e nos caminhos do agendador. AWS O Transform ajuda a priorizar quais trabalhos testar e identifica os artefatos específicos necessários para cada caso de teste. O processo de planejamento do teste é dividido em três fases principais: configuração, escopo e revisão.

Para criar um plano de teste

1. Definir as configurações do plano de teste
 - a. No painel de navegação esquerdo, em Planejar seus testes, escolha Definir configurações.
 - b. (Opcional) Forneça caminhos S3 para sua extração lógica de negócios (BLE). Esses artefatos aprimoram a qualidade do plano de teste. Sem artefatos BLE, alguns campos no plano de teste podem permanecer incompletos.
2. Defina o escopo do plano de teste
 - a. Selecione pontos de entrada, como trabalhos em lotes, para incluir em seu plano de teste.
 - b. Filtre e classifique trabalhos com base em vários atributos:
 - Funções de negócios (extraídas do BRE BLE)
 - Domínios (da fase de decomposição)
 - Caminhos e localizações de arquivos
 - Critérios de pesquisa personalizados
 - c. Selecione trabalhos individuais ou grupos inteiros para testes.
 - d. Analise as relações de trabalho e as dependências.
3. Revise e ajuste o plano de teste

O plano de teste gerado fornece informações abrangentes, incluindo:

- Ordem de execução preferencial com base nas dependências
- Tarefas de grupos de trabalho a partir do agendador
- Pontuações de complexidade, que são pontuações agregadas para casos de teste
- Associações de domínio comercial
- Métricas de complexidade ciclomática

- Dependências de conjuntos de dados e tabelas
- Linhas de métricas de código
- Mapeamentos de funções de negócios

Opções de personalização do plano de teste

Seu plano de teste pode ser personalizado para atender a necessidades específicas. Por exemplo, você pode:

- Crie novos casos de teste selecionando vários pontos de entrada
- Mescle casos de teste existentes para combinar funcionalidades relacionadas
- Divida os casos de teste para testes mais granulares
- Remova casos de teste desnecessários
- Adicione ou remova pontos de entrada para casos de teste existentes
- Modifique as descrições e os atributos dos casos de teste
- Ajustar a ordem de execução

Informações detalhadas do caso de teste

Cada caso de teste fornece detalhes que descrevem seu conteúdo e o conjunto de dados ou arquivos de dados relacionados:

- Descrição abrangente do escopo do teste
- Lista completa de pontos de entrada incluídos
- Métricas agregadas que mostram complexidade e tamanho
- Regras de negócios e orientação automatizada de casos de teste
- Dependências de conjuntos de dados e tabelas com direction () input/output
- Visualização interativa do gráfico de dependências
- Pré-requisitos e requisitos de execução

Recursos de gerenciamento de dados

Esses detalhes ajudam você a entender os dados relacionados ao caso de teste. Você pode:

- Filtrar conjuntos de dados por input/output direção
- Identifique os artefatos necessários para a execução do teste
- Acompanhe as dependências de dados entre os casos de teste
- Monitore o uso do conjunto de dados em todos os planos de teste

 Note

AWS O Transform analisa automaticamente as dependências do agendador e atribui pontuações de complexidade para ajudar a priorizar os esforços de teste. Pontuações mais altas de complexidade indicam trabalhos que podem exigir testes ou isolamento mais completos durante o processo de teste.

Regras de negócios e orientação de casos de teste

O plano de teste AWS Transform fornece recomendações para seu plano de caso de teste com base na extração de regras de negócios:

- Processamento automático de regras de negócios usando LLM
- Geração de casos de teste sintéticos
- Orientação de teste para cenários comerciais específicos
- Rastreabilidade entre regras e casos de teste

O plano de teste final é armazenado no local especificado do S3 e inclui todas as informações necessárias para executar sua estratégia de teste com eficiência. Você pode exportar o plano de teste para integração com outras ferramentas de teste ou sistemas de documentação.

 Note

Embora a orientação sintética do caso de teste seja fornecida, os artefatos de teste reais devem ser criados separadamente com base na orientação. O plano de teste serve como um modelo abrangente para sua estratégia de teste, mas não gera os dados de teste nem os scripts de execução.

Regras de criação de casos de teste - Resumo

Regras gerais

- Um caso de teste contém de 1 a muitos JCLs na ordem de execução do cronograma
- Os casos de teste são criados a partir de agendadores compatíveis válidos (CA7 e) Control-M
- O teste executa JCLs, não o agendador em si ou tarefas agendadas
- Uma tarefa agendada é exclusiva e executa somente um JCL
- Um JCL pode ser executado por várias tarefas agendadas
- Um JCL pode existir sem estar em um cronograma

Regras padrão de criação de casos de teste

- Se um único JCL estiver em um caso de teste:
 - A JCL não está envolvida com um cronograma
 - O JCL é executado por uma tarefa agendada que diverge em várias ramificações
 - Uma ramificação na programação contém somente esse JCL
- Se houver vários JCL em um caso de teste: representa uma sequência de caminho de execução linear em uma ramificação do cronograma
- Se a JCL estiver em uma tarefa agendada divergente: a JCL se torna seu próprio caso de teste separado
- Se a JCL estiver em uma tarefa agendada convergente: a JCL pode iniciar um novo caso de teste, mas não será incluída nas ramificações anteriores
- Os JCLs ausentes são ignorados e a execução continua (com aprimoramento futuro planejado para cortar o caso de teste no ponto JCL ausente)

Regras de operações do usuário

- Criar caso de teste: o usuário seleciona entre os JCLs disponíveis
 - Terá êxito se existirem JCLs na sequência de ramificações de execução do cronograma
 - Segue a ordem de execução do cronograma
- Adicionar um JCL ao caso de teste: o usuário seleciona entre os JCLs disponíveis
 - É bem-sucedido se o JCL puder existir na execução do cronograma do caso de teste branch/path

- Remover JCL do caso de teste: o usuário pode remover qualquer JCL de um caso de teste
 - Permitido mesmo que cause lacunas no caminho de execução
- Mesclar casos de teste: o usuário seleciona dois casos de teste para combinar
 - É bem-sucedido se os JCLs puderem existir juntos na mesma ramificação de execução do cronograma
 - Mantém a ordem de execução do cronograma
- Caso de teste dividido: o usuário seleciona um JCL em um caso de teste para divisão
 - Cria um novo caso de teste a partir do ponto de divisão
 - Caso de teste original modificado para excluir o ponto de divisão anterior do JCL
- Excluir caso de teste: o usuário pode excluir qualquer caso de teste criado

Note

Você não pode criar, adicionar ou mesclar casos de teste de um agendador branches/path diferente. Um futuro aprimoramento está planejado para permitir operações além das divergent/convergent tarefas no agendador.

Gere scripts de coleta de dados de teste

Você pode gerar scripts JCL para coletar dados de teste de seus sistemas de mainframe com base no plano de teste criado na etapa anterior. AWS O Transform cria automaticamente scripts de coleta de dados para conjuntos de dados, tabelas de banco de dados e arquivos sequenciais necessários para testes abrangentes. O processo de coleta de dados é dividido em quatro fases principais: configuração de entrada, seleção de casos de teste, configuração de scripts e geração de scripts.

Para gerar scripts de coleta de dados de teste

1. Forneça informações sobre o plano de teste
 - a. No painel de navegação esquerdo, em Coleta de dados de teste, escolha Fornecer entrada do plano de teste.
 - b. Especifique o caminho do S3 para o arquivo JSON do seu plano de teste em [Planejar seus testes de aplicativos modernizados](#).
 - c. O campo de entrada é pré-preenchido se o plano de teste tiver sido gerado em uma etapa anterior do trabalho.

- d. Você também pode selecionar o plano de teste de outros trabalhos especificando a localização apropriada do S3.
2. Selecione casos de teste para coleta de dados
 - a. Analise a lista completa de casos de teste do seu plano de teste.
 - b. Filtre e classifique os casos de teste com base em vários atributos:
 - Funções e domínios de negócios
 - Dependências da tabela do banco de dados
 - Requisitos do conjunto de dados
 - Métricas de complexidade
 - Critérios de pesquisa personalizados
 - c. Selecione casos de teste individuais ou use opções de seleção em massa.
 - d. Analise os detalhes do caso de teste, incluindo pontos de entrada, métricas e regras de negócios, clicando em um caso de teste para ver os detalhes.
3. Configurar scripts de coleta de dados
 - a. Baixe modelos de amostra e arquivos de configuração para referência.
 - AWS O Transform fornece modelos de amostra para descargas de banco de dados Db2, arquivo VSAM REPRO e processamento sequencial de conjuntos de dados para serem usados como orientação sobre os tipos de modelo esperados pelo processo.
 - Os padrões podem variar de site para site, portanto, a expectativa é que os clientes modifiquem ou substituam esses modelos de acordo com seus próprios padrões.
 - Esses modelos modificados precisam ser carregados em um bucket do S3, onde a coleta de dados de teste possa processá-los.
 - b. Forneça arquivo de configuração variável (formato JSON) contendo:
 - Prefixos de usuário e constantes específicas do ambiente
 - Parâmetros de configuração do banco de dados
 - Configurações do endpoint de destino e parâmetros de transferência de dados
 - Outros parâmetros necessários definidos pelo usuário e a serem usados em modelos JCL
 - c. Faça upload de modelos de JCL para diferentes métodos de coleta de dados:

- Modelo Db2: Para descarregar tabelas de banco de dados (personalize para BMC, IBM DSN ou outros utilitários de descarga)
- Modelo VSAM: para processamento de arquivos VSAM (normalmente usa o utilitário REPRO)
- Modelo de conjuntos de dados sequenciais: para processar conjuntos de dados sequenciais, conjuntos de dados particionados, GDGs etc.

4. Revise e gerencie scripts gerados

Os scripts gerados fornecem recursos abrangentes de coleta de dados, incluindo:

- Scripts separados para coleta de dados “antes” e “depois” da execução do teste
- Estrutura de script organizada por caso de teste e tipo de dados
- Os scripts são armazenados automaticamente no bucket do S3 para facilitar o acesso e a transferência
- Os scripts JCL gerados estão prontos para execução no mainframe
- A substituição de variáveis é baseada na configuração do usuário definida nos modelos

Recursos de geração de scripts

Os scripts gerados são personalizados automaticamente com base em seus modelos e configuração:

- Template-based geração: usa os modelos JCL fornecidos com substituição de variáveis
- Ambiente: incorpora sua configuração específica de mainframe
- Tratamento de tipos de dados: cria scripts apropriados para conjuntos de dados sequenciais, arquivos VSAM e tabelas de banco de dados
- Coleta para casos de teste: gera scripts de coleta de dados “antes” e “depois”
- Processamento sequencial do conjunto de dados: a amostra AWS fornecida fornece uma função de transferência de arquivos, mas ela pode ser personalizada para utilitários de compactação disponíveis em seu site ou utilitários como Connect Direct ou transferência gerenciada de arquivos, etc.

Estratégia de coleta de dados

Os scripts gerados oferecem suporte a estratégias abrangentes de coleta de dados:

- Coleta sequencial de conjuntos de dados: utilitários REPRO e de cópia para VSAM e arquivos simples
- Descarregamento da tabela do banco de dados: processos de descarregamento do Db2 personalizáveis
- Processamento sequencial de conjuntos de dados: pós-processamento personalizável de conjuntos de dados sequenciais, como compactação, serviços gerenciados de transferência de arquivos, etc.
- Gerenciamento de dependências: coleta coordenada com base na definição do caso de teste

 Note

AWS O Transform gera scripts com base em seus modelos e configurações. Analise todo o JCL gerado antes de executá-lo em seu ambiente de mainframe para garantir a compatibilidade com a configuração específica do sistema e os requisitos de segurança.

Personalização de modelos e melhores práticas

A coleta de dados de teste ATX fornece recursos flexíveis de personalização de modelos:

- Multi-utility suporte: Adapte modelos para diferentes utilitários de mainframe (BMC, IBM, DSN)
- Variable-driven configuração: use constantes para parâmetros específicos do ambiente
- Modelos reutilizáveis: crie modelos padronizados para geração consistente de scripts
- Tratamento de dados: incorpore os requisitos de tratamento de dados específicos da organização
- Integração de segurança: inclua controles adequados de segurança e acesso
- Otimização de desempenho: configure para coleta e transferência eficientes de dados

Estrutura de saída gerada

Os scripts gerados são organizados em seu bucket do S3 com a seguinte estrutura:

- Organização do caso de teste: scripts agrupados por casos de teste associados
- Tempo de coleta: pastas separadas para “antes” e “depois” da coleta de dados
- Classificação do tipo de dados: scripts organizados por conjuntos de dados sequenciais, tabelas de banco de dados e transferências

- Arquivos de metadados: informações resumidas e orientação de execução
- Ready-to-transfer formato: JCL formatado para implantação direta de mainframe

A coleção final de scripts é armazenada no local especificado do S3 e inclui todo o JCL necessário para executar sua estratégia de coleta de dados com eficiência. Você pode baixar os scripts para transferir para seu ambiente de mainframe ou integrá-los aos processos de implantação automatizados.

 Note

Embora scripts JCL abrangentes sejam gerados, a execução real deve ser executada em seu ambiente de mainframe. Os scripts servem como ferramentas de coleta de dados prontas para uso, mas exigem permissões apropriadas de acesso e execução ao mainframe.

Geração de scripts de automação de testes

Você pode gerar scripts de automação de teste para executar casos de teste em seu aplicativo modernizado com base no plano de teste criado na etapa anterior. AWS O Transform cria automaticamente scripts de teste abrangentes que utilizam os dados coletados do processo de coleta de dados de teste. O processo de geração de scripts de automação de testes consiste em três fases principais: configuração de entrada, seleção de casos de teste e resultados de geração de scripts.

Para gerar scripts de teste

1. Forneça informações sobre o plano de teste
 - a. No painel de navegação esquerdo, em Geração de script de automação de teste, escolha Fornecer entrada do plano de teste.
 - b. Especifique o caminho do S3 para o arquivo JSON do seu plano de teste em [Planejar seus testes de aplicativos modernizados](#).
 - c. O campo de entrada é pré-preenchido se o plano de teste tiver sido gerado em uma etapa anterior do trabalho.
 - d. Você também pode selecionar o plano de teste de outros trabalhos especificando a localização apropriada do S3.
 - e. O sistema usa esse plano de teste como base para gerar scripts de automação.

2. Selecione casos de teste para geração de scripts

- a. Analise a lista completa de casos de teste do seu plano de teste.
- b. Filtre e classifique os casos de teste com base em vários atributos:
 - Funções e domínios de negócios
 - Dependências da tabela do banco de dados
 - Requisitos do conjunto de dados
 - Métricas de complexidade
 - Critérios de pesquisa personalizados
- c. Selecione casos de teste individuais ou use as opções de seleção em massa com os botões Marcar tudo e Desmarcar tudo.
- d. Analise os detalhes do caso de teste, incluindo pontos de entrada, métricas e regras de negócios, clicando nos casos de teste individuais.

Os casos de teste selecionados terão scripts de automação gerados para execução no aplicativo modernizado.

3. Revise e gerencie os scripts de automação de testes gerados:

- O sistema exibe uma mensagem de sucesso confirmando a conclusão da geração do script.
- Os scripts de teste gerados são armazenados automaticamente no local especificado do bucket do S3.
- Acesse a lista completa dos scripts de teste gerados com suas respectivas localizações do S3.
- Cada caso de teste tem seu script de automação correspondente armazenado em locais individuais do S3.
- Os scripts estão prontos para implantação e execução em seu ambiente de aplicativos modernizado.

Recursos do script de automação de testes

Os scripts de automação gerados fornecem recursos de teste abrangentes:

- Teste de aplicativo modernizado: os scripts são projetados especificamente para executar casos de teste em seu aplicativo transformado

- Integração de dados: utiliza os dados de teste coletados na etapa anterior de coleta de dados de teste. Esses dados precisam ser copiados para pastas para cada caso de teste
- Execução automatizada: os scripts podem ser usados para configurar coletores de dados, executar casos de teste e comparar resultados. Alguns parâmetros precisarão ser definidos de acordo com seu ambiente de implantação
- Estrutura organizada: os scripts são organizados sistematicamente por caso de teste em seu bucket do S3
- Ready-to-deploy formato: os scripts são formatados para implantação direta em seu ambiente de teste

Estrutura de saída gerada

Os scripts de automação de teste gerados são organizados em seu bucket do S3 com a seguinte estrutura:

- Organização do caso de teste: cada caso de teste tem seu script dedicado armazenado em uma pasta S3 individual
- Execution-ready formato: os scripts são formatados para implantação e execução imediatas após a configuração de alguma variável, dependendo do seu ambiente
- Acesso centralizado: todos os scripts podem ser acessados em um único local de bucket do S3 para facilitar o gerenciamento

Estratégia de execução de testes

Os scripts gerados oferecem suporte a fluxos de trabalho abrangentes de execução de testes:

- Configuração do ambiente: os scripts incluem recursos para configurar os dados iniciais para executar o teste
- Preparação de dados: integração com os dados de teste coletados da etapa de coleta de dados do caso de teste
- Execução de casos de teste: execução automatizada de casos de teste individuais no aplicativo modernizado
- Comparação de resultados: Built-in recursos para comparar resultados de testes e validar o comportamento do aplicativo

 Note

AWS O Transform gera scripts de automação de teste com base no seu plano de teste e nos casos de teste selecionados. Os scripts são projetados para execução em seu ambiente de aplicativos modernizado e utilizam os dados de teste coletados na etapa anterior. Revise todos os scripts gerados antes da implantação para garantir a compatibilidade com os requisitos específicos de configuração e teste do aplicativo.

Melhores práticas para automação de testes

- Validação do ambiente: garanta que seu ambiente de aplicativos modernizado esteja configurado adequadamente antes da execução do script
- Verificação de dados: valide se os dados de teste necessários da fase de coleta estão disponíveis e acessíveis
- Personalização do script: revise e personalize os scripts gerados conforme necessário para seus requisitos específicos de teste
- Monitoramento de execução: implemente monitoramento e registro apropriados durante a execução do script de teste
- Análise de resultados: Estabeleça processos para analisar os resultados dos testes e identificar problemas de aplicação

A coleção final de scripts de automação de testes fornece uma estrutura de teste completa para validar a funcionalidade modernizada do seu aplicativo. Os scripts podem ser integrados aos seus processos de teste contínuos ou executados como parte do fluxo de trabalho de validação do aplicativo.

Capacidades de implantação em AWS Transformação

AWS O Transform ajuda você a configurar ambientes de nuvem para aplicativos de mainframe modernizados, fornecendo modelos de infraestrutura como código (IaC) prontos para uso. Por meio da interface de bate-papo do AWS Transform, você pode acessar modelos pré-criados que criam componentes essenciais, como recursos computacionais, bancos de dados, armazenamento e controles de segurança. Os modelos estão disponíveis em formatos populares, incluindo CloudFormation (CFN) e Terraform, oferecendo flexibilidade para implantar sua infraestrutura. AWS Cloud Development Kit (AWS CDK)

Esses modelos servem como elementos básicos que reduzem o tempo e a experiência necessários para configurar ambientes para seus aplicativos de mainframe modernizados. Você pode personalizar esses modelos para atender às suas necessidades, fornecendo uma base para criar seu ambiente de implantação.

Para recuperar os modelos de IaC, peça no bate-papo do AWS Transform os Infrastructure-as-Code modelos que esclarecem seu padrão de modernização preferido (como o AWS Transform for mainframe refactor), sua topologia preferida (independente versus alta disponibilidade) e seu formato preferido (versus Cloud Development CloudFormation Kit versus Terraform).

Crie e implante seu aplicativo modernizado após a refatoração

Depois de concluir o processo de refatoração com o AWS Transform, você pode criar e implantar seu aplicativo Java modernizado. Este guia explica como recuperar seu código modernizado, configurar seu ambiente e implantar e testar seu aplicativo.

Note

Além da orientação fornecida aqui, o pacote de código gerado pelo AWS Transform incluirá um documento Configurar o AWS Automated Refactor Development Environment, que fornece instruções para configurar um IDE (Ambiente de Desenvolvimento Integrado) com o [Developer Runtime](#).

Tópicos

- [Pré-requisitos](#)
- [Etapa 1: recuperar o código modernizado](#)
- [Etapa 2: criar o aplicativo modernizado](#)
- [Etapa 3: Configurar o ambiente de teste](#)
- [Etapa 4: implantar o aplicativo modernizado](#)
- [Etapa 5: testar o aplicativo modernizado](#)
- [Exemplo adicional](#)

Pré-requisitos

Antes de começar, você deve ter o seguinte:

- Concluiu com êxito um trabalho de refatoração com o Transform. AWS
- Acesso ao seu código modernizado.
- [Pilha de ferramentas de software de compilação instalada e configurada em sua máquina de desenvolvimento, como Apache Maven ou Apache Tomcat](#). Para obter mais informações sobre o controle de versão do Runtime, consulte as notas de lançamento do [AWS Transform for mainframe Runtime](#).
- Instalou e configurou o Amazon Corretto ou uma versão do Java Runtime. Para obter mais informações sobre a instalação do Amazon Corretto, consulte Amazon [Corretto 24](#).
- Acesso para criar e configurar bancos de dados Amazon Aurora PostgreSQL para componentes do Runtime, se necessário. [Para obter mais informações sobre a criação do banco de dados Aurora PostgreSQL, consulte Trabalhando com o Amazon Aurora PostgreSQL](#).
- Acesso administrativo para implantar aplicativos em seu ambiente de execução.
- Analisou os conceitos do [AWS Transform for mainframe Runtime para ver os](#) conceitos fundamentais sobre aplicativos modernizados com a solução de refatoração AWS automatizada.

Etapa 1: recuperar o código modernizado

Para recuperar o código modernizado

1. Baixe e extraia o pacote de código gerado.
2. Abra codebase/app-pom/pom.xml e anote a versão necessária do mecanismo de tempo de execução. Por exemplo, `<gapwalk.version>4.6.0</gapwalk.version>`.
3. Localize o documento Configurar o AWS Automated Refactor Development Environment no pacote de código baixado para referência.

Etapa 2: criar o aplicativo modernizado

Para criar seu aplicativo modernizado

1. Acesse o Runtime na caixa de ferramentas do AWS Transform for mainframe.
2. Baixe e instale a versão de tempo de execução apropriada (identificada em [the section called “Etapa 1: recuperar o código modernizado”](#)) em sua máquina de desenvolvimento local.

 Note

Informações adicionais para instalar as dependências de tempo de execução em sua máquina local estão disponíveis na seção 3.1 do documento Configurar o ambiente de desenvolvimento de refatores AWS automatizados.

3. Abra o prompt de comando e navegue até o diretório raiz do seu aplicativo.
4. Para criar pacotes implantáveis para o aplicativo modernizado, execute o comando de compilação do Maven:

```
mvn package
```

Consulte a página [Organização do Aplicativo](#) para obter detalhes sobre a organização básica do código modernizado. Por exemplo, para aplicativos modernizados contendo um aplicativo web front-end, você pode esperar pelo menos os seguintes `.war` agregados implantáveis, além dos componentes de tempo de execução:

- Projeto de serviço: contém elementos legados de modernização da lógica de negócios

```
<business-app>-service.*.war
```

- Projeto Web: contém a modernização dos elementos relacionados à interface do usuário

```
<business-app>-web.*.war
```

Etapa 3: Configurar o ambiente de teste

Para configurar seu ambiente de teste

1. Configure o tempo de execução de seu aplicativo modernizado. Para obter mais informações, consulte a seção [Configurar o Runtime](#) no guia AWS Mainframe Modernization do usuário.

 Note

Consulte a seção 5 do guia Configurar o ambiente de desenvolvimento de refatores AWS automatizados para ver exemplos de configuração específicos de componentes de tempo de execução.

2. Prepare conjuntos de dados de entrada e saída (I/O) para aplicativos modernizados. Aplicativos modernizados podem processar conjuntos de I/O dados sequenciais, conjuntos de dados VSAM ou outros.

 Note

Consulte a seção 6 de Configurar o ambiente de desenvolvimento AWS automatizado de refatores para ver exemplos.

3. Um ambiente de tempo de execução - Você pode usar seu ambiente de tempo de execução existente ou criar um novo ambiente de tempo de execução.
 - Para configurar um ambiente de tempo de execução não gerenciado, consulte [Configurar um aplicativo não gerenciado](#).
 - Para configurar um ambiente de tempo de execução gerenciado, consulte [Configurar um aplicativo gerenciado](#).

Depois de configurar o ambiente de teste, você passa para a próxima etapa de implantação do aplicativo modernizado.

Etapa 4: implantar o aplicativo modernizado

Implante os artefatos do aplicativo no tempo de execução que você criou and/or configurado nas [the section called “Etapa 3: Configurar o ambiente de teste”](#) seções [the section called “Etapa 2: criar o aplicativo modernizado”](#) e.

Orientações adicionais para implantar o aplicativo modernizado podem ser encontradas usando estes links:

- [Implante no Amazon EC2](#)
- [Implemente em contêineres no Amazon ECS e no Amazon EKS](#)
- [Crie um AWS Mainframe Modernization aplicativo](#)

Etapa 5: testar o aplicativo modernizado

Após a implantação,

1. Analise as [APIs de tempo de execução](#) disponíveis para conhecer formas de interagir com os aplicativos modernizados.
2. Teste seu aplicativo para alinhar sua equivalência funcional com o aplicativo legado. Por exemplo, consulte [Testar um aplicativo de amostra](#) no guia AWS Mainframe Modernization do usuário.

Exemplo adicional

Para ver um exemplo específico de modernização do aplicativo de mainframe com o AWS Transform, consulte [Modernize o CardDemo](#) aplicativo de mainframe.

Full-stack Modernização do Windows

AWS O Transform fornece modernização completa do Windows, incluindo modernização do .NET e modernização do SQL Server.

O agente AWS Transform para .NET pode ajudá-lo a modernizar seus aplicativos .NET para serem compatíveis com o .NET multiplataforma. Você pode modernizar o .NET usando o [aplicativo web .NET](#) ou [o .NET IDE](#).

AWS O Transform for [SQL Server modernization](#) é um AI-powered serviço que automatiza a modernização completa dos bancos de dados Microsoft SQL Server e seus aplicativos .NET associados ao Amazon Aurora PostgreSQL. O serviço organiza toda a jornada de migração, desde a conversão de esquemas, migração de dados e modificação do código do aplicativo para corresponder ao novo PostgreSQL de destino, tornando suas equipes mais produtivas ao automatizar tarefas complexas e trabalhosas.

Tópicos

- [Modernizando o .NET com AWS Transformação](#)
- [Modernização do SQL Server](#)

Modernizando o .NET com AWS Transformação

O agente AWS Transform para .NET pode ajudá-lo a modernizar seus aplicativos .NET para serem compatíveis com o .NET multiplataforma. Esse recurso é chamado de modernização do .NET. Depois [AWS Transforme o ambiente](#) do AWS Transform, você pode criar um trabalho de transformação de modernização do .NET.

Experiências

AWS O Transform está disponível em várias experiências:

- Console web: para transformação em grande escala de até 500 repositórios por vez.
- Visual Studio IDE: transformação liderada pelo desenvolvedor de uma solução ou projeto trabalhando junto com o agente de forma interativa e iterativa. Recomendado para projetos de médio a grande porte.

Você pode alternar livremente entre o console web e o IDE para trabalhar em um trabalho de transformação.

Você também pode invocar o AWS Transform de outros IDEs e companheiros de código de IA:

- Kiro: transforme-se de Kiro usando o poder AWS Transform for Kiro.
- Outros companheiros de código de IA: transforme-se com seus assistentes de codificação de IA preferidos usando os agentes AWS Transform MCP.

Capacidades e características-chave

- Analise as bases de código.NET Framework a partir de seus sistemas de controle de origem, o que inclui NuGet suporte privado, identificação de dependências entre repositórios e fornecimento de um relatório de análise.
- Transformação automatizada de aplicativos legados do.NET Framework para o.NET multiplataforma, notificações por e-mail e um relatório resumido da transformação.
- Fácil integração com as plataformas de controle de origem (BitBucket, GitHub, e GitLab) para ingerir o código existente e enviar o código transformado para uma nova ramificação.
- Validação do código transformado por meio de testes unitários.

Versões e tipos de projeto compatíveis

AWS O Transform oferece suporte à transformação para essas versões do.NET:

- .NET Framework 3.5+
- .NET Core 3.1
- .NET 5.x+
- .NET 8

AWS O Transform pode se transformar nessas versões de destino do.NET:

- .NET 8
- .NET 10

AWS O Transform suporta a transformação desses tipos de projetos (somente em C#):

- Bibliotecas de classes
- Aplicativos de console
- ASP.NET:
 - Controlador Model View (MVC), incluindo Razor Views front-end
 - Back-ends de aplicativo de página única (SPA) (camadas de lógica de negócios)
 - API Web
 - Formulários da Web
- Projetos de teste unitário (NUnit, xUnit e MSTest)
- Serviços do Windows Communication Foundation (WCF)
- Projetos com versões multiplataforma fornecidas para NuGet pacotes privados ou de terceiros. Se um equivalente multiplataforma estiver ausente ou indisponível, o AWS Transform for .NET tentará fazer a conversão com o melhor esforço possível.

AWS O Transform também pode transformar os seguintes tipos de projeto em um domínio.NET moderno. Esse é um recurso de pré-visualização e pode não se transformar tão completamente quanto os tipos de projetos compatíveis.

- WinForms projetos de desktop.
- Projetos de desktop WPF.
- Projetos móveis do Xamarin.
- Projetos escritos em VB.NET.

Limitações

Para obter mais informações sobre cotas e limitações do AWS Transform, consulte [Cotas para AWS Transformação](#).

AWS A transformação não transforma o seguinte:

- Componentes da interface do usuário do Blazor
- DLLs Win32 que não têm bibliotecas compatíveis com o núcleo
- Repositórios que não contêm nenhuma solução.

AWS O Transform não modificará as ramificações originais do repositório e só poderá gravar em uma ramificação de destino separada especificada em seu plano de transformação.

Intervenção humana

Durante a portabilidade dos aplicativos.NET Framework para o.NET multiplataforma, você pode ser solicitado a fornecer informações ou aprovações nos seguintes cenários:

- Configure um conector para seu código-fonte e permissões
- Valide o plano de modernização proposto
- Carregar dependências de pacotes ausentes como NuGets
- Revise e aceite o código transformado

Mais informações

Você pode modernizar seu código.NET usando o aplicativo web AWS Transform ou o AWS Toolkit for. Visual Studio

- [Modernizando seu código.NET usando o AWS Transforme o aplicativo web](#)
- [Modernizando o.NET no IDE](#)
- [Melhores práticas para transformações do.NET](#)

Modernizando seu código.NET usando o AWS Transforme o aplicativo web

AWS O Transform for .NET é um novo AI-powered agente generativo projetado para modernizar aplicativos.NET legados. Você pode modernizar seu código.NET legado usando o aplicativo web AWS Transform ou a extensão Visual Studio AWS Toolkit.

Para modernizar seu código.NET usando o aplicativo web AWS Transform, navegue até o aplicativo web e siga estas etapas detalhadas:

1. [Criando o AWS Transforme o plano de trabalho do.NET](#)
2. [Criação de um conector de repositório de código-fonte](#)
3. [Confirmando seus repositórios para se preparar para a transformação](#)
4. [Resolvendo dependências de pacotes para se preparar para a transformação](#)

5. [Analisando seu plano para se preparar para a transformação](#)
6. [Transformando seu código.NET](#)

Criando o AWS Transforme o plano de trabalho do.NET

Depois de criar seu espaço de trabalho, na guia Trabalhos, selecione Criar trabalho. Em seguida, siga as instruções do AWS Transform no painel de bate-papo usando linguagem natural. Essas são as etapas típicas para criar um trabalho de modernização do.NET.

1. AWS O Transform perguntará qual tipo de trabalho de transformação você gostaria de criar. No chat, insira modernização do.NET.
2. AWS O Transform sugerirá um nome de trabalho e perguntará se você deseja alterar o nome do trabalho. Se você quiser alterar o nome do trabalho, diga AWS Transform em linguagem natural, por exemplo, altere o nome do trabalho para ExampleCorpDotNet1. Caso contrário, no chat, você pode aceitar o nome do trabalho sugerido. Depois de aceitar o nome do trabalho, o AWS Transform notifica você na janela de bate-papo de que está criando o trabalho.
3. AWS A transformação cria o trabalho de transformação.

Componentes do AWS Transforme o plano de trabalho do.NET

A exibição da tarefa AWS Transform.NET tem 5 guias que você seleciona nos ícones verticais na extremidade esquerda: Tarefas, Painel, Aprovações, Artefatos e Registro de trabalho. Cada guia tem um painel esquerdo e um painel central de bate-papo. Às vezes, um painel de colaboração correto pode aparecer para mostrar detalhes adicionais e solicitar informações humanas.

Tarefas (Job Plan)

Essa guia exibe seu plano de trabalho no painel esquerdo. Uma tarefa do.NET tem 5 etapas:

1. Obtenha recursos a serem transformados: nesta fase, você cria um conector para seu repositório de código usando o. AWS CodeConnections Dependendo das permissões do seu repositório, um administrador do repositório de código pode precisar aprovar o conector e dar ao AWS Transform acesso ao repositório.
2. Descubra recursos para transformação: Nessa fase, o AWS Transform descobre repositórios no controle de origem e você seleciona alguns ou todos eles para avaliação.
3. Avalie o código para transformação: os repositórios selecionados são avaliados e você pode visualizar os relatórios de avaliação.

4. Prepare-se para a transformação: nesta fase, o AWS Transform notifica você se alguma dependência estiver faltando em seus repositórios. Você pode carregar as dependências ausentes ou ignorá-las. Se você não for administrador do repositório, talvez um administrador precise aprovar o plano de transformação final.
5. Transformação: nessa fase, o AWS Transform transforma seu repositório e fornece o status contínuo durante a transformação até que ela seja concluída. Você pode revisar os relatórios de transformação para entender o que foi alterado e por quê.

Você pode ver o status de cada etapa:

- Não iniciado
- Aguarde a entrada do usuário
- Em andamento
- Completed

Painel

A guia Painel fornece um resumo de alto nível da transformação. Ele exibe métricas do número de trabalhos transformados, da transformação aplicada e do tempo estimado para concluir a transformação. Abaixo do painel, há uma tabela de repositórios e seus status - In-progress, Falha ou Sucesso.

Aprovações

As solicitações de aprovação para o trabalho são exibidas e concluídas nessa guia.

Artefatos

Jjob-related artefatos são carregados ou baixados dessa guia.

Log de trabalho

AWS O Transform registra suas ações na guia Registro de trabalho. O registro de trabalho fornece um registro detalhado das ações que o AWS Transform realiza, junto com as solicitações de entrada humana e suas respostas a essas solicitações.

Criação de um conector de repositório de código-fonte

Depois [Criando o AWS Transforme o plano de trabalho do.NET](#), na guia Tarefas, o painel esquerdo da janela AWS Transformar lista as fases do trabalho de transformação. A primeira fase é Obter recursos para serem transformados. Nessa fase, você pode convidar colaboradores e conectar um repositório de código-fonte. O painel direito da janela AWS Transform é onde você especifica os detalhes.

É necessário que cada tarefa de transformação tenha somente um conector de repositório de código-fonte. O agente AWS Transform usa esse conector para baixar sua base de código.NET de GitHub, GitLab, ou Bitbucket usando. [AWS CodeConnections](#) Você deve se configurar AWS CodeConnections na mesma região do seu trabalho de AWS transformação. Como alternativa, você pode [se conectar ao código-fonte no Amazon S3 em vez de um repositório](#) de código-fonte.

Note

Se você tiver um conector de repositório de código-fonte existente, o AWS Transform o notificará. Selecione Usar conector existente para usar esse conector. Se você não quiser usar o conector existente, consulte [Excluindo um conector existente](#) antes [Adicionando um novo conector](#). Você só pode ter um conector de repositório de origem por trabalho.

Adicionando um novo conector

Para criar um novo conector de repositório de código-fonte:

1. Insira o número da AWS conta que você gostaria de usar para o AWS CodeConnections conector.
2. Se você não configurou AWS CodeConnections a mesma AWS conta, [configure AWS CodeConnections](#).
3. Use o [AWS Developer Tools Console](#) para criar uma conexão com seu [Bitbucket](#), [GitHub](#), [Enterprise Server](#) ou [AzureDevOps](#) repositório. [GitLab](#)
4. Copie o Amazon Resource Name (ARN) da conexão que você criou.
5. Volte para AWS Transform e cole o ARN da conexão que você criou.
6. Insira um nome para o conector.

 Note

Não insira informações pessoais como parte do nome do conector.

7. Selecione Iniciar criação do conector.
8. AWS O Transform solicita a criação de um conector para a AWS conta que você inseriu, na mesma região do trabalho de transformação atual, e notifica que uma solicitação de aprovação está pronta para ser aprovada pelo AWS administrador no AWS Management Console. Selecione Copiar o link de verificação.
9. Se você for o AWS administrador, faça login na AWS conta e acesse o link de verificação para aprovar a solicitação de conexão. Se você não for o AWS administrador, forneça o link de verificação ao seu AWS administrador.
10. Depois que o AWS administrador aprovar a solicitação do conector, selecione Finalizar conector para concluir o processo de criação do conector. Se você quiser usar um conector diferente, selecione Reiniciar para reiniciar o processo de criação do conector.

A guia Colaboração também inclui detalhes sobre seu conector, que incluem:

- Status -- Aprovação aprovada ou pendente
- AWS ID da conta
- AWS Região
- ARN da conexão

Excluindo um conector existente

 Note

Se você tiver um conector de repositório de código-fonte existente, o AWS Transform o notificará. Selecione Usar conector existente ou Excluir e criar um novo conector.

Se você optar por excluir uma conexão de repositório de código-fonte existente, o AWS Transform o avisará antes de realmente excluir o conector.

1. Você pode excluir um conector existente de duas maneiras:

- a. Se o AWS Transform solicitar, você poderá selecionar Excluir e criar um novo conector.
 - b. Você também pode selecionar reiniciar no prompt. Para modificar esse conector, você deve reiniciar.
2. AWS O Transform avisa que a reinicialização excluirá o conector. Para excluir o conector, selecione Reiniciar novamente.
 3. AWS O Transform avisa novamente que a exclusão do conector removerá a conexão com seu repositório de terceiros, como Bitbucket, e. GitHub GitLab Além disso, qualquer AWS tarefa de transformação que esteja usando esse conector falhará se o conector for excluído. Para confirmar a exclusão, digite delete e selecione Excluir.
 4. Para adicionar um novo conector de repositório de código-fonte, consulte [Adicionando um novo conector](#).

Conecte-se ao código-fonte no Amazon S3

Você pode conectar o AWS Transform ao código-fonte no Amazon S3 como alternativa à [conexão de um repositório de código-fonte](#).

Organização do bucket S3

O código-fonte original e o código transformado são armazenados em um bucket comum do S3, organizado conforme mostrado abaixo. Você deve configurar seu bucket do S3 na mesma região do seu trabalho de AWS transformação. Faça upload do código-fonte no bucket como um arquivo zip no nível raiz. O arquivo zip deve conter uma pasta de nível superior para cada repositório.

Durante a transformação, o AWS Transform cria uma pasta de saída de transformação e armazena os resultados da transformação nessa pasta. A transformação cria um arquivo zip chamado transformed-code.zip contendo o código transformado. Isso inclui um relatório de diferenças de código chamado diff.txt que destaca as alterações no arquivo em nível de projeto.

```
<customer-bucket>/
### source-code.zip
    ### repo 1
    ### repo 2
    ### .....
    ### repo n
### transform-output/
    ### transformed-code.zip
```

Adicionando um novo conector S3

Para criar um novo conector de repositório de código-fonte do S3:

1. No AWS console, crie um bucket S3.
2. Faça upload do código-fonte como um arquivo zip no bucket do S3.
3. No aplicativo web AWS Transform, inicie um trabalho de transformação do.NET. Na etapa Conectar um repositório de código-fonte, selecione Conectar seu código-fonte no bucket do S3 e escolha Salvar.
4. Na próxima página, insira os detalhes do bucket do S3 e escolha Enviar.
 - a. Nome do conector
 - b. AWS ID da conta
 - c. Braço de caçamba S3
 - d. Chave de criptografia do bucket S3 (opcional)
5. Aprove o conector:
 - a. Na próxima página, copie o link de verificação.
 - b. Peça a um aprovador que navegue até o link para acessar a página de solicitação de criação do conector AWS Transform.
 - c. Escolha criar uma nova função ou usar uma função existente.
 - d. Depois de analisar a solicitação, escolha Salvar e aprovar para aprová-la.
6. Especifique a localização do arquivo zip do S3:
 - a. No aplicativo web AWS Transform, aguarde até que o status mostre Aprovado.
 - b. Na página Especificar localização do ativo, insira uma URL do S3 para o arquivo zip do código no formato `s3://bucket-name/zip-file-name` e escolha Enviar para AWS transformação.
 - c. O trabalho segue para a etapa Discovery para continuar a transformação.

Excluindo um conector S3

Para excluir um conector S3 existente:

1. No aplicativo web AWS Transform, selecione Gerenciar conectores no canto superior direito.
2. Na janela Gerenciar conectores, selecione o conector.

3. Escolha Excluir.

Confirmando seus repositórios para se preparar para a transformação

Depois [Criação de um conector de repositório de código-fonte](#), confirme seus repositórios como a primeira etapa da preparação para a transformação. Você pode:

- Revise e altere [Configurações padrão](#) que afetam o conteúdo do plano.
- Analise os repositórios descobertos e selecione quais avaliar para transformação.
- Analise o [relatório de avaliação do repositório](#) e converse com a AWS Transform sobre seu conteúdo.
- [Use o plano gerado por AWS Transformação](#).
- [Personalize o plano de transformação](#) usando o aplicativo web ou baixando um arquivo JSON, modificando-o e enviando-o para o Transform. AWS

Configurações padrão

Na seção Detalhes do trabalho da guia Colaboração, você pode definir o seguinte:

Na guia Tarefas, na etapa Preparar para transformação - Confirme os repositórios a serem transformados, você pode definir o seguinte:

- Defina o nome da ramificação de destino em que o código transformado é gravado no seu repositório.
- Defina a versão de destino do.NET:
 - .NET 8: transforme todos os projetos em .NET 8
 - .NET 10: transforme todos os projetos em.NET 10
- Você pode atualizar as configurações de Job padrão ou deixá-las como estão. Isso inclui:
 - Excluir projetos do.NET Standard do plano de transformação Essa configuração é selecionada por padrão. Quando selecionada, a opção AWS Transformar exclui qualquer projeto do.NET Standard do plano de transformação. Se você desmarcar essa configuração, os projetos do.NET Standard serão transformados, o que os tornará incompatíveis com o.NET Framework.
 - Verifique as NuGet fontes e obtenha versões de pacotes compatíveis com o.NET Permita que o AWS Transform pesquise e obtenha versões de pacotes compatíveis com o.NET para o código que você gostaria de transformar.

Revise o relatório de avaliação do repositório

O relatório de avaliação do repositório fornece uma visão tabular das informações sobre cada repositório detectado pelo Transform. AWS Isso inclui:

- Proprietário do repositório
- Filial avaliada
- N° de soluções
- N° de projetos
- Total de linhas de código
- Versões detectadas do.NET
- Tipos de projeto detectados
- N° de dependências privadas do Nuget
- N° de dependências públicas do Nuget
- Complexidade da transformação

Para baixar o arquivo:

1. No seu espaço de trabalho, selecione a guia Colaboração.
2. No painel Escolher repositórios, selecione Baixar e escolha Baixar como HTML ou Baixar como JSON.

Converse sobre o relatório resumido do repositório

O resumo do seu repositório pode ser muito longo. Use o chat para entender melhor seu conteúdo. Seu relatório está disponível para bate-papo quando você vê esta mensagem na guia Registro de trabalho: O relatório de avaliação agora está disponível no chat para consultas. Para abrir o bate-papo, clique no ícone hexagonal roxo no canto inferior direito do console web. Aqui estão alguns exemplos de solicitações:

- Liste todos os repositórios descobertos ou avaliados.
- Quantos projetos do.NET 6 foram descobertos na avaliação?
- Quais projetos têm a maior complexidade?

Use o plano gerado por AWS Transformação

Você pode optar por usar o plano AWS Transform criado a partir da descoberta de repositórios com maior probabilidade de sucesso na transformação, que inclui os últimos repositórios modificados, raiz e interdependentes.

AWS Transform lista alguns detalhes de alto nível sobre o plano de transformação, que incluem:

- **Número total de repositórios descobertos** Esse número de repositórios.NET legados que o AWS Transform descobriu usando seu conector de repositório de código-fonte. AWS O Transform pode digitalizar no máximo 1.000 repositórios em cada trabalho. Se você tiver mais repositórios para digitalizar ou transformar, poderá criar vários trabalhos de transformação.
- **Repositórios selecionados** O número de repositórios.NET herdados que o AWS Transform selecionou para transformação.
- **Dependências selecionadas** O número de dependências que os repositórios selecionados exigem, que o AWS Transform detectou automaticamente e adicionou ao plano de transformação.

A tabela **Repositórios selecionados** lista os repositórios selecionados. Você pode pesquisar repositórios por nome, navegar até páginas adicionais de repositórios e baixar um arquivo formatado em JSON que lista os repositórios selecionados e suas dependências. Você pode fazer qualquer alteração nessa exibição.

A tabela **Repositórios selecionados** lista os seguintes detalhes sobre os repositórios que o AWS Transform selecionou para transformação:

- **Nome do repositório**
- **Ramificação de origem**
- **Data e hora da última modificação**
- **Linhas de código** Isso permite que você veja se você está se aproximando dos limites da cota. Para obter mais informações, consulte [Cotas para AWS Transformação](#).
- **Repositórios dependentes** Você pode clicar no número de repositórios dependentes para ver mais detalhes sobre essas dependências.

Se você estiver satisfeito com o plano de AWS transformação gerado pelo Transform, selecione **Confirmar repositórios**.

Se você quiser fazer alterações no plano de AWS transformação gerado pelo Transform, selecione [Personalize o plano de transformação](#).

Personalize o plano de transformação

Se você optar por não fazer isso [Use o plano gerado por AWS Transformação](#), poderá personalizar a lista de repositórios a serem transformados usando uma das seguintes opções:

1. Selecione repositórios na tabela Repositórios selecionados.
 - a. Quando você adiciona um repositório ao plano, o AWS Transform seleciona as dependências do repositório para você e as adiciona automaticamente ao plano de transformação.
 - b. Você também pode desmarcar repositórios na tabela.
2. Faça o download da lista JSON de repositórios e ramificações gerada pelo AWS Transform.
 - a. Selecione Baixar e, em seguida, selecione Baixar como JSON.
 - b. Revise e modifique o JSON. Você pode remover repositórios ou soluções dentro de repositórios que não deseja transformar.
 - c. Faça o upload do JSON revisado selecionando Carregar plano personalizado.
 - d. Se o upload do JSON for bem-sucedido, a tabela Repositórios selecionados exibirá as seleções que você fez.
3. Você pode selecionar Mostrar repositórios dependentes para exibir a lista de repositórios que o AWS Transform descobriu como dependências dos repositórios selecionados.
4. Você pode repetir essas etapas, se necessário. Quando estiver satisfeito com seu plano personalizado, selecione Confirmar repositórios.

Resolvendo dependências de pacotes para se preparar para a transformação

Depois [Confirmando seus repositórios para se preparar para a transformação](#), se o AWS Transform encontrar dependências de pacotes ausentes, você deverá concluir esta etapa. Você pode executar um PowerShell script do Windows para obter as dependências de pacotes ausentes do mesmo dispositivo do seu ambiente de Visual Studio desenvolvimento ou pode recuperar os pacotes ausentes manualmente. Em seguida, faça o upload dos pacotes ausentes.

As dependências do Missing Package podem ser atualizadas de duas maneiras:

- Resolva usando o Conector de Artefatos: resolva configurando um Repositório de Artefatos (Conector ADO NuGet) por meio de um fluxo de trabalho HITL dedicado do Connect Artifact Repository, que é exibido quando um Conector de Artefato não está configurado e faltam pacotes.

- Atualizar pacote ausente: o AWS Transform lista os pacotes ausentes na tabela de dependências de pacotes ausentes. Você pode pesquisar um pacote ausente pelo nome na caixa de pesquisa. Essa tabela inclui os seguintes detalhes sobre os pacotes ausentes:
 - Nome
 - Repositórios associados
 - Status da versão do framework
 - Status da versão principal

Para resolver as dependências de pacotes ausentes, [Faça o upload dos pacotes ausentes](#).

Faça o upload dos pacotes ausentes

1. Se preferir, você pode baixar um script PowerShell auxiliar do Windows para recuperar as dependências de pacotes ausentes de dentro do seu Visual Studio ambiente de desenvolvimento. Ou você pode encontrar os pacotes ausentes manualmente.

Para usar o PowerShell script do Windows:

- a. Selecione Baixar PowerShell script do Windows.
 - b. Execute o script localmente com uma conexão ativa com os repositórios que contêm os arquivos de dependência de pacotes ausentes.
 - c. Esse script permite que você baixe as dependências de pacotes ausentes para seu ambiente local.
2. O script criará um único arquivo zip para você carregar, que inclui todas as dependências em um único arquivo. Você também pode fazer upload de arquivos individuais .nupkg ou compactados para cada dependência.
 3. Selecione Carregar arquivos do pacote.
 4. No modal Carregar arquivos de dependência, selecione Escolher arquivos e navegue até o local dos arquivos de pacote compactados ausentes em seu dispositivo.
 5. Selecione Carregar.
 6. AWS O Transform valida os arquivos que você enviou. Durante a validação, você não pode fazer nenhuma atualização. AWS O Transform relata o status de validação acima da tabela de dependências de pacotes ausentes.
 7. AWS O Transform também atualiza as colunas de status na tabela de dependências de pacotes ausentes, de Ausente para Resolvido. Se um pacote falhar na validação, seu status se tornará inválido. Para arquivos inválidos, faça o seguinte:

- a. Na tabela Dependências de pacotes ausentes, selecione o pacote inválido usando a caixa de seleção.
 - b. Selecione Remover arquivo carregado.
 - c. Isso muda seu status de volta para Ausente.
8. Depois de fazer o upload dos pacotes ausentes e resolver as dependências do pacote, selecione Continuar para revisar.

Se você selecionar Prosseguir para revisar sem resolver as dependências de pacotes ausentes, o AWS Transform perguntará se você gostaria de iniciar o trabalho de transformação sem os pacotes ausentes. Se você selecionar Ignorar as dependências de pacotes ausentes, o AWS Transform usará referências de montagem para transformar o código. Prosseguir com essa ação pode afetar os recursos relacionados.

Requisitos de estrutura de pastas

Para NuGet uploads, o AWS Transform requer:

- O .nuspec arquivo a ser colocado no nível raiz para pacotes carregados manualmente, ou
- Uso do PowerShell script fornecido para gerar a estrutura correta

Requisitos de correspondência de versões

- Status da estrutura: a AWS transformação tenta combinar a versão da dependência especificada no .csproj arquivo (código-fonte) com a versão da dependência carregada. Uma correspondência exata resulta em um status de sucesso.
- Status principal: o AWS Transform espera uma especificação da versão principal na seção de dependências do .nuspec arquivo enviado. Se um for encontrado, o status principal é Sucesso.

Formato de exemplo:

```
<dependencies>
  <group targetFramework="net8.0" />
</dependencies>
```

As versões comuns incluem:

- .NET 5.0 (net5.0)

- .NET 6.0 (net6.0)
- .NET 7.0 (net7.0)
- .NET 8.0 (net8.0)

Analizando seu plano para se preparar para a transformação

Depois [Confirmando seus repositórios para se preparar para a transformação](#), e [Resolvendo dependências de pacotes para se preparar para a transformação](#), o administrador da AWS conta deve revisar o plano de transformação e aprová-lo no AWS Transform.

AWS Transform exibe a lista do job de repositórios, repositórios dependentes e pacotes dependentes que foram selecionados para transformação.

Revisando o plano de transformação

AWS Transform exibe a lista do job de repositórios, repositórios dependentes e pacotes dependentes que foram selecionados para transformação.

Note

AWS O Transform pode transformar no máximo 100 dependências e repositórios por plano de transformação.

1. Se você não for o administrador da AWS conta, revise o plano de trabalho e, se você o aceitar, selecione Enviar para aprovação.
2. Se você for o administrador da AWS conta, deverá revisar o plano e, quando estiver pronto, aprová-lo para iniciar a transformação. Depois de revisar o plano de trabalho, selecione:
 - a. Rejeitar Se o trabalho foi criado por um usuário que não é o administrador da AWS conta, sugerimos que você notifique o criador do trabalho para reiniciá-lo.
 - b. Aprove e inicie a transformação.

A avaliação do trabalho inclui os seguintes detalhes:

1. Resumo do trabalho Isso inclui:
 - a. A ramificação de destino em que o AWS Transform colocará o código transformado.
 - b. A versão de destino do.NET, .NET 8.0 ou .NET 10.

- c. As configurações do trabalho:
 - i. Excluir projetos padrão.NET
 - d. Número de repositórios selecionados para transformação
 - e. Número de repositórios dependentes
 - f. Número de NuGet pacotes privados
 - g. Total de linhas de código para o trabalho
2. Repositórios selecionados Esses são os repositórios selecionados para transformação. Eles devem ser MVC, Web, Windows Communication Foundation (WCF), console, biblioteca de classes, estrutura de interface do usuário - páginas do Razor ou pacotes de teste unitário. Essa tabela inclui as seguintes informações:
- a. Nome
 - b. Ramificação de origem
 - c. Projetos apoiados
 - d. Linhas de código
 - e. Projetos detectados
 - f. Projetos ignorados
 - g. Dependências detectadas
3. Repositórios dependentes adicionados Esses são os repositórios dependentes adicionados para transformação. Eles devem ser MVC, Web, Windows Communication Foundation (WCF), console, biblioteca de classes, estrutura de interface do usuário - páginas do Razor ou pacotes de teste unitário. Essa tabela inclui as seguintes informações:
- a. Nome
 - b. Necessário para
 - c. Ramificação de origem
 - d. Projetos apoiados
 - e. Linhas de código
 - f. Projetos detectados
 - g. Projetos ignorados
4. Pacotes dependentes Esses são os pacotes dependentes adicionados para transformação. Eles devem ser MVC, Web, Windows Communication Foundation (WCF), console, biblioteca de classes, estrutura de interface do usuário - páginas do Razor ou pacotes de teste unitário. Essa tabela inclui as seguintes informações:

- a. Nome
- b. Repositórios associados
- c. Status da versão do framework
- d. Status da versão principal

Transformando seu código.NET

Depois que o administrador da AWS conta terminar [Analisando seu plano para se preparar para a transformação](#), você poderá ver o progresso da transformação na guia Painel do seu trabalho de transformação.

Note

Além de transformar repositórios e dependências, o AWS Transform pode executar projetos de teste unitário totalmente transformados (sem erros de compilação). AWS O Transform não tem acesso aos resultados do teste unitário antes da transformação e só pode compartilhar os resultados pós-transformação. Em seguida, você pode comparar seus dados de linha de base, antes da transformação, com os resultados da pós-transformação para entender possíveis lacunas.

No canto superior direito, você pode ver o status do trabalho, que tem um dos seguintes valores:

- Aguardando a entrada do usuário
- Tempo decorrido
- Em execução

Você também pode ver os seguintes ícones:

- Um ícone de parada de transformação
- Um ícone de atualização
- Um ícone de configurações

O painel fornece um resumo de alto nível da transformação. Ele mostra métricas do número de trabalhos transformados e da transformação aplicada, além do tempo estimado para concluir a transformação.

O painel inclui:

1. A seção Detalhes do trabalho de transformação, que lista as configurações padrão e os detalhes do trabalho de transformação, incluindo:
 - a. Destino da ramificação de destino Para transformar seu código, o AWS Transform cria uma nova ramificação para o código transformado em seu repositório de código.
 - b. Versão.NET de destino, .NET 8.0 ou .NET 10
 - c. O ID do trabalho AWS Transform.
 - d. As configurações do trabalho:
 - i. Excluir projetos padrão.NET
2. A seção Resumo da transformação contém:
 - a. O número de repositórios selecionados para transformação
 - b. O número de projetos a serem transformados
 - c. O total de linhas de código nesses repositórios e projetos

Após o início da transformação, os gráficos circulares aparecem nas seções Status do repositório, Status do pacote e Status do teste de unidade, exibindo o progresso em tempo real. O status do teste de unidade mostra o status dos testes de unidade localizados em seus repositórios que o AWS Transforms executa após a transformação para testar o código transformado. AWS O Transform compartilha os resultados do teste executado, junto com o nome do teste individual, para que os clientes revisem a lista de testes unitários aprovados e reprovados.

 Note

A seção Repositórios lista os repositórios que o AWS Transform recomenda ou que você selecionou para transformação. Selecione Baixar JSON para baixar uma lista de repositórios, dependências e pacotes em seu plano de transformação.

Analise os relatórios de transformação

Depois que um trabalho de transformação for concluído, você poderá baixar os [relatórios de transformação](#):

- [Relatório resumido de transformação](#): esse relatório fornece uma visão geral da transformação no formato HTML ou JSON. Baixe o relatório resumido da transformação na guia Painel. Selecione Baixar e escolha Baixar como HTML ou Baixar como JSON.
- [Relatório detalhado da transformação](#): esse relatório fornece informações detalhadas sobre uma transformação no formato HTML. Faça o download dos relatórios detalhados da transformação na guia Painel. Selecione um link Baixar relatório detalhado na lista de repositórios para baixar um relatório detalhado.

Converse com AWS Transform sobre o relatório de transformação

Você pode conversar com o AWS Transform sobre o relatório de transformação após o processamento completo do repositório ou após a conclusão do trabalho de transformação. A guia Registro de trabalho exibe essa mensagem para cada repositório disponível para bate-papo: os detalhes da *repository_name* transformação do repositório agora estão disponíveis no chat para consultas. Ela exibe esta mensagem quando a tarefa de transformação é concluída: A tarefa de AWS transformação é concluída.

Para abrir o bate-papo, clique no ícone hexagonal roxo no canto inferior direito do console web.

Aqui estão alguns exemplos de solicitações:

- Quais projetos foram transformados com sucesso?
- Quais projetos foram parcialmente transferidos?
- Quais alterações foram feitas no `repo_name` repositório?
- Quais pacotes foram atualizados no `project_name` projeto?

Modernizando o.NET no IDE

AWS O Transform inclui um assistente de IA interativo e agente no AWS kit de ferramentas para. Visual Studio Ele permite que você modernize aplicativos por meio de uma experiência conversacional, guiada passo a passo, diretamente em seu IDE. Para transformar uma solução ou projeto do.NET, o agente AWS Transform analisa sua base de código, determina as atualizações

necessárias para portar seu aplicativo e gera um relatório de avaliação e um plano de transformação antes do início da transformação.

A experiência do Visual Studio IDE oferece suporte à autenticação somente pelo IAM Identity Center. Para obter mais informações, consulte [Adicionar usuários no IAM Identity Center](#).

A experiência IDE oferece modos autônomos e interativos. Use o modo autônomo para transformação autônoma, adequado para trabalhos noturnos ou de longa duração. Use o modo interativo para trabalhar ao lado do agente no chat, com alta visibilidade da transformação, um plano de transformação personalizável e uma análise passo a passo de cada projeto. Você pode iterar para refinar os resultados ou mudar de direção até ficar satisfeito.

Quando uma tarefa de transformação está ativa, você pode interagir com três janelas:

- A janela de bate-papo é seu principal ponto de interação com o agente de transformação. Use o chat para fazer perguntas, discutir opções, orientar a transformação e iterar.
- A janela AWS Transform Job Plan mostra as etapas de progresso e é onde você pode baixar ou carregar artefatos ou visualizar as diferenças de alteração de código.
- A janela Registro de trabalho mostra um registro da atividade de transformação em linguagem natural.

AWS O Transform executa quatro tarefas principais para portar aplicativos.NET para o Linux:

- Atualiza as versões do.NET e do idioma — Atualiza o código.NET C# mais antigo para as versões atuais do.NET e do idioma.
- Migra do .NET Framework para o .NET multiplataforma: migra projetos e pacotes do .NET Framework dependente do Windows para o .NET multiplataforma compatível com Linux.
- Reescreve o código para compatibilidade com o Linux: refatora e reescreve componentes de código obsoletos e ineficientes.
- Gera um relatório de prontidão de compatibilidade com Linux — Para tarefas abertas em que a intervenção do usuário é necessária para criar e executar o código no Linux, o AWS Transform fornece um relatório detalhado das ações necessárias para configurar seu aplicativo após a transformação.

Para obter mais informações sobre como o AWS Transform realiza transformações.NET, consulte [Como AWS O Transform moderniza aplicativos.NET](#).

Para modernizar seu código.NET usando o AWS Transform from Visual Studio IDE, consulte o seguinte:

- [Modernizando o.NET usando AWS Transforme-se em Visual Studio](#)
- [Como AWS O Transform moderniza aplicativos.NET](#)
- [Solucionar problemas com transformações .NET no IDE](#)

Cotas

Para as cotas de AWS transformação do.NET no IDE, consulte [Cotas para AWS Transformação](#).

Modernizando o.NET usando AWS Transforme-se em Visual Studio

Conclua estas etapas para portar um Windows-based aplicativo.NET para um aplicativo.NET Linux-compatible multiplataforma com o AWS Transform em Visual Studio 2026 ou 2022.

Etapas 1: pré-requisitos

Antes de continuar, verifique se você baixou e instalou a [extensão AWS Toolkit com o Amazon Q](#) do Visual Studio Marketplace. Analise os [recursos](#) e [limitações](#) do AWS Transform para a modernização do.NET para confirmar se seu código pode ser transformado.

Etapas 2: Autenticar no Visual Studio

Para se conectar às suas AWS contas a partir do Toolkit for Visual Studio, abra o Guia de introdução à interface do usuário AWS do kit de ferramentas (interface de usuário de conexão):

1. No menu principal do Visual Studio, navegue até Extensões > AWS Kit de ferramentas > Introdução para abrir a página Introdução: AWS kit de ferramentas.
2. Selecione AWS Transformar autenticação.
3. Escolha um perfil existente ou crie um novo. Ao criar um novo perfil, insira um nome para o perfil e sua URL inicial do AWS Transform, que foi enviada por e-mail para você depois que você foi adicionado ao IAM Identity Center pelo administrador.
4. Selecione Conectar. Siga as instruções para fazer login e conceder permissões de acesso por meio do seu navegador da web. No Visual Studio, você deve ver Conectado com o IAM Identity Center.
5. Depois de fazer login, você será direcionado ao AWS Transform Dashboard. Nessa página inicial, você pode fazer o seguinte:

- Selecione um perfil de AWS transformação (região)
- Selecione ou crie um espaço de trabalho
- Exibir o status dos trabalhos de transformação

Etapa 3: transformar seu aplicativo

Para transformar sua solução ou projeto .NET, realize o seguinte procedimento:

Comece a transformação

1. Abra qualquer solução ou projeto VB.NET baseado em C# ou Visual Studio que você queira transformar.
2. No Solution Explorer, clique com o botão direito do mouse em uma solução ou projeto que você deseja transformar e escolha Port with AWS Transform.
3. A caixa de diálogo Porta com AWS transformação é exibida.
 - a. No menu suspenso Escolha um espaço de trabalho, crie um espaço de trabalho ou selecione um existente. Os espaços de trabalho tornam sua atividade visível no aplicativo web AWS Transform, onde você pode convidar colaboradores para ver e conversar sobre trabalhos de transformação.
 - b. No menu suspenso Escolher um destino .NET, selecione a versão do .NET para a qual você deseja atualizar.
 - c. Para Modo de transformação, selecione Autônomo para transformação autônoma ou Interativo para transformação interativa.
 - d. Escolha Iniciar para começar a transformação.
4. Quando o trabalho de transformação é iniciado, as janelas AWS Transform Job Plan, Chat e Worklog são exibidas.

Plano de avaliação e transformação

1. Depois que o AWS Transform analisa seu código, um relatório de avaliação e um plano de transformação são exibidos no chat. No modo interativo, o bate-papo será pausado para que você os revise. Se você preferir não revisar no chat, você pode usar estas alternativas:
 - Para visualizar a avaliação ou o plano no editor de código, escolha Mostrar avaliação ou Mostrar plano de transformação na janela AWS Transform Job Plan.

- Para baixar a avaliação ou o plano, use o ícone de download na janela Job Plan.
2. Opcionalmente, modifique o plano de transformação. Você pode discutir o plano por meio do chat, por exemplo, explorando outras opções. Você faz alterações no plano dando instruções no chat ou carregando um plano de transformação revisado usando o ícone de download na janela Job Plan. Você pode adicionar, remover ou modificar etapas livremente. O Chat confirmará sua compreensão de suas instruções com um plano revisado.
 3. Opcionalmente, faça o upload de documentos de direção. Na janela de bate-papo, use o ícone de upload para fazer upload de documentos de orientação, como especificações do aplicativo, preferências e convenções da pilha de tecnologia organizacional ou exemplos de codificação. Depois de fazer o upload de um documento de orientação, descreva-o na janela de bate-papo para dar contexto ao agente.
 4. Quando estiver satisfeito com o plano, dê a aprovação no chat e a transformação começará.
 5. No modo interativo, você pode definir pontos de verificação para parar depois que um projeto for transformado para revisão. As etapas em Transformar código na janela Job Plan terão ícones de ponto de verificação redondos. Todos os projetos têm pontos de verificação ativados por padrão. Use as caixas de seleção para limpar ou definir um ponto de verificação.

Revisões de transformação e pontos de verificação

1. AWS A transformação começa a transformar seu código. Você pode monitorar o progresso das etapas de transformação na janela AWS Transform Job Plan. A janela Job Plan exibe o tempo máximo restante estimado e seu Job ID.
2. Conforme os projetos são transformados, os resumos são exibidos no chat e as alterações no código são aplicadas.
3. No modo interativo, quando um ponto de verificação é alcançado, o agente faz uma pausa para que você possa revisar os resultados. Na janela Job Plan, você verá um botão Exibir resultados para a etapa em que ele está pausado, onde você pode revisar as diferenças de código. Depois de analisar as alterações, você pode solicitar mais alterações no chat ou fazer alterações no Visual Studio código por conta própria.
4. Você pode iterar no ponto de verificação o quanto quiser. Quando estiver satisfeito, instrua o chat a continuar e ele passará para o próximo projeto.

Fim da transformação

1. Depois de transformar seus projetos, o agente.NET acionará uma compilação local para confirmar que o código foi criado com êxito em sua máquina local. Visual Studio Se houver erros, funcionará para resolvê-los.
2. Depois que a transformação for concluída, talvez sejam necessárias etapas adicionais, como tarefas de transformação que o AWS Transform não pôde realizar ou alterações necessárias para a compatibilidade com o Linux. O arquivo markdown da próxima etapa (NextSteps.md) está disponível para download, que você pode usar como instruções para um complemento de código de IA. Use o botão do ícone de download da janela Job Plan para fazer o download NextSteps.md.
3. Você pode continuar interagindo no chat para fazer perguntas ou solicitar alterações adicionais.
4. Diga ao chat quando você estiver pronto para encerrar seu trabalho de transformação.

Como AWS O Transform moderniza aplicativos.NET

Consulte as seções a seguir para obter detalhes sobre como a transformação do.NET com o AWS Transform funciona.

Analisar a aplicação e gerar um plano de transformação

Antes do início de uma transformação, o AWS Transform cria seu código localmente para verificar se ele pode ser compilado e configurado corretamente para transformação. Se o código não for compilado, o AWS Transform perguntará se deseja continuar com a transformação. AWS O Transform, em seguida, carrega seu código em um ambiente de compilação seguro e criptografado AWS, analisa sua base de código e determina as atualizações necessárias para portar seu aplicativo

Durante essa análise, o AWS Transform divide sua solução ou projeto do.NET em grupos de códigos. Um grupo de códigos é um projeto e todas as suas dependências que, juntos, geram uma unidade de código compilável, como uma biblioteca de links dinâmicos (DLL) ou um executável. Mesmo que você não tenha selecionado todas as dependências do projeto a serem transformadas, o AWS Transform determina as dependências necessárias para criar seus projetos selecionados e as transforma também, para que seu aplicativo transformado possa ser construído e esteja pronto para uso.

Depois de analisar seu código, o AWS Transform gera um plano de transformação que descreve as alterações propostas que ele fará, incluindo uma lista de grupos de códigos e suas dependências que serão transformadas.

Transformar a aplicação

Para iniciar a transformação, o AWS Transform cria seu código novamente no ambiente de compilação seguro para verificar se ele pode ser compilado remotamente. AWS Em seguida, o Transform começa a portar seu aplicativo. O processo funciona de baixo para cima, começando com a dependência de nível mais baixo. Se o AWS Transform tiver problemas com a portabilidade de uma dependência, ele interromperá a transformação e fornecerá informações sobre o que causou o erro.

A transformação inclui as seguintes atualizações na aplicação:

- Substituindo versões desatualizadas do código em C# por versões em Linux-compatible C#
- Atualização do .NET Framework para o .NET multiplataforma, incluindo:
 - Identificação e substituição iterativa de pacotes, bibliotecas e APIs
 - Atualizando e substituindo NuGet pacotes e APIs
 - Transição para o runtime multiplataforma
 - Configuração do middleware e atualização das configurações de runtime
 - Substituição de pacotes privados ou de terceiros
 - Manipulação de componentes do IIS e do WCF
 - Depuração de erros de compilação
- Reescrita de código para compatibilidade com Linux, incluindo refatoração e reescrita de código obsoleto e ineficiente para portar o código existente

Revisando o relatório de transformação e aceitando alterações

Após a conclusão da transformação, o AWS Transform fornece um relatório de transformação com informações sobre as atualizações propostas feitas em seu aplicativo, incluindo o número de arquivos alterados, pacotes atualizados e APIs alteradas. Ele sinaliza qualquer transformação malsucedida, incluindo arquivos ou partes de arquivos afetados e os erros encontrados durante uma tentativa de compilação. Você também pode ver um resumo da compilação com logs de compilação para saber mais sobre quais alterações foram feitas.

O relatório de transformação também fornece um status de portabilidade do Linux, que indica se a entrada adicional do usuário é necessária ou não para tornar o aplicativo compatível com o Linux. Se algum dos itens em um grupo de código exigir sua entrada, você baixa um relatório de preparação do Linux que contém Windows-specific considerações que o AWS Transform não conseguiu abordar no momento da criação. Se a entrada for necessária para qualquer grupo de código ou arquivo,

revise o relatório para obter detalhes sobre o tipo de alteração que ainda precisa ser feita e, se aplicável, para obter recomendações sobre como atualizar o código. Essas alterações devem ser feitas manualmente antes que a aplicação possa ser executada no Linux.

Você pode revisar as alterações propostas que o AWS Transform fez em uma visualização diferente antes de aceitá-las como atualizações locais em seus arquivos. Após atualizar os arquivos e abordar todos os itens no relatório de disponibilidade do Linux, a aplicação estará pronta para ser executada no .NET multiplataforma.

Você pode baixar um arquivo markdown do Next Steps com solicitações para transformação contínua com o AWS Transform ou um complemento de código de IA. Para baixar o arquivo, escolha o botão Baixar as próximas etapas no canto superior direito do relatório.

Solucionar problemas com transformações .NET no IDE

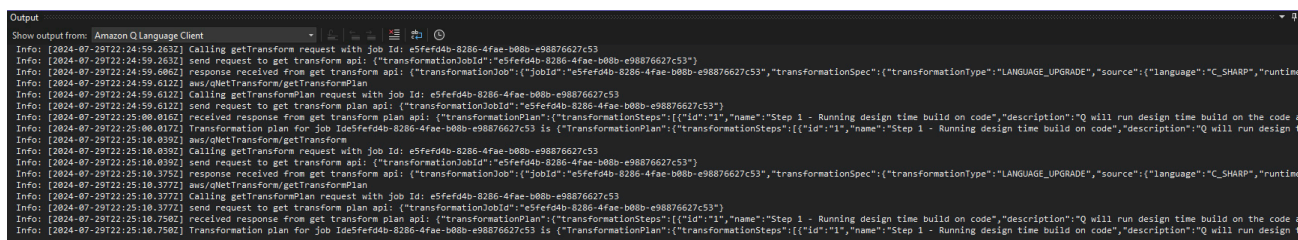
Use as seções a seguir para solucionar problemas comuns com transformações do .NET no IDE com AWS Transform.

Como posso saber se um trabalho está progredindo?

Você deve ver a atividade regular na janela do Registro de trabalho. Se o AWS Transform parecer estar gastando muito tempo em uma etapa na janela AWS Transform Job Plan, você poderá verificar se o trabalho ainda está ativo nos registros de saída. Se mensagens de diagnóstico estiverem sendo geradas, o trabalho ainda estará ativo.

Para verificar as saídas, escolha a guia Saída em Visual Studio. No menu Mostrar saída de:, selecione Amazon Q Language Client.

A captura de tela a seguir mostra um exemplo das saídas que o AWS Transform gera durante uma transformação.



```
Output
Show output from: Amazon Q Language Client
Info: [2024-07-29T22:24:59.263Z] Calling getTransform request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:24:59.263Z] send request to get transform api: {"transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53"}
Info: [2024-07-29T22:24:59.686Z] response received from get transform api: {"transformationJob":{"jobId":"e5fef04b-8286-4fae-b08b-e98876627c53"},"transformationSpec":{"transformationType":"LANGUAGE_UPGRADE","source":{"language":"C_SHARP","runtime":
Info: [2024-07-29T22:24:59.612Z] aws/dotnetTransform/getTransformPlan
Info: [2024-07-29T22:24:59.612Z] Calling getTransformPlan request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:24:59.612Z] send request to get transform plan api: {"transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53"}
Info: [2024-07-29T22:25:00.016Z] received response from get transform plan api: {"transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design time build on the code a
Info: [2024-07-29T22:25:00.017Z] Transformation plan for job Id e5fef04b-8286-4fae-b08b-e98876627c53 is {"transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
Info: [2024-07-29T22:25:10.030Z] aws/dotnetTransform/getTransform
Info: [2024-07-29T22:25:10.030Z] Calling getTransform request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:25:10.030Z] send request to get transform api: {"transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53"}
Info: [2024-07-29T22:25:10.375Z] response received from get transform api: {"transformationJob":{"jobId":"e5fef04b-8286-4fae-b08b-e98876627c53"},"transformationSpec":{"transformationType":"LANGUAGE_UPGRADE","source":{"language":"C_SHARP","runtime":
Info: [2024-07-29T22:25:10.377Z] aws/dotnetTransform/getTransformPlan
Info: [2024-07-29T22:25:10.377Z] Calling getTransformPlan request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:25:10.377Z] send request to get transform plan api: {"transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53"}
Info: [2024-07-29T22:25:10.758Z] received response from get transform plan api: {"transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
Info: [2024-07-29T22:25:10.758Z] Transformation plan for job Id e5fef04b-8286-4fae-b08b-e98876627c53 is {"transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
```

Por que alguns projetos não são selecionados para transformação?

AWS O Transform só pode transformar tipos de projetos .NET compatíveis. Para obter uma lista dos tipos de projetos compatíveis e outros pré-requisitos para transformar seus projetos .NET, consulte [Etapa 1: pré-requisitos](#).

Como posso obter suporte se meu projeto ou solução não estiver se transformando?

Se você não conseguir solucionar problemas sozinho, entre em contato com Conta da AWS nossa equipe Suporte para enviar um caso de suporte.

Para obter suporte, forneça o ID do trabalho de transformação para que AWS possa investigar um trabalho com falha. Para encontrar uma ID de tarefa de transformação, escolha a guia Saída em Visual Studio. No menu Mostrar saída de:, selecione Amazon Q Language Client.

Como posso evitar que meu firewall interfira nos trabalhos de transformação?

Se sua organização usa um firewall, ele pode interferir nas transformações do. Visual Studio Você pode desativar temporariamente as verificações de segurança Node.js para solucionar problemas ou testar o que está impedindo a execução da transformação.

A variável de ambiente `NODE_TLS_REJECT_UNAUTHORIZED` controla verificações de segurança importantes. `NODE_TLS_REJECT_UNAUTHORIZED` Definir como "0" desativa a rejeição Node.js de certificados não TLS/SSL autorizados. Isso significa que:

- Self-signed certificados serão aceitos
- Certificados expirados serão permitidos
- Certificados com nomes de host incompatíveis serão permitidos
- Quaisquer outros erros de validação de certificado serão ignorados

Se seu proxy usa um autocertificado, você pode definir as seguintes variáveis de ambiente em vez de desabilitar `NODE_TLS_REJECT_UNAUTHORIZED`:

```
NODE_OPTIONS = -use-openssl-ca  
NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs
```

Caso contrário, você deve especificar os certificados de CA usados pelo proxy para desabilitar `NODE_TLS_REJECT_UNAUTHORIZED`.

Para desativar o `NODE_TLS_REJECT_UNAUTHORIZED` no Windows:

1. Abra o menu Iniciar e pesquise Variáveis de ambiente.
2. Selecione Editar as variáveis de ambiente do sistema.
3. Na janela Propriedades do sistema, selecione Variáveis de ambiente.
4. Em Variáveis do sistema, selecione Novo.

5. Defina Nome da variável como `NODE_TLS_REJECT_UNAUTHORIZED` e Valor da variável como 0.
6. Clique em Ok para salvar as alterações.
7. Reinicie o Visual Studio.

Portando o código da camada de UI

AWS O Transform pode portar a camada de interface do usuário dos ASP.NET sites para estruturas de interface do usuário compatíveis com o ASP.NET Core, que podem ser executadas no Linux. As seguintes transformações estão disponíveis:

- Portabilidade do MVC Razor UI
- Portabilidade de formulários da Web para Blazor UI

Portabilidade do MVC Razor UI

ASP.NET Projetos MVC com a interface do Razor Views podem ser portados para o MVC Razor Views on ASP.NET Core, permanecendo na mesma estrutura de interface do usuário. Embora as visualizações do Razor sejam semelhantes entre ASP.NET e ASP.NET Core, há diferenças que exigem alterações no código de portabilidade:

- ASP.NET As visualizações MVC Razor usam o `System.Web.Mvc` namespace e estão intimamente ligadas ao .NET Framework.
- ASP.NET As Core Razor Views são modulares, integradas `Microsoft.AspNetCore.Mvc` e com injeção de dependência aprimorada.
- ASP.NET O Core tem novos recursos, incluindo Tag Helpers e View Components.

AWS O Transform detecta e porta componentes e construções comuns incompatíveis no Razor Views.

Portabilidade de formulários da Web para Blazor UI

ASP.NET A interface do usuário do Web Forms não tem uma contrapartida no ASP.NET Core. AWS O Transform pode portar o código da camada de interface do usuário do Web Forms para o Blazor Server on ASP.NET Core. O código da camada de interface do usuário é reescrito para a estrutura da interface de usuário de destino.

Para habilitar ou desabilitar a portabilidade de Web Forms para Blazor UI, marque ou desmarque a configuração de trabalho Transform UI ASP.NET Web Forms to Blazor.

Detalhes da transformação

Seu projeto Web Forms é convertido em um projeto Blazor com hospedagem no lado do servidor. As seguintes alterações no projeto e no arquivo são feitas durante a transformação:

Mapeamento de transformação de arquivos

De	Para	Description
*.aspx, *.ascx	*.navalha	páginas.aspx e controles personalizados.ascx se tornam arquivos.razor
Web.config	appsettings.json	Web.config configurações se tornam configurações appsettings.json
Global.asax	Program.cs	Global.asax código se torna Program.cs código
*.mestre	*layout.navalha	Os arquivos mestres se tornam arquivos layout.razor

Post-transformation estrutura do projeto

Após a transformação, os arquivos transformados residem nos seguintes locais do projeto:

- Pasta de componentes: todos os componentes do razor (*.razor) são colocados em uma pasta Components criada no mesmo nível do arquivo.csproj do projeto.
- Mapeamento de páginas: páginas de formulários da Web (*.aspx) são convertidas em estrutura de pastas. Components/Pages
- Mapeamento de controles: os controles do Web Forms (*.ascx) são colocados diretamente na pasta Components.

Limitações e recursos não suportados

Os seguintes recursos não são suportados no momento. Se suas cargas de trabalho usarem esses recursos, esse código precisará ser transferido manualmente ou com um código de IA complementar após a transformação.

- arquivos.svc (arquivos de serviço)
- arquivos.ashx (arquivos manipuladores genéricos)
- Referências de serviços e referências da web (arquivos reference.map, reference.cs, .wsdl)
- Misturas de arquivos.aspx (Web Forms) e arquivos.cshtml (Razor) no mesmo projeto
- Dependências em tipos de projeto ainda não suportadas pelo AWS Transform for .NET
- Third-party UI do fornecedor libraries/controls
- Projetos de sites

Somente projetos de aplicativos Web (contendo um arquivo.csproj) são suportados. Para converter um projeto de site em um projeto de aplicativo Web, consulte a orientação da Microsoft sobre como [converter um projeto de site em um projeto de aplicativo Web](#).

Relatórios de transformação

Depois que seu trabalho de transformação do.NET for concluído, esses relatórios de transformação estarão disponíveis:

- [Relatório resumido da transformação](#)
- [Relatório detalhado da transformação](#)

Relatório resumido da transformação

Após a conclusão de um trabalho de transformação, um relatório resumido da transformação fica disponível no console web. Baixe o relatório resumido da transformação na guia Painel. Selecione Baixar relatório resumido da transformação e escolha Baixar como HTML ou Baixar como JSON.

O relatório resumido da transformação fornece uma visão geral da transformação e das informações específicas de cada repositório que foi transformado, incluindo:

- Detalhes do trabalho
 - Visão geral do trabalho de transformação
 - Visão geral dos resultados da transformação
 - Visão geral dos arquivos
- Lista de repositórios e para cada repositório:
 - Visão geral do nome do repositório

- Resumo da transformação da solução
- Detalhes do projeto, incluindo status, tipo, versão.NET, total de linhas de código, linhas de código transformadas e arquivos alterados

Relatório detalhado da transformação

Após a conclusão de um trabalho de transformação, os relatórios detalhados da transformação ficam disponíveis para usuários do console web e do IDE.

- Usuários do console Web: um relatório detalhado está disponível para cada repositório transformado. Na guia Painel, use os links Baixar relatório detalhado na lista de repositórios para baixar um relatório detalhado.
- Usuários do IDE: baixem o relatório de transformação da janela AWS Transform Job Plan usando o ícone de download.

O relatório detalhado da transformação é um relatório HTML interativo. Ele contém informações detalhadas sobre a transformação, incluindo os motivos das alterações no arquivo e detalhes de erros acionáveis. As informações são organizadas na seguinte hierarquia:

- Informações sobre o trabalho
- Para cada solução:
 - Resumo da transformação da solução
 - Visão geral da transformação
 - Projetos
 - Para cada projeto:
 - Resumo do projeto
 - Resumo dos erros de compilação
 - NuGet mudanças de pacote
 - Alterações no arquivo
 - Erros de compilação
 - Resultados do teste unitário
 - Relatório de prontidão para Linux

Para ver uma visão geral das seções do relatório detalhado de transformação com exemplos, consulte a postagem do blog [Anunciando o AWS Transform para relatórios detalhados de transformação do.NET](#).

Melhores práticas para transformações do.NET

Siga esta orientação para obter melhores resultados de modernização do.NET com o AWS Transform. Essas melhores práticas se aplicam ao assistente de IA conversacional do.NET, atualmente disponível para Visual Studio IDE.

Tópicos

- [Antes de se transformar](#)
- [Avaliação e planejamento](#)
- [Transforme de forma interativa ou autônoma](#)
- [Validação e finalização](#)

Antes de se transformar

Analise as recomendações a seguir antes de iniciar um trabalho de transformação do.NET.

Use o assistente de IA conversacional do.NET

Use o novo agente.NET para obter os melhores resultados de transformação. O assistente conversacional de IA está disponível por Visual Studio meio do [AWS Toolkit for Visual Studio](#). Também está disponível para [Kiro](#) ou outros IDEs por meio dos agentes Kiro Power for AWS Transform and AWS Transform MCP. O novo agente do.NET ainda não está disponível no console web.

Use outras ferramentas se o objetivo não for a transformação do.NET em .NET

AWS O Transform for .NET é apropriado para a modernização do código.NET Framework para a modernização do código.NET e as atualizações do.NET para versões posteriores. Não é adequado para transformações que incluam linguagens que não sejam do.NET, como Java, ou estruturas que não sejam do.NET, como React. Ele também não fornece refatoração arquitetônica de aplicativos. Use o [AWS Transform custom](#) ou Kiro para esses tipos de modernização.

Use uma edição estável do Visual Studio, de preferência VS2026

Use uma edição GA Visual Studio em vez de uma versão prévia ou uma edição Insiders para evitar complicações decorrentes do software de pré-visualização. O AWS kit de ferramentas pode ser usado em Visual Studio 2026 ou 2022. O VS2026 é recomendado porque tem melhor desempenho com consumo reduzido de memória.

Use o mais recente AWS Kit de ferramentas para Visual Studio

Fique na versão mais recente do AWS Toolkit Visual Studio para obter correções de bugs e atualizações de recursos. Você pode verificar a versão do kit de ferramentas e fazer o upgrade em Extensões > Gerenciar extensões > Instalado.

Trabalhe em Visual Studio IDE para projetos de média ou alta complexidade

A experiência do IDE oferece a visão mais profunda da transformação, na qual você pode trabalhar junto com o agente.NET enquanto ele transforma projetos. Para projetos de complexidade média, alta ou crítica, use o IDE em vez do console web.

Tenha um plano de validação

Decida como você validará sua aplicação para verificar se ela está correta depois que ela for transformada. Post-transformation, você precisará confirmar se ele se comporta e tem a aparência correta quando executado e se os controles de segurança, a lógica comercial e o armazenamento de dados estão intactos. A validação será conduzida manualmente and/or usando a automação de testes? Se sua solução contiver testes de unidade, o AWS Transform os portará para você e os executará, e os resultados aparecerão no relatório de transformação.

Forneça NuGet dependências de pacotes privados

Se sua solução depender de pacotes privados, certifique-se de que eles estejam disponíveis em sua máquina local para que o IDE e o AWS Transform possam encontrá-los.

Especifique substituições de pacotes ou peça recomendações de agentes

Para pacotes que não têm versões modernas do.NET, você pode personalizar o plano de transformação para especificar as substituições de pacotes pretendidas ou pedir recomendações ao agente.

Não termine seu trabalho até ter certeza de que não deseja mais mudanças

Após a conclusão da transformação, não encerre seu trabalho imediatamente, caso queira alterações adicionais. A transformação não está completa até que você diga que está. Você pode solicitar alterações até marcar o trabalho como concluído.

Após a transformação, passe para um companheiro de código de IA para finalizar seu aplicativo

Espere combinar o AWS Transform com um complemento de código de IA, como Kiro. Um padrão comum é primeiro AWS transformar com o Transform for .NET e depois passar para um complemento de código de IA para finalizar o aplicativo. Esse trabalho de finalização pode incluir a identificação e correção de erros de tempo de execução, problemas comportamentais e estilo de UX.

Na jornada de modernização, pense no AWS Transform como a viagem expressa que leva você a um longo caminho até seu objetivo, e um complemento de código de IA como a viagem local que leva você ao seu destino final.

Para ajudar na transferência do AWS Transform para os companheiros de código de IA, o AWS Transform fornece um relatório de transformação de HTML e um documento de marcação Next Steps no final da transformação.

Avaliação e planejamento

Depois de iniciar um trabalho de transformação, o AWS Transform analisa seu código e produz um relatório de avaliação e um plano de transformação. Use as práticas recomendadas a seguir para aproveitar ao máximo essa fase.

Analise a avaliação e faça perguntas para definir suas expectativas

Analise cuidadosamente os resultados da avaliação para entender quais projetos serão difíceis de transformar e por quê. O agente apresenta projetos com um nível de complexidade (baixo, médio, alto, crítico) e explica por que eles têm essa classificação.

Faça perguntas para entender mais sobre áreas desafiadoras. Por exemplo:

- Pergunte ao agente qual é seu nível de confiança na transformação ou no caso de uso de um projeto.
- Pergunte ao agente quais tarefas de pós-transformação provavelmente serão necessárias com um complemento de código de IA.

Revise o plano e discuta as opções com o agente

O agente fornece um plano de transformação para sua análise. Você pode discutir e modificar esse plano. Comece entendendo suas opções. Pergunte ao agente quais alternativas existem para qualquer parte do plano.

Por exemplo, o plano de transformação pode propor a transformação dos serviços do WCF em APIs ASP.NET da Web. No entanto, sua organização prefere ficar com o WCF. Você pede opções ao agente e descobre que uma alternativa é transformá-las em CoreWCF.

Faça upload de documentos de orientação para personalizar um plano para sua organização

O plano de transformação original é criado sem a compreensão dos requisitos e preferências da sua organização. Você pode informar o agente sobre convenções organizacionais, especificações de aplicativos, pilha de tecnologia preferida e exemplos de padrões de codificação preferidos.

Depois de fazer o upload de um documento de orientação, explique-o para dar contexto ao agente. Com as informações adicionais dos documentos de orientação, o agente pode preparar um plano personalizado de acordo com a forma como sua organização gosta de trabalhar.

Personalize livremente o plano

O agente do.NET é flexível e você pode personalizar livremente o plano de transformação, dentro do domínio da transformação do.NET para .NET. Você pode solicitar alterações no plano no chat ou, se preferir, pode trabalhar com arquivos markdown. Revise e refine o plano até ficar satisfeito.

Se um plano precisar ser revisado por várias partes interessadas, você poderá baixá-lo como um arquivo markdown, compartilhá-lo e, posteriormente, fazer o upload de um plano personalizado.

Por exemplo, você revisa o plano de transformação e decide que deseja que os projetos da biblioteca de classes sejam transformados em .NET Standard em vez do .NET 10. No chat, você diz: "Revise o plano para transformar todas as bibliotecas de classes em .NET Standard 2.0" e o agente apresenta um plano revisado.

Transforme de forma interativa ou autônoma

A experiência do Visual Studio IDE oferece modos autônomos e interativos para controlar o grau de interatividade durante a transformação.

Use modos interativos e autônomos para controlar o grau de interatividade

Você seleciona o modo ao iniciar uma transformação e pode alterá-lo a qualquer momento por meio de um menu suspenso na parte superior da janela de bate-papo.

- Use o modo autônomo para transformação autônoma, adequado para trabalhos noturnos ou de longa duração. Você ainda tem a oportunidade de analisar os resultados e solicitar alterações no final do trabalho.
- Use o modo interativo para trabalhar com o agente no chat durante todo o processo de transformação com um plano de transformação personalizável, alta visibilidade dos detalhes da transformação e análise passo a passo de cada projeto. Você pode iterar para refinar os resultados ou mudar de direção até ficar satisfeito.

Você pode combinar modos. Por exemplo, comece no modo interativo para revisar e ajustar o plano de transformação e, em seguida, mude para o modo autônomo para transformar os projetos automaticamente.

Peça ao agente que explique as alterações no código

Se você ver alterações no código que não entende, peça ao agente que as explique.

Use pontos de verificação para parar nos projetos para revisão ou alterações

No modo interativo, depois de aprovar seu plano, você pode definir ou limpar pontos de verificação para cada projeto. Quando um projeto com um ponto de verificação é transformado, o código transformado é aplicado ao projeto no IDE e o agente faz uma pausa para sua revisão. Você pode revisar os resultados e, se não gostar deles, pode solicitar mais alterações.

Enquanto estiver parado em um posto de controle, você pode:

- Analise os resultados apresentados no chat e faça perguntas no chat. Por exemplo: “Por que você alterou a API de criptografia no arquivo X?”
- Visualize as alterações no código, escolhendo o botão Exibir Resultados do projeto na janela AWS Transform Job Plan.
- Refine a transformação solicitando alterações adicionais. Por exemplo: “Altere isso para usar o registrador X” ou “Altere isso para usar o pacote X em vez do pacote Y”.
- Repita a transformação, repetindo-a com instruções diferentes. Por exemplo: “Alterar essa biblioteca de classes para ter como alvo o.NET Standard em vez do.NET 10” ou “Tente novamente essa transformação e altere o destino de Blazor para MVC Razor Pages”.

- Faça suas próprias alterações de código no IDE.
- Peça ao agente que continue até o próximo ponto de verificação do projeto.

Repita até ficar satisfeito

A modernização é inerentemente iterativa, e você pode esperar iterar com o agente. Você pode fazer alterações nos pontos de verificação do projeto e também no final da transformação. Repita conforme necessário até ficar satisfeito. A transformação não está completa até que você diga que está.

Codifique junto com o agente quando parado em um ponto de verificação

Você pode fazer suas próprias alterações no código ao trabalhar com o agente. Quando parado em um ponto de verificação, você pode editar arquivos de código em Visual Studio. Suas alterações serão sincronizadas quando você orientar o agente a continuar.

Validação e finalização

Após a conclusão da transformação, valide seu aplicativo transformado e finalize-o para uso em produção.

Analise o relatório de transformação e as próximas etapas para entender o que é feito e o que resta

Analise o relatório de transformação de HTML para entender o que foi feito. Analise o arquivo de marcação Next Steps para entender quais tarefas ainda restam. Peça ao agente que esclareça qualquer coisa que não esteja clara.

Use um complemento de código de IA para validar, depurar e finalizar seu aplicativo

Verifique se o aplicativo transformado está correto. Use um complemento de código de IA, por exemplo, [Kiro](#) para resolver problemas.

Validar testes unitários

Se sua solução contiver projetos de teste unitário (NUnit, xUnit, ou MSTest), o AWS Transform os portará para o .NET moderno e executará os testes para você. Verifique o relatório de transformação de HTML para ver os resultados do teste de unidade. Corrija os testes que falharam com um complemento de código de IA.

Valide a funcionalidade do aplicativo

Execute seu aplicativo e confirme se sua funcionalidade corresponde à original. Observe problemas funcionais e erros de tempo de execução. Corrija com um complemento de código de IA.

Validar a interface do aplicativo

Execute seu aplicativo e confirme se ele se parece e se comporta como o original, incluindo navegação e roteamento. Se seu aplicativo não tiver estilo, pode ser que os arquivos.css não estejam no local correto. Corrija com um complemento de código de IA.

Modernização do SQL Server

AWS O Transform for SQL Server Modernization é um AI-powered serviço que automatiza a modernização completa dos bancos de dados Microsoft SQL Server e seus aplicativos.NET associados ao Amazon Aurora PostgreSQL. O serviço organiza toda a jornada de migração, desde a conversão de esquemas, migração de dados e modificação do código do aplicativo para corresponder ao novo PostgreSQL de destino, tornando suas equipes mais produtivas ao automatizar tarefas complexas e trabalhosas.

Regiões compatíveis

AWS O Transform for SQL Server está disponível no Leste dos EUA (Norte da Virgínia) - us-east-1

Cross-Region Uso: Para bancos de dados em regiões sem suporte, você pode clonar o banco de dados em uma região com suporte para transformação e, em seguida, implantar os resultados de volta na sua região de destino.

Capacidades e características principais

transformação do banco de dados

- Conversão de esquema: converte automaticamente esquemas do SQL Server em Aurora PostgreSQL, incluindo tabelas, visualizações, índices, restrições e relacionamentos
- Transformação de procedimentos armazenados: converte procedimentos T-SQL armazenados em PL/pgSQL com precisão AI-enhanced
- Migração de dados: migra dados com validação de integridade usando o AWS Database Migration Service (DMS)

- Objetos de banco de dados: suporta gatilhos, funções, visualizações, colunas computadas e colunas de identidade
- Validação: verificação automatizada da integridade dos dados e verificações de integridade referencial

Transformação de aplicativos

- Transformação do Entity Framework: atualiza as configurações do Entity Framework 6.3-6.5 e do EF Core 1.0-8.0 para PostgreSQL
- ADO.NET transformação: converte o código ADO.NET de acesso a dados do SQL Server em provedores PostgreSQL.
- Atualizações da cadeia de conexão: atualiza automaticamente todas as cadeias de conexão do banco de dados para o novo banco de dados PostgreSQL de destino
- Alterações no provedor de banco de dados: substitui os provedores do SQL Server pelo Npgsql (provedor PostgreSQL)
- Atualizações de configuração do ORM: modifica mapeamentos de tipos de dados, colunas de identidade e configurações específicas do banco de dados

Validação da orquestração &

- Wave-based modernização: organiza grandes propriedades em fases lógicas de migração
- Mapeamento de dependências: identifica relacionamentos entre aplicativos e bancos de dados
- Human-in-the-loop Pontos de verificação (HITL): fornecem portas de revisão e aprovação em estágios críticos
- Validação automatizada: testa a compatibilidade do esquema, a integridade dos dados e a funcionalidade do aplicativo
- CI/CD integração: integra-se aos pipelines de desenvolvimento existentes

Implantação

- Implantação do Amazon ECS e do Amazon EC2: implantação automatizada em contêineres com suporte de auto-scaling
- Infrastructure-as-code geração: cria nossos CloudFormation modelos de AWS CDK

- Validação automatizada da implantação: verifica a implantação bem-sucedida com verificações de integridade
- Capacidades de reversão: suporta procedimentos de reversão se surgirem problemas

Versões e tipos de projeto compatíveis

Versão do SQL Server

AWS O Transform oferece suporte às seguintes versões do SQL Server:

Versão do SQL Server	Status de Support
SQL Server 2022	Compatível
SQL Server 2019	Compatível
SQL Server 2017	Compatível
SQL Server 2016	Compatível
SQL Server 2014	Compatível
SQL Server 2012	Compatível
SQL Server 2008 R2	Compatível

Note

Todas as edições do SQL Server são suportadas (Express, Standard, Enterprise). O SQL Server pode ser hospedado no AWS (Amazon RDS for SQL Server ou SQL Server no Amazon EC2) ou hospedado fora do. AWS

Versões.NET

Versão.NET	Status de Support
.NET 10	Compatível
.NET 8	Compatível
.NET 7	Compatível
.NET 6 (núcleo)	Compatível
.NET Framework 4.x e versões anteriores	Não suportado

Important

Não há suporte para o .NET Framework 4.x herdado e versões anteriores. Se seu aplicativo usa o .NET Framework, você deve primeiro atualizar para o .NET Core 6+ usando o AWS Transform para modernização do .NET antes de usar os recursos de transformação do SQL Server.

Versões da estrutura de entidades

Framework	Versões compatíveis
Estrutura de entidades 6	6,3, 6,4, 6,5
Núcleo da estrutura de entidades	1,0 a 8,0
ADO.NET	Todas as versões (GA)

Repositórios de código-fonte

AWS O Transform é compatível com as seguintes plataformas de código-fonte:

- GitHub e GitHub Enterprise Server

- GitLab.com and GitLab Self-Managed
- Nuvem Bitbucket e data center Bitbucket
- Azure DevOps e Azure DevOps Server
- Amazon S3

Bancos de dados de destino

AWS O Transform tem como alvo o Amazon Aurora PostgreSQL (compatível com PostgreSQL 15+) com suporte para os recursos e otimizações mais recentes do Aurora.

Requisitos técnicos

Requisitos de banco de

- Microsoft SQL Server versão 2008 R2 até 2022
- SQL Server hospedado no AWS (Amazon RDS for SQL Server ou SQL Server no Amazon EC2) ou hospedado fora do AWS
- Para bancos AWS de dados hospedados, o banco de dados e o AWS Transform devem estar na mesma AWS região.
- Para bancos de dados hospedados fora do AWS, é necessária conectividade de rede com o serviço AWS Transform.
- Usuário do banco de dados com as permissões VIEW DEFINITION e VIEW DATABASE STATE
- Senhas de banco de dados usando somente caracteres ASCII imprimíveis (excluindo '/', '@', '"' e espaços)
- A VPC contendo o SQL Server de origem deve ter sub-redes em pelo menos duas zonas de disponibilidade diferentes (necessárias para grupos de sub-redes de replicação do DMS)

Requisitos de aplicação

- Aplicativos.NET Core 6, 7 ou 8
- Entity Framework 6.3-6.5 ou Entity Framework Core 1.0-8.0, ou ADO.NET
- Conexões de banco de dados detectáveis no código-fonte
- Aplicativos criados e executados com sucesso
- Código-fonte em plataformas de repositório compatíveis

AWS requisitos de conta

- AWS conta com acesso de administrador
- O IAM Identity Center está ativado
- Funções de serviço necessárias criadas (consulte as instruções de configuração abaixo)
- VPC com configuração de rede apropriada

Processamento e armazenamento de dados

Local de processamento

- O processamento do esquema ocorre em uma instância do DMS dentro da sua VPC
- A migração de dados é opcional e pode ser excluída, se necessário
- Os artefatos de transformação são armazenados na região de serviço AWS Transform

Artefatos armazenados

Os seguintes itens são armazenados na região de serviço:

- Logs de agente
- Resultados da avaliação
- Arquivos do esquema SQL
- Artefatos de saída do DMS

Important

Importante para a residência de dados: mesmo quando a migração de dados é desativada, os metadados e os artefatos de processamento são armazenados na região de serviço. Isso é importante para organizações com requisitos rígidos de residência de dados.

Gerenciamento de Artefatos

- Opção do cliente para criptografia usando suas próprias chaves KMS
- Período TTL (time-to-live) definido para todos os artefatos

- Os artefatos podem ser baixados para armazenamento off-line

Requisitos do SQL Server

Requisitos de banco de

Bancos de dados hospedados externamente

Bancos de dados hospedados fora do AWS são suportados. Para usar um banco de dados hospedado externamente, você deve garantir a conectividade de rede entre o banco de dados e o serviço AWS Transform.

Cargas de trabalho do SSIS

- Limitação: a transformação do SQL Server Integration Services (SSIS) não é suportada.
- Solução alternativa: use o AWS Glue ou outros serviços ETL para a migração do SSIS.

Servidores vinculados

- Limitação: conexões externas de banco de dados por meio de servidores vinculados exigem configuração humana.
- Solução alternativa: reconfigure os servidores vinculados após a migração ou use abordagens alternativas, como links de banco de dados ou integração em nível de aplicativo.

T-SQL Padrões complexos

- Limitação: Alguns T-SQL padrões avançados podem precisar de intervenção humana.
- Solução alternativa: use a CLI do Amazon Kiro para conversões SQL complexas. AWS Transform os sinaliza para análise durante o processo de transformação.

Requisitos de aplicação

.NET Framework legado

- Limitação: .NET Framework 4.x e versões anteriores não são compatíveis.
- Solução alternativa: use o AWS Transform for .NET para atualizar primeiro para o .NET Core 6+ e, em seguida, use a transformação do SQL Server.

Versões da estrutura de entidades

- Limitação: Somente o Entity Framework 6.3-6.5 e o EF Core 1.0-8.0 são suportados.
- Solução alternativa: atualize para uma versão compatível do Entity Framework antes da transformação.

VB.NET aplicações

- Limitação: não VB.NET é suportado.
- Solução alternativa: converta para C# ou use AWS Transform custom para converter de VB.NET para C#.

Cross-database dependências

- Limitação: desafios quando os esquemas de banco de dados interagem em vários bancos de dados.
- Solução alternativa: revise e refatore as consultas entre bancos de dados antes da migração. Considere consolidar bancos de dados ou usar esquemas do PostgreSQL.
- Impacto: pode exigir intervenção humana em cenários complexos entre bancos de dados.

Repository-database acoplamento

- Limitação: desafios quando um único repositório atende a vários bancos de dados.
- Solução alternativa: considere a reestruturação do repositório ou a abordagem de migração em fases.
- Impacto: pode exigir planejamento adicional para migrações baseadas em ondas.

Requisitos de infraestrutura

Solteiro account/region por trabalho

- Limitação: cada tarefa de transformação tem como alvo uma AWS conta e uma região.
- Solução alternativa: crie várias tarefas de transformação para implantações em várias contas ou em várias regiões.

Destinos de implantação

- Limitação: as implantações do Amazon ECS e do Amazon EC2 são suportadas.

Requisitos do repositório

NuGet Pacotes privados

- Limitação: NuGet pacotes privados exigem configuração adicional.
- Solução alternativa: configure NuGet feeds privados nas configurações de transformação antes de iniciar o trabalho.

Configuração do SQL Server

Execute essas etapas em seu ambiente SQL Server para permitir a modernização do AWS Transform.

Instalação e configuração do banco de dados

Etapas 1: Criar usuário de banco de dados com as permissões necessárias

Crie um usuário de banco de dados dedicado para o AWS Transform com as permissões necessárias. Se você já tiver um usuário do DMS Schema Conversion, poderá reutilizá-lo.

Conecte-se à sua instância do SQL Server e execute os seguintes comandos:

```
-- 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

Repita os comandos específicos do banco de dados (USE, CREATE USER, GRANT) para cada banco de dados que você deseja modernizar.

A função `db_datareader` só é necessária para a migração de dados, não somente para a conversão de esquemas.

- A função `db_datareader` concede acesso de leitura a todas as tabelas no banco de dados
- Essa função é necessária **SOMENTE** ao realizar a migração de dados.
- Somente para conversão de esquema (sem migração de dados), a função `db_datareader` **NÃO** é necessária
- As outras permissões (`VIEW DEFINITION`, `VIEW DATABASE STATE` etc.) são suficientes para a conversão do esquema

Etapa 2: armazenar credenciais em AWS Secrets Manager

Armazene suas credenciais de banco de dados com segurança no Secrets Manager AWS. Ignore esta etapa se você já tiver um segredo criado para o DMS.

1. Navegue até AWS Secrets Manager no console
2. Escolha Armazenar um novo segredo
3. Configure o segredo:
 - Tipo secreto: Credenciais para outro banco de dados
 - Banco de dados: Microsoft SQL Server
 - Nome de usuário: `atx_user` (ou seu nome de usuário escolhido)
 - Senha: A senha que você criou
 - Nome do servidor: Seu endpoint do SQL Server
 - Nome do banco de dados: nome do seu banco de dados
 - Porta: 1433 (ou sua porta personalizada)

4. Escolha Próximo.
5. Insira o nome secreto: atx-db-modernization-sqlserver
6. Adicione as tags necessárias (essas tags são obrigatórias):
 - Chave: Projeto, Valor: atx-db-modernization
 - Chave: proprietário, valor: conector de banco de dados
7. Escolha Avançar nas telas restantes
8. Escolha a loja
9. Anote o ARN secreto para uso na próxima etapa

 Important

As senhas do banco de dados devem usar somente caracteres ASCII imprimíveis, excluindo '/', '@', '' e espaços. Segredos programados para exclusão podem causar falhas na transformação.

Etapa 3: criar as funções necessárias do DMS

AWS A transformação exige funções específicas do IAM para operações do DMS. Implante essas funções usando o CloudFormation modelo abaixo.

 Note

Se sua AWS conta já tiver DMS-related funções existentes, modifique esse modelo para reutilizar esses recursos em vez de criar duplicatas.

Crie um arquivo chamado dms-roles.yaml com o seguinte conteúdo:

```
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
```

```
DMSecretsManagerRole:
  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

```

Implante a CloudFormation pilha usando a AWS CLI:

```

aws cloudformation create-stack \
  --stack-name dms-roles \
  --template-body file://dms-roles.yaml \
  --capabilities CAPABILITY_NAMED_IAM \
  --region us-east-1

```

Ou implante usando o AWS console:

1. Navegue até CloudFormation no AWS console
2. Escolha Criar pilha
3. Selecione Carregar um arquivo de modelo

4. Faça upload do arquivo dms-roles.yaml
5. Insira o nome da pilha: dms-roles
6. Reconheça os recursos do IAM
7. Escolha Criar pilha

Etapa 4: Configurar a segurança da rede

Garanta a conectividade de rede adequada entre o AWS Transform, seu banco de dados do SQL Server e outros AWS serviços.

Configuração do grupo de segurança (abordagem recomendada)

Abordagem recomendada: use controle de acesso baseado em grupos de segurança em vez IP-based de regras. Isso fornece melhor segurança, gerenciamento mais fácil e funciona perfeitamente com a arquitetura do AWS Transform.

Por que controle de Group-Based acesso de segurança?

- A conversão de esquema do DMS cria interfaces de rede elásticas (ENIs) em sua VPC
- Seus bancos de dados não precisam estar acessíveis ao público
- AWS O Transform não expõe endereços IP privados, tornando IP-based as regras complexas
- As referências de grupos de segurança fornecem atualizações dinâmicas e automáticas à medida que os recursos se expandem

Configure seu grupo de segurança do SQL Server

Ao configurar o Perfil da Instância de Conversão do Esquema DMS no AWS Transform, você especifica um Grupo de Segurança para a instância do DMS SC. Seu grupo de segurança de banco de dados deve permitir tráfego de entrada desse grupo de segurança do DMS SC.

Step-by-step configuração:

1. Identifique o grupo de segurança de conversão do esquema DMS:
 - Isso é especificado ao criar o Perfil de Instância no AWS Transform
 - Anote o ID do grupo de segurança (por exemplo, sg-0123456789abcdef0)
2. Atualize suas regras de entrada do Grupo de Segurança do SQL Server:

- Tipo: TCP personalizado
- Porta: 1433 (ou sua porta personalizada do SQL Server)
- Fonte: O ID do grupo de segurança de conversão do esquema DMS
- Descrição: “Permitir acesso à conversão do esquema DMS”

3. Para o destino do Aurora PostgreSQL (após a criação):

- Tipo: PostgreSQL
- Porta: 5432 (ou sua porta personalizada do PostgreSQL)
- Fonte: O ID do grupo de segurança de conversão do esquema DMS
- Descrição: “Permitir acesso à conversão do esquema DMS”

 Important

Importante para modelos de segurança menos privilegiados: Se sua organização usa um modelo de segurança “menos privilegiado” que bloqueia todo o tráfego por padrão, você deve permitir explicitamente o tráfego de entrada do Grupo de Segurança de Conversão de Esquema DMS para a porta do seu banco de dados. Não abra a porta 1433 para todas as fontes ou intervalos de IP.

Obrigatório AWS conectividade de serviço

Garanta que sua VPC possa se comunicar com:

- AWS Transforme os endpoints de serviço
- AWS DMS endpoints
- Endpoints Aurora PostgreSQL
- Endpoints S3 para armazenamento de artefatos
- AWS Secrets Manager endpoints
- AWS CodeConnections endpoints

VPC Endpoints: para redes privadas, configure os VPC endpoints para os AWS serviços necessários para evitar dependências de gateway de internet.

Requisitos para bancos de dados hospedados externamente

Se o banco de dados do SQL Server estiver hospedado fora do AWS, verifique se os pré-requisitos a seguir foram atendidos e, em seguida, conclua as etapas de configuração antes de iniciar a modernização.

Pré-requisitos

- Uma AWS conta com uma VPC
- Conectividade de rede entre a VPC e o banco de dados externo. Para obter informações sobre como configurar a conectividade de rede, consulte [Configurando a conectividade de rede](#) no Guia do AWS DMS usuário.

Etapas de configuração

1. Crie um segredo AWS Secrets Manager com os detalhes da conexão do banco de dados externo. Para obter mais informações, consulte [the section called “Etapa 2: armazenar credenciais em AWS Secrets Manager”](#).
2. Quando solicitado, forneça o ID da VPC e o ID do grupo de segurança para se conectar ao banco de dados externo. AWS O Transform solicita essas informações porque o nome do host do banco de dados no segredo não pode ser resolvido na AWS conta.

AWS Configuração de transformação

Comece sua jornada de modernização acessando o console do AWS Transform e iniciando um novo projeto de modernização. Essa etapa estabelece seu espaço de trabalho e configura a configuração básica para sua transformação completa.

Ações a serem concluídas:

- Navegue até AWS Transformar o serviço no AWS Management Console
- Selecione Microsoft Modernization nas opções de serviço
- Escolha Criar novo projeto de modernização
- Forneça o nome e a descrição do projeto
- Selecione sua AWS região de destino (deve corresponder à sua localização do SQL Server)
- Revise e confirme as configurações do projeto

 Note

Prática recomendada: use nomes de projetos descritivos que incluam o nome do aplicativo e o ambiente de destino (por exemplo, 'CustomerPortal-Production-Modernization') para identificar facilmente projetos em cenários de várias ondas.

Crie um trabalho de modernização do SQL Server

Connect banco de dados e repositório de código-fonte

Configurar o conector do banco

Estabeleça conectividade segura com seus bancos de dados do SQL Server configurando conectores de banco de dados. O conector realiza a análise do ambiente, a descoberta de dependências e permite que o AWS Transform acesse seus esquemas e metadados de banco de dados para avaliação e conversão.

Ações a serem concluídas:

- Selecione Configurar conector de banco de dados no assistente de configuração
- Escolha o método de conexão: Nova conexão ou conexão existente
- Forneça detalhes da conexão do SQL Server (endpoint, porta, nomes de banco de dados)
- Configure a autenticação e teste a conectividade
- Analise os bancos de dados descobertos e confirme a seleção

 Note

Conectividade de rede: garanta que seus grupos de segurança e NACLs do SQL Server permitam conexões de entrada dos pontos finais do serviço AWS Transform.

Conecte o repositório de código-fonte

Ative o AWS Transform para acessar o código-fonte do aplicativo.NET. O AWS Transform suporta três métodos para fornecer código-fonte: um conector Personal Access Token (PAT) (recomendado)

ou Amazon S3. AWS CodeConnections Essa integração permite que o serviço analise o código do seu aplicativo, identifique dependências do banco de dados e realize transformações automatizadas de código para compatibilidade com o PostgreSQL.

Ações a serem concluídas:

- Navegue até a seção Connect Source Code Repository
- Escolha seu método de autenticação: conector PAT (recomendado) ou Amazon S3 AWS CodeConnections
- Selecione repositórios contendo aplicativos.NET
- Especifique a ramificação para análise (normalmente main/master ou desenvolvimento)
- Valide o acesso ao repositório e a estrutura do código

Note

Descoberta do repositório: o AWS Transform verifica automaticamente seus repositórios para identificar projetos do.NET, configurações do Entity Framework, cadeias de conexão de banco de dados e dependências do SQL.

Note

Nota de segurança: o AWS Transform requer apenas acesso de leitura aos seus repositórios e cria novas ramificações de recursos para o código transformado. Sua filial principal permanece intocada.

Humano no circuito

AWS O Transform usa mecanismos human-in-the-loop (HITL) para garantir a qualidade e permitir que você revise e aprove decisões críticas de transformação. Os seguintes pontos de verificação exigem sua atenção:

Revisão e aprovação do plano Wave

O que você analisa: as ondas de migração propostas, incluindo quais bancos de dados e aplicativos são agrupados e a sequência das ondas.

Você pode:

- Aprovar o plano de ondas
- Personalize ondas movendo bancos de dados entre ondas
- Modificar sequência de ondas
- Dividir ou mesclar ondas

Após a aprovação, o AWS Transform prossegue com a conversão do esquema.

Análise de conversão do esquema

O que você revisa: objetos de banco de dados convertidos, incluindo tabelas, procedimentos armazenados, funções e gatilhos. Os itens de ação destacam objetos que requerem atenção.

Você pode:

- Aceite o código convertido
- Modificar código convertido
- Bandeira para revisão humana após a transformação
- Veja a comparação lado a lado do código original e convertido

O que acontece após a aprovação: o AWS Transform aplica o esquema ao Aurora PostgreSQL e prossegue com a migração de dados (se configurado).

Revisão do código do aplicativo

O que você analisa: todas as alterações no código do aplicativo, incluindo configurações do Entity Framework, cadeias de conexão, código de acesso a dados e chamadas de procedimentos armazenados.

Você pode:

- Aceite alterações para cada arquivo
- Modificar código transformado
- Rejeitar alterações (não recomendado)
- Adicione comentários para sua equipe
- Baixe o código transformado para análise local

O que acontece após a aprovação: o AWS Transform confirma as alterações em uma nova ramificação no seu repositório e prossegue com a validação.

Análise dos resultados da validação

O que você analisa: resultados de validação automatizados, incluindo compatibilidade de esquemas, verificações de integridade de dados e status de criação de aplicativos.

Você pode:

- Revise os testes aprovados
- Investigue testes que falharam
- Avisos de endereço
- Prossiga com a implantação ou retorne para corrigir problemas

O que acontece após a aprovação: o AWS Transform se prepara para a implantação em seu ambiente de destino.

Aprovação de implantação

O que você analisa: Configuração de implantação, incluindo modelos de infraestrutura como código, configuração do serviço ECS e configurações de implantação.

Você pode:

- Revise e personalize as configurações de implantação
- Aprovar a implantação para continuar
- Atrasar a implantação para testes adicionais
- Baixe o código de infraestrutura para análise

Após a aprovação, o AWS Transform implanta seu aplicativo e banco de dados modernizados no ambiente de destino.

Avaliação e planejamento de ondas

Configurar landing zone

Configure o ambiente de infraestrutura de destino em que seus aplicativos modernizados serão implantados. A configuração da landing zone inclui provisionamento do Aurora PostgreSQL, configuração de rede e configurações de implantação de referência.

Ações a serem concluídas:

- Selecione Configurar zona de pouso no menu de configuração
- Configurar o destino do Aurora PostgreSQL (versão, classe de instância) Multi-AZ
- Definir configurações de rede e segurança (VPC, sub-redes, grupos de segurança)

Note

Consideração de custo: as instâncias do Aurora PostgreSQL incorrem em custos contínuos. Considere usar o Aurora Serverless v2 para ambientes. development/testing

Avaliação

Conduza uma análise abrangente dos esquemas do banco de dados, do código do aplicativo e das dependências. A fase de avaliação fornece classificações de complexidade de transformação, identifica possíveis desafios e gera relatórios detalhados.

Ações a serem concluídas:

- Selecione a ramificação do repositório para análise de código
- Selecione repositórios e bancos de dados para transformação
- Revise os resultados da avaliação e as classificações de complexidade
- Gere relatório de avaliação com projeções de esforço
- Relatório de exportação para análise e aprovação das partes interessadas

 Note

Insights de avaliação: a avaliação fornece uma análise detalhada dos objetos do esquema, procedimentos armazenados, dependências do aplicativo e estima o nível de intervenção humana necessário.

Planejamento de ondas

Organize sua modernização em ondas gerenciáveis com base na complexidade da transformação, nas prioridades dos negócios e nas dependências dos aplicativos. AWS O Transform gera recomendações de ondas inteligentes que você pode personalizar.

Ações a serem concluídas:

- Analise o plano e as recomendações do AI-Generated Wave
- Personalize a configuração do Wave com base nas prioridades de negócios
- Valide dependências entre aplicativos e bancos de dados
- Finalize o Wave Plan usando a interface conversacional
- Defina prioridades de execução do Wave e atribua responsabilidades

 Note

AI-Powered Recomendações: você pode interagir com a IA por meio de linguagem natural para ajustar as recomendações: “Mover o CustomerDB para o Wave 1” ou “Combine esses dois aplicativos na mesma onda”.

 Note

Melhor prática: comece com uma onda piloto contendo de 1 a 2 bancos de dados de baixa complexidade para estabelecer processos e aumentar a confiança da equipe.

Migração de dados para cada onda

Conversão de esquema para cada onda

Transforme esquemas de banco de dados do SQL Server em PostgreSQL-compatible equivalentes usando recursos AI-enhanced de conversão. Esse processo converte tabelas, procedimentos armazenados, funções, acionadores e outros objetos do banco de dados.

Ações a serem concluídas:

- Forneça metas de conversão de esquema e configure preferências
- Execute a conversão automatizada usando o serviço de conversão de esquema DMS
- Analise os resultados da conversão e identifique os itens de intervenção humana
- Lidar com intervenções manuais por meio de instruções do HITL
- Valide as correções humanas e execute novamente a conversão, se necessário

Note

Intervenções manuais comuns: servidores vinculados, tipos definidos pelo usuário, T-SQL padrões avançados e recursos SQL específicos do fornecedor geralmente exigem revisão e correção humanas.

Migração de dados para cada onda

Transfira dados do SQL Server para o Aurora PostgreSQL usando a integração (). AWS Database Migration Service AWS DMS Escolha entre migração de dados de produção ou geração de dados sintéticos para fins de teste.

Ações a serem concluídas:

- Escolha a migração de dados de produção ou a geração de dados sintéticos
- Configurar a instância de replicação do DMS para transferência de dados
- Monitore o progresso da migração e resolva as inconsistências de dados
- Valide a integridade dos dados e as restrições referenciais
- Confirme a conclusão bem-sucedida antes de continuar

 Note

Integração automatizada do DMS: o AWS Transform abstrai a complexidade da configuração do DMS, manipulando automaticamente a criação de endpoints, a configuração de tarefas e os mapeamentos de tipos de dados.

 Note

Validação de dados: o serviço realiza testes empíricos executando consultas idênticas nos bancos de dados de origem e de destino para garantir a consistência dos dados.

Migração de código para cada onda

Transforme o código do aplicativo.NET para funcionar com o Aurora PostgreSQL, incluindo atualizações de configuração do Entity Framework, modificações na cadeia de conexão, adaptações de consultas SQL e ajustes específicos da estrutura.

Ações a serem concluídas:

- Execute análise automatizada de código para dependências do SQL Server
- Execute a transformação da estrutura (atualizações do provedor do Entity Framework)
- Adapte a sintaxe do SQL Query ao PostgreSQL-compatible SQL
- Configurar o Target Branch Management para código transformado
- Lide com intervenções manuais para padrões complexos

Fluxo de trabalho de modernização do SQL Server

Esta seção fornece uma explicação passo a passo do processo completo de modernização do SQL Server usando o Transform. AWS

Etapa 1: Criar um trabalho de modernização do SQL Server

Comece sua jornada de modernização criando um novo trabalho de transformação no console do AWS Transform.

1. Faça login no console do AWS Transform
2. Escolha Criar tarefa de modernização
3. Selecione a tarefa de modernização do Windows e, em seguida, selecione a modernização do SQL Server
4. Insira os detalhes do trabalho:
 - Nome do trabalho: nome descritivo do seu projeto
 - Descrição: Descrição opcional
 - Região de destino: AWS região para implantação
5. Selecione Create job (Criar trabalho)

 Important

Não inclua informações de identificação pessoal (PII) no nome do seu trabalho.

Etapa 2: Conectar-se ao banco de dados do SQL Server

Conecte o AWS Transform ao seu banco de dados do SQL Server para permitir a análise e a conversão de esquemas.

Crie um conector de banco de dados

1. Em seu trabalho de modernização do SQL Server, navegue até Connect to resources
2. Escolha Conectar ao banco de dados do SQL Server
3. Escolha Criar novo conector
4. Insira as informações do conector:
 - Nome do conector C: nome descritivo
 - AWS ID da conta: conta em que o SQL Server está hospedado
5. Depois de confirmado, você receberá um link para aprovação. Copie o link de aprovação para obter a aprovação do AWS administrador da conta. Depois de aprovados, você pode prosseguir para a próxima etapa.
6. Depois que seu administrador aprovar a solicitação do conector, clique em Enviar para prosseguir com a configuração da conexão do código-fonte.

Etapa 3: Conectar o repositório de código-fonte

AWS O Transform precisa acessar o código-fonte do aplicativo.NET para analisar e transformar o código que interage com o banco de dados do SQL Server. AWS O Transform oferece suporte a três métodos para fornecer código-fonte.

Escolha seu método de autenticação

Conector de token de acesso pessoal (PAT) (recomendado)

Ideal para equipes que precisam de escopos de permissão personalizados, suporte de provedor auto-hospedado ou acesso a APIs específicas do provedor, como segredos. GitHub Você cria um PAT em seu provedor de código-fonte com permissões personalizadas, o armazena e o AWS Transform o recupera quando necessário. AWS Secrets Manager Você é responsável por gerenciar a rotação e a expiração do token.

AWS CodeConnections

Ideal para equipes que desejam gerenciamento automatizado de credenciais. AWS CodeConnections usa uma integração de provedor gerenciado que gerencia a autenticação por meio de um fluxo de autorização do OAuth 2.0. AWS gerencia todo o ciclo de vida da credencial, incluindo atualização e rotação automáticas de tokens. Não é necessário gerenciamento manual de credenciais.

Amazon S3

Faça o upload do seu código-fonte diretamente em um bucket do Amazon S3. AWS O Transform acessa o código do bucket durante o trabalho de transformação.

Recurso	Conector PAT (recomendado)	AWS CodeConnections
Gerenciamento de credenciais	Manual (gerenciado pelo cliente)	Automático (AWS gerenciado)
Ciclo de vida do token	Rotação manual necessária	Atualização automática
Flexibilidade de permissão	Escopos totalmente pessoais	Permissões fixas

Recurso	Conector PAT (recomendado)	AWS CodeConnections
Self-hosted suporte do provedor	Compatível	Indisponível
Complexidade da configuração	Moderado (criação e armazenamento manuais de tokens)	Baixo (autorização única)
Armazenamento de tokens	Do cliente AWS Secrets Manager	Gerenciado pela AWS

Configurar um conector PAT (recomendado)

Com um conector PAT, você cria um token de acesso pessoal em seu provedor de código-fonte com permissões personalizadas, o armazena com segurança e o AWS Transform o recupera quando necessário. AWS Secrets Manager Você é responsável por gerenciar o ciclo de vida do token, incluindo rotação e expiração. AWS O Transform cria automaticamente a função IAM necessária com permissões para acessar seu segredo.

O conector PAT é compatível com os seguintes provedores, incluindo versões personalizadas DNS/URL e auto-hospedadas:

- GitHub e GitHub Enterprise Server
- GitLab.com and GitLab Self-Managed
- Nuvem Bitbucket e data center Bitbucket
- Azure DevOps e Azure DevOps Server

Crie um token de acesso pessoal

Crie um PAT no seu provedor de código-fonte. As permissões necessárias variam de acordo com o provedor. Escolha a guia do seu provedor.

Important

Copie o token imediatamente após a criação. Você não pode vê-lo novamente. Defina a expiração para a duração do trabalho de transformação. Não defina a expiração para nunca expirar.

⚠ Warning

Nunca envie tokens PAT em repositórios de código nem os compartilhe por meio de canais inseguros. Sempre os guarde AWS Secrets Manager.

GitHub

Navegue até Configurações, Configurações do desenvolvedor, Tokens de acesso pessoal, Fine-grained tokens. Selecione os repositórios a serem transformados e conceda as seguintes permissões.

Permissões do repositório

Permissão	Acesso	Finalidade
Conteúdo	Leia e escreva	Lê o código-fonte e grava o código transformado de volta no repositório
Metadados	Read-only	Acessa informações básicas do repositório

Permissões da organização (necessárias para os repositórios da organização)

Permissão	Acesso	Finalidade
Membros	Read-only	Lista as organizações acessíveis ao token para descoberta do repositório

GitLab

Navegue até Editar perfil, Tokens de acesso. Selecione os seguintes escopos.

Escopo	Finalidade
read_api	Lê metadados do repositório, informações do projeto, detalhes do usuário e lista grupos e filiais

Escopo	Finalidade
<code>read_repository</code>	Lê arquivos de código-fonte e estrutura do repositório para análise
<code>write_repository</code>	Grava o código transformado de volta no repositório

Bitbucket

Navegue até Configurações da conta, Segurança, Criar e gerenciar tokens de API. Os escopos necessários dependem do seu tipo de token.

Workspace/Repository Token (ATCT — autenticação do portador, sem necessidade de nome de usuário)

Permissão	Acesso	Finalidade
Repositórios	Leia e escreva	Lista repositórios, lê ramificações e grava código transformado via git push

Token da API da conta (ATAT — Autenticação básica com e-mail) ou Senha do aplicativo (ATBB — Autenticação básica com nome de usuário)

Escopo	Finalidade
<code>read:account</code>	Identifica o usuário autenticado para resolver a associação ao repositório
<code>read:workspace:bitbucket</code>	Lista os espaços de trabalho que o token pode acessar para que o AWS Transform possa enumerar seus repositórios. Não é necessário se você especificar uma lista de espaços de trabalho no segredo.
<code>read:repository:bitbucket</code>	Lista repositórios e lê metadados e informações de ramificações

Escopo	Finalidade
<code>write:repository:bitbucket</code>	Grava o código transformado de volta no repositório via git push

Azure DevOps

Navegue até Configurações do usuário, Tokens de acesso pessoal. Selecione Escopos personalizados definidos. Para o escopo da organização, escolha Todas as organizações acessíveis (recomendado) ou especifique uma única organização.

Escopo	Acesso	Finalidade
Código	Leia e escreva	Lê o código-fonte, lista repositórios e ramificações e grava o código transformado de volta
Perfil do usuário	Ler	Valida o acesso ao token e descobre a identidade do usuário para pesquisa da organização
Gerenciamento de direitos de membros	Ler	Lista as organizações acessíveis ao token para descoberta do repositório

Armazene o PAT em AWS Secrets Manager

1. Abra o AWS Secrets Manager console.
2. Selecione Armazenar um novo segredo.
3. Em Tipo de segredo, escolha Outro tipo de segredo.
4. Adicione pares de valores-chave com base em seu provedor e tipo de hospedagem:
 - Cloud-hosted provedores — Adicione uma chave nomeada token com seu PAT como valor.
 - Para o Azure DevOps com uma organização específica, adicione também uma chave chamada organization com o nome da sua organização.

- Para senhas do aplicativo Bitbucket (ATBB), adicione também uma chave chamada `username` com seu nome de usuário do Bitbucket. Para tokens de API da conta Bitbucket (ATAT), adicione uma chave chamada `email` com seu endereço de e-mail do Bitbucket.
- Self-hosted e DNS/URL provedores personalizados — adicione as seguintes chaves: `host` (o URL do seu servidor, por exemplo `https://github.mycompany.com`), `provider_type` (`githubgitlab,bitbucket,,ouado`) e `token` (seu PAT).
- Para o Azure DevOps com uma organização específica, adicione também uma chave chamada `organization` com o nome da sua organização.
- Para senhas do aplicativo Bitbucket (ATBB), adicione também uma chave chamada `username` com seu nome de usuário do Bitbucket. Para tokens de API da conta Bitbucket (ATAT), adicione uma chave chamada `email` com seu endereço de e-mail do Bitbucket.

O exemplo a seguir mostra como um segredo é examinado AWS Secrets Manager por um provedor GitHub hospedado na nuvem:

```
{
  "token": "your-github-personal-access-token"
}
```

O exemplo a seguir mostra uma senha do aplicativo Bitbucket (ATBB):

```
{
  "token": "your-bitbucket-app-password",
  "username": "my-bitbucket-username"
}
```

O exemplo a seguir mostra uma GitLab instância auto-hospedada:

```
{
  "host": "https://gitlab.mycompany.com",
  "provider_type": "gitlab",
  "token": "your-gitlab-personal-access-token"
}
```

5. Escolha Próximo.

6. Insira um nome secreto, por exemplo `github-pat-myproject`.

7. (Opcional) Selecione uma chave KMS gerenciada pelo cliente para criptografia.

8. Conclua o assistente e escolha Armazenar.
9. Copie o ARN secreto. Você precisa desse valor ao configurar a tarefa AWS Transform.

Se você usar uma chave KMS gerenciada pelo cliente para criptografar seu segredo (em vez da chave AWS gerenciada padrão), deverá atualizar a política de chaves do KMS para permitir que AWS o Transform decifre o segredo. Adicione a seguinte declaração à sua política de chaves do KMS gerenciada pelo cliente:

```
{
  "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 Substitua pela sua AWS região (por exemplo, *us-east-1*) e *YOUR-SECRET-ARN* pelo ARN do seu segredo. A `kms:ViaService` condição garante que a chave KMS só possa ser usada por meio do AWS Secrets Manager serviço. A `kms:EncryptionContext:SecretARN` condição restringe a decodificação ao seu segredo específico.

Para atualizar sua política de chaves do KMS:

1. Abra o console AWS KMS em. <https://console.aws.amazon.com/kms>
2. No painel de navegação, escolha Chaves gerenciadas pelo cliente.
3. Selecione sua chave KMS.
4. Na guia Política de chave, escolha Editar.
5. Adicione a declaração de política à política existente.

6. Escolha Salvar alterações.

Note

Se você usar a chave AWS gerenciada padrão (`aws/secretsmanager`), não precisará modificar nenhuma política de chave do KMS.

Configurar o AWS Transforme o trabalho

1. Em sua tarefa do AWS Transform, navegue até **Connect to resources**.
2. Escolha **Connect source code repository**.
3. Selecione o conector PAT como método de autenticação.
4. Insira o ARN secreto da etapa 2.
5. (Opcional) Insira o ARN da chave KMS se você usou uma chave KMS gerenciada pelo cliente.
6. Selecione seu repositório e ramificação.
7. Escolha **Continuar**.

AWS O Transform cria automaticamente uma função do IAM com as permissões necessárias para acessar seu segredo.

Rotação e manutenção de tokens

Você é responsável pela rotação dos tokens PAT antes que eles expirem. Para girar um token:

1. Gere um novo PAT em seu provedor de código-fonte com as mesmas permissões.
2. Atualize o valor secreto em AWS Secrets Manager.
3. Verifique se sua tarefa de AWS transformação pode acessar o repositório com o novo token.
4. Revogue o PAT antigo em seu provedor de código-fonte.

Solucionar problemas do conector PAT

Acesso negado — PAT inválido

Verifique se o PAT não expirou. Confirme se o PAT tem os escopos necessários para seu provedor. Verifique se o PAT está armazenado corretamente em AWS Secrets Manager.

Não é possível recuperar o segredo

Verifique se o ARN secreto está correto. Verifique os registros do trabalho para confirmar se o AWS Transform criou a função do IAM. Se você estiver usando uma chave KMS gerenciada pelo cliente, verifique a política de chaves.

Permissões insuficientes

O PAT pode não ter os escopos necessários para a operação. Regenere o PAT com os escopos necessários e atualize o valor secreto em AWS Secrets Manager

Configurar AWS CodeConnections

AWS CodeConnections usa uma integração de provedor gerenciado que recupera automaticamente as credenciais temporárias do OAuth por meio de um fluxo de autorização do OAuth 2.0. As permissões são configuradas no aplicativo do provedor e gerenciadas inteiramente pelo AWS. Você autoriza o aplicativo uma vez e AWS gerencia todo o gerenciamento de credenciais.

1. Em seu trabalho de modernização do SQL Server, navegue até Connect to resources.
2. Escolha Connect source code repository.
3. Se você não tiver uma conexão existente, escolha Criar conexão.
4. Selecione seu provedor de repositório:
 - GitHub / GitHub Empresa
 - GitLab.com
 - Bitbucket Cloud
 - Repositórios do Azure
5. Siga o fluxo de autorização do seu provedor.
6. Após a autorização, escolha Connect.

Selecione seu repositório e ramificação

1. Selecione seu repositório na lista.
2. Escolha a ramificação que você deseja transformar (normalmente principal, principal ou desenvolver).
3. (Opcional) Especifique um subdiretório se seu aplicativo.NET não estiver na raiz do repositório.
4. Escolha Continuar.

 Note

AWS A transformação cria uma nova ramificação para o código transformado. Você pode revisar e mesclar as alterações por meio do processo normal de revisão de código.

Aprovação do acesso ao repositório

Para GitHub algumas outras plataformas, o administrador do repositório deve aprovar a solicitação de conexão:

1. AWS O Transform exibe um link de verificação.
2. Compartilhe esse link com o administrador do repositório.
3. O administrador analisa e aprova a solicitação nas configurações do repositório.
4. Depois que o administrador aprova a solicitação, o status da conexão muda para Aprovado.

 Important

O processo de aprovação pode levar algum tempo, dependendo das políticas da sua organização. Planeje adequadamente.

Etapa 4: Criar conector de implantação (opcional)

Se você quiser implantar os aplicativos transformados em sua AWS conta, você tem a opção de selecionar um conector de implantação.

Configurar o conector de implantação

1. Selecione Sim se quiser implantar seus aplicativos. Selecionar Não ignorará essa etapa.
2. Adicione sua AWS conta onde você deseja implantar os aplicativos transformados.
3. Adicione um nome que ajude você a se lembrar facilmente do conector
4. Envie a solicitação do conector para aprovação.

Aprovação do conector de

O administrador AWS da sua conta deve aprovar a solicitação de conexão para o conector de implantação.

1. AWS O Transform exibe um link de verificação
2. Compartilhe este link com o administrador AWS da sua conta
3. O administrador revisa e aprova a solicitação nas configurações do repositório
4. Depois de aprovado, o status da conexão muda para Aprovado

Important

O processo de aprovação pode levar algum tempo, dependendo das políticas da sua organização. Planeje adequadamente.

Etapa 5: confirme seus recursos

Depois de se conectar ao seu banco de dados e repositório, o AWS Transform verifica se todos os recursos necessários estão acessíveis e prontos para a transformação.

O que AWS A transformação verifica

- Conectividade do banco de dados: a conexão está ativa, o usuário tem as permissões necessárias, os bancos de dados estão acessíveis, a versão é suportada
- Acesso ao repositório: o repositório está acessível, a ramificação existe, os arquivos do projeto.NET foram detectados, as conexões do banco de dados podem ser descobertas
- Preparação do ambiente: a configuração da VPC suporta DMS, existem funções de serviço AWS necessárias, conectividade de rede estabelecida, compatibilidade regional confirmada

Revise a lista de verificação antes do voo

1. Navegue até Confirmar seus recursos no plano de trabalho
2. Analise os itens da lista de verificação:
 - # Conexão com o banco de dados
 - # Acesso ao repositório confirmado

- # Versão do.NET suportada
 - # Entity Framework ou ADO.NET detectado
 - # Configuração de rede válida
 - # Permissões necessárias concedidas
3. Se todos os itens aparecerem como concluídos, escolha Continuar
 4. Se algum item mostrar avisos ou erros, resolva-os antes de continuar

Etapa 6: descoberta e avaliação

AWS O Transform analisa seu banco de dados SQL Server e o aplicativo.NET para entender o escopo e a complexidade da modernização.

O que é descoberto

- Objetos de banco de dados: tabelas, visualizações, índices, procedimentos armazenados, funções, acionadores, restrições, tipos de dados, colunas computadas, colunas de identidade, relacionamentos de chave estrangeira
- Código do aplicativo: estrutura do projeto.NET, modelos e configurações do Entity Framework, código de acesso a ADO.NET dados, cadeias de conexão de banco de dados, chamadas de procedimentos armazenados, consultas SQL em código
- Dependências: quais aplicativos usam quais bancos de dados, dependências entre bancos de dados, procedimentos armazenados compartilhados, padrões comuns de acesso a dados

Processo de descoberta

- AWS A transformação começa a ser descoberta automaticamente após a confirmação do recurso
- A descoberta normalmente leva de 5 a 15 minutos, dependendo do tamanho do banco de dados e da complexidade do aplicativo
- Monitore o progresso no registro de trabalho
- AWS O Transform exibe atualizações em tempo real à medida que os objetos são descobertos

Análise os resultados da descoberta

Após a conclusão da descoberta, navegue até Descoberta e avaliação para analisar:

Análise de banco de dados:

- Contagem de objetos: número de tabelas, visualizações, procedimentos armazenados, funções, gatilhos
- Pontuação de complexidade: avaliação da complexidade da transformação (baixa, média, alta)
- Itens de ação: objetos que podem exigir atenção humana
- Recursos suportados: recursos de banco de dados que serão convertidos automaticamente
- Recursos não suportados: recursos que exigem soluções alternativas

Análise de aplicativos:

- Tipo de projeto: ASP.NET Core, aplicativo de console, biblioteca de classes, etc.
- Versão.NET: versão detectada do .NET Core
- Estrutura de acesso a dados: versão do Entity Framework ou ADO.NET
- Conexões de banco de dados: Número de cadeias de conexão encontradas
- Complexidade do código: avaliação da complexidade da transformação

Mapa de dependências:

- Representação visual das relações entre aplicativos e bancos de dados
- Cross-database dependências
- Componentes compartilhados

Entendendo a avaliação da complexidade

AWS O Transform classifica sua modernização em três categorias:

Complexidade	Características	Resultado esperado
Baixo (Classe A)	Padrões SQL padrão (ANSI SQL), procedimentos simples armazenados, tipos de dados básicos, Entity Framework com configurações padrão	Mínima intervenção humana esperada, alta taxa de sucesso de automação

Complexidade	Características	Resultado esperado
Médio (Classe B)	T-SQL Padrões avançados, procedimentos armazenados complexos com lógica de negócios, funções definidas pelo usuário, colunas computadas	Alguma intervenção humana é necessária, revisão de especialistas recomendada
Alto (Classe C)	Assemblies CLR, servidores vinculados, Service Broker, pesquisa complexa de texto completo	É necessária uma refatoração humana significativa, considere a abordagem em fases

Relatório de avaliação da

AWS O Transform gera um relatório de avaliação detalhado que inclui:

- Resumo executivo com visão geral de alto nível
- Inventário completo do banco de
- Inventário de aplicativos
- Porcentagem de prontidão para transformação
- Estimativa de esforço
- Estratégias de avaliação e mitigação de riscos
- (Abordagem recomendada)

Você pode baixar o relatório de avaliação para análise off-line e compartilhamento com as partes interessadas.

Etapa 7: gerar e revisar o plano de ondas

Para grandes propriedades com vários bancos de dados e aplicativos, o AWS Transform gera um plano de ondas que sequencia a modernização em grupos lógicos.

O que é um plano de ondas?

Um plano de ondas organiza sua modernização em fases (ondas) com base em:

- Dependências entre bancos de dados e aplicativos

- Prioridades de negócios
- tolerância ao risco
- Disponibilidade de recursos
- Complexidade técnica

Cada onda contém um grupo de bancos de dados e aplicativos que podem ser modernizados juntos sem quebrar dependências.

Revise o plano de ondas

1. Navegue até Planejamento do Wave no plano de trabalho
2. Revise as ondas propostas
3. Para cada onda, analise:
 - Bancos de dados incluídos
 - Aplicativos incluídos
 - Dependências de outras ondas
 - Tempo estimado de transformação
 - Nível de complexidade
 - Aplicativos implantáveis

Personalize o plano de ondas

Você pode personalizar o plano wave para atender às necessidades da sua empresa de duas maneiras:

Usando JSON:

1. Escolha Baixar todas as ondas para obter um arquivo JSON com todas as ondas
2. Modifique as ondas no JSON da seguinte forma:
 - Movendo bancos de dados entre ondas
 - Dividindo ondas em grupos menores
 - Mesclando ondas
 - Alterando a sequência de ondas
 - Adicionar ou remover bancos de dados do escopo

3. Faça o upload do arquivo JSON de volta para o console escolhendo Carregar plano de onda
4. AWS O Transform valida suas alterações e avisa se as dependências forem violadas
5. Escolha Confirmar ondas para atualizar o plano de ondas

Usando o Chat:

Você pode modificar os planos de ondas conversando com o agente e solicitando que ele mova os repositórios e bancos de dados para ondas específicas. Essa abordagem funciona bem se você precisar fazer pequenas edições nas ondas.

 Important

Certifique-se de que as dependências sejam respeitadas ao personalizar ondas. Transformar um aplicativo dependente antes de seu banco de dados pode causar problemas.

Modernização de banco de dados único

Se você estiver modernizando um único banco de dados e aplicativo, o AWS Transform cria um plano simples com uma única onda. Você pode prosseguir diretamente para a transformação sem planejar ondas.

Aprovar o plano de ondas

1. Depois de revisar e personalizar (se necessário), escolha Aprovar plano de ondas
2. AWS O Transform bloqueia o plano de ondas e prossegue com a transformação
3. Você ainda pode modificar o plano posteriormente escolhendo Editar plano de onda

Etapa 8: conversão do esquema

AWS O Transform converte seu esquema de banco de dados SQL Server em Aurora PostgreSQL, incluindo tabelas, visualizações, procedimentos armazenados, funções e gatilhos.

Como funciona a conversão de esquemas

AWS O Transform usa a conversão de esquema AWS DMS aprimorada com IA generativa para:

- Analise esquemas e relacionamentos do SQL Server
- Mapeie tipos de dados do SQL Server para equivalentes do PostgreSQL

- Transformar T-SQL em PL/pgSQL
- Lidar com colunas de identidade, colunas computadas e restrições
- Valide a conversão e a integridade referencial
- Gere itens de ação para objetos que exigem revisão humana

Conversões suportadas

Convertido automaticamente:

- Tabelas, visualizações e índices
- Chaves primárias e chaves estrangeiras
- Verifique as restrições e os valores padrão
- Tipos de dados mais comuns
- Procedimentos simples de armazenamento
- Funções básicas e gatilhos
- Colunas de identidade (convertidas em SERIAL ou GERADAS)
- Colunas mais computadas

Pode exigir revisão humana:

- Procedimentos armazenados complexos com recursos avançados T-SQL
- Server-specific Funções SQL (GETUTCDATE, SUSER_SNAME etc.)
- Colunas computadas com expressões complexas
- Full-text índices de pesquisa
- Operações de tipo de dados XML
- Tipo de dados HIERARCHYID (requer extensão Itree)

Não convertido automaticamente:

- Conjuntos CLR
- Servidores vinculados
- Service Broker
- Trabalhos do SQL Server Agent

Iniciar conversão do esquema

1. Navegue até Conversão de esquema no plano de trabalho
2. Revise as configurações de conversão:
 - Versão de destino do PostgreSQL
 - Opções de extensão (ltree, PostGIS, etc.)
 - Convenções de nomenclatura
3. Escolha Iniciar conversão
4. Monitore o progresso no registro de trabalho
5. A conversão normalmente leva de 10 a 30 minutos, dependendo do número de objetos do banco de dados

Analise os resultados da conversão

Depois que a conversão for concluída, navegue até Revisar conversão do esquema:

Resumo da conversão:

- Objetos convertidos: contagem de objetos convertidos com sucesso
- Itens de ação: objetos que requerem atenção humana
- Advertências: possíveis problemas a serem analisados
- Erros: objetos que não puderam ser convertidos

Análise por tipo de objeto:

- Tabelas: mapeamentos de tipos de dados, restrições, índices
- Procedimentos armazenados: T-SQL para PL/pgSQL conversão
- Funções: assinatura da função e alterações lógicas
- Acionadores: mudanças na sintaxe e temporização do gatilho

Revise os itens de ação

1. Escolha Exibir itens de ação
2. Para cada item de ação, revise:
 - Nome do objeto: O objeto do banco de dados

- Tipo de problema: O que requer atenção
 - Gravidade: crítica, advertência ou informação
 - Recomendação: resolução sugerida
 - Código original: versão SQL Server
 - Código convertido: versão PostgreSQL
3. Para cada item de ação, você pode:
- Aceitar: use o código convertido
 - Modificar: edite o código convertido
 - Sinalizar para mais tarde: Marque para revisão humana após a transformação

Exemplo: conversão de procedimento armazenado

Servidor SQL 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
```

PostgreSQL PL/pgSQL convertido:

```
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;
```

Alterações feitas:

- Procedimento convertido em função retornando TABLE
- Nomes de parâmetros prefixados com p_
- TOP convertido em LIMIT
- DATEDIFF convertido em EXTRACT
- GETUTCDATE () convertido em NOW ()
- Nomes de colunas convertidos em minúsculas (convenção PostgreSQL)

Aprovar a conversão do esquema

1. Depois de revisar todos os itens de ação e fazer as modificações necessárias
2. Escolha Aprovar conversão de esquema
3. AWS O Transform prepara o esquema convertido para implantação no Aurora PostgreSQL

Note

Você pode baixar o esquema convertido como scripts SQL para análise offline ou controle de versão.

Etapa 9: migração de dados (opcional)

AWS O Transform fornece opções para migrar dados do SQL Server para o Aurora PostgreSQL. A migração de dados é opcional e pode ser ignorada se você precisar apenas da transformação do esquema e do código.

Opções de migração de dados

Opção 1: migração de dados de produção

Migre seus dados reais de produção usando o AWS DMS:

- Carga inicial completa de todos os dados
- Replicação contínua durante o teste (CDC)
- Redução mínima do tempo de inatividade
- Validação de dados e verificações de integridade

Opção 2: ignorar a migração de dados

Transforme somente o esquema e o código:

- Útil para development/testing ambientes
- Quando os dados serão migrados separadamente
- Para projetos de prova de conceito

Configurar a migração de dados

1. Navegue até Migração de dados no plano de trabalho
2. Escolha sua opção de migração:
 - Migre dados de produção
 - Ignorar a migração de dados
3. Se estiver migrando dados de produção, configure:
 - Tipo de migração: carga total ou carga total + CDC
 - Validação: habilitar a validação de dados
 - Desempenho: tamanho da instância do DMS
 - Escolha >Iniciar a migração

Processo de migração de dados de produção

Se você optar por migrar os dados de produção:

1. Sincronização inicial: o AWS DMS executa a carga total de todas as tabelas
2. Replicação contínua: (se o CDC estiver ativado) Mantém os dados sincronizados
3. Validação: verifica a contagem de linhas e a integridade dos dados
4. Preparação da transição: se prepara para a sincronização final

Cronograma de migração:

- Bancos de dados pequenos (< 10 GB): 30 minutos - 2 horas
- Bancos de dados médios (10 a 100 GB): 2 a 8 horas
- Bancos de dados grandes (> 100 GB): mais de 8 horas

Validação de dados

AWS O Transform valida os dados migrados com as seguintes verificações:

- Comparação da contagem de linhas (origem versus destino)
- Integridade da chave primária
- Relacionamentos de chave estrangeira
- Compatibilidade do tipo de dados
- Resultados da coluna computada
- Manipulação de valores nulos

Etapa 10: transformação do código do aplicativo

AWS O Transform transforma o código do aplicativo.NET para funcionar com o Aurora PostgreSQL em vez do SQL Server. Ele solicita um nome de ramificação de destino em seus repositórios para confirmar o código-fonte transformado. Depois de inserir o nome da ramificação, o AWS Transform criará uma nova ramificação e iniciará a transformação para corresponder ao banco de dados PostgreSQL.

O que é transformado

Alterações na estrutura da entidade:

- Provedor de banco de dados: UseSqlServer () → UseNpgsql ()
- Cadeias de conexão: formato SQL Server → formato PostgreSQL
- Mapeamentos de tipos de dados: tipos do SQL Server → Tipos do PostgreSQL
- DbContext configurações: SQL → Server-specific PostgreSQL-specific
- Arquivos de migração: atualizados para compatibilidade com o PostgreSQL

ADO.NET Mudanças:

- Classes de conexão: SqlConnection → NpgsqlConnection
- Classes de comando: SqlCommand → NpgsqlCommand
- Leitor de dados: SqlDataReader → NpgsqlDataReader
- Parâmetros: SqlParameter → NpgsqlParameter
- Sintaxe S SQL: T-SQL → PostgreSQL → SQL

Alterações na configuração:

- Cadeias de conexão em appsettings.json
- NuGet Pacotes de provedores de banco
- Configurações de injeção de dependência
- Startup/Program.cs configurações

Inicie a transformação do código

1. Navegue até Transformação de aplicativos no plano de trabalho
2. Revise as configurações de transformação:
 - Versão.NET de destino (se estiver atualizando)
 - Versão do provedor PostgreSQL
 - Preferências de estilo de código
3. Escolha Iniciar transformação
4. Monitore o progresso no registro de trabalho
5. A transformação normalmente leva de 15 a 45 minutos, dependendo do tamanho da base de código

Etapa 11: Analisar os resultados da transformação

Antes de prosseguir com a implantação, analise os resultados completos da transformação para garantir que tudo esteja pronto para o teste.

Você pode baixar o código transformado da ramificação do repositório para:

- Teste e validação locais
- Revisão de código em seu IDE
- Integração com seu CI/CD funil
- Confirmação de controle de versão

Você também pode baixar o resumo da transformação para revisar as alterações na linguagem natural feitas pelo AWS Transform como parte da transformação.

Resumo da transformação

1. Navegue até o resumo da transformação no plano de trabalho
2. Analise os resultados gerais:
 - Conversão de esquema: objetos convertidos, itens de ação, avisos
 - Migração de dados: tabelas migradas, linhas transferidas, status de validação
 - Transformação de código: arquivos alterados, linhas modificadas, problemas resolvidos
 - Pontuação de prontidão: prontidão geral para implantação

Gerar relatório de transformação

AWS O Transform gera um relatório de transformação abrangente:

1. Escolha Gerar relatório
2. Selecione o tipo de relatório:
 - Resumo executivo: High-level visão geral para as partes interessadas
 - Detalhes técnicos: documentação completa de transformação
 - Itens de ação: Lista de tarefas humanas necessárias
3. Escolha Baixar relatório

O relatório inclui:

- Escopo e objetivos da transformação
- Objetos e código transformados
- Problemas encontrados e soluções
- Resultados da validação
- Avaliação da prontidão para implantação
- Recomendações para testes

Etapa 12: Validação e teste

Antes de implantar na produção, verifique se o aplicativo transformado funciona corretamente com o Aurora PostgreSQL.

Tipos de validação

Validação automatizada: o AWS Transform realiza verificações automatizadas:

- Validação do esquema em relação ao banco de dados de origem
- Verificação de integridade dos dados
- Teste de equivalência de consultas
- Validação da cadeia de conexão
- Validação de configuração

Validação humana: você deve realizar testes adicionais:

- Teste funcional dos recursos do aplicativo
- Teste de integração com outros sistemas
- Teste de desempenho e benchmarking
- Teste de aceitação do usuário
- Teste de segurança

Execute a validação automatizada

1. Navegue até Validação no plano de trabalho
2. Escolha Executar validação
3. AWS O Transform executa testes de validação:

- Conectividade com o banco de dados
- Compatibilidade de esquemas
- Integridade dos dados
- Construção de aplicativos
- Funcionalidade básica

4. Analise os resultados da validação:

- Aprovado: testes bem-sucedidos
- Falhou: testes que precisam de atenção
- Avisos: possíveis problemas a serem analisados

Lista de verificação de testes

Funcionalidade do banco de dados:

- Todas as mesas acessíveis
- Os procedimentos armazenados são executados corretamente
- As funções retornam os resultados esperados
- Aciona o fogo de forma adequada
- Restrições aplicadas adequadamente
- Os índices melhoram o desempenho da consulta

Funcionalidade do aplicativo:

- O aplicativo é iniciado com sucesso
- Conexões de banco de dados
- As operações do CRUD funcionam corretamente
- As chamadas de procedimento armazenadas foram bem-sucedidas
- Transações commit/rollback adequadas
- O tratamento de erros funciona conforme o esperado

Integridade dos dados:

- A contagem de linhas corresponde à fonte

- Chaves primárias exclusivas
- Chaves estrangeiras válidas
- Colunas computadas corretas
- Tratamento nulo apropriado
- Tipos de dados compatíveis

Desempenho:

- Tempos de resposta da consulta aceitáveis
- Pool de conexões configurado
- Índices otimizados
- Sem problemas de consulta N+1
- Operações em lote eficientes
- Utilização de recursos razoável

Etapa 13: Implantação

Após a validação bem-sucedida, implante seu aplicativo e banco de dados modernizados para produção.

Opções de implantação

- Amazon ECS e Amazon EC2 Linux

Pre-deployment lista de verificação

Antes da implantação na produção:

- Todos os testes de validação foram aprovados
- Teste de desempenho concluído
- Análise de segurança concluída
- Plano de backup e reversão documentado
- Monitoramento e alertas configurados
- Equipe treinada em novo ambiente

- Partes interessadas informadas sobre a implantação
- Janela de manutenção programada

Implantar no Amazon ECS

1. Navegue até Implantação no plano de trabalho
2. Escolha Implantar no ECS
3. Defina as configurações de implantação:
 - Cluster: selecione ou crie um cluster ECS
 - Serviço: Configurar o serviço ECS
 - Definição da tarefa: Revise a definição da tarefa gerada
 - Balanceador de carga: Configurar ALB/NLB
 - Auto-scaling: Defina políticas de escalabilidade
4. Revise a infraestrutura como código (modelo ou código CDK) CloudFormation AWS
5. Escolha Implantar

Monitore a implantação

AWS O Transform implanta seu aplicativo:

1. Cria o cluster Aurora PostgreSQL
2. Aplica o esquema do banco de dados
3. Carrega dados (se aplicável)
4. Implanta contêineres de aplicativos
5. Configura o balanceador de carga
6. Configura o auto-scaling

Monitore o progresso da implantação e verifique:

- Provisãoamento de infraestrutura
- Inicialização do banco de dados
- Implantação de aplicações
- Verificações de saúde aprovadas

- Aplicativo acessível
- As conexões de banco de dados funcionam
- Registros mostrando a operação normal

Post-deployment validação

Após a implantação:

Teste de fumaça:

- Verifique a funcionalidade crítica
- Teste os principais fluxos de trabalho do usuário
- Verifique os pontos de integração
- Monitore as taxas de erro

Monitoramento de desempenho:

- Monitore os tempos de resposta
- Monitore consultas ao banco de dados
- Verifique a utilização dos recursos
- Revise os registros do aplicativo

Validação do usuário:

- Realizar testes de aceitação do usuário
- Colete feedback
- Resolva quaisquer problemas
- Documente as lições aprendidas

Procedimentos de reversão

Se surgirem problemas após a implantação:

Reversão imediata:

- Reverter para a versão anterior do aplicativo

- Volte para o SQL Server (se ainda estiver disponível)
- Restaure a partir do backup, se necessário

Reversão parcial:

- Reverta componentes específicos
- Mantenha as alterações no banco de dados
- Reverter somente o código do aplicativo

Correção direta:

- Aplique o hotfix à versão do Aurora PostgreSQL
- Implantar código de aplicativo atualizado
- Monitor para resolução

 Important

Mantenha seu banco de dados SQL Server disponível por um período após a transferência para permitir a reversão, se necessário.

Post-deployment otimização

Após a implantação bem-sucedida:

Ajuste de desempenho:

- Otimize consultas lentas
- Ajustar as configurações do pool de conexões
- Fine-tune Parâmetros do Aurora PostgreSQL
- Revise e otimize índices

Otimização de custos:

- Right-size Instância do Aurora

- Configure o auto-scaling de forma adequada
- Revise as configurações de armazenamento
- Otimize a retenção de backup

Configuração de monitoramento:

- Configurar CloudWatch painéis
- Configurar alertas
- Habilitar monitoramento avançado
- Configurar Performance Insights

Documentação:

- Atualizar runbooks
- Mudanças na arquitetura do documento
- Equipe de operações de treinamento
- Crie guias de solução de problemas

Teste e implante após a transformação

Implante seus aplicativos transformados na landing zone e valide a conectividade entre seus aplicativos e o banco de dados transformado e, opcionalmente, configure CI/CD pipelines. Exemplos de configurações de CI/CD pipeline são gerados como referência para ajudá-lo a implementar sua automação de implantação. Essa fase final valida a modernização completa.

Configurar recursos

Você precisa configurar os recursos usados na implantação, como funções do IAM, perfis de instância e bucket do S3. AWS O Transform não tem permissões para criar buckets do S3 ou fazer alterações em seu IAM. Essa ação precisa ser executada por um usuário que tenha permissões para criar novas funções. Normalmente, é administrador da conta.

Para simplificar o processo, fornecemos um script de configuração que automaticamente:

- Executa os modelos necessários CloudFormation
- Cria a função ECS Service-Linked

- Configura todos os recursos necessários do IAM

Important

Execute o script de configuração fornecido como está - não modifique nenhum nome de recurso nos modelos ou no script, pois isso pode afetar o processo de implantação.

Para Linux:

```
./setup.sh --region <YOUR-Region>
```

Para Windows:

```
./setup.ps1 -Region <YOUR-Region>
```

Verifique os grupos de segurança em sua VPC

AWS O Transform implanta os aplicativos na mesma sub-rede e no mesmo grupo de segurança da instância do Aurora PostgreSQL.

Para que o aplicativo se conecte à instância do Aurora, certifique-se de que esse grupo de segurança tenha regras de saída que permitam a conexão com o mesmo grupo de segurança e regras de entrada que permitam a conexão do mesmo grupo de segurança.

Selecione e configure aplicativos

A interface do usuário do AWS Transform mostra uma lista de aplicativos que podem ser implantados. Selecione o aplicativo e clique em Configurar e confirmar para abrir uma janela de configuração na qual você pode especificar:

- Infraestrutura de destino para os aplicativos: selecione o ECS ou uma das instâncias do EC2
- Parâmetros do aplicativo ou da instância

Depois de concluir e fechar a janela de configuração, AWS Transforme:

- Gera artefatos de implantação com base na sua configuração

- Confirma esses artefatos em seu repositório, incluindo:
 - Scripts de implantação
 - CloudFormation modelos
 - Exemplos de configurações de CI/CD pipeline (que você pode usar como referência para configurar sua automação de implantação)

Depois que a confirmação é concluída, o status do aplicativo muda para Configurado e confirmado. Em seguida, você pode selecionar os aplicativos e usar o botão Implantar no canto superior direito para iniciar a implantação.

Implantação do ECS

Todos os aplicativos com ECS de destino são implantados em um novo cluster ECS criado em sua conta. Cada aplicativo é implantado em seu próprio contêiner dedicado. Não há suporte para vários aplicativos por contêiner. Você configura os parâmetros do contêiner para cada aplicativo individualmente, como CPU e memória necessárias.

Implantação do EC2

Você pode selecionar uma das instâncias do EC2 propostas e configurar seus parâmetros, como tipo de instância. Vários aplicativos podem ser implantados na mesma instância do EC2:

- Para implantar vários aplicativos em uma única instância, selecione a mesma instância EC2 de destino para cada um desses aplicativos durante a configuração.
- Todos os aplicativos que têm a mesma instância selecionada como destino são implantados nessa instância e recebem portas aleatórias diferentes.
- Observe que, se você editar os parâmetros da instância de um aplicativo e depois editar outro aplicativo direcionado à mesma instância, as alterações afetarão todos os aplicativos implantados nessa instância.

Sucesso na implantação

Após a implantação bem-sucedida, seus aplicativos são executados no Aurora PostgreSQL com custos de licenciamento reduzidos, desempenho aprimorado e escalabilidade nativa da nuvem. O trabalho permanece aberto, a menos que seja explicitamente interrompido. Isso permite a opção de uma possível reimplantação com parâmetros de implantação atualizados.

Práticas recomendadas e solução de problemas

Melhores práticas e problemas comuns e suas soluções durante o processo de modernização.

Registros de aplicativos do ECS

CloudWatch troncos

- Todos os registros de contêineres do ECS são enviados automaticamente para CloudWatch Logs
- Acesse os registros no CloudWatch console em Grupos de registros
- Formato de nomenclatura do grupo de registros: `/aws/ecs/{application-name}`
- Cada instância de contêiner cria um novo fluxo de log dentro do grupo.

Visualizar logs

Por meio AWS do console:

- Navegue até CloudWatch > Grupos de registros
- Selecione o grupo de registros do seu aplicativo
- Escolha o fluxo de registros relevante para visualizar os registros do contêiner

Usando a AWS CLI:

```
aws logs get-log-events --log-group-name /aws/ecs/your-app-name --log-stream-name your-stream-name
```

Localizações comuns de registros

- Registros do aplicativo: CloudWatch registros
- Eventos do serviço ECS: Console do ECS > Cluster > Serviço > guia Eventos
- Contêiner health/status: Console do ECS > Cluster > Serviço > guia Tarefas

Gerenciamento de conexões de banco de dados

Os aplicativos usam variáveis de ambiente para configurações de conexão do banco de dados

Se você tiver problemas de conectividade:

- Verifique as configurações de conexão atuais em suas variáveis de ambiente
- Atualize as variáveis de ambiente para modificar as cadeias de conexão do banco de dados conforme necessário
- Alterações na cadeia de conexão podem ser feitas por meio de atualizações de variáveis de ambiente sem a reimplantação do aplicativo

Problemas de conexão de banco de dados

Problema: Não é possível conectar o AWS Transform ao SQL Server

Soluções:

- Verifique a conectividade de rede entre o AWS Transform e o SQL Server
- Verifique as regras do grupo de segurança para acesso adequado à porta (1433)
- Confirme as credenciais do banco de dados no Secrets Manager
- Teste as permissões do banco de dados com o usuário criado
- Verifique se o SQL Server está configurado para autenticação em modo misto
- Verifique se o segredo tem as tags necessárias (Projeto: atx-db-modernization, proprietário: database-connector)

Problemas de firewall e grupos de segurança

Problema: tempo limite de conexão ou erros de “não é possível acessar o banco de dados”

Causa raiz: grupos de segurança ou ACLs de rede bloqueando o tráfego

Soluções:

1. Verifique a configuração do grupo de segurança:

- Confirme se seu grupo de segurança do SQL Server tem uma regra de entrada que permite a porta 1433 do grupo de segurança DMS Schema Conversion
- Verifique se a origem é o ID do grupo de segurança (por exemplo, sg-0123456789abcdef0), não um endereço IP
- Verifique se o grupo de segurança DMS Schema Conversion está especificado corretamente no Perfil da Instância

- Certifique-se de que não haja regras de negação conflitantes
2. Verifique as ACLs de rede:
- Verifique se as ACLs de rede no nível da sub-rede permitem tráfego de entrada na porta 1433
 - Certifique-se de que as ACLs de rede permitam portas efêmeras de saída para tráfego de retorno
 - Verifique as ACLs de rede da sub-rede do banco de dados e da sub-rede do DMS
3. Verifique a configuração da VPC:
- Confirme se a instância de conversão do esquema DMS e o SQL Server estão na mesma VPC ou têm o emparelhamento de VPC adequado
 - Verifique se as tabelas de rotas permitem o tráfego entre sub-redes
 - Verifique se nenhum dispositivo de firewall está bloqueando o tráfego
4. Teste a conectividade:
- Execute uma instância EC2 de teste na mesma sub-rede do DMS Schema Conversion
 - Anexe o mesmo grupo de segurança que o DMS Schema Conversion
 - Teste a conexão com o SQL Server usando telnet ou SQL Server Management Studio
 - Se o teste for bem-sucedido, o problema é com a configuração do AWS Transform; se falhar, o problema é network/firewall

Erro comum: abrir a porta 1433 para 0.0.0. 0/0 (todas as fontes) é um risco de segurança. Sempre use o controle de acesso baseado em grupos de segurança para limitar o acesso somente ao grupo de segurança DMS Schema Conversion.

Problemas de conversão de esquema

Problema: a conversão do esquema mostra muitos itens de ação

Soluções:

- Revise os itens de ação no relatório de conversão
- Priorize com base no impacto
- Use o Amazon Q Developer para conversões complexas de SQL
- Consulte o AWS Support para obter orientação
- Considere a abordagem em fases para bancos de dados complexos

Problemas de transformação de aplicativos

Problema: falha na construção da transformação do aplicativo

Soluções:

- Analise os erros de construção no relatório de transformação
- Configure NuGet feeds privados, se necessário
- Atualize as referências do pacote, se necessário
- Verifique as Windows-specific dependências
- Analise os registros de transformação para ver erros detalhados

Problemas de migração de dados

Problema: falha na validação da migração de dados

Soluções:

- Revise o relatório de validação para falhas específicas
- Verifique os mapeamentos de tipos de dados
- Verifique a configuração da coluna de identidade (GERADA POR PADRÃO versus GERADA SEMPRE)
- Revise as expressões de coluna computadas
- Entre em contato com o AWS Support para problemas complexos de dados

Problemas de limpeza de recursos

Problema: falha na tarefa de transformação com erros de recursos

Soluções:

- Verifique os recursos existentes do DMS (projetos de migração, provedores de dados, perfis de instância)
- Limpe recursos falhados ou incompletos de tentativas anteriores
- Verifique se os segredos não estão programados para exclusão
- Verifique as cotas de serviço para DMS e Aurora PostgreSQL

- Entre em contato com o AWS Support se a limpeza não resolver o problema

Problemas de implantação

Problema: o aplicativo transformado não consegue se conectar ao Aurora PostgreSQL

Soluções:

- Verifique o formato da cadeia de conexão para o PostgreSQL
- Verifique as regras do grupo de segurança
- Verifique as credenciais do banco de dados no Secrets Manager
- Verifique SSL/TLS se está configurado corretamente
- Teste a conexão usando psql ou pgAdmin

Obter ajuda adicional

Ao entrar em contato com o AWS Support, forneça:

- ID do trabalho de transformação
- AWS ID da conta
- Região
- Mensagens de erro e capturas de tela
- Registros de transformação (disponíveis no console do AWS Transform)

Segurança em AWS Transformação

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Third-party auditores testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao AWS Transform, consulte [AWS Serviços no escopo por programa de conformidade AWS](#) .
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AWS Transform. Os tópicos a seguir mostram como configurar o AWS Transform para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do AWS Transform.

Tópicos

- [Proteção de dados em AWS Transform](#)
- [Gerenciamento de identidade e acesso para AWS Transformação](#)
- [Validação de conformidade AWS Transformação](#)
- [Resiliência em AWS Transformação](#)
- [AWS Transform e endpoints de interface \(AWS PrivateLink\)](#)
- [Acessando o AWS Transform aplicativo web a partir de uma VPC](#)

Proteção de dados em AWS Transform

O [modelo de responsabilidade AWS compartilhada](#) se aplica à proteção de dados em AWS Transform. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de dados](#). Para obter mais informações sobre a proteção de dados na Europa, consulte o artigo do blog [AWS Shared Responsibility Model and GDPR](#) no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Recomendamos usar o TLS 1.2 ou posterior.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços de segurança gerenciados avançados Amazon Macie, como, que ajudam a descobrir e proteger dados confidenciais armazenados em. Amazon S3
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-2](#).

É altamente recomendável que informações confidenciais ou sigilosas, como endereços de e-mail de clientes, sejam colocadas em [tags](#) ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS Transform ou Serviços da AWS usa a API Console de gerenciamento da AWS, AWS Command Line Interface (AWS CLI) ou AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Para obter mais informações sobre como AWS Transform usa o conteúdo, consulte [AWS Transform melhoria do serviço](#).

AWS Transform armazena suas perguntas, suas respostas e contexto adicional, como metadados e código do console em seu IDE, para gerar respostas às suas perguntas. Para obter informações sobre como os dados são criptografados, consulte [Criptografia de dados em AWS Transform](#). Para obter informações sobre como AWS podemos usar algumas perguntas que você faz AWS Transform e suas respostas para melhorar nossos serviços, consulte [AWS Transform melhoria do serviço](#).

Em AWS Transform, seus dados são armazenados na AWS região em que seu AWS Transform perfil foi criado.

Com a inferência cruzada, suas solicitações AWS Transform podem ser processadas em uma região diferente dentro da geografia em que seus dados estão armazenados. Para obter mais informações, consulte [Cross-Region inferência](#).

Tópicos

- [Cross-region processamento em AWS Transform](#)
- [Criptografia de dados em AWS Transform](#)
- [AWS Transform melhoria do serviço](#)

Cross-region processamento em AWS Transform

As seções a seguir descrevem como a inferência entre regiões e as chamadas entre regiões são usadas para fornecer o serviço. AWS Transform

Cross-region inferência

AWS Transform é desenvolvido pelo Amazon Bedrock e usa inferência entre regiões para distribuir o tráfego entre diferentes regiões para aprimorar o desempenho e Regiões da AWS a confiabilidade da inferência do modelo de linguagem grande (LLM). Com a inferência entre regiões, é possível obter:

- Maior throughput e resiliência durante períodos de alta demanda
- Melhoria de desempenho
- Acesso a AWS Transform capacidades e recursos recém-lançados que dependem dos LLMs mais poderosos hospedados no Amazon Bedrock

Cross-region as solicitações de inferência são mantidas dentro do Regiões da AWS que faz parte da geografia em que os dados residem originalmente. Por exemplo, uma solicitação feita a partir de uma AWS Transform configuração nos EUA é mantida Regiões da AWS nos EUA. Embora a

inferência entre regiões não altere onde os dados são armazenados, as solicitações e os resultados de saída podem sair da região nas quais os dados residem originalmente. Todos os dados serão criptografados enquanto forem transmitidos pela rede segura da Amazon. Não há custo adicional para usar a inferência entre regiões.

A inferência entre regiões não afeta o local onde seus dados são armazenados. Para obter informações sobre onde os dados são armazenados quando você usa AWS Transform, consulte [Proteção de dados em AWS Transform](#).

Regiões suportadas para AWS Transform inferência entre regiões

Certas solicitações que você faz AWS Transform podem exigir chamadas entre regiões. A tabela a seguir descreve para quais regiões suas solicitações podem ser encaminhadas, dependendo da geografia de origem da solicitação.

Região de origem	Regiões de destino
Leste dos EUA (Norte da Virgínia) (us-east-1)	Leste dos EUA (Norte da Virgínia) (us-east-1) Leste dos EUA (Ohio) (us-east-2) Oeste dos EUA (Oregon) (us-west-2)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1) UE (Estocolmo) (eu-north-1) UE (Milão) (eu-south-1) Europa (Espanha) (eu-south-2) Europa (Irlanda) (eu-west-1) Europa (Paris) (eu-west-3)
Ásia-Pacífico (Mumbai) (ap-south-1)	Ásia Pacific (Tóquio) (ap-northeast-1) Ásia-Pacífico (Seul) (ap-northeast-2) Ásia-Pacífico (Osaka) (ap-northeast-3) Ásia-Pacífico (Mumbai) (ap-south-1)

Região de origem	Regiões de destino
	Ásia-Pacífico (Hyderabad) (ap-south-2) Ásia-Pacífico (Singapura) (ap-southeast-1) Ásia-Pacífico (Sydney) (ap-southeast-2) Ásia-Pacífico (Melbourne) (ap-southeast-4)
Ásia Pacific (Tóquio) (ap-northeast-1)	Ásia Pacific (Tóquio) (ap-northeast-1) Ásia-Pacífico (Osaka) (ap-northeast-3)
Ásia-Pacífico (Seul) (ap-northeast-2)	Ásia Pacific (Tóquio) (ap-northeast-1) Ásia-Pacífico (Seul) (ap-northeast-2) Ásia-Pacífico (Osaka) (ap-northeast-3) Ásia-Pacífico (Mumbai) (ap-south-1) Ásia-Pacífico (Hyderabad) (ap-south-2) Ásia-Pacífico (Singapura) (ap-southeast-1) Ásia-Pacífico (Sydney) (ap-southeast-2) Ásia-Pacífico (Melbourne) (ap-sudeste-4)
Ásia-Pacífico (Sydney) (ap-southeast-2)	Ásia-Pacífico (Sydney) (ap-southeast-2) Ásia-Pacífico (Melbourne) (ap-southeast-4)

Região de origem	Regiões de destino
Europa (Londres) (eu-west-2)	Europa (Frankfurt) (eu-central-1)
	UE (Estocolmo) (eu-north-1)
	UE (Milão) (eu-south-1)
	Europa (Espanha) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (Londres) (eu-west-2)
	Europa (Paris) (eu-west-3)
Canadá (Central) (ca-central-1)	Comercial Regiões da AWS + Canadá (Central) (ca-central-1)
América do Sul (São Paulo) (sa-east-1)	Comercial Regiões da AWS + América do Sul (São Paulo) (sa-east-1)

Para obter uma lista completa das regiões onde você pode usar AWS Transform, consulte [Regiões suportadas para AWS Transform](#).

Cross-Region conhecimento

Quando você faz uma pergunta geral sobre AWS Transform serviços, fluxos de trabalho de transformação ou AWS documentação relacionada, AWS Transform pode fazer solicitações entre regiões para o Leste dos EUA (Virgínia) (us-east-1) para as regiões dos EUA ou para a Europa (Frankfurt) (eu-central-1) para todas as outras regiões para recuperar a documentação e atender à sua solicitação. Por exemplo, quando você faz perguntas sobre como usar outros AWS serviços, como o Lambda, AWS Transform pode fazer uma chamada entre regiões para recuperar a AWS documentação relevante para responder à sua pergunta. A tabela a seguir descreve para quais regiões suas solicitações podem ser encaminhadas, dependendo da geografia de origem da solicitação.

Região de origem	Regiões de destino
Leste dos EUA (Norte da Virgínia) (us-east-1)	Leste dos EUA (Norte da Virgínia) (us-east-1)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1)
Europa (Londres) (eu-west-2)	Europa (Frankfurt) (eu-central-1)
Ásia Pacífico (Tóquio) (ap-northeast-1)	Europa (Frankfurt) (eu-central-1)
Ásia-Pacífico (Sydney) (ap-southeast-2)	Europa (Frankfurt) (eu-central-1)
Ásia-Pacífico (Seul) (ap-northeast-2)	Europa (Frankfurt) (eu-central-1)
Ásia-Pacífico (Mumbai) (ap-south-1)	Europa (Frankfurt) (eu-central-1)
Canadá (Central) (ca-central-1)	Europa (Frankfurt) (eu-central-1)
América do Sul (São Paulo) (sa-east-1)	Europa (Frankfurt) (eu-central-1)

Esta definição é habilitada por padrão. Um administrador da conta pode modificar essa configuração. A desativação desse recurso resulta na perda de acesso aos recursos que exigem AWS Transform a recuperação de conhecimento de outras regiões. Isso pode resultar em respostas menos precisas.

Para desativar as chamadas entre regiões feitas por: AWS Transform

1. Ao fazer a primeira configuração AWS Transform, navegue até a página Get Started e conclua a configuração. Para uma AWS Transform configuração existente, navegue até a página Configurações.
2. Alterne a opção Ativar chamadas entre regiões para responder a perguntas gerais AWS relacionadas à posição desligada.

AWS Transform para inferência entre regiões do Windows

A tabela a seguir mostra as regiões de origem das quais você pode chamar o perfil de inferência e as regiões de destino para as quais as solicitações podem ser roteadas:

Região de origem	Regiões de destino de inferência
Leste dos EUA (Norte da Virgínia) (us-east-1)	Leste dos EUA (Norte da Virgínia) (us-east-1) Leste dos EUA (Ohio) (us-east-2) Oeste dos EUA (Oregon) (us-west-2)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1) UE (Estocolmo) (eu-north-1) UE (Milão) (eu-south-1) Europa (Espanha) (eu-south-2) Europa (Irlanda) (eu-west-1) Europa (Paris) (eu-west-3)
Ásia Pacific (Tóquio) (ap-northeast-1)	Ásia Pacific (Tóquio) (ap-northeast-1) Ásia-Pacífico (Osaka) (ap-northeast-3)
Ásia-Pacífico (Sydney) (ap-southeast-2)	Ásia-Pacífico (Sydney) (ap-southeast-2) Ásia-Pacífico (Melbourne) (ap-southeast-4)
Ásia-Pacífico (Seul) (ap-northeast-2)	Todas as regiões comerciais
Ásia-Pacífico (Mumbai) (ap-south-1)	Todas as regiões comerciais
Canadá (Central) (ca-central-1)	Todas as regiões comerciais

AWS Transform para inferência entre regiões de migrações

A tabela a seguir mostra as regiões de origem das quais você pode chamar o perfil de inferência e as regiões de destino para as quais as solicitações podem ser roteadas:

Região de origem	Regiões de destino de inferência
Leste dos EUA (Norte da Virgínia) (us-east-1)	Todas as regiões comerciais
Europa (Frankfurt) (eu-central-1)	Todas as regiões comerciais
Europa (Londres) (eu-west-2)	Todas as regiões comerciais
Ásia Pacific (Tóquio) (ap-northeast-1)	Ásia Pacific (Tóquio) (ap-northeast-1) Ásia-Pacífico (Osaka) (ap-northeast-3)
Ásia-Pacífico (Sydney) (ap-southeast-2)	Ásia-Pacífico (Sydney) (ap-southeast-2) Ásia-Pacífico (Melbourne) (ap-southeast-4)
Ásia-Pacífico (Seul) (ap-northeast-2)	Todas as regiões comerciais
Ásia-Pacífico (Mumbai) (ap-south-1)	Todas as regiões comerciais
Canadá (Central) (ca-central-1)	Todas as regiões comerciais

AWS Transform para inferência entre regiões de mainframe

AWS Transform para mainframe usa a inferência geográfica entre regiões do Amazon Bedrock. Isso significa que algumas de suas chamadas podem ser roteadas para Regiões da AWS fora da sua região de origem. A tabela a seguir mostra as regiões de origem das quais você pode chamar o perfil de inferência e as regiões de destino para as quais as solicitações podem ser roteadas:

Região de origem	Regiões de destino de inferência
Leste dos EUA (Norte da Virgínia) (us-east-1)	Leste dos EUA (Norte da Virgínia) (us-east-1) Leste dos EUA (Ohio) (us-east-2) Oeste dos EUA (Oregon) (us-west-2)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1) UE (Estocolmo) (eu-north-1)

Região de origem	Regiões de destino de inferência
	UE (Milão) (eu-south-1) Europa (Espanha) (eu-south-2) Europa (Irlanda) (eu-west-1) Europa (Paris) (eu-west-3)
Europa (Londres) (eu-west-2)	Europa (Frankfurt) (eu-central-1) UE (Estocolmo) (eu-north-1) UE (Milão) (eu-south-1) Europa (Espanha) (eu-south-2) Europa (Irlanda) (eu-west-1) Europa (Londres) (eu-west-2) Europa (Paris) (eu-west-3)
Ásia Pacífico (Tóquio) (ap-northeast-1)	Ásia Pacífico (Tóquio) (ap-northeast-1) Ásia-Pacífico (Osaka) (ap-northeast-3)
Ásia-Pacífico (Sydney) (ap-southeast-2)	Ásia-Pacífico (Sydney) (ap-southeast-2) Ásia-Pacífico (Melbourne) (ap-southeast-4)
Ásia-Pacífico (Seul) (ap-northeast-2)	Todas as regiões comerciais
Ásia-Pacífico (Mumbai) (ap-south-1)	Todas as regiões comerciais
Canadá (Central) (ca-central-1)	Canadá (Central) (ca-central-1) Leste dos EUA (Norte da Virgínia) (us-east-1) Leste dos EUA (Ohio) (us-east-2) Oeste dos EUA (Oregon) (us-west-2)

Região de origem	Regiões de destino de inferência
América do Sul (São Paulo) (sa-east-1)	Todas as regiões comerciais

AWS Transform Personalizada

AWS Transform usa de forma personalizada a inferência geográfica entre regiões do Amazon Bedrock. Isso significa que algumas de suas chamadas podem ser roteadas para Regiões da AWS fora da sua região de origem. A tabela a seguir mostra as regiões de origem das quais você pode chamar o perfil de inferência e as regiões de destino para as quais as solicitações podem ser roteadas:

Região de origem	Regiões de destino de inferência
Leste dos EUA (Norte da Virgínia) (us-east-1)	Leste dos EUA (Norte da Virgínia) (us-east-1) Leste dos EUA (Ohio) (us-east-2) Oeste dos EUA (Oregon) (us-west-2)
Europa (Frankfurt) (eu-central-1)	Europa (Frankfurt) (eu-central-1) UE (Estocolmo) (eu-north-1) UE (Milão) (eu-south-1) Europa (Espanha) (eu-south-2) Europa (Irlanda) (eu-west-1) Europa (Paris) (eu-west-3)
Europa (Londres) (eu-west-2)	Europa (Frankfurt) (eu-central-1) UE (Estocolmo) (eu-north-1) UE (Milão) (eu-south-1) Europa (Espanha) (eu-south-2)

Região de origem	Regiões de destino de inferência
	Europa (Irlanda) (eu-west-1)
	Europa (Londres) (eu-west-2)
	Europa (Paris) (eu-west-3)
Ásia Pacific (Tóquio) (ap-northeast-1)	Todas as regiões comerciais
Ásia-Pacífico (Sydney) (ap-southeast-2)	Ásia-Pacífico (Sydney) (ap-southeast-2)
	Ásia-Pacífico (Melbourne) (ap-southeast-4)
Ásia-Pacífico (Seul) (ap-northeast-2)	Todas as regiões comerciais
Ásia-Pacífico (Mumbai) (ap-south-1)	Todas as regiões comerciais
Canadá (Central) (ca-central-1)	Canadá (Central) (ca-central-1)
	Leste dos EUA (Norte da Virgínia) (us-east-1)
	Leste dos EUA (Ohio) (us-east-2)
	Oeste dos EUA (Oregon) (us-west-2)

Criptografia de dados em AWS Transform

Este tópico fornece informações específicas AWS Transform sobre criptografia em trânsito e criptografia em repouso.

AWS Transform fornece criptografia por padrão para proteger dados confidenciais do cliente em repouso com criptografia usando chaves AWS próprias.

Tipos de criptografia

Criptografia em trânsito

A comunicação entre clientes AWS Transform e entre suas dependências posteriores é protegida usando conexões TLS 1.2 ou superior.

⚠ Important

Quando você [conecta uma conta de descoberta](#), o AWS Transform cria um bucket Amazon S3 em seu nome nessa conta. Esse bucket não está SecureTransport habilitado por padrão. Se você quiser que a política de bucket inclua transporte seguro, você deve atualizar a política. Para obter mais informações, consulte [Melhores práticas de segurança para o Amazon S3](#).

Criptografia em repouso

AWS Transform armazena dados em repouso usando o Amazon DynamoDB e o Amazon Simple Storage Service (Amazon S3). Os dados em repouso são criptografados usando soluções de AWS criptografia por padrão. AWS Transform criptografa seus dados com criptografia usando chaves AWS próprias do AWS Key Management Service (AWS KMS). Você não precisa realizar nenhuma ação para proteger as chaves AWS gerenciadas que criptografam seus dados. Para obter mais informações, consulte [Chaves de propriedade da AWS](#) no AWS Key Management Service Guia do desenvolvedor do .

Tipo de dados	AWS- criptografia de chave própria	Criptografia de chave gerenciada pelo cliente (opcional)
Dados do bucket do cliente	Habilitado	Habilitado
Entradas e saídas do cliente, como código e documentação armazenados em um bucket do Amazon S3		
Loja de Artifatos	Habilitado	Habilitado
Artefatos intermediários como parte da transformação de código armazenados em um bucket S3		
Objetivo do trabalho	Habilitado	Habilitado

Tipo de dados	AWS- criptografia de chave própria	Criptografia de chave gerenciada pelo cliente (opcional)
A intenção do cliente em relação ao trabalho armazenada em um bucket do Amazon S3		
Mensagens de chat	Habilitado	Habilitado
Mensagens entre o cliente e AWS Transform armazenadas em um bucket do Amazon S3		
Base de conhecimento do Chat	Habilitado	Habilitado
Dados indexados relevantes AWS Transform e bate-papo com clientes armazenados na Amazon OpenSearch e processados via AWS Bedrock		

Observação: o cliente pode registrar sua própria Chave Gerenciada pelo Cliente (CMK) para ser usada na criptografia de todos os tipos de dados acima.

As chaves gerenciadas pelo cliente são chaves KMS em sua AWS conta que você cria, possui e gerencia para controlar diretamente o acesso aos seus dados, controlando o acesso à chave KMS. Somente chaves simétricas têm suporte. Para obter informações sobre como criar sua própria chave KMS, consulte [Criação de chaves](#) no Guia do AWS Key Management Service desenvolvedor.

Quando você usa uma chave gerenciada pelo cliente, AWS Transform faz uso de concessões do KMS, permitindo que usuários, funções ou aplicativos autorizados usem uma chave KMS. Quando um AWS Transform administrador opta por usar uma chave gerenciada pelo cliente para criptografia durante a configuração, uma concessão é criada para ele. Essa concessão é o que permite que o

usuário final use a chave de criptografia para criptografia de dados em repouso. Para obter mais informações sobre concessões, consulte [Grants in AWS KMS](#).

AWS Chaves próprias (padrão)

Note

AWS chaves próprias — AWS Transform usa essas chaves por padrão para criptografar automaticamente dados de identificação pessoal. Você não pode visualizar, gerenciar ou usar chaves AWS próprias nem auditar seu uso. No entanto, não é necessário realizar nenhuma ação nem alterar qualquer programa para proteger as chaves que criptografam seus dados. Para obter mais informações, consulte chaves AWS próprias no Guia do desenvolvedor do AWS Key Management Service.

Por padrão, a criptografia de dados em repouso ajuda a reduzir a sobrecarga operacional e a complexidade envolvidas na proteção de dados confidenciais. Ao mesmo tempo, ela permite que você crie aplicações seguras que atendam aos rigorosos requisitos regulatórios e de conformidade de criptografia.

Embora você não possa desabilitar essa camada de criptografia ou selecionar um tipo de criptografia alternativo, você pode adicionar uma segunda camada de criptografia sobre as chaves de criptografia de AWS propriedade existentes escolhendo uma chave gerenciada pelo cliente ao criar sua transformação:

Chaves gerenciadas pelo cliente (opcional)

Chaves gerenciadas pelo cliente — AWS Transform suporta o uso de uma chave simétrica gerenciada pelo cliente que você cria, possui e gerencia para adicionar uma segunda camada de criptografia sobre a criptografia existente usando chaves AWS próprias. Como você tem controle total dessa camada de criptografia, você pode realizar tarefas como:

- Estabelecer e manter as políticas de chave
- Estabelecer e manter subsídios e IAM policies
- Habilitar e desabilitar políticas de chaves
- Alternar os materiais de criptografia de chave
- Adicionar etiquetas
- Criar réplicas de chaves

- Alternar os materiais de criptografia de chave
- Adicionar etiquetas
- Criar réplicas de chaves
- Chaves de agendamento para exclusão
- Para obter mais informações, consulte [chave gerenciada pelo cliente](#) no Guia do desenvolvedor do AWS Key Management Service.

 Note

AWS Transform ativa automaticamente a criptografia em repouso usando chaves AWS próprias para proteger dados de identificação pessoal sem nenhum custo. No entanto, AWS KMS cobranças são cobradas pelo uso de uma chave gerenciada pelo cliente. Para obter mais informações sobre preços, consulte [definição de preços da AWS Key Management Service](#).

Para obter mais informações sobre AWS KMS, consulte [O que é AWS Key Management Service?](#)

Como AWS Transform usa subsídios em AWS Key Management Service

AWS Transform exige uma concessão para usar sua chave gerenciada pelo cliente.

Quando você cria um [Nome do recurso] criptografado com uma chave gerenciada pelo cliente, AWS Transform cria uma concessão em seu nome enviando uma CreateGrant solicitação para AWS Key Management Service. As concessões AWS Key Management Service são usadas para dar AWS Transform acesso a uma chave KMS em uma conta de cliente.

AWS Transform exige que a concessão use sua chave gerenciada pelo cliente para as seguintes operações internas:

- Envie solicitações da [API KMS] para verificar se AWS KMS a ID simétrica da chave KMS gerenciada pelo cliente inserida ao criar o [Nome do recurso] é válida.
- Envie solicitações da [API KMS] AWS KMS para gerar chaves de dados criptografadas pela chave gerenciada pelo cliente.
- Envie solicitações da [API KMS] para AWS KMS descriptografar as chaves de dados criptografadas para que elas possam ser usadas para criptografar seus dados.

É possível revogar o acesso à concessão, ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, AWS Transform não conseguirá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afeta as operações que dependem desses dados. Por exemplo, se você tentar obter [Nome do recurso] de um [Nome do recurso] criptografado que não AWS Transform pode ser acessado, a operação retornará um `AccessDeniedException` erro.

Criar uma chave gerenciada pelo cliente

Você pode criar uma chave simétrica gerenciada pelo cliente usando o AWS Management Console ou as AWS Key Management Service APIs.

Para criar uma chave simétrica gerenciada pelo cliente, siga as etapas em [Criação de chave simétrica gerenciada pelo cliente](#) no Guia do desenvolvedor do AWS Key Management Service .

Para usar sua chave gerenciada pelo cliente com seus AWS Transform recursos, as seguintes operações de API devem ser permitidas na política de chaves:

kms: CreateGrant — Adiciona uma concessão a uma chave gerenciada pelo cliente. Concede acesso de controle a uma chave KMS especificada, o que permite o acesso AWS Transform necessário às operações de concessão. Para obter mais informações sobre [Utilizar concessões](#), consulte o Guia do desenvolvedor do AWS Key Management Service .

Isso permite AWS Transform fazer o seguinte:

- Chame a [API KMS ([GenerateDataKeyWithoutPlainText/GenerateDatakey](#))] para gerar uma chave de dados criptografada e armazená-la, pois a chave de dados não é usada imediatamente para criptografar.
- Chame a [API KMS ([Decrypt](#))] para usar a chave de dados criptografada armazenada para acessar dados criptografados.
- Configure uma entidade principal aposentada para permitir que o serviço para [RetireGrant](#).
- [kms: DescribeKey](#) — Fornece os detalhes da chave gerenciada pelo cliente para permitir que [Nome do serviço] valide a chave.

Criptografia para modernização do SQL

Durante o processo de [modernização do SQL Server](#), AWS Transform cria recursos em sua conta, como instâncias EC2, clusters ECS, imagens ECR e objetos S3. Você tem a opção de fornecer uma

chave gerenciada pelo cliente para criptografar dados em sua conta. Você precisará marcar sua chave KMS com a chave CreatedFor o valor AWSTransform. Este exemplo de política lista as permissões mínimas exigidas em sua política de chaves se você não tiver uma política de chaves padrão. Se você tiver uma política de chaves padrão, ainda precisará atualizar manualmente a chave KMS, além da política de chaves padrão, para permitir que o ECS use sua chave.

```
"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"
      }
    }
  }
}
]

```

Criptografia para migração de banco de dados

Durante o processo de migração do banco de dados, AWS Transform usa o AWS Database Migration Service (DMS) para migrar os dados do banco de dados. Opcionalmente, você pode fornecer uma chave gerenciada pelo cliente para criptografar os dados do banco de dados durante a migração.

A política a seguir contém três declarações. A primeira declaração concede permissões de conta raiz para a AWS KMS chave. A segunda declaração permite que a função do conector valide a chave durante a descoberta. A terceira declaração permite que a função de conector use a chave para operações do DMS.

```

"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"
    }
}
}
```

Usar chaves do KMS gerenciadas pelo cliente

Depois de criar uma chave KMS gerenciada pelo cliente, um AWS Transform administrador deve fornecer a chave no AWS Transform console para usá-la para criptografar dados.

Para configurar uma chave gerenciada pelo cliente para criptografar dados AWS Transform, os administradores precisam de permissões para usar. AWS KMS

Para usar a funcionalidade criptografada com uma chave gerenciada pelo cliente, os usuários precisam de permissões para permitir o acesso AWS Transform à chave gerenciada pelo cliente.

Se você ver um erro relacionado às concessões do KMS durante o uso AWS Transform, provavelmente precisará atualizar suas permissões para permitir AWS Transform a criação de concessões. Para configurar automaticamente as permissões necessárias, acesse o AWS Transform console e escolha Atualizar permissões no banner na parte superior da página. Para permitir AWS Transform a criação de concessões, você precisa atualizar as permissões na página do AWS Transform console.

Permitir AWS Transform acesso às chaves gerenciadas pelo cliente

O exemplo de declaração de política a seguir concede aos usuários permissões para acessar recursos criptografados com uma chave gerenciada pelo cliente, permitindo o AWS Transform

acesso à chave. Essa política deve ser usada AWS Transform se um administrador tiver configurado uma chave gerenciada pelo cliente para criptografia.

Note

Essas informações não se aplicam ao fluxo de trabalho de implantação de modernização do SQL Server usando CMK.

```
"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 melhoria do serviço

Para ajudar a AWS Transform fornecer as informações mais relevantes, podemos usar determinados conteúdos AWS Transform, como perguntas que você faz AWS Transform e suas respostas, para melhorar o serviço. Esta página explica qual conteúdo usamos e como optar por não participar.

AWS Transform conteúdo usado para melhoria do serviço

Podemos usar determinados conteúdos de AWS Transform para melhorar o serviço. AWS Transform pode usar esse conteúdo, por exemplo, para fornecer respostas melhores a perguntas comuns, corrigir problemas AWS Transform operacionais, para depuração ou para treinamento de modelos.

O conteúdo que AWS pode ser usado para melhorar o serviço inclui, por exemplo, suas perguntas AWS Transform e as respostas e o código AWS Transform gerado.

Como cancelar

A forma como você opta por não AWS Transform usar o conteúdo para melhorar o serviço depende do ambiente em que você usa AWS Transform.

Para AWS Transform configurar uma política de exclusão de serviços de IA em AWS Organizations Para obter mais informações, consulte [Políticas de exclusão dos serviços de IA](#) no Guia do usuário do AWS Organizations .

Para optar por não compartilhar seu conteúdo no Visual Studio IDE, use o procedimento a seguir.

Vá para Ferramentas -> Opções -> Kit de ferramentas da AWS -> Amazon Q

Altere a opção Compartilhar conteúdo do Amazon Q com a AWS para Verdadeiro ou Falso.

Para optar por não compartilhar seus dados de telemetria no AWS Toolkit for Visual Studio, use este procedimento:

1. Em Ferramentas, escolha Opções.
2. No painel Opções, escolha Kit de ferramentas da AWS e, em seguida, escolha Geral.
3. Desmarque Permitir que o AWS Toolkit colete informações de uso.

Gerenciamento de identidade e acesso para AWS Transformação

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do AWS Transform. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticação com identidades](#)
- [Gerenciar o acesso usando políticas](#)
- [Como AWS O Transform funciona com o IAM](#)
- [Identity-based exemplos de políticas para AWS Transformação](#)
- [Solução de problemas AWS Transforme a identidade e o acesso](#)
- [Usando funções vinculadas a serviços para AWS Transform](#)
- [AWS políticas gerenciadas para AWS Transformação](#)
- [AWS Referência de permissões de transformação](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte [Solução de problemas AWS Transforme a identidade e o acesso](#)).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte [Como AWS O Transform funciona com o IAM](#))
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte [Identity-based exemplos de políticas para AWS Transformação](#))

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte [Como fazer login em sua Conta da AWS](#) no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte [AWS Signature Version 4 para solicitações de API](#) no Guia do usuário do IAM.

Conta da AWS usuário-raiz

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em [Tarefas que exigem credenciais de usuário-raiz](#) no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte [O que é o IAM Identity Center?](#) no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte [Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias](#) no Guia do usuário do IAM.

Um [grupo do IAM](#) especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte [Casos de uso de usuários do IAM](#) no Guia do usuário do IAM.

Perfis do IAM

Uma [perfil do IAM](#) é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função [mudando de um usuário para uma função do IAM](#)

[\(console\)](#) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte [Métodos para assumir um perfil](#) no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte [Visão geral das políticas JSON](#) no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Identity-based políticas

Identity-based políticas são documentos de políticas de permissões JSON que você anexa a uma identidade (usuário, grupo ou função). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

Identity-based as políticas podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do usuário do IAM.

Resource-based políticas

Resource-based políticas são documentos de política JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em

serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário [especificar uma entidade principal](#) em uma política baseada em recursos.

Resource-based políticas são políticas embutidas que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do usuário do IAM.
- Políticas de Controle de Serviços (SCPs): as SCPs especificam o número máximo de permissões para uma organização ou uma unidade organizacional no AWS Organizations. Para saber mais, consulte [Políticas de controle de serviço](#) no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs): definem o número máximo de permissões disponíveis para recursos em suas contas. Consulte mais informações em [Resource control policies \(RCPs\)](#) no Guia do usuário do AWS Organizations .
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte [Políticas de sessão](#) no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte [Lógica de avaliação de políticas](#) no Guia do usuário do IAM.

Como AWS O Transform funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao AWS Transform, saiba quais recursos do IAM estão disponíveis para uso com o AWS Transform.

Recurso do IAM	AWS Suporte ao Transform
Identity-based políticas	Sim
Resource-based políticas	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Service-linked funções	Sim

Para ter uma visão de alto nível de como o AWS Transform e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte [AWS os serviços que funcionam com o IAM](#) no Guia do usuário do IAM.

Identity-based políticas para AWS Transformação

Compatível com políticas baseadas em identidade: sim

Identity-based políticas são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como um usuário do IAM, um grupo de usuários ou uma função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais atributos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para

saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte [Referência de elemento de política JSON do IAM](#) no Guia do usuário do IAM.

Identity-based exemplos de políticas para AWS Transformação

Para ver exemplos de políticas baseadas em identidade do AWS Transform, consulte [Identity-based exemplos de políticas para AWS Transformação](#)

Resource-based políticas dentro AWS Transformação

Compatibilidade com políticas baseadas em recursos: não

Resource-based políticas são documentos de política JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Ações políticas para AWS Transformação

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do AWS Transform, consulte [Ações, recursos e chaves de condição do AWS Transform](#) na Referência de Autorização de Serviço.

Para ver uma lista de ações do AWS Transform custom, consulte [Ações, recursos e chaves de condição do AWS Transform custom](#) na Referência de autorização de serviço.

As ações de política no AWS Transform usam o seguinte prefixo antes da ação:

```
transform
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [  
    "transform:action1",  
    "transform:action2"  
]
```

Para ver exemplos de políticas baseadas em identidade do AWS Transform, consulte [Identity-based exemplos de políticas para AWS Transformação](#)

Recursos políticos para AWS Transformação

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do AWS Transform e seus ARNs e com quais ações você pode especificar o ARN de cada recurso, [consulte Ações, recursos e chaves de condição do Transform na Referência AWS de Autorização de Serviço](#).

Para ver uma lista dos tipos de recursos e seus ARNs e com quais ações você pode especificar o ARN de cada recurso AWS para o Transform custom, [consulte Ações, recursos e chaves AWS de condição do Transform](#) custom na Referência de autorização de serviço.

Para ver exemplos de políticas baseadas em identidade do AWS Transform, consulte [Identity-based exemplos de políticas para AWS Transformação](#)

Chaves de condição de política para AWS Transformação

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do AWS Transform e com quais ações e recursos você pode usar uma chave de condição, consulte [Ações, recursos e chaves de condição do AWS Transform](#) na Referência de Autorização de Serviço.

Para ver uma lista de chaves de condição e com quais ações e recursos você pode usar uma chave de condição para AWS Transform custom, consulte [Ações, recursos e chaves de condição para AWS Transform custom](#) na Referência de autorização de serviço.

Para ver exemplos de políticas baseadas em identidade do AWS Transform, consulte. [Identity-based exemplos de políticas para AWS Transformação](#)

ACLs em AWS Transformação

Compatível com ACLs: não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS Transformação

Compatível com ABAC (tags em políticas): parcial

Attribute-based controle de acesso (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte [Definir permissões com autorização do ABAC](#) no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte [Usar controle de acesso por atributo \(ABAC\)](#) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS Transformação

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte [Credenciais de segurança temporárias no IAM](#) e [Serviços da AWS que funcionam com o IAM](#) no Guia do usuário do IAM.

Cross-service permissões principais para AWS Transformação

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Sessões de acesso direto](#).

Funções de serviço para AWS Transformação

Compatível com perfis de serviço: sim

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.

 Warning

Alterar as permissões de uma função de serviço pode interromper a funcionalidade do AWS Transform. Edite as funções de serviço somente quando o AWS Transform fornecer orientação para fazer isso.

Service-linked funções para AWS Transformação

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir a função de realizar uma ação em seu nome. Service-linked as funções aparecem no seu Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço AWS Transform, consulte [Usando funções vinculadas a serviços para AWS Transform](#)

Identity-based exemplos de políticas para AWS Transformação

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS Transform. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte [Criar políticas do IAM \(console\)](#) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo AWS Transform, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte [Ações, recursos e chaves de condição para o AWS Transform](#) na Referência de autorização de serviço.

Tópicos

- [Práticas recomendadas de política](#)
- [Usar o AWS Console de transformação](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)
- [Permita que os administradores aceitem uma solicitação de conector da conta com AWS Transformação](#)

- [Permita que os administradores atribuam usuários existentes do IAM Identity Center e criem novos usuários do IAM Identity Center aos quais atribuir AWS Transformação](#)
- [Permitir que os administradores habilitem AWS Transformação](#)
- [Permitir que os usuários acessem AWS Transforme com credenciais do IAM](#)

Práticas recomendadas de política

Identity-based as políticas determinam se alguém pode criar, acessar ou excluir recursos do AWS Transform em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte [Elementos da política JSON do IAM: condição](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do Usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

Usar o AWS Console de transformação

Para acessar o console do AWS Transform, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do AWS Transform em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
  "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": "*"
    }
  ]
}

```

Permita que os administradores aceitem uma solicitação de conector da conta com AWS Transformação

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-*"
    }
]
}

```

Permita que os administradores atribuam usuários existentes do IAM Identity Center e criem novos usuários do IAM Identity Center aos quais atribuir AWS Transformação

A política a seguir concede as permissões que um administrador precisa para gerenciar usuários e grupos do IAM Identity Center no console do AWS Transform. Com essa política, um administrador pode atribuir e remover usuários e grupos, visualizar nomes de exibição, criar novos usuários do IAM Identity Center, gerenciar atribuições de aplicativos e definir as configurações da sessão do aplicativo.

```

{
  "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"
      }
    }
  }
]
}

```

Permitir que os administradores habilitem AWS Transformação

A política a seguir concede as permissões que um administrador precisa para habilitar e administrar o AWS Transform por meio do AWS console. Isso inclui gerenciar perfis, configurar agentes e gerenciar conectores. Essa política é destinada somente a administradores e deve ser direcionada aos diretores confiáveis em sua conta.

```

{
  "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": "*"
    }
  ]
}

```

```
]
}
```

Permitir que os usuários acessem AWS Transforme com credenciais do IAM

A política a seguir concede a um principal do IAM acesso ao aplicativo web e às APIs do AWS Transform usando credenciais do IAM. Essa política é necessária para o IAM-only acesso e para que o acesso ao IAM seja habilitado junto com um provedor de identidade.

Substitua *regionaccount-id*, e *profile-id* por seus valores. Você pode encontrar o ID do perfil no console do AWS Transform em Configurações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccess",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/profile-id"
    }
  ]
}
```

Para conceder acesso a todos os perfis em uma conta, use um caractere curinga para o ID do perfil:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccessAllProfiles",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/*"
    }
  ]
}
```

 Note

A `transform:AccessTransformProfile` ação concede acesso somente ao AWS Transform. As ações nos espaços de trabalho são controladas pelas funções do espaço de trabalho do AWS Transform (administrador, colaborador, aprovador Read-only), não pelas políticas do IAM. As funções do espaço de trabalho determinam o que um usuário pode fazer, como criar trabalhos, gerenciar colaboradores ou aprovar tarefas.

Solução de problemas AWS Transforme a identidade e o acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AWS Transform e o IAM.

Tópicos

- [Não estou autorizado a realizar uma ação em AWS Transformação](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha Conta da AWS para acessar meu AWS Transforme recursos](#)

Não estou autorizado a realizar uma ação em AWS Transformação

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo `my-example-widget` fictício, mas não tem as permissões AWS Transform:`GetWidget` fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: AWS Transform: GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso `my-example-widget` usando a ação AWS Transform:`GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Transform.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no AWS Transform. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS para acessar meu AWS Transforme recursos

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), é possível usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o AWS Transform é compatível com esses recursos, consulte [Como AWS O Transform funciona com o IAM](#).

- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui](#) no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como [fornecer acesso Contas da AWS a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Usando funções vinculadas a serviços para AWS Transform

AWS Transform usa funções [vinculadas ao serviço AWS Identity and Access Management](#) (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS Transform Service-linked as funções são predefinidas AWS Transform e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Usando funções vinculadas a serviços para AWS Transform

AWS Transform usa funções [vinculadas ao serviço AWS Identity and Access Management](#) (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS Transform Service-linked as funções são predefinidas AWS Transform e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração AWS Transform porque você não precisa adicionar manualmente as permissões necessárias. AWS Transform define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS Transform pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus AWS Transform recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a [AWS serviços](#), consulte [serviços que funcionam com IAM](#) e procure os serviços que têm Sim na coluna

de Service-linked funções. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Service-linked permissões de função para AWS Transform

AWS Transform usa a função vinculada ao serviço chamada [AWSServiceRoleForAWSTransform](#)—Essa Service-Linked função fornece ao AWS Transform a capacidade de fornecer informações de uso.

A função AWSServiceRoleForAWSTransform vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `transform.amazonaws.com`

A política de permissões de função nomeada AWSServiceRoleForAWSTransform AWS Transform permite concluir as seguintes ações nos recursos especificados:

- `cloudwatch: PutMetricData`
 - Envie métricas personalizadas CloudWatch para AWS Transform operações
 - Acompanhe o progresso da transformação, as taxas de sucesso e as métricas de desempenho
 - Ative o monitoramento e a emissão de alertas sobre fluxos de trabalho de transformação
- `então: DescribeApplication`
 - Exibir detalhes sobre um aplicativo específico no Identity Center
 - Obtenha metadados do aplicativo, como nome, descrição, status e configuração
- `então: GetApplicationAssignmentConfiguration`
 - Recuperar as configurações de atribuição para um aplicativo
 - Veja como `users/groups` estão configurados para serem atribuídos ao aplicativo
- `então: ListApplicationAssignmentsForPrincipal`
 - Listar todos os aplicativos atribuídos a um usuário ou grupo específico (principal)
 - Veja a quais aplicativos uma identidade específica tem acesso
- Permite a descryptografia de KMS-encrypted dados quando acessados por meio do IAM Identity Center. Só funciona quando o contexto de criptografia contém um ARN válido da instância do IAM Identity Center e deve ser acessado por meio dos endpoints de serviço do IAM Identity Center.

- Permite a descryptografia de KMS-encrypted dados quando acessados por meio do Identity Store. Só funciona quando o contexto de criptografia contém um ARN válido do Identity Store e deve ser acessado por meio dos endpoints do serviço Identity Store.
- gerente de segredos: GetSecretValue
 - Acesse segredos AWS Transform vinculados ao serviço usados para armazenar segredos de clientes para provedores de identidade externos
 - Recurso: `arn:aws:secretsmanager:*:*:secret:transform-preprod!` *
 - Condição: deve pertencer ao serviço transform-preprod e ser acessado pela mesma conta
- suporte:CreateCase, suporte:DescribeCases, suporte:DescribeCommunications, suporte:AddCommunicationToCase, suporte: ResolveCase
 - Crie e gerencie casos de suporte premium a partir do aplicativo AWS Transform web
 - Veja os detalhes do caso e as comunicações
 - Adicione comunicações e resolva casos de suporte

Você deve configurar permissões para permitir que seus usuários, grupos ou perfis criem, editem ou excluam um perfil vinculado ao serviço. Para obter mais informações, consulte [as permissões de Service-linked função](#) no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para AWS Transform

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria um perfil para AWS Transform no Console de gerenciamento da AWS, AWS Transform cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você atualiza as configurações, AWS Transform cria a função vinculada ao serviço para você novamente.

Você também pode usar o console do IAM ou a AWS CLI para criar uma função vinculada ao serviço com o nome do serviço. `transform.amazonaws.com` Para saber mais, consulte [Criar um perfil vinculado a serviço](#) no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editar uma função vinculada ao serviço para AWS Transform

AWS Transform não permite que você edite a função `AWSServiceRoleForAWSTransform` vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil,

pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para saber mais, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Transform

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

Note

Se o AWS Transform serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForAWSTransform` vinculada ao serviço. Para saber mais, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Regiões suportadas para AWS Transform funções vinculadas ao serviço

AWS Transform não oferece suporte ao uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Você pode usar a `AWSServiceRoleForAWSTransform` função nas seguintes regiões. Para obter mais informações, consulte [Regiões e endpoints da AWS](#).

Nome da região	Identidade da região	Support em AWS Transform
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Europa (Frankfurt)	eu-central-1	Sim

Usando funções vinculadas a serviços para AWS Transformar de forma personalizada

AWS O Transform Custom usa a função vinculada ao serviço chamada `AWSServiceRoleForAWSTransformCustom` para publicar métricas e registros em sua conta em seu nome. Essas métricas permitem monitorar contagens de transformação, latências e códigos de status diretamente em seus painéis. Os registros fornecem visibilidade dos problemas encontrados durante as transformações.

Essa [função vinculada ao serviço](#) é predefinida pelo AWS Transform Custom e inclui somente as permissões de que o serviço precisa. Você não precisa adicionar nenhuma permissão manualmente, e a função só pode ser assumida pelo AWS Transform Custom. Para obter informações gerais sobre funções vinculadas a serviços, consulte Como [usar funções vinculadas a serviços no Guia do usuário do IAM](#).

Service-linked permissões de função para AWS Transformar de forma personalizada

A função `AWSServiceRoleForAWSTransformCustom` vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `transform-custom.amazonaws.com`

A política de permissões de função chamada `AWSServiceRoleForAWSTransformCustom` permite que o AWS Transform Custom conclua as seguintes ações nos recursos especificados:

- `cloudwatch:PutMetricData` em todos os AWS recursos
 - Publique métricas operacionais abaixo do `AWS/TransformCustom` namespace
 - Acompanhe contagens de transformação, latências e códigos de status
 - Definido para o `AWS/TransformCustom` namespace por meio da chave de condição `cloudwatch:namespace`
- `logs:CreateLogGroup` `logs:PutRetentionPolicy` no grupo `/aws/TransformCustom` de registros
 - Crie o grupo CloudWatch de registros de registros para publicar registros de transformação
 - Defina políticas de retenção de registros no grupo de registros
 - Definido `arn:aws:logs:*:*:log-group:/aws/TransformCustom` com uma `aws:ResourceAccount` condição que garanta o acesso somente dentro da sua conta
- `logs:CreateLogStream` `logs:PutLogEvents` em fluxos de log dentro do grupo de `/aws/TransformCustom` registros

- Crie fluxos de log e publique eventos de log para operações de transformação
- Definido `arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*` com uma `aws:ResourceAccount` condição que garanta o acesso somente dentro da sua conta

Você deve configurar permissões para permitir que seus usuários, grupos ou perfis criem, editem ou excluam um perfil vinculado ao serviço. Para obter mais informações, consulte [as permissões de Service-linked função](#) no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para AWS Transformar de forma personalizada

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você executa uma transformação usando a CLI do AWS Transform Custom, o AWS Transform Custom cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você executa uma transformação usando a CLI do AWS Transform Custom, o AWS Transform Custom cria a função vinculada ao serviço para você novamente.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso `AWSServiceRoleForAWSTransformCustom`. Na AWS CLI ou na AWS API, crie uma função vinculada ao serviço com o nome `transform-custom.amazonaws.com` serviço. Para saber mais, consulte [Criar um perfil vinculado a serviço](#) no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editar uma função vinculada ao serviço para AWS Transformar de forma personalizada

AWS O Transform Custom não permite que você edite a função `AWSServiceRoleForAWSTransformCustom` vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para saber mais, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Transformar de forma personalizada

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não terá uma entidade não utilizada que não seja ativamente monitorada ou mantida.

A função `AWSServiceRoleForAWSTransformCustom` vinculada ao serviço não cria recursos persistentes em sua conta. Você pode excluí-lo diretamente sem qualquer limpeza de recursos.

Se você excluir essa função e depois executar uma transformação usando a CLI personalizada do AWS Transform, a função vinculada ao serviço será recriada automaticamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForAWSTransformCustom` vinculada ao serviço. Para saber mais, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Regiões suportadas para AWS Transforme funções personalizadas vinculadas a serviços

AWS O Transform Custom oferece suporte ao uso de funções vinculadas a serviços em todas as regiões em que o AWS Transform Custom está disponível. Para obter uma lista das regiões suportadas, consulte [Regiões suportadas](#).

AWS políticas gerenciadas para AWS Transformação

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as [políticas gerenciadas pelo cliente](#) que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para saber mais, consulte [AWS Políticas gerenciadas pela](#) no Guia do usuário do IAM.

AWS Transforme atualizações para AWS políticas gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do AWS Transform desde 1º de março de 2021.

Alteração	Descrição	Data
<u>AWSTransformInfrastructureExecutorAccessBatch</u> – Nova política	Foi adicionada uma nova política AWS gerenciada que concede as permissões necessárias para executar avaliações e AWS transformações da Modernização Contínua do Transform usando o AWS Batch, incluindo o upload do código-fonte, a recuperação de resultados, o monitoramento do status do trabalho em lote, a leitura de registros e o gerenciamento de cronogramas de transformação.	20 de julho de 2026
<u>AWSTransformInfrastructureExecutorAccessEC2</u> – Nova política	Foi adicionada uma nova política AWS gerenciada que concede as permissões necessárias para executar avaliações e AWS transformações da Modernização Contínua do Transform usando o Amazon EC2, incluindo o upload do código-fonte, a recuperação de resultados, o monitoramento do status do trabalho e o gerenciamento de cronogramas de transformação.	20 de julho de 2026
<u>AWSTransformSecurityAgentExecutorAccess</u> – Nova política	Foi adicionada uma nova política AWS gerenciada que concede à AWS Transform Continuous Modernization	30 de junho de 2026

Alteração	Descrição	Data
	as permissões necessárias para invocar o serviço AWS Security Agent para análises e correções automatizadas de segurança de código, incluindo o upload de artefatos de digitalização e a recuperação de descobertas.	
AWSServiceRoleForAWSTransformCustom : política atualizada	Foram adicionadas permissões de CloudWatch registros para permitir que o AWS Transform custom publique registros no grupo de registros em sua conta. /aws/TransformCustom	5 de maio de 2026
AWSTransformCustomExecuteTransformations : política atualizada	Foi adicionada permissão para criar a função vinculada ao serviço personalizado AWS Transform (AWSServiceRoleForAWSTransformCustom) para permitir a emissão de CloudWatch métricas para contas de clientes.	27 de abril de 2026

Alteração	Descrição	Data
<u>AWSTransformCustomManageTransformations:</u> política atualizada	Foi adicionada permissão para criar a função vinculada ao serviço personalizado AWS Transform (AWSServiceRoleForAWSTransformCustom) para permitir a emissão de CloudWatch métricas para contas de clientes.	27 de abril de 2026
<u>AWSTransformCustomFullAccess:</u> política atualizada	Foi adicionada permissão para criar a função vinculada ao serviço personalizado AWS Transform (AWSServiceRoleForAWSTransformCustom) para permitir a emissão de CloudWatch métricas para contas de clientes.	7 de abril de 2026
<u>AWSServiceRoleForAWSTransformCustom</u> – Nova política	Foi adicionada uma nova política AWS gerenciada para a função vinculada ao serviço personalizado AWS Transform . Essa política permite que o AWS Transform custom publique CloudWatch métricas em sua conta.	23 de março de 2026
<u>DBModProvisioningAndMigration</u> – Nova política	Essa política concede recursos de provisionamento e migração de banco de dados.	24 de março de 2026

Alteração	Descrição	Data
DBModDiscoveryAndAssessment – Nova política	Foi adicionada uma nova política AWS gerenciada que fornece recursos abrangentes de descoberta e avaliação da modernização do banco de dados.	24 de março de 2026
AWSTransformCustomFullAccess – Nova política	Foi adicionada uma nova política AWS gerenciada que fornece acesso total ao AWS Transform custom.	5 de dezembro de 2025
AWSTransformCustomExecuteTransformations – Nova política	Foi adicionada uma nova política AWS gerenciada que fornece acesso para executar transformações no AWS Transform custom.	5 de dezembro de 2025
AWSTransformCustomManageTransformations – Nova política	Foi adicionada uma nova política AWS gerenciada que fornece acesso para criar, atualizar, ler e excluir recursos de transformação no AWS Transform custom, bem como executar transformações.	5 de dezembro de 2025

Alteração	Descrição	Data
<u>AWSServiceRoleForAWSTransform</u> : política atualizada	Foram adicionadas permissões para acessar o segredo vinculado ao serviço AWS Transform usado para armazenar o segredo do cliente para provedores de identidade externos. Foram adicionadas permissões para criar um caso de suporte premium a partir do aplicativo web AWS Transform.	1 de dezembro de 2025
<u>AWSTransformApplicationECSDeploymentPolicy</u> : política atualizada	Foram adicionadas permissões de inspeção de função do IAM, criação de função vinculada ao serviço ECS e permissões KMS para suporte à criptografia ECR.	22 de novembro de 2025
<u>AWSTransformApplicationDeploymentPolicy</u> : política atualizada	Foram adicionadas permissões de rede EC2, permissões de inspeção de funções do IAM, permissões de listagem de buckets do S3 e suporte à criptografia KMS para recursos aprimorados de implantação.	22 de novembro de 2025
<u>AWSServiceRoleForAWSTransform</u> : política atualizada	Foi adicionado suporte para chaves gerenciadas pelo cliente no IAM Identity Center.	17 de setembro de 2025

Alteração	Descrição	Data
AWSTransformApplicationDeploymentPolicy – Nova política	Foi adicionada uma nova política AWS gerenciada que permite à AWS Transform implantar aplicativos.NET transformados criando e gerenciando instâncias, CloudFormation pilhas e recursos associados do Amazon EC2.	28 de agosto de 2025
AWSServiceRoleForAWSTransform : política atualizada	Nova política adicionada.	15 de maio de 2025

AWS política gerenciada: AWSServiceRoleForAWSTransform

Essa política é anexada à função [AWSServiceRoleForAWSTransform](#) vinculada ao serviço (SLR).

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte [AWSServiceRoleForAWSTransform](#) Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSServiceRoleForAWSTransformCustom

Essa política é anexada à função [AWSServiceRoleForAWSTransformCustom](#) vinculada ao serviço (SLR). Essa função permite que o AWS Transform custom publique CloudWatch métricas e registros em sua conta em seu nome.

Descrição

Esta política inclui as seguintes permissões:

- Amazon CloudWatch — Permite a publicação de métricas CloudWatch sob o AWS/TransformCustom namespace. Isso permite o monitoramento de contagens de transformação, latências e códigos de status em seus CloudWatch painéis.

- Amazon CloudWatch Logs — Permite criar grupos de registros, fluxos de registros, definir políticas de retenção e publicar eventos de `/aws/TransformCustom` log no grupo de registros. Isso fornece visibilidade dos problemas encontrados durante as transformações.

AWS política gerenciada: AWSTransformApplicationDeploymentPolicy

Essa política permite que a AWS Transform implante aplicativos.NET transformados criando e gerenciando instâncias, CloudFormation pilhas e recursos associados do Amazon EC2.

Descrição

Esta política inclui as seguintes permissões:

- CloudFormation— Permite criar, atualizar, excluir e descrever CloudFormation pilhas com nomes que começam com AWS Transform. As operações de pilha são restritas aos recursos marcados com `CreatedBy: AWSTansform` e limitadas à mesma conta. AWS
- Amazon EC2 — Permite descrever VPCs, sub-redes, grupos de segurança, imagens, instâncias, tabelas de rotas e gateways de internet. Permite executar, iniciar, interromper, encerrar e modificar instâncias do EC2, mas somente quando chamadas. CloudFormation A criação de tags é restrita a chaves de tag específicas permitidas e somente durante CloudFormation as operações.
- AWS Identity and Access Management (IAM) — Permite obter e transmitir funções específicas do IAM para instâncias de implantação do AWS Transform. Inclui permissões para inspecionar políticas e anexos de funções. O acesso é restrito à mesma AWS conta.
- Amazon EC2 Systems Manager (SSM) — Permite recuperar parâmetros do Amazon Linux AMI do armazenamento de AWS parâmetros gerenciado e enviar comandos para instâncias. `AWSTransform-tagged`
- Amazon S3 — Permite gerenciar objetos em buckets de implantação do AWS Transform, incluindo listar buckets e obter localizações de buckets na mesma conta. AWS
- AWS Key Management Service (KMS) — Permite operações de criptografia e descriptografia usando chaves KMS marcadas para o AWS Transform, com restrições ao uso dos serviços S3 e EC2.

A política implementa o acesso com privilégios mínimos por meio de permissões em nível de recurso, condições baseadas em tags, restrições de uso de controle de serviço, restrições em nível de conta e declarações explícitas de `aws:CalledVia` negação para evitar modificações não autorizadas de tags fora das operações. CloudFormation

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte

[AWSTransformApplicationDeploymentPolicy](#)o Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSTransformApplicationECSDeploymentPolicy

Essa política permite que a AWS Transform implante aplicativos transformados no Amazon ECS criando e gerenciando clusters, serviços, tarefas e recursos associados do ECS.

Descrição

Esta política inclui as seguintes permissões:

- CloudFormation— Permite criar, atualizar, excluir e descrever CloudFormation pilhas com nomes que começam com AWS Transform. As operações de pilha são restritas aos recursos marcados com CreatedBy: AWSTransform e limitadas à mesma conta. AWS
- Amazon ECS — Permite criar, atualizar e excluir clusters, serviços e definições de tarefas do ECS. Permite executar tarefas, listar tarefas e descrever o status da tarefa. Todas as operações são restritas a recursos com nomes começando com AWSTransform e marcados com CreatedBy: AWSTransform.
- AWS Identity and Access Management (IAM) — Permite obter e transmitir funções específicas do IAM para tarefas do ECS (AWSTransform-Deploy-ECS-Task-Role e AWSTransform-Deploy-ECS-Execution-Role). Inclui permissões para inspecionar políticas de função e criar a função vinculada ao serviço ECS quando necessário.
- Amazon CloudWatch Logs — Permite criar, excluir e gerenciar grupos de logs com nomes que começam com aws/ecs //AWSTransform. Permite recuperar eventos de log para solucionar problemas de aplicativos implantados.
- Amazon ECR — Permite criar repositórios de contêineres com nomes começando com awstransform para armazenar imagens de contêineres de aplicativos.
- AWS Key Management Service (KMS) — Permite criar concessões e gerar chaves de dados para criptografia ECR ao usar chaves KMS gerenciadas pelo cliente.

A política implementa o acesso com privilégios mínimos por meio de permissões em nível de recurso, condições baseadas em tags e restrições em nível de conta para garantir que as operações sejam limitadas aos recursos da mesma conta. AWSTransform-managed AWS

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte

[AWSTransformApplicationECSDeploymentPolicy](#)o Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSTransformCustomFullAccess

Essa política fornece acesso total ao AWS Transform custom.

Descrição

Esta política inclui as seguintes permissões:

- AWS Transformar Personalizado — Permite todas as ações em todos os recursos personalizados do AWS Transform. Isso fornece acesso administrativo completo ao serviço.
- AWS Identity and Access Management (IAM) — Permite criar a [função vinculada ao serviço](#) personalizada AWS Transform (`AWSServiceRoleForAWSTransformCustom`). Essa função é necessária para que o AWS Transform custom emita CloudWatch métricas e registros para sua conta. O escopo da permissão é permitir somente a criação dessa função específica vinculada ao serviço.

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte [AWSTransformCustomFullAccess](#)o Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSTransformCustomExecuteTransformations

Essa política fornece acesso para executar transformações no AWS Transform custom.

Descrição

Esta política inclui as seguintes permissões:

- AWS Transform Custom — Permite transmitir conversas, executar transformações e gerenciar campanhas. Inclui permissões para obter detalhes da campanha, atualizar o status do repositório da campanha e atualizar campanhas.
- AWS Identity and Access Management (IAM) — Permite criar a [função vinculada ao serviço](#) personalizada AWS Transform (`AWSServiceRoleForAWSTransformCustom`). Essa função é necessária para que o AWS Transform custom emita CloudWatch métricas e registros para sua conta. O escopo da permissão é permitir somente a criação dessa função específica vinculada ao serviço.

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte

[AWSTransformCustomExecuteTransformations](#)so Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSTransformCustomManageTransformations

Essa política fornece acesso para criar, atualizar, ler e excluir recursos de transformação no AWS Transform custom, bem como executar transformações.

Descrição

Esta política inclui as seguintes permissões:

- AWS Transform Custom — permite o gerenciamento abrangente dos recursos de transformação, incluindo streaming de conversas, execução de transformações e gerenciamento de pacotes de transformação. Permite criar, obter e excluir URLs de pacotes de transformação e concluir uploads de pacotes.
- Gerenciamento de conhecimento — permite listar, obter, excluir e atualizar itens de conhecimento e suas configurações e status.
- Gerenciamento de campanhas — Permite obter detalhes da campanha, atualizar o status do repositório da campanha e atualizar as campanhas.
- Marcação de recursos — Permite listar, adicionar e remover tags para recursos personalizados do AWS Transform.
- AWS Identity and Access Management (IAM) — Permite criar a [função vinculada ao serviço](#) personalizada AWS Transform (`AWSServiceRoleForAWSTransformCustom`). Essa função é necessária para que o AWS Transform custom emita CloudWatch métricas e registros para sua conta. O escopo da permissão é permitir somente a criação dessa função específica vinculada ao serviço.

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte

[AWSTransformCustomManageTransformations](#)so Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSTransformInfrastructureExecutorAccessBatch

Essa política concede as permissões necessárias para executar avaliações e AWS transformações da Modernização Contínua do Transform usando o Batch. AWS Anexe essa política a uma função do

IAM em sua conta. A CLI e o agente do AWS Transform Continuous Modernization assumem essa função para carregar o código-fonte, recuperar resultados, monitorar o status do trabalho em Batch, ler registros e gerenciar cronogramas de transformação.

Descrição

Esta política inclui as seguintes permissões:

- AWS Lambda — Permite invocar e recuperar a configuração de funções atx Lambda com prefixo que orquestram o fluxo de trabalho de transformação.
- Amazon S3 — Permite fazer upload do código-fonte em atx-source-code-* buckets e baixar resultados de transformação de e buckets. atx-custom-output-* atx-ct-output-*
- AWS Key Management Service (KMS) — Permite criptografia e descriptografia de dados usando a chave de criptografia AWS Transform (). alias/atx-encryption-key
- Amazon CloudWatch Logs — Permite a leitura de eventos de log de execução do Batch job e do Lambda para monitoramento e depuração da transformação.
- Amazon CloudWatch — Permite obter e listar o painel do AWS Transform CLI para visibilidade operacional.
- AWS Batch — Permite descrever e listar ambientes computacionais, filas de tarefas, definições de tarefas e status de tarefas.
- CloudFormation— Permite descrever e listar as pilhas de infraestrutura do AWS Transform para verificar o status da implantação.
- API de marcação de grupos de recursos — permite recuperar recursos marcados para descobrir a infraestrutura AWS Transform em sua conta.
- AWS Secrets Manager— Permite recuperar e descrever os segredos do AWS Transform armazenados sob o atx/ prefixo.
- Amazon EventBridge Scheduler — Permite gerenciar trabalhos de transformação programados dentro do grupo atx-ct de agendamentos.
- Amazon EC2 — Permite descrever a configuração de VPC, sub-rede, grupo de segurança, tabela de rotas e gateway NAT para redes de ambiente computacional Batch.
- AWS Identity and Access Management (IAM) — Permite ler configurações ATX de função com prefixo e Atx prefixo para validar a configuração da infraestrutura e passá-las para o AtxSchedulerInvocationRole Amazon EventBridge Scheduler para que ele possa invocar trabalhos agendados.

A política implementa o acesso com privilégios mínimos por meio de permissões em nível de recurso, condições baseadas em tags, `aws:ResourceAccount` condição e condições com escopo de serviço para garantir que as operações sejam limitadas aos recursos do Transform na `iam:PassedToService` mesma conta. AWS AWS

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte

[AWSTransformInfrastructureExecutorAccessBatcho](#) Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AWSTransformInfrastructureExecutorAccessEC2

Essa política concede as permissões necessárias para executar avaliações e AWS transformações da modernização contínua do Transform usando o Amazon EC2. Anexe essa política a uma função do IAM em sua conta. A CLI e o agente do AWS Transform Continuous Modernization assumem essa função para carregar o código-fonte, recuperar resultados, monitorar o status do trabalho e gerenciar os cronogramas de transformação.

Descrição

Esta política inclui as seguintes permissões:

- CloudFormation— Permite descrever as pilhas da infraestrutura, os eventos da pilha, os recursos da pilha e o status de detecção de desvios do AWS Transform, listando as pilhas e validando os modelos antes da implantação. CloudFormation
- Amazon EC2 — Permite descrever instâncias, AMIs, VPCs, sub-redes, grupos de segurança, pares de chaves, tabelas de rotas, gateways NAT e gateways de internet. Permite iniciar e interromper instâncias do EC2 marcadas com `atx-remote-infra: true`
- Amazon EC2 Systems Manager (SSM) — Permite monitorar o status de execução do comando e executar comandos e sessões AWS Transform-tagged em instâncias, incluindo a execução `AWS-RunShellScript` do documento.
- Amazon S3 — Permite gerenciar o código-fonte e os artefatos de saída nos buckets do AWS Transform, incluindo obter, colocar e excluir objetos e listar buckets.
- AWS Key Management Service (KMS) — Permite criptografia e descriptografia de dados usando a chave de criptografia AWS Transform (). `alias/atx-encryption-key`
- AWS Secrets Manager— Permite recuperar e descrever segredos de transformação, como credenciais do repositório, armazenados sob o prefixo. `atx/`

- Amazon EventBridge Scheduler — Permite gerenciar trabalhos de transformação programados dentro do grupo `atx-ct` de agendamentos.
- API de marcação de grupos de recursos — permite recuperar recursos marcados para descobrir a infraestrutura AWS Transform em sua conta.
- AWS Identity and Access Management (IAM) — Permite passar a `atx-transform-role*` função para o Amazon EC2 e o `AtxSchedulerInvocationRole` Amazon EventBridge Scheduler e ler a configuração da função e do perfil da instância para instâncias do EC2.

A política implementa o acesso com privilégios mínimos por meio de permissões em nível de recurso, condições baseadas em tags, `aws:ResourceAccount` condição e condições com escopo de serviço para garantir que as operações sejam limitadas aos recursos do Transform na `iam:PassedToService` mesma conta. AWS AWS

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte

[AWSTransformInfrastructureExecutorAccessEC2](#)o Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: `AWSTransformSecurityAgentExecutorAccess`

Essa política concede à AWS Transform Continuous Modernization as permissões necessárias para invocar o serviço AWS Security Agent para análises e correções automatizadas de segurança de código. Vincule essa política a uma função do IAM em sua conta que a CLI e o agente do AWS Transform Continuous Modernization presumem para carregar artefatos de digitalização e recuperar descobertas.

Descrição

Esta política inclui as seguintes permissões:

- AWS Security Agent — Permite listar espaços de agentes, criar análises de código, iniciar trabalhos de revisão de código, listar e recuperar descobertas e iniciar a correção de código. Essas ações têm como escopo os espaços do agente em sua conta.
- Amazon S3 — Permite baixar resultados e descobertas de escaneamento do `kct-security-agent-*` bucket e fazer upload do código-fonte para escaneamento de segurança para o `security-scans/*` prefixo dentro desse bucket.
- AWS Identity and Access Management (IAM) — Permite passar a `security-agent-*` função para o serviço AWS Security Agent para que ele possa realizar a verificação.

A política implementa o acesso com privilégios mínimos por meio de permissões em nível de recurso, bucket do S3 e prefixos de chave, `s3:ResourceAccount` condições e e uma `iam:PassedToService` condição com escopo de serviço para `aws:ResourceAccount` garantir que as operações sejam limitadas aos recursos do Security Agent na mesma conta. AWS AWS

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte

[AWSTransformSecurityAgentExecutorAccess](#)o Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: DBModDiscoveryAndAssessment

Essa política fornece recursos abrangentes de modernização de banco de dados, descoberta e avaliação para o AWS Transform.

Descrição

Esta política inclui as seguintes permissões:

- Amazon EC2 — Permite descrever componentes de infraestrutura, incluindo instâncias, VPCs, sub-redes, grupos de segurança, zonas de disponibilidade, VPC endpoints e gateways de internet.
- Amazon RDS — Permite descrever instâncias de banco de dados, clusters e grupos de sub-redes. Permite modificar grupos de sub-redes de banco de dados na mesma AWS conta para preparação da migração.
- API de dados do Amazon RDS — Permite ativar e desativar endpoints HTTP e executar instruções SQL em clusters de banco de dados marcados para o projeto de modernização do banco de dados.
- AWS DMS— Permite descrever endpoints, instâncias de replicação, tarefas, grupos de sub-redes e instâncias solicitáveis. Permite listar provedores de dados, perfis de instância e projetos de migração. Permite descrever estatísticas de tabelas, execuções de avaliação e operações do modelo de metadados. As operações detalhadas de descrição e metadados são restritas aos recursos marcados para o projeto de modernização do banco de dados.
- — Permite listar segredos para descobrir as credenciais do banco de dados.
- AWS Identity and Access Management (IAM) — Permite inspecionar funções AWS DMS de serviço específicas e suas políticas associadas. Inclui acesso a AWS DMS políticas AWS gerenciadas por leitura.
- AWS Key Management Service (KMS) — Permite listar aliases de chave e descrever chaves. Permite a decodificação de segredos por meio da integração, restrita à mesma conta. AWS

A política implementa o acesso com privilégios mínimos por meio de permissões em nível de recurso, condições baseadas em tags e restrições em nível de conta para garantir que as operações sejam limitadas aos recursos do projeto de modernização do banco de dados na mesma conta. AWS

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte [DBModDiscoveryAndAssessment](#)o Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: DBModProvisioningAndMigration

Essa política fornece recursos de provisionamento e migração de banco de dados para projetos de modernização do banco de dados AWS Transform. Ele inclui permissões para criar e gerenciar a infraestrutura de migração, provisionar bancos de dados de destino e armazenar dados de migração.

Descrição

Esta política inclui as seguintes permissões:

- AWS DMS— permite criar e gerenciar grupos de sub-redes de replicação, perfis de instância, provedores de dados, projetos de migração, endpoints, instâncias de replicação e tarefas de replicação. Inclui operações de conversão de esquema, como importação, conversão, exportação e avaliação de modelos de metadados. Permite o gerenciamento do ciclo de vida de instâncias de replicação (criar, excluir, modificar, reinicializar) e tarefas de replicação (excluir, iniciar, interromper, avaliar). Todas as operações de gravação são restritas aos recursos marcados para o projeto de modernização do banco de dados.
- Amazon RDS — Permite criar grupos de sub-redes de banco de dados, clusters de banco de dados e instâncias de banco de dados. Todos os recursos devem ser marcados para o projeto de modernização do banco de dados.
- — Permite criar, atualizar e marcar segredos com o prefixo de nomenclatura de modernização do banco de dados. Permite recuperar valores secretos e descrever segredos para recursos marcados.
- Amazon S3 — Permite criar e gerenciar buckets e objetos do S3 para armazenamento de dados de migração. Inclui marcação de bucket, controle de versão e operações de ciclo de vida de objetos. Restrito a buckets com o prefixo de nomenclatura de modernização do banco de dados.
- AWS Identity and Access Management (IAM) — Permite transmitir funções AWS DMS de serviço específicas AWS DMS e serviços de conversão de esquemas. Permite criar a função vinculada ao serviço Amazon RDS necessária para operações de banco de dados.

A política implementa o acesso com privilégios mínimos por meio de permissões em nível de recurso, condições baseadas em tags e restrições em nível de conta para garantir que as operações sejam limitadas aos recursos do projeto de modernização do banco de dados na mesma conta. AWS

Detalhes das permissões

Para ver os detalhes da permissão da política, consulte [DBModProvisioningAndMigration](#) no Guia de referência de políticas AWS gerenciadas.

AWS Referência de permissões de transformação

Esta seção fornece informações sobre as APIs usadas pelo AWS Transform e o que elas fazem.

Tópicos

- [AWS APIs de transformação](#)

AWS APIs de transformação

- transformar: BatchGetMessage
- transformar: BatchGetUserDetails
- transformar: CompleteArtifactUpload
- transformar: CreateArtifactDownloadUrl
- transformar: CreateArtifactUploadUrl
- transformar: CreateAssetDownloadUrl
- transformar: CreateConnector
- transformar: CreateFeedback
- transformar: CreateJob
- transformar: CreateSession
- transformar: CreateWorkspace
- transformar: DeleteConnector
- transformar: DeleteJob
- transformar: DeleteSelfRoleMappings
- transformar: DeleteUserRoleMappings

- transformar: DeleteWorkspace
- transformar: DetectIsAllowedForOperation
- transformar: GetConnector
- transformar: GetFeedbackQuestions
- transformar: GetHitITask
- transformar: GetJob
- transformar: GetLoginRedirectUri
- transformar: GetUserDetails
- transformar: GetUserPreferences
- transformar: GetWebAppUrl
- transformar: GetWorkspace
- transformar: ListArtifacts
- transformar: ListConnectors
- transformar: ListHitITasks
- transformar: ListJobPlanSteps
- transformar: ListJobs
- transformar: ListMessages
- transformar: ListPlanUpdates
- transformar: ListUserRoleMappings
- transformar: ListWorklogs
- transformar: ListWorkspaces
- transformar: PutUserPreferences
- transformar: PutUserRoleMappings
- transformar: RevokeSession
- transformar: SearchUsers
- transformar: SearchUsersTypeahead
- transformar: SendMessage
- transformar: StartJob

- transformar: StopJob
- transformar: SubmitCriticalHitITask
- transformar: SubmitStandardHitITask
- transformar: TestReleaseTraitPreProd
- transformar: TestReleaseTraitProd
- transformar: UpdateHitITask
- transformar: UpdateJob
- transformar: UpdateWorkspace
- transformar: VerifySession

Validação de conformidade AWS Transformação

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade](#) [Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#) .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a [Documentação AWS de segurança](#).

Resiliência em AWS Transformação

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

Além da infraestrutura AWS global, o AWS Transform oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

AWS Transform e endpoints de interface (AWS PrivateLink)

Você pode estabelecer uma conexão privada entre sua VPC e criar uma AWS Transform interface VPC endpoint. Os endpoints de interface são alimentados por [AWS PrivateLink](#) uma tecnologia que permite acessar o AWS Transform console de forma privada sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão. Direct Connect O tráfego entre sua VPC e AWS Transform não sai da rede Amazon.

Cada endpoint de interface é representado por uma ou mais [Interfaces de Rede Elástica](#) nas sub-redes.

Para obter mais informações, consulte [Endpoints da VPC da interface \(AWS PrivateLink\)](#) no Manual do Usuário do Amazon VPC.

Note

Para obter PrivateLink documentação AWS Transform personalizada, consulte [AWS Transform endpoints personalizados e de interface \(AWS PrivateLink\)](#).

Considerações para AWS Transform Endpoints da VPC

Antes de configurar uma interface para o VPC endpoint AWS Transform, certifique-se de revisar as [propriedades e limitações do endpoint da interface no](#) Guia do usuário do Amazon VPC.

Pré-requisitos

Antes de começar, verifique se você tem:

- Uma AWS conta com as permissões apropriadas para criar e configurar recursos.
- Uma VPC já criada em sua AWS conta.
- Familiaridade com AWS serviços, especialmente Amazon VPC e. AWS Transform

Criação de uma interface VPC endpoint para AWS Transform

Você pode criar um VPC endpoint para o AWS Transform serviço usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte [Criar um endpoint de interface](#) no Guia do usuário da Amazon VPC.

AWS Transform oferece suporte aos seguintes serviços de endpoint de VPC:

Nome do serviço	Endpoint	Observação
Ambiente de gerenciamento	<code>com.amazonaws.<i>region</i>.transform</code>	
API agente	<code>com.amazonaws.<i>region</i>.transform-agents</code>	
Aplicativo Web	<code>com.amazonaws.<i>region</i>.api.transform</code>	Necessário para o aplicativo o AWS Transform web. Esse endpoint deve ter o DNS privado ativado (a opção Habilitar nome DNS) para que seja <code>api.transform.<i>region</i>.on.aws</code> resolvido como um endereço IP privado em sua VPC.

region Substitua pela AWS região em que seu AWS Transform perfil está instalado, por exemplo, `com.amazonaws.us-east-1.transform`.

Note

Se você usa o aplicativo AWS Transform web, o `api.transform` endpoint é necessário. Para obter o guia de configuração completo, consulte [Acessando o AWS Transform aplicativo web a partir de uma VPC](#).

Para obter mais informações, consulte [Regiões suportadas para AWS Transform](#) [Acessar um serviço por meio de um endpoint de interface](#) no Guia do usuário da Amazon VPC.

Usando um computador local para se conectar a um AWS Transform endpoint

Esta seção descreve o processo de usar um computador local para se conectar AWS Transform por meio de um AWS PrivateLink endpoint em sua AWS VPC.

1. [Crie uma conexão VPN entre seu dispositivo on-premises e sua VPC.](#)
2. [Crie uma interface VPC endpoint para. AWS Transform](#)
3. [Configure um endpoint de entrada do Amazon Route 53.](#) Isso permitirá que você use o nome DNS do seu AWS Transform endpoint a partir do seu dispositivo local.

Acessando o AWS Transform aplicativo web a partir de uma VPC

Quando você usa AWS PrivateLink para acessar a AWS Transform API de forma privada a partir da sua VPC, o aplicativo web exige configuração de rede adicional. Ele fornece conteúdo estático (HTML JavaScript, CSS) CloudFront, o que requer conectividade com a Internet. As chamadas de API do aplicativo web passam pelo seu VPC endpoint e permanecem totalmente privadas.

Este guia mostra como configurar a saída controlada da Internet da sua VPC para que a aplicação web possa ser carregada e, ao mesmo tempo, manter sua VPC bloqueada somente nos domínios necessários.

Como funciona

O aplicativo AWS Transform web usa dois caminhos de rede:

- Chamadas de API — Quando você interage com o aplicativo web (iniciando trabalhos, visualizando espaços de trabalho etc.), o navegador envia solicitações de API para `api.transform.region.on.aws`. Com o `com.amazonaws.region.api.transform` VPC endpoint e o DNS privado habilitados, essas solicitações são resolvidas para um endereço IP privado em sua VPC e nunca saem da rede. AWS
- Conteúdo estático — Os arquivos HTML e CSS do aplicativo web são servidos por CloudFront meio de `tenant-id.transform.region.on.aws`. JavaScript O carregamento desses arquivos

requer conectividade com a Internet porque a entrega de CloudFront conteúdo só está disponível pela Internet pública.

- Autenticação — Uso de fluxos de login do AWS IAM Identity Center `region.signin.aws`, que também requer conectividade com a Internet.

Para habilitar o aplicativo web enquanto mantém a segurança, você cria um caminho de saída controlado usando o AWS Network Firewall com filtragem baseada em domínio. Isso permite que sua VPC alcance somente os domínios específicos exigidos pelo aplicativo web e bloqueie todos os outros tráfegos da Internet.

Arquitetura

O diagrama a seguir mostra o caminho de rede para o tráfego de aplicativos web:

```
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

O Firewall de Rede deve ver as duas direções do tráfego (roteamento simétrico) para realizar a inspeção TLS SNI. Você deve configurar uma rota de retorno na sub-rede do NAT Gateway que envie o tráfego destinado à sub-rede privada de volta pelo firewall. Sem isso, as regras de filtragem baseadas em domínio não funcionarão.

Pré-requisitos

Antes de começar, verifique se você tem:

- Uma AWS conta com permissões para criar recursos de VPC, Network Firewall e NAT Gateways.
- Uma VPC com uma sub-rede privada na qual suas instâncias ou cargas de trabalho são executadas.
- Um gateway de internet conectado à VPC (ou permissões para criar um).
- Um endpoint AWS Transform VPC com `.amazonaws.region.api.transform` com DNS privado habilitado. Esse é o endpoint usado pelo cliente do navegador de aplicativos web. Para obter instruções sobre a criação de endpoints, consulte [AWS Transform e endpoints de interface \(AWS PrivateLink\)](#).

Configurando a política de VPC endpoint

Se seu `.amazonaws.region.api.transform` VPC endpoint tiver uma política de endpoint personalizada, você deverá adicionar uma declaração que permita operações. AWS Transform Sem isso, o aplicativo web não conseguirá fazer chamadas de API por meio do endpoint.

Adicione a seguinte declaração à sua política de VPC endpoint.

`AWS_TRANSFORM_PROFILE_ARN` Substitua pelo ARN do seu perfil de AWS Transform serviço, que você pode encontrar no AWS Transform console na página Configurações.

```
{
  "Statement": [
    {
      "Sid": "AllowAWSTransform",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalArn": [
            "AWS_TRANSFORM_PROFILE_ARN"
          ]
        }
      }
    }
  ]
}
```

```
]
}
```

Note

Se seu VPC endpoint usa a política padrão (acesso total), nenhuma alteração é necessária e você pode pular esta etapa.

Configurando a saída controlada da Internet

Conclua as etapas a seguir para configurar o Firewall de Rede com filtragem baseada em domínio para o AWS Transform aplicativo web.

Etapa 1: criar a sub-rede do firewall

Crie uma pequena sub-rede /28 dedicada ao endpoint do Network Firewall. Essa sub-rede deve estar na mesma zona de disponibilidade da sua sub-rede privada.

```
aws ec2 create-subnet \  
  --vpc-id your-vpc-id \  
  --cidr-block firewall-subnet-cidr \  
  --availability-zone your-az \  
  --region region
```

Etapa 2: Criar uma sub-rede pública para o NAT Gateway

```
aws ec2 create-subnet \  
  --vpc-id your-vpc-id \  
  --cidr-block public-subnet-cidr \  
  --availability-zone your-az \  
  --region region
```

Etapa 3: Configurar a tabela de rotas de sub-rede pública

Crie uma tabela de rotas para a sub-rede pública que roteia o tráfego da Internet para o gateway da Internet.

```
# 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
```

Etapa 4: Criar o gateway NAT

```
# 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
```

Etapa 5: Criar o grupo de regras do Firewall de Rede

Crie um grupo de regras com estado que permita tráfego somente para os domínios exigidos pelo aplicativo AWS Transform web.

```
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 Substitua pela AWS região em que seu AWS Transform perfil está instalado (por exemplo, us-east-1). *directory-id* Substitua pelo ID do diretório do IAM Identity Center (por exemplo, d-1234567890). Você pode encontrar seu ID de diretório no console do IAM Identity Center.

A tabela a seguir explica os domínios permitidos.

Domínio	Finalidade
<code>.cloudfront.net</code>	CloudFront CDN — serve ativos estáticos de aplicativos web (CSSJavaScript, imagens)
<code>.transform. <i>region</i>.on.aws</code>	URL do locatário do aplicativo Web — o navegador carrega a página inicial desse domínio via CloudFront
<code><i>region</i>.signin.aws</code>	Página de redirecionamento de login com SSO
<code>.s3.<i>region</i>.amazonaws.com</code>	URLs pré-assinados do S3 — uploads e downloads de artefatos
<code>oidc.<i>region</i>.amazonaws.com</code>	Troca de tokens OIDC para autenticação SSO
<code>portal.sso. <i>region</i>.amazonaws.com</code>	Página de login do portal SSO
<code>assets.sso-portal. <i>region</i>.amazonaws.com</code>	Ativos estáticos do portal SSO (CSS, JavaScript)
<code><i>directory-id</i>.awsapps.com</code>	Portal do IAM Identity Center para sua organização

Note

O `.cloudfront.net` curinga permite tráfego para qualquer CloudFront distribuição, não apenas para a aplicação AWS Transform web. Um filtro de domínio mais estreito não é possível porque os IPs de CloudFront borda são compartilhados entre distribuições e a inspeção TLS SNI não consegue distinguir distribuições individuais por trás do mesmo domínio.

Note

As chamadas de API `api.transform.region.on.aws` devem ser AWS PrivateLink processadas e não exigem saída da Internet. Eles não são afetados pelo firewall.

Etapa 6: criar a política de firewall

A política deve usar a avaliação da STRICT_ORDER regra com drop_established como ação padrão. Isso garante que qualquer tráfego que não corresponda à lista de permissões seja descartado.

```
# 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
```

Etapa 7: Criar o Firewall de Rede

```
# 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
```

Etapa 8: Obter o ID do endpoint do firewall

```
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"
```

Etapa 9: Configurar a tabela de rotas de sub-rede do firewall

Roteie o tráfego vinculado à Internet da sub-rede do firewall para o NAT Gateway.

```
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
```

Etapa 10: Atualizar a tabela de rotas da sub-rede privada

Encaminhe todo o tráfego vinculado à Internet da sub-rede privada por meio do firewall.

```
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
```

Se já existir uma rota padrão, use `replace-route` em vez de `create-route`.

Etapa 11: Adicionar a rota de retorno simétrica (obrigatório)

Important

Essa etapa é fundamental. O Network Firewall usa a inspeção TLS SNI e deve ver as duas direções de uma conexão TCP. Adicione uma rota na tabela de rotas da sub-rede do NAT Gateway que envie o tráfego de retorno destinado à sub-rede privada de volta pelo firewall.

```
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 Substitua pelo bloco CIDR da sua sub-rede privada (por exemplo, `10.0.144.0/20`).

Sem roteamento simétrico, o firewall vê apenas uma direção do tráfego. O mecanismo de inspeção TLS não pode extrair a Indicação de Nome do Servidor (SNI) do handshake TLS, e todas as regras baseadas em domínio falharão silenciosamente.

Etapa 12: Remover a rota padrão IPv6 (se presente)

Se a tabela de rotas da sub-rede privada tiver uma rota padrão IPv6 (`:::/0`) apontando diretamente para um gateway da Internet, ela ignorará o firewall para os destinos. IPv6-capable Remova-o:

```
aws ec2 delete-route \  
  --route-table-id private-subnet-route-table-id \  
  --destination-ipv6-cidr-block :::/0 \  
  --region region
```

Verificação

Em uma instância na sub-rede privada, verifique a configuração:

```
# 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)
```

Solução de problemas

As chamadas de API para `api.transform` são bloqueadas pelo seu firewall

O domínio `api.transform.region.on.aws` deve ser resolvido para um endereço IP privado por meio do VPC endpoint e não deve acessar seu firewall da Internet.

- Verifique se você criou o `com.amazonaws.region.api.transform` endpoint.
- Verifique se o DNS privado está habilitado no endpoint:

```
aws ec2 describe-vpc-endpoints \
  --filters "Name=service-name,Values=com.amazonaws.region.api.transform" \
  --query 'VpcEndpoints[*].[State,PrivateDnsEnabled]' \
  --output table
```

Saída esperada: `available | True`

O aplicativo web não carrega (tempo limite de conexão)

- Verifique se a tabela de rotas da sub-rede privada tem uma `0.0.0.0/0` rota apontando para o endpoint do firewall.
- Verifique se a tabela de rotas de sub-rede do firewall tem uma `0.0.0.0/0` rota apontando para o NAT Gateway.
- Verifique se o NAT Gateway está em um `available` estado.

Non-allowlisted domínios não estão bloqueados

- Verifique se há uma `::/0` rota IPv6 apontando para o gateway da Internet. Isso ignora o firewall. Remova-o (Etapa 12).
- Verifique se o roteamento simétrico está configurado. A tabela de rotas de sub-rede do NAT Gateway deve ter uma rota de retorno pelo firewall para o CIDR da sub-rede privada (Etapa 11).
- Verifique se a política de firewall é usada `STRICT_ORDER` com `drop_established` e `alert_established` como ações padrão.

Considerações sobre custos

Recurso	Custo aproximado
Network Firewall	~\$0. 395/hr (~\$288/month) por zona de disponibilidade
NAT Gateway	~\$0. 045/hr (~\$33/month) + taxas de processamento de dados
IP elástico (IPv4 público)	~\$0. 005/hr (~\$3. 60/month)
Processamento de dados do Network Firewall	\$0. 065/GB
Processamento de dados do NAT Gateway	\$0. 045/GB

O custo base estimado é de aproximadamente \$ 325/month para uma única implantação de zona de disponibilidade. Para implantações de produção, implante o firewall, o NAT Gateway e as sub-redes associadas em cada zona de disponibilidade em que existam sub-redes privadas.

Limpeza

Para remover todos os recursos criados por este guia, execute os comandos a seguir na ordem inversa. Substitua os espaços reservados pelos IDs de recursos da sua implantação. Você pode encontrar esses valores no AWS Management Console ou usando os `describe` comandos das etapas de configuração.

```
# 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
```

Monitoramento AWS Transformação

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do AWS Transform e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar o AWS Transform, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. Você pode coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).
- O Amazon CloudWatch Logs permite que você monitore, armazene e acesse seus arquivos de log a partir de instâncias do Amazon EC2 e de outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch Logs](#).
- A Amazon EventBridge pode ser usada para automatizar seus AWS serviços e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Você pode escrever regras simples para determinar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o [Guia EventBridge do usuário da Amazon](#).
- AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

Registro em log AWS Transforme chamadas de API usando AWS CloudTrail

AWS O Transform é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no AWS Transform. CloudTrail captura todas as

chamadas de API para AWS Transform como eventos. As chamadas capturadas incluem chamadas do console do AWS Transform e chamadas de código para as operações da API AWS Transform. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para AWS o Transform. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à AWS Transform, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

AWS Transforme informações em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no AWS Transform, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do AWS Transform, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- [Visão geral da criação de uma trilha](#)
- [CloudTrail serviços e integrações suportados](#)
- [Configurando notificações do Amazon SNS para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#) e [Recebendo arquivos de CloudTrail log de várias contas](#)

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).

- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

Noções básicas AWS Transformar entradas do arquivo de log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Notificações

AWS O Transform fornece notificações por e-mail para mantê-lo informado sobre mudanças no acesso ao espaço de trabalho, atualizações do status do trabalho e solicitações pendentes de colaboradores.

Notificações por e-mail

As notificações por e-mail são ativadas por padrão e são enviadas aos usuários que têm permissões de somente leitura ou mais altas em um trabalho. Os usuários podem modificar suas preferências de notificação. Há três categorias de notificações por e-mail:

- Atualizações de acesso ao espaço de trabalho

Você recebe uma notificação quando é adicionado a um novo espaço de trabalho e quando sua função é alterada dentro de um espaço de trabalho.

- E-mails de resumo diário

Você recebe um e-mail de resumo diário às 9h, horário do Pacífico, resumindo seus trabalhos em andamento, caso tenha vagas ativas com uma ou mais solicitações de colaboração obrigatórias abertas. O e-mail inclui uma tabela mostrando o nome do espaço de trabalho, o nome do trabalho, o status do trabalho, os detalhes da solicitação do colaborador e as ações necessárias (limitado a 10 linhas)

 Note

Os e-mails de resumo diário são enviados somente para trabalhos que tenham exigido solicitações de colaboradores. Solicitações opcionais de colaboradores não acionam e-mails resumidos.

- Atualizações do status do trabalho

Você recebe um e-mail quando um trabalho ao qual você tem acesso é concluído ou falhado.

- Atualizações de solicitações de colaboradores

Você recebe um e-mail sempre que uma tarefa exige sua contribuição, revisão ou aprovação.

Gerenciando notificações por e-mail

Você pode modificar suas preferências de notificação por e-mail no aplicativo web clicando na engrenagem Configurações no canto superior direito do aplicativo e escolhendo Configurações de notificação.

A página de configurações de notificação fornece os seguintes controles:

Tipo de notificação	Description	Configuração padrão
Atualizações do Workspace Access	Receba e-mails quando adicionado a um espaço de trabalho ou quando sua função for alterada dentro de um espaço de trabalho	Habilitado
Resumo diário de solicitações de colaboradores	Receba um resumo diário das solicitações abertas de colaboradores para trabalhos em espaços de trabalho acessíveis	Habilitado
Atualizações de conclusão de trabalhos	Receba e-mails quando um trabalho for concluído ou falhar	Habilitado
Atualizações de solicitações de colaboradores	Receba e-mails quando uma entrada ou aprovação for exigida de você	Desabilitado

Você pode usar uma configuração geral para ativar ou desativar todas as notificações ou configurar tipos de notificação individuais separadamente.

Cotas para AWS Transformação

Sua AWS conta tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. Salvo indicação em contrário, cada cota é Region-specific. Você pode solicitar o aumento de algumas cotas, porém, algumas delas não podem ser aumentadas.

Para ver as cotas do AWS Transform, abra o console [Service Quotas](#). No painel de navegação, escolha AWS serviços e selecione AWS Transformar.

Para solicitar o aumento da cota, consulte [Solicitar um aumento de cota](#) no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível em Service Quotas, use [o formulário de aumento de limite](#).

Sua AWS conta tem as seguintes cotas relacionadas ao AWS Transform.

Workload	Dimensão	Quota	Ajustável	Description
Plataforma	Espaços de trabalho Região da AWS por conta AWS Transform habilitada	100 espaços de trabalho para cada um com suporte Região da AWS	Sim	O número máximo de espaços de trabalho por conta AWS Transform habilitada por Região da AWS
Migração da VMware	Contagem de servidores para cada onda	Cada onda: 150 servidores	Não	O número máximo de servidores em uma onda
Mainframe	Trabalhos simultâneos para cada conta do IAM Identity Center	10 empregos para cada região apoiada	Sim	Número máximo de trabalhos simultâneos no mainframe em uma conta do Centro de

Workload	Dimensão	Quota	Ajustável	Description
				Identidade do IAM
	Linhas de código para cada trabalho	3.000.000 de linhas de código para cada região suportada	Não	O número máximo de linhas de código para cada tarefa.
	Análise de linhas de código mensais	100.000.000 de linhas de código para cada região suportada	Sim	Número máximo de linhas de código para o objetivo de trabalho Analisar código em um mês civil
	Linhas de código mensais de geração de documentos comerciais	50.000.000 de linhas de código para cada região suportada	Sim	Número máximo de linhas de código para o objetivo de trabalho Geração de documentos comerciais em um mês civil
	Geração de documentos técnicos: linhas de código mensais	50.000.000 de linhas de código para cada região suportada	Sim	Número máximo de linhas de código para o objetivo do trabalho Geração de documentos técnicos em um mês civil

Workload	Dimensão	Quota	Ajustável	Description
	Transformação de linhas de código	10.000.000 de linhas de código para cada região suportada	Sim	O número máximo de linhas de código transformadas em um mês civil
	Decomposição de linhas mensais de código	50.000.000 de linhas de código para cada região suportada	Sim	Número máximo de linhas de código para o objetivo de trabalho Decomposição em um mês civil
	Reforje linhas de código mensais	50.000.000 de linhas de código para cada região suportada	Sim	Número máximo de linhas de código para o objetivo de trabalho Reforje em um mês civil
	Linhas de código mensais de lógica de negócios extraídas	50.000.000 de linhas de código para cada região suportada	Sim	O número máximo de linhas de código para o objetivo do trabalho Extracted Business Logic em um mês civil

Workload	Dimensão	Quota	Ajustável	Description
.NET	Linhas de código mensais .NET (Web e IDE)	1.000.000 de linhas de código para cada região suportada	Sim	O máximo de linhas do código do aplicativo .NET que podem ser transformadas em um mês civil em cada conta compatível com Região da AWS o IAM Identity Center
	Trabalhos simultâneos.NET com a extensão Microsoft Visual Studio para cada conta do IAM Identity Center	10 empregos para cada região apoiada	Sim	O número máximo de trabalhos simultâneos de transformação do.NET em cada conta compatível com Região da AWS o IAM Identity Center ao usar a extensão do Microsoft Visual Studio.

Workload	Dimensão	Quota	Ajustável	Description
	Trabalhos simultâneos na web.NET para cada conta do IAM Identity Center	5 empregos para cada região apoiada	Sim	O número máximo de trabalhos simultâneos de transformação do.NET em cada conta compatível com Região da AWS o IAM Identity Center ao usar o aplicativo web AWS Transform.
Transformações personalizadas	Definições de transformação personalizadas	1.000	Sim	O número máximo de definições de transformação personalizadas
	Tamanho de definição de transformação personalizada	10 MB	Não	O tamanho total máximo de todos os arquivos incluídos na definição de transformação, incluindo referências de documentos.

Workload	Dimensão	Quota	Ajustável	Description
	Solicitações mensais de conversação CLI de transformação personalizada	1.000.000	Sim	O número máximo de solicitações de conversação de transformação personalizadas feitas na CLI permitidas em um mês civil
Avaliação	Limite de contagem de servidores para cada avaliação	Cada avaliação: 30.000 servidores	Não	O número máximo de servidores em um único trabalho de avaliação

Regiões suportadas para AWS Transform

Note

Se você fizer uma solicitação que exija AWS Transform a recuperação de informações de uma região opcional não listada nesta página, AWS Transform poderá fazer chamadas para essa região. Para gerenciar o acesso às regiões para as quais AWS Transform posso fazer chamadas, consulte [Segurança em AWS Transformação](#).

Este tópico descreve Regiões da AWS onde você pode usar AWS Transform. Para obter mais informações sobre Regiões da AWS, consulte [Especificar qual Regiões da AWS conta pode ser usada](#) no Guia de AWS Gerenciamento de contas referência.

Seus dados podem ser processados em uma região diferente da região em que você usa AWS Transform. Para obter informações sobre o processamento entre regiões em AWS Transform, consulte [Cross-region processamento](#). Para obter informações sobre onde os dados são armazenados durante o processamento, consulte [Proteção de dados](#).

Compatível Regiões da AWS (ativado por padrão)

Você pode criar AWS Transform espaços de trabalho da seguinte Regiões da AWS forma. Essas regiões são ativadas por padrão. Você não precisa habilitá-las antes de usá-las. Para obter mais informações, consulte [Regions that are enabled by default](#).

- Leste dos EUA (Norte da Virgínia)
- Europa (Frankfurt)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)
- Europa (Londres)
- Ásia-Pacífico (Seul)
- Canadá (Central)
- América do Sul (São Paulo) - Somente agentes de modernização de mainframe

O espaço de trabalho no qual você cria um trabalho determina o Região da AWS do trabalho. Para criar um trabalho em uma região diferente, você deve usar um espaço de trabalho diferente que esteja na região desejada.

Para projetos da VMware, a região do espaço de trabalho é usada para descoberta. No entanto, você pode especificar uma região diferente como destino da migração. Essa região de destino é onde suas cargas de trabalho são hospedadas quando a migração é concluída. Para obter mais informações sobre Região da AWS considerações sobre migrações da VMware, incluindo a lista de possíveis regiões de destino, consulte [the section called “Regiões-alvo suportadas”](#)

AWS suporte para AWS Transform

AWS Transform permite que você crie e gerencie casos de AWS Support por meio do chat se você encontrar problemas durante seus trabalhos de transformação. Seus casos são automaticamente enriquecidos com o contexto do trabalho e encaminhados para a equipe de suporte apropriada. Se você for um cliente ativo do Countdown Premium, seu engenheiro designado entrará em contato para gerenciar a resolução do problema. Saiba mais em [AWS Countdown Premium](#). Caso contrário, seu caso será investigado pela equipe de AWS Transform suporte na fila de suporte.

Pré-requisitos

Antes de usar o gerenciamento de casos de suporte, você precisa:

- Um plano de AWS Support ativo — Business On-Ramp, Enterprise ou Enterprise
- Um AWS Transform aplicativo existente

Habilitando o Support Case Management

1. Abra o AWS Transform console.
2. No painel de navegação, selecione Configurações.
3. Em Support, escolha Enable Support case management.
4. Escolha Salvar alterações.

AWS Transform usa uma função vinculada ao serviço (SLR) para criar e gerenciar casos de suporte em seu nome. Nenhuma permissão adicional do IAM é necessária.

Criando um Support Case

Para criar um caso de suporte, use a interface de bate-papo:

1. Peça para criar um caso de suporte. Por exemplo:
 - “Crie um caso de suporte para meu trabalho de transformação fracassado”
 - “Preciso de ajuda com erros de trabalho, crie um caso”
2. O chat solicita que você forneça as informações necessárias:

- Uma breve descrição do seu problema
 - Uma descrição detalhada
3. Confirme a criação do caso quando solicitado.

O caso é preenchido automaticamente com o contexto do seu trabalho de transformação, incluindo:

- ID e status do Job
- Metadados do trabalho
- Registros de execução de trabalhos (registros de trabalho)
- Plano de trabalho

O caso é atribuído automaticamente com base no seu tipo de trabalho e categoria de problema.

Exibindo Support Cases

Para ver seus casos de suporte, ative o chat:

- “Listar meus casos de suporte”
- “Mostre-me casos de suporte abertos”
- “Qual é a situação dos meus casos?”

O bate-papo exibirá:

- ID do caso
- Sujeito
- Status, como Aberto, Pendente, Resolvido ou Fechado
- Data da última atualização
- ID do trabalho associado

Para ver detalhes de um caso específico:

- “Mostre-me detalhes do caso [case-id]”
- “Qual é a atualização mais recente sobre o caso [case-id]?”

Adicionando comunicações a um caso

Para adicionar uma mensagem a um caso existente:

1. Pergunte ao chat: “Adicionar uma mensagem ao caso [case-id]”
2. Forneça sua mensagem quando solicitado.
3. O bate-papo confirmará que a mensagem foi adicionada.

Você receberá notificações quando o AWS Support responder ao seu caso.

Resolvendo um caso

Para resolver um caso de suporte:

1. Pergunte no chat: “Resolver caso [case-id]”
2. Confirme a resolução quando solicitado.

Note

Você só pode resolver casos que tenham sido tratados pelo AWS Support.

Desativando o Support Case Management

1. Abra o AWS Transform console.
2. No painel de navegação, selecione Configurações.
3. Em Support, escolha Disable Support case management.
4. Escolha Salvar alterações.

Note

A desativação do gerenciamento de casos do Support remove a interface de gerenciamento de casos baseada em bate-papo, mas não fecha os casos existentes. Você ainda pode acessar seus casos por meio do AWS Support Center.

Telemetria de uso

O plug-in AWS Transform IDE, o AWS Transform Agent Skill e o AWS Transform Kiro Power coletam telemetria de uso por padrão durante a execução da transformação. A telemetria consiste em pontos de dados diferentes, como o nome do IDE (por exemplo, VS Code ou Kiro), o nome do agente de IA (por exemplo, Claude Code ou OpenAI Codex) e o modo de execução (local ou remoto). Esses dados são usados pelo AWS Transform para priorizar os testes de compatibilidade, bem como a latência e a confiabilidade.

Para desativar a telemetria, informe ao agente durante sua sessão de bate-papo que você não quer que a telemetria seja emitida. Essa desativação se aplica somente à sessão de bate-papo atual e deve ser repetida para cada nova sessão. Se você estiver executando a CLI do AWS Transform diretamente, defina a variável de `ATX_DISABLE_TELEMETRY=true` ambiente.

Dados operacionais

Podemos coletar sinais operacionais sobre seu uso do AWS Transform, como quais recursos você usa, registros de erros e métricas com base em seu feedback em linguagem natural (como se você aprovou a continuidade de um plano de transformação ou forneceu instruções para iterar um plano proposto) para fornecer o serviço e avaliar o desempenho do serviço.

Log de alterações

A tabela a seguir descreve os lançamentos e atualizações notáveis do AWS Transform.

Data	Título	Description	Links
2026-07-16	AWS O Transform for Migrations adiciona um relatório resumido do espaço de trabalho disponível para download	AWS O Transform for Migrations agora permite gerar um relatório resumido do espaço de trabalho como um PDF para download. O relatório consolida dados de todos os trabalhos de migração em seu espaço de trabalho, incluindo status do trabalho, progresso das etapas do fluxo de trabalho, planejamento de ondas, migração de rede, configuração da landing zone, progresso da rehostagem e artefatos produzidos.	Baixando um relatório resumido do espaço de trabalho
2026-07-03	AWS A ferramenta de descoberta Transform adiciona suporte ao Oracle Database	A ferramenta de descoberta AWS Transform agora coleta metadados detalhados da Oracle diretamente de seus bancos de dados em	Descoberta do banco de dados Oracle

Data	Título	Description	Links
		servidores VMware e bare Hyper-V metal. Você pode descobrir instâncias Oracle por meio de conexões SQL diretas. A ferramenta coleta a enumeração do Container Database/Pluggable Database (CDB/PDB), o inventário de componentes e o dimensionamento do arquivo de dados. Ele também captura sinalizadores de topologia para Real Application Clusters (RAC), Data Guard e arquitetura multilocatária. Se você não configurou as credenciais do banco de dados, a ferramenta volta à OS-level detecção. Todas as versões do Oracle são suportadas.	

Data	Título	Description	Links
2026-06-22	Suporte regional da América do Sul (São Paulo) para agentes de modernização de mainframe	AWS O Transform para agentes de modernização de mainframe agora está disponível na região da América do Sul (São Paulo) (sa-east-1). Foi adicionado sa-east-1 às regiões suportadas e às tabelas de inferência entre regiões.	Regiões suportadas, Cross-region inferência
2026-06-22	AWS O Transform for VMware migration s oferece suporte à localização	AWS O Transform for VMware migration s agora oferece suporte à localização. Você pode alterar o idioma de exibição do aplicativo web ao trabalhar com fluxos de trabalho de migração da VMware escolhendo o ícone Configurações e selecionando seu idioma preferido.	Configurações de localização

Data	Título	Description	Links
2026-06-18	AWS O Transform for Migrations suporta todas as regiões AWS comerciais como alvos de migração	AWS O Transform for VMware migration s suporta todas as regiões AWS comerciais como alvos de migração, exceto Oriente Médio (Bahrein) e Oriente Médio (Emirados Árabes Unidos). Uma região alvo de migração é a AWS região em que os recursos migrados são implantados, incluindo zonas de aterrissagem, infraestrutura de rede e rehostedagem de servidores.	Regiões-alvo de migração suportadas

Data	Título	Description	Links
2026-06-18	AWS O Transform for Migrations permite que você anexe ENIs existentes ao seu modelo de lançamento	AWS O Transform permite que você anexe interfaces de rede elásticas (ENIs) existentes ao seu modelo de lançamento para sua migração. AWS O Transform exibe todos os ENIs existentes encontrados em sua conta de destino, e você pode marcá-los para que estejam disponíveis para uso por meio da configuração de execução quando as instâncias forem iniciadas.	Marcação de recursos ENI para migração
2026-06-18	AWS O Transform for Migrations permite que você defina as configurações de replicação e inicialização.	AWS O Transform permite que você defina suas configurações de replicação e de inicialização para sua migração. Você pode definir a configuração de acordo com sua conta de destino ou em servidores de origem específicos.	Configurações de replicação e inicialização

Data	Título	Description	Links
2026-06-17	Model-to-model avaliação de migração para cargas de trabalho generativas de IA	AWS O Transform agora oferece uma transformação personalizada de migração de modelo para modelo. A transformação avalia suas cargas de trabalho generativas de IA. Ela produz um plano de migração para migrar de fornecedores terceirizados para o Amazon Bedrock. O AI-powered agente escaneia sua base de código para identificar cada SDK e modelo de IA em uso. O agente reúne os requisitos de migração por meio de perguntas interativas. Em seguida, mapeia modelos para equivalentes do Amazon Bedrock com comparações transparentes de custos e alterações de código prontas para produção. Suporta migrações do OpenAI, do Google	O que há de novo, Transformações personalizadas

Data	Título	Description	Links
		Gemini, do uso direto do Anthropic SDK e de modelos de código aberto por meio do LiteLM ou do Ollama. Lida com integrações diretas de SDK e padrões agrupados em estrutura LangChain , incluindo LlamaIndex, CrewAI e camadas de roteamento de vários provedores. LangGraph Disponível sem custo adicional além do preço padrão do AWS Transform.	

Data	Título	Description	Links
2026-06-16	AWS O Transform for mainframe oferece um fluxo de trabalho rastreável e reimagina do	AWS O Transform for mainframe agora oferece uma experiência de reimaginação conectada e rastreável, desde a avaliação até a geração de código. As empresas que executam z/OS COBOL e PL/I cargas de trabalho podem avaliar seu portfólio para identificar funções comerciais distintas, extrair regras de negócios, gerar requisitos prontos para o desenvolvimento e produzir código nativo da nuvem rastreável em um único fluxo de trabalho conectado. Cada requisito remonta ao código-fonte para total auditabilidade.	O que há de novo: postagem, documentação

Data	Título	Description	Links
2026-06-16	AWS O Transform agora oferece suporte ao Amazon FSx for NetApp ONTAP como armazenamento de destino (prévia pública)	Agora você pode migrar cargas de trabalho de armazenamento em blocos para o Amazon FSx for NetApp ONTAP, além do Amazon EBS, como parte da nova hospedagem computacional. AWS O Transform replica dados de armazenamento em blocos diretamente nos volumes FSx for ONTAP dentro da mesma onda de migração que lida com computação e rede.	O que há de novo: postagem, documentação

Data	Título	Description	Links
2026-06-05	Suporte à avaliação de TCO do Amazon RDS for SQL Server	Agora você pode estimar os custos ao migrar bancos de dados SQL Server locais para o Amazon RDS for SQL Server. Use a avaliação de AI-powered TCO no AWS Transform para analisar seu ambiente e obter recomendações ideais de instância de banco de dados. A avaliação suporta as opções Bring Your Own Media (BYOM) e License Included (LI) com Database Savings Plans para uma economia de até 20%.	O que há de novo: postagem , documentação

Data	Título	Description	Links
2026-06-04	AWS Ferramenta de descoberta de transformação agora suportada como fonte de entrada de migração de rede	Agora você pode usar a ferramenta de descoberta AWS Transform como fonte para migração de rede junto com o ModelizeIT, permitindo migrações de rede híbrida para ambientes que executam cargas de trabalho VMware e não VMware.	Guia do usuário
2026-05-27	AWS A documentação personalizada do Transform adiciona exemplos de habilidades e melhores práticas do lado do cliente	A documentação de habilidades do lado do cliente agora inclui exemplos práticos de conformidade com o Dockerfile, segurança de migração de banco de dados, aplicação de políticas do Terraform e auxiliares de descontinuação de API, além das melhores práticas para criar e compartilhar habilidades.	Documentação

Data	Título	Description	Links
2026-05-22	Novos recursos de avaliação de migração de agentes agora disponíveis com AWS o Transform	AWS O Transform agora oferece recursos avançados de avaliação de migração, incluindo cenários hipotéticos, suposições personalizáveis, suporte flexível a formatos de arquivo e vários novos recursos de avaliação do custo total de propriedade (TCO).	O que há de novo: postagem , documentação
2026-05-20	AWS O Transform detecta VPCs existentes durante a análise da migração de rede	AWS O Transform agora detecta VPCs existentes em sua conta de destino durante a análise da migração da rede. Você pode ver as VPCs existentes junto com as VPCs mapeadas, identificar conflitos de CIDR e resolvê-los antes da implantação.	Documentação

Data	Título	Description	Links
2026-05-14	AWS Agentes de transformação agora disponíveis em Kiro, Claude, Cursor e Codex	AWS Os agentes de transformação agora podem ser acessados por meio de um Kiro power, de plug-ins de agente e do servidor AWS Transform MCP, permitindo que os desenvolvedores consumam recursos de transformação diretamente de seu ambiente de desenvolvimento preferido.	O que há de novo post
2026-05-14	AWS A Transform apresenta o kit de ferramentas do Agent Builder para criar agentes de transformação personalizados	Agora, parceiros e clientes podem criar, compartilhar e registrar agentes de transformação especializados usando o kit de ferramentas de criação de agentes Kiro power, integrand o ferramentas e fluxos de trabalho personalizados com o Transform. AWS	O que há de novo post

Data	Título	Description	Links
2026-05-14	AWS O Transform adiciona um assistent e de IA agente ao AWS Toolkit for Visual Studio	Agora, os desenvolvedores.NET podem modernizar aplicativos por meio de uma experiência conversacional guiada passo a passo diretamente no Visual Studio, com o contexto completo preservado no IDE e no console web.	O que há de novo post
2026-05-14	AWS O Transform agora oferece suporte a lojas de artefatos de propriedade do cliente	Você pode configurar seu próprio bucket Amazon S3 e, opcionalmente, criptografar artefatos com sua própria chave AWS KMS, dando controle total sobre onde os artefatos de transformação são armazenados.	O que há de novo, postagem, guia do usuário

Data	Título	Description	Links
2026-05-14	AWS Transform adiciona recomendações de estratégia de migração (7Rs)	Com o AWS Transform, agora você pode analisar seu inventário descoberto e obter uma recomendação de estratégia de migração para cada servidor e aplicativo. As recomendações seguem as sete estratégias de migração (7Rs) padrão do setor. Cada recomendação inclui um serviço AWS alvo sugerido, uma pontuação de confiança e o raciocínio por trás disso. Você pode gerar um painel HTML interativo, PDF ou PowerPoint saída da Microsoft.	Recomendações 7Rs

Data	Título	Description	Links
2026-05-11	AWS O Transform adiciona capacidade e de containerização durante as migrações	AWS O Transform agora oferece suporte à replataforma de aplicativos em contêineres durante a migração, automatizando a geração de Dockerfile, a criação de imagens de contêineres com digitalização CVE e a implantação no Amazon ECS ou no Amazon EKS.	O que há de novo, postagem, guia do usuário
2026-05-01	AWS A Transform agora oferece agentes de migração de BI do Power BI e do Tableau para o Quick	Partner-built agentes da Wavicle Data Solutions convertem painéis do Power BI e do Tableau em ativos do Quick dentro do fluxo de trabalho Transform. AWS	O que há de novo post
2026-04-21	AWS O Transform custom agora está disponível em seis AWS regiões adicionais	AWS O Transform custom se expande para a Ásia-Pacífico, Canadá e Europa (Londres), atingindo um total de oito AWS regiões.	O que há de novo post

Data	Título	Description	Links
2026-04-15	AWS O Transform adiciona a criação de landing zone aos fluxos de trabalho de migração	Foi adicionada a criação de landing zone diretamente nos fluxos de trabalho de migração. AWS O Transform verifica uma base existente, recomenda estruturas de unidades organizacionais (OU) e contas-alvo e oferece implantação totalmente automatizada ou saída de infraestrutura como código (IaC) (CloudFormationformatos AWS CDK ou Landing Zone Accelerator (LZA)).	O que há de novo: postagem, documentação

Data	Título	Description	Links
2026-04-15	AWS O Transform adiciona diagramas e relatórios de planejamento de migração	Agora você pode gerar diagramas interativos e relatórios analíticos durante o planejamento da migração. Os tipos de diagramas incluem mapas de topologia de rede, gráficos de dependência de aplicativos, gráficos de Gantt de ondas e gráficos gerais. Os tipos de relatórios incluem avaliações de risco, recomendações de 7Rs e relatórios analíticos personalizados. As saídas estão disponíveis como arquivos HTML, PDF ou Microsoft PowerPoint (.pptx) interativos.	Diagramação e geração de relatórios

Data	Título	Description	Links
2026-04-14	AWS O Transform agora está disponível no Kiro e no VS Code	AWS As transformações personalizadas do Transform agora podem ser acessadas no Kiro e no VS Code, com o estado do trabalho compartilhado entre as superfícies de IDE, CLI e console web.	O que há de novo post
2026-04-10	AWS Transform adiciona DHCP com mapeamento de grupos de segurança para migração de rede	Foi adicionado suporte para DHCP com mapeamento de grupos de segurança durante a migração da rede. Se você tem cargas de trabalho de DHCP-enabled migração, agora você pode garantir que suas regras de segurança permaneçam válidas após a migração. Isso se aplica tanto à referência de grupos de segurança na VPC quanto às regras de saída entre VPCs e entre contas via Transit Gateway.	Documentação

Data	Título	Description	Links
2026-03-31	AWS Transform custom anuncia a disponibilidade geral da análise automatizada de base de código	A transformação abrangente da análise da base de código atinge a disponibilidade geral, gerando documentos de arquitetura, relatórios técnicos de débito e recomendações de modernização em qualquer idioma.	O que há de novo post
2026-03-31	AWS O Transform custom apresenta novas transformações gerenciadas para modernizar o código em grande escala	Foram adicionadas sete novas transformações gerenciadas, incluindo Node.js atualizações (disponibilidade geral), otimização de Java, migração do Log4j, atualizações do Angular e atualizações do Vue (acesso antecipado). Angular-to-React	O que há de novo post
2026-03-20	AWS O Transform adiciona APIs públicas para migração de rede	Foram adicionadas as APIs públicas para migração de rede, permitindo o acesso programático e de parceiros aos recursos de migração de rede.	API Reference

Data	Título	Description	Links
2026-01-14	AWS O Transform custom adiciona AWS PrivateLink suporte e se expande para a Europa (Frankfurt)	AWS O Transform custom agora oferece suporte ao acesso privado à VPC via AWS PrivateLink e está disponível na Europa (Frankfurt), além do Leste dos EUA (Norte da Virgínia).	O que há de novo post
23/12/25	AWS O Transform permite a conversão de rede para migrações de data centers híbridos	AWS O Transform for VMware converte automaticamente configurações de rede de data center híbrido (VLANs, intervalos de IP) em AWS VPCs, sub-redes e grupos de segurança sem mapeamento manual.	O que há de novo post
2025-12-01	AWS lança o AWS Transform custom para acelerar a modernização de toda a organização	AWS O Transform custom atinge a disponibilidade geral, permitindo que as organizações automatizem transformações de código repetíveis em grande escala por meio de um único comando de CLI.	O que há de novo post

Data	Título	Description	Links
2025-12-01	AWS O Transform adiciona novos recursos de IA agente para migrações corporativas da VMware	AWS O agente VMware da Transform agora pode descobrir ambientes locais, mapear dependências, gerar planos de onda de migração e migrar entre destinos HyperV, Nutanix, KVM e bare-metal.	O que há de novo post
2025-12-01	AWS A Transform lança um agente de IA para a modernização completa do Windows	Um novo agente Windows completo automatiza a transformação de aplicativos.NET e bancos de dados SQL Server para o Aurora PostgreSQL, implantando em contêineres no Amazon ECS ou no EC2 Linux.	O que há de novo post
2025-12-01	AWS O Transform expande os recursos de transformação do.NET e aprimora a experiência do desenvolvedor	AWS O Transform adiciona suporte a o.NET 10, ASP.NET Web Forms à portabilidade do Blazor e uma experiência de IDE interativa aprimorada por meio do AWS Toolkit for Visual Studio.	O que há de novo post

Data	Título	Description	Links
2025-12-01	AWS O Transform for mainframe oferece novos recursos de automação de testes	AWS O Transform for mainframe introduz a geração automatizada de planos de teste, scripts de coleta de dados de teste e automação de casos de teste para acelerar os testes de modernização do mainframe.	O que há de novo post
2025-12-01	AWS O Transform for mainframe agora oferece suporte à reimaginação de aplicativos	Novas análises de dados e atividades, além de recursos de extração de lógica de negócios, permitem a decomposição de aplicativos de mainframe legados em arquiteturas nativas da nuvem.	O que há de novo post
2025-11-13	AWS O Transform automatiza a configuração de rede do Landing Zone Accelerator	AWS O Transform for VMware gera automaticamente arquivos YAML de LZA-compatible rede, simplificando a configuração da infraestrutura de nuvem de várias contas a partir de ambientes VMware.	O que há de novo post

Data	Título	Description	Links
2025-07-16	AWS O Transform for mainframe apresenta recursos aprimorados de refatoração de código e lógica de negócios	AWS O Transform for mainframe adiciona a disponibilidade geral do reforge (reestruturação do código) e a extração expandida da lógica de negócios em nível de aplicativo para melhorar a qualidade do código.	O que há de novo post
2025-05-15	AWS O Transform for VMware agora está disponível ao público em geral	AWS O Transform for VMware, um serviço de IA agente que automatiza todo o ciclo de vida de modernização da VMware, desde a descoberta até a implantação, atinge a disponibilidade geral.	O que há de novo post
2025-05-15	AWS O Transform for mainframe agora está disponível ao público em geral	AWS O Transform for mainframe, o primeiro serviço de IA agente para modernizar z/OS aplicativos IBM em grande escala, alcança disponibilidade geral com novos recursos de análise, decomposição e gerenciamento de tarefas.	O que há de novo post

[Baixe esses dados.](#)

Histórico do documento para o AWS Guia do usuário do Transform

A tabela a seguir descreve o histórico do documento do Guia do Usuário do AWS Transform.

Alteração	Descrição	Data
Análise e remediação contínuas do portfólio de modernização	Foi adicionado um novo capítulo documentando o recurso de modernização contínua do AWS Transform (atx ctsubcomandos) para análise e correção automatizadas de código. Veja a modernização contínua .	3 de junho de 2026
Rede Brownfield: visibilidade de VPCs existentes	Foi adicionada a detecção de VPC existente durante a análise da migração da rede. AWS O Transform detecta automaticamente VPCs já implantadas em sua conta de destino e sinaliza conflitos de CIDR com suas VPCs mapeadas. Consulte VPCs existentes em sua conta de destino .	18 de maio de 2026
Formato de habilidades, habilidades do lado do cliente e registros de subagentes adicionados para o Transform custom AWS	As definições de transform ação agora usam o formato de habilidades (SKILL .mdcom frontmatter YAML e pasta opcional)references/ . Foram adicionadas habilidades do lado do cliente para ampliar o agente com recursos	11 de maio de 2026

adicionais e registros do subagente para melhorar a depuração. Requer a versão 2.0 ou posterior da CLI.

Consulte [Definições e Client-Side habilidades de transformação](#).

[Adicionada a containerização do código-fonte](#)

AWS O Transform agora pode containerizar seus aplicativos usando IA generativa. Forneça seu código-fonte a partir de repositórios Git ou uploads zip, e o AWS Transform o analisa, gera artefatos do Docker, publica imagens de contêineres no Amazon ECR, gera infraestrutura como código e implanta no Amazon Elastic Container Service ou no Amazon Elastic Kubernetes Service. Consulte [Containerização do código-fonte](#).

7 de maio de 2026

[Operações de otimização de rede adicionadas e recomendações guiadas](#)

Etapa 5 adicionada: revisar e otimizar a rede, com operações de VPC e sub-rede (excluir, excluir, mesclar, dividir, redimensionar, renomear, alterar endereço IP) e recomendações guiadas para padronização de nomenclatura, análise do escopo, dimensionamento correto da capacidade, análise de segurança e consolidação da VPC. Consulte [Analisar e otimizar a rede](#).

27 de abril de 2026

[AWS O Transform Custom está disponível em 6 novas regiões](#)

[Foi adicionado suporte para ca-central-1, eu-west-2, ap-northeast-1, ap-northeast-1, ap-northeast-2, ap-southeast-2 e ap-south-1 no Transform custom.AWS](#)

21 de abril de 2026

[Documentação atualizada de permissões do conector](#)

Foi adicionada uma análise detalhada das permissões para o Conta da AWS conector de destino, abrangendo as permissões do S3, MGN, Migration Hub, migração da carga de trabalho e provisionamento da infraestrutura da landing zone. Consulte [Connect target Conta da AWS s](#).

19 de abril de 2026

[Tipos de trabalho de migração da VMware atualizados](#)

Foram adicionados os tipos de trabalho de planejamento de descoberta e migração, zona de aterrissagem e zona de aterrissagem, rede e migração de servidor. Migração de rede renomeada somente para migração de rede e Planejamento de migração para criar plano de migração. Veja os [tipos de trabalho de migração da VMware](#).

19 de abril de 2026

[Destinos reestruturados do Connect Conta da AWS](#)

Reestruturou a configuração do conector em três etapas: seleção do tipo de migração, contrato MAP e configuração do conector, incluindo regiões de destino suportadas, funções da conta, orientação do administrador delegado e funções do IAM. Consulte [Connect target Conta da AWS](#).

19 de abril de 2026

[Foram adicionadas outras regiões-alvo somente para migração de servidores](#)

Documentou 14 regiões comerciais adicionais disponíveis para trabalhos de migração de servidores sem migração de rede, com exigência de lista de permissões até o terceiro trimestre de 2026. Consulte [Regiões de destino suportadas](#).

19 de abril de 2026

Foi adicionado o capítulo Migrar servidores	Foi adicionado um novo capítulo sobre servidores do Migrate , abordando todo o fluxo de trabalho de rehostagem, incluindo estrutura da conta, funções do IAM, configuração de administrador delegado, implantação, testes e transição do agente de replicação.	19 de abril de 2026
Adicionado o capítulo Build landing zone	Foi adicionado o novo capítulo Criar zona de pouso com detalhes das permissões do conector para o provisionamento da zona de pouso.	19 de abril de 2026
Mapeamento e referenciamento de grupos de segurança	Foram adicionadas estratégias de mapeamento de grupos de segurança (MAP, MAP_DHCP, SKIP) e documentação de referência de grupos de segurança à rede do Migrate.	13 de abril de 2026
Auto-conversion para tipos de arquivo de rede não suportados	Foi adicionado suporte para conversão automática de tipos de arquivo de configuração de rede não suportados na rede do Migrate .	6 de abril de 2026
Política de chaves KMS adicionada para migração de banco de dados	Foi adicionada a seção Criptografia para migração de banco de dados.	26 de março de 2026

Nova política AWS gerenciada documentada	DBModProvisioningAndMigration Seção adicionada.	24 de março de 2026
Nova política AWS gerenciada documentada	DBModDiscoveryAndAssessment Seção adicionada.	24 de março de 2026
Geração de diagramas de rede	Foi adicionada a geração opcional de diagramas de rede (formatos Mermaid e PNG) à rede do Migrate .	18 de março de 2026
Suporte a arquivos de configuração de firewall e SDN	Foi adicionado suporte para arquivos de configuração Palo Alto Networks, Fortinet FortiGate e Cisco ACI para migração de rede na rede Migrate .	11 de fevereiro de 2026
Marcação personalizada para recursos de rede	Foi adicionado suporte de marcação VPC-level personalizada e em nível de trabalho para migração de rede na rede do Migrate .	28 de janeiro de 2026
Documentação de suporte adicionada	Adicionado AWS suporte para a seção.	23 de dezembro de 2025
Novas políticas AWS gerenciadas documentadas	Adicionado AWSTransformCustomFullAccess , AWSTransformCustomExecuteTransformations , e AWSTransformCustomManageTransformations seções.	7 de dezembro de 2025
Migração da VMware	A seção de migração do VMware foi atualizada.	1 de dezembro de 2025

Política AWS gerenciada atualizada	A AWSServiceRoleForAWSTransform documentação foi atualizada para refletir as permissões adicionais.	1 de dezembro de 2025
Regiões compatíveis	O tópico Regiões suportadas foi atualizado.	1 de dezembro de 2025
Modernização do mainframe	A seção de modernização do mainframe foi atualizada.	1 de dezembro de 2025
Começando	Atualizou o tópico de introdução .	1 de dezembro de 2025
Full-stack Modernização do Windows	Foi adicionado o tópico de modernização Full-stack do Windows , que inclui a seção.NET atualizada e a nova seção de modernização do SQL Server .	1 de dezembro de 2025
Ferramenta de descoberta	Foi adicionada a seção de ferramentas Discovery .	1 de dezembro de 2025
Política AWS gerenciada atualizada	Atualizado AWSTransformApplicationECSEmploymentPolicy com permissões expandidas de inspeção de função do IAM, criação de função vinculada ao serviço ECS e permissões KMS para suporte à criptografia ECR.	22 de novembro de 2025

Política AWS gerenciada atualizada	Atualizado AWSTransformApplicationDeploymentPolicy com redes EC2 adicionais, inspeção de funções do IAM, gerenciamento de buckets do S3 e permissões de criptografia KMS.	22 de novembro de 2025
Colecionador Discovery	Foi adicionada a ferramenta de descoberta AWS Transform documentação.	31 de outubro de 2025
Diagrama da arquitetura de migração da VMware adicionado	Foi adicionado um diagrama da arquitetura de migração da VMware na rede do Migrate .	23 de outubro de 2025
Atualização dos resultados da migração da VMware	Informações atualizadas dos resultados da migração na rede do Migrate .	12 de outubro de 2025
Atualização dos resultados da migração da VMware	Informações atualizadas dos resultados da migração na rede do Migrate .	12 de outubro de 2025
Documentação do conector S3	Foi adicionada a documentação do conector S3 para o aplicativo web.NET.	8 de outubro de 2025
Novo tópico sobre conectores de usuário	Tópico adicionado sobre conectores de usuário .	21 de setembro de 2025
Política AWS gerenciada atualizada	Atualizou a AWSServiceRoleForAWSTransform documentação.	17 de setembro de 2025

Suporte para avaliação de armazenamento	Foi adicionado suporte a arquivos do NetApp Data Infrastructure Insights (DII) para avaliações de armazenamento .	2 de setembro de 2025
Atualização das regiões de destino	Foram adicionadas três regiões-alvo suportadas .	31 de agosto de 2025
Atualização da política gerenciada	Foram adicionadas permissões somente de leitura do IAM Identity Center para serem usadas por. AWSServiceRoleForAWSTransform	29 de agosto de 2025
Nova política AWS gerenciada documentada	AWSTransformApplicationDeploymentPolicy Seção adicionada.	28 de agosto de 2025
endpoints de interface	Tópico de endpoints de interface adicionado.	9 de julho de 2025
Lançamento inicial	Versão inicial do Guia do usuário do AWS Transform.	15 de maio de 2025

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.