



Guía del usuario de

AWS Transformar



AWS Transformar: Guía del usuario de

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

Las marcas registradas y la imagen comercial de Amazon no se pueden utilizar en ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es? AWS ¿Transformar?	1
Terminología	1
Introducción	4
Configuración	4
Antes de empezar	4
Inscríbase en una Cuenta de AWS	4
Cómo empezar con IAM-only el acceso	4
Uso de credenciales de IAM	5
Introducción al AWS Organizations	6
Introducción al AWS IAM Identity Center	7
Uso de proveedores de identidad de terceros	8
Incorporación	11
Con su propio bucket de S3	13
Habilitado AWS Transformar	22
Inicio rápido: ¿Lo estoy intentando AWS Transformar	23
Administración de usuarios	24
Adición de usuarios en el Centro de identidades de IAM	24
Añadir usuarios a AWS Transformar	25
Administrar los usuarios con IAM-only acceso	25
Entender los permisos de los colaboradores	26
AWS Transforme el entorno	29
Configuración de idioma	30
Inicie su proyecto	31
AWS Transforma el chat	32
Herramientas para desarrolladores	34
Kiro Power	34
Plugin de agente	34
Complemento IDE	35
Servidor MCP	35
Autenticación	36
Cree agentes personalizados para AWS Transformar	37
Evaluaciones de migración	38
Requisitos previos	38
Cómo funcionan las evaluaciones de migración	38

Cargar datos de inventario	39
Revisar los resultados del descubrimiento	40
Administrar el alcance del inventario	40
Configuración de escenarios de evaluación	40
Capacidades de evaluación	41
Tamaño correcto de Amazon EC2	41
Almacenamiento en Amazon EBS	41
Amazon FSx	42
Amazon RDS para SQL Server	42
Amazon EC2 SQL Server	43
On-premises precios	43
Sostenibilidad	43
Evaluación del valor empresarial	43
Costos de red	44
Costes de soporte	44
Informática para usuarios finales	44
Uso de evaluaciones basadas en el chat	44
Estimación aproximada con datos limitados	44
Añadir inventario a través del chat	45
Modificar los costos y agregar servicios	45
Comparación de escenarios	45
Creación de escenarios	45
Ejecutando comparaciones	46
What-if análisis	46
Generar entregables	46
Temas relacionados	47
Personalizada	48
¿Qué es? AWS ¿Transformar de forma personalizada?	48
Capacidades clave	48
Patrones de transformación	48
Cómo AWS Transforme obras personalizadas	51
Comprensión de conceptos clave de	52
Definiciones de transformación	52
Registro de transformaciones	53
Transformaciones preliminares frente a transformaciones publicadas	53
Referencias frente a lecciones	54

Comandos de compilación y validación	54
Aprendizaje continuo	55
Client-Side Habilidades	56
Introducción	56
Requisitos previos	56
Instalación de la AWS Transformar CLI	57
Configuración de la autenticación	58
Configuración AWS Region	60
Ejecutando su primera transformación	63
Comprender los resultados de la transformación	64
Crear una transformación personalizada	64
AWS Transformar la aplicación web (opcional)	65
Introducción a los comandos de transformación personalizados	66
Flujos de trabajo	67
Ejecutando transformaciones	67
Aprendizaje continuo	72
Configuración avanzada	73
Cree transformaciones personalizadas	87
Referencia de comandos	91
Comandos interactivos	91
Comandos de definición de transformaciones	92
Comandos de la lección	96
Etiquete los comandos	96
Comandos de actualización	97
Comandos MCP	97
AWS-Transformaciones gestionadas	97
Descripción general de	97
Disponible AWS-Transformaciones gestionadas	98
Personalización AWS-Transformaciones gestionadas	116
Casos de uso común	116
Actualizaciones de Lambda Runtime	116
Puntos de conexión de VPC (AWS PrivateLink)	118
Consideraciones para AWS Transform puntos finales de VPC personalizados	119
Requisitos previos	119
Creación de un punto final de VPC de interfaz para AWS Transform personalizado	119
Crear una política de puntos de conexión de VPC para AWS Transform personalizado	120

Utilizar un ordenador local para conectarse a un AWS Transform punto de conexión personalizado	120
Resolución de problemas	121
Registrar ubicaciones	121
Problemas comunes	122
Cómo obtener soporte	124
Problemas de acceso a S3	124
Historial de versiones de CLI	125
Modernización continua	136
¿Qué es? AWS ¿Transformar la modernización continua?	136
Capacidades clave	136
Tipos de análisis	137
Descripción de los conceptos clave	138
Orígenes	138
Repositorios	139
Análisis	139
Hallazgos	139
Remediaciones	139
Definiciones de transformación	139
Cómo AWS Transforme las obras de modernización continua	140
Opciones de computación	140
Configuración del agente de seguridad	142
Introducción	143
Requisitos previos	143
Inicio rápido	144
Trabajando con una modernización continua	144
Administración de fuentes	144
Descubrimiento y administración de repositorios	146
Ejecutando el análisis	146
Administración de resultados	147
Creando soluciones	148
AWS Transforma la aplicación web (opcional)	148
Herramientas para desarrolladores	149
Habilidades del agente	149
Referencia de la CLI	150
Resolución de problemas	152

Herramienta de descubrimiento	154
Flujo de trabajo	154
Configure la herramienta de descubrimiento	155
Requisitos previos	155
Implemente en VMware	157
Implemente en Hyper-V	159
Implemente en Linux	159
Configure la herramienta de detección	162
Permisos necesarios	176
vCenter de VMware	176
Hyper-V hosts (Windows)	176
Servidores Linux (SSH)	177
Servidores Windows (WinRM): métricas del sistema operativo	179
Servidores Windows (WinRM): colección SQL Server	180
Base de datos Oracle (SQL)	181
Recopilación de redes	182
Referencia rápida: permisos mínimos por caso de uso	183
Recopilación de datos	184
Calendario de recolección	184
Inventario descubierto	185
OS-related datos	191
Consideraciones de seguridad	210
Proteger la máquina virtual de la herramienta de descubrimiento	210
Asegurar las credenciales	211
Almacenamiento de credenciales	212
Uso de la Auto-Connect función con precaución	213
Seguridad de importación de CSV	214
Consideraciones sobre la revocación del acceso	215
Solucione los problemas de la herramienta de detección	215
Verificación de la conectividad de la herramienta de detección con vCenter	215
Solución de problemas de WinRM	217
Solución de problemas de Kerberos	218
Solución de problemas de bases de datos	222
Solución de problemas de SNMP	223
Errores de recopilación de redes	224
Errores de recopilación de métricas del sistema operativo	225

Problemas de acceso en el inventario descubierto	226
Solución de problemas de autenticación con clave SSH	226
Solución de problemas con el instalador	227
Mensajes de error comunes	228
Notas de la versión	229
Connectors	235
Trazabilidad de los usuarios para las operaciones de los agentes	235
Administrar los conectores	237
Migraciones (incluida VMware)	239
Capacidades y características clave	239
Arquitectura	239
Trabajos de migración	240
Obtener un espacio de trabajo	240
Tipos de trabajo	241
Crear e iniciar un trabajo	242
Descargar un informe resumido del espacio de trabajo	242
Limitaciones	243
Descubra los datos de origen	243
Crea un plan de migración	244
Flujo de trabajo	246
Recomendaciones de las 7R	248
Diagramas e informes	250
Connect target Cuenta de AWS s y regiones	251
Paso 1: Selección del tipo de migración	251
Paso 2: acuerdo MAP	251
Paso 3: Configuración del conector	252
Construye landing zone	258
Configuración del conector	258
Configuración básica	260
Diseño de cuentas de carga de trabajo	263
Formatos iAC	265
Proceso de aprobación de despliegues	266
Etiqueta: landing zone resources	267
Revertir los cambios	267
Recursos relacionados	268
Migre su red a AWS	268

Paso 1: mapeo de la red de origen	269
Paso 2: Archivos de configuración adicionales	270
Paso 3: Topologías de red	271
Paso 4: mapeo de grupos de seguridad	274
Paso 5: Revise y optimice su red	277
Paso 6: diagrama de red	281
Paso 7: Configurar el etiquetado de recursos	281
Paso 8: Implemente su red	283
Elimine los recursos de red desplegados	284
Extracción del archivo de configuración	284
Migrar servidores	286
Requisitos previos y configuración de los valores predeterminados de migración	287
Paso 1: Configurar la ola de migración	289
Paso 2: Validar y confirmar el inventario	293
Paso 3: Implementar agentes de replicación	294
Paso 4: Replicación de datos	301
Paso 5: Probar	303
Paso 5b: Marque las aplicaciones como listas para la transición	303
Paso 6: transición	303
Estados del ciclo de vida del servidor	304
Aprobaciones de implementación	305
Notas de la versión	306
Junio de 2026	306
Mayo de 2026	306
Abril de 2022	307
Marzo de 2026	307
Febrero de 2026	307
Enero de 2026	307
Diciembre de 2025	307
Octubre de 2025	308
Septiembre de 2025	308
Agosto de 2025	308
Mayo de 2025	308
Contenedorización del código fuente	310
Capacidades y características clave	310
Cómo funciona la contenedorización	311

Requisitos previos	311
Flujo de trabajo de contenedorización	312
Inicio de un trabajo de contenerización	312
Permisos	313
Política base	313
Política de redes	314
Política de almacenamiento	314
AWS KMS policy	314
Política de Amazon ECS	315
Política de Amazon EKS	315
Paso 1: Exención de responsabilidad de seguridad	316
Qué cubre el descargo de responsabilidad	316
Qué necesita	316
Paso 2: clona el código fuente	317
Opción 1: repositorios de Git	317
Opción 2: carga de archivos zip	318
Opcional: configure las dependencias privadas	318
Confirmar las preferencias de contenedorización	319
Paso 3: Contenerizar	319
¿Qué ocurre durante la contenedorización	319
Tipos de aplicaciones compatibles	320
Qué necesita	320
Paso 4: Revisa los artefactos	320
Revisar los cambios de los repositorios de Git	321
Revisar los cambios de las subidas en formato zip	321
¿Solicitando cambios?	321
Paso 5: Publica imágenes	321
¿Qué ocurre durante la publicación	321
Qué necesita	322
Paso 6: Generar laC	322
Amazon Elastic Kubernetes Service (Kubernetes)	323
Amazon Elastic Container Service (Terraform)	323
Validación y escaneo de seguridad automatizados	324
Generar laC sin imágenes publicadas	324
Qué necesita	324
Paso 7: Implementar una infraestructura de prueba	325

¿Qué ocurre durante la implementación de la prueba	325
Qué necesita	325
Iterando en la infraestructura	326
Recuperación de sesión	326
Paso 8: Limpiar la infraestructura de pruebas	326
Qué necesita	326
Paso 9: Implemente una infraestructura de transición	327
Qué necesita	327
Recuperación de sesiones	328
Modernización de la unidad central	329
Capacidades y características clave	329
High-level tutorial	330
Human in the Loop (HITL)	330
Tipos de archivos compatibles para la transformación de aplicaciones de mainframe	331
Regiones y cuotas compatibles para AWS Transforme el mainframe	332
El viaje de modernización	332
Fase 1: Evaluar	332
Fase 2: Movilizar	333
Fase 3: Migrar y modernizar	334
Fase 4: Operar, optimizar e innovar	336
Transformación del flujo de trabajo de las aplicaciones de mainframe	337
Requisito previo: preparar las entradas del proyecto en S3	337
Colección de artefactos fuente de mainframe	338
Sign-in y crear un trabajo	347
Seguimiento del progreso de la transformación	348
Configure un conector	348
Evalúe y reimagine el plan de trabajo	353
Reimagine el plan de trabajo	358
Plan de trabajo personalizado	359
Cree e implemente una aplicación modernizada	391
Requisitos previos	392
Paso 1: Recupere el código modernizado	392
Paso 2: Cree la aplicación modernizada	393
Paso 3: Configurar el entorno de prueba	394
Paso 4: Implemente la aplicación modernizada	395
Paso 5: Pruebe la aplicación modernizada	395

Ejemplo adicional	395
Full-stack Modernización de Windows	396
.NET	396
Experiencias	396
Capacidades y características clave	397
Versiones y tipos de proyectos compatibles	397
Limitaciones	398
Intervención humana	399
Más información	399
Aplicación web.NET	399
.NET IDEA.NET	416
Portar código de capa de interfaz de usuario	425
Informes de transformación	427
Prácticas recomendadas	429
Modernización de SQL Server	435
Regiones admitidas	435
Capacidades y características clave	435
Versiones y tipos de proyectos compatibles	437
Requisitos de SQL Server	441
Requisitos de solicitud	441
Requisitos de infraestructura	442
Requisitos de repositorio	443
Configuración de SQL Server	443
AWS Configuración de transformación	451
Cree un trabajo de modernización de SQL Server	452
Flujo de trabajo de modernización de SQL Server	459
Pruebe e implemente después de la transformación	491
Prácticas recomendadas y solución de problemas	494
Seguridad	500
Protección de datos	501
Cross-region procesamiento	502
Cifrado de datos	511
Mejora del servicio	521
Identity and Access Management	522
Público	523
Autenticación con identidades	523

Administración del acceso con políticas	525
Cómo AWS Transform funciona con IAM	526
Identity-based ejemplos de políticas	532
Resolución de problemas	542
Cómo utilizar roles vinculados a servicios	544
AWS políticas gestionadas	550
AWS Referencia de permisos de transformación	566
Validación de conformidad	568
Resiliencia	569
Puntos de conexión de VPC (AWS PrivateLink)	569
Consideraciones para AWS Transform Puntos de conexión de VPC	570
Requisitos previos	570
Creación de un punto final de VPC de interfaz para AWS Transform	570
Utilizar un ordenador local para conectarse a un AWS Transform punto de conexión	571
Acceso a VPC a aplicaciones web	571
Funcionamiento	572
Arquitectura	572
Requisitos previos	573
Configuración de la política de puntos finales de la VPC	573
Configurar la salida controlada de Internet	574
Verificación	582
Resolución de problemas	582
Consideraciones sobre costos	583
Limpieza	584
Supervisión	586
CloudTrail registros	587
AWS Transforma la información en CloudTrail	587
Descripción AWS Transforma las entradas del archivo de registro	588
Notificaciones	588
Notificaciones por correo electrónico	588
Cuotas	591
Regiones admitidas	597
compatible Regiones de AWS (activado de forma predeterminada)	597
Soporte	599
Requisitos previos	599
Habilitación de Support Case Management	599

Creación de un caso de soporte	599
Visualización de casos de soporte	600
Añadir comunicaciones a un caso	601
Resolver un caso	601
Desactivación de Support Case Management	601
Telemetría de uso	602
Datos operativos	603
Registro de cambios	604
Historial de revisión	631
.....	dcxl

¿Qué es? AWS ¿Transformar?

AWS Transform es un servicio que le ayuda a acelerar y simplificar la transformación de la infraestructura, las aplicaciones y el código con una experiencia de inteligencia artificial propia de los agentes. Proporciona herramientas especializadas para agilizar los esfuerzos de modernización y migración en diversas cargas de trabajo.

Con AWS Transform, puede:

- Modernice y migre IBM z/OS y Fujitsu GS21 a AWS
- Migre las cargas de trabajo de VMware a Amazon EC2
- Modernice las aplicaciones.NET para convertirlas en aplicaciones.NET multiplataforma Linux-ready
- Evalúe las cargas de trabajo para determinar si están preparadas para

AWS Transform le ayuda a delegar las tareas de transformación complejas y laboriosas de las fases de descubrimiento, planificación y ejecución en manos de agentes de IA con experiencia en lenguajes, marcos e infraestructuras. Este enfoque permite a sus equipos centrarse en la innovación y, al mismo tiempo, transformar de manera eficiente proyectos complejos y a gran escala mediante una experiencia web unificada.

El uso de AWS Transform no conlleva ningún coste adicional.

Terminología

En esta sección, las cursivas indican un término oficial dentro de la definición de un término diferente.

Conexión de cuentas

En este contexto, la cuenta es una referencia generalizada a un contenedor propiedad del cliente o a un límite de seguridad para los recursos AWS o el servicio remoto, por ejemplo, una cuenta Cuenta de AWS o GitHub .

Artefacto

Un producto final producido por AWS Transform.

Administrador

Los administradores pueden leer y mutar todo el contenido del espacio de trabajo. Pueden iniciar conversaciones con AWS Transform, iniciar y detener trabajos y upload/download artefactos. Los

administradores pueden interactuar con las tareas en ejecución para realizar acciones informales (HITL) y pueden aprobar acciones fundamentales de HITL, como la fusión con la principal, la descomposición de gráficos o la implementación de código en entornos de producción. [Los administradores pueden cambiar los espacios de trabajo, los conectores y los usuarios.](#)

¿Agente

Un servicio para tareas específicas que ejecuta un tipo de transformación específico. Por ejemplo, las migraciones a VMware.

Aprobador

Los aprobadores tienen permisos similares a los de los administradores, con la salvedad de que no tienen permisos para cambiar los espacios de trabajo, los conectores o los usuarios. [Los aprobadores no pueden mutar los espacios de trabajo, los conectores o los usuarios.](#)

Activo

Insumos para un [trabajo](#) de transformación. Por ejemplo, el código fuente, el servidor, la base de datos o la red del cliente. Se accede a los activos a través de un [conector](#).

Solicitud de colaborador

Una tarea en la que AWS Transform pide a un humano que haga algo.

Conector

Los conectores son proveedores de activos que permiten el acceso a los recursos propiedad del cliente en un sistema externo a AWS Transform.

Al configurar un conector, el administrador de la cuenta a la que se está conectando debe aceptar la conexión. Para aceptar la conexión, deben tener los permisos establecidos en [la política de aceptadores de conectores](#).

Las dos cuentas siguientes deben ser idénticas o pertenecer a la misma AWS Organizations organización:

- La cuenta desde la que el administrador de AWS Transform habilita el servicio.
- La cuenta que recibirá la transformación. A esta cuenta se le debe asignar una función de IAM que le permita usar un [conector](#).

Colaborador

Los colaboradores pueden leer todo lo que hay en el espacio de trabajo. Pueden iniciar conversaciones con AWS Transform, iniciar y detener trabajos, cargar o descargar artefactos e

interactuar con los [trabajos](#) en ejecución para realizar acciones de HITL. Sin embargo, no pueden realizar acciones críticas de HITL, como fusionarlos con los archivos principales, realizar la descomposición de gráficos o implementar código en entornos de producción. [Los colaboradores tampoco pueden mutar los espacios de trabajo, los conectores o los usuarios.](#)

Objetivo

Un estado final definido por el usuario que AWS Transform trabaja para alcanzar. Los usuarios escriben esto y, a continuación, AWS Transform convierte el objetivo en una serie de tareas que realiza junto con los usuarios cuando es necesario.

Job

Un proceso de larga duración (weeks/months+) en el que trabaja AWS Transform para cumplir un [objetivo](#) definido por un usuario. Compuesto por múltiples [tareas](#) y solicitudes de [colaboradores](#).

Planifica

Una lista de [las tareas](#) que AWS Transform lleva a cabo (con la ayuda de usuarios humanos) en pos de un [objetivo](#).

Lector

Los lectores pueden ver el estado y los resultados de las tareas de AWS Transform, pero no pueden realizar ningún cambio. Pueden leer todo lo que hay en el [espacio de trabajo](#), descargar artefactos, ver los [trabajos](#) y ver las acciones de una persona al tanto (HITL). Sin embargo, los lectores no pueden realizar acciones de mutación en Transform. AWS

Tarea

Unidad de trabajo individual que forma parte de un [trabajo](#).

Registro de trabajo

Un registro de las acciones que AWS Transform y los usuarios han realizado como parte de un [trabajo](#).

Espacio de trabajo

Un recurso de AWS transformación que contiene otros recursos, como [conectores](#) y [trabajos](#). Un [espacio de trabajo](#) sirve como límite de permisos.

Introducción al AWS Transformar

Temas

- [Configuración AWS Transformar](#)
- [Habilitado AWS Transformar](#)
- [Inicio rápido: ¿Lo estoy intentando AWS Transformar](#)
- [Administrar usuarios](#)
- [AWS Transforma el entorno](#)

Configuración AWS Transformar

Antes de empezar

Antes de configurar AWS Transform, asegúrate de tener una AWS cuenta con acceso de administrador

Note

Si quieres probar AWS Transform como prueba de concepto o para entornos de prueba, consulta [Quick Start: Trying Transform. AWS](#)

Inscríbese en una Cuenta de AWS

Para empezar AWS, necesitas un Cuenta de AWS. Para obtener información sobre cómo crear un Cuenta de AWS, consulte [Cómo empezar con un Cuenta de AWS](#) en la Guía de AWS Account Management referencia.

Cómo empezar con IAM-only el acceso

Con el IAM-only acceso, los usuarios se autentican con sus AWS credenciales existentes.

Para configurar el IAM-only acceso:

1. En la AWS consola, dirígete a AWS Transformar y selecciona Comenzar.
2. Complete la configuración de los ajustes de la cuenta.

3. En Acceso de usuario, selecciona IAM-only acceso.
4. Selecciona Activar para crear tu perfil.

Los usuarios inician sesión en la aplicación web AWS Transform mediante [AWS Sign-In](#). Su identificador de usuario en la aplicación web se basa en su principal IAM.

 Important

No puede añadir un proveedor de identidad una vez finalizada la configuración. Para administrar los usuarios con el Centro de identidades de IAM o con un proveedor de identidad existente, elija una de estas opciones durante la configuración inicial.

Con el IAM-only acceso, cualquier director de IAM con el `transform:AccessTransformProfile` permiso correspondiente al recurso de perfil puede acceder a AWS Transform. El acceso de los usuarios se gestiona mediante las políticas de IAM y no mediante la asignación de usuarios a los proveedores de identidad.

La `transform:AccessTransformProfile` acción solo otorga acceso a AWS Transform. Una vez dentro de AWS Transform, los roles del espacio de trabajo controlan las acciones que puede realizar un usuario. Estos roles incluyen administrador, colaborador, aprobador y Read-only. Los roles del espacio de trabajo se aplican independientemente de cómo se haya autenticado el usuario.

Uso de credenciales de IAM

Manejo de la información del usuario

Cuando los directores de IAM acceden a AWS Transform, el servicio gestiona la identidad del usuario de forma diferente que con el acceso basado en el proveedor de identidad.

Identidad de usuario

[Los usuarios de IAM se identifican por su director de IAM.](#)

Identidad dual

Un usuario que tiene una identidad de proveedor de identidad (como el IAM Identity Center) y una sesión de IAM aparece como dos usuarios independientes en AWS Transform. Su trabajo no está vinculado entre las dos identidades.

Notificaciones por correo electrónico

Las notificaciones por correo electrónico solo están habilitadas para los usuarios de SSO. Los directores de IAM aún se pueden añadir a los espacios de trabajo, pero no recibirán notificaciones por correo electrónico.

Auditoría

Las llamadas a la API de IAM se registran AWS CloudTrail con la identidad de IAM de la persona que llama. Las acciones realizadas por los usuarios de IAM en un trabajo también se pueden rastrear en los registros de trabajo de Transform. AWS

Habilitar el acceso a IAM junto con un proveedor de identidad

Si configuras AWS Transform con IAM Identity Center o con un proveedor de identidad externo, también puedes habilitar el acceso a IAM como una forma adicional de autenticarte. Esto permite a los directores de IAM acceder a AWS Transform junto con los usuarios actuales del proveedor de identidad.

El acceso a IAM está habilitado de forma predeterminada al crear un perfil en el IAM Identity Center o en un proveedor de identidad externo. Para activar o desactivar el acceso a IAM en cualquier momento:

1. En la consola AWS Transform, vaya a Configuración.
2. En Acceder a AWS Transform con credenciales de IAM, activa o desactiva la opción Habilitar el acceso a IAM.

Cuando el acceso a IAM está habilitado, tanto los usuarios proveedores de identidad como los directores de IAM pueden usar Transform. AWS Los usuarios de IAM y los usuarios de proveedores de identidad pueden colaborar en el mismo espacio de trabajo.

Introducción al AWS Organizations

Siga estos pasos para configurar AWS Transform:

1. Inicie sesión en su AWS cuenta de administración de Organizations.
2. Navegue hasta el servicio AWS Transform.
3. Elija Habilitar el servicio para que su organización utilice AWS Transform.

4. Configure los permisos necesarios para las cuentas de los miembros de la organización.
5. Acceda a la experiencia web de AWS Transform desde sus cuentas de miembros.

Note

Para usar Landing Zone Accelerator (LZA) en una AWS solución para crear tu zona de aterrizaje junto con las capacidades de AWS Transform for Migration, tu cuenta de AWS Transform y la instalación de LZA deben estar en la misma organización. AWS No se admite el uso de ID de organización independientes para las implementaciones de LZA y AWS Transform, ya que esto puede provocar inconsistencias en la administración de la organización y las implementaciones de recursos. Para obtener información sobre cómo configurar su instalación de LZA mediante Organizations, consulte [Implemente una base en la nube para soportar cargas de trabajo altamente reguladas y requisitos de cumplimiento complejos](#) en la guía del usuario de Landing Zone Accelerator on AWS Implementation Guide.

Introducción al AWS IAM Identity Center

Siga estos pasos para utilizar IAM Identity Center for AWS Transform y añadir usuarios y grupos.

De forma predeterminada, ningún usuario tiene acceso a AWS Transform cuando lo habilitas por primera vez.

Note

El centro de identidad de IAM no se limita a la región en la que está configurado. Si ya ha configurado el Centro de identidad de IAM en una región que AWS Transform no admite, puede usarlo para AWS Transform.

1. Configure el Centro de identidad de IAM siguiendo las instrucciones de [Para habilitar una instancia del Centro de identidades de IAM](#).

Configure el Centro de identidades de IAM para que utilice un proveedor de identidad empresarial externo y replique la información de sus usuarios y grupos en el Centro de identidades de IAM.

2. En la AWS consola, seleccione AWS Transformar y elija Comenzar.
3. Elija Habilitar el servicio para que su organización utilice AWS Transform.
4. Seleccione una clave de cifrado. La selección predeterminada es una clave AWS gestionada. Para usar una clave personalizada:
 - a. En Clave de cifrado, selecciona Personalizar la configuración de cifrado.
 - b. Selecciona Usar una clave AWS KMS.
 - c. Elige una clave existente o crea una nueva.
 - d. Selecciona Enviar para aplicar los cambios y, a continuación, selecciona Activar la AWS transformación.

Seleccione Ver perfil para ver la configuración. Los usuarios utilizan la URL de la aplicación web para acceder a la experiencia web unificada de AWS Transform.

5. Seleccione Usuarios en el panel de navegación y seleccione Asignar usuarios o grupos.
6. Busque el nombre del usuario o los grupos que desea autorizar a usar AWS Transform. La búsqueda hace referencia a los usuarios y grupos propagados desde su proveedor de identidad.
7. Seleccione un grupo o un usuario, seleccione Listo y, a continuación, Asignar. Estos usuarios están autorizados a utilizar la interfaz web unificada de AWS Transform.

Uso de proveedores de identidad de terceros

AWS Transform admite la integración con proveedores de identidad de terceros (IdPs), como Azure Active Directory (Entra ID) y Okta Workforce Identity. Esto le permite usar su sistema de administración de identidades existente para la autenticación de usuarios.

Requisitos previos

Antes de configurar la integración de un proveedor de identidad externo, asegúrese de que los usuarios de su proveedor de identidad tengan configurados los atributos de nombre, correo electrónico y nombre de usuario

Información almacenada

Cuando utiliza AWS Transform with IdPs, AWS almacena una cantidad mínima de información de usuario cifrada y protegida:

Información de usuario almacenada

AWS Transform almacena la información básica del perfil de usuario al iniciar sesión por primera vez, como el nombre para mostrar, la dirección de correo electrónico, el nombre de usuario (`preferred_username`) y un identificador de usuario único. Esta información se cifra mediante una clave KMS propiedad del cliente o una clave propiedad del servicio, según la configuración del perfil de Transform del cliente. AWS Los datos se almacenan en la base de datos de autenticación de AWS Transform y solo se recopilan durante la sesión de inicio de sesión inicial. Esto rellena los resultados de la búsqueda al invitar a otros usuarios a un espacio de trabajo.

Ciclo de vida de

La información de los usuarios se almacena solo para los usuarios que han iniciado sesión en la aplicación web AWS Transform al menos una vez y puede quedar obsoleta si los usuarios actualizan su información en su proveedor de identidad sin volver a iniciar sesión en AWS Transform. Toda la información de usuario almacenada se elimina cuando se elimina el perfil de AWS Transform.

Almacenamiento de secretos del cliente

El secreto de cliente proporcionado durante la configuración se almacena AWS Secrets Manager mediante un secreto vinculado a un servicio (SLS) en su cuenta.

Manejo de identificadores de usuario

Entra

Utiliza la afirmación «oid» (identificador de objeto) como identificador de usuario único, que es inmutable e identifica de forma exclusiva a los usuarios en todo el inquilino de Microsoft. Los clientes pueden ver este valor en la consola de Entra y aparece en CloudTrail los registros.

Identidad de la fuerza laboral de Okta

Utiliza diferentes afirmaciones para identificar al usuario según el tipo de token: la afirmación «secundaria» en los tokens de ID y la afirmación «uid» en los tokens de acceso. AWS Transform valida que ambas notificaciones contengan el mismo valor durante la autenticación. Los clientes pueden ver este valor en la consola de Okta y aparece en CloudTrail los registros.

Configuración de Azure Active Directory (Entra ID)

Para configurar la integración de Azure Active Directory con AWS Transform:

1. Vaya al portal de Azure y seleccione Azure Active Directory.
2. En el panel de navegación izquierdo, elija Administrar > Registros de aplicaciones.
3. Seleccione + Nuevo registro.
4. Introduzca el nombre de la aplicación, elija el tipo de cuenta compatible, deje en blanco el URI de redireccionamiento y seleccione Registrar.
5. En el menú de navegación de la izquierda, seleccione Administrar > Manifiesto.
6. Actualice `requestedAccessTokenVersion` desde `null` a `2` y seleccione Guardar.
7. Seleccione Administrar > Exponer una API y seleccione Añadir un ámbito.
8. Cree un URI de ID de aplicación con la estructura predeterminada `api://<client-id>`.
9. Añada el ámbito `transform:read_write`.
10. Seleccione Añadir un certificado o secreto y cree un nuevo secreto de cliente. Guarde este valor, ya que es necesario para la creación del perfil.
11. Busque la URL del emisor seleccionando Endpoints y seleccionando el documento de metadatos de OpenID Connect. El campo «emisor» de los metadatos es la URL del emisor.
12. Cree un perfil en la consola AWS Transform con el ID de cliente, el secreto del cliente y la URL del emisor.
13. Tras crear el perfil, añada un URI de redireccionamiento. Para ello, seleccione Añadir una plataforma, seleccione Web e introduzca `<web-application-url>/login/callback`.

Configuración de Okta Workforce Identity

Para configurar la integración de Okta Workforce Identity con AWS Transform:

1. Navegue hasta la consola de Okta Workforce Identity.
2. Elija Aplicaciones > Aplicaciones y seleccione Crear integración de aplicaciones.
3. Seleccione OIDC - OpenID Connect and Web Application y, a continuación, elija Siguiente.
4. Asigne un nombre a su solicitud, deje el tipo de concesión como código de autorización, deje en blanco los URI de redireccionamiento, configure las asignaciones de usuarios y seleccione Guardar.
5. Vaya a la pestaña Iniciar sesión y configure el emisor como URL de Okta en lugar de como dinámico.
6. Copie el ID de cliente y configúrelo como la audiencia de su servidor de autorización. Para ello, vaya a Seguridad > API y añada un servidor de autorización.

7. En el servidor de autorización, añada el ámbito `transform:read_write` en la pestaña Ámbitos.
8. Agregue una política de acceso que permita a la aplicación OIDC utilizar este servidor de autorización y configurar una regla para la política.
9. En la página de configuración del servidor de autorización, anote la URL del emisor para la creación del perfil en Transform. AWS
10. Cree un perfil en AWS Transform utilizando la URL del emisor, el ID de cliente y el secreto del cliente desde la configuración de la aplicación.
11. Después de crear el perfil, `<web-application-url>/login/callback` agréguelo como URL de redireccionamiento en la pestaña General de la aplicación.

Note

Si quieres que te redirijan de nuevo a la aplicación web AWS Transform después de cerrar sesión, tendrás que configurar la URL de la aplicación web como un origen de confianza en Seguridad > API.

Incorporación de usuarios

En esta sección se describe la experiencia de los usuarios a los que se les ha concedido acceso a AWS Transform.

¿Aceptar la invitación

Cuando se agrega un usuario a AWS Transform, recibe una invitación por correo electrónico que contiene:

- Un saludo e información sobre la invitación
- La URL de la aplicación web AWS Transform
- Su nombre de usuario
- Un enlace para aceptar la invitación y configurar su contraseña

Para configurar su cuenta:

1. El usuario hace clic en el enlace «Aceptar la invitación» del correo electrónico.

2. En la página «Registro de nuevo usuario», introduce y confirma una contraseña.
3. La contraseña debe cumplir con los requisitos de seguridad, que incluyen:
 - Al menos 8 caracteres
 - Al menos una letra mayúscula
 - Al menos una letra minúscula
 - Al menos un número
 - Al menos un carácter especial
4. Tras crear una contraseña, ven una confirmación de que su cuenta se ha creado correctamente.

Iniciar sesión en AWS Transformar

Para iniciar sesión en AWS Transform:

1. Navega hasta la URL de la aplicación web AWS Transform que aparece en el correo electrónico de invitación.
2. Introduzca el nombre de usuario.
3. Elija Siguiente.
4. Introduzca la contraseña.
5. Seleccione Iniciar sesión.

Experiencia de bienvenida

Al iniciar sesión por primera vez, los usuarios ven la página de bienvenida de AWS Transform con:

- Un saludo personalizado
- Capacidades de transformación disponibles
- Opción para crear un espacio de trabajo

La página de bienvenida proporciona información sobre las capacidades de transformación disponibles en AWS Transform, que incluyen:

- Modernice las z/OS migraciones de IBM a AWS
- Migre las cargas de trabajo de VMware a Amazon EC2
- Modernice las aplicaciones.NET a una versión multiplataforma de .NET Linux-ready

- Evalúe las cargas de trabajo para determinar si están preparadas para

Los usuarios pueden empezar por crear un espacio de trabajo o pedir a su equipo que lo añada a un espacio de trabajo existente.

Uso de su propio bucket de Amazon S3

De forma predeterminada, AWS Transform usa un bucket de Amazon S3 administrado por un servicio para almacenar los artefactos de transformación. En su lugar, puede optar por utilizar su propio bucket de Amazon S3 para tener un mayor control sobre el almacenamiento de datos, el cifrado y las políticas de acceso.

Note

Si tiene un bucket de Amazon S3 para transformaciones de mainframe, puede seguir utilizando ese conector S3 y no necesita usar esta funcionalidad.

Note

Su bucket de Amazon S3 almacena solo las cargas y los artefactos de transformación con los que interactúa. Los artefactos internos generados por el sistema no se almacenan en su depósito. Además, AWS Transform indexa los artefactos de su depósito. Almacena los datos indexados en una base de conocimientos gestionada por el servicio que se utiliza para proporcionarle una experiencia de chat enriquecida.

Requisitos previos

Antes de configurar su propio bucket de Amazon S3, asegúrese de que se cumplen los siguientes requisitos:

- El bucket debe estar en la misma AWS región en la que está habilitada la AWS transformación.
- La política de bucket requerida debe aplicarse a tu bucket. Para obtener más información, consulte [the section called “Política de bucket obligatoria”](#).
- Si usa la aplicación web AWS Transform, CORS debe estar configurado en su bucket. Para obtener más información, consulte [the section called “Configuración CORS requerida”](#).

- Si usa una clave AWS KMS personalizada, debe aplicarse la política de claves requerida. Para obtener más información, consulte [the section called “Política de claves de KMS \(opcional\)”](#).

Configuraciones de cifrado compatibles

Su depósito debe usar una de las siguientes configuraciones de cifrado:

- SSE-S3 (AES256): deje el campo de clave KMS vacío. AWS Transform escribe objetos sin especificar un encabezado de cifrado y Amazon S3 aplica el cifrado predeterminado del bucket con S3-managed claves. Para obtener más información, consulte [Uso del cifrado del lado del servidor con claves administradas de Amazon S3 \(SSE-S3\)](#) en la Guía del usuario de Amazon S3.
- SSE-KMS con una clave de KMS administrada por el cliente: proporcione el ARN de la clave de KMS. AWS Transform escribe objetos `x-amz-server-side-encryption: aws:kms` con la clave proporcionada. Realice un seguimiento de [the section called “Política de claves de KMS \(opcional\)”](#).

No se admiten las siguientes:

- SSE-KMS con una clave KMS AWS administrada (por ejemplo, `aws/s3`)
- SSE-C
- DSSE-KMS
- Claves KMS asimétricas o claves KMS con una especificación clave distinta de `SYMMETRIC_DEFAULT`

Warning

AWS-No se admiten las claves KMS administradas. Si su depósito está cifrado con `aws/s3`, migre a una clave administrada por el cliente o SSE-S3 antes de usarlo con Transform. AWS

Configuración del bucket de Amazon S3

Puede configurar AWS Transform para que utilice su propio bucket de Amazon S3 desde la consola de AWS Transform.

Para usar su propio bucket de Amazon S3

1. En la consola AWS Transform, selecciona Configuración.
2. En Almacenamiento de artefactos, selecciona Usar mi propio depósito S3. Puedes usar un depósito en tu cuenta actual Cuenta de AWS o en otra.
3. Para Bucket, introduzca el URI de Amazon S3.
4. (Opcional) Para la clave de KMS, introduzca un AWS ARN de clave de KMS para cifrar los objetos del depósito. Si deja este campo vacío, AWS Transform escribirá los objetos sin un encabezado de cifrado y Amazon S3 aplicará la configuración de cifrado predeterminada del bucket. Para obtener más información, consulte [Establecer el comportamiento del cifrado predeterminado del lado del servidor para los buckets de Amazon S3](#), en la Guía del usuario de Amazon S3.

Si el cifrado predeterminado de su bucket es SSE-KMS, introduzca el ARN de la clave KMS administrada por el cliente en este campo y actualice la política de claves. Para obtener más información, consulte [the section called “Política de claves de KMS \(opcional\)”](#).

5. Selecciona Guardar. AWS Transform valida la configuración y los permisos del bucket antes de aplicar la configuración.

Tras guardar la configuración, AWS Transform utiliza el depósito para almacenar los artefactos de transformación.

Note

AWS Transform valida la configuración solo cuando la guardas. Si más adelante cambias la política de bucket, la configuración de CORS o la política de claves de KMS, vuelve a guardar la configuración de tu perfil para volver a validarla.

Política de bucket obligatoria

Debe configurar la política de bucket para conceder el acceso a AWS Transform. Añada la siguiente política de bucket a su bucket de Amazon S3 para permitir que el director del servicio AWS Transform lea, escriba, elimine y enumere los artefactos de transformación.

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

```

Reemplace los siguientes valores:

- *bucket-name*— El nombre de su bucket de Amazon S3.
- *profile-account-id*— El Cuenta de AWS ID asociado a tu perfil de AWS Transform.
- *profile-arn*— El ARN de tu perfil de AWS Transform.

Configuración CORS requerida

Si utiliza la aplicación web AWS Transform, debe configurar Cross-Origin Resource Sharing (CORS) en su bucket de Amazon S3. Puede encontrar el dominio de la aplicación web después de activar AWS Transform. Para obtener más información, consulte [Introducción](#).

```
[
  {
    "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
  }
]
```

```
}
]
```

Reemplace los siguientes valores:

- ***webapp-domain***— La URL de origen de su aplicación web (por ejemplo, `https://1a2b3c4d5e6f7a8b9.transform.us-east-1.on.aws`), que se encuentra en la página de configuración de AWS Transform. No incluya la barra diagonal final.

Política de claves de KMS (opcional)

Esta sección solo se aplica cuando el depósito está cifrado con una clave KMS administrada por el cliente. Si tu bucket lo usa SSE-S3, omite esta sección.

Si especificas tu propia clave AWS KMS para el cifrado del bucket, añade la siguiente declaración a tu política de claves. AWS Transform se basa en Forward Access Sessions (FAS) para crear subvenciones para su director de servicio. Estas concesiones se utilizan para validar su clave y acceder a los artefactos de su bucket de 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"
    }
  }
}
```

Reemplace los siguientes valores:

- ***key-owner-account-id***— El Cuenta de AWS ID propietario de la clave KMS.

- **region**— La AWS región en la que está habilitada la AWS transformación (por ejemplo, us-east-1).

Volver al depósito predeterminado

Puedes volver al depósito gestionado por el servicio en cualquier momento.

Para cambiar a AWS Transforme el almacenamiento gestionado

1. En la consola AWS Transform, selecciona Configuración.
2. En Almacenamiento de artefactos, selecciona Editar.
3. Elige AWS Transformar el almacenamiento gestionado.
4. Seleccione Save.

Warning

Si cambia las configuraciones de almacenamiento mientras las tareas de transformación están en curso, esas tareas fallarán. Tampoco se podrá acceder a ningún artefacto que ya haya sido generado por esos trabajos en curso.

Important

Cuando vuelvas al depósito gestionado por el servicio:

- Los artefactos de su depósito no se migran automáticamente. Para conservar cualquier artefacto, descárguelo de su bucket de Amazon S3 y vuelva a subirlo a través de la aplicación web AWS Transform al almacén de artefactos para el espacio de trabajo y el trabajo correspondientes.
- AWS Transform retira la concesión de su clave de KMS. Los objetos escritos en su depósito permanecen en él; elimínelos manualmente si ya no los necesita.

Cargar archivos directamente a tu bucket

Puede cargar archivos directamente a su bucket de Amazon S3 sin utilizar la aplicación web AWS Transform. Para que los archivos cargados estén disponibles para los agentes de transformación,

cárguelos en la User Uploads carpeta correspondiente al trabajo. La ruta del directorio de esta carpeta utiliza el siguiente formato:

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

Reemplace los siguientes valores:

- *workspace-id*— El ID de su espacio de trabajo de AWS Transform.
- *job-id*— El ID de la tarea de transformación.

Cada trabajo de AWS Transform tiene su propia User Uploads carpeta. Los archivos que suba a esta ruta aparecen en la aplicación web y están disponibles para los agentes de transformación mientras completan el trabajo.

Las rutas de los archivos no deben contener . . espacios ni al principio ni al final; los agentes no pueden ver los archivos que infrinjan estas restricciones. //

Important

Si tu bucket lo usa SSE-KMS, incluye los siguientes encabezados en cada carga directa:

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

Los objetos deben cifrarse con la clave KMS registrada en tu perfil de AWS Transform. AWS Transform no puede acceder a los objetos cifrados con cualquier otra clave.

Matriz de compatibilidad

En la siguiente tabla se resume la compatibilidad de AWS Transform con las características habituales de los buckets de Amazon S3.

Característica	Compatibilidad	Notas
Control de versiones del bucket	compatible	Administre las versiones no actuales con una regla de ciclo de vida.

Característica	Compatibilidad	Notas
Propiedad del objeto	Obligatorio: se impone al propietario del bucket	No se admiten el propietario del bucket ni el escritor de objetos.
ACL	No compatible	Las ACL deben estar deshabilitadas en el bucket.
Bloqueo de objetos (modo de gobierno)	Compatible parcialmente	Las eliminaciones pueden estar bloqueadas por la configuración de retención.
Bloqueo de objetos (modo de conformidad)	No compatible	—
Block Public Access	compatible	—
Pago por el solicitante	No compatible	—
Puntos de acceso de S3	No compatible	Usa el nombre del depósito.
Puntos de acceso de S3 Object Lambda	No compatible	Usa el nombre del depósito.
S3 on Outposts	No compatible	—
S3 Express One Zone (depósitos de directorio)	No compatible	—
Cross-Region cubos	No compatible	—
Cross-account cubos	compatible	—
Cross-account claves KMS	No compatible	—

Característica	Compatibilidad	Notas
Regla del ciclo de vida	compatible	—
CloudTrail eventos de datos	compatible	—

Habilitado AWS Transformar

Para activar AWS Transform:

1. Inicie sesión en la consola AWS de administración.
2. En la barra de búsqueda situada en la parte superior de la consola, busca AWS Transform.
3. Selecciona AWS Transformar en los resultados de la búsqueda.
4. Selecciona Comenzar para habilitar el servicio en tu región actual.
5. Opcional: configure el centro de identidad de IAM. También podrás optar por utilizar un [proveedor de identidad \(IdP\) externo](#) en un paso posterior.
6. Seleccione una clave de cifrado: clave AWS gestionada por defecto o personalice la configuración de cifrado.
7. Opcional: utilice su propio bucket de Amazon S3. De forma predeterminada, AWS Transform usa un bucket de Amazon S3 administrado por un servicio para almacenar los artefactos de transformación. En su lugar, puede optar por utilizar su propio depósito. Para obtener más información, consulte [Uso de su propio bucket de Amazon S3](#).
8. Elija qué capacidades de AWS transformación quiere habilitar:
 - Interfaz de línea de comandos (CLI), necesaria para crear y ejecutar [transformaciones personalizadas](#). Para habilitar la CLI, consulte y siga las instrucciones de descarga.
 - Aplicación web, la interfaz de usuario de la agencia para la modernización. Elija Activar la aplicación web para utilizarla.
9. Seleccione Activar AWS transformación.
10. Opcional: seleccione Activar la visualización del perfil para acceder a las pestañas AWS Transformar usuarios, Configuración y Conectores, o Administrar usuarios para gestionar los usuarios.

Puede acceder a las pestañas Usuarios, Configuración y Conectores en cualquier momento seleccionando el icono de menú situado en la esquina superior izquierda de la consola.

11. Configure el acceso de los usuarios seleccionando una de las siguientes opciones:

- IAM Identity Center
- Un [proveedor de identidad \(IdP\) externo](#)
- [IAM-only access](#)

 Note

Esta elección está finalizada y no se puede cambiar al activar AWS Transform.

12. Elija Habilitar aplicación web.

13. El sistema muestra «Habilitar la AWS transformación» mientras crea los recursos necesarios.

Una vez habilitada la AWS transformación, la pestaña Configuración muestra la siguiente información:

- URL de la aplicación web: la URL para acceder a la aplicación web AWS Transform
- URL de inicio del IDE: la URL para acceder a AWS Transform en entornos de desarrollo integrados
- Región: la AWS región en la que AWS Transform está activado

Inicio rápido: ¿Lo estoy intentando AWS Transformar

La forma más sencilla de probar AWS Transform es con una AWS cuenta independiente. Es posible que desee hacerlo como prueba de concepto o para entornos de prueba. Utilice este procedimiento:

1. Inicie sesión en la consola AWS de administración.
2. Navegue hasta el servicio AWS Transform.
3. Seleccione Comenzar para habilitar el servicio.
4. Seleccione y configure su proveedor de identidad.
5. Asigne usuarios al servicio AWS Transform.
6. Una vez habilitado el servicio, verá la URL de la aplicación web AWS Transform.

7. Abre esa URL en una nueva ventana del navegador para acceder a la experiencia web de AWS Transform.

Ahora estás listo para configurar tu espacio de trabajo.

Administrar usuarios

La forma de gestionar el acceso de los usuarios a AWS Transform depende del modelo de acceso que haya elegido durante la configuración. Si ha configurado el Centro de identidades de IAM, puede añadir usuarios a través del Centro de identidades de IAM. Si configuró un proveedor de identidades externo, administrará los usuarios de ese proveedor. Si elige el IAM-only acceso, el acceso de los usuarios se gestiona mediante políticas de IAM.

Adición de usuarios en el Centro de identidades de IAM

Para añadir usuarios al Centro de identidades de IAM:

1. Navegue hasta la consola del Centro de identidades de IAM.
2. En el panel de navegación, seleccione Usuarios.
3. Elija Añadir usuario.
4. Introduzca la información requerida:
 - Nombre de usuario: un identificador único para el usuario (no se puede cambiar más adelante)
 - Dirección de correo electrónico: la dirección de correo electrónico del usuario
 - Nombre y apellidos: nombre del usuario
 - Nombre para mostrar: el nombre que aparece en la lista de usuarios
5. En Contraseña, elija cómo recibirá el usuario su contraseña:
 - Enviar un correo electrónico: envíe las instrucciones de configuración por correo electrónico
 - Genera una contraseña de un solo uso: crea una contraseña para compartirla manualmente
6. Seleccione Siguiente para revisar la información del usuario.
7. Revisa los detalles y selecciona Añadir usuario.

Una vez añadido el usuario, recibirá una invitación por correo electrónico para configurar su cuenta del IAM Identity Center. El enlace de invitación es válido durante 7 días.

También puede obtener información sobre cómo trabajar con IAM Identity Center y AWS Transform en este vídeo:

[VideoTitle](#)

Añadir usuarios a AWS Transformar

Tras añadir usuarios al Centro de identidades de IAM, puede concederles acceso a AWS Transform:

1. Vuelva a la consola de AWS Transform.
2. En el panel de navegación, elija Usuarios y grupos.
3. Seleccione la pestaña Usuarios o la pestaña Grupos.
4. Busque y seleccione los usuarios o grupos que desee añadir en el Centro de identidades de IAM.
5. Elija Asignar usuarios y grupos para conceder a los usuarios o grupos seleccionados acceso a AWS Transform.

Tras añadir usuarios, aparecen en la lista de usuarios con el estado «Pendiente» hasta que acepten la invitación e inicien sesión.

Administrar los usuarios con IAM-only acceso

Si configuró AWS Transform con IAM-only acceso, el acceso de los usuarios se gestiona mediante políticas de IAM. Cualquier director de IAM con el `transform:AccessTransformProfile` permiso correspondiente al recurso de perfil puede acceder a AWS Transform.

Para conceder a un usuario o rol acceso a AWS Transform:

1. Vaya a la consola de IAM.
2. Adjunta una política que incluya la `transform:AccessTransformProfile` acción al usuario o rol de IAM. Para ver un ejemplo de política, consulte [Permitir a los usuarios acceder a AWS Transform con credenciales de IAM](#).

Para revocar el acceso, elimine la política del usuario o rol de IAM.

Entender los permisos de los colaboradores

AWS Transform utiliza un modelo de permisos basado en el espacio de trabajo para controlar el acceso a los recursos y las acciones. A cada usuario se le asigna una función específica dentro de un espacio de trabajo, que determina las acciones que puede realizar. Un usuario puede tener diferentes funciones en distintos espacios de trabajo.

Roles de usuario

AWS Transform admite cinco roles de usuario en cada espacio de trabajo. Estos roles se aplican en el contexto de un espacio de trabajo, y a un usuario se le asignarán roles en cada espacio de trabajo del que sea miembro. Los permisos de acceso definidos para cada rol son independientes del espacio de trabajo, por lo que el usuario A con el rol de administrador en el espacio de trabajo A tiene los mismos permisos que el usuario B con el rol de administrador en el espacio de trabajo B.

Permisos de rol

Permisos detallados para cada función:

Action	ResourceType	Administrador	Aprobador	Colaborador	ReadOnly
Crear	Espacio de trabajo	✓	✓	✓	✓
Enumeración	Espacio de trabajo	✓	✓	✓	✓
Get	Espacio de trabajo	✓	✓	✓	✓
Actualización	Espacio de trabajo	✓	✗	✗	✗
Eliminar	Espacio de trabajo	✓	✗	✗	✗
Crear	ChatMessage	✓	✓	✓	✗
Lectura	ChatMessage	✓	✓	✓	✓
Crear	RoleAssociation	✓	✗	✗	✗

Action	ResourceType	Administrador	Aprobador	Colaborador	ReadOnly
Lectura	RoleAssociation	✓	✓	✓	✓
Actualización	RoleAssociation	✓	✗	✗	✗
Eliminar	RoleAssociation	✓	✗	✗	✗
Lectura	Tarea crítica de Hitl	✓	✓	✓	✓
Actualización	Tarea crítica de Hitl	✓	✓	✗	✗
Eliminar	Tarea crítica de Hitl	✓	✓	✗	✗
Lectura	Tarea Hitl	✓	✓	✓	✓
Actualización	Tarea HitlTask	✓	✓	✓	✗
Eliminar	Tarea HitlTask	✓	✓	✓	✗
Crear	Trabajo	✓	✓	✓	✗
Lectura	Trabajo	✓	✓	✓	✓
Actualización	Trabajo	✓	✓	✓	✗
Eliminar	Trabajo	✓	✓	✓	✗
Lectura	Registro de trabajo	✓	✓	✓	✓
Crear	Artefacto	✓	✓	✓	✗
Lectura	Artefacto	✓	✓	✓	✓
Actualización	Artefacto	✓	✓	✓	✗

Action	ResourceType	Administrador	Aprobador	Colaborador	ReadOnly
Eliminar	Artefacto	✓	✓	✓	x
Crear	Connector	✓	✓	✓	x
Lectura	Connector	✓	✓	✓	✓
Actualización	Connector	✓	✓	✓	x
Eliminar	Connector	✓	✓	✓	x

Human-in-the-loop (HITL) acciones

AWS Transform ofrece dos tipos de acciones de HITL: estándar y críticas:

Acciones estándar de HITL

Se trata de acciones rutinarias que pueden realizar los usuarios con funciones de colaborador, aprobador o administrador.

Acciones críticas de HITL

Se trata de acciones con un impacto significativo y, por lo tanto, requieren niveles de permiso más altos. Entre los ejemplos se incluyen:

- Fusionar el código con las ramas principales
- Realización de la descomposición de gráficos
- Implementación de código en entornos de producción

Las acciones críticas de HITL solo las pueden realizar los usuarios con funciones de aprobador o administrador.

Para garantizar que en las políticas de AuthZ haya una diferencia entre las acciones de HITL estándar y las de HITL críticas, AWS Transform proporciona dos API de HITL independientes, una para llevar a cabo una acción de HITL estándar y otra para completar una acción de HITL crítica.

AWS Transforma el entorno

AWS Transform es un servicio de agencia que utiliza el procesamiento del lenguaje natural para ayudarlo a planificar y ejecutar las transformaciones de la carga de trabajo. Usted interactúa con AWS Transform principalmente a través de una interfaz conversacional, en la que el servicio se adapta y responde en función del contexto de la conversación. Por ejemplo, puede empezar por describir su arquitectura actual y sus objetivos de transformación utilizando un lenguaje cotidiano, como «Necesito migrar mis máquinas virtuales locales a EC2».

Mientras conversa con AWS Transform, el servicio crea un plan de trabajo personalizado que se ajusta a sus requisitos específicos. El flujo de conversación es dinámico e impulsado por usted, lo que le permite refinar su plan de transformación de forma iterativa. Puedes modificar el plan de trabajo durante la conversación haciendo peticiones como «añadir una fase de pruebas antes de la transición a la producción» o «eliminar la fase de respaldo, ya que ya tenemos una solución». También puedes volver a una tarea anterior y volver a realizarla. AWS Transform actualiza continuamente el plan en función de sus aportaciones, lo que garantiza que la estrategia de transformación final satisfaga sus necesidades técnicas y empresariales.

Esto es lo que ve al abrir AWS Transform.

- Ver panel de control: es el panel estrecho situado a la izquierda de AWS Transform. Puede elegir uno de los iconos para elegir qué vista se muestra a la derecha del panel de control de la vista. Pase el ratón sobre cada icono para ver una información sobre herramientas que explica la vista. Las siguientes vistas estándar, de arriba a abajo, son:
 - Plan de trabajo
 - Panel
 - Aprobaciones
 - Artefactos
 - Registro de trabajo

Algunos flujos de trabajo proporcionan vistas adicionales.

Cuando se trabaja en un plan de trabajo, las vistas son:

- Chat
- Aprobaciones
- Tienda de artefactos
- Registro de trabajo

Cuando estás en un espacio de trabajo, las vistas están en la parte superior:

- Trabajos
- Artefactos
- Colaboradores (usuarios)
- Connectors
- Configuración
- El panel de visualización se encuentra junto a los controles de visualización.
- El panel de chat está en el centro. Aquí es donde mantienes tu conversación con AWS Transform.

 Note

Los usuarios con permisos de solo lectura no pueden enviar mensajes en el chat.

- A la derecha está el panel de colaboración. Aparece cuando se realizan actividades de Human in the Loop (HITL), como:
 - Carga de archivos de datos
 - Revisar la información y los planes proporcionados por Transform AWS

Configuración de idioma

AWS Transform admite la localización de determinados flujos de trabajo. Puede cambiar el idioma de visualización de la aplicación web seleccionando el icono de configuración en la esquina superior derecha y seleccionando el idioma que prefiera en el menú Idioma.

Se admiten los siguientes idiomas:

- English (EE. UU.)
- Inglés (Reino Unido)
- Deutsch (alemán)
- Español (español)
- Français (francés)
- (japonés)
- Bahasa Indonesia (indonesio)

- Italiano (italiano)
- Português (portugués)
- (coreano)
- () (chino simplificado)
- () (chino tradicional)
- Türkçe (turco)

Los siguientes flujos de trabajo admiten la localización:

- [Migraciones \(incluida VMware\)](#)

Note

Actualmente, otros flujos de trabajo de AWS Transform solo están disponibles en inglés. Es posible que en futuras actualizaciones se añada soporte de localización para flujos de trabajo adicionales.

Inicie su proyecto

AWS Transform lo guía a través de sus proyectos de modernización y migración. Primeros pasos:

1. Cree un espacio de trabajo para alojar su proyecto. En el panel Espacios de trabajo, elija Crear espacio de trabajo. Sigue las instrucciones y, a continuación, abre el espacio de trabajo.
2. En el panel de chat, escribe «crear un trabajo»
3. Elija un trabajo y siga las instrucciones de AWS Transform. Si se requiere su entrada, aparece el panel de colaboración y se explica qué es lo que se requiere.

Flexibilidad de flujo

El entorno de flujo de trabajo AWS Transform proporciona flexibilidad en la progresión de sus proyectos de modernización. Al usar un lenguaje natural en el panel de chat, puede:

- Vuelva a intentar una tarea que AWS Transform ya haya completado y, a lo largo del proceso, recibirá información diferente y constante.

- Vuelva a ejecutar un trabajo, por ejemplo, si se han producido cambios en las fuentes de modernización.

Conversando con AWS Transformar

AWS El chat de Transform está disponible en todas las etapas de tu proyecto. Para abrir el chat, haz clic en el icono hexagonal morado situado en la esquina inferior derecha de la consola web.

El chat está ahí para que preguntes cualquier cosa. Por ejemplo, puedes pedir al chat que te explique conceptos, te guíe a lo largo de un proceso, explique una solicitud o respuesta de AWS Transform o te explique un informe de AWS Transform.

Note

Los usuarios con permisos de solo lectura no pueden enviar mensajes en el chat.

AWS Transforma las integraciones de chat

AWS El chat de Transform está integrado con:

Experience-Based Aceleración

[Experience-BasedLa aceleración \(EBA\)](#) se ofrece a través del chat AWS Transform. Le permite realizar una evaluación EBA para las cargas de trabajo de Windows y generar un plan. Puede empezar importando los resultados de la evaluación desde CAST. Le ayuda a descubrir su cartera de aplicaciones, tras lo cual puede utilizar el chat de AWS Transform para seleccionar las aplicaciones que mejor se adapten a sus necesidades empresariales (por ejemplo, filtrando las aplicaciones en función de la complejidad o de las líneas de código). A continuación, puede realizar una evaluación más profunda de la aplicación seleccionada y generar un plan de modernización.

AWS Countdown Premium

[AWS La tecnología Countdown Premium](#) (CDP) integrada en AWS Transform proporciona una orientación continua y experta con el apoyo de ingeniería designado AWS . El ingeniero de CDP designado profundiza en su oferta tecnológica y le brinda asistencia personalizada y adaptada al contexto cuando surgen problemas. Los usuarios pueden aprovechar AWS Transform para registrar un ticket de soporte directamente desde su interfaz de chat. El ticket de soporte incorpora los detalles del registro de trabajo y del plan de trabajo para ayudar al soporte a comprender el

contexto del cliente. Si un cliente o socio forma parte del programa CDP, el ticket de soporte se envía automáticamente al ingeniero de CDP designado, quien puede ayudarlo a solucionar los problemas, interpretar los resultados de la transformación e impulsar el progreso para agilizar la resolución de los problemas. Por ejemplo:

- En el caso de las cargas de trabajo de.NET, CDP puede ayudar con los problemas relacionados con los conectores de repositorios, la resolución de dependencias y la implementación posterior a la transformación.
- En los escenarios de mainframe, el CDP puede ayudar a solucionar problemas con el código Java refactorizado, configurar las herramientas de migración de bases de datos y crear canalizaciones. CI/CD
- En las migraciones de VMware, el CDP puede acelerar la configuración de la red, la configuración de MGN y la instalación de agentes.

AWS Creador de habilidades

[AWS Skill Builder](#) proporciona módulos de aprendizaje relevantes a través del chat. Puedes preguntar a AWS Transform Chat sobre tus necesidades de aprendizaje y te presentará el catálogo de cursos correspondiente. Skill Builder ofrece experiencias de microaprendizaje contextuales a medida que avanzas en las etapas de transformación.

Herramientas para desarrolladores

Puede acceder a los agentes de AWS Transform desde los IDE de los agentes, los complementos de los agentes y el servidor MCP. Elija la superficie que mejor se adapte a su flujo de trabajo.

Note

Los complementos Kiro Power y el agente instalan automáticamente el servidor MCP. Solo necesita instalar el servidor MCP manualmente si quiere usarlo sin un Kiro Power o un complemento de agente.

Kiro Power

El [AWS Transform Kiro Power](#) proporciona acceso completo a los agentes de AWS Transform desde el IDE de Kiro.

Para instalar la de AWS Transforma Kiro Power

1. Abre el IDE de Kiro y navega hasta el panel de Powers.
2. Busca AWS Transform en la lista e instálalo.
3. Abre Kiro Chat, haz clic en Power y selecciona Probar power.

Como alternativa, en el panel de Poderes, selecciona Añadir potencia personalizada > Importar potencia desde GitHub y pega: <https://github.com/kirodotdev/powers/tree/main/aws-transform>

Plugin de agente

El complemento AWS Transform agent está disponible en [awsllabs/agent-plugins](#) on GitHub, en el `plugins/aws-transform` directorio. El complemento es compatible con Claude Code, Codex y Cursor.

El complemento incluye `.claude-plugin.codex-plugin`, y `.mcp.json` configuraciones. Proporciona acceso a todos los agentes de AWS Transform, como .NET, mainframe, VMware, SQL Server y transformaciones personalizadas.

Para instalar en Claude Code

Ejecute los siguientes comandos :

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

Para instalar en Codex o Cursor

Siga las instrucciones del archivo README del repositorio agent-plugins.

Complemento IDE

El complemento AWS Transform IDE está disponible en los editores compatibles con VS Code y Open VSX. Expone las funciones personalizadas de AWS Transform, incluida la creación y ejecución de definiciones de transformación. También expone las características del mainframe, incluida la trazabilidad entre los requisitos de modernización, las reglas empresariales y el código fuente, así como la capacidad de generar documentación técnica a pedido. Para empezar, instálelo mediante uno de los siguientes métodos:

- VS Code: instálelo desde [VS Code Marketplace](#).
- Abrir VSX: realizar la instalación desde el registro de [Open VSX](#).

Servidor MCP

Utilice el servidor MCP para integrar AWS Transform mediante programación con cualquier cliente. MCP-compatible Puede instalar el servidor MCP desde PyPI como. `awslibs.aws-transform-mcp-server` Proporciona 19 herramientas para la gestión del espacio de trabajo, la gestión de tareas, las tareas informales (HITL), el manejo de artefactos, la administración de conectores, el chat y la búsqueda de recursos.

Requisitos previos

- Python 3.10 o posterior

Instalación

Código Claude

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

Kiro

Añadir a `~/.kiro/settings/mcp.json`:

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

Para obtener detalles de configuración para su cliente MCP específico, consulte el archivo README [aws-transform-mcp-server](#) en GitHub.

Autenticación

AWS Transform admite el SSO (Identity Center) y la autenticación basada en roles de IAM. AWS Identity and Access Management

SSO (Centro de identidad de IAM)

Pide a tu asistente de IA que «Configure AWS Transform with SSO». El asistente proporciona una URL de inicio y abre el navegador para iniciar sesión.

Rol de IAM

Su entorno proporciona AWS las credenciales automáticamente. Configure `AWS_PROFILE` en el env bloque de configuración del cliente MCP para seleccionar un perfil específico.

Para obtener información sobre cómo configurar la autenticación para AWS Transform, consulte [Introducción al AWS Transformar](#).

Cree agentes personalizados para AWS Transformar

El [kit de herramientas de creación de agentes](#) permite a los AWS socios y clientes crear agentes adaptados a sus necesidades de modernización específicas que funcionen dentro de AWS Transform.

Para instalar el kit de herramientas de creación de agentes

1. Abre el IDE de Kiro y navega hasta el panel de Powers.
2. Busca el kit de herramientas AWS Transform Agent en la lista e instálalo.

Como alternativa, en el panel Powers, selecciona Añadir potencia personalizada > Importar potencia desde GitHub y pega: `https://github.com/kirodotdev/powers/tree/main/aws-transform-agent-toolkit`

El kit de herramientas Agent Builder permite a los socios, ISV o clientes con competencias en migración y modernización crear soluciones de transformación para casos de uso específicos. Puede integrar agentes, herramientas, bases de conocimiento y flujos de trabajo especializados con las funciones de inteligencia artificial de AWS Transform Agentic.

Ciclo de vida de

Build

Utilice Kiro Power para combinar el agente base y el SDK para crear su propio agente personalizado.

Share

Distribuya los agentes con los equipos o entre las redes de socios.

Regístrese

Registre los agentes en AWS Transform para que otros usuarios los descubran.

Evaluaciones de migración

AWS Las evaluaciones de transformación le ayudan a evaluar el costo, la viabilidad y el valor empresarial de migrar una infraestructura local a una. AWS Las evaluaciones proporcionan recomendaciones automatizadas sobre el tamaño correcto, comparaciones de varios escenarios y mejoras interactivas a través del chat.

Puede utilizar las evaluaciones de migración para:

- Obtenga estimaciones de costes de Amazon RDS para SQL Server, Amazon EC2, Amazon EBS, Amazon S3 y Amazon FSx
- Reciba recomendaciones automatizadas sobre el tamaño correcto
- Evalúe el valor empresarial y el impacto en la sostenibilidad
- Compare varios escenarios de migración uno al lado del otro
- Perfeccione las evaluaciones de forma interactiva a través del chat
- Genere presentaciones ejecutivas e informes detallados

Requisitos previos

Antes de crear una evaluación de migración, confirme que dispone de lo siguiente:

- Un espacio de trabajo de AWS Transform
- Los datos de inventario están en un formato compatible, o puedes usar una estimación aproximada a través del chat
- Permisos adecuados para crear y ejecutar evaluaciones

Cómo funcionan las evaluaciones de migración

Las evaluaciones de migración siguen un flujo de trabajo estructurado que lo guía desde la carga inicial de los datos hasta la generación del producto final.

Para completar una evaluación de la migración

1. Cree un trabajo de evaluación de la migración en su espacio de trabajo de AWS Transform.
2. Cargue sus datos de inventario local.

3. Revise los resultados de descubrimiento que AWS Transform genera a partir de sus datos.
4. Gestione el alcance del inventario excluyendo los servidores o ajustando las agrupaciones.
5. Configure su escenario de evaluación con hipótesis de precios e infraestructura.
6. Ejecute la evaluación.
7. Revisa y refina los resultados a través del chat.

Tras revisar los resultados, puede crear escenarios adicionales, compararlos y generar resultados, como presentaciones e informes.

Cargar datos de inventario

AWS Transform acepta datos de inventario de múltiples fuentes. En la siguiente tabla se enumeran los formatos de datos admitidos.

Origen de datos	Description (Descripción)
AWS Exportación de Transform Discovery Tool	Inventario automatizado de servidores descubierto por la herramienta de descubrimiento AWS Transform
RVTools	Exporta desde entornos VMware en ZIP/CSV formato Excel. Se admiten tanto las exportaciones completas como Info-only las exportaciones v.
Datos de CMDB	Exportaciones de bases de datos de administración de
Herramientas de descubrimiento de socios	Datos de las herramientas de descubrimiento de AWS socios
Evaluador de migración	Archivo Quick Insights de la consola de Migration Evaluator
Formato MPA	Archivo de importación de Migration Portfolio Assessment
AWS Transforme la plantilla de datos	Archivo de Microsoft Excel creado a partir de la plantilla AWS Transform Assessment Data

AWS Transform identifica automáticamente el formato del archivo durante la ingesta. El proceso de ingesta valida los datos, acepta datos parciales cuando faltan algunos campos y admite las cargas

incrementales. Puedes subir archivos adicionales en cualquier momento para complementar tu inventario.

Revisar los resultados del descubrimiento

Una vez que AWS Transform procesa los datos de inventario, genera un resumen del descubrimiento. En concreto, la tabla resumen incluye la información siguiente:

- Recuento de servidores por sistema operativo
- Desglose de servidores físicos y virtuales
- Detección de SQL Server
- Resúmenes de almacenamiento
- Advertencias de calidad de datos

Revise los resultados del descubrimiento para confirmar que AWS Transform identificó correctamente su infraestructura antes de continuar con la evaluación.

Administrar el alcance del inventario

Tras revisar los resultados del descubrimiento, puede afinar el alcance de la evaluación. Usa las siguientes acciones para gestionar el alcance de tu inventario:

- Consulta el inventario para servidores o cargas de trabajo específicos
- Excluya los servidores del ámbito de la evaluación
- Revise las agrupaciones de servidores y las dependencias de las aplicaciones
- Identifique las cargas de trabajo de SQL Server para una evaluación especializada

Configuración de escenarios de evaluación

Antes de ejecutar una evaluación, configure las suposiciones que AWS Transform utiliza para generar recomendaciones. Puede modificar estas suposiciones en cualquier momento y ejecutar nuevos escenarios con diferentes configuraciones.

En la siguiente tabla se enumeran las categorías de hipótesis disponibles.

Suposición	Description (Descripción)
Modelo de precios	Database Savings Plans (para Amazon RDS para SQL Server) o On-Demand instancias reservadas
Destino Región de AWS	El Región de AWS lugar donde planea alojar las cargas de trabajo migradas
Exclusiones de tipos de instancia	Familias o tipos de instancias de Amazon EC2 que se van a excluir de las recomendaciones
Configuración de Amazon EBS	Tipo de volumen y configuración de rendimiento para el almacenamiento
Licencias de SQL Server	Bring Your Own Media (BYOM) o licencia incluida (LI) para Amazon RDS for SQL Server; licencia incluida (LI) o Bring Your Own License (BYOL) para SQL Server en EC2

Capacidades de evaluación

AWS Las evaluaciones de Transform cubren múltiples dimensiones de su migración. En las siguientes secciones se describe cada capacidad de evaluación.

Tamaño correcto de Amazon EC2

AWS Transform analiza las especificaciones de sus servidores locales y recomienda instancias Amazon EC2 del tamaño adecuado. Las recomendaciones tienen en cuenta los requisitos de CPU, memoria y rendimiento.

Almacenamiento en Amazon EBS

AWS Transform recomienda los tipos y configuraciones de volúmenes de Amazon EBS en función de sus requisitos actuales de rendimiento y uso del almacenamiento.

Amazon FSx

AWS Transform evalúa las cargas de trabajo de almacenamiento de archivos y proporciona recomendaciones para la migración a Amazon FSx, incluidas estimaciones de costos para los tipos de sistemas de archivos de Amazon FSx compatibles.

Amazon RDS para SQL Server

AWS Transform evalúa el costo de migrar las bases de datos de SQL Server locales a Amazon RDS for SQL Server. Mediante el uso de AI-powered agentes, AWS Transform analiza su entorno local de SQL Server y ofrece un modelo de negocio de migración completo en cuestión de minutos, con recomendaciones de cómputo y memoria adaptadas a sus requisitos de carga de trabajo para evitar el sobreaprovisionamiento y pagar solo por lo que necesita.

La evaluación de RDS para SQL Server incluye las siguientes capacidades:

- Las licencias Bring Your Own Media (BYOM), que le permiten utilizar sus licencias de SQL Server existentes
- Opciones de licencia con licencia incluida (LI)
- Optimización de costos mediante Database Savings Plans, que ofrecen hasta un 20% de ahorro en comparación con On-Demand los precios
- Evaluación de elegibilidad para el AWS Migration Acceleration Program (MAP), que proporciona créditos y apoyo para compensar los costos de migración

Puede iniciar su evaluación de RDS para SQL Server con cualquier formato de datos compatible, incluidas las exportaciones de RVTtools, los datos de la base de datos de gestión de la configuración (CMDB), las exportaciones de la herramienta de descubrimiento AWS Transform y otras herramientas de descubrimiento de terceros. Cree escenarios hipotéticos para comparar varios modelos de costes con hipótesis personalizadas, como la región, la utilización de los recursos y las condiciones de precios.

Ejemplos de peticiones:

- «Calcule el costo de migrar mis bases de datos de SQL Server a RDS for SQL Server»
- «Compare los precios de BYOM con los de licencia incluida de RDS para SQL Server»
- «Muéstreme las opciones de Database Savings Plans para mis cargas de trabajo de RDS»

Amazon EC2 SQL Server

AWS Transform evalúa las cargas de trabajo de SQL Server y proporciona recomendaciones para ejecutar SQL Server en Amazon EC2, incluidos análisis de licencias y mapeos de hosts dedicados.

On-premises precios

AWS Transform calcula sus costos locales actuales para proporcionar una base de comparación con AWS los precios. Puede realizar ajustes de costos generales a través del chat. On-premises Los ajustes de costes se reflejan en el informe en PDF y en las respuestas del chat, pero no en la exportación a PPTX.

Ejemplos de peticiones:

- «Actualice el costo del servidor local a 500 dólares por servidor al mes»
- «Añada 50 000\$ a los costes anuales de las instalaciones del centro de datos»

Sostenibilidad

AWS Transform estima la reducción de la huella de carbono que se produce al migrar a. AWS Puedes explorar las métricas de sostenibilidad a través del chat.

Prueba con indicaciones como las siguientes:

- «Muéstreme la reducción de carbono estimada para esta migración»
- «¿En qué consiste la mejora de la eficiencia energética de mis cargas de trabajo AWS?»

Evaluación del valor empresarial

AWS Transform evalúa el valor empresarial más amplio de la migración, más allá del ahorro de costes de infraestructura. La evaluación abarca la productividad, la resiliencia y la agilidad empresarial del personal.

A continuación, se muestran algunos ejemplos de instrucciones:

- «Calcule las ganancias de productividad del personal al migrar a» AWS
- «¿Qué mejoras de resiliencia puedo esperar tras la migración?»

- «Muéstreme los beneficios de esta migración en materia de agilidad empresarial»

Costos de red

AWS Transform calcula los costos relacionados con la red para su migración, incluidos los requisitos de transferencia de datos y conectividad.

Costes de soporte

AWS Transform incluye los costos del plan AWS Support en la evaluación en función del nivel de soporte seleccionado.

Informática para usuarios finales

AWS Transform evalúa las cargas de trabajo informáticas de los usuarios finales y proporciona recomendaciones para los servicios informáticos de los usuarios AWS finales.

Uso de evaluaciones basadas en el chat

Puede interactuar con AWS Transform a través del chat para crear y refinar las evaluaciones. El chat admite tres modos de interacción.

Puede refinar su evaluación de forma iterativa continuando la conversación. AWS Transform mantiene el contexto en todos los mensajes y actualiza los resultados de la evaluación en función de sus comentarios.

Estimación aproximada con datos limitados

Puedes obtener una estimación aproximada de los costes describiendo tu entorno en el chat sin tener que subir ficheros de inventario detallados. La estimación aproximada es una función independiente y no se puede combinar con los datos de inventario subidos ni con el enriquecimiento de los datos a través del chat.

Puedes usar indicaciones como las siguientes:

- «Tengo 200 servidores Windows y 150 servidores Linux, calcule mis AWS costes»
- «Deme una estimación aproximada de la migración de 500 máquinas virtuales a» AWS
- «Calcule los costes de 50 servidores con una media de 8 CPU y 32 GB de RAM»

Añadir inventario a través del chat

Puedes proporcionar los detalles del inventario directamente a través del chat para complementar o reemplazar los archivos subidos.

Usa indicaciones como las siguientes:

- «Incluya un servidor de bases de datos que ejecute Oracle en 4 CPU con 128 GB de RAM»
- «Añada 20 servidores web que ejecuten Linux con 4 CPU y 16 GB de RAM»

Modificar los costos y agregar servicios

Puede ajustar los costos locales y añadir AWS servicios a su evaluación a través del chat.

Ejemplos de solicitudes para realizar ajustes en las instalaciones:

- «Aumente los costes locales en un 15% para tener en cuenta las próximas actualizaciones de hardware»
- «Añada 100 000\$ de costes de mantenimiento anuales a la base de referencia local»

También puedes añadir estimaciones aproximadas de los costes de AWS los servicios que no estén totalmente respaldados por las evaluaciones de AWS Transform. Esto proporciona un análisis más completo, pero estas estimaciones son menos precisas que las recomendaciones automatizadas.

- «Añadir costes AWS de Backup a todos los servidores migrados»
- «Incluya los costos CloudWatch de monitoreo de Amazon en la estimación»
- «Agregue los costos de AWS Direct Connect para una conexión de 10 Gbps»

Comparación de escenarios

Puede crear varios escenarios de evaluación con diferentes suposiciones y compararlos para identificar la estrategia de migración óptima.

Creación de escenarios

Prueba con indicaciones como las siguientes:

- «Cree un escenario de BYOM para migrar las bases de datos de SQL Server a RDS para SQL Server»
- «Cree un escenario con Database Savings Plans for RDS for SQL Server»
- «Cree un escenario de LI para todas las cargas de trabajo de SQL Server en EC2»
- «Cree un escenario con todas las cargas de trabajo en us-west-2»

Ejecutando comparaciones

A continuación, se muestran algunos ejemplos de instrucciones:

- «Muéstreme una comparación de costos en todos los escenarios»
- «¿Qué escenario tiene el coste total de propiedad más bajo?»

What-if análisis

Modele el impacto de cambios específicos sin crear un escenario completamente nuevo.

Ejemplos de peticiones:

- «¿Qué sucede si muevo mis cargas de trabajo de SQL Server a RDS for SQL Server en lugar de a EC2?»
- «¿Cuál es la diferencia de coste entre el BYOM y la licencia incluida para RDS for SQL Server?»
- «¿Qué sucede si excluyo los 50 servidores más pequeños de la migración?»
- «¿Qué sucede si solo uso instancias optimizadas para el almacenamiento?»
- «¿Cuál es el impacto de pasar de los volúmenes gp3 a io2?»

Generar entregables

Una vez finalizada la evaluación, puede generar los entregables en varios formatos. En la siguiente tabla se describen los formatos de salida disponibles.

Formato	Description (Descripción)	Personalización
PPTX () PowerPoint	Presentación ejecutiva con un resumen de las conclusiones y recomendaciones	Estructura fija

Formato	Description (Descripción)	Personalización
XLSX (Excel)	Exportación de datos detallada con recomendaciones a nivel de servidor y desgloses de costos	Estructura fija
PDF	Documento de informe	Personalizable a través del chat

Temas relacionados

- [Introducción](#)
- [Trabajos personalizados](#)
- [Herramienta de descubrimiento](#)

Personalizada

¿Qué es? AWS ¿Transformar de forma personalizada?

AWS Transform custom utiliza la IA de los agentes para modernizar a gran escala el software, el código, las bibliotecas y los marcos a fin de reducir la deuda técnica. Gestiona diversos escenarios, como las actualizaciones de las versiones lingüísticas, las migraciones de API y servicios, las actualizaciones y migraciones de los marcos, la refactorización del código y las transformaciones específicas de la organización.

Gracias al aprendizaje continuo, el agente mejora a partir de cada ejecución y de los comentarios de los desarrolladores, y ofrece transformaciones repetibles y de alta calidad sin necesidad de conocimientos especializados en automatización.

Capacidades clave

AWS Transform custom ofrece las siguientes funciones:

- Definición de transformación basada en el lenguaje natural: cree transformaciones personalizadas utilizando el lenguaje natural, la documentación y los ejemplos de código
- Ejecución de transformaciones: aplique transformaciones de forma coherente y fiable en varias bases de código
- Aprendizaje continuo: mejore automáticamente la calidad de la transformación en cada ejecución
- AWS-transformaciones gestionadas: utilice transformaciones revisadas y listas para usar en escenarios AWS comunes

Patrones de transformación

AWS Transform custom admite diversos patrones de transformación para abordar sus necesidades de modernización. Cada patrón tiene características de complejidad diferentes según el alcance y la naturaleza de los cambios necesarios.

Patrón	Description (Descripción)	Complejidad	Ejemplos
Migraciones de API y servicios	Migración entre versiones de API o servicios equivalentes manteniendo la funcionalidad	Medio	AWS SDK v1→v2 (Java, Python JavaScript), Boto2→Boto3, JUnit 4→5, javax→Jakarta
Actualizaciones de la versión del idioma	Actualización a versiones más recientes del mismo lenguaje de programación, adopción de nuevas funciones y sustitución de funciones obsoletas	Low-Medium	Java 8→17, Python 3.9→3.13, 12→22, actualizaciones de versión Node.js TypeScript
Actualizaciones del marco	Actualización a versiones más recientes del mismo marco, abordando los cambios más importantes	Medio	Spring Boot 2.x→3.x, React 17→18, actualizaciones de Angular, actualizaciones de Django
Migraciones de marcos	Migración a marcos completamente diferentes que cumplen propósitos similares	Alto	Angular → React, Redux → Zustand, → React Vue.js
Actualizaciones de bibliotecas y dependencias	Actualización de bibliotecas de terceros a versiones más recientes manteniendo el	Low-Medium	Pandas 1.x→2.x, NumPy actualizaciones, actualizaciones de bibliotecas, Hadoop/HBase/Hive

Patrón	Description (Descripción)	Complejidad	Ejemplos
	mismo lenguaje y marco		actualizaciones de Lodash
Refactorización de código y modernización de patrones	Modernizar los patrones de código y adoptar las mejores prácticas sin cambiar la funcionalidad externa	Low-Medium	Imprimir → Marcos de registro, concatenación de cadenas → cadenas f, adopción de sugerencias de tipos, instrumentación de observabilidad
File-by-File Guión y traducciones	Traducir scripts o archivos de configuración independientes, en los que la mayoría de los archivos son independientes	Low-Medium	AWS CDK→Terraform, Terraform →, Excel→Cuadernos Python, CloudFormation Bash→ PowerShell
Migraciones de arquitectura	Migración entre arquitecturas de hardware o entornos de ejecución con cambios de código mínimos	Medium-High	x86 →AWS Graviton (ARM), local → Lambda, servidor tradicional → contenedores
Language-to-Language Migraciones	Traducir bases de código de un lenguaje de programación a otro	Muy alto	Java→Python, JavaScript →, C→Rust, TypeScript Python→Go

Patrón	Description (Descripción)	Complejidad	Ejemplos
Organization-Specific Personalización y transformaciones	Requisitos organizativos únicos y necesidades de modernización especializadas	Varía	Migraciones de bibliotecas internas personalizadas, estándares de codificación específicos de la organización, migraciones de marcos patentados

Note

Para los COBOL/mainframe idiomas, utilice AWS Transform for Mainframe. Para las actualizaciones de .NET Framework a .NET Core, considere AWS Transform para Windows. Para migraciones a VMware AWS, considere AWS Transform for VMware.

Cómo AWS Transforme obras personalizadas

AWS Transform custom se suele utilizar en proyectos a gran escala en los que se transforman varias bases de código o módulos. Los equipos suelen seguir un flujo de trabajo de cuatro fases:

Defina la transformación: proporcione instrucciones en lenguaje natural, documentación y ejemplos de código al agente, lo que generará una definición inicial de la transformación. Esta definición se puede refinar de forma iterativa mediante el chat o mediante ediciones directas. Esta fase se puede omitir cuando se utilizan AWS transformaciones gestionadas.

Realice una prueba piloto o Proof-of-Concept pruebe la transformación en bases de código de muestra y fíjela en función de los resultados. Esta fase de validación ayuda a estimar el coste y el esfuerzo de la transformación completa. El aprendizaje continuo mejora la calidad durante esta fase.

Ejecución escalada: configure la ejecución masiva automatizada mediante la CLI, con los desarrolladores revisando y validando los resultados. Supervise el progreso mediante la aplicación web y realice un seguimiento de las transformaciones en varios repositorios.

Supervise y revise: el aprendizaje continuo mejora automáticamente la calidad de la transformación. Revisa las lecciones extraídas de series anteriores para asegurarte de que cumplen con los estándares de calidad y archiva las que no sean útiles.

Comprensión de conceptos clave de

En esta sección se explican los conceptos clave para trabajar con AWS Transform custom.

Definiciones de transformación

Una definición de transformación contiene las instrucciones y los conocimientos necesarios para realizar una transformación de código específica. Se representa como una habilidad y consiste en:

- `SKILL.md`(obligatorio): instrucciones en Markdown con material (`name` y `description` campos) de YAML que contienen la lógica de transformación básica y las instrucciones de ejecución
- `references/`carpeta (opcional): la documentación se carga según sea necesario durante la ejecución de la transformación
- `scripts/`carpeta (opcional): scripts que la transformación descarga y ejecuta durante la ejecución

AWS Transform CLI descarga automáticamente las definiciones de transformación en el directorio actual cuando es necesario para su ejecución, inspección o modificación.

Important

Al publicar una transformación, el directorio debe contener solo `SKILL.md` y de forma opcional la `references/` carpeta, la `scripts/` carpeta o ambas. No se permiten otros archivos o subdirectorios.

Note

La versión 2.0 y posteriores de CLI utilizan el formato `skills`. La CLI gestiona automáticamente las definiciones de transformación existentes.

Registro de transformaciones

El registro de transformaciones es el repositorio centralizado de su AWS cuenta para almacenar y gestionar las definiciones de transformación. Las transformaciones en el registro pueden ser:

- Se enumeran usando `atx custom def list`
- Se ejecuta en múltiples bases de código
- Compartido con otros usuarios de tu cuenta AWS
- Version-controlled

Important

Las definiciones de transformación son específicas de cada cuenta. Si desea utilizar una transformación en una AWS cuenta diferente, debe publicarla por separado en esa cuenta.

Transformaciones preliminares frente a transformaciones publicadas

AWS Transform custom admite dos estados para las transformaciones del registro:

Los borradores de las transformaciones son definiciones de transformación en curso o no probadas. Se guardan como versiones específicas y los usuarios que utilizan esa versión específica pueden recuperarlas, actualizarlas y ejecutarlas. Los borradores son útiles para el desarrollo, las pruebas y el perfeccionamiento iterativos antes de que la transformación esté lista para compartirse con tu equipo. Los borradores también se asocian a conversaciones específicas. Si reinicia la CLI, puede `atx --conversation-id {id}` utilizarla para restaurar una anterior.

Las transformaciones publicadas están disponibles en el registro de transformaciones de su cuenta para que las ejecuten otros usuarios con los permisos de IAM necesarios. Las transformaciones publicadas se pueden descubrir utilizando `atx custom def list`.

El flujo de trabajo típico es:

1. Cree la transformación a nivel local
2. Guardar como borrador para probarlo (`atx custom def save-draft`)
3. Refina y valida
4. Publica para compartir con tu equipo (`atx custom def publish`)

También puedes publicar una transformación directamente sin guardarla como borrador.

Referencias frente a lecciones

AWS Transform custom utiliza dos tipos de conocimiento para mejorar la calidad de la transformación:

Las referencias son documentación proporcionada por el usuario que se almacena en la `references/` carpeta de una definición de transformación. Las referencias solo admiten archivos de texto (máximo 10 MB en total para todos los archivos) y, por lo general, contienen documentación, especificaciones de API, guías de migración y ejemplos de código. Las referencias se cargan según sea necesario durante la ejecución de la transformación. Las referencias se añaden al crear o actualizar una definición de transformación en modo interactivo.

Las lecciones se extraen automáticamente de las ejecuciones anteriores de una transformación. El sistema de aprendizaje continuo las genera a partir de las trayectorias de ejecución, los comentarios de los desarrolladores y las correcciones de código que encuentra durante las transformaciones. Agrupa las lecciones relacionadas en categorías para que puedan repasarlas juntas. A diferencia de las referencias, que se proporcionan por adelantado, las lecciones se acumulan con el tiempo a medida que se ejecuta la transformación en diferentes bases de código, y el sistema las aplica automáticamente para mejorar las ejecuciones futuras. Con ellas revisas y gestionas las lecciones de forma interactiva.

```
atx custom def learnings
```

Comandos de compilación y validación

El comando de compilación o validación es un parámetro opcional que especifica cómo validar el código durante el proceso de transformación. Este comando se ejecuta en varios puntos de la transformación para garantizar la integridad del código.

Proporcionar un comando que valide los resultados y devuelva problemas si la validación falla es muy importante para mejorar la calidad de la transformación mediante el aprendizaje continuo. Si no es necesario compilarlo ni validarlo, omítelo en la entrada.

Para ver ejemplos y una guía detallada, consulta los comandos de compilación y validación en la sección Flujos de trabajo.

Aprendizaje continuo

El aprendizaje continuo es el sistema que captura automáticamente los comentarios de cada ejecución de una transformación y mejora la calidad de la transformación con el tiempo. El sistema recopila información a través de:

- Comentarios explícitos: los comentarios y las correcciones de código se proporcionan en el modo interactivo
- Observaciones implícitas: problemas que encuentra el agente al transformar y depurar el código

El sistema de aprendizaje continuo procesa esta información para crear lecciones que agrega a la definición de transformación para mejorar las transformaciones futuras. El sistema ejecuta el proceso de aprendizaje automáticamente una vez finalizadas las transformaciones, sin requerir ninguna intervención adicional por tu parte.

Important

Las lecciones son específicas de cada transformación y no se comparten entre distintas transformaciones o cuentas de clientes.

Gestión de las lecciones

El sistema genera las lecciones automáticamente, pero tú tienes el control de cuáles se aplican a futuras tiradas. El `atx custom def learnings` comando abre una sesión terminal interactiva para revisar y seleccionar las lecciones acumuladas durante la transformación.

En esta sesión, puede:

- Explore las lecciones agrupadas en categorías y vea cuántas lecciones activas contiene cada categoría.
- Abre una lección para leer todos sus detalles, incluidos el cuerpo de la lección, su impacto y el número de sesiones anteriores en la que se ha consultado.
- Archiva una lección para evitar que el sistema la aplique en futuras ejecuciones y restaúrela más tarde si es necesario.
- Elimine permanentemente una lección archivada que ya no sea útil.

Para obtener instrucciones paso a paso, consulte [the section called “Aprendizaje continuo”](#).

Client-Side Habilidades

Client-side las habilidades son capacidades adicionales que amplían al agente durante las ejecuciones de transformación. A diferencia de las definiciones de transformación, que definen qué transformación realizar, las habilidades del lado del cliente proporcionan herramientas, scripts e instrucciones adicionales que el agente puede utilizar junto con sus capacidades integradas durante cualquier transformación.

Client-side las habilidades se descubren en los directorios a nivel de proyecto y de usuario. Sitúe las habilidades en el nivel de proyecto cuando hagan cumplir los estándares específicos de un repositorio, y en el nivel de usuario cuando se apliquen a todos sus proyectos. Project-level Las habilidades solo están disponibles cuando se proporciona una ruta al repositorio de código. Para obtener información detallada sobre la configuración y el uso, consulte [the section called “Client-Side Habilidades”](#).

Introducción

En esta sección se describe cómo configurar AWS Transform custom y ejecutar la primera transformación.

Requisitos previos

Antes de instalar AWS Transform custom, asegúrese de disponer de lo siguiente:

Plataformas admitidas

AWS Transform custom es compatible con los siguientes sistemas operativos:

- Linux: soporte completo para todas las distribuciones de Linux
- macOS: compatibilidad total con los sistemas macOS
- Windows: soporte completo para Windows nativo mediante Windows Terminal y PowerShell (los `atx` y `ct` comandos aún no son compatibles con Windows)
- Subsistema de Windows para Linux (WSL): compatible cuando se ejecuta en WSL

Software necesario

- Node.js 22 o posterior: se puede descargar desde <https://nodejs.org/en/download>

- Git: debe estar instalado y el directorio de trabajo debe ser un repositorio de Git válido para ejecutar una transformación. Ejecuta `git init`; `git add .`; `git commit -m "Initial commit"` para inicializar un repositorio de Git en tu directorio de trabajo.

Requisitos de red

Se requiere una conexión a Internet con acceso a los siguientes puntos finales:

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

Si trabaja en un entorno con acceso restringido a Internet, actualice las reglas del firewall para incluir estas URL en una lista de direcciones URL permitidas.

Instalación de la AWS Transformar CLI

El método de instalación recomendado es utilizar el script de instalación. Seleccione la pestaña correspondiente a su sistema operativo.

Para instalar la CLI de AWS Transform

1. Ejecute el script de instalación:

Linux and macOS

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

Windows (PowerShell)

En el sistema nativo de Windows, ejecute el script de instalación desde la Terminal de Windows utilizando PowerShell.

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

2. Verificar la instalación:

```
atx --version
```

El comando debe mostrar la versión instalada de la CLI de AWS Transform.

Configuración de la autenticación

AWS Transform custom requiere AWS credenciales para autenticarse en el servicio. Configure la autenticación mediante uno de los siguientes métodos.

Variables de entorno

Configure las siguientes variables de entorno.

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"
```

También puede especificar un perfil mediante la variable de AWS_PROFILE entorno.

Linux and macOS

```
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

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

Note

Las variables de entorno configuradas con `$env :` in PowerShell se aplican únicamente a la sesión actual. Para conservarlas en todas las

sesiones, configúrelas en Propiedades del sistema > Variables de entorno o utilícelas `[System.Environment]::SetEnvironmentVariable()`.

AWS Archivo de credenciales

Configure las credenciales en el archivo de AWS credenciales, ubicado `~/.aws/credentials` en Linux y macOS, o `%USERPROFILE%\aws\credentials` en Windows:

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

Permisos de IAM

Sus AWS credenciales deben tener permisos para llamar al servicio personalizado AWS Transform. Te recomendamos adjuntar la política [AWSTransformCustomFullAccess](#) AWS gestionada a tu usuario o rol de IAM. Esta política proporciona acceso completo a AWS Transform custom, incluido el permiso para crear el [rol vinculado al servicio](#) necesario para la emisión de CloudWatch métricas a tu cuenta.

Para un control más detallado, AWS Transform custom también proporciona las siguientes políticas AWS gestionadas:

- [AWSTransformCustomExecuteTransformations](#)— Proporciona acceso para ejecutar transformaciones.
- [AWSTransformCustomManageTransformations](#)— Proporciona acceso para crear, actualizar, leer y eliminar recursos de transformación, así como para ejecutar transformaciones.

Para obtener más información sobre estas políticas, consulte las [políticas AWS gestionadas de AWS Transform](#). Para obtener información sobre las políticas de IAM personalizadas con permisos a nivel de recursos, consulte la Guía de referencia de autorización de [servicios de IAM personalizados de AWS Transform](#).

Note

- Las definiciones de transformación son AWS recursos con ARN (Amazon Resource Names). Puede usar las políticas de IAM para controlar el acceso a transformaciones o

grupos de transformaciones específicos especificando el ARN de la transformación en sus declaraciones de recursos de políticas de IAM. Las etiquetas se pueden utilizar para el control de acceso agrupado.

- AWS Se requiere el IAM Identity Center para acceder a la AWS transformación, pero no es necesario para usar la CLI.

Configuración AWS Region

AWS La transformación personalizada está disponible en AWS regiones específicas y detecta automáticamente la configuración de la región mediante la prioridad AWS CLI estándar.

Regiones admitidas

AWS La transformación personalizada está disponible en las siguientes AWS regiones:

- `us-east-1`(EE. UU. Este - Norte de Virginia)
- `eu-central-1`(Europa: Fráncfort)
- `eu-west-2`(Europa - Londres)
- `ca-central-1`(Canadá - Central)
- `ap-northeast-1`(Asia-Pacífico - Tokio)
- `ap-northeast-2`(Asia-Pacífico - Seúl)
- `ap-southeast-2`(Asia-Pacífico - Sídney)
- `ap-south-1`(Asia Pacífico - Bombay)

¿Cómo se determina la región

La CLI comprueba estas fuentes en orden de prioridad para determinar qué región utilizar:

1. `AWS_REGION` variable de entorno (máxima prioridad)
2. `AWS_DEFAULT_REGION` variable de entorno
3. Perfil seleccionado en el archivo de AWS configuración (mediante una variable de `AWS_PROFILE` entorno)
4. Perfil predeterminado en el archivo de AWS configuración

5. Recurso predeterminado a us-east-1 si no se encuentra ninguna configuración

Note

El archivo de AWS configuración se encuentra `~/.aws/config` en Linux y macOS, o `%USERPROFILE%\aws\config` en Windows.

Note

Si `ATX_CUSTOM_ENDPOINT` está establecida, la región se extrae de la URL del punto final y anula todos los demás ajustes.

Configuración de su región

Elija uno de estos métodos para configurar su región:

Opción 1: Variable de entorno (recomendada para uso temporal):

Linux and macOS

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

Windows (PowerShell)

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

Opción 2: configuración AWS CLI (recomendada para una configuración permanente):

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

Opción 3: Profile-specific configuración:

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"
```

Opción 4: Edición directa de archivos:

Edite el archivo de AWS configuración directamente (~/.aws/config en Linux y macOS, o %USERPROFILE%\aws\config en Windows):

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

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

Verificación de la configuración de su región

Para comprobar qué región utilizará AWS Transform Custom:

Compruebe la configuración de región actual:

```
aws configure get region
```

Compruebe las variables de entorno:

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"
```

Vea la resolución detallada de la región en los registros de depuración:

Linux and macOS

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

Windows (PowerShell)

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

Ejemplo de salida de registro que muestra la fuente de la región:

```
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"
}
```

El `regionSource` campo muestra el origen de la región (por ejemplo, «aws-config (profile: default)», «AWS_REGION», «default»).

Important

Si la configuración de su región apunta a una región no compatible, la CLI mostrará un mensaje de error claro con instrucciones para actualizar la configuración a una región compatible.

Ejecutando su primera transformación

La forma más rápida de empezar es utilizar una transformación AWS gestionada. AWS-las transformaciones gestionadas son transformaciones prediseñadas y AWS examinadas que están listas para usarse sin necesidad de configuración alguna.

Para ejecutar una transformación gestionada de forma interactiva AWS:

```
atx
```

A continuación, pida al agente que ejecute una transformación:

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

Para ejecutar una transformación de forma no interactiva:

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

Para obtener información detallada sobre los modos de ejecución, las opciones de configuración y los indicadores de comando, consulte. [the section called “Referencia de comandos”](#)

Comprender los resultados de la transformación

Cuando se completa una transformación, AWS Transform custom proporciona un informe en el que se describen los resultados. Si la transformación no se validó (por ejemplo, si se creó correctamente una aplicación Java), el informe proporciona recomendaciones para tomar medidas adicionales.

La mayoría de las transformaciones se realizan en varios pasos, utilizando Git para confirmar las intermedias. Puedes revisar los cambios realizados por la transformación mediante los comandos estándar de Git:

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

Crear una transformación personalizada

Cuando las transformaciones AWS gestionadas no satisfacen sus necesidades, puede crear transformaciones personalizadas adaptadas a sus requisitos específicos.

Para crear una transformación personalizada

1. Inicie la CLI de AWS transformación en modo interactivo:

```
atx
```

2. Dígame al agente que desea crear una nueva transformación y describa sus requisitos.
3. Proporcione materiales de referencia, como documentación y ejemplos de códigos, para mejorar la calidad.

4. Pruebe y perfeccione la transformación de forma iterativa.
5. Publíquela en el registro de transformaciones de su organización.

Para obtener instrucciones detalladas sobre cómo crear transformaciones personalizadas, consulte [the section called “Flujos de trabajo”](#).

AWS Transformar la aplicación web (opcional)

La aplicación web AWS Transform es una interfaz opcional para supervisar las campañas de transformación a gran escala en varios repositorios. Antes de usar la aplicación web AWS Transform, debe tener habilitada una identidad de usuario para acceder a AWS Transform en su organización. Para obtener información sobre cómo habilitar AWS Transform, consulte [Configuración de AWS Transform](#).

Para usar la aplicación web AWS Transform:

1. Visite <https://aws.amazon.com/transform/> e inicie sesión con las credenciales AWS del IAM Identity Center.
2. Seleccione el tipo de trabajo «Personalizado/código» en la aplicación web AWS Transform.
3. Indique al agente el nombre de la definición de transformación que desea utilizar.
4. La aplicación web proporciona un comando AWS Transform CLI que se puede compartir con su equipo. Este comando invoca la definición de transformación y registra los resultados de la ejecución en la aplicación web.
5. Una vez capturados los resultados de la transformación, consulte las estadísticas, las medidas de ahorro de tiempo y formule preguntas sobre el progreso de su trabajo en el panel de control.

La aplicación web está diseñada para operaciones a escala empresarial en las que se necesita una supervisión centralizada de las transformaciones en múltiples bases de código.

Note

AWS Se requiere el IAM Identity Center para acceder a la aplicación web Transform. AWS La CLI no requiere el Centro de identidad de IAM; solo se necesitan AWS credenciales estándar.

Introducción a los comandos de transformación personalizados

Estos son algunos de los comandos que puede utilizar con las transformaciones personalizadas. La lista completa de comandos se encuentra en la [referencia de comandos AWS Transformar transformaciones personalizadas](#).

- `atx custom`
 - Ejecuta una experiencia interactiva de transformación personalizada, lo que permite la creación, el descubrimiento, la ejecución y el perfeccionamiento de las transformaciones.
 - Este es el comando predeterminado para `atx`
 - `--trust-all-tools(-t)` es opcional y permite implícitamente todas las solicitudes de herramientas solicitadas por el agente. Úselo con precaución, especialmente en entornos de producción. Puede configurar la confianza en las herramientas para herramientas y comandos específicos mediante el [archivo de configuración de confianza](#).
- `atx custom --help` | `atx custom -h`
 - Muestra el menú de ayuda.
 - Cada comando también incluye un menú de ayuda, por ejemplo, `atx custom def exec --help`.
- `atx --version` | `atx -v`
 - Muestra la versión.
 - El número de versión cambia con cada versión.
- `atx custom def list`
 - Imprime la lista de transformaciones disponibles en el registro de transformaciones.
- `atx custom def exec`
 - Ejecuta una transformación
- `atx custom def learnings`
 - Abre una sesión interactiva para ver y gestionar las lecciones que una transformación ha aprendido de las ejecuciones anteriores
- `atx mcp`
 - Se utiliza para administrar las configuraciones del servidor MCP

Flujos de trabajo

Ejecutando transformaciones

En esta sección se describen las diferentes formas de ejecutar las transformaciones y las opciones para controlar el comportamiento de la ejecución.

Modos de ejecución

AWS Transform custom admite tres modos de ejecución para adaptarse a diferentes flujos de trabajo.

Modo conversacional interactivo

Inicie la CLI con `atx` y pídale al agente que ejecute una transformación a través del lenguaje natural. Este modo le permite mantener una conversación completa con el agente, interrumpir la ejecución en cualquier momento y proporcionar comentarios durante el proceso de transformación.

Utilice este modo cuando desee tener el máximo control y la capacidad de guiar al agente a través de escenarios complejos.

Ejecución interactiva directa

Se utiliza `atx custom def exec -n <transformation-name> -p <path>` para iniciar una transformación específica de forma interactiva. Este modo le permite revisar el agente e interactuar con él al principio, durante o al final de la ejecución. El agente hará una pausa en los puntos clave de la decisión y le pedirá su opinión.

Esto es ideal para probar y refinar las transformaciones antes de ejecutarlas de forma autónoma.

Puede ejecutar las transformaciones en modo no interactivo o en modo headless. Non-interactive el modo suprime las solicitudes durante una transformación con nombre. El modo Headless permite ejecutar el agente con un mensaje de texto sin formato, sin tener que recurrir por completo a la interfaz interactiva.

Non-interactive modo

Úselo `atx custom def exec -n <transformation-name> -p <path> -x -t` para una automatización total. `-x` Añádalo para ejecutar en modo no interactivo y `-t` para confiar en todas las herramientas automáticamente sin preguntar.

Este modo está diseñado para la integración CI/CD de procesos y la ejecución masiva cuando no se requiere ni se requiere la intervención humana.

Modo Headless

Para completar las tareas sin interactuar con el agente, ejecute `atx -x "<prompt>" -t` y proporcione sus instrucciones en texto plano.

Ejecución de transformaciones sin interrupciones

Utilice este modo para aplicar una definición de transformación existente a su base de código. La transformación ejecuta cada paso automáticamente sin requerir su aprobación.

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

Desarrollo de una transformación sin precedentes

Cree o modifique las definiciones de transformación.

Para convertir una definición de transformación antigua al nuevo formato de habilidad (SKILL.md + referencias/), ejecute el siguiente comando:

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

Para crear una nueva definición de transformación, ejecute el siguiente comando:

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

Indicadores de comando comunes

Al ejecutar transformaciones con `atx custom def exec`, se suelen utilizar los siguientes indicadores:

- `-no--transformation-name`: especifica el nombre de la transformación que se va a ejecutar
- `-po --code-repository-path` - Especifica la ruta a su código base (utilice «.» para el directorio actual)

- `-co --build-command` - Especifica el comando de compilación o validación que se va a ejecutar
- `-xo --non-interactive` - Activa el modo no interactivo (sin solicitudes de usuario)
- `-to --trust-all-tools` - Confía automáticamente en todas las herramientas sin preguntar
- `-do --do-not-learn` - Impide que se extraiga la lección de esta ejecución
- `--tvo--transformation-version`: especifica una versión específica de la transformación
- `-go--configuration`: proporciona un archivo de configuración o una configuración en línea

Important

El `--trust-all-tools` indicador `-t` o aprueba automáticamente todas las ejecuciones de las herramientas sin solicitarlo y pasa por alto la mayoría de las barreras de seguridad (los comandos que coincidan con su `alwaysPromptCommands` lista aún requieren un permiso explícito a menos que los anule). `trustedShellCommands` Se transfiere `--non-interactive` y `--trust-all-tools` es obligatorio para una experiencia totalmente autónoma, pero no es obligatorio para ejecutar la transformación. Úsela con precaución en entornos de producción.

Uso de archivos de configuración

AWS Transform custom admite archivos de configuración opcionales en formato YAML o JSON. Los archivos de configuración permiten especificar los parámetros de ejecución y proporcionar contexto adicional al agente.

Para usar un archivo de configuración:

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

También puede proporcionar la configuración como pares clave-valor en línea:

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

Ejemplo de archivo de configuración (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
```

El `additionalPlanContext` parámetro proporciona un contexto adicional para el plan de ejecución del agente. Esto resulta especialmente útil con las transformaciones AWS gestionadas para personalizar su comportamiento en función de sus necesidades específicas.

Comandos de compilación y validación

El comando de compilación o validación es un parámetro opcional que especifica cómo validar el código durante el proceso de transformación. AWS Transform custom intentará deducir cuál es el mejor comando de compilación en función de la transformación si no se especifica, aunque se recomienda que sea específico para garantizar la calidad.

Ejemplos de comandos de compilación y validación:

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

Incluso para los lenguajes o las transformaciones que no requieren creación, es muy importante proporcionar un comando que valide los resultados y devuelva los problemas si la validación falla para mejorar la calidad de la transformación.

Si no es necesario compilar ni validar, omítelo en la entrada.

Controlar el comportamiento de aprendizaje

De forma predeterminada, AWS Transform custom extrae las lecciones de cada ejecución de transformación. Puede impedir el aprendizaje para determinadas ejecuciones.

Para evitar aprender de una ejecución:

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

El `--do-not-learn` indicador `-d` o no permite extraer lecciones de la ejecución actual.

Reanudar conversaciones

AWS Transform custom te permite reanudar las conversaciones anteriores en un plazo de 30 días a partir de su creación.

Para reanudar la conversación más reciente:

```
atx --resume
```

Para reanudar una conversación específica:

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

Important

Las conversaciones solo se pueden reanudar en un plazo de 30 días a partir de su creación. Transcurridos 30 días, la conversación ya no se podrá reanudar.

Rastreando las actas de

AWS Transform custom rastrea los [minutos de los agentes](#) consumidos durante una sesión de transformación. Los minutos de los agentes se acumulan a lo largo del ciclo de vida de la conversación y se muestran al finalizar la conversación:

```
Agent minutes used: 12.50
```

Los minutos de los agentes persisten a pesar de las interrupciones. Si interrumpe una sesión con `Ctrl+C` y la reanuda más tarde, los minutos acumulados anteriormente se acumulan y continúan acumulándose en la sesión reanudada.

Para consultar los minutos de los agentes durante una sesión interactiva:

Escriba `/usage` en el indicador de entrada para mostrar los minutos de agente acumulados actualmente sin finalizar la conversación.

Para establecer un límite presupuestario para los minutos de los agentes:

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

La `--limit` opción establece un presupuesto máximo de [minutos de agente](#) para la sesión. Los minutos del agente reflejan el tiempo de trabajo del agente activo, no el tiempo del reloj de pared. Cuando se alcanza el límite, la CLI muestra un mensaje y sale con instrucciones para reanudar:

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

Puede reanudar la conversación más adelante con un límite mayor:

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

Aprendizaje continuo

Esta sección describe cómo revisar y gestionar las lecciones creadas por el aprendizaje continuo.

Comprensión de las lecciones

El sistema de aprendizaje continuo extrae automáticamente las lecciones de las fases anteriores de una transformación. El sistema las crea de forma asíncrona en función de:

- Los comentarios de los desarrolladores se proporcionan en modo interactivo
- Problemas de código encontrados durante las transformaciones

Las lecciones se acumulan con el tiempo a medida que se ejecuta la transformación en diferentes bases de código. El sistema las aplica automáticamente para mejorar las carreras futuras. Cada lección pertenece a una categoría que contiene todas las lecciones de un dominio similar para que puedan repasar las lecciones relacionadas juntas. En el caso de las lecciones que no desee utilizar, puede archivar o eliminar la lección por completo.

Visualización y administración de las lecciones

Utilice el `learnings` comando para abrir una sesión interactiva para explorar y gestionar las lecciones de una definición de transformación.

Para abrir el visor de lecciones:

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

El visor se abre en una lista de categorías de lecciones, cada una de las cuales muestra cuántas lecciones activas contiene. Seleccione una categoría para ver sus lecciones y, a continuación, seleccione una lección para ver todos sus detalles, incluido el cuerpo de la lección, su impacto y el número de sesiones anteriores en las que se consultó.

Archivar y restaurar las lecciones

El sistema aplica las lecciones automáticamente. Si no desea que el sistema aplique una lección, puede archivarla. El sistema conserva las lecciones archivadas, pero no las aplica a futuras ejecuciones. Todas las lecciones archivadas se agrupan para que puedas revisarlas y volver a utilizarlas de forma activa.

Eliminar lecciones

Eliminar permanentemente una lección que no sea útil. La eliminación no se puede deshacer y el sistema podría volver a aprender la lección eliminada en futuras ejecuciones.

Una lección debe archivararse antes de poder eliminarla.

Configuración avanzada

En esta sección se describen las funciones avanzadas y las opciones de configuración de AWS Transform custom.

Variables de entorno

Puede personalizar el comportamiento de la CLI mediante variables de entorno.

Note

Los siguientes ejemplos muestran la sintaxis de Linux y macOS (`export`). En Windows, defina las variables de entorno en PowerShell uso `$env:NAME="value"`. Consulte las pestañas Windows (PowerShell) para ver los comandos equivalentes.

ATX_SHELL_TIMEOUT

Anula el tiempo de espera predeterminado para los comandos del shell (900 minutos). seconds/15

Linux and macOS

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

Windows (PowerShell)

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

Esto resulta útil para bases de código grandes o procesos de compilación de larga duración.

ATX_DISABLE_UPDATE_CHECK

Deshabilite las comprobaciones automáticas de versiones y las notificaciones de actualización durante la ejecución del comando.

Linux and macOS

```
export ATX_DISABLE_UPDATE_CHECK=true
```

Windows (PowerShell)

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

ATX_GIT_COMMITTER_NAME y ATX_GIT_COMMITTER_EMAIL

Configura la identidad del autor utilizada para las confirmaciones de puntos de control que Transform custom crea en tu repositorio a medida que aplica los cambios durante una transformación. AWS Cuando estas variables no están configuradas, las confirmaciones de puntos de control se atribuyen a una identidad predeterminada ()ATX Bot <checkpoint@atx.bot>. Configure ambas variables para atribuir los puntos de control a un 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"
```

Configuración de confianza

La configuración de confianza le permite preaprobar herramientas y comandos específicos para que se ejecuten sin tener que solicitarlo. También puede requerir un permiso explícito para comandos de shell específicos, independientemente del nivel de confianza. Estos ajustes se configuran en el archivo `~/.aws/atx/trust-settings.yaml`.

El archivo contiene tres listas:

- `trustedTools`- Herramientas que se pueden ejecutar sin preguntar
- `trustedShellCommands`- Comandos de shell que se pueden ejecutar sin preguntar
- `alwaysPromptCommands`- Patrones de comandos de shell que requieren un permiso explícito a menos que sean anulados por `trustedShellCommands`, independientemente del `-t` indicador o la confianza de la sesión. Estos patrones no se aplican en el modo no interactivo (`()`). `-x`

Herramientas de confianza predeterminadas:

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

Edición de la configuración de confianza:

Puedes editar manualmente el archivo `trust-settings.yaml` para añadir o eliminar herramientas y comandos de confianza. Ambos admiten el uso de patrones comodín `trustedShellCommands` globosos. `alwaysPromptCommands *`

Note

Si un comando coincide con ambas listas, `trustedShellCommands` tiene prioridad.

A continuación se describe cada lista de comandos y se proporcionan ejemplos:

- `trustedShellCommands`- Los comandos que coincidan con estos patrones se ejecutan sin que se les pida permiso y se saltan todas las demás barreras de seguridad. Los patrones se comparan con los de toda la cadena de comandos.

Ejemplos:

- `cd *`- Coincide con los comandos compuestos que comienzan por `cd`
- `*&&*`- Confía en todos los comandos con operadores `&&`
- `alwaysPromptCommands`- Los comandos que coincidan con estos patrones requieren un permiso explícito a menos que sean anulados por `trustedShellCommands`, independientemente del `-t` indicador o la confianza de la sesión. Estos patrones no se aplican en el modo no interactivo (`()`). `-x` Los patrones se comparan con cada subcomando en las expresiones compuestas (sustituciones de comandos `&& | | ,`).

Ejemplos:

- `rm -rf *`- Siempre solicita comandos recursivos de borrado forzado
- `sudo *`- Siempre solicita que los comandos se ejecuten con `sudo`
- `find * -exec *`- Siempre solicita comandos de búsqueda con `-exec`

Session-level confianza:

Durante las indicaciones interactivas, puede elegir:

- `(y)es`- Ejecutar una vez
- `(n)o`- Denegar
- `(t)rust`- Confianza solo para la sesión actual

Session-level la configuración de confianza es temporal y se restablece cuando se reinicia la CLI, lo que proporciona una aprobación temporal sin modificar permanentemente `trust-settings.yaml`.

Note

La confianza en la sesión no está disponible para los comandos que coincidan con tu lista. `alwaysPromptCommands`

Servidores Model Context Protocol (MCP)

La CLI de AWS Transform es compatible con los servidores del Model Context Protocol (MCP), que amplían su funcionalidad con herramientas adicionales.

Configuración:

Configure los servidores MCP en el `~/.aws/atx/mcp.json` archivo. La CLI de AWS Transform admite dos tipos de servidores MCP: servidores locales basados en comandos y servidores HTTP remotos.

Servidores locales basados en comandos:

Los servidores locales se ejecutan como procesos secundarios en su máquina. Configúrelos con la `command` propiedad:

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

Servidores HTTP remotos:

Los servidores remotos se conectan a servidores MCP alojados en una URL HTTP o HTTPS. Configúrelos con la `url` propiedad:

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

La `headers` propiedad es opcional y admite la expansión de variables de entorno mediante la `${VAR_NAME}` sintaxis. Esto le permite almacenar valores confidenciales, como los tokens de API, en las variables de entorno en lugar de guardarlos en el archivo de configuración.

Propiedades de configuración:

Los servidores locales basados en comandos admiten las siguientes propiedades:

- `command`(obligatorio): el comando para ejecutar el servidor
- `args`(opcional) - Matriz de argumentos de la línea de comandos
- `env`(opcional): variables de entorno para pasarlas al proceso del servidor

Los servidores HTTP remotos admiten las siguientes propiedades:

- `url`(obligatorio): la URL HTTP o HTTPS del servidor MCP remoto
- `headers`(opcional): encabezados HTTP para incluir en las solicitudes, con soporte para la expansión de variables de `${VAR_NAME}` entorno

Administración de servidores MCP:

Vea la lista de servidores MCP configurados:

```
atx mcp tools
```

Enumere las herramientas disponibles que ofrece un servidor MCP específico:

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

Seguimiento del uso:

La CLI rastrea automáticamente el uso de la herramienta MCP durante las ejecuciones de la transformación. Las estadísticas de uso se conservan al igual que `mcp_usage.json` en el directorio de conversaciones. `metadata.json` El archivo registra las métricas por herramienta para cada ejecución, incluidas las siguientes:

- Número de invocaciones por herramienta
- Número de errores por herramienta
- Tiempo total de ejecución por herramienta

- Detalles del último error (si lo hubiera)

Client-Side Habilidades

Client-side las habilidades son capacidades adicionales que amplían al agente durante las ejecuciones de transformación. Permiten proporcionar herramientas, scripts e instrucciones personalizados que el agente puede utilizar junto con sus funciones integradas.

Directorios de descubrimiento de habilidades:

Las habilidades se descubren en cuatro directorios en orden de prioridad. Si una habilidad con el mismo nombre existe en varios directorios, el primer directorio de la lista tiene prioridad:

1. <project>/aws/atx/skills/- Project-level, AWS Transformar CLI-specific
2. <project>/agents/skills/- Project-level, multicliente (disponible para cualquier herramienta de agente compatible)
3. ~/.aws/atx/skills/- User-level, Transformar AWS CLI-specific
4. ~/.agents/skills/- User-level, multicliente (disponible para cualquier herramienta de agente compatible)

Los .aws/atx/skills/ directorios son específicos de la CLI de AWS transformación. Los .agents/skills/ directorios son multicliente, lo que significa que las habilidades colocadas allí están disponibles para cualquier herramienta de agente compatible más allá de la AWS CLI de Transform.

Estructura del directorio de habilidades:

Cada habilidad es un directorio que contiene un SKILL.md archivo con la información preliminar de 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...
```

El name campo debe coincidir con el nombre del directorio principal.

Desactivar una habilidad:

Para evitar que una habilidad se cargue sin eliminar sus archivos, añade `disable-model-invocation: true` a la portada lo siguiente:

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

Cuando se establece esta propiedad, la CLI omite la habilidad durante el descubrimiento. El agente no puede ver ni utilizar la habilidad a menos que una definición de transformación le indique explícitamente que lea el archivo de habilidades. Utilízalo para desactivar temporalmente una habilidad, marcarla como en progreso o conservar material de referencia destinado únicamente a lectores humanos.

Note

Los archivos de una habilidad desactivada permanecen en el disco. Si una definición de transformación indica al agente que lea una ruta de archivo específica, el agente podrá seguir accediendo al contenido. La `disable-model-invocation` propiedad impide la detección automática y la inyección de contexto, no el acceso al sistema de archivos.

Disponibilidad de habilidades por modo de ejecución:

- Modo ejecutivo (`atx custom def execon--code-repository-path`): descubre habilidades en directorios a nivel de usuario y de proyecto.

- Modo interactivo (atx): inicialmente solo se descubren las habilidades a nivel de usuario. Al proporcionar una ruta al repositorio de código durante la sesión, también se cargan las habilidades a nivel de proyecto.

Verificar el descubrimiento de habilidades:

Consulte el registro de depuración de la CLI después de una ejecución para comprobar qué habilidades se descubrieron:

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
```

Las habilidades que no pasan la validación se omiten con una advertencia en los registros de depuración.

Note

Client-side las habilidades requieren CLI versión 2.0 o posterior.

Elegir entre Project-Level y User-Level habilidades

El lugar donde coloques una habilidad determina quién se beneficia de ella y cuándo se activa.

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

Compromételas al control de versiones para que cada miembro del equipo que ejecute transformaciones en el repositorio las descubra automáticamente. Usa tus habilidades a nivel de proyecto para:

- Repository-specific comprobaciones de cumplimiento (reglas de Dockerfile, políticas de Terraform, validadores de seguridad en materia de migración)

- Estándares de codificación organizacional que se aplican a esta base de código (patrones de observabilidad, manejo de errores, convenciones de nomenclatura)
- Cree o pruebe scripts exclusivos del proyecto (linters personalizados, funciones de adecuación de la arquitectura)
- Guías de migración de API para las bibliotecas internas utilizadas en este repositorio

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

Permanecen en su máquina y se activan durante todas las transformaciones, independientemente del repositorio al que se dirija. Utilice sus habilidades a nivel de usuario para:

- Herramientas de flujo de trabajo personales (generadores de registros de cambios, formateadores de mensajes de confirmación)
- Cross-project preferencias (patrones de prueba preferidos, recordatorios de estilo de documentación)
- Las comprobaciones de conformidad de las licencias que su organización exige en todos los repositorios
- Umbrales de cobertura o límites de calidad que impongas en cada base de código con la que trabajes

Consejos para desarrollar habilidades eficaces:

- Escribe `description` campos claros en tu `SKILL.md` portada. El agente usa este campo para decidir cuándo una habilidad es relevante.
- Cierre los scripts de validación con el código 0 en caso de éxito y distinto de cero en caso de error. El agente interpreta los códigos de salida para determinar el cumplimiento.
- Imprima mensajes de error claros y procesables en los scripts. El agente lee los resultados para saber qué corregir.
- Coloque las habilidades en el directorio multicliente (`.agents/skills/`) en cualquier nivel para compartirlas con otras herramientas de desarrollo de IA además de la CLI de AWS Transform.

Client-Side Ejemplos de habilidades

Estos ejemplos muestran dos patrones comunes: una habilidad de validación basada en guiones y una habilidad solo de referencia.

Ejemplo: Dockerfile Compliance Checker () Script-Based

Esta habilidad valida los archivos de Dockerfiles según las mejores prácticas operativas y de seguridad. Utiliza un script de validación que el agente ejecuta antes y después de realizar los cambios.

Estructura de directorios:

```
.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.
```

El script de validación comprueba si hay etiquetas de imagen base no ancladas, si se ejecutan como root, si hay secretos codificados en ENV las directivas o si faltan definiciones. HEALTHCHECK El

agente ejecuta el script, corrige las infracciones utilizando patrones del archivo de referencia y vuelve a ejecutar el script para confirmar su conformidad.

Ejemplo: API Deprecation Helper () Reference-Only

Esta habilidad guía al agente a reemplazar las llamadas a la API obsoletas durante las transformaciones de la actualización. Utiliza solo archivos de referencia sin scripts.

Estructura de directorios:

```
.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
```

Los archivos de referencia contienen ejemplos de código del antes y el después. Por ejemplo, `aws-sdk-v2-to-v3.md` mapea patrones similares `s3.putObject(params).promise()` a los del equivalente modular de la versión 3 utilizando `y.S3Client PutObjectCommand`

Etiquetas y organización

Puede organizar las transformaciones con etiquetas para el control de acceso y la categorización.

Note

Algunos de estos comandos requieren especificar el nombre de recurso de Amazon (ARN) para una definición de transformación. La estructura del ARN es: `arn:aws:transform-custom:<region>:<account-id>:package/<td-name>`

Para enumerar las etiquetas de una transformación:

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

Para añadir etiquetas a una transformación:

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

Para eliminar etiquetas de una transformación:

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

Las etiquetas se pueden utilizar para el control de acceso agrupado en las políticas de IAM. Puede crear políticas que concedan permisos a todas las transformaciones con etiquetas específicas (por ejemplo, todas las transformaciones etiquetadas con `team:frontend` o `environment:production`).

Registros

AWS La CLI de Transform mantiene tres tipos de registros para la solución de problemas y la depuración.

Registros de conversaciones:

Linux and macOS

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

Windows

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

Estos registros contienen el historial completo de conversaciones de una sesión específica.

Registros de subagentes:

Linux and macOS

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

Windows

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

Estos registros contienen los resultados de los subagentes que el agente principal genera durante las transformaciones. No es necesario gestionar los subagentes directamente.

Registros de depuración de desarrolladores:

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
```

Estos registros proporcionan información avanzada de solución de problemas para la propia CLI.

 Note

Es posible que haya varios archivos de registro de depuración en el directorio de registros (por ejemplo, debug1.log o debug2.log). Revise y proporcione todos los registros relevantes, por ejemplo, `~/ .aws/atx/custom/ /*` y `<conversation-id>~/ .aws/atx/logs/ *`, al abrir los tickets de soporte para una resolución más rápida.

Actualizaciones de CLI

Mantenga su CLI actualizada para acceder a nuevas funciones y mejoras.

Para comprobar si hay actualizaciones:

```
atx update --check
```

Para actualizar a la versión más reciente:

```
atx update
```

Para actualizar a una versión específica:

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

Cree transformaciones personalizadas

En esta sección se describe cómo crear, modificar y administrar las definiciones de transformación personalizadas.

Crear una nueva transformación

Utilice la CLI interactiva para crear una nueva definición de transformación.

Para crear una definición de transformación

1. Inicie la CLI de AWS transformación:

```
atx
```

2. Dígale al agente que quiere crear una nueva transformación.
3. Proporcione una descripción clara y detallada del objetivo de la transformación. Incluya:
 - El estado de origen y destino (por ejemplo, «actualizar de la versión X a la versión Y»)
 - Se requieren cambios específicos (por ejemplo, «actualizar las declaraciones de importación, reemplazar los métodos obsoletos»)
 - ¿Alguna consideración o restricción especial
4. Cuando el agente solicite aclaraciones o información adicional, proporcione ejemplos específicos y materiales de referencia.
5. Revise la definición de transformación inicial creada por el agente.
6. Pruebe la transformación en una base de código de muestra.
7. Realice una iteración proporcionando comentarios, correcciones de código o ejemplos adicionales.
8. Guarde la transformación localmente o publíquela en el registro.

Mejores prácticas para crear transformaciones:

- Comience con transformaciones simples y bien definidas antes de intentar transformaciones complejas
- Proporcione materiales de referencia completos, incluidas guías de migración y ejemplos de códigos
- Pruebe con varios ejemplos de bases de código antes de publicarlos
- Utilice comandos deterministas de construcción o validación para permitir el aprendizaje continuo
- Considere dividir las transformaciones complejas en varios pasos más pequeños
- Marque la información crucial con «CRÍTICA:» o «IMPORTANTE:» en sus definiciones de transformación para asegurarse de que el agente priorice estos requisitos
- Cuando necesite cumplir requisitos exactos (como usar un comando o un valor de cadena específico), especifique explícitamente la cadena completa en sus definiciones de transformación. Puedes ponerlos entre comillas bash para indicar claramente que se trata de comandos de terminal o cadenas literales, lo que reduce la variabilidad y garantiza una ejecución coherente

Proporcionar materiales de referencia

Puede proporcionar archivos de referencia a AWS Transform custom especificando las rutas de los archivos durante la conversación. Estos archivos se almacenan en la `references/` carpeta de la definición de transformación.

Tipos de archivos de referencia recomendados:

- Before/after código de ejemplo
- Documentación de las API, bibliotecas o funciones involucradas
- Human-readable guías de migración

Para proporcionar un archivo de referencia:

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

También puede proporcionar un directorio que contenga varios archivos de referencia:

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

Note

Solo se admiten archivos basados en texto (.md, .html, .txt, archivos de código). Los archivos binarios, las imágenes y los archivos de texto enriquecido (por ejemplo, .pdf, .png, .docx) no son compatibles actualmente. A menudo es posible extraer el contenido del texto y usarlo como referencia. Si tiene muchos archivos de texto pequeños, considere la posibilidad de concatenarlos en unos pocos archivos con nombres descriptivos. Hay un límite de 10 MB en total para todos los archivos.

Modificación de una transformación existente

Puede modificar las transformaciones personalizadas antes y después de guardarlas como borradores o publicarlas. No puede modificar las transformaciones AWS gestionadas por terceros. Si necesita personalizarlas, puede proporcionar contexto adicional mediante el archivo de configuración.

Para modificar una transformación existente

1. Inicie la CLI de AWS transformación:

```
atx
```

2. Dígame al agente que desea modificar una transformación existente.

3. Elija si desea:

- Proporcione una ruta de archivo a una transformación almacenada localmente (es decir, no a un borrador guardado o publicado)
- Solicite la lista de transformaciones del registro

4. Si elige una transformación del registro, seleccione la transformación que desee modificar.

5. Trabaje con el agente para describir los cambios que desea realizar.

6. Pruebe la transformación actualizada en una base de código de muestra.

7. Publique las actualizaciones en el registro si lo desea.

Publicar y gestionar las transformaciones

Puede publicar y gestionar sus transformaciones mediante la experiencia interactiva o con los siguientes comandos.

Para guardar una transformación como borrador:

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

Para publicar una transformación:

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

Para ver una lista de las transformaciones disponibles:

```
atx custom def list
```

Para descargar una definición de transformación:

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


De este modo, se descarga la definición de transformación en su directorio de trabajo actual. Puede especificar un directorio de destino con la `--td` marca y una versión con la `--tv` marca.

Para eliminar una definición de transformación:

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

Important

De esta forma, se elimina permanentemente la definición de transformación especificada de su cuenta.

Gestión de las versiones de transformación

AWS Transform custom mantiene las versiones de sus definiciones de transformación. Puede especificar una versión al ejecutar o descargar una transformación.

Para ejecutar una versión específica:

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

Para descargar una versión específica:

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

Si no se especifica ninguna versión, se utiliza la versión más reciente.

Referencia de comandos

Esta sección proporciona una referencia completa de todos los comandos CLI personalizados de AWS Transform.

Comandos interactivos

atx

Inicie una conversación interactiva con la CLI de 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 sesión interactivos

Los siguientes comandos se pueden escribir en la línea de entrada durante una sesión interactiva:

- /usage- Muestra los [minutos de agente](#) acumulados en la sesión actual

Comandos de definición de transformaciones

atx custom def exec

Ejecute una definición de transformación en un repositorio de código.

Opción	Formulario largo	Parámetro	Description (Descripción)
-p	--code-repository-path	<path>	Ruta al repositorio de código que se va a transformar. Para el directorio actual, utilice «.»
-c	--build-command	<command>	Comando que se ejecuta al crear el repositorio
-n	--transformation-name	<name>	Nombre de la definición de transformación en el registro
-x	--non-interactive	-	Ejecuta la transformación sin la asistencia del usuario
-t	--trust-all-tools	-	Confía en todas las herramientas (no

Opción	Formulario largo	Parámetro	Description (Descripción)
			hay solicitudes de herramientas)
-d	--do-not-learn	-	Opte por no permitir la extracción de lecciones de esta ejecución
-g	--configuration	<config>	Ruta al archivo de configuración (JSON o YAML) o a los pares clave=valor
--tv	--transformation-version	<version>	Versión de la definición de transformación que se va a utilizar
--limit	--limit	<limit>	Establezca el límite presupuestario de Agent Minutes . La transformación finaliza cuando se alcanza el límite y se puede reanudar con un límite aumentado
-h	--help	-	Muestra la ayuda para el comando

lista de definición personalizada atx

Enumere las definiciones de transformación disponibles.

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

atx custom def get

Obtenga detalles de una definición de transformación específica.

Opción	Formulario largo	Parámetro	Description (Descripción)
-n	--transformation-name	<name>	El nombre de la definición de transformación que se va a recuperar
--tv	--transformation-version	<version>	La versión de la definición de transformación que se va a recuperar
--td	--target-directory	<directory>	El directorio de destino en el que se va a guardar la definición de transformación (predeterminado: «.»)
--json	--json	-	Respuesta de salida en formato JSON
-h	--help	-	Muestra la ayuda para el comando

atx custom def delete

Elimine una definición de transformación de forma permanente.

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

atx custom def publish

Publica una definición de transformación en el registro.

Opción	Formulario largo	Parámetro	Description (Descripción)
-n	--transformation-name	<name>	El nombre de la definición de transformación que se va a publicar
--tv	--transformation-version	<version>	La versión de la definición de transformación que se va a utilizar (no se aplica a --description ni a --source-directory)
--sd	--source-directory	<directory>	El directorio de origen desde el que leer los archivos de definición de transformación locales (no se aplica a --transformation-version)
--description	--description	<description>	Una descripción de la definición de transformación (no aplicable a --transformation-version)
--json	--json	-	Respuesta de salida en formato JSON
-h	--help	-	Muestra la ayuda para el comando

borrador guardado de atx custom def

Guarde una definición de transformación como borrador en el registro. Los borradores caducan a los 30 días y no aparecen en el registro. Este comando devuelve el número de versión del borrador. Debe ejecutar y recuperar los borradores de forma explícita utilizando el nombre de la transformación y el número de versión.

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

Comandos de la lección

Aprendizajes de definición personalizada de atx

Abra una sesión interactiva para ver y gestionar las lecciones que una definición de transformación ha aprendido de ejecuciones anteriores. Busque las lecciones por categoría, vea los detalles de las lecciones y archive, restaure o elimine las lecciones.

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

Etiquete los comandos

etiquetas de lista de definición personalizadas atx

Enumere las etiquetas de una definición de transformación.

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

etiqueta de definición personalizada atx

Añada etiquetas a una definición de transformación.

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

etiqueta de definición personalizada atx

Eliminar etiquetas de una definición de transformación.

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

Comandos de actualización

actualización de impuestos

Actualice la CLI de AWS transformación.

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

Comandos MCP

herramientas atx mcp

Permite a los clientes configurar view/confirm sus herramientas MCP. Las actualizaciones de las configuraciones se deben gestionar directamente a través del archivo ~/.aws/atx/mcp.json

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

AWS-Transformaciones gestionadas

AWS-las transformaciones gestionadas son transformaciones prediseñadas y AWS examinadas para casos de uso comunes que están listas para usarse sin necesidad de ninguna configuración adicional.

Descripción general de

AWS-las transformaciones gestionadas tienen las siguientes características:

- Validadas por AWS: estas transformaciones han sido verificadas por AWS ser de alta calidad
- Listo para usar: no se requiere ninguna configuración adicional
- Crecimiento continuo: se añaden continuamente transformaciones adicionales
- Personalizable: Pre-built las transformaciones se pueden personalizar proporcionando orientación o requisitos adicionales específicos para las necesidades de su organización mediante el parámetro `additionalPlanContext` de configuración
- Soporte de acceso anticipado: algunas transformaciones pueden marcarse como de acceso anticipado a medida que se someten a pruebas y mejoras adicionales

Disponible AWS-Transformaciones gestionadas

El siguiente catálogo enumera las transformaciones AWS administradas que están disponibles actualmente, agrupadas por caso de uso. Cada tabla muestra el nombre de la transformación, el idioma o la pila a la que se aplica y su estado. Para encontrar una transformación rápidamente, usa el cuadro de búsqueda de la parte superior de esta página para buscar por nombre, idioma o caso de uso.

Este catálogo es la lista canónica de transformaciones AWS gestionadas. El Kiro Power, el complemento del agente, el complemento VS Code y la CLI ejecutan las mismas transformaciones. Para enumerar las transformaciones disponibles en su registro, ejecute `atx custom def list`.

Note

Las transformaciones marcadas como Acceso anticipado son funcionales, pero es posible que se actualicen con frecuencia en función de los comentarios de los clientes.

Actualizaciones en el tiempo

Actualice un idioma o un motor de ejecución a una versión más reciente, o cambie la distribución del tiempo de ejecución.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/java-version-upgrade	Java	Disponibilidad general	Actualice las aplicaciones Java con cualquier sistema de compilación, desde cualquier versión de JDK de origen a cualquier versión de JDK de destino, con la modernización de las dependencias, incluida la migración a Jakarta EE, los

Transformación	Idioma/pila	Status	Description (Descripción)
			controladores de bases de datos, los marcos ORM y las actualizaciones del ecosistema Spring. Especifique la versión del JDK de destino en el chat o con el parámetro <code>.additionalPlanContext</code>
AWS/python-version-upgrade	Python	Disponibilidad general	Migre los proyectos de Python de Python 3.8 o 3.9 a Python 3.11, 3.12 o 3.13 sin perder la funcionalidad y el rendimiento. Especifique la versión de Python de destino en el chat o con el <code>additionalPlanContext</code> parámetro.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/nodejs-version-upgrade	Node.js	Disponibilidad general	Actualice Node.js las aplicaciones desde cualquier Node.js versión de origen a cualquier Node.js versión de destino. Especifique la versión de destino en el chat o con el additionalPlanContext parámetro.
AWS/lambda-nodejs-runtime-upgrade	Node.js (Lambda)	Acceso anticipado	Actualice las funciones de AWS Lambda de los entornos de Node.js ejecución más antiguos (de nodejs4.3 a nodejs22.x) a nodejs24.x para abordar los cambios importantes en el cliente de interfaz de ejecución de Lambda (RIC) y en el motor de ejecución de 24 idiomas. Node.js

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/oracle-java-to-corretto	Java (distribución JDK)	Acceso anticipado	Migre proyectos Java de Oracle JDK a Amazon Corretto. Sustituye las API Oracle-specific internas por equivalentes estándar de Java, actualiza las configuraciones de compilación (Maven y Gradle) y las imágenes base de contenedores, elimina los indicadores comerciales de JVM y genera un informe de licencias.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/ruby-upgrade	Ruby	Acceso anticipado	Actualice las aplicaciones de Ruby de Ruby 2.x a Ruby 4.0 y sus marcos a Rails 8.0 o Sinatra 4.1. Puedes usar esta transformación con Rails y ActiveRecord aplicaciones, aplicaciones de Sinatra y gemas independientes. La transformación combina cada mejora de la versión de Ruby con la actualización del marco correspondiente y ejecuta el conjunto de pruebas. Luego aísla las fallas antes de pasar a la siguiente versión.

Migraciones de SDK

Migre entre las versiones principales de un AWS SDK.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/java-aws-sdk-v1-to-v2	Java	Disponibilidad general	Actualice el AWS SDK de la versión 1 a la versión 2 para

Transformación	Idioma/pila	Status	Description (Descripción)
			proyectos de Java con Maven o Gradle.
AWS/python-boto2-to-boto3	Python	Disponibilidad general	Migre las aplicaciones de Python de boto2 a boto3, según la documentación oficial de migración. AWS
AWS/nodejs-aws-sdk-v2-to-v3	Node.js	Disponibilidad general	Actualice Node.js las aplicaciones del AWS SDK de la versión JavaScript 2 a la versión 3 para obtener una arquitectura modular, un TypeScript soporte de primera clase y un rendimiento mejorado, sin cambiar la versión. Node.js

Actualizaciones y migraciones del marco

Actualice un marco a una versión más reciente o migre a un marco diferente.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/spring-boot-version-upgrade	Java/Spring Boot	Disponibilidad general	Actualice una aplicación anterior de Spring Boot a una versión de Spring Boot de destino,

Transformación	Idioma/pila	Status	Description (Descripción)
			incluidos los archivos de compilación y los elementos de arranque, las propiedades, los paquetes Jackson 3, el DSL de Spring Security 7, la infraestructura de pruebas y las dependencias de observabilidad.
AWS/JBoss-to-Spring-Boot	Java (JBoss o Spring Boot) WildFly	Acceso anticipado	Migre las aplicaciones empresariales Java EE o Jakarta EE que se ejecutan en JBoss EAP o WildFly Spring Boot, eliminando las dependencias del servidor de aplicaciones y optando por un modelo de despliegue en contenedores nativo de la nube.
AWS/early-access-angular-to-react-migration	De Angular a React	Acceso anticipado	Transforma una aplicación angular en React.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/angular-version-upgrade	Angular	Acceso anticipado	Actualice una aplicación Angular anterior a una versión Angular de destino, que incluya componentes, servicios, plantillas y enrutamiento.
AWS/vue.js-version-upgrade	Vue.js	Acceso anticipado	Realice una actualización de la versión principal de Vue.js 2 a Vue.js 3, modernizando los componentes, la administración del estado, el enrutamiento y las API globales. Las actualizaciones menores y las actualizaciones de parches están fuera del alcance.

Migraciones de GenAI y modelos

Migre las cargas de trabajo de IA generativa a.

Transformación	Idioma o pila	Status	Description (Descripción)
AWS/GenAI-to-Bedrock-Migration-Assessment	Cargas de trabajo de IA generativas	Acceso anticipado	Evalúe las cargas de trabajo generativas de IA para la migración de proveedores

Transformación	Idioma o pila	Status	Description (Descripción)
			externos (OpenAI, Google Gemini, Anthropic direct y modelos de código abierto) a. Descubre el uso y los modelos del SDK, aclara los requisitos, diseña un mapeo de modelos, estima los costos y los riesgos y genera artefactos de evaluación. Assessment-only; no modifica el código fuente. También cubre marcos de agentes como CrewAI y Strands. LangGraph

Language-to-language migraciones

Traduce una base de código de un lenguaje de programación a otro.

Transformación	Lenguaje/pila	Status	Description (Descripción)
AWS/vba-to-python-migration	VBA a Python	Acceso anticipado	Migre las macros UserForms, los módulos y la lógica integrada de Excel VBA a scripts y módulos de Python equivalentes,

Transformación	Lenguaje/pila	Status	Description (Descripción)
			mediante openpyxl, pandas, tkinter o PyQt 6 y bibliotecas estándar. El lenguaje de destino es Python 3.8 o posterior. Úselo al convertir código VBA embebido en .bas, .cls, .frm o .xlsm.

Migraciones de bases de datos

Actualmente, no hay disponibles transformaciones AWS administradas específicas de la base de datos. Para modernizar las bases de datos de Microsoft SQL Server y sus aplicaciones.NET asociadas a Amazon Aurora PostgreSQL, consulte. [the section called “Modernización de SQL Server”](#)

Observabilidad

Modernice el registro y la supervisión a servicios nativos. AWS

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/early-access-log4j-to-slf4j-migration	Java (registro)	Acceso anticipado	Migre las aplicaciones Java de Log4j (1.x o 2.x) a SLF4J con un backend Logback. Gestiona el código fuente, la gestión de dependencias (Maven y Gradle) y el registro de los archivos de

Transformación	Idioma/pila	Status	Description (Descripción)
			configuración, y los valida mediante compilación, prueba y escaneo de importaciones residuales.
AWS/datadog-monitors-to-cloudwatch-alarms	Infraestructura como código o monitoreo	Acceso anticipado	Migre los monitores de DataDog métricas que rastrean las métricas de AWS servicio y las métricas personalizadas a CloudWatch alarmas nativas, tanto de infraestructura como de código. Genera CloudFormation YAML, CDK TypeScript y Terraform HCL.

Arquitectura

Re-architect, rediseñe la plataforma u optimice las aplicaciones para. AWS

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/java-performance-optimization	Java (rendimiento)	Disponibilidad general	Optimice el rendimiento de las aplicaciones Java analizando los datos de creación de perfiles JFR para detectar los puntos

Transformación	Idioma/pila	Status	Description (Descripción)
			de acceso y los antipatrones de la CPU y la memoria y, a continuación, aplique correcciones de código específicas. Para obtener instrucciones sobre cómo recopilar datos de JFR, consulte la guía de tiempo de ejecución de JFR.
AWS/early-access-java-x86-to-graviton	Java (Arm64/Graviton)	Acceso anticipado	Valide la compatibilidad de las aplicaciones Java con la arquitectura Arm64 para los procesadores AWS Graviton y resuelva las incompatibilidades actualizando las dependencias, detectando patrones de código específicos de la arquitectura y recompilando las bibliotecas nativas cuando el código fuente esté disponible. Muchas aplicaciones Java modernas ya lo están. Arm64-compatible

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/oracle-service-bus-to-aws	Integración de Java/sin servidor	Acceso anticipado	Migre las configuraciones de los procesos Oracle Service Bus (OSB) y BPEL a una arquitectura AWS nativa sin servidor y genere un proyecto de CDK desplegable con Amazon TypeScript API Gateway, AWS Lambda y Step Functions. AWS

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/mulesoft-to-aws-native	Java//a una versión sin servidor MuleSoft	Acceso anticipado	Transforme las aplicaciones MuleSoft Mule 3.x y 4.x en arquitecturas AWS sin servidor (Amazon API Gateway, Lambda AWS y Step AWS Functions) orientadas a Java 17 en Lambda con. AWS SnapStart La transformación asigna los activadores de flujo a las fuentes de AWS eventos, convierte DataWeave las expresiones MEL (lenguaje de MuleSoft expresión) en AWS equivalentes y reemplaza los conectores por llamadas a AWS SDK for Java v2. Produce plantillas SAM, controladores AWS Lambda y pruebas JUnit 5.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/payshield-hsm-to-aws-payment-cryptography	Java (desde HSM hasta criptografía de pagos) AWS	Disponibilidad general	Migre las aplicaciones Java del protocolo del módulo de seguridad de PayShield hardware (HSM) de Thales al SDK de criptografía de AWS pagos v2. La migración incluye el mapeo de comandos, la migración de claves, la configuración de dependencias y las pruebas de paridad.

Análisis de código base

Analice las bases de código y las carteras para planificar la modernización. Estas transformaciones producen informes y no modifican el código.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/comprehensive-codebase-analysis	Múltiples idiomas	Disponibilidad general	Realice un análisis estático profundo de una base de código para generar documentación jerárquica con referencias cruzadas que combine el análisis del

Transformación	Idioma/pila	Status	Description (Descripción)
			comportamiento, la documentación arquitectónica y la inteligencia empresarial, haciendo hincapié en la información técnica sobre la deuda.
AWS/agentic-readiness-analysis	Múltiples idiomas	Acceso anticipado	Evalúe si los sistemas están preparados para que los agentes de IA los llamen de forma segura, incluyendo las API, la identidad, la gestión del estado, la interacción humana y la observabilidad.
AWS/modernization-readiness-analysis	Múltiples idiomas	Acceso anticipado	Escanee las carteras para detectar las brechas de madurez de los entornos nativos de la nube y mapee los hallazgos con las vías de AWS modernización.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/portfolio-agentic-readiness-analysis	Portafolio	Acceso anticipado	Combine los informes de análisis individuales de la preparación de los agentes en una cartera de aplicaciones para identificar los obstáculos transversales, los patrones de remediación compartidos y las recomendaciones priorizadas.
AWS/portfolio-modernization-readiness-analysis	Portafolio	Acceso anticipado	Combine los informes de análisis de modernización individuales de una cartera en una hoja de ruta consolidada con las oleadas de migración priorizadas y las vías de modernización recomendadas.

Transformación	Idioma/pila	Status	Description (Descripción)
AWS/business-rules-extraction	Múltiples idiomas	Acceso anticipado	Esta transformación analiza de forma estática una base de código monolítica para producir documentación lista para su reescritura sin necesidad de compilar, ejecutar o modificar el código fuente. Descompone el sistema en dominios acotados y extrae las reglas empresariales, los flujos de trabajo, las preocupaciones transversales y la estructura de la base de datos por dominio. El resultado incluye un manifiesto legible por máquina, un panel interactivo y especificaciones de implementación independientes del idioma por dominio para guiar la modernización o la reescritura completa.

Personalización AWS-Transformaciones gestionadas

Puede personalizar las transformaciones AWS administradas para satisfacer las necesidades específicas de su organización proporcionando un contexto adicional a través del parámetro de `additionalPlanContext` configuración.

Ejemplo: personalizar la actualización de la versión de 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.
```

Ejemplo: personalizar AWS la migración del 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 común

Esta sección proporciona una guía paso a paso para los escenarios de transformación comunes mediante la CLI de AWS transformación.

Actualizaciones de Lambda Runtime

Lambda desaprueba periódicamente los tiempos de ejecución de lenguajes más antiguos, lo que obliga a los equipos a actualizar sus funciones de Lambda a versiones compatibles. AWS Transform custom puede automatizar estas actualizaciones mediante las transformaciones de actualización de las versiones de idiomas AWS gestionadas. Por ejemplo, para actualizar una función Lambda escrita en Python 3.9 a Python 3.13, utilizaría la transformación. `AWS/python-version-upgrade` Hay transformaciones similares disponibles para Java (`AWS/java-version-upgrade`) y Node.js (`AWS/nodejs-version-upgrade`), que abarcan los lenguajes de ejecución Lambda más comunes.

Para actualizar una sola función de Lambda de forma interactiva, vaya a la raíz del repositorio de origen de la función e inicie la AWS CLI de transformación con. `atx` En la sesión interactiva, describa la actualización que necesita, por ejemplo, «Actualice esta función Lambda de Python 3.9 a Python 3.13». El agente seleccionará la transformación AWS gestionada adecuada, analizará el código, actualizará la sintaxis del lenguaje, ajustará las dependencias y modernizará las llamadas a la API obsoletas. Puede proporcionar un comando de compilación o validación para que el agente pueda comprobar `python -m py_compile *.py` que el código transformado se compila y supera las pruebas. `pytest` A lo largo de la sesión interactiva, puede revisar los cambios propuestos por el agente, enviar comentarios y solicitar ajustes antes de aceptar el resultado final.

Cuando necesite actualizar los tiempos de ejecución de Lambda en muchos repositorios, utilice el modo no interactivo para ejecutar transformaciones a escala. Para cada repositorio, invoque la CLI con los indicadores adecuados para que se ejecute sin la intervención del usuario. Por ejemplo, para actualizar una función de Node.js 16 Lambda a 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
```

El `-x` indicador ejecuta la transformación de forma no interactiva y `-t` confía en todas las ejecuciones de la herramienta, por lo que no se requieren solicitudes. Puede programar este comando en docenas o cientos de repositorios mediante un simple bucle de shell. Cuando se complete cada transformación, revisa la diferencia de Git para verificar los cambios y ejecuta tu conjunto de pruebas para confirmar que la función actualizada funciona correctamente. También puede integrar AWS Transform custom en su CI/CD canalización para identificar las funciones Lambda obsoletas de forma continua. Este enfoque no solo aborda el problema inmediato de los tiempos de ejecución obsoletos, sino que también establece un proceso continuo para detectar y actualizar las funciones antes de que lleguen al estado de fin de soporte.

Los equipos de la plataforma central pueden crear campañas a través de la [aplicación web AWS Transform](#) para definir la transformación, especificar los repositorios Lambda de destino y realizar un seguimiento del progreso en toda la organización. Para obtener un recorrido detallado sobre la creación de una solución de implementación escalada de nivel de producción mediante AWS Batch, consulte [Creación de una solución de modernización de código escalable](#) con Transform custom.

AWS

AWS Transform puntos finales personalizados y de interfaz (AWS PrivateLink)

Puede establecer una conexión privada entre su VPC y la VPC AWS Transform personalizada mediante la creación de un punto final de VPC de interfaz. Los puntos finales de la interfaz funcionan con una tecnología que le permite acceder de forma privada a servicios AWS Transform personalizados sin necesidad de una pasarela de Internet, un dispositivo NAT, una conexión VPN o una conexión. [AWS PrivateLink](#) Direct Connect El tráfico entre tu VPC y la AWS Transform personalizada no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más [interfaces de red elásticas](#) en las subredes.

Para obtener más información, consulte [Puntos de conexión de VPC de interfaz \(AWS PrivateLink\)](#) en la Guía del usuario de Amazon VPC.

Note

- Debe habilitar la AWS PrivateLink integración de Amazon S3, ya que las llamadas a la API de S3 se realizan de forma AWS Transform personalizada. Para obtener instrucciones detalladas, consulte [AWS PrivateLink la documentación de Amazon S3](#). Si tiene problemas de acceso a S3 al usar la versión AWS Transform personalizada, consulte nuestra [guía de solución de problemas](#).
- Si no utilizas la función de DNS AWS PrivateLink privado (consulta [DNS privado](#)), debes:
 - Configure el enrutamiento a los puntos finales de la interfaz de VPC (consulte la documentación sobre el enrutamiento [a los puntos finales de la interfaz de VPC](#))
 - Configure la variable de ATX_CUSTOM_ENDPOINT entorno para especificar su dominio personalizado, por ejemplo:

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

Consideraciones para AWS Transform puntos finales de VPC personalizados

Antes de configurar un punto de enlace de VPC de interfaz para AWS Transform personalizarlo, asegúrese de revisar las [propiedades y limitaciones del punto de enlace de interfaz](#) en la Guía del usuario de Amazon VPC.

AWS Transform custom permite realizar llamadas a todas sus acciones de API a través del punto final de la interfaz.

Requisitos previos

Antes de comenzar cualquiera de los procedimientos siguientes, asegúrese de que dispone de lo siguiente:

- Una AWS cuenta con los permisos adecuados para crear y configurar recursos.
- Ya se ha creado una VPC en su cuenta. AWS
- Familiaridad con AWS los servicios, especialmente Amazon VPC AWS Transform y Custom.

Creación de un punto final de VPC de interfaz para AWS Transform personalizado

Puede crear un punto de enlace de VPC para el servicio AWS Transform personalizado mediante la consola de Amazon VPC o el (). AWS Command Line Interface AWS CLI Para obtener más información, consulte [Creación de un punto de conexión de interfaz](#) en la Guía del usuario de Amazon VPC.

Cree los siguientes puntos finales de VPC para AWS Transform personalizarlos con este nombre de servicio:

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

region Sustitúyala por AWS la región en la que desees usar una CLI AWS Transform personalizada, por ejemplo, com.amazonaws.us-east-1.transform-custom.

Para más información, consulte [Acceso a un servicio a través de un punto de conexión de interfaz](#) en la Guía del usuario de Amazon VPC.

Crear una política de puntos de conexión de VPC para AWS Transform personalizado

Puede adjuntar una política de punto final a su punto final de VPC que controle el acceso a la AWS Transform personalización. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para más información, consulte [Control del acceso a los servicios con puntos de enlace de la VPC](#) en la Guía del usuario de Amazon VPC.

Ejemplo: política de puntos finales de VPC para AWS Transform acciones personalizadas

El siguiente es un ejemplo de una política de puntos finales AWS Transform personalizada. Cuando se adjunta a un punto final, esta política otorga acceso a las acciones AWS Transform personalizadas enumeradas a todos los principales de todos los recursos.

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

Utilizar un ordenador local para conectarse a un AWS Transform punto de conexión personalizado

En esta sección, se describe el proceso de usar un equipo local para conectarse a un dispositivo AWS Transform personalizado a través de un AWS PrivateLink punto final de la AWS VPC.

1. [Cree una conexión de VPN entre el dispositivo en las instalaciones y la VPC.](#)

2. [Cree un punto final de VPC de interfaz para AWS Transform personalizarlo.](#)
3. [Configure un punto de conexión entrante de Amazon Route 53.](#) Esto le permitirá usar el nombre DNS de su punto de conexión AWS Transform personalizado desde su dispositivo local.

Resolución de problemas

Esta sección proporciona orientación para solucionar problemas comunes con Transform custom.
AWS

Registrar ubicaciones

AWS La CLI de Transform mantiene los registros en las siguientes ubicaciones:

Registros de conversaciones:

Linux and macOS

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

Windows

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

Estos registros contienen el historial completo de conversaciones para depurar ejecuciones de transformaciones específicas.

Registros de subagentes:

Linux and macOS

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

Windows

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

Estos registros contienen los resultados de los subagentes que el agente principal genera durante las transformaciones. No es necesario gestionar los subagentes directamente.

Registros de depuración de desarrolladores:

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
```

Estos registros proporcionan información detallada sobre las operaciones y los errores de la CLI. Cada archivo de registro tiene un límite de 5 MB antes de transferirse. Es posible que haya varios registros de depuración en este directorio, como debug1.log y debug2.log.

Problemas comunes

Problemas de instalación:

Si la instalación falla, asegúrese de tener Node.js 22 o una versión posterior instalada:

```
node --version
```

Node.js Descárguelo desde <https://nodejs.org/en/download> si es necesario.

Problemas de autenticación:

Compruebe que sus AWS credenciales estén configuradas correctamente:

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

Asegúrese de que su usuario o rol de IAM tenga los transform-custom:* permisos necesarios.

Problemas de conectividad de red:

Si se producen errores de conexión, compruebe el acceso de la red a los puntos finales necesarios:

- transform-cli.awsstatic.com
- transform-custom.<region>.api.aws

- *.s3.amazonaws.com

Si trabajas en un entorno con acceso restringido a Internet, actualiza las reglas del firewall para incluir estas URL en una lista de direcciones URL permitidas.

Problemas de configuración regional:

Si encuentra errores relacionados con la región:

- Comprueba que tu región sea compatible
- Compruebe si hay variables de entorno que puedan anular su configuración: `echo $AWS_REGION $AWS_DEFAULT_REGION`
- Compruebe la configuración de su región: `aws configure get region`
- Actualice su región si es necesario: `aws configure set region <your-region>`
- Consulte los registros de depuración para obtener detalles sobre la resolución de la región

Problemas con Git:

Asegúrate de que Git esté instalado y de que tu repositorio esté bajo el control de código fuente de git:

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

AWS Transform custom requiere que los repositorios estén bajo el control de código fuente de git.

Problemas de ejecución de la transformación:

Si una transformación falla:

1. Revise los registros de conversaciones en `~/.aws/atx/custom/<conversation_id>/logs/`
2. Compruebe si hay errores de compilación o prueba en el resultado de la transformación
3. Compruebe que el comando build es correcto para su proyecto
4. Intenta ejecutar la transformación en modo interactivo para enviar comentarios

Problemas con la reanudación de la conversación:

Si no puedes reanudar una conversación:

- Verifica que la conversación tenga menos de 30 días
- Comprueba que el identificador de la conversación sea correcto
- Asegúrese de tener conectividad de red

Cómo obtener soporte

Para obtener asistencia adicional, visita AWS Support through the [AWS Console](#).

Al abrir un ticket de soporte, incluye:

- Registros de conversaciones de `~/.aws/atx/custom/<conversation_id>/logs/`
- El subagente registra desde `~/.aws/atx/custom/<conversation_id>/logs/subagents/`
- Depurar registros de `~/.aws/atx/logs/`
- Pasos para reproducir el problema
- AWS Transformar la versión CLI (`atx --version`)

Problemas de acceso a S3

El servicio personalizado AWS Transform vende las URL prefirmadas de S3 para facilitar la carga y descarga de los archivos de transformación, que pueden ser de gran tamaño en las máquinas cliente. to/from Esto significa que la CLI no solo interactúa con los puntos finales del servicio AWS Transform, sino que también interactúa con los puntos finales del servicio S3. Estas interacciones utilizan URL prefirmadas, por lo que las credenciales de IAM de su cliente no requieren ningún permiso de S3, pero a veces las configuraciones del servidor proxy de su máquina local y las políticas de punto final de VPC de S3 de su red pueden restringir este tráfico.

Examine los mensajes de error más detallados [the section called “Registrar ubicaciones”](#) para ayudar a identificar la causa de cualquier fallo en las herramientas o la denegación del acceso a S3 relacionados con la descarga y la carga de archivos de transformación.

Si utiliza un VPN/Proxy servidor que aprovecha las variables de `no_proxy` entorno `https_proxy` y las variables de entorno, considere la posibilidad de añadir los siguientes valores al valor de la variable de `no_proxy` entorno para evitar el proxy de los puntos finales de los servicios personalizados de S3 y AWS Transform, por ejemplo:

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"
```

Si utiliza una [AWS PrivateLink para Amazon S3](#) en su VPC, es posible que tenga una política definida para restringir el tráfico de S3. Asegúrese de que su política de puntos finales de VPC de S3 permita GetObject y PutObject opere para los buckets propiedad del servicio personalizado de AWS Transform. Esto se puede lograr añadiendo la siguiente declaración a la política de puntos finales de la VPC:

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

DenyLas declaraciones explícitas en las políticas tienen prioridad sobre Allow las declaraciones. Consulte las políticas de puntos finales de VPC de S3 para ver las Deny afirmaciones que puedan restringir el acceso.

AWS Historial de versiones de Transform CLI

Consulte la siguiente tabla para obtener detalles sobre las versiones actuales y anteriores de la CLI de AWS Transform. La tabla incluye la versión, la fecha de publicación y las notas de publicación de cada versión.

Versión	Fecha de publicación	Notas de la versión
3.6.0 (última)	17 de julio de 2026	Se agregó el <code>atx custom def learnings</code> subcomando, que abre una sesión interactiva de TUI para ver y gestionar los aprendizajes generados automáticamente

Versión	Fecha de publicación	Notas de la versión
		para una definición de transformación basada en ejecución es anteriores. • Se agregó la recopilación de telemetría de uso durante la ejecución de la transformación. Para deshabilitar la telemetría, defina la variable de entorno. <code>ATX_DISABLE_TELEMETRY=true</code> Para obtener más información, consulte Telemetría de uso. • Se ha corregido un problema en Windows por el que las operaciones con archivos que ~ utilizaban rutas (directorio principal) se resolvían en un directorio inesperado. Esto provocaba read/write errores en los archivos durante una sesión. • Se ha corregido un problema que provocaba que los nombres de servidores y herramientas MCP que contenían caracteres especiales pudieran provocar fallos de conexión. La CLI ahora limpia automáticamente los nombres para usar solo caracteres válidos.

Versión	Fecha de publicación	Notas de la versión
3.5.0	8 de julio de 2026	• Se agregó soporte nativo para Windows. Ahora puede ejecutar los comandos AWS Transform Custom directamente en Windows. (Los <code>atx ct</code> comandos aún no son compatibles con Windows) • Se agregaron entradas de orientación para <code>atx ct analysis run</code> que los análisis de la preparación de los agentes y de la preparación para la modernización reflejen sus preferencias. <code>--context</code> Úselos como marco estratégico, para configurar el acceso de los agentes <code>--agent-scope</code> para que estén preparados para ellos y <code>--prefer</code> para orientar las recomendaciones de modernización <code>--avoid</code> hacia tecnologías específicas o alejarlas de ellas. • Las definiciones de transformación en el formato de habilidad ahora pueden incluir una <code>scripts/</code> carpeta, lo que permite agrupar guiones auxiliares junto con los suyos y sus referencias. <code>SKILL.md</code> • Se ha añadido <code>--wait aatx ct remediation create</code>, que espera a que se complete la corrección. • Se agregó el modo sin cabeza para la ejecución de un solo disparo. Corre <code>atx -x "prompt" -t</code> para pasar un mensaje, obtén una respuesta y sal sin indicaciones interactivas. El modo Headless requiere confiar en todas las herramientas.
3.4.1	2 de julio de 2026	• Se ha corregido un problema de sesión interactiva introducido en la versión 3.4.0. Una vez que el agente termine de responder, es posible que la CLI permanezca en la línea de comandos «Pensando» (que se muestra con puntos suspensivos en la interfaz de usuario) en lugar de volver a la línea de entrada. La CLI ahora lo devuelve al indicador de entrada después de cada respuesta.

Versión	Fecha de publicación	Notas de la versión
3.4.0 (no se recomienda)	29 de junio de 2026	 Problema conocido En las sesiones interactivas, la CLI puede permanecer en el indicador «Pensar» (que se muestra con puntos suspensivos en la interfaz de usuario) una vez que el agente termine de responder. Esto le impide escribir el siguiente mensaje. Para resolver este problema, ejecute <code>atx update</code> la actualización a la versión 3.4.1 o posterior. • Se agregó <code>atx context schema</code> un manifiesto legible por máquina de toda la superficie de <code>atx context</code> comandos para la creación de scripts y la automatización. • Se ha añadido la validación del ámbito simbólico al añadir o actualizar una fuente, lo que permite detectar problemas con las credenciales o los permisos de forma inmediata, en lugar de que se produzcan errores más adelante durante el análisis. • Se mejoraron las solicitudes de cambios de corrección automática para incluir la búsqueda de contexto y el modo borrador de soporte para obtener relaciones públicas más revisables. • Retroalimentación mejorada del progreso de la CLI con contexto en tiempo real sobre la actividad actual, los minutos estimados de los agentes y la actividad de los subagentes. • Se agregó un punto de control configurable que confirma la identidad del autor a través de las variables <code>ATX_GIT_COMMITTER_NAME</code> de <code>ATX_GIT_COMMITTER_EMAIL</code> entorno. • Varias pequeñas correcciones de errores y mejoras.

Versión	Fecha de publicación	Notas de la versión
3.3.0	18 de junio de 2026	• Se agregó consistencia <code>--json</code> y <code>--help</code> compatibilidad con todos <code>atx</code> ct los comandos. • Se ha corregido la configuración del agente de seguridad , por lo que el espacio de agentes se crea durante la configuración y se elimina al desmontarlo. • Varias pequeñas correcciones de errores y mejoras.
3.2.0	15 de junio de 2026	• Se agregaron comandos de modernización continua (<code>atx</code> ct) a la distribución CLI estándar para todos los usuarios. • Se ha mejorado la ejecución de los subagentes para mostrar el efecto de «pensar...» mientras se espera la respuesta del servidor, lo que proporciona información visual clara de que el trabajo está en marcha. • Se ha mejorado el spinner para que se reinicie automáticamente con el mensaje «Working on it...» tras 3 segundos de silencio tras la salida del agente, de forma que el terminal nunca parezca congelado entre los pasos de procesamiento. • La rueda giratoria pensante mejorada cuenta con una sutil animación brillante que ofrece una apariencia visual más pulida.

Versión	Fecha de publicación	Notas de la versión
3.1.0	3 de junio de 2026	• Se agregó una variable de <code>ATX_MAX_VALIDATION_LOOPS</code> entorno para configurar los bucles de validación máximos. • La comprobación de actualizaciones fijas ya no muestra falsas advertencias de «actualización disponible» cuando la versión instalada ya es más reciente que la versión de registro. • Se corrigió el error: ya <code>delete --transformation-name ""</code> no mostraba un mensaje de confirmación absurdo; los valores vacíos ahora se rechazan con un claro error de validación. • Se ha corregido un error: los subcomandos no reconocidos ahora muestran un «comando desconocido» en lugar de un confuso mensaje de error interno. • Se corrigió la comparación de versiones para utilizar la comparación numérica en lugar de la desigualdad de cadenas para las comprobaciones de actualizaciones.

Versión	Fecha de publicación	Notas de la versión
3.0.0	21 de mayo de 2026	• Se agregó la validación de nombres previa a la transformación, que sugiere nombres similares de su registro cuando no se encuentra ningún nombre, lo que ayuda a detectar errores tipográficos sin necesidad de un comando de lista independiente. • Se han añadido explicaciones opcionales para los comandos de shell, que muestran lo que hacen y por qué. • Se ha mejorado el banner de configuración de confianza para incluir más información sobre los permisos de las herramientas. • Se ha añadido un banner que indicaba que el aprendizaje estaba desactivado cuando se utilizaba la marca «no se aprende», lo que permite ver la función de aprendizaje y saber cómo activarla. • Cambio de última hora: ahora es necesario tener Node.js 22 o una versión posterior. Actualice desde una versión anterior https://nodejs.org/ si está utilizando una versión anterior.

Versión	Fecha de publicación	Notas de la versión
2.0.0	14 de mayo de 2026	• Se agregó la compatibilidad con servidores MCP remotos: conéctese a servidores MCP HTTP y HTTPS con el respaldo automático de SSE, la autenticación mediante token Bearer con expansión de variables de entorno en los encabezados y la compatibilidad con proxy (). HTTP_PROXY/HTTPS_PROXY • Se agregó <code>atx resume</code> un subcomando como alias para. <code>atx --resume</code> • Se agregó <code>grep</code> una herramienta para la búsqueda de texto en varios archivos con control de salida: admite patrones de expresiones regulares, filtrado global de archivos, búsqueda sin distinción entre mayúsculas y minúsculas, límites configurables y truncamiento de salida. <code>depth/result</code> • Implementación de MCP mejorada para utilizar el SDK de MCP estándar para un comportamiento más coherente y un soporte más sencillo para las futuras funciones de MCP. • Gestión mejorada de la salida por shell: la salida ahora se trunca correctamente a 30 000 caracteres por secuencia, en lugar de provocar un error grave, conservando el principio y el final de la salida por motivos de contexto. • Se solucionó un problema que provocaba que, durante una sesión interactiva, <code>Ctrl+C</code> se cerrara prematuramente de la CLI en Linux/macOS lugar de abortar la operación actual y volver a la línea de comandos. • Se corrigió el mensaje de rechazo de confianza para mostrar un motivo específico por el que la confianza no está disponible, aparte del motivo por el que el comando necesitaba autorización. • Se corrigió una advertencia de comando peligroso que ya no mencionaba confiar cuando el comando estaba activo <code>alwaysPromptCommands</code> .

Versión	Fecha de publicación	Notas de la versión
1.10.0	29 de abril de 2026	• Se han mejorado las descripciones de las herramientas con una guía multiherramienta, lo que ayuda al agente a elegir la mejor herramienta para cada tarea y reduce el uso innecesario del shell. • Se agregó <code>alwaysPromptCommands</code> <code>trust-settings.yaml</code> : configure patrones de comandos de shell que siempre requieran un permiso explícito, independientemente de la configuración de confianza. Admite caracteres comodín globales y realiza coincidencias con cada subcomando en las expresiones compuestas. <code>trustedShellCommands</code> puede anular estos patrones. No se aplica en el modo no interactivo para evitar interrumpir las canalizaciones automatizadas. • Las rutas relativas fijas no se resolvían en rutas absolutas.
1.9.0	23 de abril de 2026	• Indicaciones de aprobación de herramientas mejoradas : ahora, cada opción muestra lo que hace en línea, un mensaje con el mensaje «Por qué» explica por qué es necesaria la aprobación y la confirmación de confianza incluye una sugerencia sobre <code>trust-settings.yaml</code> la confianza permanente.
1.8.0	16 de abril de 2026	• Se cambió el prefijo de salida del agente de <code>></code> a <code>ATX:</code> para establecer una distinción visual más clara entre la entrada del usuario y la salida del agente. • Se ha corregido la visualización del comando de reanudación cuando se agotan los reintentos de CLI. • Currículum fijo desde un directorio de trabajo diferente. En el modo interactivo, solicita la ruta corregida; en el modo no interactivo, falla rápidamente con un error descriptivo.

Versión	Fecha de publicación	Notas de la versión
1.7.1	9 de abril de 2026	• Se corrigió el error de inicio de sesión único («no se encontró el token de sesión o no es válido») cuando la región del proveedor de credenciales es diferente a la del perfil. <code>sso_region</code> • Se ha corregido el almacenamiento en caché de credenciales para que las sesiones de larga duración no produzcan errores al rotar las credenciales en el disco.
1.7.0	2 de abril de 2026	• Se corrigió <code>exec</code> el comando para que saliera con el código 1 en los errores de validación de entrada, lo que hacía que la CLI fuera confiable en los scripts y CI/CD canalizaciones. • Se agregó la visualización de los mensajes de advertencia del servicio. • Se agregó la compatibilidad con solicitudes de MFA para los perfiles de AWS credenciales. • Se corrigieron las llamadas a credenciales STS para respetar la configuración del proxy HTTP (S).
1.6.0	18 de marzo de 2026	• Se agregó <code>--limit <minutes></code> la opción de establecer el presupuesto <code>exec</code> y los <code>interactive</code> comandos de Agent Minutes. Cuando se alcanza el límite, la CLI muestra el uso y sale con las instrucciones de reanudación. • Se ha corregido el registro del mensaje inicial del usuario en los registros de conversaciones.
1.5.0	11 de marzo de 2026	• Se agregó soporte para la ejecución simultánea de tareas, lo que permite transformaciones más rápidas. • Se agregó la visualización de los minutos de uso del agente al final de cada conversación y un <code>/usage</code> comando en modo interactivo para comprobar el uso en cualquier momento.

Versión	Fecha de publicación	Notas de la versión
1.4.0	2 de marzo de 2026	• Se han mejorado los mensajes de error al guardar las definiciones de transformación con archivos no compatibles. • Se agregó tiempo de espera a las llamadas de servicio para evitar que la CLI se bloquee cuando se interrumpe la conexión. • Se corrigió el bloqueo del proceso CLI después de completarse correctamente. • Se ha corregido la validación de la región al reanudar las conversaciones.
1.3.0	19 de febrero de 2026	• Se ha eliminado la restricción para las rutas de los servidores MCP: los usuarios ahora pueden especificar cualquier ruta para la command propiedad en la configuración de MCP. • Se ha mejorado la estabilidad de las conexiones del servidor MCP.
1.2.0	9 de febrero de 2026	• Se agregó soporte para la configuración del proxy mediante variables de entorno (<code>https_proxy</code> <code>no_proxy</code>, etc.). • Mejoras generales de estabilidad y correcciones de errores.
1.1.1	16 de enero de 2026	Correcciones de errores y mejoras en la estabilidad.
1.1.0	13 de enero de 2026	Se agregó compatibilidad con la configuración regional de AWS CLI, comprobaciones tempranas de validación de credenciales y funcionalidad fija de reanudación de campañas.
1.0.1	18 de diciembre de 2025	Cierres elegantes, registros de errores más limpios y mejoras generales.
1.0.0	1 de diciembre de 2025	Versión inicial de la CLI de AWS Transform.

AWS Transforme la modernización continua

¿Qué es? AWS ¿Transformar la modernización continua?

AWS La modernización continua de Transform proporciona análisis y soluciones para sus repositorios de código fuente. Puedes conectar GitHub organizaciones, GitLab grupos, espacios de trabajo de Bitbucket y repositorios locales y, a continuación, ejecutar análisis automatizados para identificar la deuda técnica, las vulnerabilidades de seguridad, las oportunidades de modernización y la disponibilidad de los agentes en toda tu base de código.

Todos los análisis y las correcciones se ejecutan tú mismo con tus credenciales. Cuenta de AWS Su código fuente permanece bajo su control.

Note

Te recomendamos empezar con el plugin Kiro Power o el plugin de agente. La habilidad del agente organiza la configuración, la incorporación y el uso continuo de la modernización continua, que incluye el aprovisionamiento de la infraestructura, la configuración de las fuentes, la ejecución de los análisis, la clasificación de los hallazgos y la corrección. Para obtener las instrucciones de instalación, consulta [Herramientas para desarrolladores](#).

Capacidades clave

AWS La modernización continua de Transform ofrece las siguientes capacidades:

- **Análisis de la deuda tecnológica:** escanee los repositorios en busca de dependencias obsoletas, vulnerabilidades de seguridad, problemas de calidad del código y oportunidades de modernización. Realice escaneos rápidos de metadatos en los manifiestos de paquetes o realice análisis exhaustivos a nivel de código. Defina criterios de análisis personalizados mediante definiciones de transformación adaptadas a su entorno.
- **Remediación autónoma:** genere solicitudes de cambios validadas a escala. Cada hallazgo se puede corregir automáticamente mediante su definición de transformación asociada. Remediation crea ramas y se abre PRs/MRs automáticamente entre Bitbucket y GitHub GitLab Bitbucket.

- **Informes:** genera informes HTML que muestren los resultados por gravedad, repositorio y tipo de análisis. Realice un seguimiento del progreso de la remediación y busque soluciones a lo largo del tiempo.
- **Supervisión continua:** programe análisis periódicos con Amazon EventBridge Scheduler. Configure programas cron diarios, semanales o personalizados para supervisar continuamente su cartera de productos en busca de nuevos números.

Tipos de análisis

AWS La modernización continua de Transform admite los siguientes tipos de análisis para satisfacer sus necesidades de modernización.

Tipo	Description (Descripción)
<code>rapid-techdebt-analysis</code>	Escanea rápidamente los manifiestos de los paquetes (<code>pom.xml</code> , <code>package.json</code> , <code>requirements.txt</code>) únicamente con metadatos para identificar las versiones obsoletas y las dependencias obsoletas. No analiza el código fuente.
<code>tech-debt-comprehensive</code>	Análisis técnico profundo de la deuda a nivel de código mediante el agente AWS Transform. Examina el código fuente para identificar los patrones de endeudamiento, los problemas de calidad del código, los problemas de arquitectura y las oportunidades de mejora.
<code>security</code>	Detección de vulnerabilidades de seguridad y CVE mediante el AWS Security Agent. Analiza el código fuente y las dependencias en busca de vulnerabilidades conocidas, patrones de codificación inseguros y puntos débiles que puedan explotarse. Requiere una configuración de infraestructura única.

Tipo	Description (Descripción)
agentic-readiness	Evaluación de la preparación para la integración de la IA y los agentes. Califica 56 criterios en cinco categorías: infraestructura y plataforma, arquitectura de aplicaciones Identity/Security/Governance, bases de datos y operaciones y observabilidad.
modernization-readiness	Evaluación de las oportunidades de modernización de la nube. Evalúa la preparación en todas las dimensiones de la infraestructura, las aplicaciones, los datos, la seguridad y las operaciones. Identifica a los candidatos para la contenedorización, la migración sin servidores y las actualizaciones de la plataforma.
custom	Ejecute cualquier definición de transformación (TD) como análisis. Utilice este tipo para definir sus propios criterios de análisis o para ejecutar transformaciones AWS gestionadas que no estén incluidas en los tipos integrados.

Descripción de los conceptos clave

Orígenes

Una fuente indica a Continuous Modernization dónde están sus repositorios. Tipos de orígenes compatibles:

- GitHub— Organizaciones con tokens de acceso personal (clásico)
- GitLab— Grupos o usuarios, incluidas las instancias autohospedadas
- Bitbucket: espacios de trabajo (nube) o proyectos (centro de datos)
- Local: directorios principales que contienen repositorios de git

Repositorios

Los repositorios se descubren escaneando las fuentes. Tras el descubrimiento, puede filtrar por fuente, etiquetas u otros criterios; aplicar etiquetas por organización (equipo, prioridad, oleada de migración) y seleccionar repositorios específicos para analizarlos o corregirlos.

Análisis

Un análisis es un escaneo de uno o más repositorios mediante un tipo de análisis específico. Cada análisis produce resultados que identifican problemas en el código. Puede ejecutar los análisis a pedido o programarlos para que se ejecuten automáticamente. Los tipos de análisis incluyen el análisis rápido de la deuda tecnológica, el análisis exhaustivo de la deuda tecnológica, el de seguridad, el de preparación para los agentes, el de preparación para la modernización y el personalizado. Cada análisis hace un seguimiento de su estado (pendiente, en ejecución, completo, cancelado o fallido) y de los repositorios que ha escaneado.

Hallazgos

Los hallazgos son los resultados del análisis. Cada hallazgo incluye la gravedad (alta, media o baja), el estado (abierto, descartado u obsoleto) y la transformación de corrección que puede remediarlo (si se puede corregir automáticamente). Los nuevos hallazgos comienzan como abiertos. Los usuarios pueden descartar los hallazgos con un motivo. Re-analysis marca automáticamente los hallazgos resueltos como obsoletos.

Remediaciones

Las remediaciones aplican definiciones de transformación para corregir los hallazgos. Tres modos: basado en hallazgos (cada hallazgo usa su propia transformación fija), anulación de TD (invalida la definición de transformación para hallazgos específicos) y TD directo (ejecuta una transformación en un repositorio sin hallazgos). El resultado depende del proveedor de origen (GitHub PR, GitLab MR, Bitbucket PR o sucursal local).

Definiciones de transformación

Una definición de transformación contiene las instrucciones y los conocimientos necesarios para realizar una transformación de código específica. La modernización continua utiliza definiciones de transformación para el análisis personalizado (`--type custom --transformation-name name`) y la corrección (`--transformation-name name`). Enumere las definiciones de transformación disponibles con `conatx custom def list`.

Cómo AWS Transforme las obras de modernización continua

AWS La modernización continua de Transform se suele utilizar en proyectos a gran escala en los que es necesario analizar y corregir varias bases de código de forma continua. Los equipos suelen seguir este flujo de trabajo:

1. **Connect Sources:** añada GitHub organizaciones, GitLab grupos, espacios de trabajo de Bitbucket o directorios locales como fuentes. Proporcione los tokens de autenticación con los alcances adecuados.
2. **Descubra repositorios:** ejecute escaneos de detección para enumerar todos los repositorios de sus fuentes. Usa etiquetas para organizar los repositorios por equipo, prioridad u oleada de migración.
3. **Ejecute análisis:** ejecute análisis en toda su cartera. Elija escaneos rápidos para obtener resultados rápidos o análisis exhaustivos para obtener resultados detallados. El análisis de seguridad requiere una configuración de infraestructura única.
4. **Clasificación de los resultados:** revise los hallazgos por gravedad, repositorio o tipo de análisis. Rechaza los falsos positivos con motivos documentados. Re-run análisis para marcar los problemas resueltos como obsoletos.
5. **Remediar:** cree soluciones para corregir los hallazgos. La modernización continua crea sucursales automáticamente y abre pull/merge las solicitudes con las correcciones. Realice un seguimiento del estado de las correcciones y vuelva a intentar los errores.
6. **Configure el análisis continuo:** programe análisis periódicos con Amazon EventBridge Scheduler. Configure la cadencia de análisis (diaria, semanal o personalizada) para supervisar continuamente su cartera de productos en busca de nuevos problemas. Combínelo con la corrección automática para mantener el código en buen estado a lo largo del tiempo.

Opciones de computación

La modernización continua admite tres opciones de procesamiento para ejecutar los análisis y la corrección. Las habilidades de agente del Kiro Power y el complemento para agentes le ayudan a configurar la infraestructura para cada opción.

 Note

Independientemente de la opción de procesamiento, todos los análisis y las correcciones se realizan Cuenta de AWS utilizando sus credenciales. El código fuente permanece bajo su control.

Local (predeterminado)

De forma predeterminada, los análisis se ejecutan en su máquina local. Esta opción no requiere ninguna infraestructura adicional. El servidor se ejecuta de forma local y ejecuta los análisis mediante recursos informáticos locales. Ideal para probar la herramienta, para pequeños repositorios o para uso individual.

Amazon EC2

Ejecute análisis en una instancia persistente de Amazon EC2 en su. Cuenta de AWS Esta opción reduce la carga de cómputo de su máquina local, admite análisis de mayor tamaño y permite realizar análisis programados recurrentes. La instancia permanece en funcionamiento entre los envíos.

La habilidad del agente proporciona una AWS CloudFormation pila que incluye:

- Una instancia de Amazon EC2 (Amazon Linux 2023) con Docker y el contenedor de modernización continua
- Un rol de IAM con permisos para AWS Transform, Amazon S3, AWS KMS, Secrets Manager y el agente de seguridad
- AmazonSSMManagedInstanceCore para acceso al shell a través de SSM (no se requieren puertos de entrada ni un par de claves SSH)
- Un grupo de seguridad sin reglas de entrada

Su usuario o rol de IAM necesita permisos para la administración del ciclo de vida de Amazon EC2, las operaciones de apilamiento AWS CloudFormation, la creación de roles de IAM, las operaciones de bucket de Amazon S3, la administración de secretos de Secrets Manager y los comandos de SSM.

Para configurar la ejecución de EC2, instale el complemento Kiro Power o del agente (consulte [Herramientas para desarrolladores](#)) y, a continuación, pregunte al agente: «Configure una instancia de EC2 para un análisis continuo de la modernización». El agente aprovisiona la

infraestructura, verifica que el contenedor esté en buen estado y envía los análisis mediante SSM, sin necesidad de SSH.

AWS Batch (Fargate)

Ejecute análisis como trabajos aislados en AWS Batch con Fargate para una computación sin servidor. Cada análisis se ejecuta en su propio contenedor sin administrar una infraestructura persistente. Ideal para el análisis paralelo de múltiples fuentes o tipos de análisis.

Esta opción reutiliza la pila de infraestructura AWS Transform CDK. La habilidad de agente despliega la infraestructura requerida, que incluye:

- AWS Entorno de procesamiento y cola de trabajos por lotes
- Definición de trabajos con la imagen del contenedor de modernización continua
- Funciones de IAM para la ejecución de trabajos por lotes
- Una función Lambda para el envío de trabajos

Para configurar la ejecución por lotes, instale el complemento Kiro Power o del agente (consulte [Herramientas para desarrolladores](#)) y, a continuación, pregunte al agente: «Ejecute mi análisis en Fargate» o «Configure la ejecución por lotes para una modernización continua». El agente despliega la pila de CDK, almacena las credenciales de origen en Secrets Manager y envía los trabajos de análisis a Batch. AWS

Configuración del agente de seguridad

El tipo de security análisis utiliza el servicio AWS Security Agent para la detección de vulnerabilidades y CVE. A diferencia de otros tipos de análisis, requiere una configuración de infraestructura única en su Cuenta de AWS.

El comando setup proporciona una AWS CloudFormation pila que incluye:

- Un bucket de Amazon S3 para cargar el código fuente
- Una función de IAM asumida por `securityagent.amazonaws.com`
- Una política gestionada para la función de agente de seguridad

Su usuario o rol de IAM debe tener los siguientes permisos adicionales para ejecutar la configuración:

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

Utilice los siguientes comandos para administrar la infraestructura de los agentes de seguridad:

```
# 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
```

Una vez completada la configuración, puede ejecutar los análisis de seguridad de la misma forma que otros tipos de análisis.

Introducción

Requisitos previos

Para utilizar la modernización continua de forma eficaz, debes tener conocimientos básicos del control de versiones de Git, estar familiarizado con tu plataforma de código fuente (o Bitbucket) GitHub GitLab, tener conocimientos básicos de los permisos de AWS IAM y experiencia con las herramientas de línea de comandos.

Antes de utilizar la modernización continua, comprueba que tienes lo siguiente:

- AWS Transform CLI instalada:

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

- Node.js 2.2 o una versión posterior
- AWS Credenciales válidas (`AWS_PROFILE` o variables de entorno)
- La política AWS gestionada `AWSTransformCustomFullAccess` asociada a su usuario o función de IAM

Inicio rápido

1. Inicie el servidor de modernización continua:

```
atx ct server &
```

2. Agregue una fuente:

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

Dónde *name* hay un identificador descriptivo para su fuente, *provider* es la plataforma (github, gitlabbucket, olocal), *org-or-group* es el nombre de su organización o grupo y *token* es su token de autenticación.

3. Descubra los repositorios:

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

4. Ejecute un análisis:

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

5. Explore los hallazgos:

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

6. Remedie los hallazgos:

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

Trabajando con una modernización continua

Administración de fuentes

Utilice `atx ct source` comandos para conectar los repositorios. Proveedores compatibles: GitHub, Bitbucket GitLab, local.

GitHub organizaciones

Token: token de acceso personal (clásico) con repo alcance. Read-only para su análisis, repositorio completo para su corrección.

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

GitLab grupos y usuarios

Token: token de acceso personal con api alcance.

```
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
```

Espacios de trabajo y proyectos de Bitbucket

Bitbucket Cloud: ámbitos:read:repository:bitbucket,,, write:repository:bitbucket
read:pullrequest:bitbucket write:pullrequest:bitbucket También necesita --email
y. --username

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

Centro de datos de Bitbucket:

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

Repositorios locales

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

Important

--path deben apuntar a un directorio principal que contenga repositorios de git como subdirectorios, no a un único repositorio.

Administrar fuentes

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

Descubrimiento y administración de repositorios

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

Tras el descubrimiento:

```
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"
```

Ejecutando el análisis

El `--type` indicador especifica el tipo de análisis que se va a ejecutar:

- `rapid-techdebt-analysis`— Dependencias anticuadas y ganancias fáciles.
- `tech-debt-comprehensive`— AI-powered Un análisis más profundo que abarca los hallazgos sobre la dependencia, la seguridad, los patrones, el rendimiento, la capacidad de mantenimiento, la arquitectura, la calidad del código y la infraestructura.
- `security`— Vulnerabilidades y exposiciones de seguridad.
- `agentic-readiness`— Preparación de sus repositorios para los agentes de IA (marcos, API, documentación).
- `modernization-readiness`— Oportunidades de modernización en todas las dimensiones de la infraestructura, las aplicaciones, los datos, la seguridad y las operaciones.

```
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]
```

Análisis personalizado

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

Configuración con -g indicador: clave-valor, JSON o ruta de archivo.

Listar los TD: `atx custom def list`

Administración de resultados

```
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
```

Búsqueda de estados

- open— Activo
- dismissed— Descartado manualmente (requiere un motivo)
- obsolete— System-set cuando el nuevo análisis ya no produce el hallazgo

```
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
```

¿Descubriendo la obsolescencia

Re-analysis marca los hallazgos resueltos como obsoletos. No se puede volver a abrir. Conservado para su auditoría.

Creando soluciones

Tres modos: basado en hallazgos, anulación de TD, TD directo.

```
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
```

Salida por proveedor: GitHub PR, GitLab MR, Bitbucket PR, sucursal local.

Note

El token debe tener acceso de escritura para su PR/MR creación.

Ejecución local con `--local` indicador.

```
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 Transforma la aplicación web (opcional)

La aplicación web AWS Transform es una interfaz opcional para monitorear los análisis, hallazgos y correcciones continuos de la modernización en toda su cartera de fuentes de código.

Antes de utilizar la aplicación web AWS Transform, debe tener habilitada una identidad de usuario para acceder a AWS Transform en su organización. Para obtener información sobre cómo habilitar AWS Transform, consulte [Configuración de AWS Transform](#).

Para usar la aplicación web AWS Transform:

1. Visite <https://aws.amazon.com/transform/> e inicie sesión con las credenciales AWS del IAM Identity Center.
2. Si la modernización continua no aparece después de iniciar sesión, inicie sesión con las credenciales de IAM. Para habilitar el inicio de sesión con las credenciales de IAM:

- a. En la consola AWS de administración, abra AWS Transform y seleccione Configuración.
 - b. En la sección AWS Transformación de acceso con credenciales de IAM, habilite el acceso a las credenciales de IAM.
 - c. En la misma página de configuración, copia el enlace de inicio de sesión que aparece en la URL de la aplicación web (con IAM).
 - d. Pegue la URL de inicio de sesión en la misma ventana del navegador en la que está abierta la consola AWS de administración. Esto garantiza que la aplicación web utilice las AWS credenciales de esa cuenta.
3. Abra el menú de navegación de la izquierda y elija la modernización continua. El panel muestra un resumen de las estadísticas, incluidas las fuentes, los repositorios, el total de hallazgos por gravedad y los tipos de análisis.
 4. Utilice las pestañas Análisis, Hallazgos y Remediaciones para ver los resultados detallados.
 5. Chatee con AWS Transform directamente desde la aplicación web para hacer preguntas sobre sus análisis, hallazgos o soluciones.

La aplicación web está diseñada para operaciones a escala empresarial en las que se necesita una visibilidad centralizada de los análisis y las soluciones de modernización continuos en múltiples bases de código.

Herramientas para desarrolladores

Puede acceder a la modernización continua desde los IDE de los agentes mediante el complemento AWS Transform Power y el agente. El agente organiza la configuración, la incorporación y el uso continuo de la modernización continua mediante la interacción conversacional.

- Kiro IDE: [instale el Transform Kiro Power.AWS](#) Abre Kiro Chat y pide al agente que te ayude con los flujos de trabajo de modernización continua.
- Claude Code, Codex, Cursor: instale el [awslabs/agent-plugins \(directorio\)](#)plugins/aws-transform. El complemento del agente ofrece las mismas capacidades que el Kiro Power.

Habilidades del agente

El Kiro Power y el complemento para agentes incluyen habilidades que permiten organizar flujos de trabajo de modernización continua mediante la interacción conversacional:

Habilidad	Description (Descripción)
Guía	Integración interactiva que le guía paso a paso por todo el flujo de trabajo
origen	Agregue, enumere y elimine las conexiones de origen
Discovery	Escanea las fuentes para descubrir repositorios
Análisis	Ejecute y gestione análisis de todos los tipos
Hallazgos	Consulte, filtre y gestione los resultados de los análisis
Corrección	Cree y gestione soluciones para corregir los hallazgos
Ejecución de EC2	Aprovisione y gestione una instancia Amazon EC2 para el análisis remoto
Ejecución por lotes	Envíe trabajos de análisis a AWS Batch with Fargate
Schedule	Configure el análisis periódico según un cronograma cron con Amazon EventBridge Scheduler
Informes	Genere informes HTML independientes con gráficos que muestren los hallazgos, la distribución de la gravedad y el progreso de la remediación

Referencia de la CLI

En la siguiente tabla se resumen todos los subcomandos. `atx ct`

Subcomando	Description (Descripción)
<code>atx ct server</code>	Inicie el servidor de modernización continua
<code>atx ct status</code>	Vea el estado del sistema, incluidas las fuentes, los repositorios, los análisis, las conclusiones y las correcciones
<code>atx ct source add</code>	Agrega una fuente (GitHub GitLab, Bitbucket o local)
<code>atx ct source list</code>	Listar las fuentes configuradas
<code>atx ct source remove</code>	Eliminar una fuente
<code>atx ct discovery scan</code>	Descubre repositorios a partir de una fuente
<code>atx ct discovery status</code>	Compruebe el estado del escaneo de detección
<code>atx ct repository list</code>	Enumere los repositorios con filtros opcionales
<code>atx ct repository get</code>	Obtenga un repositorio único
<code>atx ct repository update</code>	Actualice las etiquetas del repositorio
<code>atx ct repository delete</code>	Eliminar un repositorio
<code>atx ct analysis run</code>	Ejecute un análisis en los repositorios
<code>atx ct analysis get</code>	Obtenga detalles del análisis
<code>atx ct analysis list</code>	Enumere los análisis con filtros de estado y tipo opcionales
<code>atx ct analysis cancel</code>	Cancele un análisis en ejecución
<code>atx ct analysis delete</code>	Eliminar un análisis
<code>atx ct findings list</code>	Enumere los hallazgos con filtros según el repositorio, la fuente, la gravedad, el tipo, el estado y el análisis

Subcomando	Description (Descripción)
<code>atx ct findings get</code>	Obtenga un único hallazgo
<code>atx ct findings update</code>	Actualice el estado de la búsqueda (abierta o descartada)
<code>atx ct findings batch-update</code>	Actualización por lotes de varios hallazgos
<code>atx ct findings delete</code>	Elimine un hallazgo desestimado u obsoleto
<code>atx ct remediation create</code>	Cree una solución a partir de los hallazgos o una definición de transformación
<code>atx ct remediation list</code>	Enumere todas las remediaciones
<code>atx ct remediation status</code>	Compruebe el estado de las correcciones y consulte los enlaces PR/MR
<code>atx ct remediation retry</code>	Vuelva a intentar una corrección fallida
<code>atx ct remediation delete</code>	Eliminar una corrección
<code>atx ct setup security-agent</code>	Aprovisione o administre la infraestructura de agentes de seguridad
<code>atx ct schema</code>	Imprima un manifiesto JSON legible por máquina con toda la superficie de <code>atx ct</code> comandos (cada comando, opción y argumento) para que los agentes y la automatización puedan descubrir la CLI sin analizar el texto de ayuda

Resolución de problemas

Conexión rechazada o el servidor no está funcionando

La CLI de modernización continua requiere un servidor en ejecución. Comience con `atx ct server &` y verifique con `atx ct status --health`.

El escaneo de Discovery no devuelve ningún repositorio

En el caso de las fuentes locales, compruebe que `--path` apuntan a un directorio principal que contenga repositorios como subdirectorios (por ejemplo, `/home/user/repos`) y no directamente a un repositorio (por ejemplo, `/home/user/repos/my-app`). El escáner busca directorios secundarios que contengan una `.git` carpeta.

Error SETUP_REQUIRED

La fuente existe en su cuenta, pero las credenciales no están configuradas en este equipo. Ejecute `atx ct source add --name name` para configurar las credenciales localmente.

Error AUTH_REQUIRED

No se encontró un token válido para la fuente. Compruebe que tu token es correcto y tiene los alcances necesarios. Para ello GitHub, asegúrate de que el token tenga `repo` alcance. Para GitLab, asegúrese `api` del alcance.

Error INVALID_INPUT

Compruebe que está utilizando el nombre correcto del tipo de análisis. Los valores válidos son: `rapid-techdebt-analysis`, `tech-debt-comprehensive`, `security`, `agentic-readiness`, `modernization-readiness`, `custom`.

Errores de permisos durante la corrección

La corrección crea ramas y pull/merge solicitudes, lo que requiere acceso de escritura al repositorio. Actualiza tu token con permisos de escritura. Para ello GitHub, asegúrate de tener un `repo` alcance total. Para GitLab, asegúrese `api` del alcance. En el caso de Bitbucket, asegúrate `write:repository:bitbucket` y `write:pullrequest:bitbucket` alcances.

La configuración del agente de seguridad falla

Compruebe que su usuario o rol de IAM tiene los permisos necesarios AWS CloudFormation, de IAM y de Amazon S3 que se indican en la sección de configuración del agente de seguridad de [Cómo AWS Transforme las obras de modernización continua](#). Compruebe el estado con `atx ct setup security-agent --status`

La modernización continua no es visible en la aplicación web

Si la modernización continua no aparece después de iniciar sesión en la aplicación web AWS Transform, inicie sesión con las credenciales de IAM del lugar Cuenta de AWS donde AWS Transform esté activado en lugar de con AWS IAM Identity Center. Para ver los pasos, consulte [AWS Transforma la aplicación web \(opcional\)](#).

Herramienta de descubrimiento

La herramienta de AWS Transform detección le ayuda a descubrir automáticamente el inventario de servidores de su organización para prepararse para la migración. La herramienta es compatible con VMware vCenter Hyper-V, Microsoft y servidores importados. Para usar la herramienta de detección, debe configurar una o más fuentes de detección, dejar que la herramienta se ejecute y, a continuación, revisar los resultados en el panel Inventario descubierto.

Tras configurar una fuente de detección, la herramienta de detección comienza a recopilar información. El tiempo que necesita la herramienta de detección para analizar completamente la red depende del tamaño del entorno. Para un modelo de negocio de migración direccional, puede utilizar los archivos de evaluación de la cartera de migración (MPA) que la herramienta genera una vez finalizada la recopilación de servidores.

Flujo de trabajo de la herramienta

El flujo de trabajo de la herramienta de descubrimiento consta de dos tipos de actividades:

- Actividades de configuración
- Revisión y uso de los datos

Los siguientes pasos describen cómo instalar y utilizar la herramienta de descubrimiento y cómo trabajar con los datos recopilados:

1. Instale la herramienta de detección.
2. Configure las fuentes de descubrimiento. Puede configurar una o más de las siguientes opciones: VMware vCenter, Hyper-V hosts de Microsoft o servidores mediante la importación de un archivo CSV. La detección de datos comienza después de configurar cualquier fuente.
3. Configure el acceso al sistema operativo y, a continuación, revise el estado de la recopilación de los servidores, las bases de datos y las conexiones de red.
 - Ajuste las credenciales del sistema operativo según sea necesario.
4. (Opcional) Configure las credenciales de Oracle para permitir la recopilación directa de SQL o utilice la detección OS-level alternativa mediante SSH o WinRM.
5. Para generar un modelo de negocio de migración, cargue el archivo.zip a [Migration Assessment](#) o descomprímalo y cargue los archivos MPA desde el directorio mpa_exports. La exportación

incluye datos de todas las fuentes configuradas y contiene archivos MPA para VMware y servidores importados. Hyper-V

La herramienta de detección admite las siguientes rutas de detección:

- Descubrimiento automático de VMware vCenter: descubra automáticamente los servidores administrados por VMware vCenter.
- Hyper-V detección automática: descubre automáticamente los servidores administrados por los Hyper-V hosts de Microsoft.
- Importación de servidores: importe manualmente el inventario de servidores a través de un archivo CSV.

Configuración de la herramienta de detección

Requisitos previos

Los siguientes son los requisitos previos para utilizar la herramienta de AWS Transform descubrimiento:

Requisitos previos generales

- La herramienta requiere 4 vCPU, 16 GB de RAM y un disco duro de 35 GB.
- El DHCP debe estar disponible en la red para la máquina virtual de la herramienta de detección.
- La herramienta recopila datos mediante un enfoque centralizado. Los servidores incluidos en el programa deben permitir la conectividad entrante desde la máquina virtual de la herramienta de detección (puertos predeterminados, se admite la configuración de puertos personalizada):
 - Linux: SSH TCP/22
 - Windows: TCP/5985 para HTTP, TCP/5986 para HTTPS
 - SNMP: UDP/161 (se usa solo para la recopilación de redes, no para las métricas del sistema operativo)
- Para Linux, cuentas de usuario que pueden usar SSH para conectarse al servidor. La herramienta de detección ejecuta comandos a través de SSH para la recopilación de redes y las métricas del sistema operativo. La mayoría de los comandos se ejecutan como un usuario normal. Un número reducido de comandos intenta sudo y recurre automáticamente a él si no está disponible: `dmidecode` (UUID del servidor y fabricante), `lvs` (detección de LVM) `ss` o `netstat`

(conexiones de red con información del proceso). Sin sudo, la herramienta de detección sigue recopilando la mayoría de los datos, pero no se mostrarán los detalles del UUID, el LVM y la red a nivel de proceso. Recomendamos configurar el sudo sin contraseña para el usuario de SSH a fin de garantizar una recopilación de datos completa. Para obtener un desglose completo, consulte [the section called “Permisos necesarios”](#)

Requisitos previos de VMware

- VMware vCenter Server versión 6.5, 6.7, 7.0 u 8.0.
- Permisos para implementar una OVA en su vCenter de VMware.
- Para la configuración de VMware vCenter Server, un usuario de vCenter con la Read-Only función asignada en el nivel del centro de datos raíz. Para obtener más información, consulte [the section called “Permisos necesarios”](#).

Hyper-V Requisitos previos

- Windows Server con la función habilitada. Hyper-V
- WinRM está habilitado en Hyper-V los hosts.
- Una cuenta de usuario que es miembro de los grupos de usuarios de administración remota, Hyper-V administradores y usuarios del monitor de rendimiento de cada Hyper-V host, con acceso de lectura de WMI al root\cimv2 espacio de nombres. Para obtener más información, consulte [the section called “Permisos necesarios”](#).
- Autenticación compatible: NTLM (solo HTTPS) y Kerberos (HTTP o HTTPS).

Requisitos previos para la importación del servidor

- Un archivo CSV con los nombres de host o las direcciones IP del servidor y los nombres de las credenciales (opcional) que se corresponden con los nombres descriptivos de las credenciales del sistema operativo configuradas o que se van a configurar en la herramienta de detección. El CSV debe usar los siguientes encabezados:

```
hostname_or_ip,os_credential_name,oracle_credential_name
```

- Se debe poder acceder a los servidores desde la máquina virtual de la herramienta de detección. Puertos predeterminados: puerto SSH 22 para Linux, 5985/5986 puerto WinRM para Windows. Se admiten puertos personalizados.

Requisitos previos del instalador de Linux

- Una distribución de Linux compatible: Amazon Linux 2, Amazon Linux 2023, RHEL 8—9, Rocky Linux 8—9, 9, Ubuntu 20.04—24.04, AlmaLinux Debian 10—12 o SLES 15 SP5.
- Mínimo 4 vCPU, 16 GB de RAM y 35 GB de espacio disponible en disco.
- El puerto 5000 debe estar disponible (no debe estar siendo utilizado por otro servicio).
- systemd es necesario para la administración del servicio.
- La máquina virtual de la herramienta de detección debe tener acceso de red a la infraestructura de destino. Puertos predeterminados: vCenter en el puerto 443, Hyper-V hosts en el puerto 5985/5986 y servidores en el puerto 22. Los puertos personalizados son compatibles con SSH, WinRM y SNMP.

Requisitos previos de Oracle Database

- Acceso a la red desde la herramienta de detección a los hosts de Oracle en el puerto 1521 (o puerto personalizado).
- Versiones de Oracle compatibles: puede recopilar Oracle Database 12c versión 1 (12.1) y versiones posteriores mediante conexiones SQL directas. OS-level La detección alternativa funciona con todas las versiones de Oracle.
- Una cuenta de servicio de Oracle de solo lectura con la concesión SELECT_CATALOG_ROLE. Para obtener más información, consulte [the section called “Base de datos Oracle \(SQL\)”](#).
- Para la detección OS-level alternativa: acceso SSH o WinRM al host de Oracle (utiliza las credenciales del sistema operativo existentes).

Implemente en VMware

Especificaciones de la máquina virtual VMware

- Sistema operativo — Amazon Linux 2023
- RAM: 16 GB
- CPU: 4 núcleos
- Discos: 35 GB
- Requisitos de VMware: consulte los [requisitos de host de VMware para ejecutar el AL2023 en VMware](#)

Implemente la OVA de VMware

1. Descargue el archivo OVA desde esta URL: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.ova>
2. Inicie sesión en vCenter como administrador de VMware.
3. Utilice uno de estos modos para instalar el archivo OVA:
 - a. Utilice la interfaz de usuario: elija Archivo, elija Implementar plantilla de OVF, seleccione el archivo OVA de la herramienta de detección que descargó en el paso 1 y, a continuación, complete el asistente. Asegúrese de que la configuración del proxy en el panel de administración del servidor esté configurada correctamente.
 - b. Utilice la línea de comandos: para instalar el archivo OVA de la herramienta de detección desde la línea de comandos, descargue y utilice la herramienta de formato de virtualización abierta de VMware (ovftool). Para descargar ovftool, seleccione una versión de la página de documentación de la herramienta [OVF](#). Este es un ejemplo del uso de la herramienta de línea de comandos ovftool para instalar el archivo OVA de la herramienta de detección.

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

Descripciones de los valores reemplazables en el ejemplo:

- El nombre es el nombre que desea usar para la máquina virtual de su herramienta de descubrimiento.
 - El almacén de datos es el nombre del almacén de datos de su vCenter.
 - El nombre del archivo OVA es el nombre del archivo OVA de la herramienta de detección descargado.
 - username/password Son sus credenciales de vCenter.
 - La URL de vCenter es la URL de su vCenter.
 - La ruta vi es la ruta a su host VMware ESXi.
4. Localice la herramienta de detección implementada en su vCenter. Right-click la máquina virtual y, a continuación, seleccione Power, Power On.
 5. Después de unos minutos, la dirección IP de la herramienta de detección aparece en vCenter. Esta dirección IP se utiliza para conectarse a la herramienta de detección.

Implemente en Hyper-V

Hyper-V especificaciones de máquinas virtuales

- Sistema operativo — Amazon Linux 2023
- RAM: recomendamos asignar al menos 16 GB
- CPU: recomendamos asignar al menos 4 núcleos
- Discos: 35 GB (incluidos en el VHD)
- Hyper-V requisitos: consulte los [requisitos del Hyper-V host para ejecutar AL2023 en Hyper-V](#)

Implemente el VHD Hyper-V

1. Descargue el archivo VHD desde esta URL: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.vhd>
2. Copie el archivo VHD en el equipo Windows Server que tiene la Hyper-V función habilitada.
3. Abra el Hyper-V administrador.
4. Elija Nueva y, a continuación, elija Máquina virtual.
5. Complete el asistente de configuración. En la página Especificar generación, seleccione Generación 1. Las máquinas virtuales de segunda generación no admiten el formato VHD. En la página Asignar memoria, asigne al menos 16384 MB. En la página Connect Virtual Hard Disk, elija Usar un disco duro virtual existente y seleccione el archivo VHD que ha copiado.
6. Inicie la máquina virtual. Transcurridos unos minutos, consulte la pestaña Redes de la máquina virtual en el Hyper-V Administrador para buscar la dirección IP o conéctese a la consola de la máquina virtual y ejecute `ip addr`. Esta dirección IP se utiliza para conectarse a la herramienta de detección.

Implemente en Linux

La herramienta de detección está disponible como un instalador de Linux independiente para su implementación en las distribuciones de Linux compatibles. Utilice esta opción si desea instalar la herramienta de detección directamente en un servidor Linux existente en lugar de implementar una máquina virtual.

Especificaciones del servidor Linux

- RAM: recomendamos asignar al menos 16 GB
- CPU: recomendamos asignar al menos 4 núcleos
- Discos: 35 GB

Distribuciones admitidas

- Amazon Linux — Amazon Linux 2, Amazon Linux 2023
- Red Hat Enterprise Linux y 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 la herramienta de detección

Descargue el script de instalación desde esta URL: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh>

Para instalar la herramienta de detección en Linux

1. Descargue el script de instalación en su 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) Ejecute la comprobación de compatibilidad para comprobar que el sistema cumple los requisitos.

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

3. Instale la herramienta de detección. Elija una de las siguientes opciones:

Opción 1: instalar con una instalación automática de dependencias (recomendada)

Esta opción instala automáticamente las dependencias del sistema que falten antes de instalar el servicio.

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

Opción 2: Instalar sin instalar automáticamente las dependencias

Esta opción comprueba si faltan dependencias y muestra los errores con las instrucciones de instalación manual si faltan dependencias críticas. Utilice esta opción si su organización restringe la instalación automática de paquetes y prefiere administrar los paquetes del sistema manualmente.

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

4. Inicie el servicio de herramientas de detección.

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

5. Acceda a la herramienta de descubrimiento en `https://ip_address:5000`.

Para desinstalar la herramienta de detección, ejecute `sudo ./AWS-Transform-discovery-tool.sh uninstall`.

También puede usar los siguientes comandos para administrar el servicio:

- `sudo ./AWS-Transform-discovery-tool.sh status`— Compruebe si el servicio se está ejecutando.
- `sudo ./AWS-Transform-discovery-tool.sh stop`— Detenga el servicio.
- `sudo ./AWS-Transform-discovery-tool.sh logs`— Ver los registros del servicio.

Dependencias del sistema

El instalador comprueba las siguientes dependencias del sistema:

Dependencia	Gravedad	Finalidad
OpenSSL	Critico	Genera la clave de cifrado de la base de datos
libcrypt	Critico	Requerido por el motor de ejecución de Python

Dependencia	Gravedad	Finalidad
Bibliotecas Kerberos	Advertencia	Necesarias para la autenticación de Kerberos en los servidores Windows. Sin esto, la autenticación básica y NTLM seguirán funcionando.

Se requieren dependencias críticas para que se inicie la herramienta de descubrimiento. Si faltan y ha elegido la opción 2 (sin ella `--install-deps`), el instalador mostrará un error con instrucciones para instalarlas manualmente. Warning-level las dependencias son opcionales: el instalador le avisa, pero continúa con la instalación.

Note

El instalador comprueba la compatibilidad del sistema, incluida la versión de glibc y la disponibilidad de systemd. En sistemas con systemd 250 o posterior (Amazon Linux 2023, RHEL 9, Rocky 9, 9, Ubuntu 24.04+, AlmaLinux Debian 12+), la clave de cifrado de la base de datos se cifra en reposo mediante systemd-creds. En los sistemas más antiguos, la clave de cifrado se guarda como un archivo protegido con permisos.

Configure la herramienta de detección

Acceda a la consola de la herramienta de detección

1. En un navegador web, acceda a: `https://ip_address:5000`, donde *ip_address* está la dirección IP de la herramienta de descubrimiento de Deploy Discovery Tool. La herramienta de detección utiliza un certificado autofirmado para la conexión HTTPS, lo que genera una advertencia de seguridad. Seleccione Aceptar el riesgo y continúe hasta la consola de la herramienta de detección.
2. Si accede a la consola de la herramienta de descubrimiento por primera vez, cree una contraseña de inicio de sesión de la herramienta de descubrimiento. Cree una contraseña, que utilizará para futuros inicios de sesión.

Important

Recuerde esta contraseña: no hay ningún mecanismo de recuperación de la contraseña.

Acceder a la herramienta de descubrimiento VM

- La máquina virtual de la herramienta de descubrimiento viene de forma predeterminada con un nombre de usuario y una contraseña («descubrimiento», «contraseña»). Para garantizar una mayor seguridad, le recomendamos que actualice la contraseña `sudo passwd discovery` después de iniciar sesión en la máquina virtual a través de la consola del hipervisor (por ejemplo, vSphere Client for VMware Hyper-V o Manager Hyper-V for).
- El acceso SSH está deshabilitado de forma predeterminada. Los usuarios pueden usar `disablessh` alias `enablessh` y preconfigurados para acceder mediante `enable/disable` SSH a la máquina virtual de la herramienta de detección. Los usuarios pueden acceder mediante SSH a la máquina virtual `ssh discovery@<VM-IP>` después de habilitar el acceso SSH. Se recomienda a los usuarios que mantengan el acceso SSH desactivado la mayoría de las veces y que lo habiliten solo cuando sea necesario de forma activa. El cambio de contraseña se impone cuando se ejecuta `enablessh`.
- Para acceder al directorio de datos de la herramienta de detección en `/home/ec2-user/.local/share/DiscoveryTool`, le recomendamos que lo `ec2-user` cambie corriendo `sudo su ec2-user`.

Configuración de la autenticación de Kerberos

La autenticación Kerberos es el método recomendado para conectarse a los servidores Windows desde la herramienta de detección. La máquina virtual de la herramienta de descubrimiento utiliza bibliotecas Kerberos nativas de Amazon Linux 2023 para autenticarse en su dominio de Active Directory.

Los siguientes son puntos clave sobre la autenticación Kerberos en la máquina virtual de la herramienta de descubrimiento:

- Utilice el `kinit` comando para obtener un vale de Kerberos y `klist` verificarlo.
- El archivo de configuración de Kerberos se encuentra en `/etc/krb5.conf`
- Antes de configurar la herramienta de detección, compruebe que funciona `kinit` correctamente desde la CLI de la máquina virtual de la herramienta de detección.

Requisitos previos de Kerberos

Antes de configurar la autenticación Kerberos, compruebe que dispone de la siguiente información y conectividad de red.

1. Obtenga la siguiente información del administrador de Active Directory:
 - El nombre de dominio de Kerberos (normalmente, el nombre de dominio en mayúsculas, por ejemplo). `EXAMPLE.COM`
 - El nombre de host o la dirección IP del centro de distribución de claves (KDC), que suele ser un controlador de dominio (por ejemplo,). `dc01.example.com`
 - Una cuenta de servicio con permisos para autenticarse en los servidores Windows de destino.
2. Compruebe que la máquina virtual de la herramienta de detección tenga conectividad de red con lo siguiente:
 - El KDC en el puerto 88 (TCP y UDP) para la autenticación Kerberos.
 - Los servidores Windows de destino en los puertos WinRM (5985 para HTTP, 5986 para HTTPS).

Configurar Kerberos

Complete los siguientes pasos para configurar la autenticación Kerberos en la máquina virtual de la herramienta de detección.

1. Utilice SSH para la máquina virtual de la herramienta de detección.

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

2. Edite el archivo de configuración de Kerberos en. `/etc/krb5.conf`

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

Añada la siguiente configuración y sustituya los valores de los marcadores de posición por los detalles de su entorno.

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

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

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

Important

Kerberos distingue entre mayúsculas y minúsculas. El nombre del territorio debe estar en mayúsculas (por ejemplo `EXAMPLE.COM`, no `example.com`). El nombre de dominio de la `[domain_realm]` sección debe estar en minúsculas.

Varios dominios de Active Directory

La herramienta de detección admite varias credenciales de Kerberos para distintos dominios de Active Directory. Cada credencial se autentica de forma independiente, por lo que puede configurar varias credenciales de forma normal y el aislamiento es automático.

Si tiene servidores en varios dominios, añada entradas para cada dominio del archivo `/etc/krb5.conf`:

```
[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. Compruebe que puede obtener un vale de Kerberos ejecutando el `kinit` comando.

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

Introduzca la contraseña cuando se le pida. Si el comando se completa sin errores, la autenticación se realizó correctamente.

4. Compruebe el ticket ejecutando el `klist` comando.

```
klist
```

El resultado esperado es similar al siguiente.

```
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 la herramienta de detección con el mismo principio, que distingue entre mayúsculas y minúsculas, que utilizó `kinit` (por ejemplo, `username@REALM.COM`).

Es posible que no sea necesaria una `krb5.conf` configuración explícita si su entorno tiene registros SRV de DNS configurados para la detección del servicio Kerberos. [Para obtener más información sobre las opciones de configuración de Kerberos, consulte la documentación del MIT sobre Kerberos `krb5.conf` y el ejemplo del archivo `krb5.conf`.](#)

Busque la configuración de Kerberos en máquinas unidas a un dominio

Si no tiene los detalles de configuración de Kerberos, puede recuperarlos de una máquina Windows que esté unida al dominio. Ejecute los siguientes comandos desde una línea de comandos en la máquina unida a un dominio.

Para buscar el nombre de dominio, ejecute el siguiente comando.

```
echo %USERDNSDOMAIN%
```

Ejemplo de código de salida:

```
EXAMPLE.COM
```

Para buscar el nombre de host del controlador de dominio, ejecute el siguiente comando.

```
nlttest /dsgetdc:EXAMPLE.COM
```

Ejemplo de código de salida:

```
DC: \\dc01.example.com
Address: \\10.0.1.100
Dom Guid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx
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
```

Asigne el resultado a su `krb5.conf` configuración de la siguiente manera:

- Reino: utilice el valor de `%USERDNSDOMAIN%` en mayúsculas (por ejemplo, `EXAMPLE.COM`).
- KDC: utilice el nombre de host DC de la `nlttest` salida (por ejemplo, `.dc01.example.com`)

Configurar el acceso a vCenter

1. En la página de la herramienta de detección, en el paso 1. Configure las fuentes de detección, elija Configurar fuentes.
2. En la página Configurar fuentes de detección, proporcione el nombre descriptivo, el vCenter FQDN/IP, el nombre de usuario y la contraseña.
3. Seleccione Guardar configuración.

La herramienta de detección comienza a recopilar información de vCenter, tal como se describe en [Discovered](#) Inventory.

Tras la configuración inicial, elija Editar acceso a vCenter en el marco de estado de la herramienta Discovery para cambiar la configuración de acceso a vCenter.

La herramienta de detección recopila datos de todos los servidores vCenter configurados en paralelo. Si no se puede acceder a un servidor vCenter durante la recopilación, la herramienta informa de un éxito parcial y continúa recopilando datos del resto de los servidores vCenter.

Si una máquina virtual aparece en varios servidores vCenter (por ejemplo, debido a hosts ESXi compartidos o a vCenter vMotion), la herramienta de detección deduplica automáticamente las máquinas virtuales. Cada máquina virtual única aparece solo una vez en el inventario.

Configure el Hyper-V acceso

1. En la página de la herramienta de detección, en el paso 1. Configure las fuentes de detección, elija Configurar fuentes.
2. En la página Configurar fuentes de detección, proporcione un nombre descriptivo, el FQDN o la dirección IP del host, el tipo de autenticación (NTLM o Kerberos), el nombre de usuario de WinRM y la contraseña de WinRM.
3. Seleccione Guardar configuración.

[La herramienta de detección comienza a recopilar Hyper-V información, tal y como se describe en el inventario descubierto.](#)

La recopilación comienza automáticamente después de guardar las credenciales.

En el Hyper-V caso de los clústeres de conmutación por error, puede añadir varios hosts en el mismo clúster. La herramienta deduplica automáticamente las máquinas virtuales que aparecen en más de un host.

Importa servidores

1. Navegue hasta la página de importación de servidores desde la página de inicio de la herramienta Discovery.
2. Prepare un archivo CSV con las siguientes columnas: `hostname_or_ip` (obligatorio), `os_credential_name` (opcional) y `oracle_credential_name` (opcional).
 - El `hostname_or_ip` valor debe ser una dirección IPv4 válida o un nombre de dominio completo (FQDN).
 - El `os_credential_name` valor, si se proporciona, debe coincidir con el nombre descriptivo de una credencial del sistema operativo que ya haya configurado (SSH, WinRM o SNMP). Déjelo en blanco para los servidores en los que aún no haya configurado una credencial de sistema operativo.
 - El `oracle_credential_name` valor, si se proporciona, debe coincidir con el nombre descriptivo de una credencial de Oracle que ya haya configurado.

3. Cargue el archivo CSV. La herramienta valida todas las filas y rechaza el archivo si alguna fila no es válida.

Tras una importación correcta, la herramienta comienza automáticamente a recopilar las métricas de la base de datos, la red y el sistema operativo de los servidores importados, si las credenciales del sistema operativo están configuradas. Si carga otro archivo CSV, los registros existentes se actualizan sin crear duplicados y los registros nuevos se combinan en el inventario.

Importe una entidad emisora de certificados autofirmada a la herramienta de detección (opcional)

Esto es necesario cuando utiliza WinRM a través de HTTPS y los servidores de destino utilizan certificados HTTPS de WinRM firmados por una autoridad de certificación (CA) autofirmada, y si desea habilitar la opción «Validar el certificado SSL del servidor» en la herramienta de detección.

Requisitos previos

1. Self-signed Certificado de CA que se utilizó para firmar los certificados HTTPS de WinRM en los servidores de destino
2. Certificado en formato PEM (extensión.pem o.crt)

Para importar una entidad emisora de certificados autofirmada en la máquina virtual de la herramienta de detección:

1. SSH a la máquina virtual de la herramienta Discovery
2. Coloque los certificados de CA que firmaron los certificados WinRM de los servidores de destino en el directorio de almacenamiento de confianza de la máquina virtual de la herramienta de /etc/pki/ca-trust/source/anchors/ detección. Por ejemplo: `sudo cp winrm-ca.pem /etc/pki/ca-trust/source/anchors/winrm-ca.pem`. Nota: Si los servidores de destino utilizan certificados firmados por distintas CA, copie todos los certificados de CA pertinentes en este directorio.
3. Actualice el almacén de confianza de certificados: `sudo update-ca-trust`
4. Reinicie la máquina virtual
5. (Opcional) Para comprobar que los certificados se han importado correctamente, puede ejecutar el siguiente comando. `sudo trust list --filter=ca-anchors | grep -A 5 "<certificate_name>"`

Consulte [Instalación y configuración de la administración remota de Windows](#)

Configure la herramienta de detección para el acceso al sistema operativo

Configure el acceso al sistema operativo para que la herramienta de detección pueda:

- Descubra las bases de datos para realizar una evaluación de las bases de datos y ayudar en la migración de las máquinas virtuales,
- Realice un seguimiento de las conexiones de red entre los servidores de su inventario, incluido el proceso asociado a cada conexión, para facilitar el mapeo de las dependencias de las aplicaciones y la planificación de las oleadas. Solo se incluyen las conexiones en las que ambos puntos finales estén en el inventario de la herramienta de detección.

Habilite la herramienta de detección OS Access

1. Diríjase a la página de configuración del acceso al sistema operativo para proporcionar las credenciales de Windows y Linux.
2. Elija un protocolo para el que desee añadir credenciales.
3. Proporcione las credenciales necesarias para el protocolo seleccionado.
4. Seleccione esta opción Auto-connect para que la herramienta de detección pruebe todas las credenciales proporcionadas en los servidores detectados hasta que se encuentren las credenciales coincidentes de cada servidor.

Consulte [the section called “Uso de la Auto-Connect función con precaución”](#) las recomendaciones de seguridad importantes relacionadas con la función de conexión automática.

5. Selecciona Configurar y conectar.

Cuando se complete el proceso de coincidencia del sistema operativo, verá un mensaje que indica que la recopilación de datos está en curso y un error relacionado con los servidores en los que no se encontró ninguna coincidencia de credenciales.

Configuración de protocolos compatibles

Debe configurar los protocolos WinRM, SSH y SNMP en los servidores de destino para que la herramienta de detección se comuniquen con ellos.

Configuración de WinRM y WMI

WinRM se instala automáticamente con todas las versiones actualmente compatibles del sistema operativo Windows.

Para comprobar o editar la configuración de WinRM, utilice la herramienta de línea de `winrm` comandos:

- Compruebe los oyentes WinRM instalados: `winrm enumerate winrm/config/listener`
- Compruebe las configuraciones de WinRM: `winrm get winrm/config`
- Ejemplo de comando para configurar WinRM: `winrm quickconfig -transport:https`

Puertos de escucha

El puerto HTTP predeterminado es 5985; HTTPS es 5986. Puede utilizar otros puertos según sea necesario. Los puertos deben estar abiertos entre la herramienta de detección y los servidores de destino.

Cifrado

La herramienta de detección utiliza una comunicación WinRM cifrada. Recomendamos que los oyentes de WinRM en los servidores de destino también utilicen el cifrado: `winrm set winrm/config/service '@{AllowUnencrypted="false"}'`

NTLM frente a Kerberos

La herramienta de detección admite los protocolos de autenticación WinRM Kerberos y NTLM. NTLM solo se puede usar con HTTPS y Kerberos se puede usar tanto con HTTP como con HTTPS.

Requisitos de WMI

La herramienta de detección consulta los siguientes espacios de nombres de WMI. La cuenta WinRM necesita acceso de lectura a cada espacio de nombres relevante para los módulos de su colección:

Espacio de nombres WMI	Utilizado por
<code>root\cimv2</code>	Métricas del sistema operativo, metadatos Hyper-V del host, colección de SQL Server
<code>root\virtualization\v2</code>	Hyper-V Inventario de máquinas virtuales

Espacio de nombres WMI	Utilizado por
root\StandardCIMV2	Recopilación de redes
root\Microsoft\SqlServer\ComputerManagement*	Colección SQL Server
root\Microsoft\SqlServer\ReportServer*	Colección SQL Server (SSRS)

Para la recopilación en red, asegúrese de que se cumplan estas condiciones:

- Permita la conectividad de red a través de ICMP
- Permita la conectividad de red a través del puerto TCP 135 o un rango de puertos TCP efímeros (49152 - 65535)
- Deshabilite el UAC
- Los permisos DCOM remotos están configurados
- Cree una cuenta de servicio dedicada con los permisos mínimos necesarios
- Los permisos de espacio de nombres de WMI están configurados para las cuentas de Windows con los espacios de nombres:, clase \\root\\standardcimv2 MSFT_NetTCPConnection

Para la recopilación de SQL Server, se requiere una cuenta de Windows (local o de dominio) que pertenezca al grupo de administradores locales debido a los complejos requisitos de permiso de los objetos de WMI.

Configurar SSH

- El puerto predeterminado es 22. Se admiten los puertos personalizados. El puerto configurado debe estar abierto entre la herramienta de detección y los servidores de destino.
- Para que la recopilación de redes SSH funcione correctamente, proporcione un usuario configurado para realizar operaciones de sudo sin contraseña.
- Asegúrese de que los siguientes comandos estén disponibles en los servidores Linux de destino (instalados de forma predeterminada en la mayoría de las distribuciones): ss o netstat para la recopilación de redes y, lsblk, iostat dmidecode smartctl top ps freeip, y df para la recopilación de métricas del sistema operativo.

La herramienta de detección admite dos métodos de autenticación para SSH:

Opción 1: nombre de usuario y contraseña

Proporcione el nombre de usuario y la contraseña de SSH. Este es el método de autenticación predeterminado.

Opción 2: clave privada SSH

Proporcione el nombre de usuario de SSH y una clave privada en formato PEM. Para usar esta opción, elija la clave SSH en el menú desplegable del tipo de autenticación al configurar las credenciales SSH. Si la clave privada está cifrada con una frase de contraseña, introdúzcala en el campo opcional Frase de contraseña clave.

Se admiten los siguientes formatos de clave:

- RSA
- ECDSA
- Ed25519
- Formato OpenSSH
- Formato PKCS #8

Ambos métodos de autenticación admiten la conexión automática. Las credenciales se almacenan cifradas en reposo.

Configure SNMP

- El puerto predeterminado es 161/UDP. Se admiten puertos personalizados. El puerto configurado debe estar abierto entre la herramienta de detección y los servidores de destino.
- Para SNMP v2: proporcione una cadena de comunidad de solo lectura que pueda acceder a los OID de conexión TCP.
- Para SNMP v3: proporcione username/password auth/privacy detalles con un permiso de solo lectura que pueda acceder a los OID de conexión TCP

La herramienta de detección requiere acceso 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 el acceso a la base de datos Oracle

Configure el acceso a la base de datos Oracle para recopilar metadatos detallados de la base de datos Oracle directamente a través de conexiones SQL. Los metadatos recopilados incluyen la topología de CDB y PDB, el uso de las funciones y las opciones instaladas. Estos datos le ayudan a planificar las migraciones de bases de datos Oracle con mayor precisión. Puede recopilar Oracle Database 12c versión 1 (12.1) y versiones posteriores mediante conexiones SQL directas. OS-level la detección alternativa funciona con todas las versiones de Oracle.

Configure las credenciales de Oracle en la herramienta de detección

1. En la página de la herramienta de detección, en la barra lateral, elija Acceso a la base de datos.
2. Seleccione Añadir credencial de Oracle.
3. Proporcione la información siguiente:
 - Nombre descriptivo: nombre descriptivo de esta credencial (por ejemplo, Oracle Production).
 - Puerto: el puerto de escucha de Oracle (predeterminado, 1521).
 - Nombre del servicio: el nombre del servicio de Oracle para la base de datos de destino.
 - Nombre de usuario: el nombre de usuario de la cuenta de servicio de Oracle.
 - Contraseña: la contraseña de la cuenta de servicio de Oracle.
 - Auto-connect— Active esta opción para probar la credencial en todos los servidores de su inventario. Desactive esta opción para asignar manualmente la credencial a servidores específicos.
4. Para añadir más credenciales (por ejemplo, para distintos entornos de Oracle), vuelva a seleccionar Añadir credenciales de Oracle.
5. Seleccione Save.

Modos de credenciales

Al configurar las credenciales de Oracle, puede elegir entre dos modos:

- **Manual:** fije una credencial a un servidor específico. La herramienta de detección usa esa credencial exclusivamente para ese servidor. Si se produce un error en la conexión, no se produce ningún retroceso. Corrija la configuración de credenciales para resolver el problema.
- **Auto-connect—** La herramienta de detección prueba cada credencial de conexión automática con todos los servidores de su inventario. Cuando una credencial es correcta para un servidor, la herramienta de detección la usa en todas las rondas de recolección posteriores.

Flujo de detección

Al configurar las credenciales de Oracle, la herramienta de detección primero intenta establecer una conexión SQL directa. Si fallan todas las credenciales de la base de datos, la herramienta recurre a la OS-level detección mediante SSH o WinRM, por lo que puede seguir detectando instalaciones de Oracle sin acceso a la base de datos.

Actualización de la herramienta de detección

La herramienta de detección no tiene una función de actualizaciones automáticas; sin embargo, recibirá una notificación de recordatorio después de 30 días de la instalación para actualizar. Se recomienda mantener la aplicación actualizada para recibir las últimas funciones y parches de seguridad.

Para actualizar la herramienta manualmente

1. Descargue el archivo de imagen más reciente de la herramienta de detección (OVA para VMware o VHD para Hyper-V) desde el enlace proporcionado.
2. (Opcional) Se recomienda eliminar el archivo de imagen de la herramienta de detección anterior antes de implementar el más reciente.
3. Siga los pasos de la sección Implementar la herramienta de descubrimiento para implementar la versión actualizada.

Revocar el acceso

Puede revocar el acceso a cada fuente de descubrimiento de forma independiente. Al revocar el acceso a una fuente, los datos de otras fuentes no se ven afectados.

- **Revocar el acceso a vCenter:** elimina las credenciales y los datos de vCenter. VMware-collected No elimina Hyper-V los datos, los datos de servidor importados ni las credenciales del sistema operativo.

- Revocar el Hyper-V acceso: solo elimina Hyper-V las credenciales y Hyper-V-collected los datos.
- Eliminar servidores importados: elimina los servidores importados del inventario. Se conservan los datos de recopilación posteriores (red, base de datos) que se recopilaban de esos servidores.

Permisos necesarios para la herramienta de detección

La herramienta de descubrimiento se conecta a su infraestructura mediante varios protocolos. Cada protocolo y módulo de recopilación requiere permisos de cuenta específicos. En esta sección se describen los permisos mínimos necesarios para completar la recopilación de datos y los datos que se pierden si determinados permisos no están disponibles.

vCenter de VMware

La herramienta de detección se conecta a VMware vCenter Server en el puerto 443 (HTTPS) y realiza operaciones de solo lectura. No se realizan cambios en el entorno de vCenter.

Función mínima requerida: Read-Only, asignada en el nivel raíz de vCenter.

El Read-Only rol proporciona todo el acceso que la herramienta de detección necesita para recopilar el inventario de las máquinas virtuales (nombre, UUID, CPU, memoria, disco, red, estado de alimentación, sistema operativo huésped) y métricas de rendimiento (uso de la CPU, uso de memoria, IOPS del disco y rendimiento).

Recomendación: cree un usuario de vCenter dedicado con la Read-Only función integrada en el nivel del centro de datos raíz.

Hyper-V hosts (Windows)

La herramienta de detección se conecta a los Hyper-V hosts a través de WinRM (puerto 5985 para HTTP, puerto 5986 para HTTPS) y ejecuta PowerShell comandos para recopilar el inventario de las máquinas virtuales, los metadatos del host y el rendimiento del almacenamiento.

Pertenencias de grupo mínimas requeridas en cada host: Hyper-V

Grupo de Windows	¿Por qué es necesario
Usuarios de administración remota	Acceso remoto básico a WinRM

Grupo de Windows	¿Por qué es necesario
Hyper-V Administradores	Recopilación de inventario de máquinas virtuales (lista de máquinas virtuales, disco, red, memoria, sistema operativo huésped)
Usuarios del monitor de rendimiento	Contadores de I/O rendimiento de almacenamiento (read/write IOPS y rendimiento por máquina virtual)

La cuenta también necesita acceso de lectura de WMI al espacio de `root\cimv2` nombres de la versión del sistema operativo del host y del UUID del hardware. Este acceso se concede de forma predeterminada a los administradores locales, pero debe configurarse de forma explícita para las cuentas que no son de administrador.

Recomendación: Cree una cuenta de servicio de dominio dedicada y agréguela a los grupos de usuarios de administración remota, Hyper-V administradores y usuarios del monitor de rendimiento de cada Hyper-V host. Evite utilizar cuentas de administrador de dominio.

Servidores Linux (SSH)

La herramienta de detección se conecta a los servidores Linux a través de SSH (puerto 22) para recopilar las métricas del sistema operativo, las conexiones de red y el inventario de los servidores. La mayor parte de la recopilación de datos se ejecuta como un usuario normal. Si el comando `sudo` no está disponible, un pequeño número de comandos lo intentan `sudo` y se retiran automáticamente.

Acceso mínimo requerido: una cuenta de usuario SSH que pueda iniciar sesión en el servidor de destino.

Acceso recomendado: el mismo usuario de SSH configurado con `sudo` sin contraseña para una recopilación completa de datos.

Qué requiere `sudo` y qué sucede sin él:

Datos recopilados	¿Se necesita Sudo?	¿Qué pierdes sin sudo
Nombre del servidor, sistema operativo, CPU, memoria, IP, número de discos	No	Nada: se recopiló como usuario normal
Utilización de la CPU, la memoria y la red	No	Nada: se recopiló como usuario habitual
IOPS, rendimiento y espacio en disco	No	Nada: se recopiló como usuario habitual
Configuración de la interfaz de red	No	Nada: se recopiló como usuario habitual
Procesos en ejecución (nombre, PID, comando)	No	Nada: se recopiló como usuario normal
UUID del servidor y UUID de SMBIOS	Sí	Los campos UUID están vacíos en la exportación
Fabricante de hardware (detección física frente a detección virtual)	Sí	La detección del tipo de recurso es menos precisa en las distribuciones más antiguas
Detección de volumen lógico LVM	Sí	No se detectaron los volúmenes LVM; el tipo de volumen puede mostrarse como «Desconocido»
Conexiones de red con nombre de proceso y PID	Sí	Las conexiones se siguen recopilando, pero sin la atribución del proceso (las columnas PID y nombre del proceso están vacías)
OS-level Detección de bases de datos Oracle (alternativa cuando las credenciales de Oracle no están configuradas)	Sí	La detección básica de presencia de Oracle (oratab, monitor de procesos) funciona sin sudo. La recopilación detallada (opatch, lsnrctl, ASM, Grid Infrastructure) requiere el acceso sin contraseña a los archivos binarios raíz de Oracle. <code>sudo -u oracle</code>

Note

La herramienta de descubrimiento nunca falla por completo debido a la falta de sudo. Recopila todo lo que puede e informa de resultados parciales. Sin embargo, para obtener los datos más completos, especialmente el mapeo de dependencias de la red con los nombres de los procesos, recomendamos utilizar el método sudo sin contraseña.

Utilidades necesarias en los servidores de destino: deberían estar disponibles los siguientes comandos (instalados de forma predeterminada en la mayoría de las distribuciones de Linux): `ss` o `netstat`, `lsblk`, `top`, `ps`, `free`, `ip`, `df`, `hostname`, `cat` y `nproc` `grep`. Opcional para datos adicionales: `iostat` (I/O detalle del disco), `dmidecode` (UUID de hardware), `smartctl` (tipo de interfaz de disco), `lvdisplay` (detección LVM).

Servidores Windows (WinRM): métricas del sistema operativo

La herramienta de detección se conecta a los servidores Windows a través de WinRM para recopilar métricas del sistema operativo (inventario del servidor, rendimiento, almacenamiento, interfaces de red y procesos en ejecución).

Acceso mínimo requerido: una cuenta WinRM-enabled de usuario con acceso remoto al servidor de destino.

Acceso recomendado: un usuario del grupo de administradores local para una recopilación completa de datos.

Nivel de permiso	Qué permite	¿Qué pierdes sin él
Usuarios de administración remota (acceso WinRM)	Toda la recopilación de datos de Windows	No se recopilaron datos del servidor
Acceso de lectura WMI a <code>root\cimv2</code>	Nombre del servidor, versión del sistema operativo, memoria, UUID, serie de la BIOS, espacio en disco	Los campos del inventario del servidor están vacíos
Usuarios del monitor de rendimiento	Utilización de la CPU, rendimiento de la red, IOPS de disco y rendimiento	No se recopilaron métricas de rendimiento

Nivel de permiso	Qué permite	¿Qué pierdes sin él
Administrador local	Nombres de los propietarios del proceso en ejecución	Se recopiló la lista de procesos, pero la user/owner column está vacía

Note

La membresía de administrador local otorga implícitamente a los usuarios de Performance Monitor acceso y acceso de lectura a WMI, por lo que cumple todos los requisitos anteriores.

Note

La detección OS-level alternativa de bases de datos Oracle en Windows utiliza consultas de registro Get-Service y Get-Process comandos cuando las credenciales de Oracle no están configuradas. Estos comandos solo requieren el acceso estándar de los usuarios de Remote Management. No se necesitan permisos adicionales más allá de los requisitos de las métricas del sistema operativo.

Servidores Windows (WinRM): colección SQL Server

La colección SQL Server detecta las instancias de SQL Server, Reporting Services (SSRS) e Integration Services (SSIS) en servidores Windows.

Acceso recomendado: un usuario del grupo de administradores local de cada servidor Windows de destino.

Se recomienda el administrador local porque la detección de SQL Server consulta varios espacios de nombres de WMI y requiere un acceso elevado para algunas operaciones:

¿Qué se descubre	Se necesita permiso	¿Qué pierdes sin él
Instancias del motor de base de datos de SQL Server (versión, edición, estado)	Acceso de lectura de WMI a los espacios de root\Micr	No se detectaron instancias de SQL Server

¿Qué se descubre	Se necesita permiso	¿Qué pierdes sin él
	Microsoft\SqlServer\ComputerManagement* nombres	
SQL Server Reporting Services (SSRS)	Acceso de lectura de WMI a los espacios de root\Microsoft\SqlServer\ReportServer nombres	No se detectaron los componentes de SSRS
Configuración de puertos y URL de SSRS	Privilegios elevados (administrador local)	Faltan los detalles de reserva de la URL de SSRS
SQL Server Integration Services (SSIS)	Acceso de lectura al registro (HKLM)	Faltan la versión y la edición del SSIS
Port-to-service asociación	Acceso a la enumeración de receptores TCP	No se pueden asociar los puertos de escucha a los servicios de SQL Server

Note

La colección de SQL Server es Windows-only. La herramienta de detección omite los servidores Linux para la detección de SQL Server.

Base de datos Oracle (SQL)

La colección de bases de datos Oracle se conecta directamente a las instancias de Oracle en el puerto 1521 (o un puerto personalizado) para recopilar los metadatos de la base de datos. La herramienta de descubrimiento no requiere privilegios de DBA o SYSDBA.

Acceso mínimo requerido: una cuenta de servicio de Oracle de solo lectura con la concesión `SELECT_CATALOG_ROLE`.

La herramienta de detección no accede a las vistas de Diagnostics Pack ni Tuning Pack, por lo que no se requiere ninguna licencia adicional de Oracle para la recopilación de datos.

SQL para crear la cuenta:

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

OS-level alternativa: si las credenciales de la base de datos no están configuradas o se produce un error en la conexión, la herramienta de detección utiliza las credenciales de SSH o WinRM OS existentes para detectar las instalaciones de Oracle. No se necesitan permisos de Oracle-specific sistema operativo adicionales más allá de lo que requiere el módulo de métricas del sistema operativo.

Recopilación de redes

La recopilación de redes utiliza diferentes protocolos según el sistema operativo del servidor:

Sistema operativo del servidor	Protocolo	Permisos necesarios
Linux	SSH	Usuario habitual de datos de conexión. Se recomienda usar el sudo sin contraseña para obtener detalles a nivel de proceso (PID y nombre del proceso).
Linux	SNMPv2	Cadena comunitaria de solo lectura con acceso a la MIB de TCP (tcpConnState, tcpConnectionProcess) y a la MIB de recursos de host (hr). SWRunName
Linux	SNMPv3	Un usuario de USM con acceso de lectura a las mismas MIB que el SNMPv2. Admite los niveles de seguridad noAuthNoPriv, auth y NoPriv AuthPriv.
Windows	WinRM	Acceso de lectura de WMI al espacio de root\StandardCIMV2 nombres (clase MSFT_NetTCPConnection).

Referencia rápida: permisos mínimos por caso de uso

Caso de uso	Tipo de cuenta	Permisos mínimos
Descubrimiento de máquinas virtuales de VMware	Usuario de vCenter	Read-Only rol en el nivel del centro de datos raíz
Hyper-V Descubrimiento de máquinas virtuales	Dominio de Windows o cuenta local	Usuarios de administración remota, Hyper-V administradores y usuarios del monitor de rendimiento en cada host
Métricas del sistema operativo Linux: datos completos	Usuario de SSH	Sudo sin contraseña
Métricas del sistema operativo Linux: datos parciales	Usuario de SSH	Usuario normal (sin sudo). Faltará la información sobre el UUID, el fabricante, el LVM y el proceso de red.
Métricas del sistema operativo Windows: datos completos	Usuario de WinRM	Administrador local
Métricas del sistema operativo Windows: datos básicos	Usuario de WinRM	Usuarios de gestión remota + acceso de lectura WMI a root\cimv2
Descubrimiento de bases de datos de SQL Server	Usuario de WinRM	Administrador local
Descubrimiento de bases de datos Oracle (SQL)	Cuenta de servicio de Oracle	SELECT_CATALOG_ROLE (de solo lectura, sin DBA ni SYSDBA)

Caso de uso	Tipo de cuenta	Permisos mínimos
Colección de redes: Linux (SSH)	Usuario de SSH	Sudo sin contraseña para datos a nivel de proceso; usuario normal solo para datos de conexión
Recopilación de redes: Linux (SNMP)	Cadena comunitaria SNMP o usuario USM	Acceso de lectura a las MIB de TCP y Host Resources
Recopilación de redes: Windows	Usuario de WinRM	Acceso de lectura de WMI a root\StandardCIMV2

Recopilación de datos

Calendario de recopilación de herramientas de descubrimiento

Tras la recopilación inicial de datos de detección, la herramienta de detección sigue funcionando de forma escalonada para evitar la escasez de recursos:

- Descubrimiento de VMware: cada hora (a las 00:00 UTC)
- Hyper-V descubrimiento: cada hora (a las 1:20 UTC)

La herramienta de descubrimiento también recopila las métricas del sistema operativo a través de los siguientes módulos independientes, cada uno con su propio cronograma escalonado:

- Métricas de red: cada 15 segundos, pueden ser menos frecuentes en entornos grandes
- Métricas de rendimiento del servidor: cada 10 minutos (a las :03, :13, :23, :33, :43, :53 UTC)
- Métricas de rendimiento del almacenamiento: cada 10 minutos (a las :07, :17, :27, :37, :47, :57 UTC)
- Procesos en ejecución: cada hora (a las 7:40 UTC)
- Datos de aprovisionamiento de servidores: todos los días (a las 00:05 UTC)
- Datos de aprovisionamiento de almacenamiento: todos los días (a las 00:35 UTC)
- Interfaces de red: todos los días (a las 01:05 UTC)
- Descubrimiento de SQL Server: todos los días (a las 03:05 UTC)
- Descubrimiento de bases de datos Oracle: todos los días (a las 05:05 UTC)

Puede iniciar, detener o activar cada módulo de métricas del sistema operativo de forma independiente mediante **Collect data now**.

Para ejecutar una recopilación manualmente, en el menú **Acciones**, seleccione:

- **Inicio**: habilita el módulo de descubrimiento.
- **Detener**: desactiva el módulo de detección.
- **Recopile datos ahora**: inicia la detección de forma inmediata. Utilice esta opción, por ejemplo, después de realizar un cambio en la red.

Estas acciones se aplican a cada módulo. Puede controlar los módulos de métricas del sistema operativo de forma individual.

Intentos de recopilación de datos del sistema operativo

Cuando se descubre un servidor nuevo, la herramienta de detección prueba cada credencial configurada para cada dirección IP y nombre de host. Una vez que la herramienta de detección encuentra una credencial válida, sigue utilizándola a menos que añada una nueva.

Tras un error de recopilación, la herramienta de detección intenta recopilar los datos de red de un servidor transcurridos 3 minutos, 30 minutos, 2 horas y, después, 6 horas. Tras cuatro intentos fallidos, la herramienta de detección sigue probando todas las credenciales configuradas una vez cada 6 horas.

Inventario descubierto

Tras configurar una fuente de detección, el valor del número de servidores descubiertos en el marco de estado de la herramienta de detección comienza a aumentar. El estado de detección de la fuente configurada cambia a **Habilitado** en el marco del módulo de recopilación. La página de inventario muestra los servidores de todas las fuentes configuradas: máquinas virtuales de VMware, Hyper-V máquinas virtuales y servidores importados. Cada servidor muestra su origen y el estado de la colección por módulo.

Navegue a la página de inventario descubierto para ver los servidores que ha encontrado la herramienta de detección. En esta página, seleccione **Descargar inventario** para descargar un archivo ZIP (`discovery_tool_export.zip`) que contenga hasta 30 días de datos recopilados, incluidos los archivos MPA de todas las fuentes configuradas, los datos de utilización del rendimiento, la información de la base de datos y la información de comunicación entre servidores.

Puede descargar el archivo ZIP mientras la herramienta de detección sigue funcionando y obtener resultados parciales. Cargue este archivo a [Migration Assessment](#) para obtener un modelo de negocio a favor de la migración.

Opciones de exportación

Al exportar datos, puede personalizar la exportación con las siguientes opciones:

Rango de fechas

Seleccione una fecha de inicio y una fecha de finalización para exportar solo los datos recopilados durante ese período de tiempo. Ambas fechas son inclusivas. El intervalo máximo de fechas es de 30 días.

Note

La herramienta de descubrimiento almacena hasta 30 días de datos recopilados. Si necesita datos que abarquen más de 30 días, realice exportaciones incrementales cada 30 días para capturar todos los datos.

Selección de módulos

Elija los módulos de datos que desee incluir en la exportación. Puede exportar todos los módulos o seleccionar algunos específicos:

Módulo	Description (Descripción)
Datos de VMware	Inventario de máquinas virtuales desde servidores vCenter
Hyper-V datos	Inventario de máquinas virtuales desde los Hyper-V hosts
Datos de red	Conexiones de red entre servidores
Inventario de servidores	Información sobre el hardware y el sistema operativo del servidor
Métricas de rendimiento del servidor	Utilización de la CPU, la memoria y la red

Módulo	Description (Descripción)
Rendimiento del almacenamiento del servidor	IOPS y rendimiento del disco
Configuración de almacenamiento	Configuración de disco y volumen
Interfaces de red	Detalles del adaptador de red
Métricas de proceso	Procesos en ejecución
Datos de SQL Server	Inventario de bases de datos de SQL Server
Datos de la base de datos Oracle	Inventario de bases de datos Oracle: CDB, PDB, características, opciones y componentes

Si no selecciona ningún módulo, la herramienta de descubrimiento exporta todos los datos disponibles.

Puntos de datos recopilados

La herramienta de descubrimiento recopila datos completos sobre los componentes de VMware Hyper-V, las métricas del sistema operativo, la base de datos y la red. En las siguientes secciones se detallan los puntos de datos específicos recopilados para cada componente.

Recopilación de datos de VMware

En esta tabla se describe la información de la máquina virtual de VMware recopilada por la herramienta de detección:

Name	Tipo	Categoría	Valor de muestra
vm_name	Cadena	Información de máquina virtual	«w2k22-snmpd-v2-en-us-mssql-2022testcase4-1»
vm_id	Cadena	Información sobre	«vm-30920»

Name	Tipo	Categoría	Valor de muestra
		la máquina virtual	
vm_uuid	Cadena	Información sobre la máquina virtual	«4201ecf8-cc44-ee7e-01da-34dfb2acf6c0»
estado de alimentación	Cadena	Información de máquina virtual	«Encendido»
host	Cadena	Información sobre la máquina virtual	«esxi-70-node1.testlab.local»
dirección_ip_primaria	Cadena	Información sobre la máquina virtual	«192.168.0.52»
2 tazas	Entero	Información de máquina virtual	2
memoria	Entero	Información de máquina virtual	4096
total_disk_capacity_mib	Entero	Información sobre la máquina virtual	32768

Name	Tipo	Categoría	Valor de muestra
os_de acuerdo con el_archivo de configuración	Cadena	Información sobre la máquina virtual	«Microsoft Windows Server 2016 o posterior (64 bits)»
max_cpu_usage_pct_dec	Flotante	Rendimiento de la máquina virtual	79.33
avg_cpu_usage_pct_dec	Flotante	Rendimiento de la máquina virtual	45.06
max_ram_usage_pct_dec	Flotante	Rendimiento de la máquina virtual	63.99
avg_ram_util_pct_dec	Flotante	Rendimiento de la máquina virtual	29.27

Hyper-V recopilación de datos

En esta tabla se describe la información de la máquina Hyper-V virtual recopilada por la herramienta de detección:

Name	Tipo	Categoría	Valor de muestra
vm_name	Cadena	Información de máquina virtual	«win2022hyperv-test-01»

Name	Tipo	Categoría	Valor de muestra
vm_id	Cadena	Información sobre la máquina virtual	«a1b2c3d4-e5f6-7890-abcd-ef1234567890»
estado de alimentación	Cadena	Información de máquina virtual	«Corriendo»
tazas	Entero	Información de máquina virtual	4
memory_mb	Entero	Información sobre la máquina virtual	8192
disk_paths	Cadena	Disk	«C:\ vMS\ disk1.vhdx»
tamaño_disco_gb	Flotante	Disk	127.0
adaptadores_de red	Cadena	Network	«00:15:5» D:01:02:03
direcciones_ip	Cadena	Network	«10.0.1.50»
host_name	Cadena	Host	«hyperv-host-01.example.com»
host_os_version	Cadena	Host	«Centro de datos de Windows Server 2022»
cluster_name	Cadena	Host	«01» FailoverCluster

Name	Tipo	Categoría	Valor de muestra
hypervisor	Cadena	Información sobre la máquina virtual	"Hyper-V"

Datos de servidor importados

Los servidores importados no se detectan automáticamente. Se importan a través de un archivo CSV. La herramienta de detección no recopila datos a nivel de hipervisor para los servidores importados. En su lugar, recopila datos de métricas de la base de datos, la red y el sistema operativo mediante las credenciales del sistema operativo asociadas a cada servidor durante la importación.

Los OS-related datos de la herramienta de descubrimiento

La herramienta de detección recopila el inventario, el rendimiento, el almacenamiento, la interfaz de red y los datos de proceso del servidor a través de SSH (Linux) y WinRM (Windows). En las siguientes tablas se describen los puntos de datos recopilados.

Inventario de servidores (server_inventory.csv)

Combina el aprovisionamiento de servidores (configuración de hardware y sistema operativo) con el rendimiento agregado del almacenamiento. Se recopila cada 24 horas.

Name	Tipo	Categoría	Valor de muestra
server_id	Cadena	Información del servidor	«vm-web-server-01"
server_name	Cadena	Información del servidor	«servidor web-01"
resource_type	Cadena	Información del servidor	«máquina_virtual»
estado_alimentación	Cadena	Información del servidor	«Corriendo»

Name	Tipo	Categoría	Valor de muestra
os_type	Cadena	Información del servidor	«Linux»
os_name	Cadena	Información del servidor	«Amazon Linux»
os_version	Cadena	Información del servidor	«2023»
nombre_host principal	Cadena	Información del servidor	«web-server-01.example.com»
dirección_ip_principal	Cadena	Información del servidor	«10.0.2.101»
máscara de red	Cadena	Información del servidor	«255.255.255.0»
número total de tarjetas de red	Entero	Información del servidor	2
número_total de discos	Entero	Información del servidor	1
cpu_count	Entero	Información del servidor	4
memoria_total_gb	Flotante	Información del servidor	15.88
server_uuid	Cadena	Información del servidor	«4201ecf8-cc44-ee7e-01da-34dfb2acf6c0»
smbios_uuid	Cadena	Información del servidor	«4201ecf8-cc44-ee7e-01da-34dfb2acf6c0»
cluster_name	Cadena	Información del servidor	«clúster de producción-01»

Name	Tipo	Categoría	Valor de muestra
hypervisor_object_id	Cadena	Información del servidor	«vm-30920»
tipo_hipervisor	Cadena	Información del servidor	«VMware»
versión_del_hipervisor	Cadena	Información del servidor	«8.0.0»
hypervisor_hostname	Cadena	Información del servidor	«esxi-node1.example.com»
hypervisor_host_id	Cadena	Información del servidor	«host-1234»
hypervisor_id	Cadena	Información del servidor	«4201ecf8-cc44-ee7e-01da-34dfb2acf6c0»
disk_read_iops_avg	Flotante	Rendimiento del almacenamiento	12,5
disk_read_iops_peak	Flotante	Rendimiento del almacenamiento	245,0
disk_write_iops_avg	Flotante	Rendimiento del almacenamiento	8.3
disk_write_iops_peak	Flotante	Rendimiento del almacenamiento	180.0

Name	Tipo	Categoría	Valor de muestra
disk_total_iops_avg	Flotante	Rendimien to del almacenam iento	20.8
disk_total_iops_peak	Flotante	Rendimien to del almacenam iento	425,0
disk_read_throughput_avg_mbps	Flotante	Rendimien to del almacenam iento	1.2
disk_read_throughput_peak_mbps	Flotante	Rendimien to del almacenam iento	24,5
disk_write_throughput_avg_mbps	Flotante	Rendimien to del almacenam iento	0.8
disk_write_throughput_peak_mbps	Flotante	Rendimien to del almacenam iento	18.0
disk_total_throughput_avg_mbps	Flotante	Rendimien to del almacenam iento	2.0

Name	Tipo	Categoría	Valor de muestra
disk_total_throughput_peak_mbps	Flotante	Rendimiento del almacenamiento	42,5

Métricas de rendimiento del servidor (server_performance_metrics.csv)

Utilización del rendimiento de la CPU, la memoria y la red. Se muestrearon cada 10 minutos y se agregaron durante 30 días.

Name	Tipo	Categoría	Valor de muestra
server_id	Cadena	Información del servidor	«vm-web-server-01»
data_source	Cadena	Información del servidor	«OS»
cpu_utilization_avg_pct	Flotante	CPU	45,06
cpu_utilization_peak_pct	Flotante	CPU	79.33
cpu_count	Entero	CPU	4
memory_total_gb	Flotante	Memoria	15.88
memory_utilization_avg_pct	Flotante	Memoria	29.27
memory_utilization_peak_pct	Flotante	Memoria	63,99
red_en_avg_mbps	Flotante	Network	0.52
red_in_peak_mbps	Flotante	Network	12.3
red_out_avg_mbps	Flotante	Network	0.31
network_out_peak_mbps	Flotante	Network	8.7

Name	Tipo	Categoría	Valor de muestra
red_total_avg_mbps	Flotante	Network	0.83
red_total_peak_mbps	Flotante	Network	21.0

Rendimiento de almacenamiento (server_storage_performance.csv)

Per-volume utilización del espacio I/O y del disco. Se toman muestras cada 10 minutos y se agregan durante 30 días.

Name	Tipo	Categoría	Valor de muestra
server_id	Cadena	Información del servidor	«vm-web-server-01»
data_source	Cadena	Información del servidor	«OS»
disk_volume_id	Cadena	Información sobre el volumen	"/dev/nvme0n1p1"
disk_mount_point	Cadena	Información sobre el volumen	"/"
sistema_de_archivos	Cadena	Información de volumen	«xfs»
disk_total_gb	Flotante	Espacio en disco	30.0
disk_used_gb	Flotante	Espacio en disco	12,5
disk_free_gb	Flotante	Espacio en disco	17.5

Name	Tipo	Categoría	Valor de muestra
disk_read_iops_avg	Flotante	Disco I/O	12,5
disk_read_iops_peak	Flotante	Disco I/O	245.0
disk_write_iops_avg	Flotante	Disco I/O	8.3
disk_write_iops_peak	Flotante	Disco I/O	180.0
disk_total_iops_avg	Flotante	Disco I/O	20.8
disk_total_iops_peak	Flotante	Disco I/O	425,0
disk_read_throughput_avg_mbps	Flotante	Rendimiento del disco	1.2
disk_read_throughput_peak_mbps	Flotante	Rendimiento del disco	24,5
disk_write_throughput_avg_mbps	Flotante	Rendimiento del disco	0.8
disk_write_throughput_peak_mbps	Flotante	Rendimiento del disco	18.0
disk_total_throughput_avg_mbps	Flotante	Rendimiento del disco	2.0
disk_total_throughput_peak_mbps	Flotante	Rendimiento del disco	42.5

Configuración de almacenamiento (storage_config.csv)

Detalles del hardware del disco físico. Se recopilan cada 24 horas.

Name	Tipo	Categoría	Valor de muestra
server_id	Cadena	Información del servidor	«vm-web-server-01»
disk_controller_id	Cadena	Información del disco	"/dev/sda"
vmdk_vhd_file_name	Cadena	Información del disco	«web-server-01.vmdk»
tipo_de_volumen_disco	Cadena	Información del disco	«Virtual»
disk_provisioned_gb	Flotante	Información del disco	30.0
tipo_dispositivo de disco	Cadena	Información del disco	«DISCO DURO SCSI»
tipo_interfaz_disco	Cadena	Información del disco	«SCSI»
protocolo_disco	Cadena	Información del disco	«LSI Logic SAS»

Interfaces de red (network_interfaces.csv)

Configuración del adaptador de red. Se recopila cada 24 horas.

Name	Tipo	Categoría	Valor de muestra
server_id	Cadena	Información del servidor	«vm-web-server-01»
nombre_interfaz	Cadena	Información de la interfaz	«eth0»

Name	Tipo	Categoría	Valor de muestra
índice_interfaz	Entero	Información de interfaz	2
mac_address	Cadena	Información de interfaz	«0A:1B:2C:3D:4E:5F»
tipo_adaptador	Cadena	Información de interfaz	«vmxnet3"
nombre_de_red virtual	Cadena	Información de la interfaz	«Red VM»
virtual_network_id	Cadena	Información de interfaz	«dvportgroup-1234"
conmutador virtual	Cadena	Información de interfaz	«vSwitch0"
dirección_ipv4	Cadena	Config IP	«10.0.2.101"
ipv4_subnet_mask	Cadena	Config IP	«255.255.0"
puerta de enlace ipv4_	Cadena	Config IP	«10.0.2.1"
dirección_ipv6	Cadena	Config IP	«fe80: :a1b:2cff:fe3d:4e5f»
ipv6_prefix_length	Entero	Config IP	64
ipv6_gateway	Cadena	Config IP	«fe80: :1»
servidores dns_	Cadena	Config IP	«10.0.0.2»
dhcp_habilitado	Booleano	Config IP	false
estado_de la interfaz	Cadena	Información de interfaz	«Arriba»
vlan_id	Entero	Información de interfaz	100

Name	Tipo	Categoría	Valor de muestra
is_primary	Booleano	Información de interfaz	true

Procesos en ejecución (process_metrics.csv)

Instantánea de los procesos en ejecución. Se recopila cada hora y se deduplica durante 30 días.

Name	Tipo	Categoría	Valor de muestra
server_id	Cadena	Información del servidor	«vm-web-server-01»
process_name	Cadena	Información del proceso	«sshd»
process_id	Entero	Información del proceso	1234
línea de comandos del proceso	Cadena	Información del proceso	«/usr/sbin/sshd -D»
usuario_proceso	Cadena	Información del proceso	«raíz»

Recopilación de redes

El módulo de recopilación de redes le ayuda a descubrir las dependencias entre los servidores de su centro de datos local. Estos datos de red aceleran la planificación de la migración al proporcionar visibilidad sobre la forma en que las aplicaciones se comunican entre los servidores.

Este módulo recopila los datos de red de los servidores de todas las fuentes configuradas, incluido VMware Hyper-V, y de los servidores importados. Utiliza WinRM para recopilar datos de los servidores Windows y utiliza SSH, SNMPv2 y SNMPv3 para recopilar datos de los servidores Linux.

Recopilación de datos de red

El módulo de recopilación de redes captura las conexiones TCP IPv4 en estado ESTABLISHED o TIME_WAIT entre los servidores del inventario descubierto. La conexión aparece en la salida solo cuando las direcciones IP de origen y destino pertenecen a servidores que la herramienta de detección ha descubierto o que usted ha importado. No se incluyen las conexiones hacia o desde direcciones IP ajenas a su inventario, como servicios externos, puntos finales en la nube o servidores que aún no se han agregado a la herramienta de detección.

Este diseño centra los datos de la red en las dependencias de servidor a servidor dentro de su entorno, que es la información necesaria para mapear las dependencias de las aplicaciones y planificar las oleadas de migración.

Estos puntos de datos se recopilan para cada conexión:

Name	Tipo	Categoría	Valor de muestra
IP de origen	Cadena	Connection	«192.168.1.10»
Puerto de origen	Entero	Connection	49152
ID del proceso de origen	Entero	Proceso	1234
Nombre del proceso de origen	Cadena	Proceso	"java"
IP de destino	Cadena	Connection	«192.168.1.20»
Puerto de destino	Entero	Connection	5432
ID del proceso de destino	Entero	Proceso	5678
Nombre del proceso de destino	Cadena	Proceso	"postgres"
Estado	Cadena	Connection	«ESTABLECIDO»
Protocolo de transporte	Cadena	Connection	«TCP»
Versión de IP	Cadena	Connection	«IPv4»

Name	Tipo	Categoría	Valor de muestra
Recuento	Entero	Connection	42

 Tip

Para maximizar la integridad del mapa de dependencias de la red, configure todas las fuentes de detección (VMware y la importación de CSV del servidor) y añada las credenciales del sistema operativo antes de revisar los datos de la red. Hyper-V Cuantos más servidores haya en su inventario, más conexiones podrá capturar el módulo de red.

Recopilación de redes de direcciones privadas

De forma predeterminada, el módulo de recopilación de redes solo captura las conexiones en las que ambos puntos finales son servidores del inventario descubierto. Puede habilitar la recopilación de direcciones privadas para capturar también las conexiones desde y hacia direcciones IP privadas según la norma RFC 1918 (10.0.0. 0/8, 172.16.0. 0/12, 192.168.0. 0/16) que no están en tu inventario.

Para iniciar la recopilación de direcciones privadas

1. En la página de configuración del recopilador, busque la sección de módulos de recopilación.
2. Busque Descubrimiento de conexiones de red en Descubrimiento de aplicaciones.
3. Abre el menú desplegable Acciones.
4. Selecciona Iniciar la recopilación de direcciones privadas.
5. Si el estado del módulo era Habilitado, puede ver cómo cambia a Habilitado · Dirección privada activada.

Para detener la recopilación de direcciones privadas, abre el menú desplegable Acciones y selecciona Detener la recopilación de direcciones privadas. Los datos de direcciones privadas recopilados anteriormente se conservan incluso después de detenerlos.

Las conexiones de direcciones privadas solo aparecen en la exportación CSV completa (dentro del archivo ZIP), no en los archivos CSV de MPA. Si una dirección IP pertenece a un servidor que ya

está en tu inventario, siempre se identifica por su ID de servidor descubierto, independientemente de esta configuración.

Esta configuración se mantiene tras los reinicios. Puedes iniciar o detener la recopilación de direcciones privadas en cualquier momento. Los datos de direcciones privadas recopilados anteriormente se exportan independientemente de la configuración actual.

Recopilación de SQL Server

El módulo de recopilación de SQL Server recopila información de SQL Server de los servidores Windows de todas las fuentes configuradas, incluido VMware Hyper-V, y de los servidores importados. El módulo usa WinRM para conectarse remotamente a cada servidor de Windows y ejecutar PowerShell consultas. Recopila información sobre todos los servicios (componentes) de SQL Server instalados mediante los espacios de nombres, el registro y las propiedades de los archivos de WMI.

Un componente de SQL Server es una instancia de función o servicio específico que se instala como parte de una implementación de SQL Server en un servidor Windows. La herramienta de descubrimiento recopila el motor de base de datos, los servicios de análisis, los servicios de informes y los servicios de integración.

Recopilación de datos de SQL Server

El módulo de recopilación de SQL Server recopila información sobre los componentes de SQL Server. En esta tabla se describen los puntos de datos clave recopilados:

Name	Tipo	Categoría	Valor de muestra
Tipo de motor	Cadena	Componente	sql_server
Es un componente del motor	Booleano	Componente	Y
Status	Cadena	Servicio	Funcionando, parado, StartPending
Versión	Cadena	Servicio	2015.131.5026.0
Edition	Cadena	Servicio	Edición para desarrolladores (64 bits)

Name	Tipo	Categoría	Valor de muestra
Nombre del servicio SQL	Cadena	Servicio	MsDtsServer130, Mssql
Tipo de servicio SQL	Cadena	Servicio	Servicio SQL Server, servicio de servicios de integración
Nombre de instancia	Cadena	Instancia	MSSQLSERVER
Nombre de visualización	Cadena	Servicio	SQL Server (MSSQLSERVER2017)
Modo de inicio	Cadena	Servicio	Automático, manual, desactivado
Nombre de la cuenta de servicio	Cadena	Servicio	NT Service/MsDtsServer130
Está agrupado	Booleano	Configuración	N

Note

El formato completo incluye todos los tipos de servicios. El formato MPA incluye solo los componentes del motor de base de datos. No todos los campos están disponibles según el tipo y la configuración del servicio SQL.

Colección de bases de datos Oracle

Con la recopilación de bases de datos de Oracle, puede descubrir las instancias de bases de datos de Oracle en todas las fuentes configuradas, incluido VMware Hyper-V, y en los servidores importados. El módulo recopila los siguientes datos:

- Enumeración de bases de datos de contenedores (CDB) y bases de datos conectables (PDB)
- Versión y edición
- Opciones instaladas
- Estadísticas de uso de funciones
- Inventario de componentes (DBA_REGISTRY)

- Dimensionamiento de archivos de datos
- Indicadores de topología (RAC, Data Guard y arquitectura multiusuario)

Database-connected (SQL)

Al configurar las credenciales de Oracle, la herramienta de descubrimiento se conecta directamente a la base de datos de Oracle mediante la cuenta de servicio de solo lectura. Esto proporciona una SQL-level recopilación completa que incluye los detalles de la PDB, el uso de las funciones y las opciones instaladas. Todos los archivos CSV contienen datos completos.

OS-level alternativa

Si no ha configurado las credenciales de la base de datos o si se produce un error en la conexión, la herramienta de detección utiliza SSH o WinRM para detectar las instalaciones de Oracle. Descubre los directorios raíz, los dispositivos de escucha, los parches, la versión y la edición de Oracle sin acceso a la base de datos. En el caso de los OS-detected hosts, el CSV de CDB exportado contiene el nombre de la instancia, el nombre del host, la versión y la edición. Los archivos CSV de PDB, características, opciones y componentes no contienen filas.

La colección Oracle genera los siguientes archivos CSV en el ZIP de exportación. Cada tabla describe los puntos de datos recopilados por archivo.

Datos de CDB (oracle_data_cdb_full.csv)

Una fila por instancia de CDB. En esta tabla se describen los puntos de datos del CDB recopilados:

Name	Tipo	Categoría	Valor de muestra	origen
Nombre de instancia	Cadena	Identidad	«ORCL»	SQL, OS
Host Name	Cadena	Identidad	«oracledb01.example.com»	SQL, OS
Nombre de base de datos	Cadena	Identidad	«ORCL»	Solo SQL
Nombre único de la base de datos	Cadena	Identidad	«ORCL_PRIMARY»	Solo SQL
DBID	Entero	Identidad	1234567890	Solo SQL

Name	Tipo	Categoría	Valor de muestra	origen
Versión	Cadena	Versión	«19.0.0.0"»	SQL, OS
Versión completa	Cadena	Versión	«19.21.0.0.0"»	Solo SQL
Edition	Cadena	Versión	«Edición empresarial»	SQL, OS
Tipo de base de datos	Cadena	Configuración	«SOLTERO»	Solo SQL
Rol de base de datos	Cadena	Configuración	«PRINCIPAL»	Solo SQL
Modo abierto	Cadena	Configuración	«LEER Y ESCRIBIR»	Solo SQL
Modo de registro	Cadena	Configuración	«REGISTRO DE ARCHIVOS»	Solo SQL
Plataforma	Cadena	Configuración	«Linux x86 de 64 bits»	Solo SQL
Bandera CDB	Cadena	Configuración	«SÍ»	Solo SQL
Es RAC	Cadena	Topología	«SÍ» o «NO»	Solo SQL
¿Data Guard está en espera	Cadena	Topología	«SÍ» o «NO»	Solo SQL
Modo de protección	Cadena	Topología	«MÁXIMO RENDIMIENTO»	Solo SQL
Data Guard Broker	Cadena	Topología	«HABILITADO»	Solo SQL
Juego de caracteres NLS	Cadena	Configuración	«AL32UTF8"»	Solo SQL
Recuento de PDB	Entero	Ajuste del tamaño	3	Solo SQL
Flashback activado	Cadena	Configuración	«SÍ»	Solo SQL

Name	Tipo	Categoría	Valor de muestra	origen
Ruta de detección	Cadena	Metadatos	«fase 2» o «fase 1 b»	SQL, OS

Datos de PDB (oracle_data_pdb_full.csv)

Una fila por PDB (base de datos conectable). En esta tabla se describen los puntos de datos del PDB recopilados:

 Note

Los datos de PDB requieren credenciales de base de datos Oracle (conexión SQL). OS-level la opción alternativa no rellena este CSV.

Name	Tipo	Categoría	Valor de muestra	origen
Nombre de la instancia de CDB	Cadena	Identidad	«ORCL»	Solo SQL
Nombre de PDB	Cadena	Identidad	«APPPDB1»	Solo SQL
Modo abierto	Cadena	Status	«LEER Y ESCRIBIR»	Solo SQL
Estado del ciclo de vida	Cadena	Status	«NORMAL»	Solo SQL
Recuento de tablespaces	Entero	Ajuste del tamaño	5	Solo SQL
Recuento de archivos de datos	Entero	Ajuste del tamaño	12	Solo SQL
Tamaño total de bytes	Entero	Ajuste del tamaño	5368709120	Solo SQL

Name	Tipo	Categoría	Valor de muestra	origen
Recuento de esquemas de usuario	Entero	Ajuste del tamaño	8	Solo SQL
Número de enlaces de base de datos	Entero	Conectividad	2	Solo SQL
Componentes instalados	Cadena	Configuración	«APEX; JVM; XML»	Solo SQL
Recuento de espacios de tablas cifrados	Entero	Seguridad	1	Solo SQL

Datos de uso de funciones (oracle_data_features_full.csv)

Una fila por entrada de uso de funciones de DBA_FEATURE_USAGE_STATISTICS. En esta tabla se describen los puntos de datos de uso de funciones recopilados:

Note

Los datos de uso de las funciones requieren las credenciales de la base de datos de Oracle (conexión SQL). OS-level la opción alternativa no rellena este CSV.

Name	Tipo	Categoría	Valor de muestra	origen
Nombre de la instancia de CDB	Cadena	Identidad	«ORCL»	Solo SQL
Name	Cadena	Característica	«Particionamiento (usuario)»	Solo SQL
Usos detectados	Entero	De uso	42	Solo SQL
Usado actualmente	Cadena	De uso	«CIERTO»	Solo SQL

Name	Tipo	Categoría	Valor de muestra	origen
Primera fecha de uso	DateTime	De uso	«15-01-2020» T00:00:00	Solo SQL
Fecha de último uso	DateTime	De uso	«2026-06-01T00:00:00»	Solo SQL

Datos de opciones (oracle_data_options_full.csv)

Una fila por entrada de V\$OPTION por CDB. En esta tabla se describen los puntos de datos de las opciones instaladas recopilados:

Note

Los datos de opciones requieren credenciales de base de datos Oracle (conexión SQL). OS-level la opción alternativa no rellena este CSV.

Name	Tipo	Categoría	Valor de muestra	origen
Nombre de la instancia de CDB	Cadena	Identidad	«ORCL»	Solo SQL
Nombre de la opción	Cadena	Opción	«Análisis avanzado»	Solo SQL
Está instalado	Cadena	Opción	«CIERTO»	Solo SQL
ID del contenedor	Entero	Opción	0	Solo SQL

Datos de componentes (oracle_data_components_full.csv)

Una fila por componente DBA_REGISTRY. En esta tabla se describen los puntos de datos de los componentes recopilados:

Note

Los datos de los componentes requieren credenciales de base de datos Oracle (conexión SQL). OS-level la opción alternativa no rellena este CSV.

Name	Tipo	Categoría	Valor de muestra	origen
Nombre de la instancia de CDB	Cadena	Identidad	«ORCL»	Solo SQL
Nombre de PDB	Cadena	Identidad	«APPPDB1»	Solo SQL
ID del componente	Cadena	Componente	«ÁPICE»	Solo SQL
Nombre del componente	Cadena	Componente	«Oracle Application Express»	Solo SQL
Versión	Cadena	Componente	«22.1.0.15.0»	Solo SQL
Status	Cadena	Componente	«VÁLIDO»	Solo SQL
Esquema	Cadena	Componente	«APEX_220100»	Solo SQL

Consideraciones de seguridad

Proteger la máquina virtual de la herramienta de descubrimiento

La seguridad de la máquina virtual de la herramienta de descubrimiento es crucial porque la herramienta de descubrimiento almacena todas las credenciales, los registros y los datos de los clientes en la máquina virtual de la herramienta de descubrimiento.

La máquina virtual de la herramienta de descubrimiento tiene el acceso a SSH desactivado de forma predeterminada y solo se puede acceder a ella desde el clientevCenter UI -> "Launch Web Console".

La herramienta de detección VM viene con una contraseña de inicio de sesión predeterminada («contraseña») para el usuario «discovery».

- Le recomendamos que actualice esta contraseña inmediatamente después de la implementación.
- Es necesario que actualice la contraseña si quiere habilitar ssh mediante el comando `enablessh` después de iniciar sesión con vCenterLaunch Web Console. Tenga en cuenta que cada vez que se ejecute este comando, tendrá que restablecerlo.

Asegurar las credenciales

Mejores prácticas generales para la administración de credenciales

- Guarde las credenciales de forma segura
- Cambie todas las credenciales con regularidad
- Utilice administradores de contraseñas o bóvedas seguras
- Supervise el uso de credenciales
- Siga el principio del mínimo privilegio y conceda únicamente los permisos mínimos necesarios

Credenciales de SNMP v2

- Utilice cadenas de comunidad complejas y no predeterminadas
- Evite cadenas comunes como «pública» o «privada»
- Trate las cadenas de comunidad como contraseñas

Credenciales de SNMP v3

- Habilite tanto la autenticación como la privacidad
- Utilice protocolos de autenticación sólidos (se prefiere el SHA en lugar del MD5)
- Utilice protocolos de cifrado seguros (se prefiere el AES en lugar del DES)
- Utilice contraseñas complejas tanto para la autenticación como para la privacidad
- Usa nombres de usuario únicos (evita los nombres comunes)

Credenciales WinRM

- Evite deshabilitar la comprobación del certificado WinRM.
- Le recomendamos que cree una cuenta de servicio dedicada con los permisos mínimos necesarios.

- Evite usar cuentas de administrador de dominio o de administrador local a menos que necesite la recopilación de SQL Server. La colección de SQL Server requiere el acceso de un administrador local porque consulta varios espacios de nombres de WMI y utiliza comandos elevados. Para las métricas del sistema operativo sin detección de SQL Server, basta con una cuenta que no sea de administrador con usuarios de administración remota, usuarios del monitor de rendimiento y acceso de lectura de WMI. `root\cimv2` Consulte [the section called “Permisos necesarios”](#) para obtener información detallada por módulo.

Hyper-V credenciales

- Utilice cuentas de servicio dedicadas con permisos Hyper-V de administración mínimos.
- Evite usar cuentas de administrador de dominio.
- Hyper-V las credenciales admiten la autenticación NTLM (solo HTTPS) y Kerberos.
- La herramienta de detección almacena las credenciales cifradas en reposo mediante SQLCipher.

Credenciales de Oracle

- Utilice una cuenta de servicio dedicada de solo lectura con `SELECT_CATALOG_ROLE`. No utilice los privilegios de `DBA`, `SYSDBA` o `SYSOPER`.
- La herramienta de detección solo realiza operaciones de lectura y nunca escribe en la base de datos Oracle.
- La herramienta de detección no accede a las vistas de Diagnostics Pack ni Tuning Pack, por lo que no se requiere ninguna licencia adicional de Oracle.
- Cambie la contraseña de la cuenta de servicio de Oracle con regularidad y actualice la credencial en la herramienta de detección.

Almacenamiento de credenciales

La herramienta de descubrimiento cifra las credenciales almacenadas en reposo mediante una clave de cifrado de base de datos. En los sistemas con `systemd 250` o posterior, esta clave se cifra mediante `systemd-creds`. En los sistemas más antiguos, la clave se guarda como un archivo protegido con permisos. En ambos casos, un atacante con acceso root al host de la herramienta de descubrimiento podría acceder a la clave de cifrado y descifrar las credenciales almacenadas. Restrinja el acceso al host de la herramienta de descubrimiento y trátelo como un sistema privilegiado en su entorno.

Utilice la Auto-Connect función con precaución

La herramienta de descubrimiento utiliza dos mecanismos para asignar credenciales a los servidores durante la OS-level recopilación: conexión automática y manual. OS-level La colección incluye los módulos de métricas Network, SQL Server, Oracle Database y OS. Estos módulos se conectan a servidores individuales de todas las fuentes, incluidas las máquinas virtuales de VMware, las Hyper-V máquinas virtuales y los servidores importados.

Manual: un servidor se puede asociar manualmente a una credencial específica. En este caso, la herramienta de detección solo usa esa credencial, independientemente de si se ha realizado correctamente o no. Debe supervisar manualmente el estado de la recopilación de ese servidor y realizar los ajustes necesarios.

Auto-connect: si no hay ninguna credencial asociada manualmente al servidor, la herramienta de detección utiliza el mecanismo de conexión automática para ese servidor. Eso significa que:

- Al comienzo de cada ronda de recopilación, la herramienta de descubrimiento obtiene una lista de credenciales disponibles para ese servidor (en función del tipo de sistema operativo) y también está configurada para que se pueda «conectar automáticamente».
- A continuación, la herramienta de descubrimiento compara todas las credenciales con las del servidor de forma cíclica.
 - Si se encuentra una credencial que funcione, la ronda de recopilación del servidor se realiza correctamente. La herramienta de detección la recuerda y la probará primero la próxima vez.
 - Si no se encuentra ninguna credencial que funcione, la ronda de recopilación del servidor ha fallado.
 - Módulo de red: el servidor utiliza un programa de espera y comienza la siguiente ronda de recopilación a los 3 minutos, 30 minutos, 2 horas y 6 horas después de cada fallo (similar a un retraso exponencial).
 - Recopilación de SQL Server: la herramienta de detección no se vuelve a intentar. Realiza un intento por servidor cada día.

Impacts/Risks:

Utilice la conexión automática únicamente cuando esté seguro de que los riesgos se mitigan en su sistema:

Riesgo 1: si la conexión automática está configurada con varias credenciales incorrectas, probarlas automáticamente en los servidores podría provocar el bloqueo de cuentas en los entornos de producción en los que se configuran políticas de bloqueo. Por ejemplo, un centro de datos puede configurar sus máquinas virtuales para que se bloqueen tras tres intentos fallidos de inicio de sesión mediante SSH. En este caso, si la conexión automática está configurada para 3 credenciales SSH incorrectas, se producirán bloqueos de cuentas legítimos. Si los bloqueos se producen en varios sistemas, los procesos empresariales críticos podrían verse afectados y provocar fallos en cascada en los sistemas dependientes. Además, los centros de operaciones de seguridad podrían sufrir una tormenta de alertas a causa de fallos de autenticación masivos, lo que generaría incidentes de seguridad falsos positivos que agotarían los recursos y podrían enmascarar ataques reales.

Riesgo 2: Un actor con acceso a la herramienta de descubrimiento (conoce la contraseña de la herramienta de descubrimiento) puede forzar por fuerza bruta las credenciales del sistema operativo en todos los servidores, configurando un gran número de credenciales de prueba y utilizando la conexión automática para encontrar las correctas.

Mitigaciones:

Siga estas instrucciones:

- Asegúrese de que la contraseña de la herramienta de descubrimiento esté debidamente protegida y que solo la conozcan las personas autorizadas
- Asegúrese de introducir las credenciales adecuadas para el entorno si existen políticas de bloqueo. Recomendamos configurar únicamente las credenciales conocidas que funcionen, incluso si no existen políticas de bloqueo de cuentas, para garantizar una carga operativa mínima en las máquinas virtuales individuales.
- "Auto-connect" es una función opcional. No la seleccione y utilice la asignación manual de credenciales si los bloqueos de cuentas son un problema para el medio ambiente.

Seguridad de importación de CSV

Al importar servidores mediante un archivo CSV, tenga en cuenta las siguientes implicaciones de seguridad:

- El archivo CSV puede contener nombres de host o direcciones IP de servidores internos. Trátelos como datos confidenciales.
- Las `oracle_credential_name` columnas `os_credential_name` y hacen referencia a las credenciales preconfiguradas por un nombre descriptivo. El CSV no contiene secretos.

- All-or-nothing validación: si alguna fila del CSV no es válida, se rechaza toda la carga. Esto evita las importaciones parciales que podrían crear un estado confuso.
- Los servidores importados son visibles inmediatamente en el inventario y son aptos para su recogida. Asegúrese de que las credenciales de OS y Oracle tengan el alcance correcto antes de realizar la importación.

Consideraciones sobre la revocación del acceso

Al revocar el acceso, la eliminación se realiza en función de la fuente específica:

- Al revocar el acceso a vCenter, solo se eliminan los datos de vCenter. No afecta a los datos del servidor Hyper-V ni a los importados.
- Al revocar el Hyper-V acceso, solo Hyper-V se eliminan los datos. No afecta a VMware ni a los datos de servidor importados.
- Al eliminar los servidores importados, se eliminan del inventario, pero se conservan los datos de recopilación posteriores (redes, bases de datos, métricas del sistema operativo).
- Para eliminar todos los datos de inventario específicos de una fuente, debes revocar o eliminar cada fuente de forma independiente. Los datos de recopilación posteriores (red, base de datos, métricas del sistema operativo) se conservan incluso después de revocar todas las fuentes.

Resolución de problemas

Verificación de la conectividad de la herramienta de detección con vCenter

Cuando se produzcan errores de configuración de los módulos de VMware, siga estos pasos para verificar la conectividad:

Acceda a la herramienta de descubrimiento VM

- Log-in a la máquina virtual de la herramienta de detección, abra Remote Console en vCenter
 - Nombre de usuario: discovery
 - Contraseña: contraseña

Pruebe la conectividad de vCenter

1. Pruebe el acceso a la API de vCenter:

```
curl -v --insecure -u <username>:<password> https://<vcenter-ip-or-hostname>:443/mob
```

2. Resultado de éxito esperado:

```
[ec2-user@discoverytool ~]$ curl -v --insecure -u <user>:<password> https://vcsa/mob > tmp.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %         Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0     0  --:--:-- --:--:-- --:--:--    0*
Trying 192.168.2.125:443...
* Connected to vcsa (192.168.2.125) port 443 (#0)
...
</xml>
* Connection #0 to host vcsa left intact
```

Pruebe el certificado SSL

1. Ejecute este comando:

```
openssl s_client -showcerts -servername <hostname> -connect <hostname>:443
```

2. Resultado de éxito esperado:

- Debe mostrar los detalles del certificado de vSphere
- Verifica la SSL/TLS conectividad en el puerto 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
---

```

Solución de problemas de WinRM

Si tienes problemas de conectividad con WinRM, sigue estos pasos para probar la conexión. Estos pasos también se aplican a los problemas de Hyper-V conectividad, ya que la herramienta de detección utiliza WinRM para comunicarse con Hyper-V los hosts.

Pruebe la conectividad WinRM básica mediante los puertos 5985 (HTTP) y 5986 (HTTPS). Debemos asegurarnos de que la conectividad funcione en el puerto 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

```

Si las pruebas anteriores fallan, intente establecer una PowerShell sesión con la validación de certificados deshabilitada:

```

$cred = Get-Credential
$so = New-PsSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck

```

```
Enter-PSSession -ComputerName <HOST> -Credential $cred -Port 5985 -SessionOption $so
```

Solución de problemas de Kerberos

Si se producen errores en la autenticación de Kerberos al recopilar datos de los servidores Windows, utilice las siguientes secciones para diagnosticar y resolver los problemas más comunes.

Compruebe los requisitos de la red

Antes de solucionar los problemas de autenticación Kerberos, compruebe que la herramienta de detección pueda llegar a los puntos finales de red necesarios.

Para comprobar los requisitos de red para Kerberos

1. Compruebe la resolución de DNS en el controlador de dominio. Ejecute el siguiente comando desde la máquina virtual de la herramienta de detección:

```
nslookup dc01.example.com
```

Como alternativa también puede utilizar dig.

```
dig dc01.example.com
```

Si se produce un error en la resolución de DNS, compruebe que la máquina virtual de la herramienta de detección esté configurada para usar un servidor DNS que pueda resolver su dominio de Active Directory. Compruebe `/etc/resolv.conf` y confirme que las entradas del servidor de nombres apuntan a los servidores DNS de su dominio.

2. Compruebe la conectividad con el centro de distribución de claves (KDC) en el puerto 88. Use el siguiente comando:

```
nc -zv dc01.example.com 88
```

Resultado previsto:

```
Connection to dc01.example.com 88 port [tcp/kerberos] succeeded!
```


Si se produce un error en la conexión, compruebe que ninguna regla de firewall bloquee el tráfico desde la máquina virtual de la herramienta de detección al controlador de dominio en el puerto 88.

3. Compruebe la conectividad con los servidores Windows de destino en los puertos WinRM. Ejecute los siguientes comandos :

```
nc -zv <windows-server> 5985
nc -zv <windows-server> 5986
```

Si se produce un error en la conexión, compruebe que WinRM esté activado en el servidor de destino y que las reglas del firewall permitan el tráfico entrante en los puertos 5985 y 5986.

Problemas comunes de Kerberos

A continuación, se muestran los problemas comunes de Kerberos y sus soluciones.

Errores de distinción de mayúsculas y

Síntoma: recibe el error «No se encuentra el servidor en la base de datos de Kerberos» durante la autenticación.

Este error suele producirse cuando el nombre del territorio de Kerberos no está en mayúsculas. Los dominios de Kerberos deben especificarse en mayúsculas en el archivo. `krb5.conf` Por ejemplo, utilice `EXAMPLE.COM` en lugar de `example.com`.

Prevención del bloqueo de cuentas

La herramienta de detección utiliza un mecanismo de espera para evitar el bloqueo de cuentas debido a intentos de autenticación fallidos repetidos. Si su cuenta de servicio queda bloqueada, puede restablecer el proceso de recopilación deteniendo e iniciando el módulo de recopilación a través de la interfaz de usuario web de la herramienta de detección en. `https://<discovery-tool-vm-ip>:5000`

kinit falla desde CLI

En la siguiente tabla se enumeran `kinit` los errores más comunes y sus soluciones.

Error	Causa	Solución
No se encuentra el KDC para el dominio	No se puede acceder al nombre de host o la dirección IP del KDC, o el dominio no está configurado en <code>krb5.conf</code>	Compruebe que el <code>krb5.conf</code> archivo contiene el nombre de host y el dominio correctos del KDC. Confirme la resolución del DNS y la conectividad de red con el KDC en el puerto 88.
Falló la autenticación previa	La contraseña de la cuenta de servicio es incorrecta.	Compruebe la contraseña e inténtelo de nuevo. Si la cuenta está bloqueada, desbloquéela en Active Directory antes de volver a intentarlo.
No se encontró el cliente en la base de datos de Kerberos	El nombre principal no coincide con ninguna cuenta de Active Directory.	Compruebe que el nombre principal coincide exactamente con el nombre de la cuenta, incluidas las mayúsculas y minúsculas. Utilice el formato <code>username@REALM</code> con el dominio en mayúsculas.
No se puede resolver la dirección de red del KDC	El DNS no puede resolver el nombre de host del KDC.	Compruebe la configuración de DNS en <code>/etc/resolv.conf</code> . Confirme que el servidor DNS puede resolver el nombre de host del KDC. Pruebe con <code>nslookup</code> o <code>dig</code>

La recolección falla a pesar del éxito del `kinit`

Si se `kinit` realiza correctamente, pero la recopilación de datos sigue fallando, compruebe lo siguiente:

1. Compruebe que el nombre principal utilizado para la recopilación coincida `kinit` exactamente con el caso utilizado durante la recopilación.
2. Compruebe que la cuenta de servicio tenga los permisos necesarios en los servidores de destino.
3. Compruebe que WinRM esté activado en los servidores de destino.
4. Compruebe que el nombre de host utilizado para la recopilación coincida con el nombre de host registrado en Active Directory.

Kerberos funciona en algunos servidores, pero no en otros

Si la autenticación Kerberos se realiza correctamente en algunos servidores pero no en otros, investigue las siguientes áreas:

Si sus servidores abarcan varios dominios de Active Directory, configure una credencial Kerberos independiente para cada dominio. Asegúrese de que el `/etc/krb5.conf` archivo incluya entradas para todos los dominios. Cada dominio requiere su propia credencial con el director `correctusername@REALM`.

Compare la configuración de WinRM en un servidor en funcionamiento con la de un servidor defectuoso. Ejecute el siguiente comando en cada servidor:

```
winrm get winrm/config
```

Pruebe la conectividad con Remote Desktop para aislar el problema. La herramienta de detección usa el `formatusername@DOMAIN`, mientras que Remote Desktop usa el `formatDOMAIN\username`.

Compruebe que la cuenta de servicio es miembro del grupo de administradores local del servidor que falla. Ejecute el siguiente comando en el servidor de destino:

```
net localgroup Administrators
```

WMI requiere privilegios de administrador local para acceder a la información del sistema operativo. La recopilación de SQL Server también requiere que la cuenta de servicio tenga acceso de administrador local en el servidor de destino.

Lista de verificación de configuración de Kerberos

Utilice la siguiente lista de comprobación para comprobar la configuración de Kerberos antes de iniciar la recopilación de datos.

- El `krb5.conf` archivo existe en la máquina virtual de la herramienta de detección.
- El nombre del dominio está escrito en mayúscula. `krb5.conf`
- La ejecución `kinit` con la cuenta de servicio se realiza correctamente sin errores.
- Si se ejecuta, se `klist` muestra un billete válido y no caducado.
- El nombre principal coincide exactamente con el nombre de la cuenta de Active Directory.
- La resolución de DNS funciona para el nombre de host del KDC.

- Se ha confirmado la conectividad de red con el KDC en el puerto 88.
- Se ha confirmado la conectividad de red con los servidores Windows de destino en los puertos 5985 y 5986.
- (Multi-domain) Cada dominio de Active Directory tiene su propia credencial configurada en la herramienta de detección [realms] y krb5.conf contiene [domain_realm] entradas para todos los dominios.

Solución de problemas de bases de datos

Para diagnosticar problemas de recopilación de bases de datos Oracle, como datos faltantes o errores, compruebe lo siguiente.

Conexión rechazada o se ha agotado el tiempo de espera

Síntoma: el estado de recopilación de Oracle muestra un error de conexión para un servidor.

Para solucionar este problema, compruebe lo siguiente:

- Compruebe que el agente de escucha de Oracle se esté ejecutando en el host de destino:
`lsnrctl status`
- Compruebe la conectividad de red desde la herramienta de detección al host de Oracle en el puerto 1521 (o en su puerto personalizado): `nc -zv <oracle-host> 1521`
- Compruebe que las reglas del firewall permiten las conexiones entrantes en el puerto de escucha de Oracle.
- Compruebe el nombre del servicio ejecutándolo `lsnrctl services` en el host de Oracle. Si el nombre del servicio es incorrecto, el agente de escucha de Oracle rechaza la conexión.

Fallos de autenticación () ORA-01017

Síntoma: la recopilación falla debido a un error de nombre de usuario o contraseña no válidos.

Para solucionar este problema, compruebe lo siguiente:

- Compruebe que la cuenta de servicio de Oracle existe y no está bloqueada: `SELECT account_status FROM dba_users WHERE username = 'DISCOVERY_USER';`
- Compruebe que la contraseña es correcta conectándose manualmente: `sqlplus discovery_user/<password>@<host>:1521/<service_name>`

- Si la cuenta está bloqueada, desbloquéela: `ALTER USER discovery_user ACCOUNT UNLOCK;`

Privilegios insuficientes (ORA-01031)

Síntoma: la conexión se realiza correctamente, pero la recopilación devuelve datos incompletos.

Para solucionar este problema, compruebe lo siguiente:

- Compruebe que se concede `SELECT_CATALOG_ROLE`: `SELECT * FROM dba_role_privs WHERE grantee = 'DISCOVERY_USER';`
- Otorgue la función requerida si falta: `GRANT SELECT_CATALOG_ROLE TO discovery_user;`

La credencial manual muestra un error, pero la conexión automática funciona

Al fijar una credencial manualmente a un servidor, la herramienta de detección no recurre a ella si se produce un error en la conexión. Compruebe que el nombre del puerto y del servicio que configuró en la credencial coincidan con el agente de escucha de Oracle de ese servidor específico. Si el servidor tiene un nombre de puerto o servicio no estándar, actualice la configuración de credenciales en consecuencia.

OS-level alternativa: no detecta Oracle

Si no se ha configurado ninguna credencial de base de datos y la OS-level alternativa no detecta Oracle:

- Compruebe que las credenciales de los sistemas operativos SSH o WinRM estén configuradas y funcionen para el servidor (compruebe el estado de la recopilación de métricas del sistema operativo).
- En el caso de los hosts Linux, compruebe que los procesos del monitor de procesos de Oracle (pmon) /etc/oratab existan o que estén en ejecución.
- En el caso de los hosts de Windows, compruebe que las entradas de registro de Oracle estén en ejecución HKLM\SOFTWARE\Oracle o que oracle.exe los procesos se estén ejecutando.

Solución de problemas de SNMP

Acceda a la herramienta de descubrimiento VM

- Log-in a la máquina virtual de la herramienta de detección, abra Remote Console en vCenter

- Nombre de usuario: discovery
- Contraseña: contraseña

Instale las herramientas SNMP (si es necesario)

- `sudo yum install net-snmp-utils -y`

Pruebe la conexión SNMP a los servidores Linux

1. `snmptable -v 2c -c <COMMUNITY_STRING>
<REMOTE_SERVER_IP> .1.3.6.1.2.1.6.13.1`
2. Ejemplo:

```
#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
```

Errores de recopilación de redes

se necesita un terminal para leer la contraseña

Error:

```
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
```

El comando `ss` solicita la contraseña del usuario. El usuario `ssh` configurado debe estar en el grupo `sudoers` y estar configurado con `sudo` sin contraseña para el comando. `ss/netstat` Para configurar el `sudo` sin contraseña:

1. Crea un nuevo archivo sudoers:

```
sudo vi -f /etc/sudoers.d/<username>
```

2. Añada la línea:

```
<username> ALL=(ALL) NOPASSWD: /usr/sbin/ss, /usr/bin/netstat
```

3. Después de este cambio, se ejecuta `sudo ss -tnap` y `sudo netstat -tnap` debería ejecutarse sin solicitar una contraseña

La recopilación de redes se ejecutó sin sudo

Si ves la siguiente advertencia en la página de inventario descubierto:

```
Network collection ran without sudo. Process-level connection data may be missing.
```

Esta advertencia indica que la cuenta de usuario de SSH no tiene acceso de sudo al servidor de destino. Sin sudo, la herramienta de detección aún puede recopilar datos de conexión de red, pero no puede determinar qué proceso es el propietario de cada conexión. Para recopilar datos de conexión completos a nivel de proceso, asegúrese de que el usuario de SSH tenga acceso sudo al servidor de destino.

Errores de recopilación de métricas del sistema operativo

Falta el UUID del servidor para los servidores Linux

Si la herramienta de detección no puede recopilar el UUID del servidor (aparece vacío o falta) para los servidores Linux, compruebe que las credenciales SSH configuradas para esos servidores tengan privilegios de sudo. La herramienta se utiliza `dmidecode` para leer el UUID del servidor. Si `dmidecode` está instalada, la herramienta vuelve a la lectura `/sys/class/dmi/id/product_uuid`, que también requiere acceso sudo. Sin sudo, ninguno de los métodos puede recuperar el UUID.

Solución: asegúrese de que la cuenta de usuario SSH proporcionada a la herramienta de detección tenga acceso sudo en los servidores Linux de destino.

Problemas de acceso en el inventario descubierto

Si aparece un mensaje en el estado de recopilación del servidor, como Credenciales faltantes o Acceso denegado:

1. Seleccione el servidor en la tabla de servidores detectados.
2. Elija Administrar credenciales de acceso. Puede elegir entre:
 - a. Seleccione credenciales alternativas en el menú desplegable Seleccionar credenciales.
 - b. Seleccione Usar credenciales nuevas y proporcionar credenciales nuevas.
3. Save (Guardar).

La herramienta de detección vuelve a intentar la conexión después de guardar los cambios.

Solución de problemas de autenticación con clave SSH

Probar la conectividad de la clave SSH desde la herramienta de descubrimiento

Si se produce un error en la autenticación de la clave SSH, compruebe la conectividad de la herramienta de detección con el servidor de destino:

1. Inicie sesión en la herramienta de detección (mediante la consola vSphere o mediante SSH en el host Linux).
2. Pruebe la conectividad SSH con su clave privada:

```
ssh -i /path/to/private_key -o StrictHostKeyChecking=no <username>@<target_ip>
```

3. Si la conexión se realiza correctamente, el problema está relacionado con la forma en que se cargó la clave en la herramienta de detección. Re-upload la clave y verifica que el nombre de usuario coincida.
4. Si se produce un error en la conexión, compruebe el mensaje de error de la siguiente tabla.

Mensaje de error	Causa	Resolución
Permission denied (publickey)	La clave pública no está en el authorized_keys	Agregue la clave pública ~/.ssh/authorized_keys al servidor de destino para el usuario correcto. Compruebe los permisos

Mensaje de error	Causa	Resolución
	archivo del servidor de destino o el nombre de usuario es incorrecto.	de los archivos: <code>chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys</code> .
Connection timed out after 20s	No se puede acceder al puerto 22 desde la herramienta de detección.	Compruebe que el puerto 22 esté abierto entre la herramienta de detección y el servidor de destino. Compruebe los firewalls y los grupos de seguridad.
Connection refused	El servicio SSH no se está ejecutando en el servidor de destino.	Inicie el servicio SSH: <code>sudo systemctl start sshd</code>
Invalid SSH key for credential ' <i>name</i> '	El formato de clave no es compatible, los datos de la clave están dañados, o falta la contraseña o es incorrecta.	Compruebe que el formato de la clave es RSA, ECDSA o Ed25519 en formato PEM, OpenSSH o PKCS #8. Si la clave está cifrada, asegúrese de que la contraseña sea correcta.

Solución de problemas con el instalador

El puerto 5000 ya está en uso

Síntoma: el servicio de la herramienta de detección no se inicia después de la instalación.

Solución: identifique y detenga el proceso mediante el puerto 5000:

```
sudo ss -tlnp | grep :5000
```

Detenga el proceso conflictivo y, a continuación, reinicie la herramienta de detección:

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

Mensajes de error comunes

En esta tabla se describen los mensajes de error más comunes y sus explicaciones:

Mensaje	Ubicación	Explicación
Ya se ha creado una contraseña	Crear página de contraseñas	Condición de carrera cuando dos usuarios crean contraseñas al mismo tiempo; actualice
Falló la exportación	Página de inventario	Vuelva a intentarlo o envíe los registros
Ya hay una recopilación bajo demanda en curso	Página de inventario	Condición de carrera cuando dos usuarios inician la recolección manual al mismo tiempo; inténtelo de nuevo una vez finalizada la recopilación manual actual
Command timed out after 60s	Estado de la recopilación del servidor	Un comando del servidor de destino no se completó en 60 segundos. Esto puede ocurrir en servidores muy cargados. Vuelva a intentar la recopilación o investigue la carga del servidor de destino.
Una o más credenciales contienen UUID desconocidos	Página de acceso al sistema operativo	Condición de carrera cuando dos usuarios editan las credenciales del sistema operativo al mismo tiempo; inténtelo de nuevo
Contraseña no válida	Sign-in página	Contraseña incorrecta para iniciar sesión; ponte en contacto con el administrador o comunícate con
Tu sesión ha caducado. Vuelva a iniciar sesión.	Sign-in página	Se agotó el tiempo de espera de la sesión, es necesario volver a iniciar sesión

Mensaje	Ubicación	Explicación
Se ha producido un error interno	Varias páginas	Vuelva a intentarlo o envíe los registros

Notas de la versión

En esta sección se describen las funciones, mejoras y correcciones de errores de la herramienta de AWS Transform descubrimiento, organizadas por fecha de lanzamiento.

Date	Versión	Notas de la versión
30 de junio de 2026	1.0.1646	Nuevas características - Se agregó la detección de bases de datos Oracle. La herramienta recopila la topología, la versión, la edición, las opciones instaladas, el uso de las funciones y el inventario de componentes de la CDB y la PDB. La herramienta de detección admite conexiones SQL directas (mediante SELECT_CATALOG_ROLE) y la detección de alternativas mediante SSH o OS-level WinRM. - Se agregó compatibilidad con varias credenciales de Kerberos en distintos dominios de Active Directory. Cada credencial se autentica de forma independiente, lo que permite recopilarla desde servidores Windows de varios dominios sin conflictos de autenticación. Mejoras - Recopilación mejorada de métricas del sistema operativo para los hosts antiguos. Se agregó la recopilación de datos alternativa para los sistemas operativos más antiguos (RHEL 5, SLES 11, Windows Server 2008 R2) en los que los comandos modernos no están disponibles. Los datos de almacenamiento, rendimiento e interfaz de red ahora se recopilan mediante interfaces de sistema alternativas.

Date	Versión	Notas de la versión
		Correcciones de errores • Se corrigieron los errores de autenticación de Kerberos detectados a través Hyper-V de Kerberos en los servidores. La herramienta de detección ahora resuelve correctamente el nombre de host del servidor (FQDN) a partir de los metadatos del Hyper-V huésped, lo cual es necesario para hacer coincidir el SPN de Kerberos.

Date	Versión	Notas de la versión
14 de mayo de 2026	1.0.1363	Nuevas características • Se agregó un instalador de Linux para implementar la herramienta de descubrimiento en las distribuciones de Linux compatibles (Amazon Linux 2, Amazon Linux 2023, RHEL 8—9, Rocky Linux 8—9, Ubuntu 20.04—24.04, Debian AlmaLinux 10—12, SLES 15 SP5). • Se agregó soporte para configurar varios servidores VMware vCenter con deduplicación automática de máquinas virtuales en todos los vCenters. • Se agregó la autenticación mediante clave privada SSH como alternativa al nombre de usuario y la contraseña para el acceso al sistema operativo Linux. Los formatos clave compatibles incluyen RSA, ECDSA, Ed25519, OpenSSH y PKCS #8. • Se agregó una recopilación de redes de direcciones privadas para capturar las conexiones desde y hacia las direcciones IP privadas de la RFC 1918 que no figuran en el inventario descubierto. • Se agregaron opciones de exportación para seleccionar un rango de fechas personalizado y elegir qué módulos de datos incluir en la exportación. Mejoras • Se mejoró la confiabilidad de la recopilación programada al escalonar los horarios de los recopiladores. • Se mejoró el rendimiento de la recopilación de métricas del sistema operativo mediante el procesamiento por lotes de comandos SSH. • Los cambios de credenciales ahora reintentan inmediatamente los servidores que anteriormente fallaban.

Date	Versión	Notas de la versión
		• La recopilación de métricas del sistema operativo ahora informa de un estado parcial cuando algunos comandos devuelven resultados vacíos. • Se ha mejorado la visibilidad de los errores de conexión de vCenter en el panel de control.
7 de abril de 2026	1.0.1074	Nuevas características • Se agregó soporte para la Hyper-V detección de Microsoft, incluida la detección automática de máquinas virtuales desde Hyper-V hosts con deduplicación de clústeres de conmutación por error. • Se agregó soporte para la importación de servidores mediante la carga de archivos CSV. • Se agregó la recopilación de métricas del sistema operativo con seis módulos independientes: rendimiento del servidor, rendimiento del almacenamiento, aprovisionamiento del servidor, aprovisionamiento del almacenamiento, interfaces de red y procesos en ejecución. • Se agregó la opción Hyper-V de implementación mediante un archivo de imagen VHD. • Se mejoró el refuerzo de la seguridad local al eliminar EC2-specific los servicios y bloquear el acceso al punto final de metadatos de la instancia.

Date	Versión	Notas de la versión
26 de marzo de 2026	1.0.1014	Mejoras y correcciones de errores • Se ha trasladado la validación de las mayúsculas de los dominios de Kerberos del backend al frontend. • Cambió de Python-kerberos a Python-pykerberos y estableció la caché basada en archivos como predeterminada. • Se corrigió la validación del ID del servidor de edición masiva sin distinción de mayúsculas y minúsculas. • Se ha corregido el nombre de archivo ZIP de exportación (<code>ahoradiscovery_tool_export.zip</code>). • Se corrigió la comprobación del servicio y se agregaron registros de depuración para las credenciales del sistema. • Se agregó un script de configuración de red para construir un artefacto.
16 de diciembre de 2025	1.0.718	Nuevas características y mejoras • Se agregó la compatibilidad con los UUID de SMBIOS para evitar la duplicación de máquinas virtuales en los servicios descendentes. • Se introdujeron las métricas Min/Max/Avg de seguimiento y almacenamiento ampliadas para mejorar la supervisión de los recursos. • Se agregaron mejoras en la validación de la API. • Se agregó la funcionalidad del panel de ayuda con orientación contextual. • Se actualizó la terminología de «recopilador» a «herramienta» en toda la interfaz.

Date	Versión	Notas de la versión
31 de octubre de 2025	1.0.0	Versión inicial Lanzamiento inicial de la herramienta de AWS Transform descubrimiento. Esta versión incluye: • Recopilación sin conexión (no depende de una AWS cuenta ni de Application Discovery Service). • Descubrimiento y monitoreo de VMware. • Descubrimiento de bases de datos de SQL Server. • Server-to-server recopilación de comunicaciones a través de SSH, WMI y SNMP.

AWS Transformar conectores

AWS Los conectores Transform le permiten acceder de forma segura a los recursos a través de los límites de las cuentas para los flujos de trabajo de migración y modernización. Esto le permite acceder a los recursos y administrarlos más allá de los límites de las cuentas y, al mismo tiempo, mantener los controles de seguridad y los permisos. Un conector representa una conexión entre la cuenta de AWS Transform-enabled origen y los recursos externos de las cuentas de AWS destino o de sistemas de terceros.

Los conectores requieren solicitudes de acceso desde el conector de origen y la aprobación del propietario de la cuenta de destino. Realiza esta solicitud al configurar un conector de origen. Del mismo modo, es posible que reciba solicitudes para aprobar los conectores de destino a fin de permitir que otras cuentas accedan a su cuenta.

- Creación de conectores: cree conectores en su cuenta de AWS Transform-enabled origen, especificando la cuenta de destino y los permisos necesarios
- Configuración de permisos: AWS Transform requiere funciones y permisos de IAM específicos en la cuenta de destino para realizar acciones de migración, que incluyen:
 - Administrar los datos de migración con AWS KMS
 - Realizar llamadas a la API entre regiones
 - Instalación de agentes de replicación en servidores VMware
 - Creación de infraestructura de red (VPC, subredes, enrutamiento)
 - Lanzamiento de instancias de Amazon EC2 e implementación de pilas CloudFormation
 - Ejecución de flujos de trabajo de migración a través de Migration Hub
- Proceso de aprobación: debe aprobar las solicitudes de conectores de destino antes de que AWS Transform pueda acceder a sus recursos.
- Conexión activa: una vez que apruebas un conector, AWS Transform Jobs podrá acceder a los recursos de la cuenta de destino y gestionarlos de forma segura.

Trazabilidad de los usuarios para las operaciones de los agentes

De forma predeterminada, AWS CloudTrail registra las acciones de los agentes en sus AWS recursos con la identidad del servicio AWS Transform. La trazabilidad de los usuarios atribuye esas

acciones al usuario específico del AWS IAM Identity Center que inició el trabajo o interactuó con él, lo que permite realizar auditorías de seguridad e investigar incidentes a nivel de usuario individual.

 Note

La trazabilidad de los usuarios solo es compatible con los usuarios del IAM Identity Center (IDC).

Para habilitar la trazabilidad de los usuarios, habilite la sesión en segundo plano en la configuración de su AWS perfil de Transform. Cuando está activado, AWS Transform crea automáticamente una [sesión en segundo plano](#) del Centro de Identidad de IAM cuando interactúa con un trabajo y la utiliza para crear sesiones de roles de IAM con una identidad mejorada para las operaciones de conexión. Estas sesiones incorporan su identidad de usuario en las llamadas de servicio y los eventos posteriores AWS . AWS CloudTrail Cuando las sesiones en segundo plano están deshabilitadas, AWS Transform recurre a las sesiones estándar con roles asumidos sin contexto de identidad de usuario.

Los nuevos conectores se configuran automáticamente para facilitar la trazabilidad de los usuarios. En el caso de los conectores existentes, debe `sts:SetContext` añadir manualmente la política de confianza de la función 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" }
      }
    }
  ]
}
```

Puede ver y revocar las sesiones en segundo plano activas desde la pestaña Sesiones en segundo plano de la página de trabajo. La revocación de una sesión la invalida inmediatamente, así como cualquier sesión de conexión derivada de ella.

Para obtener más información, consulte [Descripción general de la propagación de identidades confiables](#) en la AWS Guía del usuario de Centro de identidades de IAM.

Administrar los conectores

En la página de conectores, puede ver:

- Pestaña de conectores de origen: muestra todos los conectores que ha creado para conectarse a otras cuentas y muestra las cuentas de destino y el estado de los conectores
- Pestaña Conectores de destino: muestra las solicitudes de conexión entrantes de otras cuentas que desean acceder a tus recursos y que requieren tu aprobación o rechazo

AWS Transform requiere la confirmación de las acciones críticas, como la aprobación, el rechazo o la eliminación de conectores, a fin de evitar cambios accidentales que puedan interrumpir los flujos de trabajo de migración activos.

Para crear un conector

1. Acceda a la pestaña Conectores de origen.
2. Especifique la cuenta de destino y el tipo de recurso.
3. Configure los permisos y el alcance de acceso necesarios.

Configuración de permisos de

1. Elija crear un nuevo rol de IAM con los permisos necesarios, o
2. Seleccione un rol existente que haya creado anteriormente para los conectores.
3. Asegúrese de que el rol tenga todos los permisos necesarios para las operaciones de AWS transformación.

Para gestionar las solicitudes entrantes

1. Revise las solicitudes de conectores en la pestaña Conectores de destino.
2. Apruebe las solicitudes legítimas para permitir el acceso entre cuentas.
3. Rechaza los intentos de conexión no autorizados o innecesarios.

Para gestionar sus conectores

1. Supervise sus conectores activos para garantizar la seguridad y el cumplimiento.
2. Elimine los conectores cuando ya no los necesite. Tenga en cuenta que esto provocará que se produzcan errores en los trabajos que se estén ejecutando con el conector.
3. Actualice los permisos a medida que cambien sus requisitos.

Migraciones (incluida VMware)

AWS Transform puede ayudarlo a migrar sus entornos de servidores virtuales y físicos a Amazon EC2 mediante el uso de IA generativa, que incluye VMware Hyper-V, y otras fuentes. En este capítulo se proporciona una descripción general de las capacidades de migración de AWS Transform y del flujo de trabajo del proceso de migración.

Capacidades y características clave

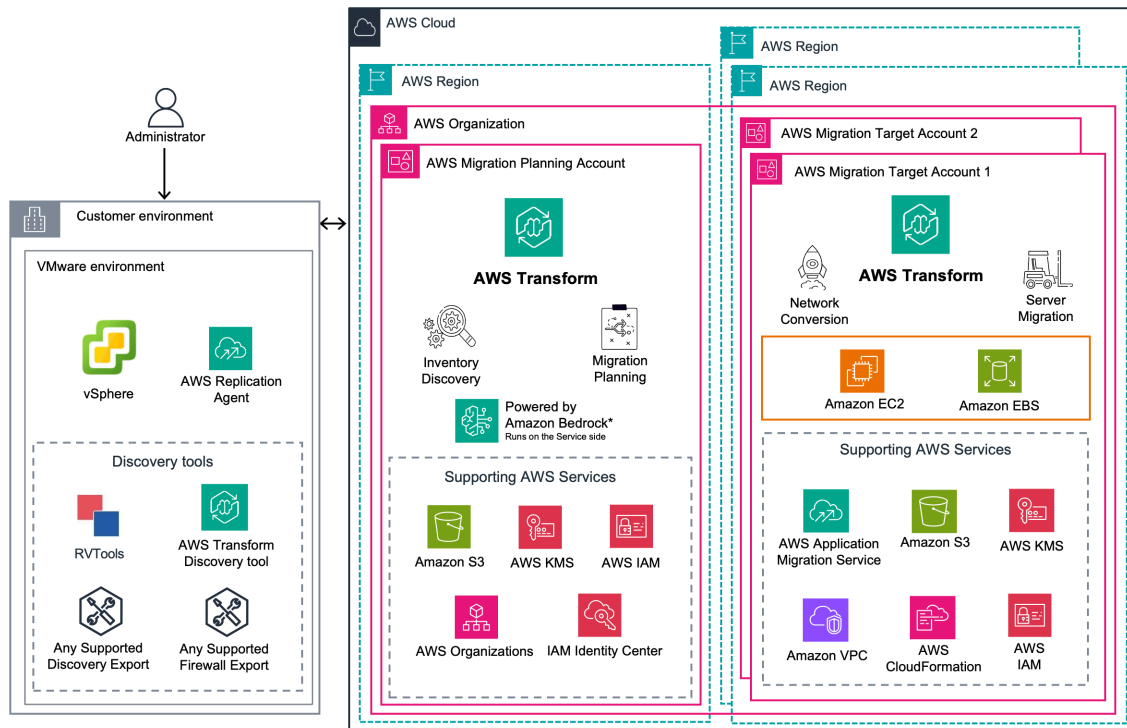
AWS Transform ofrece las siguientes capacidades y funciones clave para migrar sus entornos de servidores a AWS.

- Múltiples opciones de descubrimiento:
 - Descubrimiento asistido de su entorno VMware mediante el uso de recopiladores de AWS Application Discovery Service.
 - Utilice la herramienta de código abierto [Export for vCenter](#) (entornos VMware).
 - Importación de datos de descubrimiento recopilados de forma independiente (en cualquier entorno de origen).
- AI-driven conversión de la configuración de red de origen a una arquitectura de red de Amazon VPC.
- AI-driven generación de planes de migración, incluida la agrupación de aplicaciones y las oleadas de migración sugeridas.
- Realojar sus servidores para que se ejecuten de forma nativa en Amazon EC2.
- Interfaz de aplicación web localizada, que le permite utilizar AWS Transform para las migraciones en el idioma que prefiera. Para obtener más información, consulte [Configuración de idioma](#).

AWS Transform admite la migración de servidores Windows y Linux de sistemas operativos compatibles. Para ver la lista completa de sistemas operativos compatibles, consulte [Sistemas operativos compatibles](#) en la Guía del AWS Transform MGN usuario.

AWS Transforme la arquitectura de migración

Este diagrama muestra una descripción general de la arquitectura de migración de AWS Transform.



Trabajos de migración

Para usar AWS Transform para las migraciones, primero necesita un espacio de trabajo, que es un contenedor lógico en el que puede crear uno o más trabajos de transformación. En las secciones de este tema se describe cómo obtener un espacio de trabajo y cómo crear e iniciar un trabajo de migración en él.

Obtener un espacio de trabajo

Para obtener información sobre cómo obtener un espacio de trabajo, consulta [Cómo empezar](#).

El espacio de trabajo que utilice determina el Región de AWS lugar en el que puede crear trabajos de transformación. Ahí es Región de AWS donde residirán sus trabajos. Sus datos de descubrimiento y sus recomendaciones de AWS transformación también residirán en él Región de AWS. Para crear espacios de trabajo y trabajos en otro lugar Región de AWS, pida al administrador que cree un espacio de trabajo diferente para usted. Para obtener información sobre lo compatible Regiones de AWS, consulte [Regiones admitidas](#).

Aunque el administrador de AWS Transform determine Región de AWS dónde puede crear trabajos y almacenar los datos de descubrimiento y las recomendaciones, puede especificar un destino

diferente Región de AWS para la migración. En otras palabras, puede ejecutar la detección y recibir las recomendaciones de AWS Transform en una Región de AWS, pero luego crear su entorno de destino en otro diferente Región de AWS. Si lo hace, transferirá sus datos de un lado a otro Regiones de AWS. Para obtener más información, consulte [the section called “Connect target Cuenta de AWS s y regiones”](#).

Tipos de trabajo

AWS Transform ofrece los siguientes tipos de trabajos de migración entre los que puede elegir en función de sus necesidades de migración. Además de estas opciones preestablecidas, puede añadir o eliminar de forma dinámica cualquier paso de su trabajo en cualquier momento para personalizar su flujo de trabajo de migración.

End-to-end migración

1. Realizar un descubrimiento
2. Cree un plan de migración
3. Connect cuentas de destino
4. Construye landing zone
5. Migre la red
6. Migre los servidores

Planificación de la detección y la migración

1. Realice el descubrimiento
2. Cree un plan de migración

Migración de red

1. Connect cuentas de destino
2. Migre la red

Zona de aterrizaje

1. Connect cuentas de destino
2. Construye landing zone

Migración de zonas de aterrizaje, redes y servidores

1. Connect cuentas de destino
2. Construye landing zone
3. Migre la red
4. Migre los servidores

Planificación de la migración y migración de servidores

Incluye detección, plan de oleaje y realojamiento.

1. Realice el descubrimiento
2. Cree un plan de migración
3. Connect cuentas de destino
4. Migre los servidores

Crear e iniciar un trabajo

El primer paso de un proyecto de migración es crear un trabajo de AWS Transform. Para los proyectos de migración, puede elegir diferentes tipos de trabajo, en función de sus objetivos. El siguiente procedimiento describe cómo crear e iniciar un nuevo trabajo de migración de cualquier tipo. Para obtener información sobre los distintos tipos de trabajo, consulte [the section called “Tipos de trabajo”](#).

Para crear e iniciar un nuevo trabajo de migración

1. En la página de inicio de tu espacio de trabajo, selecciona Crear un trabajo.
2. Elige la opción de migración y, a continuación, especifica el tipo de trabajo de migración que deseas crear. Para obtener información sobre los pasos incluidos en cada uno de los tipos de trabajo de migración, consulte [the section called “Tipos de trabajo”](#).
3. Después de responder a todas las preguntas del chat, selecciona Crear trabajo.

Descargar un informe resumido del espacio de trabajo

Puedes generar un informe resumido del espacio de trabajo en formato PDF descargable en cualquier momento durante la migración. El informe proporciona una visión consolidada de todos

los trabajos de migración de su espacio de trabajo, incluidos los estados de los trabajos y los pasos actuales del flujo de trabajo, las acciones y aprobaciones de los usuarios, los detalles de la planificación de las oleadas, la topología de migración de la red, la configuración de las zonas de aterrizaje, el progreso del realojamiento, las decisiones de contenedorización y los principales elementos producidos. Para generar un informe, pide al agente en el chat un resumen del espacio de trabajo, por ejemplo: «Deme un resumen del espacio de trabajo con el progreso de mi migración en todos los trabajos». El agente recopila los datos de todos los trabajos y entrega el PDF directamente en el chat como un archivo descargable. Puedes usar este informe para hacer un seguimiento del progreso general de la migración o compartir el estado con las partes interesadas.

Limitaciones

AWS Transform tiene las siguientes limitaciones:

- Si detiene un trabajo de migración en ejecución y, a continuación, pide al agente que lo reinicie, el trabajo volverá a empezar desde el principio y perderá todo el progreso que haya realizado en él. Sin embargo, los artefactos creados en la tarea antes de reiniciarla seguirán estando disponibles.
- Puede especificar un objetivo Región de AWS por cada trabajo de migración. Para migrar las aplicaciones a distintas regiones de destino, cree varios trabajos de migración.
- Multi-account migración: solo en una región: puede migrar a varias cuentas dentro de una sola Región de AWS. Para las migraciones multirregionales, debe crear proyectos independientes para cada región de destino.
- Multi-account migración: una cuenta por oleada: cada oleada de migración solo puede dirigirse a una cuenta. Las solicitudes que requieran cuentas de destino diferentes se deben colocar en grupos separados.
- Multi-account migración: se requieren AWS organizaciones: todas las cuentas de destino deben formar parte de una AWS organización.

Descubra los datos de origen

Para descubrir y recopilar datos locales, puede utilizar la [herramienta de descubrimiento AWS Transform](#), el recopilador AWS Migration Evaluator o cargar las exportaciones de RVTools y Modelizelt, así como las exportaciones en formato MPA (AWS Migration Portfolio Assessment) generadas por herramientas como Cloudamize. AWS Transform puede procesar las exportaciones de la herramienta de descubrimiento de AWS Transform como archivos CSV y JSON en formato de archivo ZIP, RVTools exporta como un archivo de Excel o un archivo ZIP que contiene archivos CSV

y Modelizelt CSV exporta en un archivo ZIP. Para cada fuente de datos, AWS Transform acepta el archivo del servidor principal de forma individual. Sin embargo, los archivos adicionales, como las conexiones, solo se procesarán cuando se incluyan en un archivo ZIP con los archivos del servidor o en un archivo de Excel con la hoja del servidor.

Le recomendamos que cargue los datos más detallados disponibles y revise los archivos de exportación antes de cargarlos para garantizar la integridad y precisión de los datos. Compruebe que todos los archivos necesarios estén incluidos en la carga y confirme que los datos reflejan el estado actual de su entorno. Esta revisión preliminar ayuda a minimizar la necesidad de volver a cargarlos y garantiza que AWS Transform pueda capturar con mayor precisión su entorno local y respaldar mejor la planificación de la migración, incluida la agrupación de aplicaciones y la planificación de oleadas. También puede añadir datos de forma incremental a medida que vaya obteniendo mejores datos.

AWS Transform detecta automáticamente el formato y la estructura de los archivos, analiza y extrae los registros de entidades estructurados, elimina los duplicados en varios archivos, valida la calidad de los datos y notifica los problemas y, a continuación, prepara un resumen listo para planificar la migración posterior.

Después de compartir y confirmar los datos locales, puede revisar los datos de descubrimiento ampliando Discover on-premise data en el Job Plan y seleccionando Resumen de preparación del inventario. También puedes hacer preguntas sobre los datos que has subido para comprobar que AWS Transform ha ingerido todos los datos correctamente o para identificar y corregir cualquier error en el procesamiento de los datos. Por ejemplo, puedes preguntar sobre el sistema operativo y las versiones. Si necesitas corregir errores, puedes volver a cargar los datos de inventario desde la herramienta de detección que utilizaste y AWS Transform procesará, deduplicará y combinará automáticamente los registros actualizados. También puedes eliminar un archivo cargado anteriormente si ya no quieres usar esos datos de inventario.

Crea un plan de migración

El paso de planificación de la migración de AWS Transform for VMware consiste en una experiencia colaborativa basada en el chat para planificar grandes migraciones. AWS Los agentes de Transform aplican AWS las directrices prescriptivas para guiar a los clientes desde el análisis de los datos locales hasta la finalización de los planes de migración.

Una vez que el trabajo de Descubra los datos locales se complete correctamente, AWS Transform utiliza los datos de descubrimiento para agrupar las aplicaciones en oleadas de migración. AWS Transform le guía paso a paso para analizar y determinar el alcance de sus servidores, agruparlos

en aplicaciones, generar grupos de movimientos y crear oleadas de migración. Al analizar su entorno local, puede hacer preguntas para comprender mejor cómo AWS Transform analizó el software instalado, por ejemplo, las dependencias de los servidores y la arquitectura de red.

AWS Transform admite los ajustes de alcance dentro de los grupos y oleadas de aplicaciones. Puede volver a cargar los datos de descubrimiento en cualquier momento y AWS Transform procesará, desduplicará y combinará automáticamente los nuevos registros con los datos existentes. Cuando se detecten cambios, como dependencias descubiertas recientemente o incorporaciones de infraestructura, AWS Transform señalará los grupos de dependencia afectados y ofrecerá recomendaciones para ajustar el plan de oleada. La planificación de la migración también puede utilizar datos de texto no estructurados para enriquecer el proceso de planificación.

Hay cuatro etapas de planificación de la migración:

- En Alcanzar y analizar, puede revisar los datos de descubrimiento, hacer preguntas sobre el software y el entorno de red y determinar los recursos que están a punto de migrar.
- En las aplicaciones grupales, puede proporcionar una combinación de normas empresariales y técnicas relacionadas, por ejemplo, con el análisis del nombre de host, las dependencias de la red y las reglas empresariales, de modo que la planificación de la migración pueda agrupar su infraestructura en aplicaciones. Si ya tiene un inventario de sus aplicaciones, la planificación de la migración puede utilizarlo en su lugar.
- En Generate Move Groups, puede definir a la planificación de la migración sus requisitos técnicos y empresariales para que pueda determinar qué aplicaciones deben transferirse juntas. Las dependencias técnicas incluyen bases de datos, colas de mensajes u otros recursos compartidos entre varias aplicaciones. Las dependencias comerciales y operativas incluyen la importancia de la empresa, el RPO y el RTO, la ubicación del centro de datos y los propietarios de las aplicaciones.
- Por último, en Build waves, puede dar un contexto a la planificación de la migración sobre sus plazos y prioridades, de modo que pueda crear un plan de oleada que pueda migrar. Puede seleccionar grupos de movimientos para incluirlos en una oleada en función de factores como la puntuación de prioridad, el tamaño del grupo de movimientos, el número de usuarios y la complejidad de la aplicación.

Terminología de planificación de la migración:

- Las oleadas de migración son grupos lógicos que se migran de forma conjunta. Las oleadas de migración se componen de uno o más grupos de movimientos.

- Un grupo de movimientos es un conjunto de aplicaciones codependientes que se deben mover juntas. Pueden tener dependencias técnicas, como una base de datos compartida, o tener dependencias comerciales, como el soporte de una función empresarial compartida.
- Una dependencia es una relación entre sistemas. Existen varios tipos de dependencias, entre las que se incluyen:
 - Dependencias críticas o duras, en las que los sistemas no pueden funcionar sin la dependencia. Ejemplos comunes de esto son las aplicaciones que dependen de bases de datos, otras aplicaciones o servicios.
 - Dependencias blandas, que no son fundamentales para el funcionamiento del sistema. Algunos ejemplos comunes de esto son las dependencias insensibles a la latencia que se pueden migrar de forma independiente.
 - Non-technical Las dependencias incluyen dependencias empresariales, organizativas, operativas y de cumplimiento. Se trata de dependencias relacionadas con su organización y sus prioridades. Algunos ejemplos de esto incluyen la función empresarial compartida y la propiedad organizacional.

Flujo de trabajo

La planificación de la migración es un flujo de trabajo interactivo e iterativo. Puede volver atrás y realizar cambios en los pasos anteriores en cualquier momento. Un flujo de trabajo típico de planificación de la migración es:

1. La planificación de la migración comienza resumiendo los datos de descubrimiento disponibles. Revise los datos disponibles y vuelva al paso de descubrimiento en cualquier momento para proporcionar datos adicionales.
2. En el paso de análisis y análisis, puede hacer preguntas sobre su entorno local para validar los datos que ha recopilado. Entre las preguntas de ejemplo se incluyen:
 - a. Listar mis servidores por sistema operativo
 - b. Resuma la topología de mi red local
 - c. Enumere las tecnologías más comunes que se ejecutan en mi entorno.
3. Al analizar su entorno, si identifica servidores que no deberían estar sujetos a la migración, puede indicarle a AWS Transform que excluya esos recursos. Ejemplos:
 - a. Elimine todos los servidores que tengan un nombre de host heredado
 - b. Elimine todos los servidores de la versión 10.0.2. 0/24 subred

- c. Elimine todos los servidores que ejecuten versiones de Windows anteriores a 2022
4. Una vez que haya explorado suficientemente su entorno y determinado el alcance de la migración, puede indicarle a AWS Transform que pase al siguiente paso de planificación de la migración.
5. El siguiente paso es agrupar las aplicaciones. Si ya tiene los servidores asignados a las aplicaciones, puede decirle a AWS Transform que utilice esa asignación y saltarse este paso. Si no tiene sus aplicaciones predefinidas, puede proporcionar la lógica técnica y empresarial que las define. AWS Transform lo guiará a través del proceso de agrupación de aplicaciones y le sugerirá los puntos de datos que puede proporcionar para agrupar eficazmente sus servidores en aplicaciones. Cuanta más información pueda proporcionar sobre sus aplicaciones locales, más eficazmente podrá AWS Transform agrupar sus servidores en aplicaciones. Una vez que haya proporcionado suficiente información, puede indicar a AWS Transform que agrupe las aplicaciones.
6. Una vez realizada la agrupación de aplicaciones, revise los grupos de aplicaciones. Puede indicar a AWS Transform que realice los cambios necesarios, por ejemplo:
 - a. Mueva el servidor example-server a application-5
 - b. Cambie el nombre de la aplicación-5 a «HR App Test Environment»
 - c. Elimine todos los servidores Linux de la granja de desarrolladores de IIS
7. Una vez agrupadas las aplicaciones, indique a AWS Transform que pase al siguiente paso
8. El siguiente paso es mover la agrupación. En el paso de agrupamiento de movimientos, identifica las aplicaciones que deben moverse juntas. Proporcione un contexto en torno a sus dependencias técnicas y no técnicas. AWS Transform lo guiará a lo largo del proceso y le sugerirá puntos de datos que puede proporcionar para agrupar sus aplicaciones. En esta fase hay que tener en cuenta varias consideraciones, entre las que se incluyen las siguientes:
 - a. ¿Cuál debería ser el tamaño objetivo del grupo de mudanzas?
 - b. ¿Desea combinar entornos (por ejemplo, desarrollo, prueba y producción) para cada aplicación o dividirlos?
 - c. ¿Cómo desea considerar las dependencias de la red? ¿Todas las dependencias son críticas o algunas pueden considerarse dependencias blandas y dividirse en grupos de movimiento?
9. Una vez que hayas establecido las reglas para la agrupación de movimientos, pide a AWS Transform que ejecute tu estrategia de agrupación de movimientos. A continuación, podrás revisar y modificar tus grupos de movimientos. Una vez que haya revisado los grupos de mudanzas, puede indicarle a AWS Transform que pase al paso final de planificación de la migración.
- 10 La planificación de oleadas es el paso final de la planificación de la migración. En este paso, agrupa los grupos de mudanzas en oleadas de migración y prioriza esas oleadas. En la fase de

planificación de la oleada, AWS Transform le guiará para establecer la priorización empresarial necesaria para agrupar sus grupos de mudanzas en oleadas y, a continuación, priorizar dichas oleadas. Las consideraciones a tener en cuenta en la planificación de olas incluyen:

- a. La importancia empresarial de cada uno de sus grupos de mudanzas
- b. Los plazos de migración y los plazos de cada grupo de mudanzas
- c. Los riesgos asociados a cada grupo de mudanzas
- d. La cantidad de servidores que se van a migrar por oleada

11. Una vez que haya proporcionado la orientación suficiente sobre cómo agruparse en oleadas, pida a AWS Transform que ejecute la planificación de la oleada. A continuación, puede revisar sus olas y modificarlas.

12. Una vez que haya finalizado su plan de oleada, podrá completar la planificación de la migración y pasar a la fase de ejecución. Puede volver a planificar la migración en cualquier momento para afinar e iterar su plan.

13. Para cada oleada, puede asignar una estrategia de migración: rehospedar (migrar los servidores a Amazon EC2) y contenerizar (contenedorizar el código fuente e implementarlo en Amazon Elastic Container Service o Amazon Elastic Kubernetes Service). Al asignar a una oleada la estrategia de contenerización, AWS Transform ejecuta el flujo de trabajo de contenerización del código fuente para esa oleada durante la ejecución de la migración. Para obtener más información, consulte [Contenedorización del código fuente](#). Para obtener información sobre las estrategias AWS recomendadas en el marco de las 7R antes de asignarlas, consulte [the section called “Recomendaciones de las 7R”](#)

Recomendaciones de estrategia de migración (7R)

Durante la planificación de la migración, AWS Transform puede analizar el inventario descubierto y recomendar una estrategia de migración (una de las 7 R estándar del sector) para cada servidor y aplicación. Cada recomendación incluye una sugerencia de servicio AWS objetivo, una puntuación de confianza y las razones que la sustentan. Esto le proporciona un punto de partida defendible para su plan de oleaje y presenta oportunidades de modernización que, de otro modo, podría perder.

Las siete estrategias son realojar, reorganizar, refactorizar, recomprar, retirar, retener y reubicar. AWS Transform lee las señales de sus datos, como el sistema operativo, la utilización y el tipo de carga de trabajo, para hacer recomendaciones explicables. Por ejemplo, puede recomendar retirar los servidores inactivos o al final de su vida útil, trasladar SQL Server o bases de datos de código abierto a Amazon RDS, trasladar las cargas de trabajo de correo electrónico y colaboración

a Microsoft 365, conservar los sistemas heredados especializados y realojar las cargas de trabajo restantes en Amazon EC2. Las recomendaciones van desde los servidores individuales hasta las aplicaciones y abarcan toda la cartera, con una visión de la criticidad por estrategia y resúmenes por oleada.

Para generar un informe sobre la estrategia de migración (7 R):

1. Complete el paso Descubra los datos locales y agrupe los servidores en aplicaciones. Ambos son necesarios para que AWS Transform pueda ofrecer recomendaciones por servidor y por aplicación.
2. En el chat de planificación de la migración, solicite a AWS Transform un informe de estrategia de migración (7R), por ejemplo, Generar un informe. R-strategy. Una vez finalizada la agrupación de aplicaciones, AWS Transform también le ofrecerá la posibilidad de generar el informe automáticamente.
3. AWS Transform analiza su inventario, aplica el marco de las 7R y genera el informe. Puede proporcionar detalles como el nombre de su organización y cualquier filtro para analizar el alcance del análisis.
4. Revise las recomendaciones. Para ajustar una recomendación, dígaselo a AWS Transform en el chat: cambie un solo servidor o aplicación o aplique un cambio de forma masiva (por ejemplo, por sistema operativo, entorno, oleada o prioridad). AWS Transform actualiza el informe con los cambios.

De forma predeterminada, AWS Transform crea un panel HTML interactivo que puede filtrar y explorar. Si lo solicita, también puede generar un documento PDF para compartirlo con las partes interesadas o un conjunto de diapositivas de Microsoft PowerPoint (PPTX) para presentarlo; el PDF y los PowerPoint resultados son instantáneas puntuales del mismo análisis. El informe incluye una estrategia recomendada y un servicio AWS objetivo para cada servidor y aplicación, puntuaciones de confianza y razonamiento, oportunidades destacadas de modernización, una visión de la criticidad por estrategia, resúmenes a nivel de oleada y señales de riesgo.

La estrategia recomendada en este informe complementa la estrategia por oleada que se asigna durante la planificación de la oleada. Para obtener información sobre la contenedorización del código fuente, consulte [Contenedorización del código fuente](#)

Diagramación e informes

Durante la planificación de la migración, AWS Transform convierte el inventario descubierto y los resultados de planificación en diagramas visuales e informes analíticos. Los genera de forma conversacional en el chat de planificación, por ejemplo, «Muéstreme un diagrama de topología de red» o «genere un informe de riesgos». AWS Transform los crea a partir de los datos que ya ha proporcionado, sin necesidad de configuración.

Los diagramas son interactivos y le permiten explorar su entorno de forma visual. Los diagramas disponibles incluyen:

- Topología de red: un mapa interactivo de sus servidores y sus relaciones de red, diseñado para ampliarse a entornos grandes de miles de nodos.
- Dependencia de las aplicaciones: relaciones dirigidas entre aplicaciones derivadas de las conexiones de red observadas.
- Diagrama de Gantt de ondas: una vista cronológica de las oleadas de migración que muestra los cronogramas, las dependencias, los hitos y el progreso (disponible después de la planificación de la oleada).
- Gráficos generales: gráficos circulares, gráficos de barras, histogramas, mapas de árbol y tablas de resumen sobre las dimensiones de los datos que elija.

Los informes proporcionan análisis narrativos y recomendaciones sobre los datos de migración. Los informes disponibles incluyen:

- Evaluación de riesgos: clasifica cada aplicación en función de la complejidad técnica, el riesgo de dependencia, la preparación para la migración y el riesgo operativo, con resúmenes por aplicación, por oleada y por toda la cartera.
- Estrategia de migración (7 R) y recomendaciones de estrategia por aplicación. Per-server Para obtener más información, consulte [the section called “Recomendaciones de las 7R”](#).
- Informes generales y personalizados: informes analíticos para solicitudes, como resúmenes de la preparación de los ejecutivos, compensaciones entre costos y riesgos y evaluaciones de los candidatos a la contenedorización.

Algunos resultados dependen del grado de planificación en el que se encuentre. Por ejemplo, los diagramas de dependencia de las aplicaciones utilizan los datos de conexión de red. El diagrama de Gantt de oleaje y los resúmenes de los informes a nivel de oleaje están disponibles una vez

finalizada la planificación de la oleada. Si falta un requisito previo, AWS Transform le indica lo que se necesita y puede ejecutar primero el paso necesario.

AWS Transform ofrece diagramas en formato HTML interactivo que puede filtrar y explorar. De forma predeterminada, AWS Transform entrega los informes como un archivo HTML independiente. Previa solicitud, AWS Transform también puede generar un documento PDF para compartirlo con las partes interesadas o un conjunto de diapositivas de Microsoft PowerPoint (PPTX) para presentarlo. El PDF y PowerPoint los resultados son instantáneas puntuales del mismo análisis.

Connect target Cuenta de AWS s y regiones

Configura tu Cuenta de AWS conector de destino para la migración de la red, la creación de landing zone y la migración de servidores. Esto consta de tres pasos: seleccione el tipo de migración, proporcione los detalles del acuerdo MAP (si corresponde) y configure el conector. Esta configuración se aplica a todas las etapas de la migración: migración de red, landing zone y realojamiento de servidores.

Paso 1: Selección del tipo de migración

Elija si va a realizar una migración de una o varias cuentas:

- Single-account migración: todas las cargas de trabajo migran a un destino. Cuenta de AWS La cuenta de destino del conector y la cuenta de destino son la misma.
- Multi-account migración: las cargas de trabajo migran a cuentas de destino diferentes. El conector debe estar conectado a la cuenta de administración de la organización o a una cuenta de administrador delegado (DA) registrada para ambas AWS Transform MGN . CloudFormation StackSets

Paso 2: acuerdo MAP

Si su migración forma parte del AWS Migration Acceleration Program (MAP 2.0), proporcione su ID de Migration Portfolio Experience (MPE), un código de 10 caracteres con letras mayúsculas y dígitos (por ejemplo, ABCDE12345). Cuando proporciona su ID de MPE, la etiqueta MAP se aplica a todos los recursos creados en las etapas de migración de la red, landing zone y rehost del servidor. El formato de la etiqueta es:

- Clave: map-migrated Valor: migMPE_ID

Debe aplicar las etiquetas MAP para recibir el crédito MAP. Para obtener más información sobre MAP, consulte [AWS Migration Acceleration Program](#).

Paso 3: Configuración del conector

El conector de la cuenta de destino se utiliza para conectar el trabajo de migración al AWS entorno en el que se alojarán las cargas de trabajo tras la migración. Antes de empezar, compruebe que su destino Cuenta de AWS tenga los permisos, las cuotas y las configuraciones necesarios para admitir la infraestructura migrada.

Cuando apruebas la solicitud de conector, concedes permisos de AWS Transform a:

- Gestione las operaciones de bucket de Amazon S3 (read/write) para la migración a VMware, junto con el acceso a AWS Migration Hub y AWS Application Migration Service (MGN). Esto incluye los permisos para los siguientes elementos, todos restringidos a los recursos de la cuenta de destino que estén etiquetados con `CreatedBy:AWSTransform` o `CreatedFor:AWSTransform`:
 - Gestione las oleadas de migración.
 - Gestione las configuraciones de red (Amazon EC2, VPC, Transit Gateway, Direct Connect, Load Balancers, Network Firewall).
 - Gestione las implementaciones CloudFormation de pilas.
 - Realice instalaciones automatizadas de agentes a través de Systems Manager.
- Migre sus cargas de trabajo locales al destino Cuenta de AWS y a la región utilizando la información almacenada en la región de descubrimiento.
- Aprovisiona y gestione la infraestructura de la zona de aterrizaje en el objetivo Cuenta de AWS y la región. Esto incluye los permisos para los siguientes elementos, restringidos a los recursos que estén etiquetados, `CreatedBy:AWSTransform` cuando proceda:
 - Realice operaciones de bucket de Amazon S3 (crear, leer, escribir, eliminar) para los buckets que comiencen con `transform-vmware-landing-zone-`.
 - Gestiona los despliegues de CloudFormation pilas y cambia los conjuntos de pilas de landing zone.
 - Realice las operaciones AWS de la Torre de Control. Puede administrar las zonas de aterrizaje, habilitar las líneas de base y habilitar los controles.
 - Manage AWS Organizations. Puede crear y administrar unidades organizativas, crear cuentas y mover cuentas.
 - Administre las políticas de control de servicios (SCP) a través de la Torre AWS de Control.

- Administre los artefactos de aprovisionamiento de AWS Service Catalog.

Note

Los tipos de conectores pueden actualizarse cuando las nuevas funciones requieran cambios en los permisos. La versión actual del tipo de conector de la cuenta de destino es la 2.0. Al crear un conector nuevo, utiliza la versión más reciente.

Antes de configurar el conector, comprenda las funciones de la cuenta que intervienen en la migración:

Cuenta	Description (Descripción)
AWS Transforma la cuenta	Cualquier cuenta de miembro de su AWS organización en la que haya configurado AWS Transform. Aquí es donde se ejecuta tu espacio de trabajo de AWS Transform. No es necesario que sea la cuenta de administración.
Cuenta de destino de Connector	La cuenta en la que está configurado su conector AWS Transform. Esto depende del tipo de migración: • Single-accountmigración: Conéctese a la cuenta a la que está migrando las cargas de trabajo. La cuenta de destino del conector y la cuenta de destino son la misma. • Multi-accountmigración: Conéctese a la cuenta de administración de la organización o a una cuenta de administrador delegado (DA). La cuenta DA debe estar registrada como administradora delegada tanto en MGN como CloudFormation StackSets en su organización. AWS AWS Transform comprueba si la cuenta conectada es la cuenta de administración o una cuenta DA y ajusta su comportamiento en consecuencia.
Cuenta de destino	El Cuenta de AWS lugar al que se migran sus cargas de trabajo. En una migración de una sola cuenta, es la misma que la cuenta de destino del conector. En una migración de varias cuentas, estas son las cuentas de los miembros individuales que reciben las cargas de trabajo migradas.

Uso de una cuenta de administrador delegado

Para las migraciones de varias cuentas, se AWS recomienda utilizar una cuenta de administrador delegado (DA) en lugar de la cuenta de administración de la organización directamente. Una cuenta DA sigue el principio del privilegio mínimo al limitar el alcance de los permisos necesarios para las operaciones de migración. La cuenta DA debe estar registrada como administradora delegada tanto en MGN como CloudFormation StackSets en su AWS organización.

La diferencia clave entre las dos opciones es:

- Cuenta de administración: puede permitir un acceso confiable para MGN y para CloudFormation StackSets toda la organización. AWS Transforma las CloudFormation StackSets API de llamadas con `CallAs: SELF`.
- Cuenta de administrador delegado: no se puede habilitar el acceso confiable directamente (debe hacerse desde la cuenta de administración), pero puede administrar los servidores de origen de MGN, lanzar instancias e implementarlos CloudFormation StackSets en todas las cuentas de los miembros. AWS Transforma las CloudFormation StackSets API de llamadas con `CallAs: DELEGATED_ADMIN`

Para obtener más información, consulte [Administrador delegado de MGN](#) en la Guía del usuario de MGN.

Funciones de IAM creadas durante la configuración del conector

Durante la configuración del conector, AWS Transform crea la siguiente función de IAM en la cuenta de destino:

- `AWSTransform-Connector-role`— Se crea al configurar el conector de cuentas de destino, en la cuenta de administración o en la cuenta de administrador delegado de su AWS organización. Esta función permite a AWS Transform conectarse a tu cuenta de destino y actuar en tu nombre para ejecutar las operaciones de migración.

Configuración del conector de la cuenta de destino

Important

Durante la configuración del conector, se crea un bucket de Amazon S3 en su destino Cuenta de AWS. Este bucket no impondrá el HTTPS-only acceso (SecureTransport) de

forma predeterminada. Si quieres que la política de cubos incluya el transporte seguro, debes actualizarla tú mismo. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon S3](#).

Para usar un conector de cuenta de destino existente

1. En el panel Plan de trabajo, expanda Elegir cuenta de destino y, a continuación, elija Crear o seleccionar conectores.
2. En la pestaña Colaboración, seleccione un conector existente y, a continuación, elija Usar conector. Si un conector no está disponible, su versión no es compatible con el tipo de trabajo que ha seleccionado.

 Important

Si especifica un conector con un destino Región de AWS diferente al de la región de transformación, AWS AWS Transform transferirá los datos de un lado a otro Regiones de AWS.

3. Elija Continuar.

Para crear un conector nuevo

1. En el panel Job Plan, expanda la cuenta de destino de Connect y, a continuación, elija Crear o seleccionar conectores.
2. Especifique el Cuenta de AWS y Región de AWS para su destino y, a continuación, seleccione Siguiente.

 Important

Si el objetivo Región de AWS es diferente del descubrimiento Región de AWS, AWS Transform transferirá los datos de un lado a otro Regiones de AWS.

3. Elija si desea utilizar las claves gestionadas de Amazon S3 para el cifrado. Si especifica su propia clave de KMS, puede usar la política de claves predeterminada o una menos permisiva. Para obtener más información sobre la creación de claves de KMS, consulte [Create a KMS key](#) en la Guía para desarrolladores de AWS Key Management Service .

AWS Transform usa el `kms:DescribeKey` permiso para comprobar que la clave existe `kms:GenerateDataKey` y `kms:Decrypt` para cifrar y descifrar los datos del trabajo en el bucket de Amazon S3. Para obtener más información, consulte [Reducir el costo de usar SSE-KMS las claves de bucket de Amazon S3](#).

4. Elija Continuar.
5. Copia el enlace de verificación, compártelo con un administrador del destino Cuenta de AWS y pídele que apruebe la solicitud de conexión.
6. Una vez que el administrador apruebe la solicitud, seleccione el conector recién creado de la lista y elija Usar conector.
7. Elija Enviar para AWS transformar.

Si planea modificar la AWS Transform MGN plantilla para habilitar las acciones posteriores al lanzamiento, añada el siguiente permiso a la función de conector de destino. Esta declaración de política de JSON otorga el `iam:PassRole` permiso para el rol de acciones posteriores al lanzamiento. Puede encontrar el nombre del rol en la pestaña Colaboración una vez creado el conector. Para obtener información sobre cómo añadir permisos a un rol, consulte [Actualizar los permisos de un rol](#) en la Guía del usuario de IAM.

```
{
  "Sid": "MGNPostLaunchActions",
  "Effect": "Allow",
  "Action": [
    "iam:PassRole"
  ],
  "Resource": "arn:aws:iam::target-account-ID:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
}
```

Regiones de destino compatibles

Una región objetivo de migración es aquella en la que Región de AWS se despliegan los recursos migrados, incluidas las zonas de destino, la infraestructura de red y el realojamiento de los servidores. Al crear el conector, especifique un destino Región de AWS. Puede utilizar cualquiera de las siguientes opciones Regiones de AWS:

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)

- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- África (Ciudad del Cabo)
- Asia Pacific (Hong Kong)
- Asia-Pacífico (Taipéi)
- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Tokio)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Nueva Zelanda)
- Asia-Pacífico (Tailandia)
- Canadá (centro)
- Oeste de Canadá (Calgary)
- Europa (Fráncfort)
- Europa (Zúrich)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (Estocolmo)
- Europa (Milán)
- Europa (España)
- Israel (Tel Aviv)
- México (centro)
- América del Sur (São Paulo)

⚠ Important

Si especificas un objetivo Región de AWS diferente del de la AWS Transformación Región de AWS, algunos de tus datos se transferirán de un lado a otro Regiones de AWS.

Tenga en cuenta que los datos de replicación del servidor van directamente del entorno de origen a la cuenta y la región de destino.

Construye landing zone

AWS Transform lo guía a través del diseño y la implementación de una AWS landing zone como parte de su proyecto de migración. Una landing zone es un AWS entorno de múltiples cuentas que sirve de base para sus cargas de trabajo con límites organizativos, controles de gobierno y estructura contable establecidos antes de que llegue cualquier carga de trabajo. AWS Transform analiza el inventario de migración y los requisitos empresariales para recomendar una unidad organizativa (OU) y una estructura contable, aplicar las políticas de control de servicios (SCP) recomendadas y generar e and/or implementar la infraestructura como código (IaC).

El agente de landing zone te guía a través de dos fases:

- Configuración básica: establezca la estructura principal de la zona de aterrizaje: Torre de AWS Control, unidades organizativas fundamentales y cuentas principales.
- Diseño de cuentas de carga de trabajo: diseñe y cree unidades organizativas y cuentas de carga de trabajo en función de sus oleadas de migración, unidades de negocio y requisitos de separación del entorno.

AWS Transform es compatible con entornos totalmente nuevos (sin zona de aterrizaje existente) y entornos abandonados (unidades organizativas y cuentas existentes ya desplegadas). En los escenarios abandonados, AWS Transform detecta la estructura organizativa existente y recomienda solo los cambios necesarios para subsanar las deficiencias en relación con las mejores prácticas.

AWS

Configuración del conector

El agente de landing zone necesita un Cuenta de AWS conector de destino para aprovisionar los recursos en la cuenta de administración de la organización. El conector tiene permisos para:

- Configurar la [Torre AWS de Control](#)

- Crea [unidades organizativas y cuentas](#)
- Configure [las políticas de control de servicios \(SCP\)](#)

Cuando apruebas la solicitud de conector, concedes permisos de AWS Transform a:

- Aprovisiona y gestiona la infraestructura de la zona de aterrizaje en el objetivo Cuenta de AWS y la región. Esto incluye los permisos para los siguientes elementos, restringidos a los recursos etiquetados con `CreatedBy:AWSTransform` y por ellos, `ATWorkspace:{workspace-id}` cuando proceda:
 - Operaciones de bucket de S3 (crear, leer, escribir, eliminar) para buckets que comiencen por `transform-vmware-landing-zone-`
 - CloudFormation despliegues de pilas y gestión de conjuntos de cambios para pilas de landing zone
 - AWS Operaciones de la Torre de Control (gestionar las zonas de aterrizaje, habilitar las líneas de base y los controles)
 - AWS Gestión de [organizaciones](#) (creación y gestión de unidades organizativas, creación de cuentas y traslado de cuentas)
 - Gestión de la política de control de servicios (SCP) a través de AWS Control Tower
 - AWS Administración de artefactos [de aprovisionamiento de Service Catalog](#)

Al crear el conector, se especifica un destino. Región de AWS Esta región debe ser la misma que la región de la Torre de Control de origen. Para obtener más información sobre las regiones de la Torre de Control, consulta [Cómo Regiones de AWS trabajar con la Torre AWS de Control](#).

Al inicio de la configuración de la landing zone, AWS Transform recupera la configuración del conector y presenta el ID de la cuenta de administración de la AWS organización y la región de destino para su confirmación. Para obtener más información, consulte [Connectors](#).

Important

Dependencia de la región del centro de identidad de IAM: AWS Transform requiere el Centro de identidad de AWS IAM (Centro de identidad de IAM), lo que significa que la región de su conector debe coincidir tanto con la región de origen de la Torre de AWS Control como con la región del centro de identidad de IAM. Si el IAM Identity Center ya está configurado en su organización, la inicialización de la Torre de AWS Control fallará si el conector se dirige a una

región diferente. Para obtener más información, consulte [Consideraciones para los clientes de IAM Identity Center](#) en la Guía del usuario de AWS Control Tower.

Configuración básica

La fase de configuración de los cimientos establece la infraestructura central de la zona de aterrizaje mediante [la Torre AWS de Control](#). Cuando AWS Control Tower configura una landing zone, aprovisiona automáticamente un conjunto de recursos gestionados en tu cuenta de administración que forman la base de gobierno de toda AWS la organización:

- Raíz: el elemento principal de nivel superior que contiene todas las unidades organizativas de tu landing zone.
- Unidad organizativa de seguridad: creada automáticamente por Control Tower. Contiene dos cuentas compartidas: la cuenta Log Archive (registro centralizado e inmutable de todas las actividades de la AWS API y los cambios en los recursos de la organización) y la cuenta de auditoría (acceso de solo lectura a todas las cuentas para comprobar la seguridad y el cumplimiento). Estas cuentas no se pueden cambiar de nombre ni reemplazar después de la configuración inicial.
- Controles obligatorios (barreras): Control Tower aplica automáticamente controles preventivos y de detección en toda la organización para hacer cumplir las políticas de gobierno básicas. No se pueden deshabilitar.
- Directorio de IAM Identity Center: Control Tower crea un directorio nativo de la nube con grupos preconfigurados y acceso de inicio de sesión único para los usuarios de tu landing zone. [Para obtener más información, consulte el Centro de identidades de IAM.AWS](#)

Control Tower utiliza estos recursos [CloudFormation StackSets](#) para implementar y administrar estos recursos de manera uniforme en todas las cuentas y regiones de su organización. No debes modificar ni eliminar los recursos gestionados por la Torre de Control Tower fuera de los métodos admitidos, ya que si lo haces, tu landing zone podría pasar a un estado desconocido.

Convención de correo electrónico de la cuenta

AWS requiere una dirección de correo electrónico única para cada cuenta. Estos correos electrónicos reciben notificaciones importantes para la cuenta. AWS Transform utiliza el direccionamiento positivo para generar correos electrónicos de cuentas únicas desde un único buzón.

Formato: `prefix+account-name@domain`

Usted proporciona un prefijo (por ejemplo `aws-admin`) y un dominio (por ejemplo, `acme.com`), y AWS Transform obtiene todos los correos electrónicos de la cuenta automáticamente. Por ejemplo:

- Cuenta de auditoría: `aws-admin+audit@acme.com`
- Cuenta de Log Archive: `aws-admin+log-archive@acme.com`
- Cuenta Sandbox: `aws-admin+sandbox@acme.com`

En situaciones de abandono industrial, AWS Transform inspecciona los correos electrónicos de las cuentas existentes para deducir la convención de direcciones adicionales que ya se utiliza y ofrece seguir con el mismo patrón.

Estructura de cimentación recomendada

Basándose en las AWS mejores prácticas, AWS Transform recomienda la siguiente estructura básica de unidades organizativas. Puede personalizarla antes de crearla.

OU	Finalidad	Cuentas
Seguridad	Registro y supervisión de auditorías centralizados. El aislamiento de estos servicios en cuentas dedicadas está diseñado para ayudar a mantener su registro de auditoría separado del de los equipos de carga de trabajo.	Auditoría, archivo de registros
Infraestructura	Redes compartidas (Transit Gateway, VPN), DNS y servicios comunes. Se recomienda centralizarlos para ayudar a reducir la duplicación y ofrecer a su equipo de red un único lugar desde el que gestionar la conectividad.	Ninguno (creado en blanco)
Entorno de pruebas	Experimentación por parte de los desarrolladores con los límites de gasto y el acceso restringido. Se recomienda dar a los desarrolladores un espacio para experimentar sin poner en riesgo los recursos de producción.	Entorno de pruebas

OU	Finalidad	Cuentas
Cargas de trabajo	Contiene subunidades de producción y Non-Production, opcionalmente, reguladas. Las cuentas de carga de trabajo se diseñan en la siguiente fase en función de sus requisitos de migración.	Ninguno (creado en blanco)

Note

La unidad organizativa de seguridad con [cuentas de auditoría y archivo de registros](#) se crea como parte de la configuración básica de la Torre de Control. Las unidades organizativas de infraestructura, sandbox y cargas de trabajo se crean por separado después de confirmar la estructura.

En los escenarios abandonados, AWS Transform compara la base existente con la estructura recomendada e informa solo de las carencias. Por ejemplo: «Su fundación tiene unidades organizativas de seguridad e infraestructura, pero no una unidad organizativa tipo sandbox».

Políticas de control de servicios (SCP)

Los SCP son [barreras de protección de permisos a nivel de la organización](#) que establecen los permisos máximos para todas las cuentas de la organización. AWS No conceden acceso, sino que definen límites que nadie en la cuenta puede superar, ni siquiera los administradores de la cuenta.

Como parte del despliegue de la Torre de Control, las barandillas de referencia se colocan automáticamente. AWS Transform también recomienda SCP adicionales diseñados para ayudar a fortalecer la postura de su organización. Se basan en las AWS mejores prácticas para una landing zone mínima viable.

Los SCP se pueden aplicar a las unidades organizativas de infraestructura, entorno aislado y cargas de trabajo. La OU de seguridad está gestionada por la Torre de Control y los SCP no pueden atacarla mediante esta herramienta.

Important

La unidad organizativa de seguridad es una unidad organizativa básica gestionada por Control Tower. No puedes añadirle cuentas, SCP ni ningún recurso a través del agente de landing zone.

En escenarios abandonados, AWS Transform comprueba qué SCP ya se han aplicado y solo recomienda aquellos que puedan cubrir los vacíos.

Despliegue básico

Una vez finalizado el diseño básico, usted elige cómo implementarlo:

- **Implemente por mí:** AWS Transform implementa las unidades organizativas, las cuentas y los SCP básicos en su AWS organización.
- **Lo implementaré por mi cuenta:** AWS Transform genera artefactos de infraestructura como código (IaC) para descargarlos en el formato que prefiera (consulte). [the section called “Formatos iAC”](#)
- **Diseño primero las cuentas de carga de trabajo:** omita la implementación y continúe con la fase de diseño de la cuenta de carga de trabajo. Puede implementar todo junto más adelante.

Inicialización de Control Tower

Si AWS Transform detecta que AWS Control Tower aún no se ha inicializado en su organización, proporciona al usuario un enlace a la página de la consola de AWS Transform. Al generar la operación en el enlace, se creará una CloudFormation pila para iniciar Control Tower. El proceso creará esta pila en la CloudFormation consola para la región de destino. Una vez finalizada la creación de la pila, AWS Transform continúa con el despliegue.

Diseño de cuentas de carga de trabajo

En la fase de diseño de la cuenta de carga de trabajo, AWS Transform diseña la unidad organizativa y la estructura contable para las cargas de trabajo de las aplicaciones en función del inventario de migración, los requisitos empresariales y las preferencias de separación del entorno.

Contexto de planificación de la migración

AWS Transform recupera los datos de la fase de planificación de la migración, incluidos los planes de oleada, las asignaciones del servidor a la aplicación y el contexto compartido. Si hay datos de

planificación de la migración disponibles, AWS Transform muestra un resumen y le pide que lo confirme o lo ajuste. Si no hay datos de planificación de la migración disponibles, AWS Transform formula directamente las preguntas de detección.

Discovery

AWS Transform formula preguntas para comprender sus requisitos de carga de trabajo. Puede omitir cualquier pregunta. Los temas incluyen:

- Número de unidades de negocio o equipos que utilizan AWS
- Industria y cualquier marco aplicable (HIPAA, SOC2 PCI-DSS, FedRAMP)
- Si las cargas de trabajo gestionan datos confidenciales (PII, PHI, financieros)
- Preferencias de separación de entornos (dev/testo staging/prod como cuentas separadas o compartidas)
- Requisitos de aislamiento de cargas de trabajo
- Aplicaciones empresariales y sus finalidades
- Agrupación de servidores en aplicaciones
- Necesidades de seguimiento y asignación de costos (por unidad de negocio, proyecto o entorno)
- Crecimiento esperado en los próximos 12 a 24 meses
- Preferencia de estrategia de cuenta (aplicación única por cuenta, agrupada o basada en el entorno)

Estructura de carga de trabajo propuesta

Basándose en sus respuestas y en los datos de planificación de la migración, AWS Transform propone una unidad organizativa y una estructura de cuentas en la unidad organizativa Workloads. La propuesta incluye el razonamiento en el que se basa cada decisión de diseño.

AWS Transform sigue estos principios de diseño:

- Todos los servidores de una oleada de migración van a la misma cuenta; las oleadas no se pueden dividir entre cuentas. Esta es una limitación de realojamiento durante la ejecución de una oleada.
- Si solicita entornos aislados, AWS Transform crea una Workloads/Non-Production subunidad Workloads/Production organizativa.

- Si se identifican los marcos aplicables, AWS Transform crea una Workloads/Regulated Workloads/Standard sub-OU.
- Si varias unidades de negocio requieren una gobernanza diferente, AWS Transform crea unidades organizativas específicas para cada unidad de negocio en el marco de Workloads.
- Las aplicaciones de datos críticos o confidenciales tienen una sola aplicación por cuenta. En este caso, es posible que se te pida que modifiques tu plan de oleaje.
- Las aplicaciones estrechamente acopladas con dependencias compartidas se agrupan en una sola cuenta.

Cada cuenta propuesta incluye: nombre, finalidad, unidad organizativa objetivo y unidad de negocio. AWS Transform muestra la convención de nomenclatura que se utiliza (por ejemplo, <business-unit>-<environment>-<workload>).

Puede revisar y modificar la estructura propuesta antes de que AWS Transform aplique los cambios. Una vez realizada la solicitud, puede realizar iteraciones y realizar cambios adicionales hasta que quede satisfecho.

Configuración de SCP de carga de trabajo

Una vez creada la estructura de la carga de trabajo, AWS Transform presenta los SCP disponibles y le pregunta si desea aplicar alguno a las unidades organizativas de la carga de trabajo. Usted selecciona qué SCP se van a aplicar y a qué OU. AWS Transform aplica los SCP y muestra el árbol organizativo actualizado con una tabla de resumen de los SCP.

Despliegue de carga

Una vez finalizado el diseño de la carga de trabajo, usted elige cómo implementar:

- Implemente por mí: AWS Transform implementa las unidades organizativas, las cuentas y los SCP de la carga de trabajo en su AWS organización.
- Lo implementaré yo mismo: AWS Transform genera artefactos de IaC para descargarlos en el formato que prefiera (consulte). [the section called “Formatos iAC”](#)

Formatos iAC

Si elige la implementación automática, AWS Transform genera artefactos de infraestructura como código en los siguientes formatos:

- [AWS Cloud Development Kit \(AWS CDK\)](#)— TypeScript proyecto para el despliegue de una infraestructura programática.
- HashiCorp Terraform: genera plantillas de lenguaje HashiCorp de configuración (HCL) para administrar los recursos de las zonas de landing zone.
- Landing Zone Accelerator (LZA): archivos YAML de configuración basados en la versión 1.1.0 de LZA Universal Configuration. Estas plantillas aptas para empresas funcionan con el Landing Zone Accelerator para establecer entornos con varias cuentas. AWS AWS Los archivos generados incluyen ajustes preconfigurados de gobierno, estructura organizativa y redes que se ajustan a las mejores prácticas. AWS Para obtener más información, consulte Configuración [universal de LZA](#).

Note

Al realizar la implementación mediante la canalización de Landing Zone Accelerator (LZA), la cuenta de AWS Transform y la instalación de LZA deben estar en la misma organización. AWS La implementación fallará si no coinciden los ID de las organizaciones utilizados en AWS Transform y LZA. Para obtener información sobre cómo configurar la instalación de LZA mediante Organizations, consulte [Instalación basada en AWS organizaciones](#).

Tras seleccionar un formato, AWS Transform genera los artefactos y los pone a disposición para su descarga.

Para comprobar que el archivo descargado no está dañado o manipulado, genera y descarga una suma de comprobación y, a continuación, compárala con un hash generado localmente mediante:

```
openssl dgst -sha256 -binary <file.zip> | base64
```

Proceso de aprobación de despliegues

Las solicitudes de despliegue en la zona de aterrizaje requieren una aprobación explícita antes de su ejecución. Cuando envías una solicitud de despliegue, se envía automáticamente a los aprobadores autorizados a través de la pestaña AWS Transformar aprobaciones.

Los aprobadores revisan CloudFormation las plantillas y las configuraciones de las zonas de landing zone. Solo los usuarios con el rol de administrador en AWS Transform pueden aprobar las solicitudes de despliegue. Cada envío desencadena un nuevo ciclo de revisión y las implementaciones solo se llevan a cabo después de recibir la confirmación.

Si un responsable de la aprobación deniega tu solicitud, ponte en contacto con él directamente para hablar de las modificaciones necesarias. El sistema realiza un seguimiento de todas las decisiones de aprobación con fines de auditoría y mantiene el historial de implementación.

Etiqueta: landing zone resources

AWS Transform etiqueta automáticamente todos los recursos generados "CreatedBy": "AWSTransform" junto con los identificadores de definición y ejecución para fines de seguimiento.

Etiquetas automáticas

Todos los recursos de la zona de landing zone reciben las siguientes etiquetas:

- CreatedBy— AWS Transform
- ATWorkspace— Identificador del espacio de trabajo

Note

Si su migración forma parte del AWS Migration Acceleration Program (MAP 2.0), puede incluir la etiqueta MAP requerida: Key: map-migrated Value: migMPE_ID (donde MPE_ID es el identificador de evaluación de su cartera de migración). La etiqueta MAP se solicita durante la fase de configuración del conector. AWS Transform aplica estas etiquetas durante el despliegue de la zona de landing zone.

Revertir los cambios

Solo se pueden eliminar los elementos no desplegados. Una vez desplegada una OU o una cuenta, no se puede eliminar a través del agente de landing zone.

A la hora de retirar elementos, el orden importa: hay que eliminar a los niños antes que a los padres:

1. Elimine primero las cuentas (por correo electrónico).
2. Elimine los SCP de las unidades organizativas.
3. Eliminar unidades organizativas secundarias: no se puede eliminar una unidad organizativa si todavía tiene cuentas o unidades organizativas anidadas.

Recursos relacionados

- [the section called “Connect target Cuenta de AWS s y regiones”](#)
- [the section called “Migre su red a AWS”](#)
- [AWS Guía del usuario de Control Tower](#)
- [AWS Guía del usuario de Organizations](#)
- [AWS Guía del usuario de IAM Identity Center](#)
- [CloudFormation Guía del usuario](#)
- [Landing Zone Accelerator activado AWS](#)
- [AWS Well-Architected Plataforma](#)
- [AWS Guía prescriptiva: construcción de zonas de aterrizaje](#)

Migre su red a AWS

Con AWS Transform, puede migrar su red a AWS. AWS Transform traduce la configuración de su entorno de origen en recursos AWS de red equivalentes: VPC, subredes, grupos de seguridad, pasarelas NAT, pasarelas de tránsito, IP elásticas, rutas y tablas de enrutamiento, según sea necesario. Puede revisar y modificar la configuración de red generada antes de la implementación. Puede implementar la configuración con AWS Transform y analizar la conectividad de la red. Como alternativa, puede elegir el despliegue automático y recibir Infrastructure as Code (IaC) en el formato que prefiera: AWS Cloud Development Kit (AWS CDK) Landing Zone Accelerator (LZA) o Terraform. HashiCorp

Para migrar su red, siga estos pasos:

1. Cargue el archivo de red de origen.
2. Cargue archivos de configuración adicionales (opcional, para entornos RVTools).
3. Seleccione una topología de red.
4. Seleccione una estrategia de mapeo de grupos de seguridad.
5. Revise y optimice su red.
6. Genere un diagrama de red (opcional).
7. Configure el etiquetado de recursos.
8. Implemente su red.

 Note

Para las implementaciones con varias cuentas, debe configurar las funciones de IAM entre cuentas y el acceso confiable para AWS Organizations antes de iniciar la migración de la red. Para obtener más información sobre los tipos de migración, consulte [the section called “Paso 1: Selección del tipo de migración”](#)

Paso 1: mapeo de la red de origen

El proceso de mapeo de red requiere que cargue un archivo de configuración desde su entorno de origen. La herramienta que elija depende del tipo de red de origen:

- Redes definidas por software (SDN): Import/Export para la virtualización de redes VMware NSX o configuración Cisco ACI para la infraestructura centrada en aplicaciones de Cisco.
- Redes VMware vSphere: [RVTools](#). Cuando utiliza archivos RVTools, AWS Transform solo genera configuraciones de Amazon VPC. Las configuraciones de los grupos de seguridad requieren una entrada adicional del firewall o de los archivos de red definidos por software. Para obtener más información sobre la generación de grupos de seguridad a partir de archivos adicionales, consulte Archivos de [configuración adicionales](#).
- Redes basadas en los datos de configuración del firewall: exporte archivos desde Palo Alto Networks Firewall, Fortinet FortiGate Firewall o Cisco ACI. Para obtener más información sobre las versiones compatibles y las instrucciones de extracción, consulte Extracción de [archivos de configuración](#).
- Redes híbridas que ejecutan cargas de trabajo tanto de VMware como de terceros: AWS [Transform Discovery Tool](#) o ModelizeIt.
- Otros tipos de archivos: si el archivo de configuración no es uno de los formatos compatibles enumerados anteriormente, el archivo se convierte automáticamente a un formato compatible. Esta conversión puede tardar hasta dos horas en función del tamaño y la complejidad del archivo.

 Note

El tamaño máximo de archivo de red de origen admitido es de 70 MB.

 Warning

Descargue RVTools únicamente desde el sitio oficial de Dell en <https://www.dell.com/en-us/shop/vmware/si/rvtools>. No descargue RVTools de fuentes no oficiales.

Cada segmento de red de origen se asigna a su propia VPC distinta. La segmentación de la red varía según el tipo de fuente:

- vNetwork: AWS transforme grupos de máquinas virtuales mediante un conmutador virtual y una LAN virtual (VLAN). Las VLAN pueden aparecer en varios conmutadores virtuales (excepto en la VLAN 0).
- Redes NSX: AWS transforme los segmentos de la red en función de los Tier-1 enrutadores, agrupe los enrutadores y recopile sus segmentos.

Paso 2: Archivos de configuración adicionales

Para los entornos de origen de RVTools, si lo desea, puede cargar archivos de configuración adicionales para permitir la generación de grupos de seguridad. Si no carga archivos de configuración adicionales, no se generará ningún grupo de seguridad para la RVTools-based migración.

AWS Transform admite los siguientes tipos de archivos de configuración adicionales. Solo puede cargar un archivo de configuración desde una plataforma.

- La infraestructura centrada en aplicaciones (ACI) de Cisco proporciona configuraciones de políticas de red.
- Palo Alto Networks proporciona políticas de seguridad de firewall.
- Fortinet FortiGate proporciona políticas de seguridad de firewall.

Al cargar un firewall o un archivo ACI de Cisco, AWS Transform genera grupos de seguridad e infraestructura de red. Cuando carga un archivo RVTools por sí solo, AWS Transform genera únicamente la infraestructura de red.

Para obtener más información sobre las versiones compatibles y las instrucciones de extracción, consulte Extracción [del archivo de configuración](#).

Paso 3: Topologías de red

Durante el paso de definición de la red, selecciona una topología de red. Puede elegir la topología de VPC aisladas o la topología Hub and Spoke.

VPC aisladas

¿Qué se implementa

Las VPC aisladas son entornos de red independientes que funcionan como unidades independientes en su interior AWS. Sus VPC están completamente aisladas, sin vías de comunicación integradas entre ellas. Esta separación proporciona el nivel más alto de protección de los límites de la red.

AWS Transform crea los siguientes recursos:

- Una VPC dedicada para cada segmento de red de origen detectado.
- Subredes privadas basadas en la configuración de la red de origen.
- Grupos de seguridad (si proporcionó archivos de configuración de firewall o SDN).

Complete la configuración

AWS Transform implementa la infraestructura de red, pero deja que usted se ocupe del acceso a Internet y la conectividad entre VPC, para que pueda elegir la configuración que cumpla con los requisitos de su organización.

Para habilitar el acceso a Internet para una VPC aislada, siga estos pasos:

1. Cree una [puerta de enlace a Internet](#) y adjúntela a la VPC.
2. Cree subredes públicas en cada zona de disponibilidad en la que necesite acceso a Internet. Agregue una ruta para `0.0.0.0/0` apuntar a la puerta de enlace de Internet. Para obtener más información sobre la configuración de [subredes](#), consulte [Subredes para su VPC](#).
3. Cree [puertas de enlace NAT en las](#) subredes públicas (una por zona de disponibilidad para una alta disponibilidad). Asigne una IP elástica para cada puerta de enlace NAT.
4. Actualice [las tablas de enrutamiento](#) de su subred privada: añada una ruta para `0.0.0.0/0` apuntar a la puerta de enlace NAT en la misma zona de disponibilidad.
5. Revise [las reglas de su grupo de seguridad](#) y asegúrese de que las reglas de salida permitan el tráfico que necesitan sus cargas de trabajo (HTTPS, DNS, etc.).

Para VPC-to-VPC la comunicación, configure la interconexión de [VPC](#) o una [Transit Gateway](#) y actualice las tablas de rutas de cada VPC para enrutar el tráfico a la conexión de interconexión o al adjunto de TGW.

Hub and Spoke

En este modelo, una [AWS Transit Gateway](#) actúa como nodo central que conecta varias VPC de carga de trabajo (los radios).

¿Qué se implementa

AWS Transform crea los siguientes recursos:

- VPC radiales: una VPC por segmento de red de origen detectado, con subredes privadas y un adjunto de Transit Gateway.
- VPC de inspección: aloja su dispositivo de firewall para la inspección del tráfico. Todo el tráfico entre VPC se enruta a través de esta VPC. El accesorio Transit Gateway utiliza el [modo dispositivo](#), una configuración que garantiza que el tráfico fluya simétricamente a través del mismo dispositivo en ambas direcciones de una conexión.
- VPC entrante: gestiona el tráfico que entra en la red desde la Internet pública (entrante de norte a sur). Incluye una [puerta de enlace a Internet](#) y subredes públicas en varias zonas de disponibilidad.
- VPC saliente: gestiona el tráfico que sale de la red hacia la Internet pública (saliente de norte a sur). Incluye una puerta de enlace a Internet, [puertas de enlace NAT](#) con [direcciones IP elásticas](#) en cada zona de disponibilidad para una alta disponibilidad y subredes privadas para el adjunto de Transit Gateway.
- Tablas de rutas de Transit Gateway: dos tablas de rutas dirigen el tráfico a través de la VPC de inspección. La tabla No inspeccionada está asociada a las VPC radiales, las VPC entrantes y las VPC salientes; enruta todo el tráfico (0.0.0). 0/0) al adjunto de la VPC de inspección y es la tabla de rutas de asociación predeterminada. La tabla Inspeccionada está asociada a la VPC de inspección: contiene las rutas propagadas de todas las VPC radiales y es la tabla de rutas de propagación predeterminada.

Para las implementaciones con varias cuentas, Transit Gateway se comparte entre las cuentas a través de [AWS Resource Access Manager \(RAM\)](#).

Flujo de tráfico

Todo el tráfico entre VPC sigue esta ruta:

1. El tráfico de una VPC radial se envía a Transit Gateway (ruta predeterminada 0.0.0. 0/0).
2. La tabla de rutas no inspeccionadas dirige el tráfico a la VPC de inspección.
3. El firewall de la VPC de inspección inspecciona el tráfico y lo reenvía a Transit Gateway.
4. La tabla de rutas inspeccionada enruta el tráfico a la VPC radial de destino mediante rutas propagadas.

Para el tráfico de Internet saliente, la tabla de enrutamiento inspeccionada enruta el tráfico a la VPC saliente. Las puertas de enlace NAT traducen las direcciones IP privadas antes de que el tráfico se reenvíe a la puerta de enlace de Internet. La tabla de rutas públicas de VPC salientes incluye rutas específicas para cada rango de enrutamiento Inter-Domain sin clase (CIDR) de VPC radial de regreso a Transit Gateway. Estas rutas permiten que el tráfico de retorno llegue a la VPC de radios correcta.

El tráfico de Internet entrante entra a través de la puerta de enlace de Internet de la VPC entrante y sigue la misma ruta de inspección para llegar a las VPC emitidas por radio.

Complete la configuración

AWS Transform despliega la infraestructura de red, pero deja que usted se ocupe de la configuración del firewall y del servicio entrante, para que pueda elegir las políticas y los dispositivos de seguridad que mejor se adapten a los requisitos de su organización.

 Note

De forma predeterminada, el tráfico entre VPC pasa a través de la VPC de inspección sin inspección. Debe implementar un firewall para permitir la inspección del tráfico.

Implemente un firewall: cree subredes adicionales en la VPC de inspección para los puntos finales del firewall. AWS Transform crea subredes únicamente para el adjunto de Transit Gateway. Dirija el tráfico desde las subredes de conexión del TGW a los puntos finales del firewall y desde las subredes del firewall de vuelta a Transit Gateway. Puede implementar [AWS Network Firewall](#) o un dispositivo de terceros. Para obtener más información sobre cómo implementar un firewall con una Transit Gateway, consulte [Creación de un firewall con una Transit Gateway](#).

Verifica la conectividad: después de implementar el firewall, prueba el acceso saliente a Internet desde una instancia de VPC radial (por ejemplo,). `curl https://aws.amazon.com` Puede utilizar el [Reachability Analyzer para solucionar problemas de conectividad](#).

Configure los servicios entrantes: para alojar servicios de acceso público, implemente un [Application Load Balancer o Network Load Balancer](#) en las subredes públicas de VPC entrantes. Configure los grupos de destino que apunten a las instancias de sus VPC radiales a través de Transit Gateway y compruebe que la tabla de rutas inspeccionada tenga rutas de retorno a la VPC entrante.

Si desea tener un control detallado de la comunicación entre las VPC, elija la opción VPC aisladas y modifique la red generada para crear las rutas de comunicación específicas que necesite.

Paso 4: mapeo de grupos de seguridad

Elija cómo se traducen sus políticas de seguridad de origen en grupos AWS de seguridad. AWS Transform crea grupos de seguridad en función de las configuraciones del entorno de origen. Las políticas de seguridad, las reglas de política de seguridad, las políticas de puerta de enlace y las reglas de política de puerta de enlace se convierten en grupos de seguridad.

Important

AWS Transform crea grupos de seguridad haciendo todo lo posible para adaptarlos a su entorno de origen. Revise y modifique los grupos de seguridad generados para asegurarse de que cumplen con las necesidades y las políticas de seguridad de su empresa.

Referencia a grupos de seguridad

Cuando se generan grupos de seguridad, AWS Transform utiliza la referencia a los grupos de seguridad cuando es posible. La referencia a los grupos de seguridad establece las reglas de seguridad en función de otro ID de grupo de seguridad y no de rangos de direcciones IP específicos (bloques CIDR). Este enfoque proporciona configuraciones de seguridad más flexibles y fáciles de mantener.

Las reglas de su grupo de seguridad solo pueden hacer referencia a otros grupos de seguridad dentro de la misma VPC o en una VPC que esté conectada dentro de la misma región. Cross-account también se admiten las referencias. No puede hacer referencia a un grupo de seguridad en una VPC no conectada ni en todas las regiones. En el caso de las VPC conectadas, solo las reglas de entrada admiten referencias a grupos de seguridad entre VPC; las reglas de salida deben usar reglas CIDR-based. La forma en que AWS Transform crea las reglas de los grupos de seguridad depende de la topología de red elegida:

- Hub and Spoke: Transit Gateway proporciona conectividad de red entre VPC. AWS Transform utiliza referencias tanto para las reglas dentro de la VPC como para las de entrada cruzada. VPC/cross-account Cross-VPC/cross-account Las reglas de salida (de salida) utilizan reglas. CIDR-based
- VPC aisladas: sus VPC no tienen conectividad de red entre ellas. AWS Transform usa referencias solo para las reglas dentro de la VPC. Todas las reglas entre cuentas y VPC utilizan reglas. CIDR-based

CIDR-based las reglas también se utilizan cuando las configuraciones de origen no son simétricas.

Elija una de las siguientes estrategias de mapeo de grupos de seguridad:

- MAP: traduce las reglas de seguridad de su entorno de origen a grupos y reglas de AWS seguridad. Utilice esta opción para las migraciones que utilizan direcciones IP estáticas.
- MAP_DHCP (Translate compatible con DHCP): traduce las reglas de seguridad de su entorno de origen con compatibilidad con DHCP. DHCP asigna direcciones IP de forma dinámica desde el rango CIDR de la subred. Como resultado, las reglas de salida entre VPC se amplían para que coincidan con el CIDR completo de la subred de destino. Un CIDR más estrecho bloquearía las DHCP-assigned IP que se encuentren fuera de ese rango; revise estas reglas después de la migración.

Utilice esta opción para admitir DHCP con la comunicación entre VPC Transit Gateway. También funciona con direcciones IP estáticas, pero puede producir reglas más amplias que las de MAP.

- SKIP: no traduce las reglas de seguridad. Configure los grupos AWS de seguridad manualmente después de la migración. Funciona tanto con entornos de IP estáticos como de DHCP. Para los entornos de origen de RVTools sin archivos de configuración adicionales, AWS Transform utiliza automáticamente SKIP.

Note

Su estrategia de mapeo determina sus opciones de asignación de IP. MAP solo admite direcciones IP estáticas. MAP_DHCP y SKIP admiten tanto el DHCP estático como el DHCP.

Enfoques de migración IP

Tiene dos opciones de configuración de red para la migración:

Selección del rango de redes

- Mantener los rangos existentes (retención de los rangos de direcciones IP): mantenga los rangos de direcciones IP originales durante la migración. Ideal para migraciones en las que se trasladan aplicaciones a otras AWS sin necesidad de modificarlas (levantarlas y desplazarlas), especialmente si se trata de aplicaciones antiguas que tienen dependencias de IP codificadas de forma rígida o reglas de firewall existentes.
- Actualización a nuevos rangos de IP (actualización CIDR): puede modificar cada rango CIDR de VPC durante la migración AWS y Transform propaga automáticamente los cambios a las subredes, tablas de enrutamiento y grupos de seguridad.

Asignación de direcciones IP

- Direcciones IP fijas (estáticas): AWS Transform asigna direcciones IP estáticas en función del CIDR. Esto es lo mejor para las aplicaciones que requieren un comportamiento de red predecible, administración de DNS o control de IP-based acceso. Las IP persisten cuando las instancias se reinician a través de las interfaces de red elásticas (ENI), que son tarjetas de red virtuales conectadas a las instancias.
- Asignación dinámica de IP (AWS DHCP): asigne automáticamente las IP de los grupos de subredes al lanzar la instancia. Óptimo para aplicaciones diseñadas para ejecutarse en la nube y cargas de trabajo que se autoescalan. Reduce la sobrecarga operativa, pero requiere que las aplicaciones utilicen DNS o la detección de servicios.

Puede combinar cualquier selección de rango con cualquier método de asignación de IP.

Note

La estrategia de asignación de direcciones IP se establece a nivel de onda. Puede asignar diferentes estrategias a servidores específicos personalizando el archivo de onda. Por ejemplo, si elige un enfoque de dirección IP estática para la oleada, pero desea asignar un enfoque dinámico a un servidor específico, debe utilizar el enfoque [RESET_VALUE] descrito en [Edición de la configuración](#) de la guía del usuario de MGN.

Paso 5: Revise y optimice su red

Una vez que AWS Transform genere la configuración de red de destino, puede revisar los segmentos de la red local convergidos en la AWS infraestructura. Utilice la interfaz visual para revisar la red y la interfaz de chat para realizar cambios y recibir recomendaciones guiadas. AWS Transform realiza un análisis de impacto en cascada e implementa los cambios necesarios para mantener la coherencia de la red y el cumplimiento de las mejores prácticas. [También puede pedirle a AWS Transform que analice su red y sugiera optimizaciones \(consulte las recomendaciones guiadas\).](#)

Las VPC existentes en tu cuenta de destino

Si su cuenta de destino ya contiene VPC (de fases de migración anteriores o proyectos de infraestructura paralela), AWS Transform las detecta automáticamente y las muestra junto con las VPC mapeadas durante el proceso de revisión. En el caso de las migraciones de varias cuentas, AWS Transform detecta las VPC existentes en todas las cuentas de su organización. AWS

Esta visibilidad le ayuda a comprender cómo se relaciona la red planificada con la infraestructura existente, a identificar posibles conflictos de CIDR y a tomar decisiones informadas antes de la implementación.

Note

AWS Transform solo detecta las VPC existentes (no las subredes u otros recursos). La detección es de solo lectura: AWS Transform no modifica las VPC existentes.

Optimice su red

Note

Estas operaciones se aplican únicamente a las VPC de carga de trabajo. Para las VPC de dispositivos en la topología Hub and Spoke (inspección, entrada y salida), solo se admite el cambio de dirección IP.

No se pueden deshacer las operaciones de eliminación, fusión y división. Revise la configuración detenidamente antes de aplicar estos cambios.

Las siguientes operaciones están disponibles para las VPC:

- **Eliminar:** elimina permanentemente una VPC de la configuración. Úselo para los segmentos de red obsoletos a los que no debería migrar AWS.
- **Excluir:** elimine temporalmente una VPC de la migración para aplicar estrategias de migración por fases. Las VPC excluidas no se implementan, pero se pueden volver a incluir más adelante.
- **Incluir:** vuelva a añadir a la migración una VPC previamente excluida.
- **Fusionar:** combine dos VPC en una sola. La primera VPC conserva su identidad y absorbe todas las subredes de la segunda VPC. Los grupos de seguridad se mueven a la VPC fusionada y sus asociaciones se reconstruyen en consecuencia. El CIDR de la primera VPC se expande hasta el rango de CIDR más pequeño que contiene los CIDR originales, y el enrutamiento se actualiza automáticamente. La segunda VPC se elimina de la configuración.

Requisitos de fusión:

- Los CIDR de subred no deben superponerse entre las dos VPC.
- El CIDR combinado no debe superar /16.
- Para las implementaciones con varias cuentas, ambas VPC deben estar asignadas a la misma cuenta.
- **Cambiar dirección IP:** cambie la dirección IP base de un CIDR de VPC manteniendo la misma longitud de prefijo. AWS Transform traduce automáticamente todos los CIDR de la subred con el mismo desfase. Por ejemplo, al cambiar una VPC de 10.0.0.0/16 a, se 10.20.0.0/16 cambia una subred de a. 10.0.1.0/24 10.20.1.0/24

Las reglas de los grupos de seguridad que coinciden exactamente con el CIDR de VPC anterior se actualizan automáticamente. Las reglas que se superponen parcialmente o que no coinciden con el CIDR anterior no se modifican; revíselas después del cambio.

- **Cambiar el nombre:** cambie el nombre de una VPC para adaptarlo a las convenciones de nomenclatura de su organización en materia de asignación de costes, seguimiento del cumplimiento y estándares operativos.
- **Cambiar el tamaño:** cambie la longitud del prefijo de un CIDR de VPC para ampliar o reducir el rango de direcciones IP.
 - **Disminución de la longitud del prefijo (más direcciones IP, por ejemplo, de /20 a /16):** las subredes siguen quedándose dentro de un rango mayor. No es necesario realizar cambios en la subred.
 - **Aumento de la longitud del prefijo (menos IP, por ejemplo, de /16 a /20):** primero se debe cambiar el tamaño de las subredes que se encuentran fuera del nuevo rango mediante la operación de cambio de tamaño de la subred.

Las reglas de los grupos de seguridad que coinciden exactamente con el CIDR de VPC anterior se actualizan automáticamente. Las reglas que se superponen parcialmente o que no coinciden con el CIDR anterior no se modifican; revíselas después de cambiarlas de tamaño.

Requisitos de cambio de tamaño:

- El nuevo CIDR debe estar entre /16 y /28.
- El nuevo CIDR no debe superponerse con otras VPC de la red (topología Hub and Spoke).
- Al reducir el CIDR, todas las subredes existentes deben caber en el nuevo CIDR. Cambie primero el tamaño de las subredes si es necesario.
- Dividir: divida una VPC en dos VPC según los límites de CIDR que proporcione. Las subredes se asignan a la nueva VPC cuyo CIDR las contiene. Los grupos de seguridad se clonan en las dos VPC nuevas, pero los CIDR de las reglas de los grupos de seguridad no se actualizan automáticamente. Revise las reglas después de dividirlos para asegurarse de que la comunicación entre las VPC funcione según lo esperado. La VPC original se sustituye por las dos VPC nuevas.

Requisitos de división:

- Debe proporcionar exactamente dos rangos de CIDR.
- Los dos CIDR no deben superponerse.
- Cada CIDR debe estar entre /16 y /28.
- Cada subred debe caber exactamente en uno de los dos CIDR. Si alguna subred no cabe, se rechaza la operación.

Las siguientes operaciones están disponibles para las subredes:

- Cambiar la dirección IP: cambie la dirección IP base de un CIDR de subred manteniendo la misma longitud de prefijo.
- Eliminar: elimina permanentemente una subred de la configuración sin que ello afecte a la VPC principal.
- Cambiar el tamaño: cambie la longitud del prefijo del CIDR de una subred para ampliar o reducir el rango de direcciones IP.

Requisitos de cambio de tamaño de subred:

- El nuevo CIDR debe estar entre /16 y /28.
- El nuevo CIDR no debe superponerse con otras subredes de la misma VPC.

- El nuevo CIDR debe estar dentro del CIDR de la VPC principal.

Después de cada operación, AWS Transform vuelve a evaluar las referencias a los grupos de seguridad, lo que puede convertir CIDR-based las reglas en referencias a los grupos de seguridad o viceversa. Revise las reglas del grupo de seguridad después de realizar los cambios para comprobar que cumplen sus requisitos.

Recomendaciones de red guiadas

AWS Transform analiza la red mapeada y proporciona recomendaciones priorizadas a través de la interfaz de chat. Las recomendaciones se basan en los datos de su red y requieren su confirmación antes de aplicar cualquier cambio.

AWS Transform podría recomendar las siguientes optimizaciones:

- Resolución de conflictos de CIDR: marca los rangos de CIDR superpuestos entre las VPC mapeadas y las VPC existentes en todas las cuentas de la organización. AWS Las VPC conflictivas se muestran primero. Puede resolver los conflictos volviendo a abordar la VPC mapeada, excluyéndola o eliminándola, o reconociendo el conflicto y resolviéndolo usted mismo después de la implementación.
- Estandarización de nombres: marca los nombres de las VPC que no siguen un patrón coherente (por ejemplo, los nombres que contienen referencias de hardware). AWS Transform solicita su convención de nomenclatura en la nube antes de proponer reemplazos.
- Revisión del alcance: identifica los segmentos de la red a los que tal vez no sea necesario migrar AWS, como los sistemas antiguos o los componentes pendientes de desmantelamiento. AWS Transform solicita su confirmación antes de excluir cualquier componente.
- Tamaño correcto de la capacidad de las VPC: muestra las VPC en las que el CIDR parece sobredimensionado o insuficiente para las subredes que contiene. AWS Transform presenta los datos de capacidad actuales y le permite decidir si desea cambiar su tamaño.
- Revisión de seguridad: marca las reglas de los grupos de seguridad que permiten el tráfico entrante sin restricciones (0.0.0.0/0) para su revisión.
- Consolidación de VPC: identifica las VPC fragmentadas que parecen estar separadas por los límites de la infraestructura física en lugar de por requisitos de aislamiento lógico, y sugiere fusionarlas.

Note

Todas las recomendaciones requieren su confirmación explícita antes de que AWS Transform aplique cualquier cambio. AWS Transform presenta desventajas cuando una recomendación afecta a varios aspectos de la red.

Paso 6: diagrama de red

Tras revisar las configuraciones de VPC generadas, si lo desea, puede generar un diagrama de red para visualizar la topología de la red. AWS Transform admite los siguientes formatos de diagrama:

- Código Mermaid (.mmd): este formato produce un archivo de definición de diagrama basado en texto que se puede renderizar con herramientas. Mermaid-compatible
- Imagen (.png): este formato produce una imagen renderizada de la topología de la red.

Paso 7: Configurar el etiquetado de recursos

Los recursos de la red se etiquetan para su lanzamiento y replicación. También puede añadir etiquetas personalizadas y etiquetas del AWS Migration Acceleration Program (MAP).

Etiquetas automáticas para el lanzamiento y la replicación

AWS Transform etiqueta automáticamente los recursos de red migrados (VPC, subredes, grupos de seguridad y tablas de enrutamiento) con las siguientes etiquetas:

- Clave: CreatedBy Valor: AWSApplicationMigrationService
- Clave: ATWorkspace Valor: *workspace-id*

Estas etiquetas permiten usar la VPC y la subred para lanzar instancias de prueba y transición. AWS

Note

Las VPC y las subredes migradas no incluyen conectividad a Internet de forma predeterminada, por lo que no son adecuadas como áreas de preparación para la replicación.

Para utilizar también la VPC y la subred como área de ensayo (replicación), añada manualmente las siguientes etiquetas:

- Clave: CreatedFor Valor: AWSTransform
- Clave: ATWorkspace Valor: *workspace-id*

También puede aplicar estas etiquetas a cualquier recurso de AWS red existente para que esté disponible para la replicación.

Busque el ID de su espacio de trabajo en la URL de la aplicación web AWS Transform: [https://...workspace-id /workspace/-id job/job](https://...workspace-id/workspace/-id/job/job)

Etiquetas personalizadas

Además de las etiquetas que AWS Transform aplica automáticamente, también puede añadir etiquetas personalizadas para organizar, realizar un seguimiento de los costes y gestionar la conformidad de los recursos de red migrados. Puede aplicar etiquetas personalizadas en dos niveles:

- Job-level etiquetas: se aplican a todos los recursos creados por este trabajo, incluidas todas las VPC, subredes, grupos de seguridad y tablas de enrutamiento.
- VPC-level etiquetas: se aplican a una VPC específica y se extienden automáticamente en cascada a todos sus recursos asociados (subredes, grupos de seguridad, tablas de enrutamiento).

Note

Máximo 40 etiquetas por solicitud. Cada etiqueta requiere una clave y un valor. AWS Se aplican las convenciones de etiquetado.

AWS Transform aplica estas etiquetas cuando genera las plantillas de infraestructura como código.

AWS Programa de aceleración de la migración

Si su migración forma parte del AWS Migration Acceleration Program (MAP 2.0), AWS Transform aplica una etiqueta MAP a sus recursos. Si proporcionó su ID de MPE al principio del proceso de migración, la etiqueta se aplicará automáticamente. De lo contrario, cuando termine de revisar las configuraciones de VPC generadas, AWS Transform le preguntará si tiene un acuerdo de MAP y le

pedirá que proporcione su ID de MPE, un código de 10 caracteres con letras mayúsculas y dígitos (por ejemplo, ABCDE12345). La etiqueta aplicada utiliza el siguiente formato:

- Clave: map-migrated Valor: migMPE_ID

Paso 8: Implemente su red

Después del etiquetado, seleccione su estrategia de despliegue:

- AWS Transform-managed implementación: AWS Transform usa CloudFormation plantillas para implementar su red y ejecuta Reachability Analyzer para comprobar la conectividad entre las subredes de varias VPC y dentro de la misma VPC.

Note

Debe obtener una aprobación explícita antes de que se ejecute su solicitud de despliegue de red. Consulte [Proceso de aprobación de despliegues](#).

- Self-deployment: AWS Transform genera plantillas de infraestructura como código (IaC). CloudFormation las plantillas se generan de forma predeterminada. También puede seleccionar formatos de salida adicionales:
 - AWS CDK genera un TypeScript proyecto para el despliegue de la infraestructura programática.
 - HashiCorp Terraform genera plantillas HashiCorp de lenguaje de configuración (HCL) para administrar los recursos de la red.
 - Landing Zone Accelerator (LZA) genera un archivo network-config.yaml para la configuración de red de LZA.

Note

Al realizar la implementación mediante la canalización de Landing Zone Accelerator (LZA), la cuenta de AWS Transform y la instalación de LZA deben estar en la misma organización. AWS La implementación fallará si no coinciden los ID de la organización.

Para el despliegue automático, utilice el enlace proporcionado para descargar un archivo zip que contiene las plantillas generadas. La carpeta zip incluye un README.md archivo que explica cómo utilizar las plantillas generadas.

Para comprobar que el archivo descargado no está dañado o manipulado, genera y descarga una suma de comprobación y, a continuación, compárala con un hash generado localmente mediante `openssl dgst -sha256 -binary <file.zip> | base64` un comando.

Proceso de aprobación de despliegues

Para garantizar que los cambios en la red cumplan con los estándares de seguridad y los requisitos de arquitectura de su organización, todas las solicitudes de implementación se someten a un flujo de trabajo de aprobación. Debe obtener una aprobación explícita antes de que se ejecute la solicitud de despliegue de la red. Cuando envía una solicitud de despliegue, se envía automáticamente a los aprobadores autorizados a través de la pestaña AWS Transformar aprobaciones. Los aprobadores validan CloudFormation las plantillas y las configuraciones de red para garantizar el cumplimiento de las normas de seguridad y los requisitos de arquitectura. Cada envío desencadena un nuevo ciclo de revisión y las implementaciones solo se llevan a cabo después de recibir la confirmación. Si un responsable de la aprobación deniega tu solicitud, ponte en contacto con él directamente para hablar de las modificaciones necesarias. AWS Transform realiza un seguimiento de todas las decisiones de aprobación con fines de auditoría y mantiene el historial de implementación.

Elimine los recursos de red desplegados

Si necesita revertir una implementación, puede eliminar los recursos de red que AWS Transform implementó. Puede eliminar los recursos inmediatamente después de que se complete la implementación. Si modifica los recursos de red implementados después de la implementación, los recursos no se pueden eliminar automáticamente.

- **AWS Transform-managed despliegues:** AWS Transform elimina todas las CloudFormation pilas que se crearon durante el despliegue. Esta acción requiere la aprobación a través de la pestaña AWS Transformar aprobaciones.
- **Self-deployments:** Debe eliminar manualmente los recursos implementados mediante la consola AWS de administración o la AWS CLI.

Extracción del archivo de configuración

Si su entorno de origen utiliza Cisco ACI, Palo Alto Networks o Fortinet FortiGate, debe extraer un archivo de configuración para proporcionárselo a Transform. AWS Puede utilizar estos archivos como archivos fuente independientes para generar grupos de seguridad e infraestructura de red, o como archivos complementarios junto con la carga de RVTools para añadir la generación de grupos de seguridad. El proceso de extracción es el mismo en ambos casos.

Para extraer los archivos de configuración de los entornos de red y firewall, siga estos procedimientos. Consulte la documentación del proveedor para obtener la información más reciente.

Fortinet FortiGate

- La versión del firmware debe ser la v7.0 o posterior.
- Necesita nuestros `super_admin` `super_admin_readonly` privilegios a nivel global.
- Pasos:
 1. Conéctese al firewall mediante SSH o un cliente CLI integrado
 2. Ejecutar: `show | grep ""` (`| grep ""` desactiva la paginación)
 3. Guarde todos los resultados en un archivo a partir del comando `show`

Palo Alto Networks

- La versión del firmware debe ser 10.1 o posterior.
- Necesita el rol de superadministrador.
- Conéctese al firewall a través de SSH, ejecute los siguientes comandos para deshabilitar la paginación, establezca el formato de salida, ingrese al modo de configuración y exporte la configuración y los objetos predefinidos. Guarde las salidas:

```
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

- La versión del firmware debe ser 6.0 o posterior.
- Necesita el rol de administrador con todos los privilegios y un destino configurado como Secure Copy Protocol (SCP), SSH File Transfer Protocol (SFTP) o File Transfer Protocol (FTP).
- Pasos:
 1. Conéctese al controlador de infraestructura de políticas de aplicaciones (APIC) a través de su navegador
 2. Abre el menú de administración y selecciona Config Rollbacks

3. En el cuadro de diálogo Realizar una instantánea, seleccione la opción de ubicación remota y elija Crear una instantánea ahora.
4. Tras recibir el mensaje «La transferencia se ha realizado correctamente», conéctese al servidor de ubicación remota y recupere el archivo de instantánea más reciente (archivo.gz)

Migrar servidores

AWS Transform utiliza AWS Transform MGN (MGN) para realojar sus servidores en Amazon EC2. El flujo de trabajo de migración de servidores lo guía a través de la configuración de cada oleada de migración, la validación del inventario de servidores, la implementación de agentes de replicación, la supervisión de la replicación de datos, las pruebas de las instancias migradas y la transición final. [Para obtener más información al respecto, consulte ¿Qué es? AWS Transform MGN](#) en la Guía del usuario de MGN.

La migración de servidores se organiza por oleadas. Cada oleada representa un grupo de servidores que se migran juntos. Para cada oleada, debe completar las siguientes fases:

En el caso de las oleadas con una estrategia de migración basada en contenedores, AWS Transform ejecuta el flujo de trabajo de contenedorización del código fuente en lugar de los pasos de realojamiento que se describen a continuación. El flujo de trabajo de contenedorización lo guía a través de la clonación del código fuente, la generación de artefactos de Docker, la publicación de imágenes de contenedores y la implementación en Amazon Elastic Container Service o Amazon Elastic Kubernetes Service. Para ver el flujo de trabajo de contenedorización completo, consulte.

[Contenedorización del código fuente](#)

1. Requisitos previos y configuración de los valores predeterminados de migración
2. Paso 1: Configurar la ola de migración
3. Paso 2: Validar y confirmar el inventario
4. Paso 3: Implementar agentes de replicación
5. Paso 4: Replicación de datos
6. Paso 5: Probar
7. Paso 6: transición

Requisitos previos y configuración de los valores predeterminados de migración

Requisitos previos

Antes de iniciar la migración de rehospedaje, asegúrese de contar con lo siguiente:

Note

Si has completado todos los pasos de un proceso de migración integral en AWS Transform, tus cuentas de destino y tu fichero de inventario ya están preparados. El fichero de inventario se habrá generado automáticamente durante el paso de planificación de la migración. La infraestructura de red configurada mediante la migración de red de AWS Transform también está lista. Si no creó su infraestructura de red mediante AWS Transform, asegúrese de que esté configurada con antelación antes de iniciar la migración del rehost.

Antes de iniciar la migración del realojamiento, compruebe que dispone de los recursos y la infraestructura de red necesarios para alojar los servidores. Puedes usar las capacidades de migración de redes y zonas de aterrizaje de AWS Transform o cualquier otra herramienta para ello.

- **Sistemas operativos compatibles:** los servidores de origen deben ejecutar un sistema operativo compatible. Para ver la lista completa, consulte [Sistemas operativos compatibles](#) en la Guía del usuario de MGN.
- **Cuentas de destino para la migración:** las Cuenta de AWS ID a las que necesita migrar sus servidores. Puedes usar AWS Transform landing zone o cualquier otra herramienta para configurar tu infraestructura.
- **Infraestructura de red implementada:** VPC, subredes y grupos de seguridad implementados y configurados. Puede usar AWS Transform Network Migration o cualquier otra herramienta para configurar su infraestructura de red.
- **Archivo de inventario:** preparado con los detalles del servidor, las asignaciones de oleadas, la información de la cuenta de destino y las preferencias de tipo de instancia de Amazon EC2. Puede utilizar la planificación de migración de AWS Transform para generar este archivo.

Configure los valores predeterminados de migración

Antes de iniciar la ejecución de la migración de varias cuentas, debe configurar los ajustes predeterminados que se apliquen a todas las cuentas de destino. Estos valores predeterminados definen cómo se lanzan las instancias de Amazon EC2 y cómo se configura la migración general. Puede anular estos valores predeterminados a nivel de oleada durante la configuración de la oleada.

Preferencias de recomendación de Amazon EC2

AWS Transform proporciona recomendaciones de tipos de instancias de Amazon EC2 en función de la especificación de uso de las máquinas virtuales de origen. Puede configurar sus preferencias de recomendación de Amazon EC2 para controlar cómo se seleccionan los tipos de instancias para los servidores migrados.

Para obtener más información sobre la generación de recomendaciones de Amazon EC2, consulte [Generación de recomendaciones de Amazon EC2](#) en AWS Migration Hub

Note

Puede modificar los tipos de instancias de Amazon EC2 sugeridos para incluir recomendaciones del [evaluador de migración](#), la evaluación de [AWS optimización y licencias \(OLA\)](#) o un [trabajo de evaluación](#) de AWS transformaciones.

Inicialización de la migración

Para iniciar la migración, AWS Transform inicializa MGN para todas las cuentas a las que vaya a migrar, así como para todas las cuentas de destino Región de AWS en las que se vaya a utilizar el servicio. Durante el proceso de inicialización:

- Se crean las funciones y políticas de IAM necesarias.
- Se configuran las plantillas predeterminadas requeridas.

Para obtener información sobre el proceso de inicialización, consulte [Inicialización AWS Transform MGN con la consola en la Guía del](#) usuario de MGN.

Plantilla de inicialización de Amazon EC2

La configuración de lanzamiento incluye dos partes: la configuración de lanzamiento general y la plantilla de lanzamiento de Amazon EC2, que determina cómo se lanza una instancia de prueba o transición para cada servidor de origen. AWS

La configuración de lanzamiento, incluida la plantilla de lanzamiento de Amazon EC2, se puede definir a nivel de cuenta y, a continuación, se aplica automáticamente a cada servidor de origen cada vez que se añade un servidor de origen a AWS Transform MGN. Los ajustes de lanzamiento predeterminados definidos en esta sección se pueden aplicar automáticamente a todas sus cuentas de destino.

AWS Transform presenta la lista de ajustes de plantilla de lanzamiento disponibles. Puede optar por continuar con los valores predeterminados o configurar la plantilla de lanzamiento. Si opta por configurarla, AWS Transform proporciona un enlace a una revisión hecha por un humano al tanto (HITL) que contiene todos los parámetros de la configuración de la plantilla de lanzamiento. También puede realizar modificaciones directamente a través de la interfaz de chat para los parámetros que desee.

Los [servidores de origen](#) se crean con la configuración de la plantilla de inicio de la cuenta. Una vez creados los servidores de origen con esta configuración predeterminada, puede cambiarlos en el nivel de configuración de lanzamiento del servidor de origen. Puede cambiar la configuración del servidor de origen en cualquier parámetro mediante la interfaz de chat o, en el caso de operaciones masivas, utilizando el archivo Excel de inventario durante el proceso [Paso 2: Validar y confirmar el inventario](#).

Para revisar la lista completa de ajustes y detalles de la plantilla de lanzamiento, consulte los [ajustes generales de lanzamiento](#) en la Guía del usuario de MGN.

Cambios adicionales en la plantilla de lanzamiento de Amazon EC2

Para realizar cambios adicionales en la plantilla de lanzamiento de Amazon EC2, debe realizarlos en el ID de plantilla de cada cuenta de destino. Esta opción está disponible dentro de la configuración de la onda. AWS Transform lo guía a través de ella y proporciona el enlace correspondiente.

Paso 1: Configurar la ola de migración

En esta fase, AWS Transform prepara la oleada de migración configurando la cuenta de destino, verificando los permisos de servicio, configurando las etiquetas de recursos, añadiendo datos de red al inventario y configurando los ajustes de replicación e inicio.

Modo de migración y configuración de la cuenta

AWS Transform admite dos modos de migración:

- Single-account migración: todos los servidores de la oleada migran a la misma cuenta de destino configurada en el conector.
- Multi-account migración: los servidores migran a diferentes cuentas de destino especificadas en tu fichero de inventario. En el caso de las migraciones de varias cuentas, tu fichero de inventario debe incluir una `mgn:account-id` columna con el ID de cuenta de destino de cada servidor.

AWS Transform confirma la configuración de la cuenta de destino y verifica que MGN esté inicializado en cada cuenta de destino. Si MGN aún no se ha inicializado, AWS Transform proporciona instrucciones para completar la inicialización. Durante la inicialización, MGN crea las siguientes funciones de servicio de IAM para las operaciones de replicación y lanzamiento:

- `AWSApplicationMigrationReplicationServerRole`
- `AWSApplicationMigrationConversionServerRole`
- `AWSApplicationMigrationMGHRole`
- `AWSApplicationMigrationLaunchInstanceWithDrsRole`
- `AWSApplicationMigrationLaunchInstanceWithSsmRole`
- `AWSApplicationMigrationAgentRole`

Para obtener más información sobre estas funciones, consulte [Inicializar MGN con la consola o Inicializar MGN con la API en la Guía del usuario de MGN](#).

Para las migraciones de varias cuentas, AWS Transform también crea el siguiente rol durante el paso de inicialización: `AWSTransformRehostSharingRole_<management-or-delegated-admin-account-id>` Esta función se implementa en todas las cuentas objetivo de la migración.

Verificación del etiquetado de recursos

Una vez confirmados los permisos del servicio, AWS Transform comprueba que todos los recursos necesarios estén correctamente etiquetados para que el agente lleve a cabo la migración correctamente. Si a algún recurso le faltan las etiquetas obligatorias, AWS Transform proporciona un enlace a la página de etiquetado en el que puede aplicar las etiquetas que faltan antes de continuar. Se requieren las siguientes etiquetas:

- Los servidores de origen existentes deben tener etiquetas `CreatedBy: AWSTransform` y `ATWorkspace: <workspace_id>`. Si ya ha iniciado la replicación en los servidores de origen y los ha creado en el servicio AWS Transform MGN, debe etiquetarlos para que AWS Transform pueda correlacionarlos con los servidores de origen detectados en su entorno local y evitar la creación innecesaria de servidores de origen duplicados. AWS Transform los correlaciona automáticamente mediante las claves de ID, FQDN o nombre de host proporcionadas por el usuario.
- Los recursos de red deben estar debidamente etiquetados tanto para las instancias de replicación (área de ensayo) como para las de lanzamiento. AWS Transform muestra la lista completa de los recursos de red de la cuenta de destino, con una indicación de si cada recurso ya está etiquetado o no. Puede revisar la lista y seleccionar los recursos sin etiquetar que desee agregar. Para cada recurso que seleccione, AWS Transform aplica la etiqueta correspondiente:
 - `CreatedBy: AWSTransform` bien `CreatedFor: AWSTransform`, según el tipo de recurso.
 - `ATWorkspace: <workspace_id>` se aplica a todos los recursos seleccionados.

Las VPC y las subredes creadas por el agente de migración de red AWS Transform se etiquetan automáticamente.

- Además de las VPC y las subredes, AWS Transform también muestra todas las interfaces de red elástica (ENI) existentes que se encuentran en la cuenta de destino. Si quieres que AWS Transform las use como parte del lanzamiento de tu instancia, debes etiquetarlas con `y. CreatedFor: AWSTransform` `ATWorkspace: <workspace_id>` Para obtener más información sobre cómo adjuntar o añadir ENI a la plantilla de lanzamiento de Amazon EC2, [consulte las consideraciones detalladas](#) en la Guía del usuario de MGN.

Añada datos de red al inventario

AWS Transform añade la información de red de la migración de la red al archivo de inventario. Este paso asigna los servidores a las subredes y grupos de seguridad de destino adecuados en función de la configuración de red generada durante la fase de migración de la red.

Configuración de replicación e inicio

Configuración de los parámetros de replicación

La configuración de replicación determina cómo se replican los datos desde los servidores de origen a AWS. Configure los ajustes de replicación en la plantilla de replicación antes de agregar los servidores de origen a AWS Transform MGN. AWS Transform le muestra todos los parámetros

de configuración de la replicación; puede configurarlos mediante un HITL específico o mediante la interfaz de chat.

Para obtener más información sobre los parámetros de configuración de replicación, consulte la [plantilla de configuración de replicación](#) en la Guía del usuario de MGN.

Inicie la configuración de la plantilla

La plantilla de lanzamiento te permite controlar la forma en que AWS Transform MGN lanza las AWS instancias. La configuración predeterminada definida en la plantilla se aplica automáticamente a cada servidor recién agregado. Puede configurar los ajustes de la plantilla de lanzamiento a través de un HITL específico o mediante la interfaz de chat.

Para obtener más información sobre los parámetros de configuración de la plantilla de lanzamiento, consulte la [plantilla de lanzamiento](#) en la Guía del usuario de MGN.

AWS Transform también proporciona un enlace al ID de la plantilla de lanzamiento de Amazon EC2 asociado a la plantilla de lanzamiento, lo que le permite cambiar los atributos adicionales de la plantilla de lanzamiento de Amazon EC2. Para editar la plantilla de lanzamiento de Amazon EC2, siga las instrucciones de la plantilla de [lanzamiento de la Guía](#) del usuario de MGN.

Estrategia de asignación de propiedad intelectual

Usted elige cómo se asignan las direcciones IP a los servidores migrados:

- IP estática: se mantiene la dirección IP del servidor de origen. Si se requiere la transformación CIDR, AWS Transform convierte automáticamente la dirección IP para que coincida con la nueva CIDR.
- IP dinámica (DHCP): a cada servidor se le asigna una nueva dirección IP del conjunto de direcciones IP de la subred.

Note

Si seleccionó la estrategia de mapeo de grupos de seguridad MAP durante la migración de la red, solo estará disponible la asignación de IP estática. Para obtener más información, consulte [Mapeo de grupos de seguridad](#).

Paso 2: Validar y confirmar el inventario

Antes de cargar los datos del servidor en MGN, AWS Transform prepara el fichero de inventario para que lo revise. Puede descargar el archivo en formato CSV o XLSX, revisar las configuraciones del servidor y realizar los cambios necesarios.

El fichero de inventario incluye detalles como los nombres de los servidores, los sistemas operativos, las recomendaciones de tipos de instancias de Amazon EC2, las subredes de destino, los grupos de seguridad, las asignaciones de IP y las opciones de licencia. Los campos obligatorios incluyen:

- Información del servidor: nombre del servidor, VMID y especificaciones de la fuente.
- Asignación de oleadas: agrupación de oleadas de migración.
- Agrupación de aplicaciones: asociaciones lógicas de aplicaciones.
- Configuración de destino: cuenta de destino, región y tipo de instancia de Amazon EC2.
- Configuración de red: subred y grupos de seguridad de destino.

Puede modificar el archivo para ajustar las configuraciones de Amazon EC2, cambiar las opciones de licencia del sistema operativo (BYOL o licencia incluida) y actualizar la configuración de arrendamiento.

Tras revisar el inventario, puede aceptarlo tal y como se muestra o subir una versión modificada. AWS Luego, Transform carga los datos en MGN, que crea registros de servidor de origen para cada servidor de la oleada.

Note

No elimines columnas ni cambies los encabezados de las columnas del fichero de inventario. AWS Transform requiere la estructura de archivos original para procesar los datos correctamente.

Note

AWS La transformación permite realizar una importación a un destino determinado Cuenta de AWS y Región de AWS a un objetivo a la vez. Si trabaja en más de una oleada simultáneamente, o si hay más de una tarea de migración en ejecución con la misma cuenta

de destino, debe esperar a que finalice la importación para poder realizar otra importación en una oleada o tarea diferente.

Puedes controlar las opciones de licencia del sistema operativo (BYOL o licencia incluida) y el arrendamiento especificando la configuración en las columnas `mgn:launch:placement:operating-system-licensing` y del fichero de inventario. `mgn:launch:placement:tenancy` Para obtener más información, consulte [Importación de parámetros](#) en la Guía del usuario de MGN.

Paso 3: Implementar agentes de replicación

Para empezar a replicar los datos desde sus servidores de origen AWS, instale el agente de AWS replicación en cada servidor de origen. AWS Transform ofrece tres métodos de instalación:

- Herramientas de organización: utilice las herramientas de implementación existentes de su organización (como SCCM, Ansible o Chef) para instalar agentes en sus servidores. AWS Transform proporciona a los comandos de instalación parámetros adicionales para una instalación silenciosa, como `--no-prompt --aws-access-key-id--aws-secret-access-key`, y. `--aws-session-token`
- Conector MGN: utilice un conector MGN para automatizar la instalación del agente. El conector se conecta a las máquinas de origen a través de SSH (Linux) o WinRM (Windows) e instala el agente de replicación automáticamente. Una vez configurado, un conector se puede reutilizar en varias ondas y en diferentes destinos. Cuentas de AWS Para obtener más información sobre el conector MGN, consulte [Configuración del conector MGN en la Guía del](#) usuario de MGN.

Note

Antes de usar el conector MGN con AWS Transform, debe etiquetar la instancia gestionada del conector en AWS Systems Manager Fleet Manager con las siguientes etiquetas:

- Clave: CreatedFor Valor: AWSTransform
- Clave: ATWorkspace Valor: *workspace-id*

Para etiquetar la instancia gestionada, abra la AWS Systems Manager consola, vaya a Fleet Manager en Node Tools, elija la instancia gestionada de su conector MGN y aplique

las etiquetas anteriores. Busca el ID de tu espacio de trabajo en la URL de la aplicación web AWS Transform: `https://.../workspace/workspace-id/job/job-id`.

- **Instalación manual:** instale el agente directamente en cada servidor de origen. Este método requiere acceso directo a cada servidor, pero le proporciona un control total sobre el proceso de instalación.

AWS Transforme la configuración del conector MGN

El conector AWS Transform MGN automatiza la implementación de agentes de replicación en los servidores de origen. El conector es un cliente ligero que se implementa en una máquina Linux dedicada en su entorno local. Se conecta a los servidores de origen a través de SSH (Linux) o WinRM (Windows) para instalar y configurar los agentes de replicación, lo que elimina la necesidad de coordinar manualmente varios AWS servicios.

Cómo funciona el conector

El conector funciona a través de los siguientes componentes:

- **Cliente Connector:** se implementa en una máquina Linux dedicada de su entorno.
- **Agente SSM:** se instala en la misma máquina para permitir una comunicación segura con AWS.
- **Activación híbrida SSM:** vincula la máquina conectora a AWS Systems Manager para ejecutar comandos de forma segura.
- **Administración de credenciales:** recupera las credenciales del servidor de origen de AWS Secrets Manager.

Al implementar agentes, AWS Transform envía un documento SSM a la máquina conectora. A continuación, el conector recupera las credenciales del servidor de origen de AWS Secrets Manager, establece una conexión con cada servidor de origen, valida que el servidor de origen cumpla los requisitos previos, instala y configura el agente de replicación y comprueba que la instalación se ha realizado correctamente.

Requisitos de la máquina de conexión

Requisito	Details
Sistema operativo	Sistema operativo Linux compatible. Para ver la lista completa, consulte los requisitos previos del conector MGN en la Guía del usuario de MGN.
Acceso a la red	Debe llegar a todos los servidores de origen (Linux a través de SSH, Windows a través de WinRM)
Conectividad a Internet	HTTPS saliente (443) a AWS puntos finales (Systems Manager, Secrets Manager, MGN)
Espacio en disco	Mínimo 200 MB libres
Permisos	Acceso root o sudo

Note

El conector debe estar instalado en una máquina Linux, pero puede implementar agentes en los servidores fuente de Linux y Windows.

Proceso de configuración

AWS Transform le guiará por los siguientes pasos para configurar el conector:

Paso 1: Configuración del conector

Proporcione un nombre para el conector o utilice el nombre predeterminado generado automáticamente. El conector se puede instalar en la cuenta de administración o en una cuenta de administrador delegado en MGN. Para las migraciones de varias cuentas, el conector puede implementar agentes en los servidores de las cuentas de los miembros.

Paso 2: AWS configuración de recursos

AWS Transform abre una página de configuración que se ejecuta en su navegador con sus AWS credenciales. Debe iniciar sesión en la consola AWS de administración con su cuenta de

administración o con su cuenta de administrador delegado. Debe ser la misma cuenta a la que está conectado su conector de destino AWS Transform.

La página de configuración crea automáticamente los siguientes recursos:

- Funciones de IAM (creadas de forma idempotente; se omiten si ya existen):
 - `AWSApplicationMigrationConnectorManagementRole`— Se utilizan durante la instalación del agente para acceder a las credenciales.
 - `AWSApplicationMigrationConnectorSharingRole_<ACCOUNT-ID>`— Contiene los permisos para la instalación del agente.
- Activación híbrida de SSM: período de caducidad de 30 días. Vincula la máquina conectora a AWS Systems Manager y genera credenciales de activación seguras.

Como alternativa, puede descargar una CloudFormation plantilla de la página de configuración para implementar las funciones de IAM usted mismo.

La página de configuración genera un comando de instalación de una línea con todas las credenciales y la configuración necesarias.

Important

Mantenga abierta la página de configuración hasta que se complete la instalación. Para cerrarla, será necesario reiniciar el proceso. Todas las credenciales solo existen en su navegador y Transform no las AWS almacena.

Paso 3: Instalación del conector

Instale el conector en una máquina Linux de su entorno:

1. Copie el enlace de instalación de la página de configuración.
2. Utiliza SSH en la máquina Linux que elijas.
3. Pegue y ejecute el comando de instalación.
4. Espere a que se complete la instalación (normalmente de 2 a 3 minutos).

Paso 4: Adjunte los servidores de origen

Tras la instalación, AWS Transform identifica todos los servidores de origen que pertenecen a la oleada actual y los conecta automáticamente al conector MGN.

Paso 5: Configurar las credenciales

Proporcione AWS los ARN de Secrets Manager para las credenciales de su servidor de origen. AWS Transform ofrece tres opciones de configuración de credenciales:

- Secreto único para servidores Linux: un secreto compartido que contiene claves SSH o username/password para todos los servidores fuente de Linux.
- Secreto único para los servidores Windows: un secreto compartido que contiene el nombre de usuario y la contraseña de todos los servidores fuente de Windows.
- Varios secretos por servidor: diferentes secretos por servidor o grupo de servidores. Úselo cuando los servidores tengan credenciales diferentes. AWS Transform genera un archivo CSV relleno previamente con su lista de servidores. Rellena la `secret_arn` columna de cada servidor y carga el archivo completo.

Note

Puede combinar las opciones de secreto único de Linux y Windows si tiene ambos tipos de servidores con un secreto compartido cada uno. La opción de secretos por servidor se excluyen mutuamente con las opciones de secreto único.

Formato de secreto de credenciales. Para obtener más información al respecto, consulte las [credenciales del conector MGN](#) en la Guía del usuario de MGN:

```
{
  "WinConnectionProtocol": "HTTPS",
  "WinUserName": "windows_username",
  "WinPassword": "windows_password",
  "LinuxUserName": "linux_username",
  "LinuxPrivateKey": "linux_private_key",
  "LinuxHostKeyValidation": false
}
```


Despliegue de agentes

Una vez configuradas y verificadas las credenciales, AWS Transform despliega los agentes de replicación en los servidores de origen. Puede implementarlos en todos los servidores de la oleada actual o seleccionar servidores específicos.

El proceso de implementación de cada servidor:

1. AWS Transform envía los comandos de despliegue al conector mediante SSM.
2. El conector recupera las credenciales de AWS Secrets Manager.
3. El conector se conecta al servidor de origen mediante las credenciales configuradas.
4. El conector valida que el servidor de origen cumpla todos los requisitos previos necesarios para ejecutar el agente de replicación.
5. El conector instala y configura el agente de replicación.
6. El conector verifica que la instalación y la conectividad se hayan realizado correctamente.

Puede supervisar el progreso de la implementación en tiempo real con un seguimiento del estado por servidor, que incluye el paso de instalación actual, el tiempo transcurrido y el tiempo restante estimado. Si algún servidor falla, AWS Transform muestra el motivo del error y ofrece opciones de reintento por servidor. Los servidores implementados correctamente pueden continuar de forma independiente mientras los servidores que fallan se vuelven a intentar.

Reutilización y ciclo de vida de los conectores

Al implementar agentes para oleadas posteriores, puede reutilizar un conector existente o crear uno nuevo. AWS Transform muestra todos los conectores configurados en su cuenta y muestra el nombre del conector, su estado (activo o caducado), el número de servidores conectados y la fecha de caducidad de la activación híbrida.

- Conector activo: la activación híbrida sigue siendo válida. AWS Transform verifica las funciones de IAM para la nueva ola y procede a la configuración de las credenciales. No se necesita una nueva activación híbrida.
- Conector caducado: la activación híbrida del SSM ha caducado. Las activaciones caducadas no se pueden renovar. Debe seleccionar un conector diferente o crear uno nuevo.

Las activaciones híbridas de SSM caducan a los 30 días. La activación solo es necesaria para instalar el conector en la máquina Linux. Una vez instalado el conector, puede seguir utilizándolo

para instalar agentes de replicación en los servidores de origen incluso después de que caduque la activación. Si necesita instalar el conector en una máquina nueva después de que la activación haya caducado, tendrá que crear un conector nuevo mediante el proceso de configuración.

Instalación manual del agente

Para la instalación manual, primero debe generar AWS las credenciales (temporales o permanentes) y, a continuación, instalar el agente en cada servidor de origen.

Opciones de credenciales:

- Credenciales temporales (recomendadas): cree un rol de IAM con la política `AWSApplicationMigrationAgentInstallationPolicy` gestionada y utilícelo `aws sts assume-role` para generar credenciales temporales. Para obtener más información al respecto, consulte los [permisos de instalación del agente](#) en la Guía del usuario de MGN.
- Credenciales permanentes: cree un usuario de IAM con la política `AWSApplicationMigrationAgentInstallationPolicy` gestionada y genere una clave de acceso.

Pasos de instalación:

Para servidores Linux, descargue y ejecute el 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, descargue y ejecute el instalador correspondiente utilizando 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

El parámetro `--user-provided-id` es obligatorio. *server-identifier* Sustitúyelo por el valor exacto de la `mgn:server:user-provided-id` columna de tu fichero de inventario. Este identificador vincula el servidor físico con su registro de servidor de origen MGN.

Para obtener más información sobre la instalación del agente, consulte el agente de [Linux y el agente](#) de [Windows](#) en la Guía del usuario de MGN.

Tras la instalación, AWS Transform comprueba que todos los agentes se hayan conectado correctamente comprobando que los servidores muestran un estado de INITIATING replicación igual o igual. INITIAL_SYNC

i Note

AWS Transform no admite la replicación sin agente MGN. Para obtener información sobre la replicación sin agente, consulte la descripción general de la [replicación sin agente](#) en la Guía del usuario de MGN.

i Note

Debe instalar el agente de replicación en todos los servidores de una sola vez. Desconecte y archive los servidores en los que no instale el agente de replicación. Puede usar el `disconnect-from-service` comando para desconectar los servidores y el `mark-as-archived` comando para archivar los servidores desconectados. El comando de archivado solo funciona para los servidores de origen cuyo estado de ciclo de vida sea DISCONNECTED.

Para conocer las cuotas relacionadas con la replicación, consulte los [límites de las cuotas de servicio de MGN](#) en la Guía del usuario de MGN.

Paso 4: Replicación de datos

Una vez instalados los agentes de replicación, la replicación de datos comienza automáticamente. AWS Transform utiliza la replicación continua a nivel de bloque para sincronizar los datos desde los servidores de origen a los mismos. AWS

El proceso de replicación consta de dos fases:

- Sincronización inicial: una copia completa de los datos del servidor de origen a AWS. Los datos se almacenan como instantáneas de Amazon Elastic Block Store (Amazon EBS) o en Amazon FSx para los volúmenes de ONTAP (FSx NetApp for ONTAP) de la cuenta de destino, según el tipo de almacenamiento de destino configurado. Para obtener más información, consulte el [tipo de almacenamiento de destino](#) en la Guía del usuario de MGN. La duración depende del volumen de datos y del ancho de banda de la red.
- Replicación continua: sincronización continua de los bloques modificados con un impacto mínimo en el rendimiento del servidor de origen. Mantiene una copia actualizada AWS.

Los servidores de replicación son instancias temporales de Amazon EC2 que se implementan en la subred del área de ensayo. Reciben datos replicados de los servidores de origen y MGN los administra automáticamente. Para obtener más información al respecto, consulte la [configuración del servidor de replicación](#) en la Guía del usuario de MGN.

AWS Transform supervisa el progreso de la replicación y proporciona actualizaciones de estado, que incluyen el estado de la replicación, el retraso de la replicación (la diferencia de tiempo entre los datos de origen y los replicados) y el uso del ancho de banda.

Durante la replicación, cada servidor pasa por los siguientes estados:

- No está listo: el servidor se encuentra en el proceso de sincronización inicial y aún no está listo para la prueba.
- Listo para la prueba: el servidor se agregó correctamente y se inició la replicación de los datos. Ahora se pueden lanzar instancias de prueba o transitorias.

Una vez que todos los servidores de la oleada hayan superado el NOT_READY estado, habrá finalizado la fase de replicación de datos y podrá continuar con las pruebas.

Puede controlar la replicación de servidores individuales o de toda la oleada en cualquier momento:

- Pausar la replicación: detenga temporalmente la replicación de servidores específicos o de toda la oleada.
- Reanudar la replicación: reanude la replicación previamente pausada.
- Detenga la replicación: detenga la replicación de forma permanente. La replicación detenida se puede reiniciar, pero comienza desde la sincronización inicial.

Paso 5: Probar

Una vez completada la replicación de los datos, puede lanzar instancias de prueba para validar los servidores migrados antes de realizar la transición final. Para obtener más información al respecto, consulte [Lanzamiento de instancias de prueba](#) en la Guía del usuario de MGN. AWS Transform admite dos opciones de prueba:

- Pruebas de oleada completa: lance instancias de prueba para todos los servidores de la oleada.
- Pruebas selectivas: lanza instancias de prueba para servidores específicos que selecciones proporcionando los ID proporcionados por el usuario en el fichero de inventario.

AWS Transform lanza las instancias de Amazon EC2 a partir de los datos replicados y proporciona los ID de las instancias para que pueda conectarse a las instancias de prueba y validarlas. Tras realizar las pruebas, puede:

- Si la prueba se realiza correctamente, proceda a la transición.
- Lance nuevas instancias de prueba para volver a realizar la prueba.
- Finalice las instancias de prueba y solucione cualquier problema antes de volver a realizar las pruebas.

Paso 5b: Marque las aplicaciones como listas para la transición

Una vez finalizadas las pruebas y cuando esté satisfecho con los resultados, marque las aplicaciones como listas para la transición. AWS Transform revisa el estado de replicación de cada aplicación y resuelve cualquier alerta de replicación antes de permitirle continuar. Solo las aplicaciones con un estado de replicación limpio se pueden marcar para su transición.

Paso 6: transición

La transición es el último paso de migración al que se trasladan las cargas de trabajo de producción. Para obtener más información al respecto, consulta [Cómo lanzar instancias transitorias en la Guía del usuario](#) de MGN. Al igual que las pruebas, AWS Transform admite la transición de onda completa o la transición selectiva para servidores específicos.

Durante la transición, AWS Transform lanza las instancias de Amazon EC2 a partir de los datos replicados más recientes y proporciona los ID de instancia de cada servidor. Tras verificar las

instancias de transición, se finaliza la transición, lo que detiene la replicación en curso de la máquina de origen.

El proceso de transición incluye los siguientes pasos:

1. Lance instancias transitorias: AWS Transform lanza instancias de Amazon EC2 para los servidores seleccionados. Puede elegir una transición de onda completa o una transición selectiva.
2. Verificar las instancias de transición: Conéctese a las instancias lanzadas y compruebe que funcionan correctamente.
3. Finalizar la transición: confirme la transición para detener la replicación de la máquina de origen. Puede finalizar todos los servidores de la oleada o seleccionar servidores específicos. La finalización impide que los agentes de replicación envíen datos, elimina los agentes de replicación de los servidores de origen y bloquea el estado del ciclo de vida del servidor. Esta acción no se puede deshacer fácilmente. Para obtener más información al respecto, consulte [Finalizar la transición en la Guía del usuario](#) de MGN.
4. Servidores de origen de archivos (opcional): una vez finalizados, puede marcar los servidores de origen como archivados para liberar la cuota de servidores de origen en su cuenta.

Important

Al finalizar la transición, se detiene la replicación en curso de la máquina de origen. Asegúrese de haber verificado las instancias de transición antes de finalizar.

Note

El tiempo de inactividad se produce entre el cierre de la fuente y la disponibilidad de la instancia transitoria. Planifique el período de transición en consecuencia.

Estados del ciclo de vida del servidor

Durante la migración, cada servidor pasa por los siguientes estados del ciclo de vida. Para obtener más información al respecto, consulte el [ciclo de vida del servidor de origen](#) en la Guía del usuario de MGN.

- No está listo: el servidor se encuentra en el proceso de sincronización inicial y aún no está listo para las pruebas.
- Listo para las pruebas: se ha iniciado la replicación de datos y se pueden lanzar instancias de prueba o de transición.
- Prueba en curso: actualmente se está lanzando una instancia de prueba.
- Listo para la transición: el servidor se ha probado y está listo para la transición.
- La transición está en curso: actualmente se está lanzando una instancia de transición.
- Transición completa: se ha realizado la transición del servidor. Todos los datos se han migrado a la instancia de transición. AWS
- Desconectado: el servidor se ha desconectado de MGN.

Puede preguntar a AWS Transform sobre el estado de sus servidores en cualquier momento durante la migración. AWS Transform proporciona una tabla de estado de oleada interactiva que muestra toda la información relevante del servidor, incluido el ciclo de vida de la migración, el estado de la replicación y los próximos pasos recomendados. También puede preguntar en lenguaje natural, por ejemplo:

- ¿Cuál es el estado de mis servidores?
- ¿Cuál es el estado de mi ola?
- ¿En qué estado se encuentra el escalón en el que me encuentro actualmente?

Durante la migración en oleada, puedes pedirle a AWS Transform que actualice o cambie el estado de los servidores individuales. Por ejemplo, si 9 de los 10 servidores de su oleada han superado la fase de prueba pero uno ha fallado, puede permitir que AWS Transform continúe trasladando los 9 servidores a la siguiente fase y, al mismo tiempo, vuelva a ejecutar la prueba en el servidor que ha fallado.

Aprobaciones de implementación

Algunas operaciones de migración requieren una aprobación explícita antes de su ejecución. Cuando una operación requiere aprobación, AWS Transform envía la solicitud a los aprobadores autorizados a través de la pestaña Aprobaciones. Solo los usuarios con el rol de administrador en AWS Transform pueden aprobar las solicitudes de implementación. Las implementaciones solo se realizan después de recibir la confirmación.

Notas de la versión

En las siguientes notas de la versión se describen los cambios más recientes de [Migraciones \(incluida VMware\)](#). Para ver las regiones de AWS transformación compatibles, consulte [Regiones compatibles](#). Para ver las regiones de destino compatibles, consulta la [página de configuración del conector de cuentas](#).

Junio de 2026

- AWS Transform for Migrations ahora admite la localización. Puede cambiar el idioma de visualización de la aplicación web al trabajar con flujos de trabajo de migración. [Más información sobre la configuración de idioma](#).
- AWS Transform ahora le permite configurar los ajustes de replicación y los ajustes de inicio para la migración. Puede establecer la configuración para su cuenta de destino o para servidores de origen específicos. [Obtenga más información sobre la configuración de replicación e inicio](#).
- AWS Transform ahora le permite conectar las interfaces de red elásticas (ENI) existentes a su plantilla de lanzamiento. Puede etiquetar los ENI en su cuenta de destino para que estén disponibles para su uso cuando se lancen las instancias. [Obtén más información sobre el etiquetado de recursos de red](#).
- AWS Transform for migrations ahora admite todas las regiones AWS comerciales como objetivos de migración, excepto Oriente Medio (Baréin) y Oriente Medio (Emiratos Árabes Unidos). [Obtenga más información sobre las regiones de destino compatibles](#).

Mayo de 2026

- AWS Transform ahora detecta las VPC existentes en su cuenta de destino durante la revisión de la migración de la red. Puede ver las VPC existentes junto con las VPC mapeadas, identificar los conflictos de CIDR y resolverlos antes de la implementación. [Más información sobre la detección de VPC existente](#).
- AWS Transform permite cambiar de plataforma los repositorios de código fuente a contenedores durante la migración a. AWS [Más información sobre](#) la contenedorización.

Abril de 2022

- Se agregó la creación de landing zone directamente en los flujos de trabajo de migración. AWS Transform comprueba una base existente, recomienda estructuras de unidades organizativas (OU) y cuentas objetivo, y ofrece un despliegue automatizado o un resultado de infraestructura como código (IaC) (formatos CloudFormation AWS CDK, o Landing Zone Accelerator (LZA)). [Más información sobre la creación de zonas de aterrizaje](#).
- Se agregó compatibilidad con DHCP con mapeo de grupos de seguridad durante la migración de la red. [Obtenga más información sobre la creación de grupos de seguridad](#).

Marzo de 2026

- Se agregaron API públicas para la migración de la red, lo que permite el acceso programático y de socios a las capacidades de migración de la red. Consulte la [referencia de la API de migración de red](#).

Febrero de 2026

- La migración de red ahora permite la ingesta de [archivos de configuración de firewall o Software-Defined redes \(SDN\)](#) sin necesidad de datos de descubrimiento de [RVTools](#). Puede utilizar los archivos de configuración de firewall o SDN de forma independiente o combinarlos con las exportaciones de RVTools.

Enero de 2026

- Se agregó compatibilidad con el etiquetado del [Migration Acceleration Program \(MAP\) y el etiquetado definido por el usuario](#) en los elementos de migración de la red, lo que le permite realizar un seguimiento de los recursos de migración para obtener créditos del MAP y con fines organizativos.

Diciembre de 2025

- Se agregó una nueva [experiencia de migración](#) con un flujo de trabajo rediseñado y una usabilidad mejorada. Para obtener más información, consulte [Acelerar la migración de VMware: la nueva experiencia de AWS Transform](#).

- Se agregó la configuración de [red Landing Zone Accelerator \(LZA\) para la configuración automática de la zona de aterrizaje](#).
- Se agregó soporte para [múltiples AWS cuentas de destino](#) en la ejecución de la migración, lo que le permite migrar cargas de trabajo entre cuentas.
- Se agregó soporte de migración de red para los [formatos de origen Cisco ACI FortiGate, Palo Alto y Modelizelt](#).

Octubre de 2025

- Se amplió la ejecución de la migración a [16 regiones de destino](#) con la incorporación de Asia-Pacífico (Osaka).

Septiembre de 2025

- Se ha añadido compatibilidad con la configuración de licencias en [las oleadas de realojamiento](#), lo que permite especificar las opciones Bring Your Own License (BYOL) o con licencia incluida en cada oleada.
- Se agregó soporte para [Terraform en la migración de redes](#), lo que le permite implementar la infraestructura de red mediante plantillas de Terraform.
- Se agregó soporte para actualizar la configuración de la subred de replicación, lo que elimina el requisito de una VPC predeterminada en la cuenta de destino.

Agosto de 2025

- Se amplió la ejecución de la migración (migración de la red y realojamiento) a [15 regiones de destino](#) con la incorporación de EE. UU. Este (Ohio), Europa (Estocolmo) y Europa (Irlanda).
- Se agregaron [capacidades de rango CIDR flexibles](#) para la migración de la red, lo que le permite personalizar los rangos de direcciones IP durante el despliegue de la red.

Mayo de 2025

- Lanzamiento inicial del servicio [Migraciones \(incluida VMware\)](#), que proporciona capacidades de migración integrales, incluidas la [detección](#), la evaluación, la [planificación de la migración, la migración](#) de la red y el realojamiento de los servidores.

- Se apoyó la ejecución de la migración en 12 [regiones objetivo](#): EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), Canadá (Centro), Sudamérica (São Paulo), Europa (Fráncfort), Europa (Londres), Europa (París), Asia Pacífico (Bombay), Asia Pacífico (Seúl), Asia Pacífico (Tokio), Asia Pacífico (Singapur) y Asia Pacífico (Sídney).

Contenedorización del código fuente

AWS Transform permite cambiar las plataformas de las aplicaciones a contenedores durante la migración a AWS. En este capítulo, se describen las capacidades de inteligencia artificial de AWS Transform para automatizar la contenerización del código fuente. Puede migrar y modernizar en paralelo, lo que reduce el tiempo y la complejidad de pasar de arquitecturas locales a arquitecturas nativas de la nube. Puede almacenar en contenedores el código fuente de GitHub, archivos Bitbucket o .zip GitLab, generar imágenes de Docker, publicarlas en Amazon Elastic Container Registry (Amazon ECR) e implementarlas en Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS). De este modo, la contenedorización forma parte del mismo flujo de trabajo que se utiliza para planificar y ejecutar las migraciones de realojamiento.

Note

La contenedorización del código fuente está diseñada para aplicaciones que aún no están contenerizadas. Requiere acceso al código fuente de la aplicación y no admite la migración de las cargas de trabajo en contenedores existentes. Para migrar los contenedores existentes AWS, utilice métodos de implementación estándar para Amazon Elastic Container Service o Amazon Elastic Kubernetes Service.

Capacidades y características clave

AWS Transform ofrece las siguientes capacidades para contenerizar sus aplicaciones.

- **AI-driven análisis del código fuente:** analiza el código fuente de la aplicación y genera automáticamente artefactos de Docker, incluidos los Dockerfiles y los archivos de configuración relacionados.
- **Creación y publicación de imágenes de contenedores:** compila y prueba imágenes de contenedores mediante compilaciones de AI-driven Docker y las publica en Amazon Elastic Container Registry con un escaneo de vulnerabilidades automatizado.
- **Infraestructura como generación de código:** genera una infraestructura de implementación para Amazon Elastic Kubernetes Service (gráficos de Helm) o Amazon Elastic Container Service (módulos de Terraform), con validación y escaneo de seguridad automatizados.

- Soporte de dependencias privadas: si lo desea, puede configurar AWS CodeArtifact repositorios (Maven, PyPI, npm) e imágenes base privadas de Amazon ECR como fuentes de dependencia para sus compilaciones.
- Implementación iterativa de pruebas y transición: despliega la infraestructura de prueba para la validación y, a continuación, implementa la infraestructura finalizada para la transición a la producción.

Cómo funciona la contenedorización

AWS Transform utiliza un AI-powered agente para guiarlo a través del proceso de contenerización en un flujo de trabajo basado en el chat. AWS Transform coordina tareas especializadas, como el análisis del código fuente, la generación de imágenes de Docker y la creación de infraestructuras. En los puntos clave del flujo de trabajo, debe revisar y aprobar el resultado antes de continuar.

Para acceder a la contenedorización del código fuente, debe crear un trabajo de migración de VMware. Dentro del trabajo, puede ejecutar la contenedorización como un flujo de trabajo independiente o como parte de una migración integral cuando la estrategia de migración de una oleada esté configurada para contenerizar. Para obtener más información sobre la migración a VMware, consulte [Migraciones \(incluida VMware\)](#).

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Un espacio de trabajo de AWS Transform. Para obtener información sobre cómo obtener un espacio de trabajo, consulte [Primeros pasos](#).
- El código fuente de su aplicación está en un repositorio de Git accesible a través AWS CodeConnections de archivos zip o empaquetados como archivos zip para cargarlos. Los archivos individuales no deben superar 1 GB y el tamaño total de todo el código fuente no debe superar los 8 GB.
- (Opcional) Un repositorio de Amazon ECR para publicar imágenes de contenedores. Puede configurar el acceso a Amazon ECR más adelante en el flujo de trabajo, cuando esté listo para publicar.
- Para las implementaciones de Amazon EKS: un clúster de Amazon EKS existente o permisos para crear la infraestructura requerida.

- Para implementaciones de Amazon ECS: permisos para crear clústeres, servicios y recursos relacionados de Amazon ECS mediante Terraform AWS CloudFormation, o. AWS Cloud Development Kit (AWS CDK)

Flujo de trabajo de contenedorización

El flujo de trabajo de contenedorización consta de los siguientes pasos. El agente de AWS Transform lo guía en cada paso de la interfaz de chat.

1. [the section called “Paso 1: Exención de responsabilidad de seguridad”](#)— Revisa y acepta el aviso de seguridad.
2. [the section called “Paso 2: clona el código fuente”](#)— Proporcione el código fuente de su aplicación.
3. [the section called “Paso 3: Contenerizar”](#)— El agente de IA analiza tu código y genera artefactos de Docker.
4. [the section called “Paso 4: Revisa los artefactos”](#)— Revisa los artefactos generados y aprueba los cambios en el código.
5. [the section called “Paso 5: Publica imágenes”](#)— Publica imágenes de contenedores en Amazon ECR.
6. [the section called “Paso 6: Generar IaC”](#)— Genere plantillas de despliegue de Amazon EKS o Amazon ECS.
7. [the section called “Paso 7: Implementar una infraestructura de prueba”](#)— Implemente y valide la infraestructura de pruebas.
8. [the section called “Paso 8: Limpiar la infraestructura de pruebas”](#)— Elimine los recursos de prueba.
9. [the section called “Paso 9: Implemente una infraestructura de transición”](#)— Implemente la infraestructura de producción.

Inicio de un trabajo de contenerización

Para contenerizar sus aplicaciones, primero debe crear un trabajo de migración de VMware en su espacio de trabajo de Transform. AWS Desde el trabajo, puede optar por ejecutar un flujo de trabajo de contenedorización independiente o un flujo de migración integral que incluya la contenedorización.

- Contenerización independiente: almacene su código fuente en contenedores sin realizar una migración completa a VMware. Elija esta opción cuando desee contenedorizar las aplicaciones independientemente de cualquier migración de infraestructura.
- End-to-end migración con contenedorización: ejecute todo el flujo de trabajo de migración de VMware con una estrategia de migración en contenedores asignada a una o más oleadas. El flujo de trabajo de contenedorización se ejecuta como parte de la migración de esas oleadas. Para obtener más información sobre la migración a VMware, consulte [Migraciones \(incluida VMware\)](#)

Para iniciar un trabajo de contenedorización

1. En la página de inicio de tu espacio de trabajo, selecciona Crear un trabajo.
2. Elige la migración a VMware.
3. Elija si desea ejecutar un flujo de trabajo de contenedorización independiente o un flujo de migración integral que incluya la contenedorización.
4. AWS Transform lo guía a través de los pasos del flujo de trabajo, empezando por [the section called “Paso 1: Exención de responsabilidad de seguridad”](#)

Permisos de contenedorización

Durante el flujo de trabajo de contenedorización, AWS Transform le asigna una función de IAM Cuenta de AWS que se utiliza para crear imágenes de contenedores e implementar la infraestructura. Se le pide que revise y apruebe la creación de este rol antes de continuar con el flujo de trabajo.

El rol recibe un nombre `AWSTransformCodeBuildExecutionRole` y se implementa a través de una AWS CloudFormation pila. Incluye las siguientes políticas administradas.

Política base

Proporciona los permisos principales para el flujo de trabajo de contenedorización:

- Amazon S3: lectura y escritura de objetos en `aws-transform-*` cubos
- Amazon ECR: autentique, extraiga imágenes (etiquetadas con `Project: atx-migration`) y envíelas a repositorios etiquetados con `CreatedBy: AWSTransform`
- AWS CodeArtifact — Lea los repositorios etiquetados con `Project: atx-migration`, enumere los repositorios, obtenga tokens de autorización y lea los puntos de enlace de los repositorios.

Estos permisos admiten tanto la resolución de dependencias públicas como las fuentes de dependencia privadas configuradas durante el flujo de trabajo

- Amazon CloudWatch Logs: cree grupos y transmisiones de registros y escriba eventos de registro para los grupos de registros de Amazon ECS
- AWS KMS — Describa y descifre las claves (con el ámbito de Amazon S3 a través del estado de servicio)
- Amazon EC2: creación y administración de interfaces de red para proyectos VPC-enabled
- AWS CodeConnections — Utilice conexiones para acceder a los repositorios de código fuente a través del ARN configurado CodeConnections

Política de redes

Administra los recursos de red para las aplicaciones implementadas:

- Elastic Load Balancing: cree, describa y gestione los balanceadores de carga, los grupos objetivo, los oyentes y las reglas (etiquetados con) `CreatedBy: AWSTransform`
- Route 53: crea y administra zonas alojadas y registros DNS
- AWS Cloud Map: cree y gestione espacios de nombres y servicios para la detección de servicios (etiquetados con) `CreatedBy: AWSTransform`

Política de almacenamiento

Administra los recursos de almacenamiento para las aplicaciones implementadas:

- Amazon S3: cree y gestione buckets, incluidas las políticas de cifrado, control de versiones, ciclo de vida y acceso
- Amazon EFS: cree y gestione sistemas de archivos, monte destinos y puntos de acceso (etiquetados con `CreatedBy: AWSTransform`)
- Amazon EBS: cree y gestione volúmenes e instantáneas (etiquetado con) `CreatedBy: AWSTransform`

AWS KMS policy

Administra las operaciones con claves de cifrado:

- Describa las claves, enumere los alias y lea las políticas de claves
- Cifrar, descifrar y generar claves de datos (sujetas a Amazon Logs CloudWatch , Amazon EFS, Amazon EC2 y Amazon S3 mediante condiciones de servicio)

Política de Amazon ECS

Administra los recursos de Amazon Elastic Container Service para las implementaciones de contenedores:

- Cree y gestione clústeres, servicios y definiciones de tareas (etiquetadas con `CreatedBy: AWSTransform`)
- Registre y anule el registro de las definiciones de tareas, ejecute tareas
- Transferir las funciones de IAM a las tareas y servicios de Amazon ECS
- Lea la información sobre las funciones de IAM y los certificados de ACM
- Describa las VPC, las subredes, los grupos de seguridad y las interfaces de red de Amazon EC2

Política de Amazon EKS

Administra los recursos de Amazon Elastic Kubernetes Service para las implementaciones de Kubernetes:

- Acceda a la API de Kubernetes, describa los clústeres y enumere los complementos
- Transferir funciones de IAM a Amazon EKS

Note

Todos los permisos dependen de usted y. Cuenta de AWS Región de AWS Los recursos creados por AWS Transform se etiquetan con esta etiqueta `CreatedBy: AWSTransform`, y las operaciones de escritura están restringidas a los recursos con esta etiqueta, cuando corresponda.

Paso 1: Revisa el aviso de seguridad

Antes de que comience el flujo de trabajo de contenedorización, AWS Transform presenta un aviso de seguridad que debe revisar y aceptar.

Qué cubre el descargo de responsabilidad

El proceso de contenedorización requiere acceso a Internet para descargar las dependencias de las aplicaciones (como paquetes de registros públicos como npm, PyPI o Maven Central). El aviso de seguridad le informa de que:

- Los entornos de compilación tendrán acceso saliente a Internet para resolver y descargar las dependencias especificadas en la configuración de compilación de la aplicación.
- Eres responsable de revisar las dependencias que requiere tu aplicación y de asegurarte de que cumplen las políticas de seguridad de tu organización.
- Si lo desea, puede configurar fuentes de dependencias privadas (como AWS CodeArtifact repositorios o imágenes base privadas de Amazon ECR) en un paso posterior para evitar la descarga de registros públicos.

Qué necesita

Para revisar y aceptar la exención de responsabilidad de seguridad

1. Lea el aviso de seguridad que presenta Transform. AWS
2. Acepte el descargo de responsabilidad para continuar con el flujo de trabajo de contenedorización.

Tras aceptar el descargo de responsabilidad, AWS Transform pasa al siguiente paso, en el que proporciona el código fuente.

Note

La configuración del conector para AWS CodeConnections Amazon ECR ya no es necesaria por adelantado. AWS Transform le pide que configure el acceso a estos servicios más adelante en el flujo de trabajo, solo cuando sea necesario. Por ejemplo, configura

CodeConnections cuándo decide clonar desde los repositorios de Git y configura el acceso a Amazon ECR cuando está listo para publicar imágenes de contenedores.

Paso 2: clonar el código fuente

En este paso, proporciona el código fuente de la aplicación a AWS Transform. Puedes proporcionar el código fuente de los repositorios de Git o cargando archivos zip.

Opción 1: repositorios de Git

Puedes proporcionar tu código fuente desde los repositorios de Git. Si aún no lo ha configurado AWS CodeConnections, AWS Transform le pedirá que proporcione su CodeConnections ARN en este momento. Dispone de dos formas de especificar sus repositorios:

- Cargue un archivo CSV: prepare un archivo CSV con columnas `repo_name` y `branch`. `repo_name` debe estar en `owner/repo-name` formato. La `branch` column es opcional; déjela vacía para usar la rama predeterminada del repositorio. Ejemplo:

```
repo_name,branch
owner/my-app,main
owner/api-service,develop
owner/another-repo,
```

- Proporciona los detalles del repositorio en el chat: dile a AWS Transform los nombres y las ramas del repositorio directamente en el chat en lugar de subir un CSV.

AWS Transform valida que cada repositorio existe y es accesible a través de tu CodeConnections configuración y, a continuación, clona los repositorios.

Note

Los archivos individuales no deben superar 1 GB y el tamaño total de todos los repositorios no debe superar los 8 GB. AWS Transforma los clones de varios repositorios de forma simultánea para un procesamiento más rápido.

⚠ Important

La opción de clonación de Git no admite aplicaciones que abarquen varios repositorios. Si tu aplicación requiere código fuente de varios repositorios, empaquéalos como un archivo zip y, en su lugar, usa la opción de carga zip.

Opción 2: carga de archivos zip

Si no lo CodeConnections configuró o prefiere cargar su código fuente directamente, puede cargar archivos zip.

Para cargar el código fuente como archivos zip

1. Cuando se le solicite, cargue un archivo zip por aplicación. Puedes arrastrar los archivos al chat o usar el botón de adjuntar archivos.
2. Cada archivo zip debe contener el código fuente de una aplicación.
3. Los archivos individuales no deben superar 1 GB y el tamaño total de todas las cargas no debe superar los 8 GB.

Opcional: configure las dependencias privadas

Si su aplicación depende de paquetes de registros privados, puede configurar las fuentes de dependencia privadas durante este paso. AWS Transform admite los siguientes tipos de dependencias privadas:

- AWS CodeArtifact repositorios: configure los repositorios Maven, PyPI o npm alojados en. AWS CodeArtifact AWS Transform presenta una lista de los repositorios disponibles en tu cuenta para que los selecciones.
- Imágenes base de Amazon ECR privadas: si sus Dockerfiles utilizan imágenes base de un repositorio privado de Amazon ECR, proporcione los detalles del repositorio para que el entorno de compilación pueda extraer estas imágenes.

Cuando configuras las dependencias privadas, AWS Transform te pide que te conectes al lugar donde están alojados estos recursos. Cuenta de AWS Esta configuración de conector solo es necesaria si utiliza dependencias privadas.

Confirmar las preferencias de contenedorización

Una vez que el código fuente esté disponible, AWS Transform le preguntará si tiene instrucciones específicas sobre cómo debe realizarse la contenerización. Si lo desea, puede especificar:

- Si se debe generar un Dockerfile nuevo o reutilizar uno existente.
- Si se debe procesar un servicio específico en un monorepo o todos los servicios.
- Cualquier otra preferencia para el proceso de contenerización.

Los valores predeterminados son:

1. Utilice la imagen base de Amazon Linux 2023 (`public.ecr.aws/amazonlinux/amazonlinux:latest`).
2. Procese todas las aplicaciones del repositorio.
3. Reutilice un Dockerfile existente si está presente, con modificaciones menores si es necesario.

Puede confirmar si desea continuar con los valores predeterminados o proporcionar instrucciones específicas.

Paso 3: Contenedorizar

En este paso, el agente AWS Transform AI analiza el código fuente de la aplicación y genera artefactos de Docker. AWS Transform examina la estructura, las dependencias y los requisitos de tiempo de ejecución de la aplicación para generar los Dockerfiles adecuados y los archivos de configuración relacionados.

¿Qué ocurre durante la contenedorización

El agente de contenerización realiza las siguientes tareas:

1. Análisis del código fuente: AWS Transform examina los archivos del proyecto, las dependencias, la configuración de compilación y los requisitos de tiempo de ejecución de la aplicación. AWS Transform también reemplaza los valores codificados (como las direcciones IP de las bases de datos o los nombres de DNS), identifica las variables de entorno, detecta los volúmenes e intenta redirigir los registros a una salida estándar.
2. Generación de Dockerfile: en función del análisis, AWS Transform genera un Dockerfile adaptado a su aplicación.

3. Creación y prueba de la imagen del contenedor: AWS Transform crea la imagen del contenedor y ejecuta una prueba para comprobar que el Dockerfile produce una imagen funcional. Si la compilación falla, AWS Transform itera en el Dockerfile automáticamente.
4. Análisis de seguridad: AWS Transform escanea los artefactos generados en busca de valores codificados, como credenciales, claves de API u otros datos confidenciales, y señala cualquier hallazgo para su revisión.

Si proporcionaste varios repositorios o un monorepo con varios servicios, procesa cada servicio en paralelo.

Tipos de aplicaciones compatibles

AWS Transform admite la contenerización de los siguientes tipos de aplicaciones:

- .NET 7 y versiones posteriores: contenedorización optimizada para las aplicaciones .NET que se ejecutan en la versión 7 o posterior.
- Aplicaciones generales: contenerización para aplicaciones creadas con cualquier lenguaje o marco, incluidos Java, Python Node.js, Go y otros.
- Aplicaciones no compatibles: no se admiten Windows, Xcode ni ningún entorno de compilación propietario.

Qué necesita

Este paso se ejecuta automáticamente. AWS Transform muestra las actualizaciones de progreso a medida que analiza y contenedoriza cada aplicación. Si AWS Transform encuentra problemas, es posible que le pida aclaraciones o información adicional.

Una vez finalizada la contenedorización, AWS Transform pasa al siguiente paso, en el que se revisan los artefactos generados. Los resultados se guardan en la Tienda de Artefactos.

Paso 4: Revise los artefactos de Docker y los cambios de código

En este paso, revisará los artefactos de Docker y los cambios de código que AWS Transform generó durante la contenerización.

Revisar los cambios de los repositorios de Git

Si has proporcionado el código fuente de los repositorios de Git, AWS Transform confirma los cambios de contenedorización en una nueva rama de cada repositorio. Si tienes varios repositorios, AWS Transform presenta todos los cambios en un lote para su revisión consolidada.

Para revisar y aprobar los cambios

1. Revise los enlaces de diferencias de código que proporciona AWS Transform. Cada diferencia muestra todos los archivos que se agregaron o modificaron, incluidos los Dockerfiles, los archivos de configuración y cualquier cambio en el código fuente.
2. Cuando AWS Transform muestre el cuadro de diálogo de aprobación, apruebe o rechace los cambios. En el caso de varios repositorios, se aprueban todos los cambios en una sola operación por lotes.
3. Si lo apruebas, AWS Transform envía los cambios a las nuevas ramas de tus repositorios.
4. Confirma que estás preparado para continuar con el siguiente paso.

Revisar los cambios de las subidas en formato zip

Si ha cargado el código fuente en forma de archivos zip, AWS Transform proporciona enlaces de descarga para los artefactos en contenedores. Descarga y revisa los artefactos, que incluyen los Dockerfiles generados y cualquier modificación del código fuente.

¿Solicitando cambios?

Si los artefactos generados necesitan modificaciones, puedes enviar comentarios a AWS Transform, reinicia el paso de contenerización con las instrucciones actualizadas y genera nuevos artefactos para que los revise.

Paso 5: Publica imágenes

En este paso, AWS Transform publica las imágenes del contenedor en Amazon Elastic Container Registry. Si aún no ha configurado el acceso a Amazon ECR, AWS Transform le pedirá que proporcione los detalles del repositorio de Amazon ECR en este momento.

¿Qué ocurre durante la publicación

AWS Transform realiza las siguientes tareas para cada imagen del contenedor:

1. Configuración del conector: si aún no ha configurado el acceso a Amazon ECR, AWS Transform presenta un formulario de conector en el que proporciona el ARN del repositorio de Amazon ECR y se conecta al suyo. Cuenta de AWS
2. Solicitud de aprobación: AWS Transform presenta la lista de imágenes que se van a publicar y solicita su aprobación. Puede aprobar o rechazar la operación de publicación.
3. Envío de imágenes: tras la aprobación, AWS Transform publica las imágenes del contenedor en su repositorio de Amazon ECR mediante. Si tiene varios servicios, AWS Transform publica todas las imágenes en una sola operación por lotes.
4. Análisis de vulnerabilidades: Amazon ECR analiza automáticamente las imágenes publicadas en busca de vulnerabilidades conocidas. AWS Transform informa de los resultados del escaneo. Para un análisis más completo, habilite el escaneo mejorado con AWS ECR y la supervisión del AWS GuardDuty tiempo de ejecución.

Note

La publicación de imágenes se ejecuta de forma asíncrona utilizando. Si la sesión se interrumpe durante la publicación, AWS Transform recupera automáticamente la operación cuando se vuelve a conectar.

Qué necesita

- Revise la lista de imágenes que se van a publicar.
- Apruebe o rechace la operación de publicación. Si la rechaza, AWS Transform omitirá la publicación de imágenes y podrá continuar con el siguiente paso sin publicar imágenes.
- Revise los resultados del análisis de vulnerabilidades una vez finalizada la publicación.

Tras la publicación, AWS Transform proporciona los URI de imagen que se utilizan en los pasos de despliegue de la infraestructura.

Paso 6: Generar infraestructura como código

En este paso, AWS Transform genera plantillas de AWS infraestructura para implementar su aplicación containerizada. Puede elegir entre Amazon Elastic Kubernetes Service y Amazon Elastic Container Service como plataforma de destino.

Amazon Elastic Kubernetes Service (Kubernetes)

Si elige Amazon EKS, AWS Transform genera gráficos de Helm con manifiestos de Kubernetes para su aplicación. Las plantillas generadas incluyen:

- Implementaciones y servicios
- Reglas de entrada
- ConfigMaps y recursos SecretProviderClass
- Cuentas de servicio
- Reclamaciones de volumen persistentes (EBS y EFS)
- Registros DNS de Route 53
- Configuraciones de Health Check

Opcional: CloudWatch registro

AWS Transform le pregunta si desea incluir el CloudWatch registro para su implementación de Amazon EKS. Si opta por participar, AWS Transform genera una DaemonSet configuración de Fluent Bit que recopila los registros de los pods y los envía a CloudWatch Logs.

Si eliges el CloudWatch registro, el administrador del clúster debe cumplir los siguientes requisitos previos antes de la implementación:

1. Cree el espacio de `amazon-cloudwatch` nombres en el clúster.
2. Cree un rol de IAM para la cuenta de servicio de Fluent Bit con permisos de escritura en CloudWatch Logs. Se le solicitará el ARN del rol durante la implementación.

Amazon Elastic Container Service (Terraform)

Si elige Amazon ECS, AWS Transform genera módulos de Terraform para implementar su aplicación. Las plantillas generadas incluyen:

- Clúster de ECS
- Servicio ECS con definiciones de tareas
- Application Load Balancer con registro de acceso
- Amazon EFS para almacenamiento persistente

- Zonas alojadas privadas para la detección de servicios
- Configuraciones de Health Check

Validación y escaneo de seguridad automatizados

AWS Transform valida automáticamente las plantillas de infraestructura generadas antes de presentárselas. La validación incluye:

- Para Terraform: `terraform fmt` y `terraform validate` para comprobar la corrección de la sintaxis y la configuración.
- Para Helm: validación de gráficos para verificar que los manifiestos generados estén bien formados.
- Escaneo de seguridad mediante Checkov para identificar posibles errores de configuración de seguridad en el código de infraestructura generado.

AWS Transform informa de cualquier problema de validación y lo resuelve antes de continuar.

Generar IaC sin imágenes publicadas

Puede generar plantillas de infraestructura aunque no haya publicado imágenes de contenedores en el paso anterior. Las plantillas generadas utilizan URI de imágenes de marcador de posición que puede actualizar más adelante con las ubicaciones reales de las imágenes.

Qué necesita

Para generar plantillas de infraestructura

1. Cuando se le solicite, elija la plataforma de destino: Amazon EKS o Amazon ECS.
2. Si eligió Amazon EKS, AWS Transform le preguntará si desea incluir el CloudWatch registro. Responda sí o no.
3. Si se te solicita, proporciona los detalles del punto final del chequeo de estado de tu aplicación (por ejemplo, una `/health` ruta).
4. AWS Transform genera y valida las plantillas de infraestructura. Este paso se ejecuta automáticamente y AWS Transform muestra las actualizaciones de progreso, incluidos los resultados de la validación o del análisis de seguridad.
5. Revise las plantillas generadas cuando AWS Transform las presente.

Paso 7: Implementar una infraestructura de pruebas

En este paso, AWS Transform despliega una infraestructura de pruebas para que pueda validar su aplicación en contenedores antes de la transición a la producción.

¿Qué ocurre durante la implementación de la prueba

AWS Transform implementa las plantillas de infraestructura generadas en el paso anterior en su Cuenta de AWS. Para las implementaciones de Amazon EKS, utiliza Helm. Para las implementaciones de Amazon ECS, utiliza Terraform.

Antes de la implementación, AWS Transform presenta un formulario de valores de infraestructura en el que puede configurar los parámetros de implementación, como los nombres de los recursos, el número de réplicas y los ajustes específicos del entorno. AWS Transform también genera una vista previa de la implementación que muestra los recursos que se crearán, para que pueda revisar los cambios antes de aprobarlos.

Qué necesita

Para implementar y validar la infraestructura de pruebas

1. Complete el formulario de valores de infraestructura con la configuración de implementación. El formulario incluye parámetros como los nombres de los clústeres, los espacios de nombres, el número de réplicas y otros ajustes específicos del entorno.
2. Revise la vista previa de la implementación, que muestra los recursos que se crearán o modificarán.
3. Apruebe el despliegue de la infraestructura cuando AWS Transform lo solicite.
4. Espere a que se complete la implementación. AWS Transform muestra los resultados del despliegue.
5. Pruebe la aplicación implementada para comprobar que se ejecuta correctamente en un contenedor y que la infraestructura cumple sus requisitos.
6. Dígame a AWS Transform si está satisfecho con la implementación o si desea modificar la infraestructura y volver a implementarla.

Iterando en la infraestructura

Si necesita modificar las plantillas de infraestructura, puede cargar las plantillas actualizadas y volver a implementarlas:

1. Dígame a AWS Transform que quiere modificar el IaC.
2. Cargue un archivo zip que contenga las plantillas de infraestructura modificadas.
3. AWS Transform reemplaza las plantillas y realiza una actualización incremental (aplicación de Terraform o mejora de Helm).
4. Revise los resultados de implementación actualizados.

Puede repetir este ciclo hasta que esté satisfecho con la implementación.

Recuperación de sesión

Las implementaciones de infraestructura se ejecutan de forma asíncrona mediante. Si la sesión se interrumpe durante una implementación, AWS Transform recupera automáticamente la operación cuando se vuelve a conectar y muestra los resultados de la implementación.

Paso 8: Limpiar la infraestructura de pruebas

Una vez finalizada la validación, AWS Transform desmonta la infraestructura de pruebas para evitar costes innecesarios.

Qué necesita

Para limpiar la infraestructura de pruebas

1. AWS Transform le informa de que la infraestructura de prueba se destruirá.
2. Apruebe la operación de destrucción cuando AWS Transform la solicite.
3. Espere a que se complete la limpieza. AWS Transform muestra los resultados cuando se han eliminado todos los recursos de la prueba.

Para las implementaciones de Amazon ECS, este paso elimina todos los recursos que se crearon durante la implementación de prueba, incluidos los recursos informáticos, los balanceadores de carga, el almacenamiento y los componentes de red.

En el caso de las implementaciones de Amazon EKS, el alcance de la limpieza depende de la etiqueta del proyecto específico. Solo se eliminan los recursos etiquetados para este flujo de trabajo de contenerización. Otras cargas de trabajo que se ejecutan en el mismo clúster de Amazon EKS no se ven afectadas.

Paso 9: Implementar una infraestructura de transición

En este último paso, AWS Transform despliega la infraestructura finalizada para su uso en producción. La implementación transitoria utiliza las mismas plantillas de infraestructura que validó durante el paso de implementación de prueba.

Qué necesita

Para implementar una infraestructura de transición

1. Complete el formulario de valores de infraestructura con la configuración de implementación de producción. Puede ajustar los parámetros de la implementación de prueba o usar los mismos valores.
2. Revise la vista previa de la implementación que muestra los recursos de producción que se crearán.
3. Apruebe el despliegue de producción cuando AWS Transform lo solicite.
4. Espere a que se complete la implementación. AWS Transform muestra los resultados de la implementación transitoria.
5. Compruebe que la aplicación se ejecute correctamente en el entorno de producción.

Important

Revise las configuraciones de infraestructura generadas con su equipo para asegurarse de que cumplen con los requisitos empresariales, de seguridad y de conformidad de su organización. Si bien AWS Transform ofrece recomendaciones de configuración automatizadas, usted es responsable de validar y ajustar la configuración para que se adapte a sus necesidades antes de continuar con la implementación transitoria.

Recuperación de sesiones

Las implementaciones de producción se ejecutan de forma asíncrona utilizando. Si la sesión se interrumpe durante el despliegue, AWS Transform recupera automáticamente la operación al volver a conectarse y muestra los resultados del despliegue.

Modernización de las aplicaciones de mainframe

AWS Transform está diseñado para acelerar la modernización de las aplicaciones de mainframe antiguas. Organiza el análisis de las bases de código de los mainframes, genera documentación, extrae la lógica empresarial, descompone las estructuras monolíticas, transforma el código heredado y gestiona todo el proceso con la intervención humana (HITL) cuando es necesario. Las capacidades de transformación de AWS Transform para modernizar y migrar las aplicaciones de mainframe le permiten modernizar sus aplicaciones fundamentales de mainframe con mayor rapidez y, al mismo tiempo, preservar la lógica fundamental de la empresa durante todo el proceso de transformación.

Temas

- [Capacidades y características clave](#)
- [High-level tutorial](#)
- [Human in the Loop \(HITL\)](#)
- [Tipos de archivos compatibles para la transformación de aplicaciones de mainframe](#)
- [Regiones y cuotas compatibles para AWS Transform el mainframe](#)
- [High-level descripción general del proceso de modernización del mainframe](#)
- [Transformación de aplicaciones de mainframe](#)
- [Cree e implemente su aplicación modernizada después de la refactorización](#)

Capacidades y características clave

AWS Transform ofrece las siguientes capacidades para la modernización del mainframe:

- Soporta la modernización de aplicaciones de z/OS mainframe escritas en COBOL (Common Business-Oriented Language) y PL/I (Programming Language One) con transacciones asociadas de JCL (Job Control Language), CICS (Customer Information Control System), pantallas BMS (Basic Mapping Support), bases de datos Db2 y archivos de datos VSAM (Virtual Storage Access Method).
- Admite la refactorización de las aplicaciones de mainframe Fujitsu GS21 con PSAM (método de acceso al servicio de presentación), juegos de caracteres japoneses y archivos de datos NDB (base de datos de red).
- Realiza el razonamiento, el análisis, la descomposición, la planificación, la generación de documentación y la refactorización del código basados en objetivos.

- Refactoriza automáticamente las cargas de trabajo del COBOL-based mainframe en aplicaciones Java modernas y optimizadas para la nube.
- Organiza e integra a la perfección las herramientas subyacentes para ejecutar el análisis, la documentación, la descomposición, la planificación y la refactorización del código.
- Le ayuda a configurar entornos de nube para aplicaciones de mainframe modernizadas al proporcionar plantillas de infraestructura como código (IaC) listas para usar.

High-level tutorial

Este es un tutorial de alto nivel sobre AWS Transform para modernizar y migrar aplicaciones de mainframe.

1. Inicie una conversación con AWS Transform e introduzca un objetivo.
2. En función de tu objetivo, AWS Transform te propone un plan de modernización, desglosando el objetivo de alto nivel en pasos intermedios.
3. Según el objetivo que hayas establecido, AWS Transform puede:
 - Evaluar y reimaginar el código base
 - Cree un trabajo personalizado en función del objetivo

Por el camino, es posible que AWS Transform te solicite información para ejecutar las tareas.

Note

Para obtener más información sobre las capacidades de refactorización de AWS Transform for mainframe, consulte [Crear un proyecto](#) en la documentación de refactorización de AWS Transform for mainframe.

Human in the Loop (HITL)

Durante la transformación de las aplicaciones de mainframe, puede supervisar el progreso y el estado de las tareas de transformación a través de la experiencia web AWS Transform.

AWS Transform recopilará información adicional sobre usted en los siguientes escenarios:

- Cuando se necesita información adicional para ejecutar tareas.

- Cuando se requiere la aprobación de artefactos intermedios (por ejemplo, la descomposición de dominios o la planificación de oleadas).
- Cuando surgen problemas que AWS Transform no puede resolver automáticamente.

Tipos de archivos compatibles para la transformación de aplicaciones de mainframe

Los tipos de archivo admitidos z/OS incluyen:

- Artefactos de COBOL y CPY (cuadernos) relacionados
- PL/I archivos fuente
- JCL (Job Control Language) y JCL Procedure (PROC)
- Definición del sistema CICS (CSD)
- BMS (Basic Mapping Support)
- Bases de datos Db2
- VSAM (método de acceso al almacenamiento virtual)
- IMS TM (administrador de transacciones)

Los tipos de archivo compatibles con el Fujitsu GS21 incluyen:

- PSAM (método de acceso al servicio de presentación)
- ADL (lenguaje de definición AIM)
- NDB (base de datos de red)

Para obtener más información sobre el Fujitsu GS21, consulte los siguientes temas en la guía de migración de AWS Transform for mainframe:

- [GS21](#)
- [Captura y reproducción: terminales GS21](#)
- [Unidad central, AS400, Open VMS y GS21](#)

Regiones y cuotas compatibles para AWS Transforme el mainframe

Para obtener una lista de las regiones compatibles, consulte [Regiones compatibles para AWS Transform](#).

Note

Es posible que sus datos se procesen en una región diferente de la región en la que usa AWS Transform. Para obtener información sobre el procesamiento entre regiones, consulte [the section called “Cross-region procesamiento”](#).

Para conocer los límites de cuota, consulte [Cuotas](#).

High-level descripción general del proceso de modernización del mainframe

La modernización de las aplicaciones de mainframe generalmente AWS se logra en cuatro fases: (a) evaluar, (b) movilizar, (c) migrar y modernizar, y (d) operar, optimizar e innovar. Cada una de estas fases se describe con más detalle con los objetivos y las actividades asociadas para respaldar su proceso de modernización.

Fases

- [Fase 1: Evaluar](#)
- [Fase 2: Movilizar](#)
- [Fase 3: Migrar y modernizar](#)
- [Fase 4: Operar, optimizar e innovar](#)

Fase 1: Evaluar

Objetivo: comprender su estado de preparación para la modernización y desarrollar planes de modernización iniciales.

Con AWS Transform, puede evaluar las aplicaciones, la infraestructura y las operaciones de su mainframe para determinar el enfoque de modernización adecuado para sus necesidades empresariales.

 Note

Cada fase contiene una lista de todas las actividades posibles que puede realizar al modernizar su aplicación de mainframe. Puede omitir algunas de las actividades que no se ajusten a su caso de uso o a sus objetivos.

Actividades

- Comienza con una conversación informal sobre la modernización y trabaja en la calificación de las oportunidades reuniendo a las personas adecuadas en la sala
- Determine la calificación de la oportunidad
- Realice una presentación en primera convocatoria con el plan de mapeo de la dependencia de las aplicaciones y la arquitectura de la aplicación
- Determine la ROM (orden de magnitud aproximado) e incluya el costo de infraestructura durante la migración, la mano de obra de migración, los costos de posproducción y la duración del proyecto
- Detección rápida de la cartera:
 - Ejecute una evaluación de la guía de patrones y herramientas
 - Haga un análisis del código fuente
 - Identifique a los candidatos a la prueba de concepto (POC)
- Cree una formación de habilitación técnica:
 - Días de inmersión
 - Talleres con temas generales
- Cree un informe de evaluación de la preparación para la migración (MRA) para grandes proyectos de modernización de mainframes o para nuevos clientes AWS
- Cree una declaración de trabajo para la fase de movilización

Fase 2: Movilizar

Objetivo: sentar las bases y validar el enfoque mediante pruebas de concepto exitosas o modernizaciones piloto.

Con la fase de movilización, puede establecer los marcos, las herramientas y los procesos necesarios para respaldar la modernización del mainframe a escala.

Actividades

- Inicie el plan de modernización con un piloto y el POC identificado:
 - Analice el piloto y configure el código de modernización
 - Cree y pruebe los datos modernizados del piloto
 - Obtenga resultados y revise el programa piloto para crear una solución detallada para una modernización de datos de mayor envergadura
- Para la plataforma:
 - Cree un plan de seguridad, cumplimiento y supervisión
 - Configure entornos de landing zone con una estructura contable y una zona de aterrizaje de AWS mainframe
 - Determine la arquitectura, la infraestructura, las aplicaciones, la integración y mucho más
- Piense en las personas y los procesos:
 - El Centro de Excelencia en la Nube es un buen recurso
 - Modelo de operación
- Cree un análisis integral de la cartera para diferentes escenarios de aplicación:
 - Descubrimiento integral que incluye documentación de alto nivel
 - Plan de descomposición (para todas las aplicaciones)
 - Guía de patrones y herramientas para todas las aplicaciones
 - Elabore un plan inicial de modernización y migración
- Cree una solución detallada teniendo en cuenta el piloto, la plataforma, las personas y los procesos, y un análisis exhaustivo de la cartera
- Determine el modelo de negocio
- Complete con éxito el proyecto piloto con una solución para la declaración de trabajo de la siguiente fase

Fase 3: Migrar y modernizar

Objetivo: completar la modernización y la migración dentro del plazo y el presupuesto planificados.

Durante esta fase, puede migrar y modernizar sus aplicaciones y datos de mainframe a AWS.

Actividades

- Asigne recursos al código de la aplicación lista para la producción
- Revise y analice el diseño utilizando la documentación existente o entrevistando a expertos en la materia (PYMES)
- Defina los escenarios de prueba
- Configure los entornos de modernización con el tiempo de ejecución, las bases de datos y el software de terceros adecuados
- Migre y modernice el código fuente y los datos:
 - Puede modernizar su aplicación de forma iterativa en función de los dominios empresariales del código base de la aplicación
 - Amplíe los entornos de modernización según sea necesario para respaldar sus cargas de trabajo de modernización
- Establezca una canalización CI/CD (integración continua, entrega continua)
- Migre las cargas de trabajo seleccionadas para iniciar su modernización.
- Transfiera los programas de aplicaciones y ajuste la escala del entorno según sea necesario:
 - Puede escalar los entornos hacia arriba o hacia abajo según sus necesidades
 - Modernice los paquetes de trabajo mediante la ejecución de pruebas de integridad del código
 - Vuelva a sincronizarlos con el código fuente según sea necesario
- Realice pruebas exhaustivas y verifique su migración:
 - Recopile los datos de estado iniciales
 - Registre los escenarios de prueba en un mainframe
 - Organice el entorno, la aplicación y los datos
 - Ejecute escenarios de prueba en la nube
 - Compare los resultados de las pruebas de origen y destino
 - Cree canalizaciones automatizadas de ejecución de escenarios de prueba
 - Genere informes y KPI
- Valide sus datos para la configuración de producción
- Valide su progreso de la siguiente manera:
 - Ejecutando pruebas de integración y sistema
 - Realización de pruebas de rendimiento
 - Realizar pruebas de aceptación por parte de los usuarios

- Ejecutando HA/DR pruebas
- Defina un plan de implementación con el propietario de la aplicación y cree un plan para la formación y la transferencia de conocimientos
- Considere la transición y ejecute las transiciones de producción
- Establezca un soporte continuo para las actividades de posproducción, como las operaciones, el monitoreo, la planificación de las capacidades y la garantía de las funciones de la aplicación

Fase 4: Operar, optimizar e innovar

Objetivo: respaldar la excelencia operativa y la mejora continua de las aplicaciones modernizadas.

Tras la modernización, puede optimizar el rendimiento, la seguridad y los costes de sus aplicaciones y, al mismo tiempo, aprovechar los AWS servicios para innovar.

Actividades

- Supervise la aplicación para:
 - Métricas de desempeño
 - Prácticas de seguridad
 - Directrices de cumplimiento
 - Costos
- Detalles de registro
- Gestione las operaciones de la aplicación:
 - Administración de la infraestructura
 - Gestión de transacciones y trabajos
 - Soporte para entornos de ejecución
- Optimización y modernización de aplicaciones
- Desarrollo y mantenimiento de aplicaciones:
 - Codificación: IDE
 - Build
 - Integración
 - Testeo
 - Implementación

Transformación de aplicaciones de mainframe

AWS Transform acelera la transformación de sus aplicaciones de modernización de mainframe. En este tema se describen las capacidades disponibles.

Temas

- [Requisito previo: preparar las entradas del proyecto en S3](#)
- [Colección de artefactos fuente de mainframe](#)
- [Sign-in y crear un trabajo](#)
- [Seguimiento del progreso de la transformación](#)
- [Configure un conector](#)
- [Evalúe y reimagine el plan de trabajo](#)
- [Reimagine el plan de trabajo](#)
- [Plan de trabajo personalizado](#)

Requisito previo: preparar las entradas del proyecto en S3

AWS Transform es capaz de gestionar bases de código de mainframe complejas. Para usar la base de código, asegúrese de tener todos los activos en su ubicación de S3.

Insumos clave del proyecto:

- **Código fuente:** debe cargar los archivos de código fuente de su mainframe a S3. Esto incluye los programas COBOL, los scripts de JCL, los cuadernos y cualquier otro archivo fuente relevante.
- **Archivos de datos:** si tiene archivos VSAM u otros archivos de datos que utilicen sus aplicaciones de mainframe, debe cargarlos en S3.
- **Archivos de configuración:** incluya los archivos de configuración específicos de su entorno de mainframe.

Otras entradas del proyecto

- **Registros del Sistema de Administración del Sistema (SMF):** si corresponde, cargue los registros SMF en una nueva carpeta del bucket S3 donde se almacena el código fuente; estos registros deben estar en formato de archivo.zip.

- **Formato:** para la generación de documentación técnica, puede utilizar un archivo de configuración opcional para generar documentos PDF que se ajusten a los formatos y estándares requeridos, incluidos encabezados, pies de página, logotipos e información personalizada.
- **Glosario:** AWS Transform AWS Transform aprovecha la automatización con la IA generativa para la generación de documentos y la extracción de reglas de negocio. Incluir un archivo CSV de glosario con información sobre abreviaturas y terminologías importantes en el directorio raíz del archivo zip ayudará a mejorar la calidad de la documentación generada.
- **Datos de prueba:** si están disponibles, cargue conjuntos de datos de prueba que puedan usarse para validar la aplicación modernizada. Estos datos deben almacenarse en una nueva carpeta en el depósito de S3 donde se almacena el código fuente.

Los detalles sobre las aportaciones del proyecto se encuentran [aquí](#).

Colección de artefactos fuente de mainframe

En este tema se describe el proceso de recopilación del código fuente del mainframe y los artefactos relacionados para respaldar las iniciativas de modernización del mainframe mediante Transform. AWS La recopilación y preparación adecuadas de los artefactos fuente son fundamentales para el éxito del análisis, la planificación de la migración y la implementación.

Inventario de código fuente

Tipos de código fuente de la aplicación

Se admiten los siguientes tipos de código fuente de aplicaciones:

- Programas COBOL
- Scripts de JCL
- Programas ensambladores
- PL/I programas
- transacciones CICS
- Programas naturales
- Guiones REXX
- Programas Easytrieve
- Cuadernos e incluye
- Bibliotecas Proc

Recursos de bases de datos

Se admiten los siguientes activos de base de datos:

- Scripts DB2, DCLGEN y DDL
- Definiciones de bases de datos IMS (PSB y DBD)
- Definiciones de archivos VSAM
- Esquemas de bases de datos físicas y lógicas
- Procedimientos y activadores de bases de datos

Extensiones de archivos de código fuente

Si no está seguro de la extensión, déjela en blanco o en formato.txt y AWS Transform la clasificará automáticamente.

En la siguiente tabla se enumeran las extensiones de archivo más comunes para los artefactos fuente de mainframe.

Extensiones de archivos de código fuente de mainframe

Language/Type	Extensiones comunes	Description (Descripción)
COBOL	.cbl, .cob, .cobol	Programas fuente de COBOL
JCL	.jcl	Guiones de Job Control Language
Ensamblador	.asm	Programas en lenguaje ensamblador
PL/I	.pl1	PL/I programas de idiomas
Definición de CICS	.csd	Definición del sistema CICS (CSD)
Natural	.nat	Programas naturales
REXX	.rex, .rexx	Secuencias de comandos REXX
Easytrieve	.ezt	Programas de informes Easytrieve
Cuadernos	.cpy	Cuadernos COBOL
BMS	.bms	Basic Mapping Support (BMS)

Language/Type	Extensiones comunes	Description (Descripción)
PL/I cuadernos	.pl1_copy	PL/I cuadernos
Db2 DCLGEN	.dcl	Generador de declaraciones de Db2
Definición de Db2	.sql, .ddl	Definiciones de bases de datos Db2
Definición de IMS	.ims	Conjunto de datos de definición de recursos IMS (IMS Stage 1)
MFS	.mfs	IMS MFS (servicio de formato de mensajes)
PSB	.psb	IMS PSB (bloque de especificaciones del programa)
DBD	.dbd	Definiciones de bases de datos IM
Proceso JCL	.prc, .proc	Bibliotecas de procedimientos JCL
JCL incluye	.inc	Archivos JCL Include
Macros	.mac	Macros de ensamblador
Tarjetas de control	.ctl	Tarjetas de control JCL Utility

Métodos de cobro

Extracción de código fuente

Utilice clientes FTP seguros (WinSCP/FileZilla) para la extracción interactiva del código fuente de las bibliotecas PDS de mainframe.

Extracción de esquemas DB2

El software de cliente DB2 LUW (Linux, UNIX y Windows) incluye la db2look utilidad como parte de su paquete de instalación. La db2look utilidad extrae las sentencias DDL (lenguaje de definición de datos) de una base de datos DB2.

Use el siguiente comando:

```
db2look -d DATABASE_NAME -i userid -w password -a -e -m -l -x -f -createdb -printdbcfg
-o DATABASE_NAME.sql
```

La siguiente lista describe los parámetros:

- -d *DATABASE_NAME*: Especifica el nombre de la base de datos de la que se va a extraer el esquema
- -i *userid*: ID de usuario para la autenticación de la base de datos
- -w *password*: Contraseña para la autenticación de bases de datos
- -a: Extrae información de autorización (concesiones)
- -e: extrae todos los objetos de la base de datos (tablas, vistas, índices, etc.)
- -m: Extrae estadísticas y características físicas
- -l: Extrae los comentarios de tablas y columnas
- -x: Los extractos explican las tablas
- -f: Formatea la salida para una mejor legibilidad
- -createdb: Incluye instrucciones de creación de bases de datos
- -printdbcfg: Incluye parámetros de configuración de la base de datos
- -o *DATABASE_NAME*.sql: Especifica el nombre del archivo de salida

Extraer la información del catálogo del mainframe

El comando LISTCAT de IDCAMS es una utilidad para recuperar la información del catálogo sobre los conjuntos de datos del ordenador central. Esto resulta útil durante los proyectos de modernización del mainframe para inventariar los conjuntos de datos y comprender sus 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.CARDDemo.*') ALL
  LISTCAT ENT('SYS1.*') ALL
/*
```

Extraer las definiciones de CICS

La utilidad IBM-provided DFHCSDUP puede extraer las definiciones de recursos del CICS del archivo de definición del sistema (CSD) del CICS.

Utilice el siguiente JCL para descargar las definiciones existentes del 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
/*
```

Extraer definiciones de IMS

Para extraer las definiciones de IMS, puede generar el archivo de transacciones de IMS mediante la utilidad DFSURDD0. Esta utilidad crea macrosentencias de fase 1 que puede utilizar con fines de migración. Actualmente, solo se admite IMS Stage 1.

Utilice el siguiente JCL para extraer las definiciones de 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
/*

```

Extraer información CA-7 del planificador

CA-7 La información del cronograma de trabajo se incluye en los informes de LJOB. Utilice la utilidad LJOB con el LIST=NODD parámetro para generar los informes en el ordenador central. Los informes deben tener una .ca7 extensión. Cada informe debe tener los caracteres de control de transporte ANSI en la columna 1. Puede crear un informe con los caracteres de control de transporte en la columna 1 especificando DCB=RECFM=FBA (o FA) en el JCL utilizado para ejecutar la utilidad LJOB.

Por ejemplo: LJOB, JOB=ZBN*, LIST=ALL

Para obtener más información, consulte la documentación de [Broadcom](#).

Extracción de datos SMF

Los registros del Sistema de Administración de Sistemas (SMF) proporcionan métricas de actividad utilizadas por AWS Transform para analizar el uso de los trabajos por lotes y las transacciones CICS. Se admiten los siguientes tipos de registros SMF: 14, 15, 30 (subtipo 5), 64, 102, 110 (subtipo 1 con clases de datos 1, 3 y 4).

Requisitos de formato para los registros SMF:

- Debe incluir los tipos de registro 30 y 110 (como mínimo)
- Debe estar en formato EBCDIC binario sin procesar con bytes RDW (Record Descriptor Word) incluidos
- Debe proporcionarse como uno de los siguientes:
 - Un archivo de hasta 600 MB comprimido en formato.zip
 - Un archivo de hasta 5 GB comprimido en formato.tar.gz o .gz

- Debe almacenarse en una carpeta independiente de su código fuente en Amazon S3

Proporcione un mínimo de 13 meses de registros SMF para capturar los ciclos de lotes anuales y los patrones estacionales que podrían pasar desapercibidos en plazos más cortos.

Opción 1: Extraer y ordenar los registros SMF

Utilice el siguiente ejemplo de JCL para extraer y ordenar los 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
/*

```

Personalice los siguientes valores en el JCL anterior:

1. Tarjeta de trabajo: actualice la cuenta, la clase y la clase de mensajes
2. DUMPIN: Apunte a sus conjuntos de datos SMF
3. DUMPOUT: especifique el nombre y el HLQ del conjunto de datos de salida
4. TIPO: Seleccione los tipos de registro (14, 15, 30, 110 u otros)
5. FECHA: Formato yyyy/ddd (por ejemplo 2026/055,2026/056)
6. ESPACIO: se ajusta en función del volumen de datos esperado
7. Elimine el paso SORT si no es necesario

Opción 2: Extraer datos SMF con DFSORT

Puede usar DFSORT para consolidar y reportar datos históricos de SMF. Esto resulta útil si almacena sus registros SMF en un GDG por día o por semana. El siguiente trabajo utiliza DFSORT para consolidar los registros SMF del archivo SORTIN y filtrarlos en función de los registros especificados en el parámetro 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 descargar los datos y conservar los datos RDW, puede utilizar un servidor FTP para recibir el archivo extraído. Asegúrese de que los datos se transfieran en formato binario y de que se utilice la opción RDW para que el RDW se incluya en la transferencia de datos. El siguiente trabajo muestra un ejemplo de trabajo de FTP para transferir este archivo.

```
//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
```

Cargando el informe SCRT

También puedes cargar un Sub-Capacity informe de la herramienta de informes (SCRT) en Transform. AWS

Carga del inventario de la aplicación

Una vez que hayas recolectado todos los artefactos, sigue estos pasos:

1. Organice los archivos en subcarpetas por tipo de artefacto (por ejemplo, /cobol, /jcl, /copybooks, /db2, /ims, /cics, /ca7).
2. Comprima la carpeta de nivel superior en un único archivo.zip.
3. Cargue el archivo.zip en el bucket de Amazon S3 conectado a su espacio de trabajo de AWS Transform.

Note

Los registros SMF deben colocarse en una carpeta independiente del código fuente dentro del bucket de Amazon S3 y deben estar en formato.tar.gz o.gz.

Para obtener instrucciones detalladas sobre cómo conectar su bucket de Amazon S3 a AWS Transform, consulte [the section called “Configure un conector”](#).

Sign-in y crear un trabajo

Para iniciar sesión en la experiencia web de AWS Transform, siga todas las instrucciones de la [Introducción al AWS Transformar](#) sección de la documentación.

Para crear e iniciar un trabajo: siga los pasos que se indican en [Comience su proyecto](#).

Crear espacio de trabajo: nombre y describa el espacio de trabajo en el que se almacenarán los trabajos, los colaboradores y los artefactos asociados.

Crear trabajo: cree un trabajo seleccionando uno de los planes de trabajo preconfigurados, o personalice el plan de trabajo en función de su objetivo seleccionándolo de la lista de capacidades compatibles.

Important

AWS Transform rechazará tus operaciones si no tienes los permisos adecuados. Por ejemplo, un colaborador no puede cancelar una tarea de transformación de aplicaciones de mainframe ni eliminar una tarea. Solo un administrador puede realizar estas funciones.

Al crear un trabajo, puede seleccionar una de las capacidades que se indican a continuación, pero el paso inicial siempre es obligatorio, ya que es donde se encuentra el código fuente del proyecto. En el primer trabajo que se configure en un espacio de trabajo, tendrá que configurar un conector para su bucket de Amazon S3.

Seguimiento del progreso de la transformación

Puede realizar un seguimiento del progreso de la transformación a lo largo del proceso de dos maneras:

- **Registro de trabajo:** proporciona un registro detallado de las acciones que lleva a cabo AWS Transform, junto con las solicitudes de participación humana y sus respuestas a esas solicitudes.
- **Panel de control:** proporciona un resumen de alto nivel de la transformación de las aplicaciones de mainframe. Muestra métricas sobre el número de trabajos transformados, la transformación aplicada y el tiempo estimado para completar la transformación de las aplicaciones de mainframe. También puede ver los detalles de cada paso, incluidas las líneas de código por tipo de archivo, la documentación generada por cada tipo de archivo, el código descompuesto y el plan de migración.

Configure un conector

AWS Transform utiliza un conector para acceder a los recursos de su cuenta necesarios para las funciones de modernización del mainframe. El conector se configura automáticamente con la primera tarea que se ejecuta en el espacio de trabajo. Según el plan de trabajo que elija, AWS Transform le guiará para crear su conector.

Reimagine el conector para mainframe

El conector para reimaginar el mainframe es para tareas que ejecutan flujos de trabajo de evaluación y reinversión. Utiliza un bucket de S3 para acceder a los recursos de transformación y almacenarlos, así como un clúster de Amazon Neptune para almacenar los artefactos extraídos. El clúster de Neptune sirve como gráfico de conocimiento unificado que almacena todos los artefactos extraídos sobre su trabajo, y el gráfico de conocimiento responde a todas las preguntas de la interfaz de chat de AWS Transform.

Implemente el clúster de Amazon Neptune en una VPC donde AWS Transform pueda crear interfaces de red elásticas (ENI). Estas son las conexiones de red que permiten a AWS Transform comunicarse de forma segura con Neptune en su VPC para cargar datos y consultar su gráfico de conocimiento.

AWS CloudFormation

Le recomendamos que utilice la siguiente CloudFormation plantilla para crear los recursos necesarios para el conector reimagine de su mainframe. Use el mismo depósito de S3 que planea usar para el conector al ejecutar la CloudFormation plantilla. Para obtener más información sobre el uso de CloudFormation plantillas, consulte [Trabajar con plantillas](#).

Para descargar la CloudFormation plantilla, selecciona [neptune-kg-setup.yaml](#).

La plantilla acepta los siguientes parámetros:

- **BucketName:** obligatorio. Nombre del bucket S3 para el acceso al cargador masivo Neptune. Debe usar el mismo depósito de S3 que planea usar en su conector AWS Transform.
- **KmsKeyId:** opcional. Clave KMS para el cifrado de Neptune. Acepta el identificador de clave, el ARN, el nombre de alias o el ARN del alias. Si se omite, toma como valor predeterminado la clave AWS administrada.

Proporcione los siguientes detalles al configurar el conector:

- ARN del bucket de S3
- Cúmulo de Neptune ARN
- ID de recurso del clúster de Neptune
- ID de subred de la aplicación
- ID del grupo de seguridad de la aplicación
- Rol de cargador masivo Neptune S3 (ARN)

Important

La pestaña Salidas de la CloudFormation plantilla incluye los detalles que debe proporcionar a AWS Transform al configurar el conector.

Configuración personalizada

Si prefiere usar una VPC existente u otras herramientas para crear la infraestructura requerida, su entorno debe cumplir los siguientes requisitos:

Cúmulo de Neptune

- Amazon Neptune Serverless con motor versión 1.4.5.1 o posterior
 - Autenticación de IAM habilitada
 - Encriptación de almacenamiento habilitada (clave AWS administrada o clave KMS administrada por el cliente)
- Configuración de escalado sin servidor (se recomienda: de 1 a 128 NCUs)
- (Recomendado) Lea la réplica en una segunda zona de disponibilidad para obtener una alta disponibilidad y un rendimiento de lectura mejorado

Red

- Una VPC con compatibilidad con DNS y nombres de host DNS habilitados
- Al menos dos subredes en zonas de disponibilidad independientes. AWS Transform crea ENI en estas subredes para acceder al clúster de Neptune, que puede residir en las mismas subredes o en subredes dedicadas. Ajuste el tamaño de las subredes a /20 para adaptarse a los ENI de aplicaciones y endpoints de la VPC.
- Conectividad de red desde las subredes a los siguientes AWS servicios a través de los puntos finales AWS PrivateLink de la interfaz de VPC ():
 - AWS API de Transform Agents: coordina las tareas de modernización del mainframe
 - Amazon Bedrock Runtime: invoca modelos básicos para el análisis y el razonamiento
 - Amazon Relational Database Service (Amazon RDS): administración de clústeres de Neptune
 - Amazon Elastic Compute Cloud (Amazon EC2): administración de ENI
 - Amazon CloudWatch : métricas para la observabilidad de las AWS transformaciones
- Un punto final de puerta de enlace S3 adjunto a las tablas de rutas asociadas a sus subredes. AWS Transform usa este punto final para cargar datos del depósito S3 al clúster de Neptune.

Grupos de seguridad

Los grupos de seguridad están conectados a los ENI, no a las subredes. Incluso cuando AWS Transform ENI y Neptune residen en la misma subred, grupos de seguridad independientes controlan el acceso entre ellos.

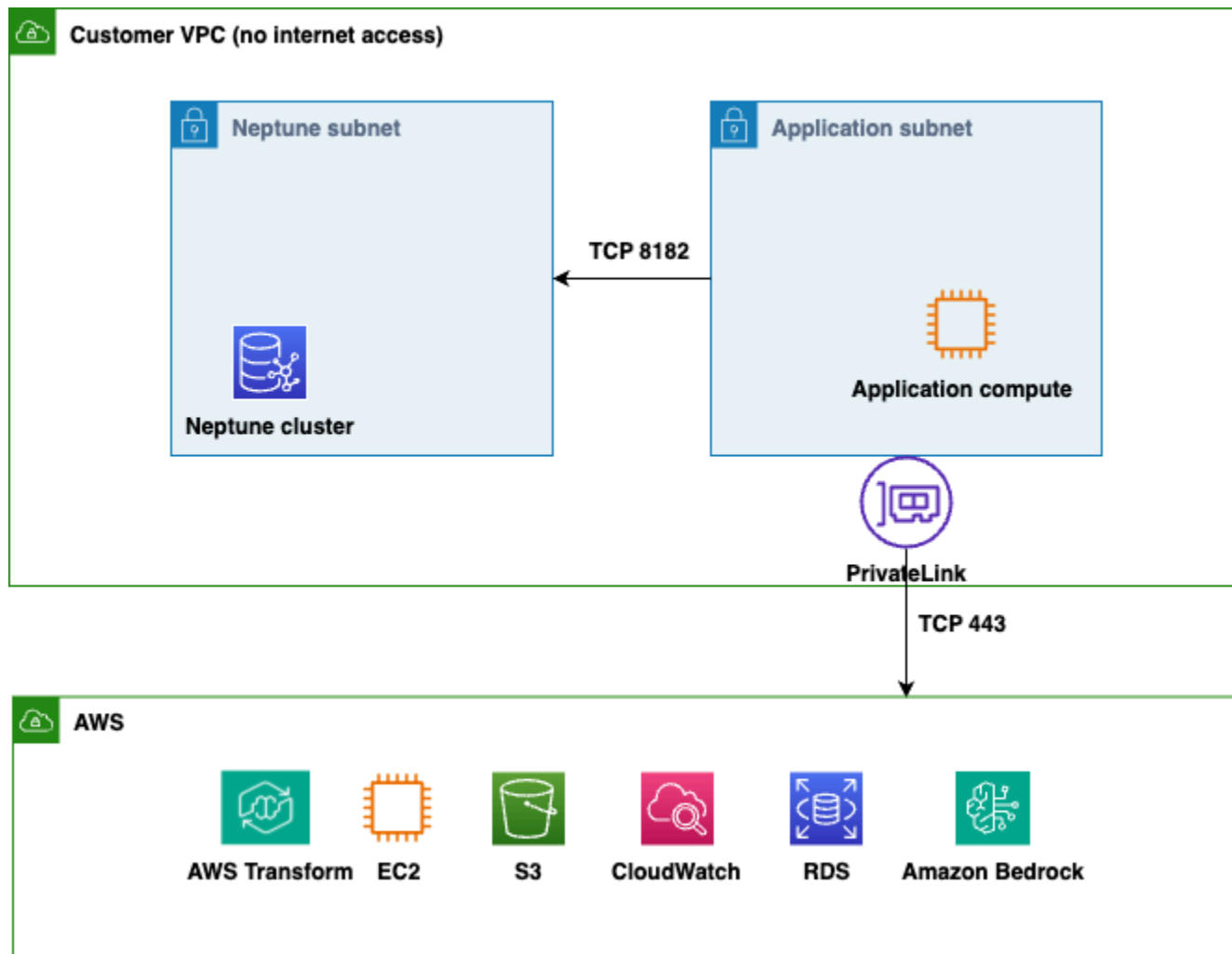
- Un grupo de seguridad (adjunto a los ENI creados por AWS Transform) que permite:
 - TCP 8182 saliente al grupo de seguridad Neptune

- TCP 443 saliente para llegar a los puntos finales de la VPC
- Un grupo de seguridad (adjunto al clúster de Neptune) que permite:
 - TCP 8182 entrante desde el grupo de seguridad de la aplicación
- Un grupo de seguridad de punto final de la VPC (adjunto a los ENI del punto final de la interfaz) que permite:
 - TCP 443 entrante desde el grupo de seguridad de la aplicación

IAM

- Un rol de IAM con una política de confianza para `rds.amazonaws.com` con `s3:GetObjects`, `s3:ListBucket`, y `s3:GetBucketLocation` en su bucket de S3
- Esta función debe estar asociada al cúmulo de Neptune para cargar de forma masiva datos de gráficos de conocimiento

El siguiente diagrama muestra la arquitectura recomendada.



Conector S3

Para los trabajos con un plan personalizado, AWS Transform puede usar un conector S3. El conector S3 utiliza un depósito S3 para acceder a los recursos de transformación y almacenarlos, y un depósito vectorial S3 para la salida indexada.

Important

Los datos se almacenan y se conservan en el almacén de artefactos AWS Transform de su espacio de trabajo y solo se utilizan para ejecutar el trabajo.

Configuración opcional del depósito vectorial de S3.

En las regiones en las que estén disponibles los cubos vectoriales de S3, AWS Transform almacenará las codificaciones vectoriales de los resultados de los trabajos que se puedan buscar en este grupo vectorial de S3 de su cuenta para ofrecer una experiencia de búsqueda y chat basada en la IA. Los datos no se utilizan fuera de este trabajo ni se utilizan para entrenar modelos. Para habilitar esto, debe crear y proporcionar un bucket vectorial S3. AWS Transform crea y adjunta automáticamente un rol con los permisos necesarios para escribir en este bucket.

Permisos CORS del bucket S3

Una vez configurado el conector, añada la siguiente política CORS a su bucket de S3 para poder ver y comparar los artefactos directamente en la consola AWS Transform. Si esta política no está configurada correctamente, es posible que no pueda utilizar las funcionalidades de visualización integrada o comparación de archivos de 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
  }
]
```

Evalúe y reimagine el plan de trabajo

El plan de trabajo de evaluación y reinención es un flujo de trabajo predefinido para modernizar las aplicaciones de mainframe. Lo guía a través de dos fases: evaluar su base de código para identificar

las funciones empresariales y reimaginar las funciones que seleccione. En su lugar, para elegir capacidades individuales, utilice el plan de trabajo personalizado.

Evaluación

Los procesos de modernización de los mainframes suelen comenzar con la evaluación del código base para identificar el contenido y comprender las relaciones y dependencias. Tras esta evaluación, puede empezar a descomponer y seleccionar partes del código fuente para modernizarlas. Los límites de la descomposición se determinan en función de las funciones empresariales.

El catálogo de funciones empresariales descompone la base de código en funciones empresariales discretas, que se basan en rutas de datos deterministas que mapean cada función empresarial de principio a fin. Una ruta de datos es la ruta que siguen los datos, desde un desencadenante empresarial hasta la escritura final en el código del mainframe. En lugar de limitar el análisis a un único punto de entrada, el sistema abarca los trabajos por lotes, las transacciones CICS y sus almacenes de datos compartidos para identificar unidades coherentes de trabajo empresarial.

Una función empresarial es un conjunto de tareas que comienza con un desencadenante empresarial y termina con un resultado empresarial mensurable. AWS Transform proporciona un catálogo de funciones empresariales sobre las que puede actuar una línea de negocio, lo que permite tomar decisiones informadas sobre qué modernizar primero.

Ventajas de evaluar su base de código para modernizarla mediante funciones empresariales:

- Full-estate visibilidad: comprenda cómo sus trabajos por lotes, las transacciones en línea y los almacenes de datos se conectan para crear funciones importantes para su empresa.
- Límites aplicables: cada función empresarial identificada es una unidad autónoma que las partes interesadas de su línea de negocio pueden revisar y priorizar para las iniciativas de modernización.
- Coherencia entre el código y la especificación: para generar sus especificaciones se utilizan los mismos bloques de código que definen una función empresarial, sin necesidad de una capa de traducción ni de conciliación.
- Reducción del tiempo de descubrimiento: la detección automatizada reemplaza meses de entrevistas manuales con conocimientos tribales por análisis sistemáticos y repetibles.

Los resultados de la evaluación se proporcionan a través del chat

Los resultados de la evaluación proporcionados a través del chat incluyen una lista de funciones empresariales, incluida la cantidad de rutas de datos, el alcance de cada función en términos de transacciones por lotes y CICS, y una descripción de la empresa. Se le proporciona un enlace a los

artefactos generados en el bucket de Amazon S3 y también puede acceder a ellos a través del chat. Se proporcionan dos artefactos: los detalles de la función empresarial y el resumen de la función empresarial.

- Resumen de las funciones empresariales: proporciona una lista de las funciones empresariales y una descripción en lenguaje natural de las funciones que desempeñan los elementos del código.
- Detalles de las funciones empresariales: proporciona un gráfico interactivo que describe las relaciones entre el código fuente.

Para interactuar con el gráfico, seleccione un elemento para mostrar detalles adicionales sobre él o abra un elemento para consultar sus detalles. En cada página, hay un resumen de todos los elementos de ese nivel y una interfaz gráfica con la que interactuar y obtener más información sobre cada componente, que incluye lo siguiente:

- Función empresarial: describe qué funciones empresariales están conectadas entre sí y proporciona una visión general de cada función empresarial. Al seleccionar una función empresarial, se proporciona la siguiente información:
 - Número de rutas de datos
 - Número de líneas de código
 - Descripción de la empresa: descripción general de la función empresarial que describe, en lenguaje natural, las funciones que desempeñan los elementos del código.
 - Interfaces: detalla cómo se relacionan los elementos de datos de la función empresarial (por ejemplo, intercambiar o escribir).
- Detalles de la función empresarial: describe las conexiones entre las rutas de datos dentro de una sola función empresarial, lo que le permite profundizar en la composición de la función empresarial. Al seleccionar un elemento, verá cómo ese elemento se conecta con la función empresarial, junto con los siguientes detalles:
 - Almacén de datos: redactores y lectores del almacén de datos.
 - Otros elementos: una descripción general de la ruta de datos relacionada que describe, en lenguaje natural, las acciones y los resultados gestionados dentro de la ruta de datos, una lista de programas y lectores y redactores.
- Rutas de datos: describe los detalles de una ruta de datos y cómo se relacionan entre sí los elementos de la ruta de datos.
 - Descripción: una descripción general de la ruta de datos que describe, en lenguaje natural, las acciones y los resultados gestionados dentro de la ruta de datos.

- Contenido de la ruta de datos:
 - Punto de entrada
 - Lecturas
 - Escrituras
 - Programas

A través del chat, puede consultar los resultados para comprender los elementos que contiene cada función empresarial y explorar los límites a través del gráfico de funciones empresariales.

Una vez que haya identificado los límites de su modernización, el chat le pedirá que seleccione las funciones empresariales que desea reimaginar. Puede seleccionar una sola función empresarial o varias funciones empresariales. AWS Transform envía los límites seleccionados y los resultados de evaluación necesarios al flujo de rediseño para continuar con el proceso de modernización.

Después de completar su primera modernización, puede usar el chat para seleccionar un conjunto adicional de funciones empresariales para modernizarlas.

Reimagine

En la fase de rediseño, puede seleccionar una o todas las funciones empresariales que la evaluación identificó y prepararlas para la modernización. Esto desencadena la extracción de la lógica empresarial, seguida de la generación de requisitos para las funciones empresariales seleccionadas. Los requisitos generados son la base principal de la ingeniería avanzada, ya que traducen la comprensión de los sistemas heredados en una especificación precisa de lo que debe ofrecer la aplicación modernizada.

Extraiga la lógica empresarial

Tras seleccionar una o más funciones empresariales, AWS Transform comienza a generar la lógica empresarial para las funciones empresariales seleccionadas. Una vez finalizada la extracción, AWS Transform almacena los resultados en un bucket de Amazon S3 en formato JSON para su uso posterior. Puede supervisar el progreso de la extracción y revisar cualquier problema directamente en la consola de AWS Transform.

Para revisar los resultados de la extracción de lógica empresarial

1. En el panel de navegación izquierdo, elija el paso Extraer la lógica empresarial para ampliarlo.
2. Vea lo siguiente en los detalles del paso:

- Enlace al bucket de S3: la ubicación donde se almacenan los resultados de la lógica empresarial extraídos en formato JSON.
- Problemas: una lista de los problemas encontrados durante el proceso de extracción de la lógica empresarial.

Si algún archivo tuvo problemas durante la extracción, se muestran los siguientes detalles de cada archivo afectado:

- Nombre de archivo: el nombre del archivo que ha detectado un problema.
- Tipo de archivo: el tipo de archivo (por ejemplo, COBOL o JCL).
- Ruta del archivo: la ubicación del archivo en la aplicación.
- Estado: el estado actual de la extracción del archivo.
- Detalles: descripción del problema detectado.

Note

Una vez finalizado el paso de extracción, AWS Transform comienza a generar requisitos automáticamente. No se le solicitará ninguna entrada adicional antes de que comience este proceso.

Genere requisitos

Una vez finalizada la extracción de la lógica empresarial, el agente de generación de requisitos consume los artefactos extraídos (análisis de código, análisis de datos, reglas empresariales) y genera los requisitos de modernización. Estos requisitos son especificaciones funcionales formales que son independientes de la tecnología e incluyen criterios de aceptación comprobables. AWS Transform produce un `requirements.md` archivo para cada función empresarial que seleccione y almacena el resultado en un bucket de Amazon S3. Para ver la ubicación de Amazon S3 de la salida, elija el paso Generar requisitos.

Cada `requirements.md` archivo está organizado en las siguientes partes:

- Título: nombra la función empresarial y el flujo de trabajo que representa.

- Condiciones previas globales: condiciones que deben mantenerse vigentes en todo el flujo de trabajo antes y durante el procesamiento. Los valores configurables aparecen como marcadores de posición de los parámetros.
- Secciones de flujo de trabajo numeradas: cada sección representa una etapa discreta de la función empresarial. Cada sección contiene lo siguiente:
 - Una historia de usuario que establece el objetivo como rol, la acción que ese rol quiere realizar y el resultado resultante.
 - Una lista de requisitos en formato EARS (Easy Approach to Requirements Syntax), cada uno con un identificador único.

Note

Al seleccionar un segundo conjunto de funciones empresariales, se reinicia el paso de rediseño de las funciones recién seleccionadas. A continuación, la consola solo muestra los resultados de la nueva selección, por lo que ya no se muestran los problemas con las reglas empresariales de sus funciones empresariales anteriores ni los enlaces de Amazon S3 que almacenan los resultados para la lógica empresarial y los requisitos. Los resultados anteriores no se pierden. Puedes seguir accediendo a ellos desde la pestaña Artefactos o en tu bucket de Amazon S3.

Trazabilidad entre los artefactos de transformación

AWS Transform mantiene la trazabilidad entre los artefactos que genera a lo largo del flujo de trabajo de evaluación y reinversión. La trazabilidad le permite rastrear cada requisito hasta las reglas empresariales extraídas o directamente hasta el código fuente original que generó el requisito.

Puede ver todos los detalles de trazabilidad de cada función empresarial mediante el `traceability.yaml` archivo. Describe cómo cada regla empresarial se ajusta a un requisito.

Para una trazabilidad interactiva, puede utilizar el complemento IDE en los editores compatibles con VS Code y Open VSX. Para obtener más información, consulte Herramientas para [desarrolladores](#).

Reimagine el plan de trabajo

En el caso de las aplicaciones que tenga previsto modernizar y que estén listas para reinventarse, puede ejecutar un trabajo de rediseño independiente. El trabajo analiza el código y los datos, extrae

la lógica empresarial, identifica los dominios empresariales y genera los requisitos de modernización para cada dominio empresarial.

Plan de trabajo personalizado

Un plan de trabajo personalizado le permite crear su propio flujo de trabajo de modernización seleccionando las capacidades que desea ejecutar. Le brinda un control total sobre las capacidades que se incluyen. Elija entre las siguientes capacidades en función de su objetivo de modernización. Algunas capacidades dependen de que otras se ejecuten primero. Por ejemplo, el análisis de código es necesario para la mayoría de las demás capacidades.

Analice el código

Después de compartir la ruta del bucket de Amazon S3 con AWS Transform, esta analizará el código de cada archivo con detalles como el nombre del archivo, el tipo de archivo, las líneas de código y sus rutas.

Note

Puede descargar los resultados del código de análisis a través de la pestaña de artefactos a nivel de trabajo o espacio de trabajo. A nivel de trabajo, vaya a la opción «Artefactos» en el menú de navegación de la izquierda y abra la carpeta de «resultados», o a nivel de espacio de trabajo, busque el nombre del trabajo y abra la carpeta de «resultados». Se descargará un archivo zip que contiene el archivo de clasificación para el flujo de trabajo de clasificación manual, la lista de activos, el archivo JSON de dependencias y la lista de archivos faltantes.

En el plan de trabajo, selecciona Analizar código en el panel de navegación izquierdo para ver los resultados. Puede ver los resultados del análisis de código de varias maneras:

- Vista de lista: todos los archivos del bucket de Amazon S3 que desea transformar para un mainframe
- Vista de tipo de archivo: se muestran todos los archivos del bucket de Amazon S3 por tipo de archivo. Para ver una lista de los tipos de archivos compatibles, consulte [Archivos compatibles](#).
- Vista de carpetas: todos los archivos del bucket de Amazon S3 se muestran en la estructura de carpetas.

En los resultados de los archivos, AWS Transform proporciona la siguiente información en función de la vista de archivos que elija:

- Name
- Tipo de archivo
- Total de líneas de código
- Ruta de archivo
- Líneas de comentarios
- Líneas vacías
- Líneas de código efectivas
- Cantidad de archivos
- Complejidad ciclomática: la complejidad ciclomática representa el número de rutas linealmente independientes que atraviesan el código fuente de un programa. AWS La transformación mostrará una complejidad ciclomática para cada uno de los archivos.

Archivos faltantes: faltan archivos en el análisis del código de modernización del mainframe. Lo ideal sería añadir estos archivos como parte de la entrada de origen en el bucket de Amazon S3 y volver a ejecutar el paso de análisis para obtener resultados mejores y coherentes.

Nombre idéntico: AWS Transform le proporciona una lista de archivos que comparten el mismo nombre y, posiblemente, las mismas características (por ejemplo, el número de líneas de código). No podrá comparar la diferencia entre el contenido de dos archivos a la vez.

Identificadores duplicados: con el programa Cobol, el campo ID del programa sirve como identificador único del archivo. Este identificador debe ser único porque se utiliza para llamar al programa en todo el proyecto. Sin embargo, algunos proyectos pueden tener archivos COBOL con nombres diferentes pero con el mismo ID de programa. Obtener la lista de esos archivos durante la evaluación puede ayudar a comprender las dependencias entre todos los programas.

 Note

Esto es específico del código y los archivos de COBOL.

Si tiene programas con ID duplicados, se sugiere cambiar los ID de programa de estos archivos para que tengan un identificador único para cada uno de ellos en el código COBOL. A continuación, puede volver a ejecutar su trabajo para obtener resultados de análisis de código más precisos y completos.

Al resolver los ID de programa duplicados, puede:

- Mejorar la claridad y la facilidad de mantenimiento del código
- Reduzca los posibles conflictos en las llamadas al programa
- Mejore la precisión del mapeo de dependencias
- Simplifique los esfuerzos de modernización del futuro

Problemas con la base de código: posibles problemas detectados en la base de código que debe resolver antes de continuar con el proyecto de modernización. Estos problemas podrían incluir la falta de referencias con las declaraciones asociadas o los enlaces no compatibles en el código.

Actualizar la clasificación: con la reclasificación manual, puedes reclasificar los archivos mediante la función de actualización masiva cargando el archivo JSON con la nueva clasificación.

 Important

Esto solo está disponible para los archivos y. UNKNOWN TXT

Tras la reclasificación, AWS Transform hará lo siguiente:

1. Actualiza los resultados de la clasificación
2. Re-runs análisis de dependencias con los nuevos tipos de archivos
3. Actualiza todos los resultados de los análisis afectados

 Note

Puede reclasificar los archivos solo después de que se complete el ciclo de análisis inicial.

Visor integrado y comparación de archivos

El visor en línea es una función de las funciones de AWS Transform for mainframe que proporciona dos funciones de visualización clave:

- Vista de archivos: vea el contenido de los archivos heredados seleccionados de los trabajos
- Comparación de archivos: compare el contenido de dos archivos antiguos uno al lado del otro

Visualización de archivos de entrada

Para ver los archivos en el Analice el código paso

- En Ver los resultados del análisis de código, seleccione un archivo mediante la casilla de verificación de la lista.

Pulse el botón de acción Ver (activado cuando se selecciona 1 elemento).

El contenido del archivo se renderizará en la pantalla en el componente File View.

Comparación de archivos

Para comparar archivos en el Analice el código paso

1. En Ver los resultados del análisis de código, seleccione dos archivos mediante las casillas de verificación de la lista.
2. Pulse el botón de acción Comparar (activado solo cuando se seleccionan 2 elementos).
3. Los archivos se mostrarán uno al lado del otro en el componente de comparación de archivos.

Note

No puede seleccionar más de dos archivos para compararlos.

Important

Si tiene problemas con el visor integrado o la comparación de archivos, asegúrese de que el bucket de S3 esté configurado correctamente. Para obtener más información sobre la política CORS del bucket de S3, consulte [the section called “Permisos CORS del bucket S3”](#)

Análisis de datos

AWS Transform proporciona análisis de datos para ayudar a comprender el impacto de las relaciones y los elementos de los datos en el proyecto de modernización del mainframe. Los dos resultados que se proporcionan son:

- Linaje de datos: traza el ciclo de vida de los datos mediante el mapeo de las relaciones entre las fuentes de datos, los trabajos y los programas
- Diccionario de datos: sirve como repositorio para documentar los metadatos estructurales de los elementos de datos heredados

Al finalizar el análisis, habrá dos pestañas para cada salida y, a continuación, estarán disponibles varias vistas, que se describen a continuación, tanto para el linaje de datos como para el diccionario.

Note

Cuando solicite un análisis de datos, AWS Transform realiza un análisis de código, que es necesario para realizar el análisis de datos.

Linaje de datos

AWS Transform proporciona múltiples vistas basadas en las relaciones de datos que deben comprenderse en toda la base de código que se está modernizando. Las cuatro vistas de tabla disponibles en el linaje de datos incluyen:

- Conjuntos de datos: esta vista proporciona un análisis de impacto completo, que incluye el seguimiento de las operaciones para ayudar a distinguir entre leer, escribir, actualizar y eliminar
- Tablas de Db2: proporcionan el análisis de impacto relacionado con las tablas de Db2 y las operaciones
- Program-to-data: Identifique qué programas de COBOL hacen referencia a cada conjunto de datos
- JCL-to-data relaciones: identifique qué scripts de JCL hacen referencia a cada conjunto de datos

El resumen proporciona una descripción general de las fuentes de datos y sus relaciones con los programas y los JCL, así como información resumida sobre cómo se aprovechan las fuentes de datos y el total de las operaciones que se encuentran en la base de código.

Diccionario de datos

Comprender los elementos de datos de las fuentes de datos presentes en el código base es el siguiente paso para darse cuenta de la dependencia de las distintas fuentes de datos. El diccionario de datos es un catálogo de datos que proporciona metadatos a nivel de campo con descripciones en el lenguaje empresarial para un mapeo de transformación preciso.

- Estructura de datos de COBOL: proporciona información de campo sobre los cuadernos de texto de COBOL y las referencias INLINE presentes en el código base, incluidas las propiedades de los campos y la definición empresarial
- Tablas de Db2: proporciona las propiedades de las columnas y tablas de las tablas de Db2 presentes en el código base, incluidas las claves principales y externas, la información de esquemas e índices y los tipos de datos

La relación entre el linaje de datos y el diccionario está disponible seleccionando la fuente de datos y, a continuación, utilizando el botón de linaje de datos o diccionario de datos para profundizar en la relación entre la fuente de datos y los elementos de datos. La navegación entre el linaje de datos y el diccionario proporciona una visibilidad integrada de los datos. El linaje de datos proporciona el «qué» (estructura y significado), junto con el «dónde» (uso y relación).

Análisis de métricas de actividad

El análisis de las métricas de actividad le permite analizar los registros de las instalaciones de administración del sistema (SMF) de los tipos 14, 15, 30, 64, 102 y 110. El análisis proporciona información sobre cómo se utilizan los elementos en su aplicación de mainframe. Puede ayudar a retirar el código no utilizado o a tomar decisiones sobre la arquitectura de destino de la aplicación modernizada. Si incluye el análisis de las métricas de actividad en su trabajo, completar primero el paso del análisis del código proporciona resultados SMF más completos, aunque no es obligatorio.

Note

Al negociar el plan de trabajo para la modernización del mainframe, completar primero los pasos de análisis y descomposición del código proporciona resultados más detallados.

Incorpore registros SMF para su análisis

Debe proporcionar la ubicación del registro de SMF en su bucket de Amazon S3 como paso inicial para el análisis de SMF. Proporcione un mínimo de 13 meses de registros para capturar las

incidencias anuales que podrían pasar desapercibidas en períodos de tiempo más cortos. Si bien se recomiendan 13 meses, cualquier período de tiempo con registros SMF detectables produce resultados de análisis.

El extracto SMF debe cumplir los siguientes requisitos de formato:

- Incluya los tipos 14, 15, 30 (subtipo 5), 64, 102 y 110.
- Utilice un archivo binario sin procesar en formato EBCDIC.
- Incluya los bytes RDW.

Proporcione un enlace a los registros SMF de su bucket de Amazon S3, asegurándose de que los registros estén en una carpeta separada de su código fuente. Las opciones de formato incluyen .zip (hasta 600 MB) o .tar.gz (hasta 5 GB) comprimidos. Si proporciona un enlace a una carpeta en la que no se detectan los registros SMF, recibirá un mensaje de error y no se completará ningún análisis.

Resultado del análisis

El resultado del análisis contiene dos componentes, según el tipo de registro: una vista tabular y un resultado en formato.csv (disponible en su bucket de Amazon S3). En AWS Transform, los resultados se muestran para los tipos 30 y 110. A través de los artefactos de su bucket de Amazon S3, puede explorar el análisis de otros tipos de registros. En la interfaz de usuario, el encabezado muestra el intervalo de tiempo de los registros proporcionados para que pueda identificar cualquier fecha clave que falte. Por ejemplo, si sus registros abarcan del 1 de mayo al 31 de octubre, pero excluyen el ajetreado día posterior al Día de Acción de Gracias, verá que faltan registros clave. Las marcas horarias de la aplicación web reflejan la zona horaria del sistema y los registros SMF.

Los artefactos disponibles en Amazon S3 proporcionan análisis para cualquier tipo de registro que se encuentre en los registros proporcionados.

Vista tabular

La vista tabular, disponible solo para las SMF 30 y 110, contiene hasta tres componentes principales para los trabajos por lotes y las transacciones CICS:

- Resumen: proporciona los principales trabajos y transacciones.
- Análisis de job/CICS transacciones por lotes: proporciona un análisis agregado de todos los trabajos y transacciones.
- Comparación del análisis de código (solo por lotes): proporciona datos de comparación cuando el paso de análisis de código se ejecuta antes del análisis SMF.

El resumen del descubrimiento proporciona tres grupos de trabajos y transacciones que le ayudan a identificar rápidamente los elementos para un análisis más profundo.

El análisis de trabajos por lotes y transacciones CICS proporciona un análisis agregado de todos los trabajos y transacciones. Algunas columnas de los resultados del análisis están ocultas de forma predeterminada. Seleccione el icono de engranaje para mostrar campos adicionales.

La clave de transacción genera una agregación de datos única para las transacciones CICS, al combinar cuatro campos en un único valor clave:

- ID de transacción
- Nombre del programa
- SysPlex ID
- SysID

Puede buscar por la clave completa o por cualquier componente de la clave en el resultado del análisis.

La comparación del análisis de código resalta los trabajos que se encuentran en los registros SMF o en el paso de análisis de código, pero que no están presentes en ambos. Esto muestra los trabajos que no se ejecutaron durante el período de tiempo récord de SMF o que no estaban presentes en el paso de análisis del código. Esta salida solo está disponible cuando ejecuta el paso de análisis de código antes del análisis SMF en su trabajo.

Prácticas recomendadas

Para obtener resultados completos para los trabajos por lotes (tipo 30), asegúrese de que el nombre del archivo JCL coincida con el nombre del trabajo para obtener resultados significativos en la comparación del análisis de código.

Genere documentación técnica

Puede generar documentación técnica para las aplicaciones de mainframe que se estén modernizando. Al analizar su código, AWS Transform puede crear automáticamente documentación detallada de sus programas de aplicación, incluidas descripciones de la lógica del programa, los flujos, las integraciones y las dependencias presentes en sus sistemas antiguos. Esta capacidad de documentación ayuda a cerrar la brecha de conocimiento, lo que le permite tomar decisiones informadas a medida que realiza la transición de sus aplicaciones a arquitecturas de nube modernas.

 Note

Cuando solicita la generación de documentación técnica, AWS Transform realiza un análisis del código, incluido el análisis de la dependencia del código, que es necesario para generar la documentación.

Para generar documentación técnica

1. En el panel de navegación izquierdo, en Generar documentación técnica, seleccione **Seleccionar archivos y configurar ajustes**.
2. Seleccione los archivos del bucket de Amazon S3 para los que desee generar documentación y configure los ajustes en la pestaña **Colaboración**.

 Note

Los archivos seleccionados deben tener el mismo tipo de codificación (es decir, todos en el mismo CCSID: UTF8 o ASCII). De lo contrario, la documentación técnica generada podría tener campos o secciones vacíos.

3. Seleccione el nivel de detalle de la documentación:
 - **Resumen:** proporciona información general de alto nivel sobre cada archivo que está dentro del ámbito. Además, ofrece un resumen de una línea de cada archivo.
 - **Especificación funcional detallada:** proporciona detalles completos de cada archivo que está incluido en el ámbito de la transformación de las aplicaciones del mainframe. Algunos detalles incluyen la lógica y el flujo, las dependencias, el procesamiento de entradas y salidas y varios detalles de las transacciones.

 Note

La documentación solo se puede generar para los archivos COBOL y JCL.

4. Elija **Continuar**.
5. Una vez que AWS Transform genere la documentación, revise los resultados de la documentación siguiendo la ruta del bucket de Amazon S3 en la consola, donde se generan y almacenan los resultados.

- Una vez generada la documentación, también puede utilizar el chat de AWS Transform para hacer preguntas sobre la documentación generada y decidir los siguientes pasos.

Añada la información del usuario a la documentación

```
ARTIFACT_ID.zip
### app/
    ### File1.CBL
    ### File2.JCL
    ### subFolder/
        # # File3.CBL
### glossary.csv
### pdf_config.json
### header-logo.png
### footer-logo.png
# ...
```

Se pueden añadir archivos opcionales al archivo zip para mejorar la calidad de la documentación generada y proporcionar una portada en PDF personalizada. Algunos de ellos pueden ser:

- Archivo `glossary.csv`: puede optar por proporcionar y cargar un glosario opcional en el archivo zip del bucket de S3. El glosario está en formato CSV. Este glosario ayuda a crear documentación con descripciones relevantes en línea con el vocabulario del cliente. Un `glossary.csv` archivo de muestra tiene el siguiente aspecto:

```
LOL,Laugh out loud
ASAP,As soon as possible
WIP,Work in progress
SWOT,"Strengths, Weaknesses, Opportunities and Threats"
```

- `pdf_config.json`: puede aprovechar este archivo de configuración opcional para generar documentos PDF que se ajusten a los formatos y estándares de su empresa, incluidos encabezados, pies de página, logotipos e información personalizada. Un ejemplo `pdf_config.json` tiene el siguiente aspecto:

```
{
  "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
}
}

```

- Encabezado:
 - Para el archivo PDF de portada, el texto predeterminado será el nombre del proyecto.
 - Para cada archivo PDF del programa, el texto predeterminado será el nombre del programa.
 - No hay ningún logotipo predeterminado. Si el logotipo del encabezado no está configurado, no se mostrará ningún logotipo.

- El tamaño de la fuente y el tamaño del logotipo se cambiarán dinámicamente en función del número de palabras o del tamaño del archivo del logotipo.
- Sección personalizada:
 - Si la sección personalizada no está configurada, se omitirá del PDF.
 - Se debe poder hacer clic en el enlace.
- Pie de página:
 - No hay texto ni logotipo predeterminados para el pie de página.
 - El número de página se mostrará en el pie de página de forma predeterminada, a menos que se configure explícitamente lo contrario.
 - El tamaño de la fuente y el tamaño del logotipo se cambiarán dinámicamente en función del número de palabras o del tamaño del archivo del logotipo.

Generar documentación (visor en línea)

Puede ver los archivos PDF en el paso de generación de documentación técnica.

Para ver los archivos PDF

1. Navegue a la pestaña Revisar los resultados de la documentación.
2. Localice el PDF en la tabla que enumera los PDF generados.
3. Seleccione el archivo y, a continuación, seleccione Ver o seleccione el elemento de enlace superpuesto al nombre del archivo.

El PDF se abre en AWS Transform, con la opción de expandir la pantalla en la parte superior derecha.

Note

AWS Transform también le permite descargar una versión XML o PDF de la documentación técnica generada.

 Important

Si tiene problemas con el visor integrado de la documentación, asegúrese de que el bucket de S3 esté configurado correctamente. Para obtener más información sobre la política CORS del bucket de S3, consulte. [the section called “Permisos CORS del bucket S3”](#)

Extraiga la lógica empresarial

Puede extraer la lógica empresarial esencial de las aplicaciones de mainframe que se están modernizando. AWS Transform analiza automáticamente el código para identificar y documentar los elementos empresariales fundamentales, incluidos los flujos de procesos detallados y la lógica empresarial integrada en sus aplicaciones. Esta capacidad sirve a múltiples partes interesadas en su proceso de modernización. Los analistas de negocios pueden aprovechar la lógica extraída para crear requisitos empresariales precisos e identificar brechas o inconsistencias en las implementaciones actuales. Los desarrolladores adquieren la capacidad de comprender rápidamente la compleja funcionalidad de los sistemas antiguos sin necesidad de contar con una amplia experiencia en mainframe.

 Note

Cuando solicita la extracción de la lógica empresarial, AWS Transform realiza el análisis del código, incluido el análisis de la dependencia del código y del punto de entrada, que son necesarios para realizar la extracción de la lógica empresarial.

Para extraer la lógica empresarial

1. En el panel de navegación izquierdo, en Extraer lógica empresarial, elija Configurar ajustes.
2. En la pestaña Colaboración, seleccione cómo desea extraer la lógica empresarial:
 - Nivel de aplicación: genera documentos empresariales para todas las funciones empresariales, transacciones, trabajos por lotes y archivos. Esto selecciona todos los archivos de la aplicación.
 - Nivel de archivo: genera documentos comerciales solo para los archivos que seleccione de la tabla de archivos.

 Note

- Para cualquiera de las dos opciones, puede seleccionar Incluir especificaciones funcionales detalladas, de modo que AWS Transform incluya el flujo de control y reglas empresariales exhaustivas para los archivos seleccionados.
- Los archivos seleccionados deben tener el mismo tipo de codificación (es decir, todos en el mismo CCSID: UTF8 o ASCII). De lo contrario, la documentación generada podría tener campos o secciones vacíos.
- La documentación solo se puede generar para los archivos COBOL y JCL.
- A nivel de aplicación, los programas utilizados en las transacciones y los trabajos por lotes de CICS se agrupan, mientras que todos los demás programas se clasifican como sin asignar.

3. Elija Continuar.
4. Una vez que AWS Transform extrae la lógica empresarial, almacena los resultados en un bucket de Amazon S3 en formato JSON para que pueda verlos en línea.

 Note

La cantidad de archivos de reglas de negocio generados puede ser mayor que la selección inicial. Algunos archivos seleccionados pueden activar la extracción de reglas de negocio para incluir archivos dependientes adicionales, que también aparecerán en la tabla de resultados.

Vea la documentación empresarial extraída en línea

Puede ver la lógica empresarial en el paso Extraer la regla empresarial. Para ello,

1. Navegue hasta Revisar los resultados de la extracción de la lógica empresarial.
2. Seleccione el documento que desee ver en la tabla y, a continuación, haga clic en el botón Ver resultados.

La página de documentación empresarial se abre en una nueva pestaña del navegador.

Descomposición

Puede descomponer el código en dominios que tengan en cuenta las dependencias entre los programas y los componentes. Esto ayuda a agrupar adecuadamente los archivos y programas relacionados en el mismo dominio. También ayuda a mantener la integridad de la lógica de la aplicación durante el proceso de descomposición.

Note

Cuando solicitas la descomposición, AWS Transform realiza un análisis del código, incluido el análisis de dependencia del código, que es necesario para llevar a cabo la descomposición. También le recomendamos que extraiga la lógica empresarial antes de la descomposición para obtener mejores resultados.

Para empezar a descomponer la aplicación:

1. Seleccione Descomponer código en el panel de navegación izquierdo.

Note

Se crea automáticamente un dominio, Sin asignar, para todos los archivos no asociados a un dominio. En la navegación inicial, todos los archivos deben estar asociados a Unassigned, a menos que los dominios se hayan propuesto a partir de una extracción de lógica empresarial a nivel de aplicación.

2. Cree un dominio nuevo a través del menú Acciones y, a continuación, seleccione Crear dominio.
3. En Crear dominio, proporciona el nombre del dominio, una descripción opcional y marca algunos archivos como iniciales.
 - Los archivos configurados por CICS (CSD) y los archivos configurados por el programador (SCL) se pueden utilizar para la detección automática de semillas.
 - También puede configurar un dominio solo como componente común. Los archivos de este dominio son comunes a varios dominios.
4. Seleccione Crear.

 Note

Puede crear varios dominios con diferentes archivos como inicialización.

5. Tras confirmar todos los dominios y semillas, selecciona Descomponer.
6. AWS Transform comprobará los archivos de código fuente y, a continuación, los descompondrá en dominios con programas y conjuntos de datos con casos de uso similares y altas dependencias de programación.

AWS Transform le ofrece una vista tabular y gráfica de los dominios descompuestos como dependencias. La vista gráfica tiene tres opciones:

- Vista de dominio: puede ver cómo se relacionan los diferentes dominios entre sí en formato visual.
- Vista de dependencias: permite ver todos los archivos de cada dominio como un gráfico de dependencias complejo. Si un nodo que se agregó a un dominio no recibió información de una raíz del mismo dominio, se predecirá que este nodo estará sin asignar (el nodo no recibió ninguna información), desconectado (en un subgráfico que no recibió información inicial) o pasará a otro dominio (el nodo recibió información de al menos ese dominio).
- Vista de subgrafos: el usuario puede crear subgráficos para visualizar un subconjunto de nodos para comprender con mayor claridad el impacto relacional y los límites de esa colección de nodos.
 - Para crear un subgrafo, seleccione un grupo de nodos y seleccione la opción Extraer subgrafo en la barra de herramientas
 - La combinación de subgráficos está disponible. Al fusionar, se crea un tercer subgrafo nuevo además de los dos subgráficos que se van a fusionar.

 Note

Repita estos pasos para añadir más dominios o para reconfigurar los dominios ya creados con un conjunto diferente de bases si no le gusta la estructura de dominios actual.

7. Cuando hayas terminado, selecciona Continuar.

Semillas

Las semillas son las entradas fundamentales para la fase de descomposición del código. Cada componente o archivo (por ejemplo, tablas JCL, COBOL, Db2, CSD y archivos de programación) se puede asignar como semilla a un solo dominio, lo que garantiza una alineación y unos límites claros durante el proceso de descomposición.

La identificación de las semillas depende de la estructura de la aplicación o cartera. En el caso de una aplicación tradicional típica de un ordenador central, las semillas suelen determinarse siguiendo las convenciones de nomenclatura establecidas, la agrupación a nivel de lote en el programador y la agrupación a nivel de transacciones definida en el sistema CICS. Además, las tablas de las bases de datos también pueden servir como base, proporcionando otra capa de estructura para la descomposición.

Importe y and/or actualice los archivos de dependencias

Durante la descomposición, puede cargar un archivo JSON para las dependencias que sustituya a los archivos existentes generados por el análisis de dependencias que realiza Transform. AWS

La función de exportación de dependencias le permite descargar el archivo json de dependencias generado en el paso de descomposición. Después de la descarga, puede modificar el archivo según sus necesidades. Luego, puede importar las dependencias mediante la función de carga de AWS Transform, que le permite cargar el nuevo archivo JSON de las dependencias que reemplaza al archivo generado por el análisis de dependencias. Después de eso, se actualizará el gráfico del paso de descomposición.

Para exportar, modificar e importar dependencias

1. En la página Ver los resultados de la descomposición, seleccione Acciones.
2. En la lista desplegable, elija la opción Actualizar el archivo de dependencias en Otras acciones.
3. En el modal Actualizar archivo de dependencias,
 - a. Descargue el archivo de dependencias AWS Transform creado a partir de los resultados del análisis existente.
 - b. En el archivo descargado, modifique las dependencias en función de lo que desee lograr.
 - c. Después de modificarlo, guarde y cargue este archivo con el botón Cargar archivo dependiente.

 Note

El único formato de archivo aceptado es el archivo JSON.

4. A continuación, selecciona Importar.

AWS Transform importará el archivo de dependencias y creará un nuevo gráfico de dependencias en función de lo que introduzcas.

Importar y and/or actualizar dominios

Para los clientes que tengan mapeadas las relaciones entre dominios, semillas y and/or archivos antes del paso de descomposición, pueden cargar esta definición de dominio mediante la función Importar archivos de dominios, disponible en el menú Acciones. Algunos ejemplos de cuándo se puede utilizar esta función:

- Adelanta la descomposición de otro trabajo
- Expertos en la materia que proporcionan este mapeo

Una vez importado el archivo de dominios, el usuario puede ejecutar la descomposición según la definición de dominio o, si está satisfecho, puede guardar y enviar la definición de dominio.

Parent/child/neighbor archivos

En un gráfico de dependencias, los programas se relacionan entre sí a través de diferentes tipos de conexiones. Comprender estas relaciones le ayuda a analizar las dependencias de los programas durante la transformación de sus aplicaciones de mainframe. También ayuda a comprender los límites de un dominio. Por ejemplo, si selecciona un dominio y, a continuación, selecciona el nivel principal, se mostrarán los nodos conectados.

Relaciones entre los padres: un archivo principal llama a otros programas o los controla. Los padres están por encima de sus programas dependientes en la jerarquía. Puede seleccionar a los padres en un nivel o en todos los niveles.

Relaciones entre hijos: el programa principal llama o controla un archivo secundario. Los niños se sitúan por debajo de sus padres en la jerarquía de archivos.

Relaciones de vecinos: los vecinos son archivos con el mismo nivel jerárquico. Comparten el mismo programa principal y pueden interactuar directamente entre sí.

Reforja el código

Reforge utiliza modelos de lenguaje grandes (LLM) para mejorar la calidad del código refactorizado. La COBOL-to-Java transformación inicial preserva la equivalencia funcional y, al mismo tiempo, conserva las estructuras de COBOL-influenced datos y los nombres de las variables del sistema anterior. Reforge reestructura este código para seguir las prácticas y expresiones idiomáticas modernas de Java, sustituyendo las COBOL-style construcciones por colecciones y convenciones de nomenclatura nativas de Java. Esto hace que el código sea más legible y fácil de mantener para los desarrolladores de Java.

Note

Las cuotas para la reforestación son:

- 3 000 000 de líneas de código por trabajo
- 50 000 000 de líneas de código por usuario al mes

Reforja tu código después de la refactorización siguiendo estos pasos:

1. Elija Reforge java code en el panel de navegación izquierdo y, a continuación, seleccione Configurar code reforge.
2. Proporcione la ubicación S3 a su proyecto fuente compilable comprimido y elija Continuar. Usa esta estructura de cremallera:

```
input.zip
  ### PROJECT-pom
  ### PROJECT-entities
  ### PROJECT-service
  ### PROJECT-tools
  ### PROJECT-web (optional)
  ### pom.xml
```

AWS Transform analiza el paquete zip para localizar los archivos dentro del PROJECT-service directorio, de modo que pueda proporcionar una lista seleccionable de clases que pueda volver a falsificar. Estas clases tienen el sufijo. `ProcessImpl.java`

3. Complete la página Seleccione las clases que desee reforjar y pulse Continuar. Realice un seguimiento del estado de la reforja en la pestaña Registro de trabajo.

4. Consulte los resultados de la reforja completada en la página Ver resultados, que muestra el estado de la reforja por clase. También especifica dónde encontrar el resultado de la reforja en el bucket de S3.

Una vez que AWS Transform reciba esta información, obtendrá un archivo descargable con los resultados de Reforge.

Esta es la estructura zip que resulta de una reforja exitosa:

```
reforge.zip
### maven_project
### reforge.log
###tokenizer_map.json
```

- maven_project contiene el código fuente reforjado.
 - Los archivos que se han refactorizado pero cuya compilación no se ha finalizado correctamente se encuentran en y reciben un nombre. /src/main/resources/reforge/originalClassName.java.incomplete originalClassName.java.incomplete Compárelos con las versiones originales de los archivos para elegir las funciones reforjadas que desee guardar.
 - Se hace una copia de seguridad de los archivos fuente proporcionados a AWS Transform y que se han refactorizado correctamente y se les asigna un nombre. src/main/resources/reforge/originalClassName.java.original originalClassName.java.original Las versiones refactorizadas de los archivos sustituyen a los archivos fuente proporcionados a Transform. AWS

 Note

Los originalClassName.java archivos se sustituyen por los archivos reforjados solo si el proceso de reforjado se realiza correctamente. De lo contrario, conservan el contenido original.

- reforge.log contiene registros que puede utilizar para diagnosticar errores en los trabajos o proporcionar AWS asistencia en caso de que surja algún problema.
- tokenizer_map.json contiene un mapeo de los identificadores de los token con sus datos, como las rutas y los class/method nombres de los archivos, que se tokenizan en los registros para proteger

la privacidad. Puedes proporcionar este archivo como soporte técnico en caso de que surja algún problema. AWS

Planifique las pruebas de sus aplicaciones modernizadas

Puede crear y administrar planes de pruebas para las aplicaciones modernizadas de su mainframe en función de los atributos del código extraído, la complejidad del trabajo y las rutas del programador. AWS Transform ayuda a priorizar los trabajos que se van a probar e identifica los artefactos específicos necesarios para cada caso de prueba. El proceso de planificación de las pruebas se divide en tres fases principales: configuración, determinación del alcance y revisión.

Para crear un plan de pruebas

1. Configure los ajustes del plan de pruebas
 - a. En el panel de navegación izquierdo, en Planifique las pruebas, elija Configurar los ajustes.
 - b. (Opcional) Proporcione las rutas S3 para su Business Logic Extraction (BLE). Estos artefactos mejoran la calidad del plan de pruebas. Sin los artefactos del BLE, algunos campos del plan de pruebas podrían quedar incompletos.
2. Defina el alcance del plan de pruebas
 - a. Seleccione los puntos de entrada, como los trabajos por lotes, para incluirlos en su plan de pruebas.
 - b. Filtre y ordene los trabajos en función de varios atributos:
 - Funciones empresariales (extraídas de BRE BLE)
 - Dominios (de la fase de descomposición)
 - Rutas y ubicaciones de los archivos
 - Criterios de búsqueda personalizados
 - c. Seleccione trabajos individuales o grupos enteros para realizar las pruebas.
 - d. Revise las relaciones y dependencias laborales.
3. Revise y ajuste el plan de pruebas

El plan de pruebas generado proporciona información completa que incluye:

- Orden de ejecución preferida basada en las dependencias
- Asignaciones de grupos de trabajo desde el programador

- Puntuaciones de complejidad, que son puntuaciones agregadas para casos de prueba
- Asociaciones de dominios empresariales
- Métricas de complejidad ciclomática
- Dependencias de conjuntos de datos y tablas
- Métricas de líneas de código
- Mapeos de funciones empresariales

Opciones de personalización del plan de pruebas

Su plan de pruebas se puede personalizar para satisfacer necesidades específicas. Por ejemplo, puede hacer lo siguiente:

- Cree nuevos casos de prueba seleccionando varios puntos de entrada
- Combine los casos de prueba existentes para combinar las funciones relacionadas
- Divida los casos de prueba para realizar pruebas más detalladas
- Elimine los casos de prueba innecesarios
- Añada o elimine puntos de entrada para los casos de prueba existentes
- Modifique las descripciones y los atributos de los casos de prueba
- Ajuste el orden de ejecución

Información detallada del caso de prueba

Cada caso de prueba proporciona detalles que describen su contenido y el conjunto de datos o archivos de datos relacionados:

- Descripción completa del alcance de la prueba
- Se incluye una lista completa de los puntos de entrada
- Métricas agregadas que muestren la complejidad y el tamaño
- Normas empresariales y orientación sobre casos de prueba automatizados
- Dependencias de conjuntos de datos y tablas con dirección () input/output
- Visualización interactiva de gráficos de dependencia
- Prerrequisitos y requisitos de ejecución

Funciones de gestión de datos

Estos detalles le ayudan a comprender los datos relacionados con el caso de prueba. Puede:

- Filtrar conjuntos de datos por input/output dirección
- Identifique los artefactos necesarios para la ejecución de las pruebas
- Realice un seguimiento de las dependencias de datos entre los casos de prueba
- Supervise el uso del conjunto de datos en todos los planes de prueba

Note

AWS Transform analiza automáticamente las dependencias de los planificadores y asigna puntuaciones de complejidad para ayudar a priorizar los esfuerzos de prueba. Los puntajes de complejidad más altos indican trabajos que pueden requerir pruebas más exhaustivas o aislamiento durante el proceso de prueba.

Normas empresariales y orientación sobre casos de prueba

El plan de pruebas AWS Transform proporciona recomendaciones para su plan de casos de prueba basadas en la extracción de reglas empresariales:

- Procesamiento automático de reglas de negocio mediante LLM
- Generación de casos de prueba sintéticos
- Guía de pruebas para escenarios empresariales específicos
- Trazabilidad entre reglas y casos de prueba

El plan de pruebas final se almacena en la ubicación S3 especificada e incluye toda la información necesaria para ejecutar la estrategia de pruebas de forma eficaz. Puede exportar el plan de pruebas para integrarlo con otras herramientas de prueba o sistemas de documentación.

Note

Si bien se proporciona una guía sintética sobre los casos de prueba, los artefactos de prueba reales deben crearse por separado según la guía. El plan de pruebas sirve como un plan

integral para su estrategia de pruebas, pero no genera los datos de las pruebas ni los scripts de ejecución.

Reglas de creación de casos de prueba: resumen

Reglas generales

- Un caso de prueba contiene de 1 a varios JCL en orden de ejecución programado
- Los casos de prueba se crean a partir de programadores compatibles y válidos (CA7 y) Control-M
- La prueba ejecuta los JCL, no el planificador en sí ni las tareas programadas
- Una tarea programada es única y ejecuta solo un JCL
- Un JCL se puede ejecutar mediante múltiples tareas programadas
- Un JCL puede existir sin estar incluido en un cronograma

Reglas de creación de casos de prueba predeterminadas

- Si un solo JCL está en un caso de prueba:
 - JCL no participa en ningún cronograma
 - JCL se ejecuta mediante una tarea programada que se divide en varias ramas
 - Una sucursal del cronograma contiene solo este JCL
- Si hay varios JCL en un caso de prueba: representa una secuencia de ruta de ejecución lineal dentro de una rama de programación
- Si JCL está realizando una tarea programada divergente: JCL se convierte en su propio caso de prueba independiente
- Si JCL tiene una tarea programada convergente: JCL puede iniciar un nuevo caso de prueba, pero no se incluirá en las sucursales anteriores
- Los JCL que faltan se omiten y la ejecución continúa (con una mejora planificada en el futuro para reducir el caso de prueba en el punto JCL faltante)

Reglas de operaciones de usuario

- Crear caso de prueba: el usuario selecciona entre los JCL disponibles
 - Tiene éxito si los JCL existen en la secuencia de ramificaciones de ejecución programada

- Sigue el orden de ejecución programado
- Agregue un JCL al caso de prueba: el usuario selecciona entre los JCL disponibles
 - Tiene éxito si el JCL puede existir en la ejecución programada del caso de prueba branch/path
- Eliminar el JCL del caso de prueba: el usuario puede eliminar cualquier JCL de un caso de prueba
 - Permitido incluso si provoca brechas en la ruta de ejecución
- Combinar casos de prueba: el usuario selecciona dos casos de prueba para combinarlos
 - Tiene éxito si los JCL pueden existir juntos en la misma rama de ejecución programada
 - Mantiene el orden de ejecución del cronograma
- Caso de prueba dividido: el usuario selecciona un JCL en un caso de prueba para dividirlo
 - Crea un nuevo caso de prueba a partir del punto de división
 - El caso de prueba original se modificó para excluir los JCL más allá del punto de división
- Eliminar caso de prueba: el usuario puede eliminar cualquier caso de prueba creado

Note

No puede crear, agregar o combinar casos de prueba desde un programador branches/path diferente. Se planea una mejora futura para permitir operaciones más allá de divergent/convergent las tareas del programador.

Genere scripts de recopilación de datos de prueba

Puede generar scripts JCL para recopilar datos de prueba de sus sistemas mainframe en función del plan de pruebas creado en el paso anterior. AWS Transform crea automáticamente scripts de recopilación de datos para los conjuntos de datos, las tablas de bases de datos y los archivos secuenciales necesarios para realizar pruebas exhaustivas. El proceso de recopilación de datos se divide en cuatro fases principales: configuración de entrada, selección de casos de prueba, configuración del script y generación de scripts.

Para generar scripts de recopilación de datos de prueba

1. Proporcione información sobre el plan de pruebas
 - a. En el panel de navegación izquierdo, en Recopilación de datos de prueba, elija Proporcionar entrada al plan de pruebas.

- b. Especifique la ruta S3 al archivo JSON del plan de pruebas en [Planifique las pruebas de sus aplicaciones modernizadas](#).
 - c. El campo de entrada se rellena automáticamente si el plan de pruebas se generó en un paso de trabajo anterior.
 - d. También puede seleccionar un plan de pruebas de otros trabajos especificando la ubicación de S3 adecuada.
2. Seleccione casos de prueba para la recopilación de datos
 - a. Revise la lista completa de casos de prueba de su plan de pruebas.
 - b. Filtra y ordena los casos de prueba en función de varios atributos:
 - Funciones y dominios empresariales
 - Dependencias de tablas de bases de datos
 - Requisitos del conjunto de datos
 - Métricas de complejidad
 - Criterios de búsqueda personalizados
 - c. Seleccione casos de prueba individuales o utilice las opciones de selección masiva.
 - d. Revise los detalles del caso de prueba, incluidos los puntos de partida, las métricas y las reglas comerciales, haciendo clic en un caso de prueba para ver los detalles.
3. Configure los scripts de recopilación de datos
 - a. Descargue plantillas de muestra y archivos de configuración como referencia.
 - AWS Transform proporciona plantillas de muestra para la descarga de bases de datos de Db2, el REPRO de archivos VSAM y el procesamiento secuencial de conjuntos de datos, que se utilizan como guía sobre los tipos de plantillas que se esperan del proceso.
 - Los estándares pueden variar de un sitio a otro, por lo que se espera que los clientes modifiquen o reemplacen estas plantillas para adaptarlas a sus propios estándares.
 - Estas plantillas modificadas deben cargarse en un depósito de S3 donde la recopilación de datos de prueba pueda procesarlas.
 - b. Proporcione un archivo de configuración variable (formato JSON) que contenga:
 - Prefijos de usuario y constantes específicas del entorno
 - Parámetros de configuración de base de datos
 - ~~Configuración del punto final de destino y parámetros de transferencia de datos~~

- Otros parámetros obligatorios definidos por el usuario y que se utilizarán en las plantillas de JCL
- c. Cargue plantillas JCL para diferentes métodos de recopilación de datos:
 - Plantilla Db2: para descargar tablas de bases de datos (personalícela para BMC, IBM DSN u otras utilidades de descarga)
 - Plantilla VSAM: para el procesamiento de archivos VSAM (normalmente utiliza la utilidad REPRO)
 - Plantilla de conjuntos de datos secuenciales: para procesar conjuntos de datos secuenciales, conjuntos de datos particionados, GDG, etc.

4. Revise y administre los scripts generados

Los scripts generados proporcionan capacidades integrales de recopilación de datos, que incluyen:

- Secuencias de comandos independientes para la recopilación de datos «antes» y «después» de la ejecución de la prueba
- Estructura del script organizada por caso de prueba y tipo de datos
- Los scripts se almacenan automáticamente en el bucket de S3 para facilitar el acceso y la transferencia
- Los scripts JCL generados están listos para su ejecución en el mainframe
- La sustitución de variables se basa en la configuración del usuario definida en las plantillas

Funciones de generación de scripts

Los scripts generados se personalizan automáticamente en función de las plantillas y la configuración:

- Template-based generación: utiliza las plantillas de JCL proporcionadas con sustitución de variables
- Entorno: incorpora su configuración de mainframe específica
- Manejo del tipo de datos: crea los scripts adecuados para conjuntos de datos secuenciales, archivos VSAM y tablas de bases de datos
- Recopilación para casos de prueba: genera scripts de recopilación de datos «antes» y «después»

- Procesamiento secuencial de conjuntos de datos: el ejemplo AWS proporcionado proporciona una función de transferencia de archivos, pero se puede personalizar con las utilidades de compresión disponibles en su sitio o con utilidades como Connect Direct o la transferencia de archivos gestionada, etc.

Estrategia de recopilación de datos

Los scripts generados respaldan estrategias integrales de recopilación de datos:

- Recopilación secuencial de conjuntos de datos: utilidades de reproducción y copia para archivos planos y VSAM
- Descarga de tablas de bases de datos: procesos de descarga de Db2 personalizables
- Procesamiento secuencial de conjuntos de datos: posprocesamiento personalizable de conjuntos de datos secuenciales, como la compresión, los servicios gestionados de transferencia de archivos, etc.
- Gestión de dependencias: recopilación coordinada basada en la definición de un caso de prueba

Note

AWS Transform genera scripts en función de sus plantillas y su configuración. Revise todos los JCL generados antes de ejecutarlos en su entorno de mainframe para garantizar la compatibilidad con los requisitos específicos de configuración y seguridad del sistema.

Personalización de plantillas y prácticas recomendadas

La recopilación de datos de pruebas de ATX proporciona capacidades flexibles de personalización de plantillas:

- Multi-utility soporte: adapte las plantillas para diferentes utilidades de mainframe (BMC, IBM, DSN)
- Variable-driven configuración: utilice constantes para los parámetros específicos del entorno
- Plantillas reutilizables: cree plantillas estandarizadas para una generación de scripts coherente
- Manejo de datos: incorpore los requisitos de manejo de datos específicos de la organización
- Integración de seguridad: incluya los controles de seguridad y acceso adecuados
- Optimización del rendimiento: configúrelo para una recopilación y transferencia de datos eficientes

Estructura de salida generada

Los scripts generados se organizan en su bucket de S3 con la siguiente estructura:

- Organización de los casos de prueba: scripts agrupados por casos de prueba asociados
- Plazo de recopilación: carpetas separadas para la recopilación de datos «antes» y «después»
- Clasificación de los tipos de datos: scripts organizados por conjuntos de datos secuenciales, tablas de bases de datos y transferencias
- Archivos de metadatos: información resumida y guía de ejecución
- Ready-to-transfer formato: formato JCL para el despliegue directo de un mainframe

La colección de scripts final se almacena en la ubicación S3 especificada e incluye todo el JCL necesario para ejecutar su estrategia de recopilación de datos de manera eficaz. Puede descargar los scripts para transferirlos a su entorno de mainframe o integrarlos en los procesos de implementación automatizados.

Note

Si bien se generan scripts JCL completos, la ejecución real debe realizarse en su entorno de mainframe. Los scripts sirven como herramientas de recopilación de datos listas para usar, pero requieren los permisos de acceso y ejecución adecuados al mainframe.

Generación de scripts de automatización de pruebas

Puede generar scripts de automatización de pruebas para ejecutar casos de prueba en su aplicación modernizada en función del plan de pruebas creado en el paso anterior. AWS Transform crea automáticamente scripts de prueba completos que utilizan los datos recopilados en el proceso de recopilación de datos de las pruebas. El proceso de generación de scripts de automatización de pruebas consta de tres fases principales: configuración de entrada, selección de casos de prueba y resultados de generación de scripts.

Para generar scripts de prueba

1. Proporcione información sobre el plan de pruebas
 - a. En el panel de navegación izquierdo, en Generación de scripts de automatización de pruebas, elija Proporcionar entrada al plan de pruebas.

- b. Especifique la ruta S3 al archivo JSON del plan de pruebas en [Planifique las pruebas de sus aplicaciones modernizadas](#).
 - c. El campo de entrada se rellena automáticamente si el plan de pruebas se generó en un paso de trabajo anterior.
 - d. También puede seleccionar un plan de pruebas de otros trabajos especificando la ubicación de S3 adecuada.
 - e. El sistema utiliza este plan de pruebas como base para generar scripts de automatización.
2. Seleccione los casos de prueba para la generación de scripts
 - a. Revise la lista completa de casos de prueba de su plan de pruebas.
 - b. Filtra y ordena los casos de prueba en función de varios atributos:
 - Funciones y dominios empresariales
 - Dependencias de tablas de bases de datos
 - Requisitos del conjunto de datos
 - Métricas de complejidad
 - Criterios de búsqueda personalizados
 - c. Seleccione casos de prueba individuales o utilice las opciones de selección masiva con los botones Marcar todo y desmarcar todo.
 - d. Revise los detalles de los casos de prueba, incluidos los puntos de partida, las métricas y las reglas comerciales, haciendo clic en los casos de prueba individuales.

Los casos de prueba seleccionados tendrán scripts de automatización generados para su ejecución en la aplicación modernizada.

3. Revise y gestione los scripts de automatización de pruebas generados:
 - El sistema muestra un mensaje de éxito que confirma que se ha completado la generación del script.
 - Los scripts de prueba generados se almacenan automáticamente en la ubicación del bucket de S3 que haya especificado.
 - Acceda a la lista completa de los scripts de prueba generados con sus respectivas ubicaciones de S3.
 - Cada caso de prueba tiene su script de automatización correspondiente almacenado en ubicaciones individuales de S3.

- Los scripts están listos para su despliegue y ejecución en su entorno de aplicaciones modernizado.

Pruebe las funciones de los scripts de automatización

Los scripts de automatización generados proporcionan capacidades de prueba integrales:

- Pruebas de aplicaciones modernizadas: los scripts están diseñados específicamente para ejecutar casos de prueba en la aplicación transformada
- Integración de datos: utiliza los datos de prueba recopilados en el paso anterior de recopilación de datos de prueba; estos datos deben copiarse en carpetas para cada caso de prueba
- Ejecución automatizada: los scripts se pueden utilizar para configurar depósitos de datos, ejecutar casos de prueba y comparar los resultados; algunos parámetros deberán configurarse en función del entorno de implementación
- Estructura organizada: los scripts se organizan sistemáticamente por caso de prueba en el bucket de S3
- Ready-to-deploy Formato: los scripts están formateados para su implementación directa en su entorno de pruebas

Estructura de salida generada

Los scripts de automatización de pruebas generados se organizan en su bucket de S3 con la siguiente estructura:

- Organización de los casos de prueba: cada caso de prueba tiene su script dedicado almacenado en una carpeta S3 individual
- Execution-ready formato: los scripts se formatean para su despliegue y ejecución inmediatos después de configurar alguna variable en función del entorno
- Acceso centralizado: se puede acceder a todos los scripts desde una única ubicación de bucket de S3 para facilitar su administración

Pruebe la estrategia de ejecución

Los scripts generados admiten flujos de trabajo integrales de ejecución de pruebas:

- Configuración del entorno: los scripts incluyen capacidades para configurar los datos iniciales para ejecutar la prueba
- Preparación de los datos: integración con los datos de prueba recopilados en la etapa de recopilación de datos del caso de prueba
- Ejecución de casos de prueba: ejecución automatizada de casos de prueba individuales en la aplicación modernizada
- Comparación de resultados: Built-in capacidades para comparar los resultados de las pruebas y validar el comportamiento de la aplicación

 Note

AWS Transform genera scripts de automatización de pruebas en función de su plan de pruebas y de los casos de prueba seleccionados. Los scripts están diseñados para ejecutarse en su entorno de aplicaciones modernizado y utilizan los datos de prueba recopilados en el paso anterior. Revise todos los scripts generados antes de la implementación para garantizar la compatibilidad con la configuración específica de la aplicación y los requisitos de prueba.

Prácticas recomendadas para la automatización de pruebas

- Validación del entorno: asegúrese de que el entorno de aplicaciones modernizado esté configurado correctamente antes de ejecutar el script
- Verificación de datos: valide que los datos de prueba requeridos de la fase de recopilación estén disponibles y accesibles
- Personalización de los scripts: revise y personalice los scripts generados según sea necesario para sus requisitos de prueba específicos
- Supervisión de la ejecución: Implemente la supervisión y el registro adecuados durante la ejecución del script de prueba
- Análisis de resultados: establezca procesos para analizar los resultados de las pruebas e identificar los problemas de las aplicaciones

La colección final de scripts de automatización de pruebas proporciona un marco de pruebas completo para validar la funcionalidad modernizada de la aplicación. Los scripts pueden integrarse

en sus procesos de pruebas continuas o ejecutarse como parte del flujo de trabajo de validación de aplicaciones.

Capacidades de despliegue en AWS Transformar

AWS Transform le ayuda a configurar entornos de nube para aplicaciones de mainframe modernizadas al proporcionar plantillas de infraestructura como código (IaC) listas para usar. A través de la interfaz de chat AWS Transform, puede acceder a plantillas prediseñadas que crean componentes esenciales, como recursos informáticos, bases de datos, almacenamiento y controles de seguridad. Las plantillas están disponibles en los formatos más populares, como CloudFormation (CFN) y Terraform AWS Cloud Development Kit (AWS CDK), lo que le brinda flexibilidad para implementar su infraestructura.

Estas plantillas sirven como componentes básicos que reducen el tiempo y la experiencia necesarios para configurar los entornos para sus aplicaciones de mainframe modernizadas. Puede personalizar estas plantillas para que se adapten a sus necesidades, lo que le proporciona una base para crear su entorno de implementación.

Para recuperar las plantillas de IaC, solicite en el chat de AWS Transform las Infrastructure-as-Code plantillas que aclaren su patrón de modernización preferido (como AWS Transform para la refactorización de mainframe), su topología preferida (independiente frente a alta disponibilidad) y su formato preferido (frente a Cloud Development CloudFormation Kit frente a Terraform).

Cree e implemente su aplicación modernizada después de la refactorización

Tras completar el proceso de refactorización con AWS Transform, puede crear e implementar su aplicación Java modernizada. Esta guía explica cómo recuperar el código modernizado, configurar el entorno e implementar y probar la aplicación.

Note

Además de las instrucciones que se proporcionan aquí, el paquete de código generado por AWS Transform incluirá un documento sobre la configuración del entorno de desarrollo con refactorización AWS automatizada, en el que se proporcionan instrucciones para configurar un IDE (entorno de desarrollo integrado) con Developer Runtime.

Temas

- [Requisitos previos](#)
- [Paso 1: Recupere el código modernizado](#)
- [Paso 2: Cree la aplicación modernizada](#)
- [Paso 3: Configurar el entorno de prueba](#)
- [Paso 4: Implemente la aplicación modernizada](#)
- [Paso 5: Pruebe la aplicación modernizada](#)
- [Ejemplo adicional](#)

Requisitos previos

Antes de empezar, asegúrese de que tiene lo siguiente:

- Completó satisfactoriamente un trabajo de refactorización con Transform. AWS
- Acceda a su código modernizado.
- Conjunto de herramientas de software de compilación instaladas y configuradas en su máquina de desarrollo, como [Apache Maven](#) o [Apache Tomcat](#). Para obtener más información sobre el control de versiones en tiempo de ejecución, consulte las notas de la versión de [AWS Transform for mainframe Runtime](#).
- Se instaló y configuró Amazon Corretto o una versión de Java Runtime. Para obtener más información sobre la instalación de Amazon Corretto, consulte Amazon [Corretto 24](#).
- Acceso para crear y configurar bases de datos PostgreSQL de Amazon Aurora para componentes de Runtime, si es necesario. Para obtener más información sobre la creación de la base de datos PostgreSQL de Aurora, [consulte Uso de Amazon Aurora PostgreSQL](#).
- Acceso administrativo para implementar aplicaciones en su entorno de ejecución.
- Revisé los conceptos de [AWS Transform for mainframe Runtime para conocer los conceptos](#) fundamentales sobre las aplicaciones modernizadas con una solución de refactorización AWS automatizada.

Paso 1: Recupere el código modernizado

Para recuperar el código modernizado

1. Descargue y extraiga el paquete de códigos generado.

2. Abra `codebase/app-pom/pom.xml` y anote la versión del motor de ejecución requerida. Por ejemplo, `<gapwalk.version>4.6.0</gapwalk.version>`.
3. Busque el documento sobre cómo configurar el entorno de desarrollo de refactorización AWS automatizada en el paquete de códigos descargado como referencia.

Paso 2: Cree la aplicación modernizada

Para crear su aplicación modernizada

1. Acceda al tiempo de ejecución desde la caja de AWS herramientas Transform for mainframe.
2. Descargue e instale la versión de ejecución adecuada (identificada en [the section called “Paso 1: Recupere el código modernizado”](#)) en su máquina de desarrollo local.

Note

Encontrará información adicional sobre cómo instalar las dependencias del entorno de ejecución en su máquina local en la sección 3.1 del documento Configurar el entorno de desarrollo de refactorización AWS automatizada.

3. Abra la línea de comandos y navega hasta el directorio raíz de la aplicación.
4. Para crear paquetes desplegables para la aplicación modernizada, ejecute el comando build de Maven:

```
mvn package
```

Consulte la página de [organización de la aplicación](#) para obtener detalles sobre la organización básica del código modernizado. Por ejemplo, en el caso de una aplicación modernizada que contenga una aplicación web front-end, cabe esperar al menos los siguientes `.war` agregados desplegables, además de los componentes de tiempo de ejecución:

- Proyecto de servicio: contiene elementos de modernización de la lógica empresarial heredados

```
<business-app>-service.*.war
```

- Proyecto web: contiene la modernización de los elementos relacionados con la interfaz de usuario

```
<business-app>-web.*.war
```

Paso 3: Configurar el entorno de prueba

Para configurar el entorno de pruebas

1. Configure el tiempo de ejecución de su aplicación modernizada. Para obtener más información, consulte la sección [Configurar la configuración para el tiempo de ejecución de](#) la guía del AWS Mainframe Modernization usuario.

Note

Consulte la sección 5 de la guía sobre cómo configurar el entorno de desarrollo de refactorización AWS automatizada para ver ejemplos de configuración específicos de los componentes en tiempo de ejecución.

2. Prepare los conjuntos de datos de entrada y salida (I/O) para las aplicaciones modernizadas. Las aplicaciones modernizadas pueden procesar conjuntos de I/O datos secuenciales, conjuntos de datos de VSAM u otros.

Note

Consulte la sección 6 de la sección Configuración del entorno de desarrollo de AWS refactorización automatizada para ver ejemplos.

3. Un entorno de ejecución: puede utilizar su entorno de ejecución existente o crear uno nuevo.
 - Para configurar un entorno de tiempo de ejecución no administrado, consulte [Configurar una aplicación no administrada](#).
 - Para configurar un entorno de tiempo de ejecución gestionado, consulte [Configurar una aplicación gestionada](#).

Tras configurar el entorno de prueba, pasará al siguiente paso: implementar la aplicación modernizada.

Paso 4: Implemente la aplicación modernizada

Implemente los artefactos de la aplicación en el tiempo de ejecución que creó y and/or configuró en las [the section called “Paso 3: Configurar el entorno de prueba”](#) secciones [the section called “Paso 2: Cree la aplicación modernizada”](#) y.

Puede encontrar orientación adicional para implementar la aplicación modernizada en estos enlaces:

- [Implementación en Amazon EC2](#)
- [Implemente en contenedores de Amazon ECS y Amazon EKS](#)
- [Cree una AWS Mainframe Modernization aplicación](#)

Paso 5: Pruebe la aplicación modernizada

Tras la implementación,

1. Revise las [API de tiempo de ejecución](#) disponibles para conocer las formas de interactuar con las aplicaciones modernizadas.
2. Pruebe su aplicación para alinear su equivalencia funcional con la aplicación antigua. Por ejemplo, consulte [Probar una aplicación de muestra](#) en la guía del AWS Mainframe Modernization usuario.

Ejemplo adicional

Para ver un ejemplo específico de cómo modernizar una aplicación de mainframe con AWS Transform, consulte [Modernizar la CardDemo](#) aplicación de mainframe.

Full-stack Modernización de Windows

AWS Transform proporciona una modernización completa de Windows, que incluye la modernización de .NET y la modernización de SQL Server.

El agente AWS Transform para .NET puede ayudarlo a modernizar sus aplicaciones .NET para que sean compatibles con .NET multiplataforma. [Puede modernizar .NET mediante la aplicación web .NET o el .NET IDE.](#)

AWS La [modernización de Transform for SQL Server](#) es un AI-powered servicio que automatiza la modernización completa de las bases de datos de Microsoft SQL Server y sus aplicaciones .NET asociadas a Amazon Aurora PostgreSQL. El servicio organiza todo el proceso de migración, desde la conversión de esquemas, la migración de datos y la modificación del código de la aplicación para adaptarlo al nuevo PostgreSQL de destino, lo que hace que sus equipos sean más productivos al automatizar tareas complejas y laboriosas.

Temas

- [Modernizar .NET con AWS Transformar](#)
- [Modernización de SQL Server](#)

Modernizar .NET con AWS Transformar

El agente AWS Transform para .NET puede ayudarlo a modernizar sus aplicaciones .NET para que sean compatibles con .NET multiplataforma. Esta capacidad se denomina modernización de .NET. Después [AWS Transforma el entorno](#) de AWS Transform, puede crear un trabajo de transformación de modernización de .NET.

Experiencias

AWS Transform está disponible en varias experiencias:

- Consola web: para la transformación a gran escala de hasta 500 repositorios a la vez.
- Visual Studio IDE: transformación de una solución o proyecto dirigida por un desarrollador que trabaja junto con el agente de forma interactiva e iterativa. Recomendado para proyectos medianos y grandes.

Puede cambiar libremente entre la consola web y el IDE para trabajar en un trabajo de transformación.

También puedes invocar AWS Transform desde otros IDE y códigos complementarios de IA:

- Kiro: transforma a Kiro con el poder de AWS Transformar para Kiro.
- Otros compañeros de programación de IA: transforma tus asistentes de programación de IA preferidos con los agentes AWS Transform MCP.

Capacidades y características clave

- Analice las bases de código de .NET Framework de sus sistemas de control de código fuente, lo que incluye NuGet soporte privado, identifique las dependencias entre repositorios y proporcione un informe de análisis.
- Transformación automatizada de aplicaciones antiguas de .NET Framework en aplicaciones multiplataforma de .NET, notificaciones por correo electrónico y un informe resumido sobre la transformación.
- Fácil integración con las plataformas de control de código fuente (BitBucket GitHub, y GitLab) para incorporar el código existente y enviar el código transformado a una nueva rama.
- Validación del código transformado mediante pruebas unitarias.

Versiones y tipos de proyectos compatibles

AWS Transform admite la transformación de las siguientes versiones de .NET:

- .NET Framework 3.5+
- .NET Core 3.1
- .NET 5.x+
- .NET 8

AWS Transform puede transformarse en las siguientes versiones de .NET de destino:

- .NET 8
- .NET 10

AWS Transform admite la transformación de estos tipos de proyectos (solo en C#):

- Bibliotecas de clases
- Aplicaciones de consola
- ASP.NET:
 - Model View Controller (MVC), que incluye la interfaz Razor Views
 - Back-ends de aplicaciones de una sola página (SPA) (capas de lógica empresarial)
 - API web
 - Formularios web
- Proyectos de pruebas unitarias (NUnit, xUnit y MSTest)
- Servicios de Windows Communication Foundation (WCF)
- Proyectos con versiones multiplataforma proporcionadas para paquetes privados NuGet o de terceros. Si falta un equivalente multiplataforma o no está disponible, AWS Transform for .NET intentará realizar la conversión al máximo.

AWS Transform también puede transformar los siguientes tipos de proyectos en la versión moderna de .NET. Se trata de una función de vista previa y es posible que no se transforme tan completamente como los tipos de proyectos compatibles.

- WinForms proyectos de escritorio.
- proyectos de escritorio de WPF.
- Proyectos móviles de Xamarin.
- Proyectos escritos en VB.NET

Limitaciones

Para obtener más información sobre las cuotas y limitaciones de AWS Transform, consulte [Cuotas para AWS Transformar](#).

AWS Transformar no transforma lo siguiente:

- Componentes de interfaz de usuario de Blazor
- DLL de Win32 que no tienen bibliotecas compatibles básicas
- Repositorios que no contienen ninguna solución.

AWS Transform no modificará las ramas del repositorio originales y solo podrá escribir en una rama de destino independiente especificada en su plan de transformación.

Intervención humana

Durante la migración de las aplicaciones .NET Framework a una plataforma multiplataforma, es posible que se le solicite que proporcione información o que dé su aprobación en los siguientes escenarios:

- Configure un conector para el código fuente y los permisos
- Valide el plan de modernización propuesto
- Cargue las dependencias de paquetes faltantes como NuGets
- Revisa y acepta el código transformado

Más información

Puede modernizar su código .NET mediante la aplicación web AWS Transform o el AWS kit de herramientas para Visual Studio

- [Modernizar el código .NET mediante el AWS Transforme la aplicación web](#)
- [Modernizar .NET en el IDE](#)
- [Mejores prácticas para las transformaciones de .NET](#)

Modernizar el código .NET mediante el AWS Transforme la aplicación web

AWS Transform for .NET es un nuevo AI-powered agente generativo diseñado para modernizar las aplicaciones de .NET antiguas. Puede modernizar su código .NET antiguo mediante la aplicación web AWS Transform o la Visual Studio AWS extensión Toolkit.

Para modernizar su código .NET mediante la aplicación web AWS Transform, navegue hasta la aplicación web y siga estos pasos detallados:

1. [Creando el AWS Transforme el plan de trabajo de .NET](#)
2. [Crear un conector para el repositorio de código fuente](#)
3. [Confirme sus repositorios para prepararse para la transformación](#)
4. [Resolver las dependencias de los paquetes para prepararse para la transformación](#)

5. [Revisar su plan para prepararse para la transformación](#)
6. [Transformando su código.NET](#)

Creando el AWS Transforme el plan de trabajo de .NET

Tras crear el espacio de trabajo, en la pestaña Trabajos, selecciona Crear trabajo. A continuación, sigue las instrucciones de AWS Transform en el panel de chat utilizando un lenguaje natural. Estos son los pasos típicos para crear un trabajo de modernización de .NET.

1. AWS Transform le preguntará qué tipo de trabajo de transformación desea crear. En el chat, escriba Modernización de.NET.
2. AWS Transform le sugerirá un nombre para el trabajo y le preguntará si desea cambiarlo. Si desea cambiar el nombre del trabajo, dígame a AWS Transform en lenguaje natural, por ejemplo, que cambie el nombre del trabajo a ExampleCorpDotNet1. De lo contrario, en el chat, puedes aceptar el nombre del trabajo sugerido. Tras aceptar el nombre del trabajo, AWS Transform le notificará en la ventana de chat que está creando el trabajo.
3. AWS Transform crea el trabajo de transformación.

Componentes del AWS Transforme el plan de trabajo de .NET

La pantalla de tareas de AWS Transform.NET tiene 5 pestañas que puede seleccionar en los iconos verticales del extremo izquierdo: tareas, panel, aprobaciones, artefactos y registro de trabajo. Cada pestaña tiene un panel izquierdo y un panel de chat central. A veces, puede aparecer un panel de colaboración a la derecha para mostrar detalles adicionales y solicitar la opinión de un humano.

Tareas (Plan de trabajo)

Esta pestaña muestra su plan de trabajo en el panel izquierdo. Un trabajo de .NET consta de 5 pasos:

1. Obtenga recursos para transformarlos: en esta fase, crea un conector a su repositorio de código mediante AWS CodeConnections. En función de los permisos del repositorio, es posible que un administrador del repositorio de código tenga que aprobar el conector y conceder a AWS Transform el acceso al repositorio.
2. Descubra los recursos para la transformación: en esta fase, AWS Transform descubre los repositorios en el control de código fuente y usted selecciona algunos o todos ellos para su evaluación.

3. Evalúe el código para la transformación: se evalúan los repositorios seleccionados y puede ver los informes de evaluación.
4. Prepárese para la transformación: en esta fase, AWS Transform le notifica si falta alguna dependencia en sus repositorios. Puedes cargar las dependencias que faltan o ignorarlas. Si no eres el administrador del repositorio, es posible que un administrador deba aprobar el plan de transformación final.
5. Transformar: en esta fase, AWS Transform transforma tu repositorio y te proporciona el estado en curso durante la transformación hasta que se complete. Puedes revisar los informes de transformación para entender qué se ha cambiado y por qué.

Puede ver el estado de cada paso:

- ¿No se ha iniciado
- Espere la entrada del usuario
- En curso
- Completado

Panel de control

La pestaña Panel de control proporciona un resumen de alto nivel de la transformación. Muestra métricas sobre el número de trabajos transformados, la transformación aplicada y el tiempo estimado para completar la transformación. Debajo del panel de control hay una tabla con los repositorios y su estado: In-progress fallido o correcto.

Aprobaciones

Las solicitudes de aprobación del trabajo se muestran y se completan en esta pestaña.

Artefactos

Jjob-related Los artefactos se cargan o descargan desde esta pestaña.

Registro de trabajo

AWS Transform registra sus acciones en la pestaña Registro de trabajo. El registro de trabajo proporciona un registro detallado de las acciones que lleva a cabo AWS Transform, junto con las solicitudes de participación humana y sus respuestas a esas solicitudes.

Crear un conector para el repositorio de código fuente

Después [Creando el AWS Transforme el plan de trabajo de .NET](#), en la pestaña Tareas, el panel izquierdo de la ventana de AWS transformación muestra las fases del trabajo de transformación. La primera fase consiste en conseguir que los recursos se transformen. En esta fase, puedes invitar a colaboradores y conectar un repositorio de código fuente. En el panel derecho de la ventana de AWS transformación se especifican los detalles.

Cada trabajo de transformación debe tener solo un conector para el repositorio de código fuente. El agente de AWS Transform usa este conector para descargar tu código base de .NET desde GitHub Bitbucket o mediante Bitbucket. GitLab [AWS CodeConnections](#) Debe configurarlo AWS CodeConnections en la misma región que su AWS trabajo de Transform. Como alternativa, puede [Conectarse al código fuente de Amazon S3 en](#) lugar de a un repositorio de código fuente.

Note

Si ya tiene un conector de repositorio de código fuente, AWS Transform se lo notificará. Seleccione Usar un conector existente para usar este conector. Si no desea utilizar el conector existente, consulte lo [Eliminar un conector existente](#) anterior [Añadir un conector nuevo](#). Solo puede tener un conector de repositorio de origen por trabajo.

Añadir un conector nuevo

Para crear un nuevo conector de repositorio de código fuente:

1. Introduzca el número de AWS cuenta que desea utilizar para el AWS CodeConnections conector.
2. Si no ha configurado AWS CodeConnections la misma AWS cuenta, [configúrela AWS CodeConnections](#).
3. Usa la [consola de herramientas para AWS desarrolladores](#) para crear una conexión a tu [Bitbucket](#) [GitHub](#), [GitHub Enterprise Server](#) o [AzureDevOps](#) repositorio. [GitLab](#)
4. Copia el nombre de recurso de Amazon (ARN) de la conexión que has creado.
5. Vuelva a AWS Transformar y pegue el ARN de la conexión que creó.
6. Introduzca un nombre para el conector.

 Note

No introduzca información personal como parte del nombre del conector.

7. Seleccione Iniciar la creación del conector.
8. AWS Transform solicita la creación de un conector para la AWS cuenta que ha introducido, en la misma región que la tarea de transformación actual, y le notifica que la solicitud de aprobación está lista para ser aprobada por el AWS administrador en la consola AWS de administración. Seleccione Copiar el enlace de verificación.
9. Si eres el AWS administrador, inicia sesión en la AWS cuenta y ve al enlace de verificación para aprobar la solicitud de conexión. Si no eres el AWS administrador, proporciona el enlace de verificación a tu AWS administrador.
10. Una vez que el AWS administrador apruebe la solicitud de conector, seleccione Finalizar el conector para completar el proceso de creación del conector. Si desea utilizar un conector diferente, seleccione Reiniciar para reiniciar el proceso de creación del conector.

La pestaña Colaboración también incluye detalles sobre el conector, entre los que se incluyen:

- Estado: aprobado o pendiente de aprobación
- AWS ID de cuenta
- AWS Región
- Conexión ARN

Eliminar un conector existente

 Note

Si ya tiene un conector de repositorio de código fuente, AWS Transform se lo notificará. Seleccione Usar un conector existente o Eliminar y crear un conector nuevo.

Si eliges eliminar una conexión al repositorio de código fuente existente, AWS Transform te avisará antes de eliminar realmente el conector.

1. Puedes eliminar un conector existente de dos maneras:

- a. Si AWS Transform se lo pide, puede seleccionar Eliminar y crear un conector nuevo.
 - b. También puede seleccionar reiniciar en el mensaje. Para modificar este conector, debe reiniciar.
2. AWS Transform le avisa de que al reiniciar se eliminará el conector. Para eliminar el conector, selecciona Reiniciar de nuevo.
 3. AWS Transform te vuelve a avisar de que al eliminar el conector se eliminará la conexión a tu repositorio de terceros, como Bitbucket GitHub, y GitLab. Además, cualquier trabajo de AWS Transform que utilice este conector fallará si se elimina el conector. Para confirmar la eliminación, escriba delete y seleccione Delete.
 4. Para añadir un nuevo conector de repositorio de código fuente, consulte [Añadir un conector nuevo](#).

Conéctese al código fuente en Amazon S3

Puede conectar AWS Transform al código fuente en Amazon S3 como alternativa a [conectar un repositorio de código fuente](#).

Organización de cubos de S3

El código fuente original y el código transformado se almacenan en un depósito de S3 común, organizado como se muestra a continuación. Debe configurar su bucket de S3 en la misma región que su trabajo de AWS Transform. Sube tu código fuente al depósito como un archivo zip a nivel raíz. El archivo zip debe contener una carpeta de nivel superior para cada repositorio.

Durante la transformación, AWS Transform crea una carpeta de salida de la transformación y almacena los resultados de la transformación en esa carpeta. La transformación crea un archivo zip denominado transformed-code.zip que contiene el código transformado. Esto incluye un informe de diferencias de código denominado diff.txt que resalta los cambios en los archivos a nivel de proyecto.

```
<customer-bucket>/
### source-code.zip
    ### repo 1
    ### repo 2
    ### .....
    ### repo n
### transform-output/
    ### transformed-code.zip
```

Añadir un nuevo conector S3

Para crear un nuevo conector de repositorio de código fuente de S3:

1. En la AWS consola, cree un bucket de S3.
2. Cargue el código fuente como un archivo zip en el bucket de S3.
3. En la aplicación web AWS Transform, inicie un trabajo de transformación de.NET. En el paso Conectar un repositorio de código fuente, selecciona Conectar tu código fuente en un bucket S3 y selecciona Guardar.
4. En la página siguiente, introduce los detalles de tu bucket de S3 y selecciona Enviar.
 - a. Nombre del conector
 - b. AWS ID de cuenta
 - c. S3 Bucket Arn
 - d. Clave de cifrado de S3 Bucket (opcional)
5. Apruebe el conector:
 - a. En la página siguiente, copia el enlace de verificación.
 - b. Pida a un aprobador que busque el enlace para acceder a la página de solicitud de creación del conector AWS Transform.
 - c. Elija crear un rol nuevo o usar uno existente.
 - d. Tras revisar la solicitud, selecciona Guardar y aprobar para aprobarla.
6. Especifique la ubicación del archivo zip de S3:
 - a. En la aplicación web AWS Transform, espere a que el estado muestre Aprobado.
 - b. En la página Especificar la ubicación del activo, introduzca una URL de S3 para el archivo de código zip en el formato `s3://bucket-name/zip-file-name` y seleccione Enviar a AWS transformación.
 - c. El trabajo continúa con la etapa de descubrimiento para continuar con la transformación.

Eliminar un conector S3

Para eliminar un conector S3 existente:

1. En la aplicación web AWS Transform, selecciona Administrar conectores en la parte superior derecha.
2. En la ventana Administrar conectores, seleccione el conector.

3. Elija Eliminar.

Confirme sus repositorios para prepararse para la transformación

Después [Crear un conector para el repositorio de código fuente](#), confirme sus repositorios como primer paso para prepararse para la transformación. Puedes:

- Revisar y cambiar [Configuración predeterminada](#) los que afecten al contenido del plan.
- Revise los repositorios descubiertos y seleccione cuáles desea evaluar para su transformación.
- Revisa el [informe de evaluación del repositorio](#) y conversa con AWS Transform sobre su contenido.
- [Utilice el plan generado por AWS Transformar](#).
- [Personalice el plan de transformación](#) utilizando la aplicación web o descargando un archivo JSON, modificándolo y subiéndolo a AWS Transform.

Configuración predeterminada

En la sección Detalles del trabajo de la pestaña Colaboración, puede configurar lo siguiente:

En la pestaña Tareas, en el paso Preparar para la transformación: confirmar los repositorios que se van a transformar, puede configurar lo siguiente:

- Defina el nombre de la rama de destino donde se escribe el código transformado en su repositorio.
- Establezca la versión de .NET de destino:
 - .NET 8: transforma todos los proyectos a .NET 8
 - .NET 10: transforma todos los proyectos a .NET 10
- Puede actualizar la configuración de trabajo predeterminada o dejarla como está. Entre ellos se incluyen:
 - Excluir los proyectos de .NET Standard del plan de transformación Esta configuración está seleccionada de forma predeterminada. Cuando se selecciona, AWS Transform excluye cualquier proyecto de .NET Standard del plan de transformación. Si deselecciona esta configuración, los proyectos de .NET Standard se transformarán, lo que hará que dejen de ser compatibles con .NET Framework.
 - Compruebe las NuGet fuentes y obtenga las versiones de los paquetes compatibles con .NET. Permita que AWS Transform busque y obtenga versiones de paquetes compatibles con .NET para el código que desea transformar.

Revise el informe de evaluación del repositorio

El informe de evaluación del repositorio proporciona una vista tabular de la información sobre cada repositorio detectado por AWS Transform. Esto incluye:

- Propietario del repositorio
- Sucursal evaluada
- N° de soluciones
- N° de proyectos
- Total de líneas de código
- Versiones de .NET detectadas
- Tipos de proyectos detectados
- Número de dependencias privadas de Nuget
- Número de dependencias de Nuget públicas
- Complejidad de transformación

Para descargar el archivo:

1. En su espacio de trabajo, seleccione la pestaña Colaboración.
2. En el panel Elegir repositorios, selecciona Descargar y elige Descargar como HTML o Descargar como JSON

Hable sobre el informe resumido del repositorio

El resumen de tu repositorio puede ser muy largo. Usa el chat para entender mejor su contenido. Su informe estará disponible para el chat cuando vea este mensaje en la pestaña Registro de trabajo: el informe de evaluación ahora está disponible en el chat para consultas. Para abrir el chat, haz clic en el icono hexagonal morado situado en la esquina inferior derecha de la consola web. Estos son algunos ejemplos de instrucciones:

- Enumere todos los repositorios descubiertos o evaluados.
- ¿Cuántos proyectos de .NET 6 se descubrieron en la evaluación?
- ¿Qué proyectos tienen la mayor complejidad?

Utilice el plan generado por AWS Transform

Puede optar por utilizar el plan AWS Transform, creado a partir de la detección de repositorios con una mayor probabilidad de éxito de la transformación, que incluye los repositorios modificados por última vez, los repositorios raíz y los dependientes entre sí.

AWS Transform enumera algunos detalles de alto nivel sobre el plan de transformación, entre los que se incluyen:

- **Número total de repositorios descubiertos** Este número de repositorios .NET antiguos que AWS Transform descubrió mediante el conector de repositorio de código fuente. AWS Transform puede escanear un máximo de 1000 repositorios en cada trabajo. Si tiene más repositorios que escanear o transformar, puede crear varios trabajos de transformación.
- **Repositorios seleccionados** El número de repositorios de .NET antiguos que AWS Transform seleccionó para su transformación.
- **Dependencias seleccionadas** La cantidad de dependencias que requieren los repositorios seleccionados, que AWS Transform detectó automáticamente y agregó al plan de transformación.

La tabla de repositorios seleccionados muestra los repositorios seleccionados. Puede buscar repositorios por nombre, navegar a páginas adicionales de los repositorios y descargar un archivo con formato JSON que muestre los repositorios seleccionados y sus dependencias. Puedes realizar cualquier cambio en esta vista.

En la tabla Repositorios seleccionados se muestran los siguientes detalles sobre los repositorios que AWS Transform ha seleccionado para su transformación:

- Nombre del repositorio
- Ramificación de origen
- Fecha y hora de la última modificación
- Líneas de código: esto te permite ver si te estás acercando a los límites de tu cuota. Para obtener más información, consulte [Cuotas para AWS Transform](#).
- Repositorios dependientes Puedes hacer clic en el número de repositorios dependientes para ver más detalles sobre estas dependencias.

Si está satisfecho con el plan de transformación generado por AWS Transform, seleccione Confirmar repositorios.

Si desea realizar cambios en el plan de transformación generado por AWS Transform, seleccione [Personalice el plan de transformación](#).

Personalice el plan de transformación

Si decide no hacerlo [Utilice el plan generado por AWS Transform](#), puede personalizar la lista de repositorios que desea transformar mediante una de las siguientes opciones:

1. Seleccione los repositorios en la tabla Repositorios seleccionados.
 - a. Al añadir un repositorio al plan, AWS Transform seleccionará automáticamente las dependencias del repositorio y las añadirá automáticamente al plan de transformación.
 - b. También puedes deseleccionar los repositorios de la tabla.
2. Descarga la lista JSON de repositorios y ramas generada por AWS Transform.
 - a. Selecciona Descargar y, a continuación, selecciona Descargar como JSON.
 - b. Revisa y modifica el JSON. Puedes eliminar repositorios, o soluciones dentro de los repositorios, que no quieras transformar.
 - c. Para cargar el JSON revisado, selecciona Cargar un plan personalizado.
 - d. Si el JSON se carga correctamente, en la tabla Repositorios seleccionados se muestran las selecciones que has realizado.
3. Puede seleccionar Mostrar repositorios dependientes para mostrar la lista de repositorios que AWS Transform descubrió que eran dependencias de los repositorios que seleccionó.
4. Puedes repetir estos pasos si es necesario. Cuando esté satisfecho con su plan personalizado, seleccione Confirmar repositorios.

Resolver las dependencias de los paquetes para prepararse para la transformación

Después [Confirme sus repositorios para prepararse para la transformación](#), si AWS Transform encuentra las dependencias de paquetes que faltan, debes completar este paso. Puede ejecutar un PowerShell script de Windows para obtener las dependencias de paquetes que faltan desde el mismo dispositivo que su entorno de Visual Studio desarrollo, o puede recuperar los paquetes que faltan manualmente. A continuación, cargue los paquetes que faltan.

Las dependencias del paquete que faltan se pueden actualizar de dos maneras:

- Resolver mediante Artifact Connector: Resuelva configurando un repositorio de artefactos (NuGet conector ADO) mediante un flujo de trabajo HITL dedicado a Connect Artifact Repository, que se muestra cuando no se ha configurado un Artifact Connector y faltan paquetes.

- Actualizar el paquete faltante: AWS Transform muestra los paquetes que faltan en la tabla de dependencias de paquetes faltantes. Puedes buscar un paquete faltante por su nombre en el cuadro de búsqueda. Esta tabla incluye los siguientes detalles sobre los paquetes que faltan:
 - Name
 - Repositorios asociados
 - Estado de la versión del marco
 - Estado de la versión principal

Para resolver las dependencias del paquete que faltan, [Cargue los paquetes que faltan](#).

Cargue los paquetes que faltan

1. Si lo desea, puede descargar un script PowerShell auxiliar de Windows para recuperar las dependencias de paquetes que faltan desde su entorno de Visual Studio desarrollo. O bien, puede encontrar los paquetes que faltan manualmente.

Para usar el PowerShell script de Windows:

- a. Selecciona Descargar el PowerShell script de Windows.
 - b. Ejecute el script localmente con una conexión activa a los repositorios que contienen los archivos de dependencia del paquete que faltan.
 - c. Este script le permite descargar las dependencias de paquetes que faltan a su entorno local.
2. El script creará un único archivo zip para que lo cargue, que incluye todas las dependencias en un solo archivo. También puede cargar archivos individuales .nupkg o zip para cada dependencia.
 3. Selecciona Cargar archivos de paquete.
 4. En el modal Cargar archivos dependientes, selecciona Elegir archivos y busca la ubicación de los archivos de paquete comprimidos que faltan en tu dispositivo.
 5. Selecciona Cargar.
 6. AWS Transformar valida los archivos que has subido. Durante la validación, no puede realizar ninguna actualización. AWS Transform indica el estado de la validación por encima de la tabla de dependencias de paquetes faltantes.
 7. AWS Transform también actualiza las columnas de estado de la tabla de dependencias de paquetes faltantes, pasando de Falta a Resuelto. Si un paquete no pasa la validación, su estado pasa a ser inválido. En el caso de los archivos no válidos, haga lo siguiente:

- a. En la tabla de dependencias de paquetes faltantes, seleccione el paquete no válido mediante la casilla de verificación.
 - b. Seleccione Eliminar el archivo cargado.
 - c. Esto cambiará su estado de nuevo a Falta.
8. Una vez que haya cargado los paquetes que faltan y haya resuelto las dependencias entre los paquetes, seleccione Proceder a la revisión.

Si selecciona Continuar con la revisión sin resolver las dependencias de los paquetes que faltan, AWS Transform le preguntará si desea iniciar el trabajo de transformación sin los paquetes que faltan. Si selecciona Ignorar las dependencias del paquete que faltan, AWS Transform utilizará referencias de ensamblaje para transformar el código. Continuar con esta acción puede afectar a los recursos relacionados.

Requisitos de estructura de carpetas

Para las NuGet cargas, AWS Transform requiere:

- El .nuspec archivo que se debe colocar en el nivel raíz en el caso de los paquetes cargados manualmente, o
- Uso del PowerShell script proporcionado para generar la estructura correcta

Requisitos de coincidencia de versiones

- Estado del marco: la AWS transformación intenta hacer coincidir la versión de la dependencia especificada en el .csproj archivo (código fuente) con la versión de la dependencia cargada. Una coincidencia exacta da como resultado un estado correcto.
- Estado principal: AWS Transform espera una especificación de la versión básica en la sección de dependencias del .nuspec archivo cargado. Si se encuentra una, el estado principal es Éxito.

Formato de ejemplo:

```
<dependencies>
  <group targetFramework="net8.0" />
</dependencies>
```

Las versiones más comunes incluyen:

- .NET 5.0 (net5.0)

- .NET 6.0 (net6.0)
- .NET 7.0 (net7.0)
- .NET 8.0 (net8.0)

Revisar su plan para prepararse para la transformación

Después [Confirme sus repositorios para prepararse para la transformación](#), y después [Resolver las dependencias de los paquetes para prepararse para la transformación](#), el administrador de la AWS cuenta debe revisar el plan de transformación y aprobarlo en AWS Transform.

AWS Transform muestra la lista de repositorios, repositorios dependientes y paquetes dependientes de la tarea que se seleccionaron para la transformación.

Revisar el plan de transformación

AWS Transform muestra la lista de repositorios, repositorios dependientes y paquetes dependientes del trabajo que se seleccionaron para la transformación.

Note

AWS Transform puede transformar un máximo de 100 dependencias y repositorios por plan de transformación.

1. Si no es el administrador de la AWS cuenta, revise el plan de trabajo y, si lo acepta, seleccione **Enviar** para su aprobación.
2. Si es el administrador de la AWS cuenta, debe revisar el plan y, cuando esté listo, aprobarlo para iniciar la transformación. Tras revisar el plan de trabajo, seleccione una de las siguientes opciones:
 - a. Rechazar Si el trabajo lo creó un usuario que no es el administrador de la AWS cuenta, le sugerimos que notifique al creador del trabajo para que lo reinicie.
 - b. Apruebe e inicie la transformación.

La revisión del trabajo incluye los siguientes detalles:

1. Resumen del trabajo Esto incluye:
 - a. La rama de destino donde AWS Transform colocará el código transformado.

- b. La versión de .NET de destino, .NET 8.0 o .NET 10.
 - c. La configuración del trabajo:
 - i. Excluya los proyectos estándar de .NET
 - d. Número de repositorios seleccionados para la transformación
 - e. Número de repositorios dependientes
 - f. Número de paquetes privados NuGet
 - g. Número total de líneas de código para el trabajo
2. Repositorios seleccionados Estos son los repositorios seleccionados para la transformación. Deben ser paquetes MVC, Web, Windows Communication Foundation (WCF), Console, biblioteca de clases, marco de interfaz de usuario (Razor pages) o paquetes de pruebas unitarias. Esta tabla incluye la siguiente información:
- a. Name
 - b. Ramificación de origen
 - c. Proyectos compatibles
 - d. Líneas de código
 - e. Proyectos detectados
 - f. Proyectos omitidos
 - g. Dependencias detectadas
3. Repositorios dependientes agregados Estos son los repositorios dependientes agregados para la transformación. Deben ser paquetes MVC, Web, Windows Communication Foundation (WCF), Console, biblioteca de clases, marco de interfaz de usuario (Razor pages) o paquetes de pruebas unitarias. Esta tabla incluye la siguiente información:
- a. Name
 - b. Necesario para
 - c. Ramificación de origen
 - d. Proyectos apoyados
 - e. Líneas de código
 - f. Proyectos detectados
 - g. Proyectos omitidos
4. Paquetes dependientes Estos son los paquetes dependientes que se agregaron para la transformación. Deben ser paquetes MVC, Web, Windows Communication Foundation (WCF),

Console, biblioteca de clases, marco de interfaz de usuario (Razor pages) o paquetes de pruebas unitarias. Esta tabla incluye la siguiente información:

- a. Name
- b. Repositorios asociados
- c. Estado de la versión del marco
- d. Estado de la versión principal

Transformando su código.NET

Cuando el administrador de la AWS cuenta finalice [Revisar su plan para prepararse para la transformación](#), podrá ver el progreso de la transformación en la pestaña Panel de control de su trabajo de transformación.

Note

Además de transformar los repositorios y las dependencias, AWS Transform puede ejecutar proyectos de pruebas unitarias completamente transformados (sin errores de compilación). AWS Transform no tiene acceso a los resultados de las pruebas unitarias anteriores a la transformación y solo puede compartir los resultados posteriores a la transformación. A continuación, puede comparar los datos de referencia, antes de la transformación, con los resultados posteriores a la transformación para comprender las posibles brechas.

En la esquina superior derecha, puedes ver el estado del trabajo, que tiene uno de los siguientes valores:

- Esperando la entrada del usuario
- Tiempo transcurrido
- Ejecutar

También puedes ver los siguientes íconos:

- Un icono de detener la transformación
- Un icono de actualización
- Un icono de configuración

El panel de control proporciona un resumen de alto nivel de la transformación. Muestra métricas del número de trabajos transformados y de transformación aplicada, así como el tiempo estimado para completar la transformación.

El panel de control incluye:

1. La sección Detalles del trabajo de transformación, que muestra la configuración y los detalles predeterminados del trabajo de transformación, que incluyen:
 - a. Destino de la rama de destino Para AWS transformar el código, Transform crea una nueva rama para el código transformado en el repositorio de código.
 - b. Versión de destino de .NET, .NET 8.0 o .NET 10
 - c. El ID del trabajo de AWS Transform.
 - d. La configuración del trabajo:
 - i. Excluya los proyectos estándar de .NET
2. La sección de resumen de la transformación contiene:
 - a. El número de repositorios seleccionados para la transformación
 - b. El número de proyectos que se van a transformar
 - c. El total de líneas de códigos de estos repositorios y proyectos

Una vez iniciada la transformación, aparecen gráficos circulares en las secciones Estado del Repositorio, Estado del Paquete y Estado de la prueba unitaria que muestran el progreso en tiempo real. El estado de las pruebas unitarias muestra el estado de las pruebas unitarias ubicadas en tus repositorios y que AWS Transforms ejecuta tras la transformación para probar el código transformado. AWS Transform comparte los resultados de las pruebas ejecutadas, junto con el nombre de cada prueba individual, para que los clientes revisen la lista de pruebas unitarias aprobadas y no aprobadas.

 Note

En la sección Repositorios se enumeran los repositorios que AWS Transform recomienda o que seleccionaste para la transformación. Selecciona Descargar JSON para descargar una lista de los repositorios, dependencias y paquetes de tu plan de transformación.

Revisa los informes de transformación

Una vez finalizado un trabajo de transformación, puede descargar [los informes de transformación](#):

- [Informe resumido de la transformación](#): este informe proporciona una descripción general de la transformación en formato HTML o JSON. Descargue el informe resumido de la transformación desde la pestaña Panel de control. Seleccione Descargar y elija Descargar como HTML o Descargar como JSON.
- [Informe detallado de la transformación](#): este informe proporciona información detallada sobre una transformación en formato HTML. Descargue los informes detallados de la transformación desde la pestaña Panel de control. Seleccione el enlace Descargar un informe detallado en la lista de repositorios para descargar un informe detallado.

Chatea con AWS Transforme sobre el informe de transformación

Puede conversar con AWS Transform sobre el informe de transformación una vez que un repositorio se haya procesado por completo o una vez que se haya completado el trabajo de transformación. La pestaña Registro de trabajo muestra este mensaje para cada repositorio disponible para el chat: los detalles de la *repository_name* transformación del repositorio ahora están disponibles en el chat para consultas. Muestra este mensaje cuando se completa el trabajo de transformación: El trabajo de AWS transformación se ha completado.

Para abrir el chat, haga clic en el icono hexagonal morado situado en la esquina inferior derecha de la consola web.

Estos son algunos ejemplos de instrucciones:

- ¿Qué proyectos se transformaron con éxito?
- ¿Qué proyectos se transfirieron parcialmente?
- ¿Qué cambios se realizaron en el `repo_name` repositorio?
- ¿Qué paquetes se actualizaron en el `project_name` proyecto?

Modernizar .NET en el IDE

AWS Transform incluye un asistente de IA interactivo y agencial en el AWS kit de herramientas para Visual Studio. Le permite modernizar las aplicaciones a través de una experiencia conversacional guiada paso a paso directamente en su IDE. Para transformar una solución o un proyecto de .NET, el

agente AWS Transform analiza el código base, determina las actualizaciones necesarias para migrar la aplicación y genera un informe de evaluación y un plan de transformación antes de que comience la transformación.

La experiencia Visual Studio IDE solo admite la autenticación mediante el IAM Identity Center. Para obtener más información, consulte [Adición de usuarios en el Centro de identidades de IAM](#).

La experiencia IDE ofrece modos autónomos e interactivos. Utilice el modo autónomo para una transformación desatendida, adecuado para trabajos nocturnos o de larga duración. Utilice el modo interactivo para trabajar junto al agente en el chat, con una alta visibilidad de la transformación, un plan de transformación personalizable y una revisión paso a paso de cada proyecto. Puede realizar iteraciones para refinar los resultados o cambiar de dirección hasta quedar satisfecho.

Cuando un trabajo de transformación está activo, puede interactuar con tres ventanas:

- La ventana de chat es su principal punto de interacción con el agente de transformación. Utilice el chat para hacer preguntas, analizar opciones, dirigir la transformación e iterar.
- La ventana AWS Transform Job Plan muestra los pasos de progreso y es donde puede descargar o cargar artefactos o ver las diferencias en los cambios de código.
- La ventana del registro de trabajo muestra un registro de la actividad de transformación en lenguaje natural.

AWS Transform realiza cuatro tareas clave para portar aplicaciones.NET a Linux:

- Actualiza las versiones de .NET y de otros idiomas: actualiza el código C# antiguo de .NET a las versiones actuales de .NET y otros idiomas.
- Migra de .NET Framework a .NET multiplataforma: migra proyectos y paquetes de .NET Framework que depende de Windows a .NET multiplataforma compatible con Linux.
- Reescribe el código para que sea compatible con Linux: refactoriza y reescribe los componentes de código obsoletos e ineficientes.
- Genera un informe de compatibilidad con Linux: en el caso de las tareas abiertas en las que es necesaria la intervención del usuario para compilar y ejecutar el código en Linux, AWS Transform proporciona un informe detallado de las acciones necesarias para configurar la aplicación tras la transformación.

Para obtener más información sobre cómo AWS Transform realiza las transformaciones de .NET, consulte [Cómo AWS Transform moderniza las aplicaciones.NET](#).

Para modernizar su código.NET mediante AWS Transform from Visual Studio IDE, consulte lo siguiente:

- [Modernizar .NET mediante AWS Transfórmese en Visual Studio](#)
- [Cómo AWS Transform moderniza las aplicaciones.NET](#)
- [Solución de problemas relacionados con las transformaciones de .NET en el IDE](#)

Cuotas

Para ver las cuotas de transformación de AWS Transform.NET en el IDE, consulte [Cuotas para AWS Transformar](#).

Modernizar .NET mediante AWS Transfórmese en Visual Studio

Complete estos pasos para migrar una Windows-based aplicación.NET a una aplicación .NET Linux-compatible multiplataforma con AWS Transform en Visual Studio 2026 o 2022.

Paso 1: requisitos previos

Antes de continuar, asegúrese de haber descargado e instalado la [extensión AWS Toolkit con Amazon Q](#) desde Visual Studio Marketplace. Revise las [capacidades](#) y [limitaciones](#) de AWS Transform para la modernización de .NET para confirmar que su código se puede transformar.

Paso 2: Autenticarse en Visual Studio

Para conectarse a sus AWS cuentas desde el Toolkit for Visual Studio, abra la interfaz de usuario Getting Started with AWS the Toolkit (interfaz de usuario de conexión):

1. En el menú principal de Visual Studio, vaya a Extensiones > AWS Kit de herramientas > Introducción para abrir la página Introducción: AWS kit de herramientas.
2. Seleccione AWS Transformar la autenticación.
3. Elige un perfil existente o crea uno nuevo. Al crear un perfil nuevo, introduzca un nombre para el perfil y la URL de inicio de AWS Transform, que se le envió por correo electrónico después de que su administrador lo añadiera al Centro de Identidad de IAM.
4. Elija Conectar. Siga las instrucciones para iniciar sesión y conceder permisos de acceso a través de su navegador web. En Visual Studio, debería ver Connected with IAM Identity Center.
5. Tras iniciar sesión, accederá al panel de control de AWS transformación. Desde esta página de inicio, puede hacer lo siguiente:

- Seleccione un perfil de AWS Transform (región)
- Seleccione o cree un espacio de trabajo
- Vea el estado de los trabajos de transformación

Paso 3: Transforma tu aplicación

Para transformar su proyecto o su solución .NET, realice el procedimiento que se muestra a continuación:

Comience la transformación

1. Abra cualquier solución o proyecto VB.NET basado en C# Visual Studio que desee transformar.
2. En el Explorador de soluciones, haga clic con el botón derecho en la solución o proyecto que desee transformar y elija Port with AWS Transform.
3. Aparece el cuadro de diálogo Puerto con AWS transformación.
 - a. En el menú desplegable Elegir un espacio de trabajo, cree un espacio de trabajo o seleccione uno existente. Los espacios de trabajo hacen que tu actividad sea visible en la aplicación web AWS Transform, donde puedes invitar a colaboradores a ver los trabajos de transformación y a conversar sobre ellos.
 - b. En el menú desplegable Elegir un destino de .NET, elija la versión de .NET a la que desee actualizar.
 - c. En el modo de transformación, selecciona Autónomo para una transformación desatendida o Interactivo para una transformación interactiva.
 - d. Seleccione Iniciar para iniciar la transformación.
4. Una vez que se inicie el trabajo de transformación, aparecerán las ventanas AWS Transform Job Plan, Chat y Worklog.

Plan de evaluación y transformación

1. Una vez que AWS Transform analiza el código, se muestran en el chat un informe de evaluación y un plan de transformación. En el modo interactivo, el chat se detendrá para que los revise. Si prefieres no opinar en el chat, puedes usar estas alternativas:
 - Para ver la evaluación o el plan en el editor de código, seleccione Mostrar evaluación o Mostrar plan de transformación en la ventana AWS Transformar el plan de trabajo.

- Para descargar la evaluación o el plan, utilice el icono de descarga de la ventana Job Plan.
- 2. Si lo desea, modifique el plan de transformación. Puede hablar del plan a través del chat, por ejemplo, explorando otras opciones. Los cambios de plan se realizan dando instrucciones en el chat o subiendo un plan de transformación revisado mediante el icono de descarga de la ventana Job Plan. Puede añadir, eliminar o modificar los pasos libremente. Chat confirmará que entiende tus instrucciones con un plan revisado.
- 3. Si lo desea, cargue los documentos de dirección. En la ventana de chat, utilice el icono de carga para cargar documentos de dirección, como las especificaciones de la solicitud, las preferencias y convenciones técnicas de la organización o ejemplos de codificación. Después de subir un documento de orientación, descríbelo en la ventana de chat para darle un contexto al agente.
- 4. Una vez que esté satisfecho con el plan, dé su aprobación en el chat y comenzará la transformación.
- 5. En el modo interactivo, puede configurar los puntos de control para que se detengan después de transformar un proyecto para su revisión. Los pasos de Transformar el código en la ventana Job Plan tendrán iconos de puntos de control redondos. Todos los proyectos tienen los puntos de control activados de forma predeterminada. Utilice las casillas de verificación para desactivar o establecer un punto de control.

Revisiones de transformación y puntos de control

1. AWS Transform comienza a transformar su código. Puede supervisar el progreso de los pasos de transformación en la ventana AWS Transform Job Plan. La ventana Plan de Trabajo muestra el tiempo máximo estimado restante y su ID de trabajo.
2. A medida que se transforman los proyectos, se muestran los resúmenes en el chat y se aplican los cambios de código.
3. En el modo interactivo, cuando se llega a un punto de control, el agente hace una pausa para que puedas revisar los resultados. En la ventana Job Plan, verá el botón Ver resultados para el paso en el que está pausado, donde podrá revisar las diferencias de código. Tras revisar los cambios, puedes solicitar más cambios en el chat o hacer cambios en el código tú mismo. Visual Studio
4. Puedes repetir en el punto de control tantas veces como desees. Cuando estés satisfecho, indica al chat que continúe y pasará al siguiente proyecto.

Fin de la transformación

1. Tras transformar sus proyectos, el agente.NET activará una compilación local para confirmar que el código se ha compilado correctamente en su máquina local. Visual Studio Si hay errores, se ocupará de resolverlos.
2. Una vez completada la transformación, es posible que se necesiten pasos adicionales, como tareas de transformación que AWS Transform no pudo realizar o cambios necesarios para garantizar la compatibilidad con Linux. Se puede descargar un archivo de anotaciones sobre los siguientes pasos (NextSteps.md), que puede utilizar como instrucciones para complementar el código de IA. Utilice el botón de descarga de la ventana Job Plan para descargar NextSteps.md.
3. Puede seguir interactuando en el chat para hacer preguntas o solicitar cambios adicionales.
4. Informe al chat cuando esté listo para finalizar su trabajo de transformación.

Cómo AWS Transform moderniza las aplicaciones.NET

Consulte las siguientes secciones para obtener detalles sobre cómo funciona la transformación de.NET con AWS Transform.

Análisis de su aplicación y generación de un plan de transformación

Antes de que comience una transformación, AWS Transform crea el código localmente para comprobar que se puede compilar y que está configurado correctamente para la transformación. Si el código no se compila, AWS Transform preguntará si desea continuar con la transformación. AWS Luego, Transform carga el código en un entorno de compilación seguro y cifrado AWS, analiza el código base y determina las actualizaciones necesarias para portar la aplicación

Durante este análisis, AWS Transform divide la solución o el proyecto de.NET en grupos de códigos. Un grupo de códigos es un proyecto y todas sus dependencias que, en conjunto, generan una unidad de código que se puede compilar, como una biblioteca de enlaces dinámicos (DLL) o un ejecutable. Incluso si no seleccionó todas las dependencias del proyecto para transformarlas, AWS Transform determina las dependencias necesarias para crear los proyectos seleccionados y las transforma también, de modo que la aplicación transformada se pueda compilar y esté lista para su uso.

Tras analizar el código, AWS Transform genera un plan de transformación en el que se describen los cambios propuestos que realizará, incluida una lista de los grupos de códigos y sus dependencias que se transformarán.

Transformación de su aplicación

Para iniciar la transformación, AWS Transform vuelve a compilar el código en un entorno de compilación seguro para comprobar si se puede compilar de forma remota. AWS Luego, Transform comienza a portar la aplicación. Funciona de abajo hacia arriba, comenzando con la dependencia de nivel más bajo. Si AWS Transform tiene un problema con la migración de una dependencia, detiene la transformación y proporciona información sobre la causa del error.

La transformación incluye las siguientes actualizaciones en su aplicación:

- Sustituir las versiones anticuadas del código de C# por versiones de Linux-compatible C#
- Actualización de .NET Framework a .NET multiplataforma, lo que incluye:
 - Identificación y reemplazo de paquetes, bibliotecas y API de forma iterativa
 - Actualización y reemplazo de NuGet paquetes y API
 - Transición a un tiempo de ejecución multiplataformas
 - Configuración del middleware y actualización de las configuraciones de tiempo de ejecución
 - Sustitución de paquetes privados o externos
 - Gestión de componentes de IIS y WCF
 - Depuración de errores de compilación
- Reescritura de código para que sea compatible con Linux, incluida la refactorización y la reescritura del código obsoleto e ineficiente para portar el código existente

Revisar el informe de transformación y aceptar los cambios

Una vez completada la transformación, AWS Transform proporciona un informe de transformación con información sobre las actualizaciones propuestas que ha realizado en la aplicación, incluida la cantidad de archivos modificados, paquetes actualizados y API cambiadas. Indica cualquier transformación fallida, incluidos los archivos afectados o las partes de los archivos y los errores detectados durante un intento de compilación. También puede ver un resumen de la compilación con los registros de la compilación para obtener más información sobre los cambios que se han realizado.

El informe de transformación también proporciona el estado de la migración a Linux, que indica si es necesaria o no la intervención adicional del usuario para que la aplicación sea compatible con Linux. Si alguno de los elementos de un grupo de códigos requiere que introduzcas información, descarga un informe de preparación para Linux que contiene Windows-specific consideraciones que AWS Transform no pudo abordar en el momento de la compilación. Si se necesita intervención para algún

grupo de códigos o archivos, revise el informe para obtener más detalles sobre el tipo de cambio que aún debe realizarse y, si procede, para obtener recomendaciones sobre cómo actualizar el código. Estos cambios deben realizarse manualmente antes de que la aplicación se pueda ejecutar en Linux.

Puede revisar los cambios propuestos por AWS Transform en una vista de diferencias antes de aceptarlos como actualizaciones internas de sus archivos. Tras actualizar los archivos y abordar cualquier elemento del informe de preparación para Linux, la aplicación estará lista para ejecutarse en .NET multiplataforma.

Puedes descargar un archivo de rebajas de Next Steps con indicaciones para continuar con la transformación con AWS Transform o un código complementario de IA. Para descargar el archivo, pulsa el botón Descargar los próximos pasos en la parte superior derecha del informe.

Solución de problemas relacionados con las transformaciones de .NET en el IDE

Utilice las siguientes secciones para solucionar problemas comunes relacionados con las transformaciones de .NET en el IDE con AWS Transform.

¿Cómo puedo saber si un trabajo está progresando?

Debería ver la actividad habitual en la ventana del registro de trabajo. Si parece que AWS Transform dedica mucho tiempo a un paso de la ventana AWS Transform Job Plan, puede comprobar si el trabajo sigue activo en los registros de salida. Si se están generando mensajes de diagnóstico, el trabajo sigue activo.

Para comprobar los resultados, seleccione la pestaña Salida en Visual Studio. En el menú Mostrar resultado de:, elija Amazon Q Language Client.

La siguiente captura de pantalla muestra un ejemplo de las salidas que AWS Transform genera durante una transformación.

```

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: ("transformationJobId":"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: [2024-07-29T22:25:10.039Z] aws/dotnetTransform/getTransform
Info: [2024-07-29T22:25:10.039Z] Calling getTransform request with Job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:25:10.039Z] 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: ("transformationJobId":"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 qué algunos proyectos no se seleccionan para la transformación?

AWS Transform solo puede transformar los tipos de proyectos de .NET compatibles. Para obtener una lista de los tipos de proyectos compatibles y otros requisitos previos para transformar sus proyectos de .NET, consulte [Paso 1: requisitos previos](#).

¿Cómo puedo obtener asistencia si mi proyecto o solución no se está transformando?

Si no puedes solucionar los problemas por tu cuenta, puedes ponerte en contacto con tu Cuenta de AWS equipo para Soporte enviar un caso de soporte.

Para obtener asistencia, proporciona el identificador del trabajo de transformación para que AWS puedas investigar un trabajo fallido. Para buscar un ID de trabajo de transformación, seleccione la pestaña Salida en Visual Studio. En el menú Mostrar resultado de:, elija Amazon Q Language Client.

¿Cómo puedo evitar que mi firewall interfiera con los trabajos de transformación?

Si su organización utiliza un firewall, es posible que esto interfiera con las transformaciones internas Visual Studio. Puede deshabilitar temporalmente los controles de seguridad Node.js para solucionar problemas o probar qué es lo que impide que se ejecute la transformación.

La variable de entorno `NODE_TLS_REJECT_UNAUTHORIZED` controla los controles de seguridad importantes. Si `NODE_TLS_REJECT_UNAUTHORIZED` se establece en «0», se deshabilita el rechazo Node.js de los certificados no autorizados. TLS/SSL Esto significa:

- Self-signed se aceptarán certificados
- Se permitirán los certificados caducados
- Se permitirán los certificados con nombres de host que no coincidan
- Se ignorará cualquier otro error de validación de certificados

Si su proxy usa un autocertificado, puede configurar las siguientes variables de entorno en lugar de deshabilitar `NODE_TLS_REJECT_UNAUTHORIZED`:

```
NODE_OPTIONS = -use-openssl-ca  
NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs
```

De lo contrario, debe especificar los certificados de CA que utiliza el proxy para deshabilitar `NODE_TLS_REJECT_UNAUTHORIZED`.

Para deshabilitar `NODE_TLS_REJECT_UNAUTHORIZED` en Windows:

1. Abra el menú Inicio y busque Variables de entorno.
2. Elija Editar las variables de entorno del sistema.
3. En la ventana Propiedades del sistema, seleccione Variables de entorno.

4. En Variables de sistema, elija Nuevo.
5. Ajuste Nombre de variable en `NODE_TLS_REJECT_UNAUTHORIZED` y Valor de variable en 0.
6. Seleccione Aceptar para guardar los cambios.
7. Reinicie Visual Studio.

Portar código de capa de interfaz de usuario

AWS Transform puede migrar la capa de interfaz de usuario de los ASP.NET sitios web a marcos de interfaz de usuario compatibles con ASP.NET Core, que se pueden ejecutar en Linux. Están disponibles las siguientes transformaciones:

- Portabilidad MVC Razor UI
- Migración de formularios web a Blazor UI

Portabilidad de la interfaz de usuario MVC Razor

ASP.NET Los proyectos de MVC con la interfaz de usuario de Razor Views se pueden portar a MVC Razor Views on ASP.NET Core y permanecer en el mismo marco de interfaz de usuario. Si bien las vistas de Razor son similares entre ASP.NET Core ASP.NET y Razor, existen diferencias que requieren la adaptación de los cambios en el código:

- ASP.NET Las vistas Razor de MVC utilizan el espacio de `System.Web.Mvc` nombres y están estrechamente relacionadas con .NET Framework.
- ASP.NET Los Core Razor Views son modulares, se basan en ellos y cuentan con una inyección de dependencias `Microsoft.AspNetCore.Mvc` mejorada.
- ASP.NET Core cuenta con nuevas funciones, como Tag Helpers y View Components.

AWS Transform detecta y transporta componentes y construcciones incompatibles comunes en Razor Views.

Migración de formularios web a la interfaz de usuario de Blazor

ASP.NET La interfaz de usuario de Web Forms no tiene una contraparte en ASP.NET Core. AWS Transform puede portar el código de la capa de interfaz de usuario de Web Forms al servidor Blazor en ASP.NET Core. El código de la capa de interfaz de usuario se reescribe para el marco de interfaz de usuario de destino.

Para activar o desactivar la migración de formularios web a la interfaz de usuario de Blazor, active o desactive la opción Transformar formularios ASP.NET web de interfaz de usuario a Blazor.

Detalles de la transformación

Su proyecto de Web Forms se convierte en un proyecto de Blazor con alojamiento en el lado del servidor. Durante la transformación, se realizan los siguientes cambios en el proyecto y en el archivo:

Mapeo de transformación de archivos

De	Para	Description (Descripción)
*.aspx, *.ascx	*.maquinilla de afeitador	Las páginas.aspx y los controles personalizados.ascx se convierten en archivos.razor
Web.config	appsettings.json	Web.config los ajustes se convierten en ajustes de appsettings.json
Global.asax	Program.cs	Global.asax el Program.cs código se convierte en código
*.master	*layout.razor	Los archivos maestros se convierten en archivos Layout.razor

Post-transformation estructura del proyecto

Tras la transformación, los archivos transformados residen en las siguientes ubicaciones del proyecto:

- Carpeta de componentes: todos los componentes de Razor (*.razor) se colocan en una carpeta de componentes creada al mismo nivel que el archivo.csproj del proyecto.
- Mapeo de páginas: las páginas de Web Forms (*.aspx) se convierten en una estructura de carpetas. Components/Pages
- Asignación de controles: los controles de los formularios web (*.ascx) se colocan directamente debajo de la carpeta Componentes.

Limitaciones y funciones no compatibles

En la actualidad, no se admiten las siguientes funciones. Si sus cargas de trabajo utilizan estas funciones, será necesario portar ese código manualmente o con un código de IA complementario después de la transformación.

- archivos.svc (archivos de servicio)
- archivos.ashx (archivos de controladores genéricos)
- Referencias de servicios y referencias web (archivos.map, reference.cs, .wsdl)
- Mezclas de archivos.aspx (formularios web) y archivos.cshtml (Razor) en el mismo proyecto
- Transform para .NET aún no admite dependencias de tipos de proyectos AWS
- Third-party interfaz de usuario del proveedor libraries/controls
- Proyectos de sitios web

Solo se admiten los proyectos de aplicaciones web (que contienen un archivo.csproj). Para convertir un proyecto de sitio web en un proyecto de aplicación web, consulte la guía de Microsoft sobre cómo [convertir un proyecto de sitio web en un proyecto de aplicación web](#).

Informes de transformación

Una vez finalizado el trabajo de transformación de .NET, estarán disponibles estos informes de transformación:

- [Informe resumido de la transformación](#)
- [Informe detallado de la transformación](#)

Informe resumido de la transformación

Una vez finalizado un trabajo de transformación, está disponible un informe resumido de la transformación en la consola web. Descargue el informe resumido de la transformación desde la pestaña Panel de control. Seleccione Descargar el informe resumido de la transformación y elija Descargar como HTML o Descargar como JSON.

El informe resumido de la transformación proporciona una descripción general de la transformación e información específica de cada repositorio que se transformó, que incluye:

- Detalles del trabajo

- Descripción general del trabajo de transformación
- Resumen de los resultados de la transformación
- Descripción general de los archivos
- Lista de repositorios y, para cada repositorio:
 - Descripción general del nombre del repositorio
 - Resumen de la transformación de la solución
 - Detalles del proyecto, incluidos el estado, el tipo, la versión.NET, el total de líneas de código, las líneas de código transformadas y los archivos modificados

Informe detallado de la transformación

Una vez finalizado un trabajo de transformación, los informes detallados de la transformación están disponibles para los usuarios de la consola web y del IDE.

- Usuarios de consolas web: hay disponible un informe detallado para cada repositorio transformado. En la pestaña Panel de control, utilice los enlaces Descargar informes detallados de la lista de repositorios para descargar un informe detallado.
- Usuarios del IDE: descarguen el informe de transformación desde la ventana AWS Transform Job Plan mediante el icono de descarga.

El informe detallado de la transformación es un informe HTML interactivo. Contiene información detallada sobre la transformación, incluidos los motivos de los cambios en los archivos y los detalles de los errores procesables. La información se organiza en la siguiente jerarquía:

- Información sobre el trabajo
- Para cada solución:
 - Resumen de la transformación de la solución
 - Descripción general de la transformación
 - Proyectos
 - Para cada proyecto:
 - Resumen del proyecto
 - Resumen de errores de compilación
 - NuGet cambios en el paquete

- Cambios en los archivos
- Errores de compilación
- Resultados de las pruebas unitarias
- Informe de preparación para Linux

Para ver un recorrido por las secciones del informe detallado de la transformación con ejemplos, consulte la entrada del blog [Anunciando los informes detallados de transformación de AWS Transform for .NET](#).

Mejores prácticas para las transformaciones de .NET

Siga esta guía para obtener mejores resultados de modernización de .NET con AWS Transform. Estas prácticas recomendadas se aplican al asistente de IA conversacional de .NET, actualmente disponible para Visual Studio IDE.

Temas

- [Antes de transformarse](#)
- [Evaluación y planificación](#)
- [Transforma de forma interactiva o autónoma](#)
- [Validación y finalización](#)

Antes de transformarse

Revise las siguientes recomendaciones antes de iniciar un trabajo de transformación de .NET.

Utilice el asistente de IA conversacional de .NET

Utilice el nuevo agente .NET para obtener los mejores resultados de transformación. El asistente de IA conversacional está disponible en Visual Studio a través del [AWS Toolkit for Visual Studio](#). También está disponible para [Kiro](#) otros IDE gracias a la tecnología de los agentes Kiro AWS Transform and AWS Transform MCP. El nuevo agente .NET aún no está disponible en la consola web.

Utilice otras herramientas si el objetivo no es la transformación de .NET a .NET

AWS Transform for .NET es adecuado para la modernización del código de .NET Framework para .NET y para las actualizaciones de .NET a versiones posteriores. No es adecuado para transformaciones que incluyen lenguajes ajenos a .NET, como Java, o marcos que no son de .NET,

como React. Tampoco proporciona una refactorización de la arquitectura de las aplicaciones. Utilice [AWS Transform custom](#) o Kiro para esos tipos de modernización.

Utilice una edición estable de Visual Studio, preferiblemente VS2026

Utilice una edición GA de Visual Studio en lugar de una versión preliminar o una edición Insiders para evitar complicaciones derivadas de la previsualización del software. El AWS kit de herramientas se puede utilizar con Visual Studio 2026 o 2022. Se recomienda el VS2026 porque funciona mejor con un consumo de memoria reducido.

Utilice la versión más reciente AWS Kit de herramientas para Visual Studio

Utilice la última versión del AWS kit de herramientas Visual Studio para obtener correcciones de errores y actualizaciones de funciones. Puede comprobar la versión de su kit de herramientas y actualizarla en Extensiones > Administrar extensiones > Instaladas.

Trabaja en Visual Studio IDE para proyectos de complejidad media o alta

La experiencia con el IDE le brinda una visión más profunda de la transformación, ya que puede trabajar junto con el agente.NET a medida que transforma los proyectos. Para proyectos de complejidad media, alta o crítica, utilice el IDE en lugar de la consola web.

Tenga un plan de validación

Decida cómo validará su solicitud para comprobar que es correcta una vez que se haya transformado. Post-transformation, tendrá que confirmar que se comporta y se ve correctamente cuando se ejecuta, y que los controles de seguridad, la lógica empresarial y el almacenamiento de datos están intactos. ¿La validación se realizará manualmente and/or mediante la automatización de pruebas? Si su solución contiene pruebas unitarias, AWS Transform las portará automáticamente y las ejecutará, y los resultados aparecerán en el informe de transformación.

Proporcione NuGet dependencias de paquetes privados

Si su solución depende de paquetes privados, asegúrese de que estén disponibles en su máquina local para que el IDE y AWS Transform puedan encontrarlos.

Especifique los reemplazos de paquetes o solicite recomendaciones a los agentes

En el caso de los paquetes que no tienen versiones modernas de.NET, puede personalizar el plan de transformación para especificar las sustituciones de paquetes que desee sustituir o pedir recomendaciones al agente.

No termine su trabajo hasta que esté seguro de que no desea realizar más cambios

Una vez finalizada la transformación, no finalice su trabajo de inmediato si desea realizar cambios adicionales. La transformación no estará completa hasta que usted diga que sí. Puede solicitar cambios hasta que marque la tarea como finalizada.

Tras la transformación, pásala a un compañero de código de IA para que finalice tu aplicación

Prepárate para combinar AWS Transform con un código complementario de IA, como Kiro. Un patrón habitual es transformar primero con AWS Transform para .NET y, después, pasárselo a un compañero de código de IA para finalizar la aplicación. Ese trabajo de finalización podría incluir identificar y corregir los errores de tiempo de ejecución, los problemas de comportamiento y el estilo de la experiencia de usuario.

En el proceso de modernización, piensa en AWS Transform como el viaje exprés que te lleva muy lejos hacia tu objetivo, y en el compañero del código de la IA como el viaje local que te lleva hasta tu destino final.

Para facilitar el traspaso del código de AWS Transform al de AI, AWS Transform proporciona un informe de transformación en HTML y un documento de rebajas sobre los próximos pasos al final de la transformación.

Evaluación y planificación

Tras iniciar un trabajo de transformación, AWS Transform analiza el código y elabora un informe de evaluación y un plan de transformación. Utilice las siguientes prácticas recomendadas para aprovechar al máximo esta fase.

Revise la evaluación y haga preguntas para establecer sus expectativas

Revise los resultados de la evaluación detenidamente para comprender qué proyectos serán difíciles de transformar y por qué. El agente presenta los proyectos con un nivel de complejidad (bajo, medio, alto, crítico) y explica por qué tienen esa calificación.

Haga preguntas para comprender mejor las áreas desafiantes. Por ejemplo:

- Pregúntele al agente cuál es su nivel de confianza en la transformación de un proyecto o en un caso de uso.
- Pregúntele al agente qué tareas posteriores a la transformación probablemente sean necesarias con un código complementario de IA.

Revise el plan y analice las opciones con el agente

El agente proporciona un plan de transformación para que lo revise. Puede analizar y modificar este plan. Comience por entender sus opciones. Pregúntele al agente qué alternativas existen a cualquier parte del plan.

Por ejemplo, el plan de transformación podría proponer la transformación de los servicios de WCF en API ASP.NET web. Sin embargo, su organización prefiere quedarse con WCF. Le pides opciones al agente y descubres que una alternativa es transformarlas CoreWCF en opciones.

Cargue los documentos de orientación para diseñar un plan para su organización

El plan de transformación original se crea sin comprender los requisitos y preferencias de la organización. Puede informar al agente sobre las convenciones organizativas, las especificaciones de las aplicaciones, el conjunto de tecnologías preferido y los ejemplos de patrones de codificación preferidos.

Después de cargar un documento de orientación, explíquelo para darle contexto al agente. Con la información adicional de los documentos de dirección, el agente puede preparar un plan adaptado a la forma en que le gusta trabajar a su organización.

Personalice el plan libremente

El agente.NET es flexible y puede personalizar libremente el plan de transformación, dentro del ámbito de la transformación de .NET a .NET. Puedes solicitar cambios de plan en el chat o, si lo prefieres, puedes trabajar con archivos rebajados. Revisa y refina el plan hasta que estés satisfecho.

Si un plan debe ser revisado por varias partes interesadas, puedes descargarlo como un archivo de descuento, compartirlo y luego subir un plan personalizado.

Por ejemplo, revisa el plan de transformación y decide que quiere que los proyectos de la biblioteca de clases se transformen a .NET Standard en lugar de .NET 10. En el chat, dice: «Revise el plan para transformar todas las bibliotecas de clases a .NET Standard 2.0» y el agente le presenta un plan revisado.

Transforma de forma interactiva o autónoma

La experiencia Visual Studio IDE ofrece modos autónomos e interactivos para controlar el grado de interactividad durante la transformación.

Utilice los modos interactivos y autónomos para controlar el grado de interactividad

Tú seleccionas el modo al iniciar una transformación y puedes cambiarlo en cualquier momento a través de un menú desplegable en la parte superior de la ventana de chat.

- Utilice el modo autónomo para una transformación desatendida, adecuado para trabajos de un día para otro o de larga duración. Aún tienes la oportunidad de revisar los resultados y solicitar cambios al final del trabajo.
- Utilice el modo interactivo para trabajar junto al agente en el chat durante todo el proceso de transformación con un plan de transformación personalizable, una gran visibilidad de los detalles de la transformación y una revisión paso a paso de cada proyecto. Puede realizar iteraciones para refinar los resultados o cambiar de dirección hasta quedar satisfecho.

Puede combinar modos. Por ejemplo, comience en el modo interactivo para revisar y ajustar el plan de transformación y, a continuación, cambie al modo autónomo para transformar los proyectos automáticamente.

Pídale al agente que le explique los cambios en el código

Si ve cambios en el código que no entiende, pídale al agente que se los explique.

Utilice los puntos de control para detenerse en los proyectos para revisarlos o modificarlos

En el modo interactivo, después de aprobar tu plan, puedes establecer o borrar puntos de control para cada proyecto. Cuando se transforma un proyecto con un punto de control, el código transformado se aplica al proyecto en el IDE y el agente hace una pausa para revisarlo. Puede revisar los resultados y, si no le gustan, puede solicitar más cambios.

Mientras esté detenido en un punto de control, podrá:

- Revisa los resultados tal y como se presentan en el chat y haz preguntas en el chat. Por ejemplo: «¿Por qué cambiaste la API de criptografía del archivo X?»
- Para ver los cambios de código, pulse el botón Ver resultados del proyecto en la ventana AWS Transform Job Plan.
- Refina la transformación solicitando cambios adicionales. Por ejemplo: «Cambia esto para usar el registrador X» o «Cambia esto para usar el paquete X en lugar del paquete Y».
- Vuelva a intentar la transformación, repitiéndola con instrucciones diferentes. Por ejemplo: «Cambie esta biblioteca de clases para que se dirija a .NET Standard en lugar de .NET 10" o «Vuelva a intentar esta transformación y cambie el destino Blazor a MVC Razor Pages».

- Realice sus propios cambios de código en el IDE.
- Dígame al agente que continúe hasta el siguiente punto de control del proyecto.

Repita hasta que esté satisfecho

La modernización es iterativa por naturaleza, y cabe esperar que se repita con el agente. Puede realizar cambios en los puntos de control del proyecto y también al final de la transformación. Repita según sea necesario hasta que esté satisfecho. La transformación no está completa hasta que usted diga que sí.

Codifique junto al agente cuando lo detengan en un punto de control

Puedes hacer tus propios cambios en el código mientras trabajas con el agente. Si se detiene en un punto de control, puede editar los archivos de código en Visual Studio él. Los cambios se sincronizarán cuando indiques al agente que continúe.

Validación y finalización

Una vez completada la transformación, valide la aplicación transformada y finalícela para su uso en producción.

Revise el informe de transformación y los próximos pasos para comprender qué se ha hecho y qué queda por hacer

Revise el informe de transformación HTML para comprender lo que se ha hecho. Revise el archivo de anotaciones de Next Steps para saber qué tareas aún quedan pendientes. Pídale al agente que aclare cualquier cosa que no esté clara.

Utilice un código complementario de IA para validar, depurar y finalizar su aplicación

Revise la aplicación transformada para comprobar si es correcta. Utilice un código complementario de IA, por ejemplo, [Kiro](#) para resolver problemas.

Valide las pruebas unitarias

Si su solución contiene proyectos de pruebas unitarias (NUnit, xUnit, o MSTest), AWS Transform los portará a la versión moderna de .NET y realizará las pruebas por usted. Consulta el informe de transformación HTML para ver los resultados de las pruebas unitarias. Corrija las pruebas fallidas con un código complementario de IA.

Valide la funcionalidad de la aplicación

Ejecute la aplicación y confirme que su funcionalidad coincide con la original. Tenga en cuenta los problemas funcionales y los errores de tiempo de ejecución. Corríjalo con un código de IA complementario.

Valide la interfaz de la aplicación

Ejecute la aplicación y confirme que se ve y se comporta como la original, incluidos la navegación y el enrutamiento. Si la aplicación no tiene estilo, es posible que los archivos.css no estén en la ubicación correcta. Corríjalo con un código de IA complementario.

Modernización de SQL Server

AWS Transform for SQL Server Modernization es un AI-powered servicio que automatiza la modernización completa de las bases de datos de Microsoft SQL Server y sus aplicaciones.NET asociadas a Amazon Aurora PostgreSQL. El servicio organiza todo el proceso de migración, desde la conversión de esquemas, la migración de datos y la modificación del código de la aplicación para adaptarlo al nuevo PostgreSQL de destino, lo que hace que sus equipos sean más productivos al automatizar tareas complejas y laboriosas.

Regiones admitidas

AWS Transform for SQL Server está disponible en EE. UU. Este (Norte de Virginia) - us-east-1

Cross-Region Uso: en el caso de las bases de datos de regiones no compatibles, puede clonar la base de datos en una región compatible para su transformación y, a continuación, volver a implementar los resultados en la región de destino.

Capacidades y características clave

Transformación de bases de

- Conversión de esquemas: convierte automáticamente los esquemas de SQL Server a Aurora PostgreSQL, incluidas tablas, vistas, índices, restricciones y relaciones
- Transformación de procedimientos almacenados: convierte los procedimientos T-SQL almacenados en archivos con precisión PL/pgSQL AI-enhanced
- Migración de datos: migra los datos con validación de integridad mediante AWS Database Migration Service (DMS)

- Objetos de base de datos: admite activadores, funciones, vistas, columnas calculadas y columnas de identidad
- Validación: verificación automatizada de la integridad de los datos y comprobaciones de integridad referencial

Transformación de aplicaciones

- Transformación de Entity Framework: actualiza las configuraciones de Entity Framework 6.3-6.5 y EF Core 1.0-8.0 para PostgreSQL
- ADO.NET transformación: convierte el código ADO.NET de acceso a datos de SQL Server a proveedores de PostgreSQL.
- Actualizaciones de cadenas de conexión: actualiza automáticamente todas las cadenas de conexión de la base de datos a la nueva base de datos PostgreSQL de destino
- Cambios en el proveedor de bases de datos: reemplaza los proveedores de SQL Server por Npgsql (proveedor de PostgreSQL)
- Actualizaciones de configuración de ORM: modifica las asignaciones de tipos de datos, las columnas de identidad y las configuraciones específicas de las bases de datos

&Validación de la orquestación

- Wave-based modernización: organiza los grandes patrimonios en fases de migración lógicas
- Mapeo de dependencias: identifica las relaciones entre las aplicaciones y las bases de datos
- Human-in-the-loop Puntos de control (HITL): proporcionan puertas de revisión y aprobación en las etapas críticas
- Validación automatizada: comprueba la compatibilidad de los esquemas, la integridad de los datos y la funcionalidad de la aplicación
- CI/CD integración: se integra con los procesos de desarrollo existentes

Implementación

- Implementación de Amazon ECS y Amazon EC2: implementación automatizada en contenedores con soporte de autoscalamiento
- Infrastructure-as-code generación: crea nuestras plantillas de CDK CloudFormation AWS

- Validación de despliegue automatizada: verifica el éxito del despliegue mediante comprobaciones de estado
- Capacidades de reversión: admite los procedimientos de reversión en caso de que surjan problemas

Versiones y tipos de proyectos compatibles

Versiones de SQL Server

AWS Transform admite las siguientes versiones de SQL Server:

Versión de SQL Server	Estado de Support
SQL Server 2022	compatible
SQL Server 2019	compatible
SQL Server 2017	compatible
SQL Server 2016	compatible
SQL Server 2014	compatible
SQL Server 2012	compatible
SQL Server 2008 R2	compatible

Note

Se admiten todas las ediciones de SQL Server (Express, Standard, Enterprise). SQL Server se puede alojar en AWS (Amazon RDS for SQL Server o SQL Server en Amazon EC2) o se puede alojar fuera de él. AWS

Versiones.NET

Versión.NET	Estado de Support
.NET 10	compatible
.NET 8	compatible
.NET 7	compatible
.NET 6 (núcleo)	compatible
.NET Framework 4.x y versiones anteriores	No es compatible

Important

No se admiten las versiones antiguas de .NET Framework 4.x y anteriores. Si su aplicación utiliza .NET Framework, primero debe actualizar a .NET Core 6+ mediante AWS Transform para modernizar.NET antes de utilizar las capacidades de transformación de SQL Server.

versiones de Entity Framework

Marcos	Versiones compatibles
Entity Framework 6	6.3, 6.4, 6.5
Entity Framework Core	De 1.0 a 8.0
ADO.NET	Todas las versiones (GA)

Repositorios de código fuente

AWS Transform es compatible con las siguientes plataformas de código fuente:

- GitHub y GitHub Enterprise Server
- GitLab.com y GitLab Self-Managed

- Bitbucket Cloud y Bitbucket Data Center
- Azure DevOps y Azure Server DevOps
- Amazon S3

Bases de datos de destino

AWS Transform apunta a Amazon Aurora PostgreSQL (compatible con PostgreSQL 15+) con soporte para las últimas funciones y optimizaciones de Aurora.

Requisitos técnicos

Requisitos de base de datos

- Microsoft SQL Server desde 2008 R2 hasta 2022
- SQL Server alojado en AWS (Amazon RDS for SQL Server o SQL Server en Amazon EC2) o alojado fuera de AWS
- En el AWS caso de las bases de datos alojadas, la base de datos y AWS Transform deben estar en la misma región. AWS
- En el caso de las bases de datos alojadas fuera de ella AWS, se requiere conectividad de red con el servicio AWS Transform.
- Usuario de base de datos con permisos VIEW DEFINITION y VIEW DATABASE STATE
- Las contraseñas de las bases de datos utilizan únicamente caracteres ASCII imprimibles (excepto '/', '@', '' y los espacios)
- La VPC que contiene el SQL Server de origen debe tener subredes en al menos 2 zonas de disponibilidad diferentes (obligatorio para los grupos de subredes de replicación de DMS)

Requisitos de la aplicación

- Aplicaciones.NET Core 6, 7 u 8
- Entity Framework 6.3-6.5 o Entity Framework Core 1.0-8.0, o ADO.NET
- Las conexiones de bases de datos se pueden detectar en el código fuente
- Las aplicaciones se compilan y ejecutan correctamente
- Código fuente en plataformas de repositorio compatibles

AWS requisitos de cuenta

- AWS cuenta con acceso de administrador
- IAM Identity Center activado
- Se crearon los roles de servicio necesarios (consulte las instrucciones de configuración que aparecen a continuación)
- VPC con la configuración de red adecuada

Procesamiento y almacenamiento de datos

Lugar de procesamiento

- El procesamiento del esquema se produce en una instancia de DMS dentro de su VPC
- La migración de datos es opcional y se puede excluir si es necesario
- Los artefactos de transformación se almacenan en la región de servicio de AWS Transform

Artefactos almacenados

Los siguientes elementos se almacenan en la región de servicio:

- Registros de agentes
- Resultados de la evaluación
- Archivos de esquema SQL
- Artefactos de salida de DMS

Important

Importante para la residencia de los datos: incluso cuando se opta por no realizar la migración de datos, los metadatos y los artefactos de procesamiento se almacenan en la región de servicio. Esto es importante para las organizaciones con requisitos estrictos de residencia de datos.

Gestión de artefactos

- Opción de cifrado para el cliente mediante sus propias claves KMS

- Periodo TTL (tiempo de vida útil) definido para todos los artefactos
- Los artefactos se pueden descargar para almacenarlos sin conexión

Requisitos de SQL Server

Requisitos de base de datos

Bases de datos alojadas extern

AWS Se admiten bases de datos alojadas fuera de él. Para utilizar una base de datos alojada externamente, debe garantizar la conectividad de red entre la base de datos y el servicio AWS Transform.

Cargas de trabajo de SSIS

- Limitación: no se admite la transformación de SQL Server Integration Services (SSIS).
- Solución alternativa: utilice AWS Glue u otros servicios de ETL para la migración de SSIS.

Servidores vinculados

- Limitación: las conexiones a bases de datos externas a través de servidores enlazados requieren una configuración humana.
- Solución alternativa: vuelva a configurar los servidores enlazados después de la migración o utilice enfoques alternativos, como los enlaces de bases de datos o la integración a nivel de aplicación.

Patrones complejos T-SQL

- Limitación: algunos T-SQL patrones avanzados pueden necesitar la intervención humana.
- Solución alternativa: utilice la CLI de Amazon Kiro para realizar conversiones SQL complejas. AWS Transform las marca para revisarlas durante el proceso de transformación.

Requisitos de solicitud

.NET Framework heredado

- Limitación: .NET Framework 4.x y versiones anteriores no son compatibles.

- Solución alternativa: utilice AWS Transform para .NET para actualizar primero a .NET Core 6+ y, a continuación, utilice la transformación de SQL Server.

versiones de Entity Framework

- Limitación: solo se admiten Entity Framework 6.3-6.5 y EF Core 1.0-8.0.
- Solución alternativa: actualice a una versión de Entity Framework compatible antes de la transformación.

VB.NET aplicaciones

- Limitación: no VB.NET es compatible.
- Solución alternativa: convierta a C# o utilice AWS Transform custom para convertir de VB.NET C#.

Cross-database dependencias

- Limitación: problemas cuando los esquemas de bases de datos interactúan entre varias bases de datos.
- Solución alternativa: revise y refactorice las consultas entre bases de datos antes de la migración. Considere la posibilidad de consolidar bases de datos o utilizar esquemas PostgreSQL.
- Impacto: podría requerir la intervención humana en escenarios complejos entre bases de datos.

Repository-database acoplamiento

- Limitación: desafíos cuando un único repositorio sirve para múltiples bases de datos.
- Solución alternativa: considere la posibilidad de reestructurar los repositorios o adoptar un enfoque de migración gradual.
- Impacto: las migraciones basadas en oleadas podrían requerir una planificación adicional.

Requisitos de infraestructura

Único account/region por trabajo

- Limitación: cada trabajo de transformación se dirige a una AWS cuenta y una región.

- Solución alternativa: cree varios trabajos de transformación para despliegues con varias cuentas o regiones.

Objetivos de implementación

- Limitación: se admiten las implementaciones de Amazon ECS y Amazon EC2.

Requisitos de repositorio

NuGet Paquetes privados

- Limitación: NuGet los paquetes privados requieren una configuración adicional.
- Solución alternativa: configure los NuGet feeds privados en los ajustes de transformación antes de iniciar el trabajo.

Configuración de SQL Server

Realice estos pasos en su entorno de SQL Server para habilitar la modernización de AWS Transform.

Instalación y configuración de la base de datos

Paso 1: Crear un usuario de base de datos con los permisos necesarios

Cree un usuario de base de datos dedicado para AWS Transform con los permisos necesarios. Si ya tiene un usuario de DMS Schema Conversion, puede reutilizarlo.

Conéctese a su instancia de SQL Server y ejecute los siguientes 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 los comandos específicos de la base de datos (USE, CREATE USER, GRANT) para cada base de datos que desee modernizar.

La función db_datareader solo es necesaria para la migración de datos, no solo para la conversión de esquemas.

- La función db_datareader concede acceso de lectura a todas las tablas de la base de datos
- Esta función solo es necesaria cuando se realiza una migración de datos.
- Solo para la conversión de esquemas (sin migración de datos), NO se requiere la función db_datareader
- Los demás permisos (VIEW DEFINITION, VIEW DATABASE STATE, etc.) son suficientes para la conversión del esquema

Paso 2: Almacene las credenciales en AWS Secrets Manager

Guarde las credenciales de su base de datos de forma segura en AWS Secrets Manager. Omita este paso si ya ha creado un secreto para DMS.

1. Navega hasta AWS Secrets Manager en la consola
2. Selecciona Guardar un secreto nuevo
3. Configura el secreto:
 - Tipo de secreto: credenciales de otra base de datos
 - Base de datos: Microsoft SQL Server
 - Nombre de usuario: atx_user (o el nombre de usuario que elija)
 - Contraseña: la contraseña que creaste
 - Nombre del servidor: su punto final de SQL Server

- Nombre de la base de datos: nombre de su base de datos
 - Puerto: 1433 (o su puerto personalizado)
4. Elija Siguiente.
 5. Introduzca el nombre secreto: atx-db-modernization-sqlserver
 6. Añada las etiquetas necesarias (estas etiquetas son obligatorias):
 - Clave: proyecto, valor: atx-db-modernization
 - Clave: propietario, valor: conector de base de datos
 7. Seleccione Siguiente en el resto de las pantallas
 8. Elige Tienda
 9. Anote el ARN secreto para usarlo en el siguiente paso

Important

Las contraseñas de las bases de datos deben utilizar únicamente caracteres ASCII imprimibles, excluyendo '/', '@', '"' y los espacios. Los secretos cuya eliminación está programada pueden provocar errores de transformación.

Paso 3: Cree las funciones de DMS necesarias

AWS Transform requiere funciones de IAM específicas para las operaciones de DMS. Implemente estas funciones mediante la siguiente CloudFormation plantilla.

Note

Si su AWS cuenta ya tiene DMS-related roles existentes, modifique esta plantilla para reutilizar esos recursos en lugar de crear duplicados.

Crea un archivo llamado dms-roles.yaml con el siguiente contenido:

```
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
  DMSecretsManagerRoleArn:
    Description: ARN of the DMS Secrets Manager Role
    Value: !GetAtt DMSecretsManagerRole.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

```

Implemente la CloudFormation pila mediante AWS CLI:

```

aws cloudformation create-stack \
  --stack-name dms-roles \
  --template-body file://dms-roles.yaml \
  --capabilities CAPABILITY_NAMED_IAM \
  --region us-east-1

```

O despléguelo mediante la AWS consola:

1. Navegue hasta CloudFormation en la AWS consola
2. Seleccione Crear pila
3. Seleccione Cargar un archivo de plantilla
4. Carga el archivo dms-roles.yaml
5. Introduce el nombre de la pila: dms-roles
6. Reconozca las capacidades de IAM
7. Elija Crear pila

Paso 4: Configurar la seguridad de la red

Asegúrese de que la conectividad de red sea adecuada entre AWS Transform, su base de datos de SQL Server y otros AWS servicios.

Configuración de grupos de seguridad (enfoque recomendado)

Enfoque recomendado: utilice un control de acceso basado en grupos de seguridad en lugar de IP-based reglas. Esto proporciona una mayor seguridad, una administración más sencilla y funciona a la perfección con la arquitectura de AWS Transform.

¿Por qué elegir Security Group-Based Access Control?

- La conversión de esquemas de DMS crea interfaces de red elásticas (ENI) dentro de su VPC
- No es necesario que sus bases de datos sean de acceso público
- AWS Transform no expone las direcciones IP privadas, lo que complica IP-based las reglas
- Las referencias a los grupos de seguridad proporcionan actualizaciones dinámicas y automáticas a medida que los recursos aumentan

Configure su grupo de seguridad de SQL Server

Al configurar el perfil de instancia de conversión del esquema de DMS en AWS Transform, se especifica un grupo de seguridad para la instancia SC de DMS. El grupo de seguridad de su base de datos debe permitir el tráfico entrante desde este grupo de seguridad SC del DMS.

Step-by-step configuración:

1. Identifique el grupo de seguridad de conversión del esquema DMS:

- Esto se especifica al crear el perfil de instancia en Transform AWS
 - Anote el ID del grupo de seguridad (por ejemplo, sg-0123456789abcdef0)
2. Actualice las reglas de entrada del grupo de seguridad de SQL Server:
- Tipo: TCP personalizado
 - Puerto: 1433 (o su puerto personalizado de SQL Server)
 - Fuente: El ID del grupo de seguridad de conversión de esquemas de DMS
 - Descripción: «Permitir el acceso a la conversión de esquemas de DMS»
3. Para el destino de Aurora PostgreSQL (después de la creación):
- Tipo: PostgreSQL
 - Puerto: 5432 (o su puerto PostgreSQL personalizado)
 - Fuente: El ID del grupo de seguridad de conversión de esquemas de DMS
 - Descripción: «Permitir el acceso a la conversión de esquemas de DMS»

 Important

Importante para los modelos de seguridad menos privilegiados: si su organización utiliza un modelo de seguridad «menos privilegiado» que bloquea todo el tráfico de forma predeterminada, debe permitir explícitamente el tráfico entrante del grupo de seguridad de conversión del esquema de DMS al puerto de su base de datos. No abra el puerto 1433 a todas las fuentes o rangos de IP.

Obligatorio AWS conectividad del servicio

Asegúrese de que su VPC pueda comunicarse con:

- AWS Transforme los puntos finales del servicio
- AWS DMS puntos finales
- Puntos finales de Aurora PostgreSQL
- Terminales S3 para almacenamiento de artefactos
- AWS Secrets Manager puntos finales
- AWS CodeConnections puntos finales

Puntos de enlace de VPC: en el caso de las redes privadas, configure los puntos de enlace de VPC para los AWS servicios necesarios a fin de evitar las dependencias de las puertas de enlace de Internet.

Requisitos para las bases de datos alojadas externamente

Si la base de datos de SQL Server está alojada fuera de AWS, asegúrese de que se cumplen los siguientes requisitos previos y, a continuación, complete los pasos de configuración antes de comenzar la modernización.

Requisitos previos

- Una AWS cuenta con una VPC
- Conectividad de red entre la VPC y la base de datos externa. Para obtener información sobre la configuración de la conectividad de red, consulte [Configuración de la conectividad de red](#) en la Guía del AWS DMS usuario.

Pasos de configuración

1. Cree una entrada secreta AWS Secrets Manager con los detalles de conexión de la base de datos externa. Para obtener más información, consulte [the section called “Paso 2: Almacene las credenciales en AWS Secrets Manager”](#).
2. Cuando se le solicite, proporcione el ID de VPC y el ID del grupo de seguridad para conectarse a la base de datos externa. AWS Transform le solicita esta información porque el nombre de host de la base de datos que figura en el secreto no se puede resolver en la cuenta. AWS

AWS Configuración de transformación

Comience su proceso de modernización accediendo a la consola AWS Transform e iniciando un nuevo proyecto de modernización. Este paso establece su espacio de trabajo y establece la configuración básica para su transformación completa.

Acciones a completar:

- Navegue hasta el servicio AWS Transform en la consola AWS de administración
- Seleccione Microsoft Modernization de las opciones de servicio
- Elija Crear un nuevo proyecto de modernización

- Proporcione el nombre y la descripción del proyecto
- Seleccione AWS la región de destino (debe coincidir con la ubicación de SQL Server)
- Revise y confirme la configuración del proyecto

 Note

Práctica recomendada: utilice nombres de proyectos descriptivos que incluyan el nombre de la aplicación y el entorno de destino (por ejemplo, CustomerPortal-Production-Modernization «') para identificar fácilmente los proyectos en escenarios de múltiples fases.

Cree un trabajo de modernización de SQL Server

Connect base de datos y repositorio de código fuente

Configurar el conector de base de datos

Establezca una conectividad segura con sus bases de datos de SQL Server configurando los conectores de bases de datos. El conector realiza análisis del entorno, descubre dependencias y permite a AWS Transform acceder a los esquemas y metadatos de la base de datos para su evaluación y conversión.

Acciones que se deben completar:

- Seleccione Configurar el conector de base de datos en el asistente de configuración
- Elija el método de conexión: conexión nueva o conexión existente
- Proporcione los detalles de la conexión a SQL Server (nombre del punto final, puerto o base de datos)
- Configure la autenticación y pruebe la conectividad
- Revise las bases de datos detectadas y confirme la selección

 Note

Conectividad de red: asegúrese de que los grupos de seguridad y las NACL de SQL Server permitan las conexiones entrantes desde los puntos finales del servicio AWS Transform.

Connect repositorio de código fuente

Habilite AWS Transform para acceder al código fuente de su aplicación.NET. AWS Transform admite tres métodos para proporcionar el código fuente: un conector de token de acceso personal (PAT) (recomendado) o Amazon S3. AWS CodeConnections Esta integración permite al servicio analizar el código de la aplicación, identificar las dependencias de las bases de datos y realizar transformaciones de código automatizadas para garantizar la compatibilidad con PostgreSQL.

Acciones que se deben completar:

- Navegue a la sección Connect Source Code Repository
- Elija su método de autenticación: PAT Connector (recomendado) o Amazon S3 AWS CodeConnections
- Seleccione los repositorios que contienen aplicaciones.NET
- Especifique la rama para el análisis (normalmente main/master o de desarrollo)
- Valide el acceso al repositorio y la estructura del código

Note

Descubrimiento de repositorios: AWS Transform escanea automáticamente los repositorios para identificar los proyectos de.NET, las configuraciones de Entity Framework, las cadenas de conexión a bases de datos y las dependencias de SQL.

Note

Nota de seguridad: AWS Transform solo requiere acceso de lectura a tus repositorios y crea nuevas ramas de funciones para el código transformado. Tu rama principal permanece intacta.

Un humano al tanto

AWS Transform utiliza los mecanismos «human-in-the-loop» (HITL) para garantizar la calidad y permitirle revisar y aprobar las decisiones críticas de transformación. Los siguientes puntos de control requieren su atención:

Revisión y aprobación del plan de olas

Lo que usted analiza: Las oleadas de migración propuestas, incluidas las bases de datos y aplicaciones que se agrupan y la secuencia de las oleadas.

Puede:

- Aprobar el plan de olas
- Personalice las olas moviendo las bases de datos entre las olas
- Modifique la secuencia de ondas
- Divida o fusione ondas

Tras la aprobación, AWS Transform continúa con la conversión del esquema.

Revisión de la conversión del esquema

Lo que revisa: objetos de base de datos convertidos, incluidas tablas, procedimientos almacenados, funciones y activadores. Los elementos de acción resaltan los objetos que requieren atención.

Puede:

- Aceptar el código convertido
- Modificar el código convertido
- Marcar para su revisión humana después de la transformación
- Vea una comparación lado a lado del código original y el convertido

Qué ocurre después de la aprobación: AWS Transform aplica el esquema a Aurora PostgreSQL y continúa con la migración de datos (si está configurada).

Revisión del código de la aplicación

Lo que revisa: todos los cambios en el código de la aplicación, incluidas las configuraciones de Entity Framework, las cadenas de conexión, el código de acceso a los datos y las llamadas a procedimientos almacenados.

Puede:

- Aceptar los cambios de cada archivo

- Modifique el código transformado
- Rechazar los cambios (no se recomienda)
- Agrega comentarios para tu equipo
- Descarga el código transformado para su revisión local

Qué ocurre después de la aprobación: AWS Transform confirma los cambios en una nueva rama de tu repositorio y continúa con la validación.

Revisión de los resultados de la validación

Lo que revisa: los resultados de la validación automatizada, incluida la compatibilidad de los esquemas, las comprobaciones de integridad de los datos y el estado de creación de la aplicación.

Puede:

- Revisar las pruebas aprobadas
- Investigue las pruebas no aprobadas
- Aborda las advertencias
- Continúe con la implementación o vuelva a solucionar los problemas

Qué ocurre después de la aprobación: AWS Transform se prepara para la implementación en el entorno de destino.

Aprobación de la implementación

Lo que debe revisar: la configuración de la implementación, incluidas las plantillas de infraestructura como código, la configuración del servicio de ECS y los ajustes de implementación.

Puede:

- Revisar y personalizar la configuración de implementación
- Apruebe la implementación para continuar
- Retrase el despliegue para realizar pruebas adicionales
- Descargue el código de infraestructura para revisarlo

Tras la aprobación, AWS Transform implementa la aplicación y la base de datos modernizadas en el entorno de destino.

Evaluación y planificación de oleadas

Configurar landing zone

Configure el entorno de infraestructura de destino en el que se implementarán las aplicaciones modernizadas. La configuración de landing zone incluye el aprovisionamiento de Aurora PostgreSQL, la configuración de red y las configuraciones de despliegue de referencia.

Acciones que se deben completar:

- Seleccione Configurar zona de aterrizaje en el menú de configuración
- Configurar el destino de Aurora PostgreSQL (versión, clase de instancia) Multi-AZ
- Configurar los ajustes de red y seguridad (VPC, subredes, grupos de seguridad)

Note

Consideración de costos: las instancias de Aurora PostgreSQL incurren en costos continuos. Considere usar Aurora Serverless v2 para development/testing entornos.

Evaluación

Realice un análisis exhaustivo de los esquemas, el código de la aplicación y las dependencias de la base de datos. La fase de evaluación proporciona clasificaciones de la complejidad de la transformación, identifica los posibles desafíos y genera informes detallados.

Acciones que se deben completar:

- Seleccione la rama del repositorio para el análisis del código
- Seleccione repositorios y bases de datos para la transformación
- Revise los resultados de la evaluación y las calificaciones de complejidad
- Genere un informe de evaluación con proyecciones de esfuerzo
- Exporte el informe para su revisión y aprobación por las partes interesadas

 Note

Perspectivas de la evaluación: la evaluación proporciona un análisis detallado de los objetos del esquema, los procedimientos almacenados y las dependencias de las aplicaciones y estima el nivel de intervención humana requerido.

Planificación de olas

Organice su modernización en fases gestionables en función de la complejidad de la transformación, las prioridades empresariales y las dependencias de las aplicaciones. AWS Transform genera recomendaciones de oleadas inteligentes que puede personalizar.

Acciones a completar:

- Revise el plan y las recomendaciones de AI-Generated Wave
- Personalice la configuración de Wave en función de las prioridades empresariales
- Valide las dependencias entre aplicaciones y bases de datos
- Finalice Wave Plan mediante una interfaz conversacional
- Establezca las prioridades de ejecución de la oleada y asigne responsabilidades

 Note

AI-Powered Recomendaciones: Puede interactuar con la IA a través de un lenguaje natural para ajustar las recomendaciones: «Mueva CustomerDB a la primera fase» o «combine estas dos aplicaciones en la misma oleada».

 Note

Práctica recomendada: comience con una oleada piloto que contenga de 1 a 2 bases de datos de baja complejidad para establecer los procesos y fomentar la confianza del equipo.

Migración de datos para cada oleada

Conversión de esquemas para cada oleada

Transforme los esquemas de bases de datos de SQL Server en PostgreSQL-compatible equivalentes mediante las capacidades AI-enhanced de conversión. Este proceso convierte las tablas, los procedimientos almacenados, las funciones, los activadores y otros objetos de la base de datos.

Acciones que se deben completar:

- Proporcione los objetivos de conversión del esquema y configure las preferencias
- Ejecute la conversión automática mediante el servicio de conversión de esquemas de DMS
- Revise los resultados de la conversión e identifique los elementos de intervención humana
- Gestione las intervenciones manuales siguiendo las instrucciones de HITL
- Valide las correcciones humanas y vuelva a ejecutar la conversión si es necesario

Note

Intervenciones manuales habituales: los servidores enlazados, los tipos definidos por el usuario, T-SQL los patrones avanzados y las funciones de SQL específicas del proveedor suelen requerir la revisión y corrección por parte de un humano.

Migración de datos para cada oleada

Transfiera datos de SQL Server a Aurora PostgreSQL AWS Database Migration Service mediante AWS DMS la integración (). Elija entre la migración de datos de producción o la generación de datos sintéticos para realizar pruebas.

Acciones a completar:

- Elija la migración de datos de producción o la generación de datos sintéticos
- Configure la instancia de replicación de DMS para la transferencia de datos
- Supervise el progreso de la migración y gestione las inconsistencias en los datos
- Valide la integridad de los datos y las restricciones referenciales
- Confirme que se ha completado correctamente antes de continuar

Note

Integración automatizada del DMS: AWS Transform resume la complejidad de la configuración del DMS y gestiona automáticamente la creación de puntos finales, la configuración de tareas y la asignación de tipos de datos.

Note

Validación de datos: el servicio realiza pruebas empíricas mediante la ejecución de consultas idénticas en las bases de datos de origen y de destino para garantizar la coherencia de los datos.

Migración de código para cada oleada

Transforme el código de la aplicación.NET para que funcione con Aurora PostgreSQL, incluidas las actualizaciones de configuración de Entity Framework, las modificaciones de las cadenas de conexión, las adaptaciones de consultas SQL y los ajustes específicos del marco.

Acciones que se deben completar:

- Ejecute un análisis de código automatizado para las dependencias de SQL Server
- Realice la transformación del marco (actualizaciones del proveedor de Entity Framework)
- Adapte la sintaxis de SQL Query a PostgreSQL-compatible SQL
- Configure Target Branch Management para el código transformado
- Gestione intervenciones manuales para patrones complejos

Flujo de trabajo de modernización de SQL Server

En esta sección se proporciona un recorrido paso a paso del proceso completo de modernización de SQL Server mediante AWS Transform.

Paso 1: Crear un trabajo de modernización de SQL Server

Comience su proceso de modernización creando un nuevo trabajo de transformación en la consola AWS Transform.

1. Inicie sesión en la consola AWS Transform
2. Elija Crear trabajo de modernización
3. Seleccione Trabajo de modernización de Windows y, a continuación, seleccione Modernización de SQL Server
4. Introduzca los detalles del trabajo:
 - Nombre del trabajo: nombre descriptivo del proyecto
 - Descripción: descripción opcional
 - Región objetivo: AWS región de despliegue
5. Seleccione Create job (Crear trabajo).

 Important

No incluya información de identificación personal (PII) en el nombre de su trabajo.

Paso 2: Conectarse a la base de datos de SQL Server

Connect AWS Transform a su base de datos de SQL Server para permitir el análisis y la conversión de esquemas.

Cree un conector de base de datos

1. En su trabajo de modernización de SQL Server, vaya a Connect to resources
2. Elija Conectar a la base de datos de SQL Server
3. Elija Crear nuevo conector
4. Introduzca la información del conector:
 - Nombre del conector C: nombre descriptivo
 - AWS ID de cuenta: cuenta donde está alojado SQL Server
5. Una vez confirmado, recibirá un enlace para su aprobación. Copia el enlace de aprobación para obtener la aprobación de la cuenta por parte de tu AWS administrador. Una vez que lo hayan aprobado, puedes continuar con el siguiente paso.
6. Una vez que el administrador haya aprobado la solicitud de conector, haga clic en Enviar para continuar con la configuración de la conexión con el código fuente.

Paso 3: Conectar el repositorio de código fuente

AWS Transform necesita acceder al código fuente de su aplicación.NET para analizar y transformar el código que interactúa con la base de datos de SQL Server. AWS Transform admite tres métodos para proporcionar el código fuente.

Elija su método de autenticación

Conector de token de acceso personal (PAT) (recomendado)

Ideal para los equipos que necesitan permisos personalizados, asistencia de proveedores autohospedados o acceso a API específicas de cada proveedor, como Secrets. GitHub Creas una PAT en tu proveedor de código fuente con permisos personalizados, la guardas en AWS Secrets Manager ella y AWS Transform la recupera cuando es necesario. Eres responsable de gestionar la rotación y el vencimiento de los tokens.

AWS CodeConnections

Ideal para los equipos que desean una gestión automatizada de las credenciales. AWS CodeConnections utiliza una integración de proveedores gestionada que gestiona la autenticación mediante un flujo de autorización de OAuth 2.0. AWS gestiona todo el ciclo de vida de las credenciales, incluida la actualización y rotación automáticas de los tokens. No se requiere una administración manual de credenciales.

Amazon S3

Sube tu código fuente directamente a un bucket de Amazon S3. AWS Transform accede al código del bucket durante el trabajo de transformación.

Característica	Conector PAT (recomendado)	AWS CodeConnections
Administración de credenciales	Manual (gestionado por el cliente)	Automático (gestionado)AWS
ciclo de vida del token	Se requiere una rotación manual	Actualización automática
Flexibilidad de permisos	Alcances totalmente personali zables	Permisos fijos

Característica	Conector PAT (recomendado)	AWS CodeConnections
Self-hosted soporte de proveedores	compatible	No disponible
Complejidad de la configuración	Moderado (creación y almacenamiento manuales de fichas)	Bajo (autorización única)
Almacenamiento de fichas	Del cliente AWS Secrets Manager	Administradas por AWS

Configurar un conector PAT (recomendado)

Con un conector PAT, puede crear un token de acceso personal en su proveedor de código fuente con permisos personalizados, almacenarlo de forma segura y AWS Transform lo recupera cuando es necesario. AWS Secrets Manager Usted es responsable de gestionar el ciclo de vida del token, incluidas la rotación y la caducidad. AWS Transform crea automáticamente el rol de IAM necesario con permisos para acceder a tu secreto.

El conector PAT es compatible con los siguientes proveedores, incluidas las versiones autohospedadas y personalizadas DNS/URL :

- GitHub y GitHub Enterprise Server
- GitLab.com y GitLab Self-Managed
- Bitbucket Cloud y Bitbucket Data Center
- Azure DevOps y Azure Server DevOps

Cree un token de acceso personal

Cree un PAT en su proveedor de código fuente. Los permisos necesarios varían según el proveedor. Elija la pestaña de su proveedor.

⚠ Important

Copia el token inmediatamente después de crearlo. No puede volver a verlo. Establezca la caducidad durante la duración del trabajo de transformación. No configure la caducidad para que no caduque nunca.

⚠ Warning

Nunca deposite los tokens PAT en repositorios de código ni los comparta a través de canales inseguros. Guárdalos siempre dentro. AWS Secrets Manager

GitHub

Ve a Configuración, Configuración de desarrollador, Tokens de acceso personal, Fine-grained Tokens. Seleccione los repositorios que desee transformar y conceda los siguientes permisos.

Permisos de repositorio

Permiso	Acceso	Finalidad
Contenido	Leer y escribir	Lee el código fuente y vuelve a escribir el código transformado en el repositorio
Metadatos	Read-only	Accede a la información básica del repositorio

Permisos de organización (necesarios para los repositorios de la organización)

Permiso	Acceso	Finalidad
Miembros	Read-only	Muestra las organizaciones a las que puede acceder el token para descubrir los repositorios

GitLab

Vaya a Editar perfil y acceda a los tokens. Seleccione los siguientes ámbitos.

Alcance	Finalidad
<code>read_api</code>	Lee los metadatos del repositorio, la información del proyecto, los detalles del usuario y enumera los grupos y las ramas
<code>read_repository</code>	Lee los archivos de código fuente y la estructura del repositorio para su análisis
<code>write_repository</code>	Vuelve a escribir el código transformado en el repositorio

Bitbucket

Ve a Configuración de la cuenta, Seguridad y Creación y administración de tokens de API. Los ámbitos necesarios dependen del tipo de token.

Workspace/Repository Token (ATCT: autenticación de portador, no se requiere nombre de usuario)

Permiso	Acceso	Finalidad
Repositorios	Lee y escribe	Enumera los repositorios, lee las ramas y escribe el código transformado mediante git push

Token de API de cuenta (ATAT: autenticación básica con correo electrónico) o contraseña de aplicación (ATBB: autenticación básica con nombre de usuario)

Alcance	Finalidad
<code>read:account</code>	Identifica al usuario autenticado para resolver la pertenencia al repositorio
<code>read:workspace:bitbucket</code>	Muestra los espacios de trabajo a los que puede acceder el token para que AWS Transform pueda enumerar sus repositorios. No es obligatorio si especificas una lista de espacios de trabajo en el secreto.

Alcance	Finalidad
<code>read:repository:bitbucket</code>	Muestra los repositorios y lee los metadatos y la información de las sucursales
<code>write:repository:bitbucket</code>	Vuelve a escribir el código transformado en el repositorio mediante git push

Azure DevOps

Navegue hasta Configuración de usuario, Tokens de acceso personal. Seleccione Ámbitos definidos personalizados. Para el ámbito de la organización, elija Todas las organizaciones accesibles (recomendado) o especifique una sola organización.

Alcance	Acceso	Finalidad
Código	Lee y escribe	Lee el código fuente, enumera los repositorios y las ramas y vuelve a escribir el código transformado
Perfil de usuario	Lectura	Valida el acceso al token y descubre la identidad del usuario para realizar búsquedas en la organización
Gestión de los derechos de los miembros	Lectura	Enumera las organizaciones a las que puede acceder el token para descubrir los repositorios

Guarde la PAT en AWS Secrets Manager

1. Abra la AWS Secrets Manager consola.
2. Elija Almacenar un secreto nuevo.
3. En Secret type (Tipo de secreto), elija Other type of secret (Otro tipo de secreto).
4. Añada pares clave-valor en función del proveedor y el tipo de alojamiento:
 - Cloud-hosted proveedores: agrega una clave nombrada token junto con tu PAT como valor.

- En el caso de Azure DevOps con una organización específica, añade también una clave `organization` con el nombre de su organización.
- En el caso de las contraseñas de aplicaciones de Bitbucket (ATBB), añade también una clave `username` con el nombre de usuario de Bitbucket. En el caso de los tokens de API (ATAT) de la cuenta de Bitbucket, añade una clave `email` con el nombre de tu dirección de correo electrónico de Bitbucket.
- Self-hosted y DNS/URL proveedores personalizados: añade las siguientes claves: `host` (la URL de tu servidor, por ejemplo `https://github.mycompany.com`), `provider_type` (`github`, `gitlab`, `bitbucket`, `oado`) y `token` (tu PAT).
- En el caso de Azure DevOps con una organización específica, añade también una clave `organization` con el nombre de su organización.
- En el caso de las contraseñas de aplicaciones de Bitbucket (ATBB), añade también una clave `username` con el nombre de usuario de Bitbucket. En el caso de los tokens de API (ATAT) de la cuenta de Bitbucket, añade una clave `email` con el nombre de tu dirección de correo electrónico de Bitbucket.

En el siguiente ejemplo, se muestra cómo busca un secreto en un GitHub proveedor alojado en AWS Secrets Manager la nube:

```
{
  "token": "your-github-personal-access-token"
}
```

En el siguiente ejemplo, se muestra una contraseña de aplicación de Bitbucket (ATBB):

```
{
  "token": "your-bitbucket-app-password",
  "username": "my-bitbucket-username"
}
```

En el siguiente ejemplo, se muestra una instancia autohospedada GitLab :

```
{
  "host": "https://gitlab.mycompany.com",
  "provider_type": "gitlab",
  "token": "your-gitlab-personal-access-token"
}
```


5. Elija Siguiente.
6. Introduce un nombre secreto, por ejemplo `github-pat-myproject`.
7. (Opcional) Seleccione una clave KMS administrada por el cliente para el cifrado.
8. Complete el asistente y elija Almacenar.
9. Copia el ARN secreto. Necesita este valor al configurar el trabajo de AWS transformación.

Si utiliza una clave de KMS administrada por el cliente para cifrar su secreto (en lugar de la clave AWS administrada por defecto), debe actualizar la política de claves de KMS para permitir que AWS Transform descifre el secreto. Añada la siguiente declaración a su política de claves de KMS administrada por el 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 Sustitúyala por tu AWS región (por ejemplo `us-east-1`) y *YOUR-SECRET-ARN* por el ARN de tu secreto. La `kms:ViaService` condición garantiza que la clave KMS solo se pueda usar a través del AWS Secrets Manager servicio. La `kms:EncryptionContext:SecretARN` condición restringe el descifrado a su secreto específico.

Para actualizar su política de claves de KMS:

1. Abra la consola AWS KMS en <https://console.aws.amazon.com/kms>.
2. En el panel de navegación, elija Claves administradas por el cliente.

3. Seleccione su clave KMS.
4. En la pestaña Política de claves, elija Editar.
5. Agregue la declaración de política a la política existente.
6. Seleccione Save changes (Guardar cambios).

 Note

Si usa la clave AWS administrada predeterminada (`aws/secretsmanager`), no necesita modificar ninguna política de claves de KMS.

Configure la AWS Transformar el trabajo

1. En su trabajo de AWS Transform, vaya a Conectarse a los recursos.
2. Elige el repositorio de código fuente de Connect.
3. Seleccione el conector PAT como método de autenticación.
4. Introduce el ARN secreto del paso 2.
5. (Opcional) Introduzca el ARN de la clave de KMS si ha utilizado una clave de KMS administrada por el cliente.
6. Seleccione el repositorio y la sucursal.
7. Elija Continuar.

AWS Transform crea automáticamente un rol de IAM con los permisos necesarios para acceder a tu secreto.

Rotación y mantenimiento de los tokens

Usted es responsable de rotar los tokens PAT antes de que caduquen. Para rotar un token:

1. Genera una nueva PAT en tu proveedor de código fuente con los mismos permisos.
2. Actualice el valor secreto en AWS Secrets Manager.
3. Compruebe que su trabajo de AWS Transform pueda acceder al repositorio con el nuevo token.
4. Revoca la PAT anterior en tu proveedor de código fuente.

Solucione los problemas del conector PAT

Acceso denegado: PAT no válida

Compruebe que la PAT no haya caducado. Confirme que la PAT tenga los alcances requeridos para su proveedor. Compruebe que la PAT esté correctamente almacenada en AWS Secrets Manager.

No se puede recuperar el secreto

Compruebe que el ARN secreto es correcto. Compruebe los registros de trabajos para confirmar que AWS Transform creó el rol de IAM. Si utiliza una clave de KMS administrada por el cliente, compruebe la política de claves.

Permisos insuficientes

Es posible que la PAT carezca de los alcances necesarios para la operación. Regenera la PAT con los alcances necesarios y actualice el valor secreto en AWS Secrets Manager.

Configuración AWS CodeConnections

AWS CodeConnections utiliza una integración de proveedores gestionada que recupera automáticamente las credenciales de OAuth temporales mediante un flujo de autorización de OAuth 2.0. Los permisos se configuran en la aplicación del proveedor y son gestionados en su totalidad por AWS. Usted autoriza la aplicación una vez y se AWS encarga de toda la administración de credenciales.

1. En su trabajo de modernización de SQL Server, vaya a Conectarse a los recursos.
2. Elige el repositorio de código fuente de Connect.
3. Si no tienes una conexión existente, selecciona Crear conexión.
4. Selecciona tu proveedor de repositorios:
 - GitHub / GitHub Empresa
 - GitLab.com
 - Bitbucket Cloud
 - Repositorios de Azure
5. Siga el flujo de autorización de su proveedor.
6. Después de la autorización, elija Connect.

Seleccione su repositorio y sucursal

1. Selecciona tu repositorio de la lista.
2. Elige la rama que quieres transformar (normalmente la principal, la principal o la de desarrollo).
3. (Opcional) Especifique un subdirectorio si la aplicación.NET no está en la raíz del repositorio.
4. Elija Continuar.

Note

AWS Transform crea una nueva rama para el código transformado. Puede revisar y combinar los cambios mediante el proceso normal de revisión del código.

Aprobación del acceso al repositorio

En el GitHub caso de las plataformas y en algunas otras, el administrador del repositorio debe aprobar la solicitud de conexión:

1. AWS Transform muestra un enlace de verificación.
2. Comparta este enlace con el administrador del repositorio.
3. El administrador revisa y aprueba la solicitud en la configuración de su repositorio.
4. Una vez que el administrador aprueba la solicitud, el estado de la conexión cambia a Aprobado.

Important

El proceso de aprobación puede llevar tiempo en función de las políticas de la organización. Planifíquelo en consecuencia.

Paso 4: Crear un conector de despliegue (opcional)

Si desea implementar las aplicaciones transformadas en su AWS cuenta, tiene la opción de seleccionar un conector de implementación.

Configure el conector de despliegue

1. Seleccione Sí si desea implementar sus aplicaciones. Si selecciona No, se omitirá este paso.

2. Añada su AWS cuenta al lugar donde desee implementar las aplicaciones transformadas.
3. Añada un nombre que le ayude a recordar el conector con facilidad
4. Envíe la solicitud de aprobación del conector.

Aprobación del conector de despliegue

El administrador de su AWS cuenta debe aprobar la solicitud de conexión para el conector de despliegue.

1. AWS Transform muestra un enlace de verificación
2. Comparta este enlace con el administrador de su AWS cuenta
3. El administrador revisa y aprueba la solicitud en la configuración de su repositorio
4. Una vez aprobada, el estado de la conexión cambia a Aprobado

Important

El proceso de aprobación puede llevar tiempo en función de las políticas de la organización. Planifíquelo en consecuencia.

Paso 5: Confirme sus recursos

Tras conectarse a la base de datos y al repositorio, AWS Transform comprueba que todos los recursos necesarios estén accesibles y listos para la transformación.

Qué AWS Transform verifica

- Conectividad a la base de datos: la conexión está activa, el usuario tiene los permisos necesarios, las bases de datos son accesibles y la versión es compatible
- Acceso al repositorio: se puede acceder al repositorio, existe una sucursal, se han detectado archivos de proyecto.NET y se pueden detectar las conexiones a las bases de datos
- Preparación del entorno: la configuración de VPC es compatible con DMS, existen las funciones de AWS servicio requeridas, se ha establecido la conectividad de red y se ha confirmado la compatibilidad regional

Revise la lista de verificación previa al vuelo

1. Navegue hasta Confirmar sus recursos en el plan de trabajo
2. Revise los elementos de la lista de verificación:
 - # Conexión a la base de datos verificada
 - # Acceso al repositorio confirmado
 - # Compatible con la versión .NET
 - # Entity Framework o ADO.NET detectado
 - # Configuración de red válida
 - # Se concedieron los permisos necesarios
3. Si todos los elementos aparecen completos, selecciona Continuar
4. Si algún elemento muestra advertencias o errores, resuélvalos antes de continuar

Paso 6: Descubrimiento y evaluación

AWS Transform analiza la base de datos de SQL Server y la aplicación.NET para comprender el alcance y la complejidad de la modernización.

¿Qué se descubre

- Objetos de base de datos: tablas, vistas, índices, procedimientos almacenados, funciones, activadores, restricciones, tipos de datos, columnas calculadas, columnas de identidad, relaciones de clave externa
- Código de aplicación: estructura de proyecto.NET, modelos y configuraciones de Entity Framework, código de acceso a ADO.NET los datos, cadenas de conexión a bases de datos, llamadas a procedimientos almacenados, consultas SQL en código
- Dependencias: qué aplicaciones utilizan qué bases de datos, dependencias entre bases de datos, procedimientos almacenados compartidos, patrones comunes de acceso a los datos

Proceso de descubrimiento

- AWS Transform inicia el descubrimiento automáticamente después de la confirmación del recurso
- El descubrimiento suele tardar entre 5 y 15 minutos, según el tamaño de la base de datos y la complejidad de la aplicación
- Supervise el progreso del registro de trabajo

- AWS Transform muestra actualizaciones en tiempo real a medida que se descubren objetos

Revise los resultados del descubrimiento

Una vez finalizado el descubrimiento, vaya a Descubrimiento y evaluación para revisar:

Análisis de bases de datos:

- Recuento de objetos: número de tablas, vistas, procedimientos almacenados, funciones, activadores
- Puntuación de complejidad: evaluación de la complejidad de la transformación (baja, media, alta)
- Elementos de acción: objetos que pueden requerir atención humana
- Funciones compatibles: funciones de la base de datos que se convertirán automáticamente
- Funciones no compatibles: funciones que requieren soluciones alternativas

Análisis de aplicaciones:

- Tipo de proyecto: ASP.NET Core, aplicación de consola, biblioteca de clases, etc.
- Versión.NET: versión de .NET Core detectada
- Marco de acceso a datos: versión de Entity Framework o ADO.NET
- Conexiones a bases de datos: número de cadenas de conexión encontradas
- Complejidad del código: evaluación de la complejidad de la transformación

Mapa de dependencias:

- Representación visual de las relaciones entre la aplicación y la base de datos
- Cross-database dependencias
- componentes compartidos

Comprender la evaluación de la complejidad

AWS Transform clasifica su modernización en tres categorías:

Complejidad	Características	Resultado esperado
Bajo (clase A)	Patrones SQL estándar (ANSI SQL), procedimientos almacenados simples, tipos de datos básicos, Entity Framework con configuraciones estándar	Se espera una intervención humana mínima, alta tasa de éxito de automatización
Medio (clase B)	T-SQL Patrones avanzados, procedimientos almacenados complejos con lógica empresarial, funciones definidas por el usuario, columnas calculadas	Se requiere alguna intervención humana, pero se recomienda la revisión por parte de un experto
Alto (clase C)	Ensamblajes CLR, servidores enlazados, Service Broker, búsqueda compleja de texto completo	Se requiere una importante refactorización humana, considere un enfoque gradual

Informes de evaluación

AWS Transform genera un informe de evaluación detallado que incluye:

- Resumen ejecutivo con información general de alto nivel
- Inventario completo de bases de datos
- Inventario de aplicaciones
- Porcentaje de preparación para la transformación
- Estimación del esfuerzo
- Estrategias de evaluación y mitigación de riesgos
- Método recomendado

Puede descargar el informe de evaluación para revisarlo sin conexión y compartirlo con las partes interesadas.

Paso 7: Generar y revisar el plan de oleaje

Para grandes propiedades con múltiples bases de datos y aplicaciones, AWS Transform genera un plan de oleada que secuencia la modernización en grupos lógicos.

¿Qué es un plan de oleaje?

Un plan de oleaje organiza la modernización en fases (oleadas) en función de:

- Dependencias entre bases de datos y aplicaciones
- Prioridades empresariales
- Tolerancia al riesgo
- Disponibilidad de recursos
- Complejidad técnica

Cada oleada contiene un grupo de bases de datos y aplicaciones que se pueden modernizar juntas sin romper las dependencias.

Revise el plan de oleaje

1. Navegue hasta la planificación de olas en el plan de trabajo
2. Revise las oleadas propuestas
3. Para cada ola, revise:
 - Bases de datos incluidas
 - Aplicaciones incluidas
 - Dependencias de otras ondas
 - Tiempo estimado de transformación
 - Nivel de complejidad
 - Aplicaciones desplegables

Personalice el plan de olas

Puede personalizar el plan de olas para que se adapte a las necesidades de su empresa de dos maneras:

Uso de JSON:

1. Elija Descargar todas las oleadas para obtener un archivo JSON con todas las oleadas
2. Modifique las ondas en el JSON de la siguiente manera:
 - Mover bases de datos entre oleadas
 - Dividir las ondas en grupos más pequeños
 - Fusionar las ondas
 - Cambiando la secuencia de ondas
 - Añadir o eliminar bases de datos del ámbito
3. Vuelva a cargar el archivo JSON en la consola seleccionando Upload wave plan
4. AWS Transform valida los cambios y advierte si se infringen las dependencias
5. Seleccione Confirmar oleadas para actualizar el plan de oleadas

Uso del chat:

Puede modificar los planes de oleadas conversando con el agente y pidiéndole que mueva los repositorios y las bases de datos a oleadas específicas. Este enfoque funciona bien si necesitas hacer pequeñas modificaciones en las oleadas.

 Important

Asegúrese de que se respeten las dependencias al personalizar las olas. Transformar una aplicación dependiente antes de su base de datos puede provocar problemas.

Modernización de una sola base

Si está modernizando una sola base de datos y una aplicación, AWS Transform crea un plan sencillo de una sola vez. Puede proceder directamente a la transformación sin necesidad de planificar las oleadas.

Apruebe el plan de oleaje

1. Tras revisarlo y personalizarlo (si es necesario), elige Aprobar el plan de oleaje
2. AWS Transform bloquea el plan de oleada y pasa a la transformación
3. Aún puede modificar el plan más adelante seleccionando Editar plan de oleaje

Paso 8: Conversión del esquema

AWS Transform convierte el esquema de la base de datos de SQL Server en Aurora PostgreSQL, lo que incluye tablas, vistas, procedimientos almacenados, funciones y activadores.

Cómo funciona la conversión de esquemas

AWS Transform utiliza la conversión de esquemas de AWS DMS mejorada con IA generativa para:

- Analice los esquemas y las relaciones de SQL Server
- Asigne tipos de datos de SQL Server a equivalentes de PostgreSQL
- Transforme en T-SQL PL/pgSQL
- Gestione las columnas de identidad, las columnas calculadas y las restricciones
- Valide la conversión y la integridad referencial
- Genere elementos de acción para los objetos que requieren una revisión humana

Conversiones compatibles

Convertido automáticamente:

- Tablas, vistas e índices
- Claves principales y claves externas
- Compruebe las restricciones y los valores por defecto
- Tipos de datos más comunes
- Procedimientos almacenados sencillos
- Funciones y activadores básicos
- Columnas de identidad (convertidas a SERIAL o GENERADAS)
- La mayoría de las columnas calculadas

Puede requerir una revisión humana:

- Procedimientos almacenados complejos con avanzados T-SQL
- Server-specific Funciones SQL (GETUTCDATE, SUSER_SNAME, etc.)
- Columnas calculadas con expresiones complejas

- Full-text índices de búsqueda
- operaciones de tipos de datos XML
- Tipo de datos HIERARCHYID (requiere la extensión ltree)

No se convierte automáticamente:

- Ensamblajes CLR
- Servidores vinculados
- Service Broker
- Trabajos de agente SQL Server

Inicie la conversión del esquema

1. Navegue hasta la conversión de esquemas en el plan de trabajo
2. Revise la configuración de conversión:
 - Versión de PostgreSQL de destino
 - Opciones de extensión (ltree, PostGIS, etc.)
 - Convenciones de nomenclatura
3. Elija Iniciar conversión
4. Supervise el progreso en el registro de trabajo
5. La conversión suele tardar entre 10 y 30 minutos, según la cantidad de objetos de la base de datos

Revise los resultados de la conversión

Cuando se complete la conversión, vaya a Revisar la conversión del esquema:

Resumen de la conversión:

- Objetos convertidos: recuento de objetos convertidos correctamente
- Objetos de acción: objetos que requieren atención humana
- Advertencias: posibles problemas que hay que revisar
- Errores: objetos que no se pudieron convertir

Revisión por tipo de objeto:

- Tablas: mapeos de tipos de datos, restricciones e índices
- Procedimientos almacenados: para conversión T-SQL PL/pgSQL
- Funciones: cambios de firma y lógica de la función
- Activadores: desencadena cambios en la sintaxis y la temporización

Revise los elementos de acción

1. Seleccione Ver elementos de acción
2. Para cada elemento de acción, revisa:
 - Nombre del objeto: el objeto de la base de datos
 - Tipo de problema: ¿Qué requiere atención
 - Gravedad: crítico, de advertencia o informativo
 - Recomendación: resolución sugerida
 - Código original: versión de SQL Server
 - Código convertido: versión PostgreSQL
3. Para cada elemento de acción, puede:
 - Aceptar: usa el código convertido
 - Modificar: edita el código convertido
 - Marcar para más adelante: marcar para su revisión humana después de la transformación

Ejemplo: conversión de procedimientos almacenados

SQL Server 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;
```

Cambios realizados:

- Procedimiento convertido en función que devuelve TABLE
- Nombres de parámetros con el prefijo p_
- TOP convertido a LIMIT
- DATEDIFF convertido a EXTRACT
- GETUTCDATE () convertido a NOW ()
- Nombres de columnas convertidos a minúsculas (convención PostgreSQL)

Aprobar la conversión del esquema

1. Tras revisar todos los elementos de acción y realizar las modificaciones necesarias
2. Elija Aprobar la conversión del esquema
3. AWS Transform prepara el esquema convertido para su implementación en Aurora PostgreSQL

Note

Puede descargar el esquema convertido como scripts de SQL para revisarlo sin conexión o controlar las versiones.

Paso 9: Migración de datos (opcional)

AWS Transform ofrece opciones para migrar datos de SQL Server a Aurora PostgreSQL. La migración de datos es opcional y se puede omitir si solo necesita transformar el esquema y el código.

Opciones de migración de datos

Opción 1: migración de datos de producción

Migre sus datos de producción reales mediante AWS DMS:

- Carga inicial completa de todos los datos
- Replicación continua durante las pruebas (CDC)
- Reducción mínima del tiempo de inactividad
- Comprobaciones de validación e integridad de los datos

Opción 2: omitir la migración de datos

Transforma solo el esquema y el código:

- Útil para development/testing entornos
- Cuándo se migrarán los datos por separado
- Para proyectos de prueba de concepto

Configure la migración de datos

1. Navegue hasta Migración de datos en el plan de trabajo
2. Elige tu opción de migración:
 - Migre los datos de producción
 - Omita la migración de datos
3. Si va a migrar datos de producción, configure:
 - Tipo de migración: carga completa o carga completa + CDC
 - Validación: habilite la validación de datos
 - Rendimiento: tamaño de la instancia de DMS
 - Seleccione >Iniciar la migración

Proceso de migración de datos de producción

Si decide migrar los datos de producción:

1. Sincronización inicial: el AWS DMS realiza la carga completa de todas las tablas
2. Replicación continua: (si está habilitada la CDC) Mantiene los datos sincronizados
3. Validación: verifica el recuento de filas y la integridad de los datos
4. Preparación de la transición: se prepara para la sincronización final

Cronograma de migración:

- Bases de datos pequeñas (< 10 GB): de 30 minutos a 2 horas
- Bases de datos medianas (10-100 GB): de 2 a 8 horas
- Bases de datos grandes (> 100 GB): más de 8 horas

Validación de datos

AWS Transform valida los datos migrados con las siguientes comprobaciones:

- Comparación del recuento de filas (origen y destino)
- Integridad de la clave principal
- Relaciones de claves externas
- Compatibilidad de tipos de datos

- Resultados de columnas calculadas
- Manejo de valores nulos

Paso 10: Transformación del código de la aplicación

AWS Transform transforma el código de su aplicación.NET para que funcione con Aurora PostgreSQL en lugar de con SQL Server. Solicita un nombre de rama de destino en sus repositorios para archivar el código fuente transformado. Una vez que introduzca el nombre de la rama, AWS Transform creará una nueva rama e iniciará la transformación para que coincida con la base de datos de PostgreSQL.

¿Qué se transforma

Cambios en el marco de la entidad:

- Proveedor de base de datos: `UseSqlServer ()` → `UseNpgsql ()`
- Cadenas de conexión: formato SQL Server → formato PostgreSQL
- Asignaciones de tipos de datos: tipos de SQL Server → tipos de PostgreSQL
- DbContext configuraciones: SQL → Server-specific PostgreSQL-specific
- Archivos de migración: actualizados para garantizar la compatibilidad con PostgreSQL

ADO.NET Cambios:

- Clases de conexión: `SqlConnection` → `NpgsqlConnection`
- Clases de comandos: `SqlCommand` → `NpgsqlCommand`
- Lector de datos: `SqlDataReader` → `NpgsqlDataReader`
- Parámetros: `SqlParameter` → `NpgsqlParameter`
- Sintaxis SQL: T-SQL → PostgreSQL SQL

Cambios de configuración:

- Cadenas de conexión en `appsettings.json`
- Paquetes NuGet de proveedores de bases de datos
- Configuraciones de inyección de dependencias
- `Startup/Program.cs` configuraciones

Inicie la transformación del código

1. Navegue hasta la transformación de aplicaciones en el plan de trabajo
2. Revise la configuración de la transformación:
 - Versión de destino de .NET (si se está actualizando)
 - Versión del proveedor de PostgreSQL
 - Preferencias de estilo de código
3. Elija Iniciar transformación
4. Supervise el progreso en el registro de trabajo
5. La transformación suele tardar entre 15 y 45 minutos, según el tamaño de la base de código

Paso 11: Revise los resultados de la transformación

Antes de proceder a la implementación, revise los resultados completos de la transformación para asegurarse de que todo esté listo para las pruebas.

Puede descargar el código transformado desde la rama del repositorio para:

- Pruebas y validación locales
- Revisión del código en su IDE
- Integración con tu CI/CD pipeline
- Compromiso de control de versiones

También puedes descargar el resumen de la transformación para revisar los cambios en el lenguaje natural que AWS Transform ha realizado como parte de la transformación.

Resumen de la transformación

1. Navegue hasta el resumen de la transformación en el plan de trabajo
2. Revise los resultados generales:
 - Conversión de esquemas: objetos convertidos, elementos de acción, advertencias
 - Migración de datos: tablas migradas, filas transferidas, estado de validación
 - Transformación de código: archivos cambiados, líneas modificadas, problemas resueltos
 - Puntuación de preparación: preparación general para la implementación

Genere un informe de transformación

AWS Transform genera un informe de transformación integral:

1. Elija Generar informe
2. Seleccione el tipo de informe:
 - Resumen ejecutivo: High-level descripción general para las partes interesadas
 - Detalles técnicos: documentación completa sobre la transformación
 - Elementos de acción: lista de tareas humanas necesarias
3. Seleccione Descargar informe

El informe incluye:

- Alcance y objetivos de la transformación
- Objetos y código transformados
- Problemas encontrados y soluciones
- Resultados de la validación
- Evaluación de la preparación para el despliegue
- Recomendaciones para las pruebas

Paso 12: Validación y pruebas

Antes de implementarla en producción, compruebe que la aplicación transformada funciona correctamente con Aurora PostgreSQL.

Tipos de validación

Validación automatizada: AWS Transform realiza comprobaciones automatizadas:

- Validación del esquema con la base de datos de origen
- Verificación de la integridad de datos
- Pruebas de equivalencia de consultas
- Validación de cadenas de conexión
- Validación de la configuración

Validación humana: debe realizar pruebas adicionales:

- Pruebas funcionales de las funciones de la aplicación
- Pruebas de integración con otros sistemas
- Pruebas de rendimiento y evaluación comparativa
- Pruebas de aceptación de usuarios
- Pruebas de seguridad

Ejecute la validación automática

1. Navegue hasta Validación en el plan de trabajo
2. Elija Ejecutar validación
3. AWS Transform ejecuta las pruebas de validación:
 - Conectividad de base de datos
 - Compatibilidad de esquemas
 - Integridad de datos
 - Compilación de aplicaciones
 - Funcionalidad básica
4. Revise los resultados de la validación:
 - Superadas: pruebas que se realizaron correctamente
 - Falló: pruebas que requieren atención
 - Advertencias: posibles problemas que hay que revisar

Lista de verificación de pruebas

Funcionalidad de base de datos:

- Se puede acceder a todas las tablas
- Los procedimientos almacenados se ejecutan correctamente
- Las funciones devuelven los resultados esperados
- Activa el fuego de forma adecuada
- Restricciones aplicadas adecuadamente
- Los índices mejoran el rendimiento de las consultas

Funcionalidad de la aplicación:

- La aplicación se inicia correctamente
- Se han establecido conexiones a la base
- Las operaciones CRUD funcionan correctamente
- Las llamadas a los procedimientos almacenados se realizan correctamente
- Transacciones commit/rollback correctamente
- La gestión de errores funciona según lo esperado

Integridad de los datos:

- Los recuentos de filas coinciden con la fuente
- Las claves principales son únicas
- Claves foráneas válidas
- Las columnas calculadas son correctas
- El manejo de nulos es apropiado
- Tipos de datos compatibles

Rendimiento:

- Tiempos de respuesta a las consultas aceptables
- Se ha configurado la agrupación de conexiones
- Índices optimizados
- No hay problemas de consulta N+1
- Operaciones por lotes eficientes
- Utilización de recursos razonable

Paso 13: Despliegue

Tras una validación correcta, implemente la aplicación y la base de datos modernizadas en producción.

Opciones de implementación

- Amazon ECS y Amazon EC2 Linux

Pre-deployment lista de verificación

Antes de la implementación en producción:

- Se superaron todas las pruebas de validación
- Se han completado las pruebas de rendimiento
- Revisión de seguridad completada
- Plan de backup y reversión documentado
- Supervisión y alertas configuradas
- Equipo formado en un nuevo entorno
- Las partes interesadas están informadas del despliegue
- Periodo de mantenimiento programado

Deploy to Amazon ECS

1. Navegue hasta Despliegue en el plan de trabajo
2. Elija Implementar en ECS
3. Configure los ajustes de implementación:
 - Clúster: seleccione o cree un clúster de ECS
 - Servicio: configure el servicio ECS
 - Definición de tarea: revise la definición de tarea generada
 - Equilibrador de cargas: configurar ALB/NLB
 - Auto-scaling: Defina políticas de escalado
4. Revise la infraestructura como código (plantilla o código CDK) CloudFormation AWS
5. Elija Implementar.

Supervise el despliegue

AWS Transform implementa su aplicación:

1. Crea un clúster de Aurora PostgreSQL
2. Aplica el esquema de la base
3. Carga datos (si corresponde)
4. Despliega contenedores de aplicaciones

5. Configura el balanceador de carga

6. Configura el autoscaling

Supervise el progreso de la implementación y verifique:

- Aprovisionamiento de la infraestructura
- Inicialización de la base de datos
- Implementación de aplicaciones
- Health chequeos aprobados
- Aplicación accesible
- Las conexiones a bases de datos funcionan
- Registros que muestran el funcionamiento normal

Post-deployment validación

Tras el despliegue:

Pruebas de humo:

- Verifique la funcionalidad crítica
- Pruebe los flujos de trabajo de los usuarios clave
- Compruebe los puntos de integración
- Supervise las tasas de error

Supervisión del rendimiento:

- Rastrea los tiempos de respuesta
- Supervisa las consultas a la base
- Compruebe la utilización de los recursos
- Revise los registros de las aplicaciones

Validación de usuario:

- Realice pruebas de aceptación de los usuarios

- Recopile comentarios
- Aborda cualquier problema
- Documente las lecciones aprendidas

Procedimientos de reversión

Si surgen problemas después de la implementación:

Reversión inmediata:

- Volver a la versión anterior de la aplicación
- Vuelva a SQL Server (si aún está disponible)
- Restaure desde la copia de seguridad si es necesario

Reversión parcial:

- Revertir componentes específicos
- Mantenga los cambios en la base de
- Revierta únicamente el código de la aplicación

Corrección hacia adelante:

- Aplicar el hotfix a la versión Aurora PostgreSQL
- Implemente el código de aplicación actualizado
- Supervise para determinar su resolución

Important

Mantenga su base de datos de SQL Server disponible durante un período después de la transición para permitir la reversión si es necesario.

Post-deployment optimización

Tras una implementación exitosa:

Ajuste del rendimiento:

- Optimice las consultas lentas
- Ajuste la configuración del grupo de conexiones
- Fine-tune Parámetros de Aurora PostgreSQL
- Revise y optimice los índices

Optimización de costes:

- Right-size Instancia Aurora
- Configura el autoscaling de forma adecuada
- Revise la configuración de almacenamiento
- Optimice la retención de respaldos

Configuración de monitoreo:

- Configurar CloudWatch paneles
- Configure las alertas
- Enable Enhanced Monitoring
- Configurar Performance Insights

Documentación:

- Actualice los runbooks
- Documente los cambios en la arquitectura
- Capacite al equipo de operaciones
- Crea guías de solución de problemas

Pruebe e implemente después de la transformación

Implemente sus aplicaciones transformadas en la landing zone y valide la conectividad entre sus aplicaciones y la base de datos transformada y, si lo desea, configure CI/CD canalizaciones. Se generan ejemplos de configuraciones de CI/CD canalización como referencia para ayudarlo

a implementar la automatización de la implementación. Esta fase final valida la modernización completa.

Configure los recursos

Debe configurar los recursos utilizados en la implementación, como las funciones de IAM, los perfiles de instancia y el bucket de S3. AWS Transform no tiene permisos para crear buckets de S3 ni para realizar cambios en su IAM. Esta acción debe realizarla un usuario que tenga permisos para crear nuevas funciones. Por lo general, es el administrador de la cuenta.

Para simplificar el proceso, proporcionamos un script de configuración que automáticamente:

- Ejecuta las plantillas necesarias CloudFormation
- Crea el rol de ECS Service-Linked
- Configura todos los recursos de IAM necesarios

Important

Ejecute el script de configuración proporcionado tal cual; no modifique el nombre de ningún recurso en las plantillas o el script, ya que esto podría afectar al proceso de implementación.

Para Linux:

```
./setup.sh --region <YOUR-Region>
```

Para Windows:

```
./setup.ps1 -Region <YOUR-Region>
```

Compruebe los grupos de seguridad de su VPC

AWS Transform implementa las aplicaciones en la misma subred y el mismo grupo de seguridad que la instancia de Aurora PostgreSQL.

Para que la aplicación se conecte a la instancia de Aurora, asegúrese de que este grupo de seguridad tenga reglas de salida que permitan la conexión al mismo grupo de seguridad y reglas de entrada que permitan la conexión desde el mismo grupo de seguridad.

Seleccione y configure las aplicaciones

La interfaz de usuario de AWS Transform muestra una lista de aplicaciones que se pueden implementar. Seleccione la aplicación y haga clic en Configurar y confirmar para abrir una ventana de configuración en la que puede especificar:

- Infraestructura de destino para las aplicaciones: seleccione ECS o una de las instancias EC2
- Parámetros de aplicación o instancia

Tras completar y cerrar la ventana de configuración, AWS transforme:

- Genera artefactos de despliegue en función de su configuración
- Confirma estos artefactos en su repositorio, que incluyen:
 - Scripts de implementación
 - CloudFormation plantillas
 - Ejemplos de configuraciones de CI/CD canalización (que puede utilizar como referencia para configurar la automatización del despliegue)

Una vez completada la confirmación, el estado de la aplicación cambia a Configurada y confirmada. A continuación, puede seleccionar las aplicaciones y utilizar el botón Implementar situado en la parte superior derecha para iniciar la implementación.

Implementación de ECS

Todas las aplicaciones con un ECS de destino se implementan en un nuevo clúster de ECS que se crea en su cuenta. Cada aplicación se implementa en su propio contenedor dedicado; no se admiten varias aplicaciones por contenedor. Los parámetros del contenedor para cada aplicación se configuran de forma individual, como la CPU y la memoria requeridas.

Implementación de EC2

Puede seleccionar una de las instancias EC2 propuestas y configurar sus parámetros, como el tipo de instancia. Se pueden implementar varias aplicaciones en la misma instancia de EC2:

- Para implementar varias aplicaciones en una sola instancia, seleccione la misma instancia EC2 de destino para cada una de estas aplicaciones durante la configuración.

- Todas las aplicaciones que tienen la misma instancia seleccionada como destino se implementan en esa instancia y se les asignan diferentes puertos aleatorios.
- Tenga en cuenta que si edita los parámetros de la instancia para una aplicación y, a continuación, edita otra aplicación destinada a la misma instancia, los cambios afectarán a todas las aplicaciones implementadas en esa instancia.

La implementación se realizó correctamente

Tras una implementación exitosa, sus aplicaciones se ejecutan en Aurora PostgreSQL con costos de licencia reducidos, rendimiento mejorado y escalabilidad nativa de la nube. El trabajo permanece abierto a menos que se detenga explícitamente. Esto permite la opción de un posible redespigie con parámetros de despliegue actualizados.

Prácticas recomendadas y solución de problemas

Las mejores prácticas y los problemas comunes y sus soluciones durante el proceso de modernización.

Registros de aplicaciones de ECS

CloudWatch registros

- Todos los registros del contenedor ECS se envían automáticamente a CloudWatch Logs
- Acceda a los registros de la CloudWatch consola, en Grupos de registros
- Formato de denominación de los grupos de registros:aws/ecs/{application-name}
- Cada instancia de contenedor crea un nuevo flujo de registro dentro del grupo

Visualización de registros

A través de AWS la consola:

- Vaya a CloudWatch > Grupos de registros
- Seleccione el grupo de registros de su aplicación
- Elija el flujo de registro correspondiente para ver los registros del contenedor

Uso de AWS CLI:

```
aws logs get-log-events --log-group-name /aws/ecs/your-app-name --log-stream-name your-stream-name
```

Ubicaciones de registro comunes

- Registros de aplicaciones: CloudWatch registros
- Eventos del servicio de ECS: Consola de ECS > Clúster > Servicio > pestaña Eventos
- Contenedor health/status: Consola ECS > Clúster > Servicio > pestaña Tareas

Administración de conexiones a bases de datos

Las aplicaciones utilizan variables de entorno para la configuración de conexión a la base de datos

Si tiene problemas de conectividad:

- Compruebe la configuración de conexión actual en las variables de entorno
- Actualice las variables de entorno para modificar las cadenas de conexión a la base de datos según sea necesario
- Los cambios en la cadena de conexión se pueden realizar mediante actualizaciones de variables de entorno sin necesidad de volver a implementar la aplicación

Problemas de conexión a bases de datos

Problema: no se puede conectar AWS Transform a SQL Server

Soluciones:

- Compruebe la conectividad de red entre AWS Transform y SQL Server
- Compruebe las reglas del grupo de seguridad para garantizar el acceso adecuado a los puertos (1433)
- Confirme las credenciales de la base de datos en Secrets Manager
- Pruebe los permisos de la base de datos con el usuario creado
- Asegúrese de que SQL Server esté configurado para la autenticación en modo mixto
- Compruebe que el secreto tiene las etiquetas requeridas (proyecto: atx-db-modernization, propietario: database-connector)

Problemas con el firewall y el grupo de seguridad

Problema: se agotó el tiempo de espera de la conexión o errores de «no se puede acceder a la base de

Causa principal: los grupos de seguridad o las ACL de red bloquean el tráfico

Soluciones:

1. Compruebe la configuración del grupo de seguridad:

- Confirme que su grupo de seguridad de SQL Server tenga una regla de entrada que permita el puerto 1433 del grupo de seguridad DMS Schema Conversion
- Compruebe que la fuente es el ID del grupo de seguridad (por ejemplo, sg-0123456789abcdef0) y no una dirección IP
- Compruebe que el grupo de seguridad de conversión de esquemas de DMS esté correctamente especificado en el perfil de instancia
- Asegúrese de que no haya reglas de denegación contradictorias

2. Compruebe las ACL de red:

- Compruebe que las ACL de red a nivel de subred permitan el tráfico entrante en el puerto 1433
- Asegúrese de que las ACL de red permitan el tráfico de retorno a los puertos efímeros salientes
- Compruebe las ACL de red de la subred de la base de datos y de la subred del DMS

3. Verifique la configuración de la VPC:

- Confirme que la instancia de conversión de esquemas de DMS y SQL Server estén en la misma VPC o que tengan el emparejamiento de VPC adecuado
- Compruebe que las tablas de rutas permiten el tráfico entre subredes
- Compruebe que ningún dispositivo de firewall esté bloqueando el tráfico

4. Pruebe la conectividad:

- Lance una instancia EC2 de prueba en la misma subred que DMS Schema Conversion
- Adjunte el mismo grupo de seguridad que DMS Schema Conversion
- Pruebe la conexión a SQL Server mediante telnet o SQL Server Management Studio
- Si la prueba se realiza correctamente, el problema está en la configuración de AWS Transform; si falla, el problema es network/firewall

Error común: abrir el puerto 1433 a 0.0.0. 0/0 (todas las fuentes) es un riesgo para la seguridad. Utilice siempre el control de acceso basado en grupos de seguridad para limitar el acceso únicamente al grupo de seguridad DMS Schema Conversion.

Problemas de conversión de esquemas

Problema: la conversión de esquemas muestra muchos elementos de acción

Soluciones:

- Revisa las acciones del informe de conversión
- Priorice en función del impacto
- Utilice Amazon Q Developer para conversiones SQL complejas
- Consulte AWS Support para obtener orientación
- Considere un enfoque gradual para bases de datos complejas

Problemas de transformación de aplicaciones

Problema: la transformación de las aplicaciones no se construye

Soluciones:

- Revise los errores de compilación en el informe de transformación
- Configure los NuGet feeds privados si es necesario
- Actualice las referencias de los paquetes si es necesario
- Compruebe si hay Windows-specific dependencias
- Revise los registros de transformación para ver si hay errores detallados

Problemas de migración de datos

Problema: la validación de la migración de datos falla

Soluciones:

- Revise el informe de validación para ver si hay errores específicos
- Compruebe las asignaciones de tipos de datos

- Verifique la configuración de las columnas de identidad (GENERADAS DE FORMA PREDETERMINADA o GENERADAS SIEMPRE)
- Revise las expresiones de columna calculadas
- Póngase en contacto con AWS Support para problemas de datos complejos

Problemas de limpieza de recursos

Problema: el trabajo de transformación falla debido a errores en los recursos

Soluciones:

- Compruebe los recursos de DMS existentes (proyectos de migración, proveedores de datos, perfiles de instancia)
- Limpie los recursos fallidos o incompletos de intentos anteriores
- Compruebe que los secretos no estén programados para su eliminación
- Compruebe las cuotas de servicio para DMS y Aurora PostgreSQL
- Ponte en contacto con AWS Support si la limpieza no resuelve el problema

Problemas de implementación

Problema: la aplicación transformada no puede conectarse a Aurora PostgreSQL

Soluciones:

- Verificar el formato de la cadena de conexión para PostgreSQL
- Compruebe las reglas de los grupos de seguridad
- Verificar las credenciales de la base de datos en Secrets Manager
- Asegúrese de SSL/TLS que esté configurado correctamente
- Probar la conexión mediante psql o pgAdmin

Cómo obtener ayuda adicional

Cuando te AWS pongas en contacto con Support, proporciona:

- ID del trabajo de transformación
- AWS ID de cuenta

- Region
- Mensajes de error y capturas de pantalla
- Registros de transformación (disponibles en la consola AWS Transform)

Seguridad en AWS Transformar

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El <https://aws.amazon.com/compliance/shared-responsibility-model/> describe estos conceptos como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de [AWS cumplimiento de los programas](#) de . Para obtener más información sobre los programas de cumplimiento que se aplican a AWS Transform, consulte [AWS Servicios dentro del alcance por programa de cumplimiento AWS](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar AWS Transform. En los temas siguientes, se muestra cómo configurar AWS Transform para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de AWS Transform.

Temas

- [Protección de datos en AWS Transform](#)
- [Administración de identidad y acceso para AWS Transformar](#)
- [Validación de conformidad para AWS Transformar](#)
- [Resiliencia en AWS Transformar](#)
- [AWS Transform y puntos finales de interfaz \(AWS PrivateLink\)](#)
- [Acceder al AWS Transform aplicación web desde una VPC](#)

Protección de datos en AWS Transform

El [modelo de responsabilidad AWS compartida](#) se aplica a la protección de datos en AWS Transform. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad Servicios de AWS que utilice. Para obtener más información sobre la privacidad de datos, consulte [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación del blog [AWS Shared Responsibility Model and GDPR](#) en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS Identity and Access Management (IAM). De esta manera, cada usuario recibe únicamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes maneras:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad gestionados avanzados Amazon Macie, como los que ayudan a descubrir y proteger los datos confidenciales almacenados en ellos Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un terminal FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Se recomienda encarecidamente no introducir nunca información confidencial, como, por ejemplo, direcciones de correo electrónico de clientes, en [etiquetas](#) o campos de formato libre, como, por ejemplo, el campo Nombre. Esto incluye cuando trabaja AWS Transform o Servicios de AWS utiliza la API AWS Management Console, AWS Command Line Interface (AWS CLI) o los SDK. AWS Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Para obtener más información sobre cómo se AWS Transform usa el contenido, consulte [AWS Transform mejora del servicio](#).

AWS Transform almacena sus preguntas, sus respuestas y el contexto adicional, como los metadatos de la consola y el código en su IDE, para generar respuestas a sus preguntas. Para obtener más información sobre cómo se cifran los datos, consulte [Cifrado de datos en AWS Transform](#). Para obtener información sobre cómo AWS utilizar algunas de sus preguntas AWS Transform y sus respuestas para mejorar nuestros servicios, consulte [AWS Transform mejora del servicio](#).

En AWS Transform, sus datos se almacenan en la AWS región en la que se creó su AWS Transform perfil.

Con la inferencia cruzada, es AWS Transform posible que sus solicitudes se procesen en una región diferente dentro de la zona geográfica en la que se almacenan sus datos. [Para obtener más información, consulte Cross-Region inferencia](#).

Temas

- [Cross-region procesamiento en AWS Transform](#)
- [Cifrado de datos en AWS Transform](#)
- [AWS Transform mejora del servicio](#)

Cross-region procesamiento en AWS Transform

En las siguientes secciones se describe cómo se utilizan la inferencia entre regiones y las llamadas entre regiones para proporcionar el servicio. AWS Transform

Cross-region inferencia

AWS Transform funciona con Amazon Bedrock y utiliza la inferencia entre regiones para distribuir el tráfico entre diferentes regiones a fin de mejorar el rendimiento y la Regiones de AWS fiabilidad de las inferencias de modelos de lenguaje grandes (LLM). Con la inferencia entre regiones, obtendrá:

- Un mayor rendimiento y resiliencia durante los periodos de alta demanda
- Un mayor rendimiento
- Acceso a funciones y AWS Transform funciones recientemente lanzadas que se basan en los LLM más potentes alojados en Amazon Bedrock

Cross-region las solicitudes de inferencia se mantienen dentro de la zona geográfica en la Regiones de AWS que se encuentran originalmente los datos. Por ejemplo, una solicitud realizada desde una

AWS Transform configuración de EE. UU. se guarda dentro de Regiones de AWS EE. UU. Aunque la inferencia entre regiones no cambia el lugar en el que se almacenan los datos, es posible que las solicitudes y los resultados de salida se trasladen fuera de la región en la que se encuentran originalmente los datos. Todos los datos se transmitirán cifrados a través de la red segura de Amazon. El uso de la inferencia entre regiones no conlleva ningún costo adicional.

La inferencia entre regiones no afecta el lugar en el que se almacenan los datos. Para obtener información sobre dónde se almacenan los datos cuando los usas AWS Transform, consulta [Protección de datos en AWS Transform](#).

Regiones compatibles para AWS Transform inferencia entre regiones

Es posible que algunas solicitudes que AWS Transform realices requieran llamadas entre regiones. En la siguiente tabla se describen las regiones a las que se pueden dirigir las solicitudes en función de la zona geográfica en la que se originó la solicitud.

Región de origen	Regiones de destino
Este de EE. UU. (Norte de Virginia) (us-east-1)	Este de EE. UU. (Norte de Virginia) (us-east-1)
	Este de EE. UU. (Ohio) (us-east-2)
	Oeste de EE. UU. (Oregón) (us-west-2)
Europa (Fráncfort) (eu-central-1)	Europa (Fráncfort) (eu-central-1)
	UE (Estocolmo) (eu-north-1)
	UE (Milán) (eu-south-1)
	Europa (España) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (París) (eu-west-3)
Asia-Pacífico (Mumbai) (ap-south-1)	Asia-Pacífico (Tokio) (ap-northeast-1)
	Asia-Pacífico (Seúl) (ap-northeast-2)
	Asia Pacific (Osaka) (ap-northeast-3)

Región de origen	Regiones de destino
	Asia-Pacífico (Mumbai) (ap-south-1)
	Asia Pacífico (Hyderabad) (ap-south-2)
	Asia-Pacífico (Singapur) (ap-southeast-1)
	Asia-Pacífico (Sídney) (ap-southeast-2)
	Asia Pacífico (Melbourne) (ap-southeast-4)
Asia-Pacífico (Tokio) (ap-northeast-1)	Asia-Pacífico (Tokio) (ap-northeast-1)
	Asia Pacific (Osaka) (ap-northeast-3)
Asia-Pacífico (Seúl) (ap-northeast-2)	Asia-Pacífico (Tokio) (ap-northeast-1)
	Asia-Pacífico (Seúl) (ap-northeast-2)
	Asia Pacific (Osaka) (ap-northeast-3)
	Asia-Pacífico (Mumbai) (ap-south-1)
	Asia Pacífico (Hyderabad) (ap-south-2)
	Asia-Pacífico (Singapur) (ap-southeast-1)
	Asia-Pacífico (Sídney) (ap-southeast-2)
	Asia Pacífico (Melbourne) (ap-southeast-4)
Asia-Pacífico (Sídney) (ap-southeast-2)	Asia-Pacífico (Sídney) (ap-southeast-2)
	Asia Pacífico (Melbourne) (ap-southeast-4)

Región de origen	Regiones de destino
Europa (Londres) (eu-west-2)	Europa (Fráncfort) (eu-central-1)
	UE (Estocolmo) (eu-north-1)
	UE (Milán) (eu-south-1)
	Europa (España) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (Londres) (eu-west-2)
	Europa (París) (eu-west-3)
Canadá (centro) (ca-central-1)	Comercial Regiones de AWS + Canadá (central) (ca-central-1)
América del Sur (São Paulo) (sa-east-1)	Comercial Regiones de AWS + Sudamérica (São Paulo) (sa-east-1)

Para obtener una lista completa de las regiones que puede utilizar AWS Transform, consulte.

[Regiones compatibles para AWS Transform](#)

Cross-Region conocimiento

Cuando haga una pregunta general sobre AWS Transform los servicios, los flujos de trabajo de transformación o la AWS documentación relacionada, AWS Transform puede realizar solicitudes entre regiones a EE. UU. Este (Virginia) (us-east-1) para las regiones de EE. UU. o Europa (Fráncfort) (eu-central-1) para todas las demás regiones a fin de recuperar la documentación y tramitar su solicitud. Por ejemplo, cuando haga preguntas sobre cómo utilizar otros AWS servicios, como Lambda, AWS Transform puede realizar una llamada entre regiones para recuperar la AWS documentación pertinente y responder a su pregunta. En la siguiente tabla se describen las regiones a las que se pueden dirigir las solicitudes en función de la zona geográfica en la que se originó la solicitud.

Región de origen	Regiones de destino
Este de EE. UU. (Norte de Virginia) (us-east-1)	Este de EE. UU. (Norte de Virginia) (us-east-1)
Europa (Fráncfort) (eu-central-1)	Europa (Fráncfort) (eu-central-1)
Europa (Londres) (eu-west-2)	Europa (Fráncfort) (eu-central-1)
Asia-Pacífico (Tokio) (ap-northeast-1)	Europa (Fráncfort) (eu-central-1)
Asia-Pacífico (Sídney) (ap-southeast-2)	Europa (Fráncfort) (eu-central-1)
Asia-Pacífico (Seúl) (ap-northeast-2)	Europa (Fráncfort) (eu-central-1)
Asia-Pacífico (Mumbai) (ap-south-1)	Europa (Fráncfort) (eu-central-1)
Canadá (centro) (ca-central-1)	Europa (Fráncfort) (eu-central-1)
América del Sur (São Paulo) (sa-east-1)	Europa (Fráncfort) (eu-central-1)

Esta configuración está activada de forma predeterminada. Un administrador de cuentas puede modificar esta configuración. Al deshabilitar esta función, se pierde el acceso a las funciones que requieren AWS Transform recuperar conocimientos de otras regiones. Esto podría provocar respuestas menos precisas.

Para deshabilitar las llamadas entre regiones realizadas por AWS Transform:

1. Al realizar la configuración por primera vez AWS Transform, diríjase a la página de introducción y complete la configuración. Para una AWS Transform configuración existente, vaya a la página de configuración.
2. Activa las llamadas entre regiones para responder a preguntas generales AWS relacionadas con la posición de desactivación.

AWS Transform para la inferencia entre regiones de Windows

La siguiente tabla muestra las regiones de origen desde las que puede llamar al perfil de inferencia y las regiones de destino a las que se pueden dirigir las solicitudes:

Región de origen	Regiones de destino de inferencia
Este de EE. UU. (Norte de Virginia) (us-east-1)	Este de EE. UU. (Norte de Virginia) (us-east-1) Este de EE. UU. (Ohio) (us-east-2) Oeste de EE. UU. (Oregón) (us-west-2)
Europa (Fráncfort) (eu-central-1)	Europa (Fráncfort) (eu-central-1) UE (Estocolmo) (eu-north-1) UE (Milán) (eu-south-1) Europa (España) (eu-south-2) Europa (Irlanda) (eu-west-1) Europa (París) (eu-west-3)
Asia-Pacífico (Tokio) (ap-northeast-1)	Asia-Pacífico (Tokio) (ap-northeast-1) Asia Pacific (Osaka) (ap-northeast-3)
Asia-Pacífico (Sídney) (ap-southeast-2)	Asia-Pacífico (Sídney) (ap-southeast-2) Asia Pacífico (Melbourne) (ap-southeast-4)
Asia-Pacífico (Seúl) (ap-northeast-2)	Todas las regiones comerciales
Asia-Pacífico (Mumbai) (ap-south-1)	Todas las regiones comerciales
Canadá (centro) (ca-central-1)	Todas las regiones comerciales

AWS Transform para la inferencia interregional de migraciones

La siguiente tabla muestra las regiones de origen desde las que puede llamar al perfil de inferencia y las regiones de destino a las que se pueden dirigir las solicitudes:

Región de origen	Regiones de destino de inferencia
Este de EE. UU. (Norte de Virginia) (us-east-1)	Todas las regiones comerciales
Europa (Fráncfort) (eu-central-1)	Todas las regiones comerciales
Europa (Londres) (eu-west-2)	Todas las regiones comerciales
Asia-Pacífico (Tokio) (ap-northeast-1)	Asia-Pacífico (Tokio) (ap-northeast-1) Asia Pacific (Osaka) (ap-northeast-3)
Asia-Pacífico (Sídney) (ap-southeast-2)	Asia-Pacífico (Sídney) (ap-southeast-2) Asia Pacific (Melbourne) (ap-southeast-4)
Asia-Pacífico (Seúl) (ap-northeast-2)	Todas las regiones comerciales
Asia-Pacífico (Mumbai) (ap-south-1)	Todas las regiones comerciales
Canadá (centro) (ca-central-1)	Todas las regiones comerciales

AWS Transform para la inferencia entre regiones de mainframe

AWS Transform para mainframe utiliza la inferencia geográfica entre regiones de Amazon Bedrock. Esto significa que es posible que algunas de sus llamadas se dirijan a Regiones de AWS fuera de su región de origen. La siguiente tabla muestra las regiones de origen desde las que puede llamar al perfil de inferencia y las regiones de destino a las que se pueden dirigir las solicitudes:

Región de origen	Regiones de destino de inferencia
Este de EE. UU. (Norte de Virginia) (us-east-1)	Este de EE. UU. (Norte de Virginia) (us-east-1) Este de EE. UU. (Ohio) (us-east-2) Oeste de EE. UU. (Oregón) (us-west-2)
Europa (Fráncfort) (eu-central-1)	Europa (Fráncfort) (eu-central-1) UE (Estocolmo) (eu-north-1)

Región de origen	Regiones de destino de inferencia
	UE (Milán) (eu-south-1) Europa (España) (eu-south-2) Europa (Irlanda) (eu-west-1) Europa (París) (eu-west-3)
Europa (Londres) (eu-west-2)	Europa (Fráncfort) (eu-central-1) UE (Estocolmo) (eu-north-1) UE (Milán) (eu-south-1) Europa (España) (eu-south-2) Europa (Irlanda) (eu-west-1) Europa (Londres) (eu-west-2) Europa (París) (eu-west-3)
Asia-Pacífico (Tokio) (ap-northeast-1)	Asia-Pacífico (Tokio) (ap-northeast-1) Asia Pacific (Osaka) (ap-northeast-3)
Asia-Pacífico (Sídney) (ap-southeast-2)	Asia-Pacífico (Sídney) (ap-southeast-2) Asia Pacífico (Melbourne) (ap-southeast-4)
Asia-Pacífico (Seúl) (ap-northeast-2)	Todas las regiones comerciales
Asia-Pacífico (Mumbai) (ap-south-1)	Todas las regiones comerciales
Canadá (centro) (ca-central-1)	Canadá (centro) (ca-central-1) Este de EE. UU. (Norte de Virginia) (us-east-1) Este de EE. UU. (Ohio) (us-east-2) Oeste de EE. UU. (Oregón) (us-west-2)

Región de origen	Regiones de destino de inferencia
América del Sur (São Paulo) (sa-east-1)	Todas las regiones comerciales

AWS Transform Personalizada

AWS Transform custom utiliza la inferencia geográfica entre regiones de Amazon Bedrock. Esto significa que es posible que algunas de sus llamadas se dirijan a Regiones de AWS fuera de su región de origen. La siguiente tabla muestra las regiones de origen desde las que puede llamar al perfil de inferencia y las regiones de destino a las que se pueden dirigir las solicitudes:

Región de origen	Regiones de destino de inferencia
Este de EE. UU. (Norte de Virginia) (us-east-1)	Este de EE. UU. (Norte de Virginia) (us-east-1)
	Este de EE. UU. (Ohio) (us-east-2)
	Oeste de EE. UU. (Oregón) (us-west-2)
Europa (Fráncfort) (eu-central-1)	Europa (Fráncfort) (eu-central-1)
	UE (Estocolmo) (eu-north-1)
	UE (Milán) (eu-south-1)
	Europa (España) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (París) (eu-west-3)
Europa (Londres) (eu-west-2)	Europa (Fráncfort) (eu-central-1)
	UE (Estocolmo) (eu-north-1)
	UE (Milán) (eu-south-1)
	Europa (España) (eu-south-2)
	Europa (Irlanda) (eu-west-1)

Región de origen	Regiones de destino de inferencia
	Europa (Londres) (eu-west-2)
	Europa (París) (eu-west-3)
Asia-Pacífico (Tokio) (ap-northeast-1)	Todas las regiones comerciales
Asia-Pacífico (Sídney) (ap-southeast-2)	Asia-Pacífico (Sídney) (ap-southeast-2)
	Asia Pacífico (Melbourne) (ap-southeast-4)
Asia-Pacífico (Seúl) (ap-northeast-2)	Todas las regiones comerciales
Asia-Pacífico (Mumbai) (ap-south-1)	Todas las regiones comerciales
Canadá (centro) (ca-central-1)	Canadá (centro) (ca-central-1)
	Este de EE. UU. (Norte de Virginia) (us-east-1)
	Este de EE. UU. (Ohio) (us-east-2)
	Oeste de EE. UU. (Oregón) (us-west-2)

Cifrado de datos en AWS Transform

En este tema se proporciona información específica AWS Transform sobre el cifrado en tránsito y el cifrado en reposo.

AWS Transform proporciona cifrado de forma predeterminada para proteger los datos confidenciales de los clientes almacenados mediante el cifrado mediante claves AWS propias.

Tipos de cifrado

Cifrado en tránsito

La comunicación entre los clientes AWS Transform AWS Transform y sus dependencias descendentes está protegida mediante conexiones TLS 1.2 o superior.

⚠ Important

Cuando [conecta una cuenta de descubrimiento](#), AWS Transform crea un bucket de Amazon S3 en su nombre en esa cuenta. Ese depósito no está SecureTransport activado de forma predeterminada. Si quieres que la política de cubos incluya el transporte seguro, debes actualizarla. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon S3](#).

Cifrado en reposo

AWS Transform almacena los datos en reposo mediante Amazon DynamoDB y Amazon Simple Storage Service (Amazon S3). Los datos en reposo se cifran mediante soluciones de AWS cifrado de forma predeterminada. AWS Transform cifra los datos mediante el uso de claves AWS propias de AWS Key Management Service (AWS KMS). No tiene que tomar ninguna medida para proteger las claves AWS administradas que cifran sus datos. Para obtener más información, consulte [AWS owned keys](#) en la AWS Key Management Service Guía para desarrolladores de .

Tipo de datos:	AWS-cifrado de claves propias	Cifrado de claves administradas por el cliente (opcional)
Datos del grupo de clientes	Habilitado	Habilitado
Entradas y salidas de los clientes, como el código y la documentación, almacenados en un bucket de Amazon S3		
Tienda de artefactos	Habilitado	Habilitado
Artefactos intermedios como parte de la transformación del código almacenados en un bucket de S3		
Objetivo del trabajo	Habilitado	Habilitado

Tipo de datos:	AWS-cifrado de claves propias	Cifrado de claves administradas por el cliente (opcional)
La intención del cliente con respecto al trabajo almacenado en un bucket de Amazon S3		
Mensajes de chat	Habilitado	Habilitado
Mensajes entre el cliente y AWS Transform almacenados en un bucket de Amazon S3		
Base de conocimientos de Chat	Habilitado	Habilitado
Datos indexados relevantes para el chat del cliente AWS Transform y almacenados en Amazon OpenSearch y procesados a través AWS de Bedrock		

Nota: El cliente puede registrar su propia clave gestionada por el cliente (CMK) para usarla para cifrar todos los tipos de datos anteriores.

Las claves administradas por el cliente son claves KMS de su AWS cuenta que usted crea, posee y administra para controlar directamente el acceso a sus datos mediante el control del acceso a la clave KMS. Solo se admiten claves simétricas. Para obtener información sobre cómo crear tu propia clave de KMS, consulta [Cómo crear claves](#) en la Guía para AWS Key Management Service desarrolladores.

Cuando utiliza una clave gestionada por el cliente, AWS Transform utiliza las concesiones de KMS, lo que permite a los usuarios, roles o aplicaciones autorizados utilizar una clave de KMS. Cuando un AWS Transform administrador decide utilizar una clave gestionada por el cliente para el cifrado durante la configuración, se crea una concesión para él. Esta concesión es lo que permite al usuario final utilizar la clave de cifrado para el cifrado de datos en reposo. Para obtener más información sobre las concesiones, consulte [Grants in AWS KMS](#).

AWS Claves propias (por defecto)

Note

AWS claves propias: AWS Transform utiliza estas claves de forma predeterminada para cifrar automáticamente los datos de identificación personal. No puede ver, administrar ni usar las claves AWS propias, ni auditar su uso. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran sus datos. Para obtener más información, consulte las claves AWS propias en la Guía AWS para desarrolladores del Servicio de administración de claves.

El cifrado de los datos en reposo de forma predeterminada ayuda a reducir la sobrecarga operativa y la complejidad que implica la protección de los datos confidenciales. Al mismo tiempo, le permite crear aplicaciones seguras que cumplen con los estrictos requisitos normativos y de conformidad con el cifrado.

Si bien no puedes deshabilitar esta capa de cifrado ni seleccionar un tipo de cifrado alternativo, puedes añadir una segunda capa de cifrado sobre las claves de cifrado que ya AWS poseas si eliges una clave gestionada por el cliente al crear la transformación:

Claves administradas por el cliente (opcionales)

Claves administradas por el cliente: AWS Transform admite el uso de una clave simétrica administrada por el cliente que usted crea, posee y administra para agregar una segunda capa de cifrado sobre el cifrado existente mediante claves AWS propias. Como usted tiene el control total de este cifrado, puede realizar dichas tareas como:

- Establecer y mantener políticas de claves
- Establecer y mantener concesiones y políticas de IAM
- Habilitar y deshabilitar políticas de claves
- Rotar el material criptográfico
- Adición de etiquetas de
- Crear alias de clave
- Rotar el material criptográfico
- Adición de etiquetas de

- Crear alias de clave
- Programar la eliminación de claves
- Para obtener más información, consulte [clave administrada por el cliente](#) en la Guía para desarrolladores de AWS Key Management Service.

 Note

AWS Transform habilita automáticamente el cifrado en reposo mediante claves AWS propias para proteger los datos de identificación personal sin coste alguno. Sin embargo, se aplican AWS KMS cargos por el uso de una clave gestionada por el cliente. Para obtener más información acerca de los precios, consulte [Precios de AWS Key Management Service](#).

Para obtener más información AWS KMS, consulte [¿Qué es AWS Key Management Service?](#)

Cómo AWS Transform utiliza las subvenciones en AWS Key Management Service

AWS Transform requiere una concesión para usar la clave gestionada por el cliente.

Al crear un [nombre del recurso] cifrado con una clave gestionada por el cliente, AWS Transform crea una concesión en tu nombre enviando una CreateGrant solicitud a AWS Key Management Service. Las concesiones in se AWS Key Management Service utilizan para dar AWS Transform acceso a una clave de KMS en la cuenta de un cliente.

AWS Transform requiere la concesión para utilizar la clave gestionada por el cliente en las siguientes operaciones internas:

- Envíe solicitudes a la [API de KMS] AWS KMS para comprobar que el identificador de clave de KMS simétrico gestionado por el cliente introducido al crear [nombre del recurso] es válido.
- Envíe solicitudes de [API de KMS] AWS KMS a para generar claves de datos cifradas por su clave administrada por el cliente.
- Envíe solicitudes a la [API de KMS] AWS KMS para descifrar las claves de datos cifradas para que puedan usarse para cifrar sus datos.

Puede revocar el acceso a la concesión o eliminar el acceso del servicio a la clave administrada por el cliente en cualquier momento. Si lo hace, AWS Transform no podrá acceder a ninguno de

los datos cifrados por la clave gestionada por el cliente, lo que afectará a las operaciones que dependen de esos datos. Por ejemplo, si intentas obtener el [nombre del recurso] de un [nombre del recurso] cifrado al que no AWS Transform se puede acceder, la operación devolverá un `AccessDeniedException` error.

Creación de una clave administrada por el cliente

Puede crear una clave simétrica gestionada por el cliente mediante la consola AWS de gestión o las AWS Key Management Service API.

Para crear una clave simétrica administrada por el cliente, siga los pasos para [crear claves asimétricas administradas por el cliente](#) de la Guía del desarrollador de AWS Key Management Service .

Para utilizar la clave gestionada por el cliente con AWS Transform los recursos, la política de claves debe permitir las siguientes operaciones de API:

kms: CreateGrant — Añade una concesión a una clave gestionada por el cliente. Otorga el acceso de control a una clave KMS específica, que permite el acceso a las operaciones de concesión AWS Transform necesarias. Para obtener más información sobre el [uso de concesiones](#), consulte la Guía para desarrolladores de AWS Key Management Service .

Esto permite AWS Transform hacer lo siguiente:

- Llame a la API [KMS ([GenerateDataKeyWithoutPlainText/GenerateDatakey](#))] para generar una clave de datos cifrada y almacenarla, ya que la clave de datos no se utiliza inmediatamente para cifrar.
- Llama a [KMS API ([Decrypt](#))] para usar la clave de datos cifrados almacenada para acceder a los datos cifrados.
- Configurar una entidad principal que se retire para permitir que el servicio [RetireGrant](#).
- [kms: DescribeKey](#) — Proporciona los detalles de la clave administrada por el cliente para permitir que [Nombre del servicio] valide la clave.

Cifrado para la modernización de SQL

Durante el proceso de [modernización de SQL Server](#), AWS Transform crea recursos en su cuenta, como instancias de EC2, clústeres de ECS, imágenes de ECR y objetos de S3. Tiene la opción de proporcionar una clave administrada por el cliente para cifrar los datos de su cuenta. Deberá

etiquetar su clave KMS con la clave CreatedFor el valor AWSTransform. En este ejemplo de política, se enumeran los permisos mínimos necesarios en su política de claves si no tiene una política de claves predeterminada. Si tiene una política de claves predeterminada, debe actualizar manualmente la clave de KMS además de la política de claves predeterminada para que ECS pueda utilizarla.

```
"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"
      }
    }
  }
}
]

```

Cifrado para migración de bases de datos

Durante el proceso de migración de la base de datos, AWS Transform utiliza AWS Database Migration Service (DMS) para migrar los datos de la base de datos. Si lo desea, puede proporcionar una clave administrada por el cliente para cifrar los datos de la base de datos durante la migración.

La siguiente política contiene tres declaraciones. La primera declaración otorga permisos a la cuenta raíz para la AWS KMS clave. La segunda afirmación permite que la función de conector valide la clave durante el descubrimiento. La tercera afirmación permite que la función de conector utilice la clave para las operaciones del 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"
  }
}
}
```

Uso de claves de KMS administradas por el cliente

Tras crear una clave de KMS gestionada por el cliente, el AWS Transform administrador debe proporcionarla en la AWS Transform consola para utilizarla para cifrar los datos.

Para configurar una clave gestionada por el cliente para cifrar los datos AWS Transform, los administradores necesitan permisos de uso. AWS KMS

Para utilizar una funcionalidad cifrada con una clave gestionada por el cliente, los usuarios necesitan permisos que les permitan acceder AWS Transform a la clave gestionada por el cliente.

Si aparece un error relacionado con las concesiones de KMS durante el uso AWS Transform, es probable que tengas que actualizar los permisos AWS Transform para poder crear concesiones. Para configurar automáticamente los permisos necesarios, ve a la AWS Transform consola y selecciona Actualizar permisos en el encabezado de la parte superior de la página. Para poder AWS Transform crear subvenciones, debes actualizar los permisos en la página de la AWS Transform consola.

Permitir AWS Transform acceso a las claves gestionadas por el cliente

El siguiente ejemplo de declaración de política otorga a los usuarios permisos para acceder a las funciones cifradas con una clave administrada por el cliente al permitir el AWS Transform acceso a la clave. Es obligatorio utilizar esta política AWS Transform si un administrador ha configurado una clave de cifrado gestionada por el cliente.

Note

Esta información no se aplica al flujo de trabajo de implementación de la modernización de SQL Server mediante 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 mejora del servicio

Para ayudarnos a AWS Transform proporcionar la información más relevante, podemos utilizar determinados contenidos AWS Transform, como las preguntas que formule AWS Transform y sus respuestas, para mejorar el servicio. En esta página se explica qué contenido utilizamos y cómo excluirse de esta opción.

AWS Transform contenido utilizado para mejorar el servicio

Es posible que usemos cierto contenido de AWS Transform para mejorar el servicio. AWS Transform podemos usar este contenido, por ejemplo, para proporcionar mejores respuestas a preguntas

comunes, solucionar problemas AWS Transform operativos, eliminar errores o para la formación de modelos.

El contenido que se AWS puede utilizar para mejorar el servicio incluye, por ejemplo, sus preguntas y las respuestas AWS Transform y el código que se AWS Transform generan.

Cómo excluirse de esta opción

La forma en que opte por dejar de AWS Transform usar el contenido para mejorar el servicio depende del entorno en el que lo utilice AWS Transform.

Para AWS Transform configurar una política de exclusión de los servicios de IA en AWS Organizations. Para obtener más información, consulte [Políticas de exclusión de servicios de IA](#) en la Guía del usuario de AWS Organizations .

Para dejar de compartir su contenido en Visual Studio IDE, utilice el siguiente procedimiento.

Vaya a Herramientas -> Opciones -> Kit de herramientas de AWS -> Amazon Q

Cambie la opción en Compartir contenido de Amazon Q Content con AWS a Verdadero o Falso.

Para dejar de compartir sus datos de telemetría en el AWS kit de herramientas Visual Studio, utilice este procedimiento:

1. En Herramientas, seleccione Opciones.
2. En el panel Opciones, elija Kit de herramientas de AWS y, a continuación, elija General.
3. Deseleccione Permitir que el AWS kit de herramientas recopile información de uso.

Administración de identidad y acceso para AWS Transformar

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar AWS los recursos de Transform. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- [Público](#)

- [Autenticación con identidades](#)
- [Administración del acceso con políticas](#)
- [Cómo AWS Transform funciona con IAM](#)
- [Identity-based ejemplos de políticas para AWS Transformar](#)
- [Resolución de problemas AWS Transforma la identidad y el acceso](#)
- [Uso de roles vinculados a servicios para AWS Transform](#)
- [AWS políticas gestionadas para AWS Transformar](#)
- [AWS Referencia de permisos de transformación](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte [Resolución de problemas AWS Transforma la identidad y el acceso](#)).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte [Cómo AWS Transform funciona con IAM](#)).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte [Identity-based ejemplos de políticas para AWS Transformar](#)).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte [AWS Signature Version 4 para solicitudes de API](#) en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Al crear una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz, que tiene acceso completo a todos los Servicios de AWS recursos. Se recomienda encarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte [¿Qué es el Centro de identidades de IAM?](#) en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte [Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

Roles de IAM

Un [Rol de IAM](#) es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol [cambiando de un rol de usuario a uno de IAM \(consola\)](#) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte [Información general de políticas de JSON](#) en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas integradas (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte [Selección entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe [especificar una entidad principal](#) en una política basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte [Políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte [Políticas de control de recursos \(RCP\)](#) en la Guía del usuario de AWS Organizations .
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

Cómo AWS Transform funciona con IAM

Antes de usar IAM para administrar el acceso a AWS Transform, infórmese sobre las funciones de IAM disponibles para su uso con Transform. AWS

Característica de IAM	AWS Soporte para transformaciones
Identity-based políticas	Sí

Característica de IAM	AWS Soporte para transformaciones
Resource-based políticas	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Service-linked roles	Sí

Para obtener una visión general de cómo funcionan AWS Transform y otros AWS servicios con la mayoría de las funciones de IAM, consulte [AWS los servicios que funcionan con IAM](#) en la Guía del usuario de IAM.

Identity-based políticas para AWS Transformar

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones.

Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte [Referencia de los elementos de la política de JSON de IAM](#) en la Guía del usuario de IAM.

Identity-based ejemplos de políticas para AWS Transformar

Para ver ejemplos de políticas de AWS Transform basadas en la identidad, consulte. [Identity-based ejemplos de políticas para AWS Transformar](#)

Resource-based políticas dentro AWS Transformar

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Acciones políticas para AWS Transformar

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de AWS transformación, consulte las [acciones, los recursos y las claves de condición de AWS Transform in the](#) Service Authorization Reference.

Para ver una lista de las acciones de AWS Transform custom, consulte [Acciones, recursos y claves de condición de AWS Transform custom](#) en la Referencia de autorización del servicio.

Las acciones políticas de AWS Transform utilizan el siguiente prefijo antes de la acción:

```
transform
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [  
    "transform:action1",  
    "transform:action2"  
]
```

Para ver ejemplos de políticas de AWS Transform basadas en la identidad, consulte. [Identity-based ejemplos de políticas para AWS Transformar](#)

Recursos de políticas para AWS Transformar

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de AWS Transform y sus ARN, y con qué acciones puede especificar el ARN de cada recurso, [consulte Acciones, recursos y claves de condición de Transform en la AWS referencia](#) de autorización del servicio.

Para ver una lista de los tipos de recursos y sus ARN y con qué acciones puede especificar el ARN de cada recurso AWS para Transform custom, [consulte Acciones, recursos y claves de condición de Transform custom en la AWS Referencia](#) de autorización del servicio.

Para ver ejemplos de políticas de AWS Transform basadas en la identidad, consulte. [Identity-based ejemplos de políticas para AWS Transformar](#)

Claves de condición de la política para AWS Transformar

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de AWS Transform y con qué acciones y recursos puede utilizar una clave de condición, consulte [Acciones, recursos y claves de condición de AWS Transform](#) en la referencia de autorización de servicio.

Para ver una lista de las claves de condición y con qué acciones y recursos puede utilizar una clave de condición para AWS Transform custom, consulte [Acciones, recursos y claves de condición de AWS Transform custom](#) en la Referencia de autorización de servicio.

Para ver ejemplos de políticas de AWS Transform basadas en la identidad, consulte. [Identity-based ejemplos de políticas para AWS Transformar](#)

ACL en AWS Transformar

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AWS Transformar

Compatibilidad con ABAC (etiquetas en las políticas): parcial

Attribute-based el control de acceso (ABAC) es una estrategia de autorización que define los permisos en función de unos atributos denominados etiquetas. Puede adjuntar etiquetas a las

entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte [Definición de permisos con la autorización de ABAC](#) en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte [Uso del control de acceso basado en atributos \(ABAC\)](#) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AWS Transformar

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte [Credenciales de seguridad temporales en IAM](#) y [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Cross-service permisos principales para AWS Transformar

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama y la que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Sesiones de acceso directo](#).

Funciones de servicio para AWS Transformar

Compatible con roles de servicio: sí

Un rol de servicio es un [rol de IAM](#) que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener

más información, consulte [Crear un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

 Warning

Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de AWS Transform. Edite las funciones de servicio solo cuando AWS Transform proporcione instrucciones para hacerlo.

Service-linked roles para AWS Transformar

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir la función de realizar una acción en su nombre. Service-linked las funciones aparecen en su nombre Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o la administración de los roles vinculados al servicio AWS Transform, consulte. [Uso de roles vinculados a servicios para AWS Transform](#)

Identity-based ejemplos de políticas para AWS Transformar

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AWS Transform. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM \(consola\)](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS Transform, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición de AWS Transform](#) en la Referencia de autorización de servicios.

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de AWS Transforma la consola](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)

- [Permita que los administradores acepten una solicitud de conexión de la cuenta con AWS Transformar](#)
- [Permita a los administradores asignar los usuarios existentes del Centro de Identidad de IAM y crear nuevos usuarios del Centro de Identidad de IAM para asignarlos AWS Transformar](#)
- [Permita que los administradores activen AWS Transformar](#)
- [Permita que los usuarios accedan AWS Transfórmese con credenciales de IAM](#)

Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear, eliminar o acceder a los recursos de AWS Transform de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de tarea](#) en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de

políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte [Validación de políticas con el Analizador de acceso de IAM](#) en la Guía del usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte [Acceso seguro a la API con MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

Uso de AWS Transforma la consola

Para acceder a la consola AWS Transform, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de AWS Transform que tiene en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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 los administradores acepten una solicitud de conexión de la cuenta con AWS Transformar

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 a los administradores asignar los usuarios existentes del Centro de Identidad de IAM y crear nuevos usuarios del Centro de Identidad de IAM para asignarlos AWS Transformar

La siguiente política concede los permisos que un administrador necesita para gestionar los usuarios y grupos del IAM Identity Center en la AWS consola Transform. Con esta política, un administrador puede asignar y eliminar usuarios y grupos, ver los nombres para mostrar, crear nuevos usuarios del IAM Identity Center, gestionar las asignaciones de aplicaciones y configurar los ajustes de las sesiones de las aplicaciones.

```

{
  "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"
        }
    }
}
]
}

```

Permita que los administradores activen AWS Transformar

La siguiente política otorga los permisos que un administrador necesita para habilitar y administrar AWS Transform a través de la AWS consola. Esto incluye la administración de perfiles, la configuración de agentes y la administración de conectores. Esta política está destinada únicamente a los administradores y debe aplicarse a los responsables de confianza de su cuenta.

```

{
    "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": "*"
}
]
}

```

Permita que los usuarios accedan AWS Transfórmese con credenciales de IAM

La siguiente política otorga a un IAM principal acceso a la aplicación web AWS Transform y a las API mediante credenciales de IAM. Esta política es necesaria para el IAM-only acceso y para que el acceso a IAM se habilite junto con un proveedor de identidad.

Reemplace *regionaccount-id*, y *profile-id* con sus valores. Puedes encontrar el ID de perfil en la consola AWS Transform, en la sección Configuración.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccess",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/profile-id"
    }
  ]
}

```

Para conceder acceso a todos los perfiles de una cuenta, utiliza un comodín como ID de perfil:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccessAllProfiles",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/*"
    }
  ]
}

```

 Note

La `transform:AccessTransformProfile` acción solo permite el acceso a AWS Transform. Las acciones dentro de los espacios de trabajo están controladas por las funciones del espacio de trabajo de AWS Transform (administrador, colaborador, aprobador Read-only), no por las políticas de IAM. Los roles del espacio de trabajo determinan lo que puede hacer un usuario, como crear puestos de trabajo, gestionar colaboradores o aprobar tareas.

Resolución de problemas AWS Transforma la identidad y el acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con AWS Transform e IAM.

Temas

- [No estoy autorizado a realizar ninguna acción en AWS Transformar](#)
- [No estoy autorizado a realizar tareas como: PassRole](#)
- [Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mi AWS Transforma los recursos](#)

No estoy autorizado a realizar ninguna acción en AWS Transformar

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio `my-example-widget`, pero no tiene los permisos ficticios AWS Transform: `GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: AWS Transform: GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso `my-example-widget` mediante la acción AWS Transform: `GetWidget`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a AWS Transform.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Transform. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir la función al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mi AWS Transforma los recursos

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS Transform admite estas funciones, consulte [Cómo AWS Transform funciona con IAM](#).

- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte [Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en](#) la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo [proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para AWS Transform

AWS Transform [usa roles vinculados al AWS Identity and Access Management servicio \(IAM\)](#).

Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Transform Service-linked Los roles están predefinidos AWS Transform e incluyen todos los permisos que el servicio necesita para llamar a otros AWS servicios en su nombre.

Utilizar funciones vinculadas al servicio para AWS Transform

AWS Transform [usa roles vinculados al AWS Identity and Access Management servicio \(IAM\)](#).

Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Transform Service-linked Los roles están predefinidos AWS Transform e incluyen todos los permisos que el servicio necesita para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Transform , ya que no es necesario añadir manualmente los permisos necesarios. AWS Transform define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Transform puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus AWS Transform recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los [AWS servicios que funcionan con IAM](#) y busque los servicios que tienen la palabra Sí en

la columna de funciones. Service-linked Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Service-linked permisos de rol para AWS Transform

AWS Transform utiliza el rol vinculado al servicio denominado [AWSServiceRoleForAWSTransform](#): este Service-Linked rol proporciona a AWS Transform la capacidad de proporcionar información de uso.

El rol AWSServiceRoleForAWSTransform vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `transform.amazonaws.com`

La política de permisos de roles denominada AWSServiceRoleForAWSTransform permite AWS Transform realizar las siguientes acciones en los recursos especificados:

- Cloudwatch: PutMetricData
 - Envíe métricas personalizadas a CloudWatch para AWS Transform las operaciones
 - Realice un seguimiento del progreso de la transformación, las tasas de éxito y las métricas de rendimiento
 - Habilite el monitoreo y las alertas sobre los flujos de trabajo de transformación
- sso: DescribeApplication
 - Vea los detalles sobre una aplicación específica en Identity Center
 - Obtenga los metadatos de la aplicación, como el nombre, la descripción, el estado y la configuración
- sso: GetApplicationAssignmentConfiguration
 - Recuperar los ajustes de configuración de las asignaciones para una aplicación
 - Vea cómo users/groups se configuran para asignarse a la aplicación
- sso: ListApplicationAssignmentsForPrincipal
 - Listar todas las aplicaciones asignadas a un usuario o grupo específico (principal)
 - Vea a qué aplicaciones tiene acceso una identidad en particular
- Permite el descifrado de KMS-encrypted los datos cuando se accede a ellos a través del IAM Identity Center. Solo funciona cuando el contexto de cifrado contiene un ARN de instancia de IAM Identity Center válido y se debe acceder a él a través de los puntos finales del servicio de IAM Identity Center.

- Permite descifrar los KMS-encrypted datos cuando se accede a ellos a través de Identity Store. Solo funciona cuando el contexto de cifrado contiene un ARN de Identity Store válido y se debe acceder a él a través de los puntos finales del servicio Identity Store.
- administrador de secretos: GetSecretValue
 - Acceda a los secretos AWS Transform vinculados al servicio que se utilizan para almacenar los secretos de los clientes para proveedores de identidad externos
 - Recurso: `arn:aws:secretsmanager:*:*:secret:transform-preprod!` *
 - Estado: Debe ser propiedad del servicio transform-preprod y acceder a él desde la misma cuenta
- soporte:CreateCase, soporte:, soporte:DescribeCases, soporte:DescribeCommunications, soporte:AddCommunicationToCase ResolveCase
 - Cree y gestione casos de soporte premium desde la aplicación AWS Transform web
 - Vea los detalles y las comunicaciones del caso
 - Agregue comunicaciones y resuelva los casos de soporte

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte [los permisos de Service-linked funciones](#) en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de AWS Transform

No necesita crear manualmente un rol vinculado a servicios. Al crear un perfil para AWS Transform en AWS Management Console, AWS Transform crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al actualizar la configuración, vuelve a AWS Transform crear el rol vinculado al servicio para usted.

También puede usar la consola de IAM o la AWS CLI para crear un rol vinculado al servicio con el nombre del `transform.amazonaws.com` servicio. Para obtener más información, consulte [Crear un rol vinculado a un servicio](#) en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Modificación de un rol vinculado a un servicio de AWS Transform

AWS Transform no permite editar el rol vinculado al `AWSServiceRoleForAWSTransform` servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias

entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS Transform

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

Note

Si el AWS Transform servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al `AWSServiceRoleForAWSTransform` servicio. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones compatibles para AWS Transform roles vinculados a servicios

AWS Transform no admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio esté disponible. Puede usar el `AWSServiceRoleForAWSTransform` rol en las siguientes regiones. Para obtener más información, consulte [Puntos de conexión y Regiones de AWS](#).

Nombre de la región	Identidad de la región	Support en AWS Transform
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Europa (Fráncfort)	eu-central-1	Sí

Uso de roles vinculados al servicio para AWS Transform Custom

AWS Transform Custom usa el rol vinculado al servicio denominado `AWSServiceRoleForAWSTransformCustom` para publicar las métricas y los registros en tu cuenta en tu nombre. Estas métricas le permiten monitorear los recuentos de transformaciones, las latencias y los códigos de estado directamente en sus paneles de control. Los registros proporcionan visibilidad de los problemas encontrados durante las transformaciones.

AWS Transform Custom predefine esta [función vinculada al servicio](#) e incluye solo los permisos que el servicio necesita. No es necesario añadir ningún permiso manualmente y AWS Transform Custom solo puede asumir el rol. Para obtener información general sobre las funciones vinculadas a servicios, consulte [Uso de funciones vinculadas a servicios en la Guía del usuario](#) de IAM.

Service-linked permisos de rol para AWS Transform Custom

El rol `AWSServiceRoleForAWSTransformCustom` vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `transform-custom.amazonaws.com`

La política de permisos de roles denominada `AWSServiceRoleForAWSTransformCustom` permite a AWS Transform Custom realizar las siguientes acciones en los recursos especificados:

- `cloudwatch:PutMetricData` en todos los AWS recursos
 - Publique las métricas operativas en el `AWS/TransformCustom` espacio de nombres
 - Realice un seguimiento de los recuentos de transformaciones, las latencias y los códigos de estado
 - Se limita al espacio de `AWS/TransformCustom` nombres mediante la clave de condición `cloudwatch:namespace`
- `logs:CreateLogGroup` y `logs:PutRetentionPolicy` en el grupo de registros `/aws/TransformCustom`
 - Cree el grupo CloudWatch de registros para publicar los registros de transformación
 - Establezca políticas de retención de registros en el grupo de registros
 - `arn:aws:logs:*:*:log-group:/aws/TransformCustom` Con una `aws:ResourceAccount` condición que garantice el acceso solo dentro de su cuenta
- `logs:CreateLogStream` y `logs:PutLogEvents` en los flujos de registros dentro del grupo de `/aws/TransformCustom` registros

- Cree flujos de registro y publique eventos de registro para las operaciones de transformación
- `arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*` Con una `aws:ResourceAccount` condición que garantice el acceso solo desde su cuenta

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte [los permisos de los Service-linked roles](#) en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de AWS Transforma de forma personalizada

No necesita crear manualmente un rol vinculado a servicios. Cuando ejecuta una transformación mediante la CLI de AWS Transform Custom, AWS Transform Custom crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando ejecuta una transformación mediante la CLI de AWS Transform Custom, AWS Transform Custom vuelve a crear el rol vinculado al servicio para usted.

También puede utilizar la consola IAM para crear un rol vinculado a servicios con el caso de uso `AWSServiceRoleForAWSTransformCustom`. En la AWS CLI o en la AWS API, cree una función vinculada al servicio con el nombre del servicio. `transform-custom.amazonaws.com` Para obtener más información, consulte [Crear un rol vinculado a un servicio](#) en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Modificación de un rol vinculado a un servicio de AWS Transforma: Personaliza

AWS Transform Custom no permite editar el rol `AWSServiceRoleForAWSTransformCustom` vinculado al servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS Transform Custom

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa.

El rol `AWSServiceRoleForAWSTransformCustom` vinculado al servicio no crea recursos persistentes en tu cuenta. Puedes eliminarlo directamente sin necesidad de limpiar ningún recurso.

Si elimina este rol y, posteriormente, ejecuta una transformación mediante la CLI AWS Transform Custom, el rol vinculado al servicio se vuelve a crear automáticamente.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al servicio. `AWSServiceRoleForAWSTransformCustom` Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones compatibles para AWS Transforme los roles personalizados vinculados a servicios

AWS Transform Custom admite el uso de roles vinculados a servicios en todas las regiones en las que AWS Transform Custom está disponible. Para ver una lista de las regiones compatibles, consulte Regiones [compatibles](#).

AWS políticas gestionadas para AWS Transformar

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir [políticas administradas por el cliente](#) específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte [Políticas administradas por AWS](#) en la Guía del usuario de IAM.

AWS Transforma las actualizaciones para AWS políticas administradas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de AWS Transform desde el 1 de marzo de 2021.

Cambio	Descripción	Fecha
<u>AWSTransformInfrastructureExecutorAccessBatch</u> : política nueva	Se agregó una nueva política AWS administrada que otorga los permisos necesarios para ejecutar las evaluaciones y transformaciones de AWS Transform Continuous Modernization mediante AWS Batch, incluida la carga del código fuente, la recuperación de los resultados, la supervisión del estado de los trabajos por lotes, la lectura de registros y la administración de los programas de transformación.	20 de julio de 2026
<u>AWSTransformInfrastructureExecutorAccessEC2</u> : política nueva	Se agregó una nueva política AWS administrada que otorga los permisos necesarios para ejecutar las evaluaciones y transformaciones de AWS Transform Continuous Modernization mediante Amazon EC2, lo que incluye la carga del código fuente, la recuperación de los resultados, la supervisión del estado de los trabajos y la administración de los programas de transformación.	20 de julio de 2026
<u>AWSTransformSecurityAgentExecutorAccess</u> : política nueva	Se agregó una nueva política AWS administrada que otorga a AWS Transform Continuous Modernization los permisos	30 de junio de 2026

Cambio	Descripción	Fecha
	necesarios para invocar el servicio AWS Security Agent para revisar y corregir automáticamente la seguridad del código, incluida la carga de artefactos escaneados y la recuperación de los resultados.	
<u>AWSServiceRoleForAWSTransformCustom</u> : política actualizada	Se agregaron permisos de CloudWatch registro para permitir que AWS Transform custom publique los registros en el /aws/TransformCustom grupo de registros de su cuenta.	5 de mayo de 2026
<u>AWSTransformCustomExecuteTransformations</u> : política actualizada	Se agregó el permiso para crear la función personalizada vinculada al servicio AWS Transform (AWSServiceRoleForAWSTransformCustom) para permitir la emisión de CloudWatch métricas a las cuentas de los clientes.	27 de abril de 2026

Cambio	Descripción	Fecha
<u>AWSTransformCustomManageTransformations:</u> política actualizada	Se agregó el permiso para crear la función personalizada vinculada al servicio AWS Transform (AWSServiceRoleForAWSTransformCustom) para permitir la emisión de CloudWatch métricas a las cuentas de los clientes.	27 de abril de 2026
<u>AWSTransformCustomFullAccess:</u> política actualizada	Se agregó el permiso para crear la función personalizada vinculada al servicio AWS Transform (AWSServiceRoleForAWSTransformCustom) para permitir la emisión de CloudWatch métricas a las cuentas de los clientes.	7 de abril de 2026
<u>AWSServiceRoleForAWSTransformCustom:</u> política nueva	Se agregó una nueva política AWS administrada para el rol vinculado a un servicio personalizado de AWS Transform. Esta política permite a AWS Transform custom publicar CloudWatch métricas en su cuenta.	23 de marzo de 2026
<u>DBModProvisioningAndMigrations:</u> política nueva	Esta política otorga capacidades de aprovisionamiento y migración de bases de datos.	24 de marzo de 2026

Cambio	Descripción	Fecha
DBModDiscoveryAndAssessment : política nueva	Se agregó una nueva política AWS administrada que proporciona capacidades integrales de modernización, descubrimiento y evaluación de bases de datos.	24 de marzo de 2026
AWSTransformCustomFullAccess : política nueva	Se agregó una nueva política AWS administrada que brinda acceso completo a AWS Transform custom.	5 de diciembre de 2025
AWSTransformCustomExecuteTransformations : política nueva	Se agregó una nueva política AWS administrada que brinda acceso para ejecutar transformaciones en AWS Transform custom.	5 de diciembre de 2025
AWSTransformCustomManageTransformations : política nueva	Se agregó una nueva política AWS administrada que proporciona acceso para crear, actualizar, leer y eliminar recursos de transformación en AWS Transform custom, así como para ejecutar transformaciones.	5 de diciembre de 2025

Cambio	Descripción	Fecha
<u>AWSServiceRoleForAWSTransform</u> : política actualizada	Se agregaron permisos para acceder al secreto vinculado al servicio AWS Transform que se utiliza para almacenar el secreto del cliente para los proveedores de identidad externos. Se agregaron permisos para crear un caso de soporte premium desde la aplicación web AWS Transform.	1 de diciembre de 2025
<u>AWSTransformApplicationECSDeploymentPolicy</u> : política actualizada	Se agregaron permisos de inspección de roles de IAM, creación de roles vinculados al servicio de ECS y permisos de KMS para la compatibilidad con el cifrado ECR.	22 de noviembre de 2025
<u>AWSTransformApplicationDeploymentPolicy</u> : política actualizada	Se agregaron los permisos de red de EC2, los permisos de inspección de roles de IAM, los permisos de lista de deseos de S3 y la compatibilidad con el cifrado KMS para mejorar las capacidades de implementación.	22 de noviembre de 2025
<u>AWSServiceRoleForAWSTransform</u> : política actualizada	Se agregó soporte para las claves administradas por el cliente en el Centro de identidad de IAM.	17 de septiembre de 2025

Cambio	Descripción	Fecha
AWSTransformApplicationDeploymentPolicy : política nueva	Se agregó una nueva política AWS administrada que permite a AWS Transform implementar aplicaciones.NET transformadas mediante la creación y administración de instancias, CloudFormation pilas y recursos asociados de Amazon EC2.	28 de agosto de 2025
AWSServiceRoleForAWSTransform : política actualizada	Se agregó una nueva política .	15 de mayo de 2025

AWS política gestionada: AWSServiceRoleForAWSTransform

Esta política está asociada a la función [AWSServiceRoleForAWSTransform](#) vinculada al servicio (SLR).

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía [AWSServiceRoleForAWSTransform](#) de referencia de políticas AWS gestionadas.

AWS política gestionada: AWSServiceRoleForAWSTransformCustom

Esta política está asociada a la función [AWSServiceRoleForAWSTransformCustom](#) vinculada al servicio (SLR). Esta función permite a AWS Transform custom publicar CloudWatch métricas y registros en tu cuenta en tu nombre.

Descripción

Esta política incluye los permisos siguientes:

- Amazon CloudWatch: permite que las métricas de publicación estén CloudWatch en el espacio de AWS/TransformCustom nombres. Esto permite monitorear los recuentos de transformaciones, las latencias y los códigos de estado en sus paneles de control. CloudWatch

- Amazon CloudWatch Logs: permite crear grupos de registros, flujos de registros, establecer políticas de retención y publicar eventos de registro en el grupo de /aws/TransformCustom registros. Esto proporciona visibilidad de los problemas encontrados durante las transformaciones.

AWS política gestionada: AWSTransformApplicationDeploymentPolicy

Esta política permite a AWS Transform implementar aplicaciones.NET transformadas mediante la creación y administración de instancias, CloudFormation pilas y recursos asociados de Amazon EC2.

Descripción

Esta política incluye los permisos siguientes:

- CloudFormation— Permite crear, actualizar, eliminar y describir CloudFormation pilas con nombres que comiencen por AWSTransform. Las operaciones de apilado están restringidas a los recursos etiquetados con CreatedBy: AWSTransform y se limitan a la misma cuenta. AWS
- Amazon EC2: permite describir las VPC, las subredes, los grupos de seguridad, las imágenes, las instancias, las tablas de enrutamiento y las puertas de enlace de Internet. Permite ejecutar, iniciar, detener, terminar y modificar instancias de EC2, pero solo cuando se accede a ellas. CloudFormation La creación de etiquetas está restringida a las claves de etiqueta específicas permitidas y solo durante CloudFormation las operaciones.
- AWS Identity and Access Management (IAM): permite obtener y transferir funciones de IAM específicas para las instancias de implementación de AWSTransform. Incluye permisos para inspeccionar las políticas de funciones y los archivos adjuntos. El acceso está restringido a la misma AWS cuenta.
- Amazon EC2 Systems Manager (SSM): permite recuperar los parámetros de la AMI de Amazon Linux del almacén de parámetros administrado y enviar comandos a AWS las instancias. AWSTransform-tagged
- Amazon S3: permite administrar objetos en los depósitos de implementación de AWSTransform, lo que incluye enumerar los cubos y obtener las ubicaciones de los depósitos dentro de la misma cuenta. AWS
- AWS Key Management Service (KMS): permite realizar operaciones de cifrado y descifrado mediante claves de KMS etiquetadas para AWSTransform, con restricciones al uso de los servicios de S3 y EC2.

La política implementa el acceso con el mínimo privilegio mediante permisos a nivel de recursos, condiciones basadas en etiquetas, control de uso del servicio, restricciones de uso, restricciones a nivel de cuenta y declaraciones de denegación explícitas para evitar la `aws:CalledVia` modificación no autorizada de las etiquetas fuera de las operaciones. CloudFormation

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía de referencia de políticas gestionadas. [AWSTransformApplicationDeploymentPolicy](#) AWS

AWS política gestionada: AWSTransformApplicationECSDeploymentPolicy

Esta política permite a AWS Transform implementar aplicaciones transformadas en Amazon ECS mediante la creación y administración de clústeres, servicios, tareas y recursos asociados de ECS.

Descripción

Esta política incluye los permisos siguientes:

- CloudFormation— Permite crear, actualizar, eliminar y describir CloudFormation pilas con nombres que comiencen por AWSTransform. Las operaciones de apilado están restringidas a los recursos etiquetados con CreatedBy: AWSTransform y se limitan a la misma cuenta. AWS
- Amazon ECS: permite crear, actualizar y eliminar clústeres, servicios y definiciones de tareas de ECS. Permite ejecutar tareas, enumerarlas y describir su estado. Todas las operaciones están restringidas a los recursos cuyos nombres comiencen por AWSTransform y estén etiquetados CreatedBy por: AWSTransform.
- AWS Identity and Access Management (IAM): permite obtener y transferir funciones de IAM específicas para tareas de ECS (y). AWSTransform-Deploy-ECS-Task-Role AWSTransform-Deploy-ECS-Execution-Role Incluye permisos para inspeccionar las políticas de funciones y crear la función vinculada al servicio de ECS cuando sea necesario.
- Amazon CloudWatch Logs: permite crear, eliminar y administrar grupos de registros con nombres que comiencen por aws/ecs /AWSTransform. Permite recuperar los eventos de registro para solucionar problemas de las aplicaciones implementadas.
- Amazon ECR: permite crear repositorios de contenedores con nombres que comiencen por awstransform para almacenar imágenes de contenedores de aplicaciones.
- AWS Key Management Service (KMS): permite crear concesiones y generar claves de datos para el cifrado ECR cuando se utilizan claves KMS administradas por el cliente.

La política implementa el acceso con privilegios mínimos mediante permisos a nivel de recursos, condiciones basadas en etiquetas y restricciones a nivel de cuenta para garantizar que las operaciones se limiten a los recursos de la misma cuenta. AWSTransform-managed AWS

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía de referencia de políticas gestionadas. [AWSTransformApplicationECSDeploymentPolicy](#) AWS

AWS política gestionada: AWSTransformCustomFullAccess

Esta política proporciona acceso completo a AWS Transform custom.

Descripción

Esta política incluye los permisos siguientes:

- AWS Transform Custom: permite realizar todas las acciones en todos los recursos personalizados de AWS Transform. Esto proporciona un acceso administrativo completo al servicio.
- AWS Identity and Access Management (IAM): permite crear el [rol vinculado al servicio](#) personalizado de AWS Transform (). `AWSServiceRoleForAWSTransformCustom` Esta función es necesaria para que AWS Transform custom emita CloudWatch métricas y registros a su cuenta. El permiso está limitado a permitir únicamente la creación de este rol específico vinculado a un servicio.

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía [AWSTransformCustomFullAccess](#) de referencia de políticas AWS gestionadas.

AWS política gestionada: AWSTransformCustomExecuteTransformations

Esta política proporciona acceso para ejecutar transformaciones en AWS Transform custom.

Descripción

Esta política incluye los permisos siguientes:

- AWS Transform Custom: permite transmitir conversaciones, ejecutar transformaciones y administrar campañas. Incluye permisos para obtener los detalles de la campaña, actualizar el estado del repositorio de la campaña y actualizar las campañas.

- AWS Identity and Access Management (IAM): permite crear el [rol personalizado vinculado al servicio AWS](#) Transform (). `AWSServiceRoleForAWSTransformCustom` Esta función es necesaria para que AWS Transform custom emita CloudWatch métricas y registros a su cuenta. El permiso está limitado a permitir únicamente la creación de este rol específico vinculado a un servicio.

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía [AWSTransformCustomExecuteTransformations](#) de referencia de políticas AWS gestionadas.

AWS política gestionada: AWSTransformCustomManageTransformations

Esta política proporciona acceso para crear, actualizar, leer y eliminar recursos de transformación en AWS Transform custom, así como para ejecutar transformaciones.

Descripción

Esta política incluye los permisos siguientes:

- AWS Transform Custom: permite la gestión integral de los recursos de transformación, incluida la transmisión de conversaciones, la ejecución de transformaciones y la administración de paquetes de transformación. Permite crear, obtener y eliminar las URL de los paquetes de transformación y completar la carga de los paquetes.
- Gestión del conocimiento: permite enumerar, obtener, eliminar y actualizar los elementos de conocimiento y sus configuraciones y estados.
- Administración de campañas: permite obtener los detalles de la campaña, actualizar el estado del repositorio de la campaña y actualizar las campañas.
- Etiquetado de recursos: permite enumerar, añadir y eliminar etiquetas para los recursos personalizados de AWS Transform.
- AWS Identity and Access Management (IAM): permite crear el rol personalizado [vinculado al servicio](#) de AWS Transform (). `AWSServiceRoleForAWSTransformCustom` Esta función es necesaria para que AWS Transform custom emita CloudWatch métricas y registros a su cuenta. El permiso está limitado a permitir únicamente la creación de este rol específico vinculado a un servicio.

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía [AWSTransformCustomManageTransformations](#) de referencia de políticas AWS gestionadas.

AWS política gestionada: AWSTransformInfrastructureExecutorAccessBatch

Esta política otorga los permisos necesarios para ejecutar las evaluaciones y transformaciones de AWS Transform Continuous Modernization mediante AWS Batch. Adjunta esta política a un rol de IAM en tu cuenta. La CLI y el agente de AWS Transform Continuous Modernization asumen esta función para cargar el código fuente, recuperar los resultados, supervisar el estado de los trabajos por lotes, leer los registros y gestionar los programas de transformación.

Descripción

Esta política incluye los permisos siguientes:

- AWS Lambda: permite invocar y recuperar la configuración de las funciones atx Lambda con prefijo que organizan el flujo de trabajo de transformación.
- Amazon S3: permite cargar el código fuente en atx-source-code-* buckets y descargar los resultados de la transformación desde buckets atx-custom-output-* y atx-ct-output-* buckets.
- AWS Key Management Service (KMS): permite cifrar y descifrar datos mediante la clave de cifrado AWS Transform (). alias/atx-encryption-key
- Amazon CloudWatch Logs: permite leer los eventos del registro de ejecución de Batch y Lambda para la supervisión y la depuración de transformaciones.
- Amazon CloudWatch: permite obtener y enumerar el panel de control AWS Transform CLI para obtener visibilidad operativa.
- AWS Batch: permite describir y enumerar los entornos de cómputo, las colas de trabajos, las definiciones de trabajos y el estado de los trabajos.
- CloudFormation— Permite describir y enumerar las pilas de infraestructuras de AWS Transform para comprobar el estado de la implementación.
- API de etiquetado de Resource Groups: permite recuperar recursos etiquetados para descubrir la infraestructura de AWS Transform en su cuenta.
- AWS Secrets Manager— Permite recuperar y describir los secretos de AWS Transform almacenados con el prefijo. atx/
- Amazon EventBridge Scheduler: permite gestionar las tareas de transformación programadas dentro del grupo atx-ct de programación.

- Amazon EC2: permite describir la configuración de VPC, subred, grupo de seguridad, tabla de enrutamiento y puerta de enlace NAT para redes de entornos de computación por lotes.
- AWS Identity and Access Management (IAM): permite leer configuraciones de roles ATX con prefijo y Atx prefijo para validar la configuración de la infraestructura y pasarlas a AtxSchedulerInvocationRole Amazon EventBridge Scheduler para que pueda invocar los trabajos programados.

La política implementa el acceso con el mínimo privilegio mediante permisos a nivel de recursos, condiciones basadas en etiquetas, la `aws:ResourceAccount` condición y condiciones relacionadas con el ámbito del servicio para garantizar que las operaciones se limiten a los recursos de Transform dentro de la misma cuenta `iam:PassedToService`. AWS AWS

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía de referencia de políticas gestionadas. [AWSTransformInfrastructureExecutorAccessBatch](#) AWS

AWS política gestionada: AWSTransformInfrastructureExecutorAccessEC2

Esta política otorga los permisos necesarios para ejecutar las evaluaciones y transformaciones de AWS Transform Continuous Modernization mediante Amazon EC2. Adjunte esta política a un rol de IAM en su cuenta. La CLI y el agente de AWS Transform Continuous Modernization asumen esta función para cargar el código fuente, recuperar los resultados, supervisar el estado de los trabajos y gestionar los programas de transformación.

Descripción

Esta política incluye los permisos siguientes:

- CloudFormation— Permite describir las pilas de infraestructuras de AWS Transform, los eventos de las pilas, los recursos de las pilas y el estado de detección de desviaciones, enumerar las pilas y validar las CloudFormation plantillas antes de su implementación.
- Amazon EC2: permite describir instancias, AMI, VPC, subredes, grupos de seguridad, pares de claves, tablas de enrutamiento, puertas de enlace NAT y puertas de enlace de Internet. Permite iniciar y detener las instancias EC2 etiquetadas con. `atx-remote-infra: true`
- Amazon EC2 Systems Manager (SSM): permite supervisar el estado de ejecución de los comandos y ejecutar comandos y sesiones AWS Transform-tagged en instancias, incluida la ejecución `AWS-RunShellScript` del documento.

- Amazon S3: permite administrar el código fuente y los artefactos de salida en los cubos de AWS Transform, lo que incluye obtener, colocar y eliminar objetos y enumerar los cubos.
- AWS Key Management Service (KMS): permite cifrar y descifrar datos mediante la clave de cifrado AWS Transform (). `alias/atx-encryption-key`
- AWS Secrets Manager— Permite recuperar y describir los secretos de la transformación, como las credenciales del repositorio, almacenadas con el `atx/` prefijo.
- Amazon EventBridge Scheduler: permite gestionar las tareas de transformación programadas dentro del grupo `atx-ct` de programación.
- API de etiquetado de Resource Groups: permite recuperar recursos etiquetados para descubrir la infraestructura de AWS Transform en su cuenta.
- AWS Identity and Access Management (IAM): permite transferir la `atx-transform-role*` función a Amazon EC2 y `AtxSchedulerInvocationRole` a EventBridge Amazon Scheduler, y leer la configuración del perfil de la función y la instancia para las instancias de EC2.

La política implementa el acceso con el mínimo privilegio mediante permisos a nivel de recursos, condiciones basadas en etiquetas, la `aws:ResourceAccount` condición y las condiciones del ámbito del servicio para garantizar que las operaciones se limiten a los recursos de Transform dentro de la misma cuenta `iam:PassedToService`. AWS AWS

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía de referencia de políticas gestionadas. [AWSTransformInfrastructureExecutorAccessEC2](#) AWS

AWS política gestionada: AWSTransformSecurityAgentExecutorAccess

Esta política otorga a AWS Transform Continuous Modernization los permisos necesarios para invocar el servicio AWS Security Agent para revisar y corregir automáticamente la seguridad del código. Adjunte esta política a una función de IAM en su cuenta que la CLI y el agente de AWS Transform Continuous Modernization asumen para cargar los artefactos de escaneo y recuperar los hallazgos.

Descripción

Esta política incluye los permisos siguientes:

- **AWS Agente de seguridad:** permite enumerar los espacios de los agentes, crear revisiones de código, iniciar trabajos de revisión de código, enumerar y recuperar los hallazgos e iniciar la corrección del código. Estas acciones se limitan a los espacios de agentes de su cuenta.
- **Amazon S3:** permite descargar los resultados y hallazgos del escaneo del `kct-security-agent-*` depósito y cargar el código fuente para el escaneo de seguridad en el `security-scans/*` prefijo incluido en ese depósito.
- **AWS Identity and Access Management (IAM):** permite transferir la `security-agent-*` función al servicio AWS Security Agent para que pueda realizar el escaneo.

La política implementa el acceso con el mínimo privilegio mediante permisos a nivel de recursos, prefijos clave y de segmento de S3, `s3:ResourceAccount` condiciones `aws:ResourceAccount` y, además, una `iam:PassedToService` condición determinada por el ámbito del servicio para garantizar que las operaciones se limiten a los recursos de Security Agent dentro de la misma cuenta. AWS AWS

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía de referencia de políticas administradas. [AWSTransformSecurityAgentExecutorAccess](#) AWS

AWS política gestionada: DBModDiscoveryAndAssessment

Esta política proporciona capacidades integrales de modernización, descubrimiento y evaluación de bases de datos para AWS Transform.

Descripción

Esta política incluye los permisos siguientes:

- **Amazon EC2:** permite describir los componentes de la infraestructura, incluidas las instancias, las VPC, las subredes, los grupos de seguridad, las zonas de disponibilidad, los puntos de enlace de las VPC y las puertas de enlace de Internet.
- **Amazon RDS:** permite describir instancias de bases de datos, clústeres y grupos de subredes. Permite modificar los grupos de subredes de bases de datos dentro de la misma AWS cuenta para preparar la migración.
- **Amazon RDS Data API:** permite habilitar y deshabilitar puntos de enlace HTTP y ejecutar sentencias SQL en clústeres de bases de datos etiquetados para el proyecto de modernización de bases de datos.

- AWS DMS— Permite describir los puntos de enlace, las instancias de replicación, las tareas, los grupos de subredes y las instancias ordenables. Permite enumerar los proveedores de datos, los perfiles de instancias y los proyectos de migración. Permite describir las estadísticas de las tablas, las ejecuciones de evaluación y las operaciones del modelo de metadatos. Las operaciones detalladas de descripción y metadatos se limitan a los recursos etiquetados para el proyecto de modernización de la base de datos.
- — Permite enumerar los secretos para descubrir las credenciales de la base de datos.
- AWS Identity and Access Management (IAM): permite inspeccionar funciones de AWS DMS servicio específicas y sus políticas asociadas. Incluye acceso a políticas de gestión de AWS lectura AWS DMS .
- AWS Key Management Service (KMS): permite enumerar los alias clave y describir las claves. Permite descifrar los secretos mediante la integración, restringida a la misma AWS cuenta.

La política implementa el acceso con el mínimo privilegio mediante permisos a nivel de recursos, condiciones basadas en etiquetas y restricciones a nivel de cuenta para garantizar que las operaciones se limiten a los recursos del proyecto de modernización de bases de datos dentro de la misma cuenta. AWS

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía de referencia de políticas gestionadas. [DBModDiscoveryAndAssessment](#) AWS

AWS política gestionada: DBModProvisioningAndMigration

Esta política proporciona capacidades de aprovisionamiento y migración de bases de datos para los proyectos de modernización de bases de datos de AWS Transform. Incluye permisos para crear y administrar la infraestructura de migración, aprovisionar las bases de datos de destino y almacenar los datos de migración.

Descripción

Esta política incluye los permisos siguientes:

- AWS DMS— Permite crear y administrar grupos de subredes de replicación, perfiles de instancias, proveedores de datos, proyectos de migración, puntos finales, instancias de replicación y tareas de replicación. Incluye operaciones de conversión de esquemas, como la importación, conversión, exportación y evaluación de modelos de metadatos. Permite gestionar el ciclo de vida de las instancias de replicación (crear, eliminar, modificar, reiniciar) y de las tareas de replicación

(eliminar, iniciar, detener, evaluar). Todas las operaciones de escritura están restringidas a los recursos etiquetados para el proyecto de modernización de la base de datos.

- Amazon RDS: permite crear grupos de subredes de bases de datos, clústeres de bases de datos e instancias de bases de datos. Todos los recursos deben estar etiquetados para el proyecto de modernización de la base de datos.
- — Permite crear, actualizar y etiquetar secretos con el prefijo de denominación de modernización de la base de datos. Permite recuperar valores secretos y describir los secretos de los recursos etiquetados.
- Amazon S3: permite crear y administrar buckets y objetos de S3 para el almacenamiento de datos de migración. Incluye el etiquetado de buckets, el control de versiones y las operaciones del ciclo de vida de los objetos. Restringido a los depósitos con el prefijo de denominación de modernización de la base de datos.
- AWS Identity and Access Management (IAM): permite transferir funciones de AWS DMS servicio específicas a los servicios de conversión de esquemas AWS DMS y convertirlos. Permite crear el rol vinculado al servicio de Amazon RDS necesario para las operaciones de la base de datos.

La política implementa el acceso con el mínimo privilegio mediante permisos a nivel de recursos, condiciones basadas en etiquetas y restricciones a nivel de cuenta para garantizar que las operaciones se limiten a los recursos del proyecto de modernización de bases de datos dentro de la misma cuenta. AWS

Detalles de los permisos

Para ver los detalles de los permisos de la política, consulte la Guía de referencia de políticas gestionadas. [DBModProvisioningAndMigration](#) AWS

AWS Referencia de permisos de transformación

En esta sección se proporciona información sobre las API que utiliza AWS Transform y su función.

Temas

- [AWS Transforma las API](#)

AWS Transforma las API

- 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

Validación de conformidad para AWS Transformar

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa de cumplimiento](#) [Servicios de AWS](#) de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y

reglamentos aplicables. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte [AWS la documentación de seguridad](#).

Resiliencia en AWS Transformar

La infraestructura AWS global se basa en zonas de disponibilidad Regiones de AWS y zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

[Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS](#)

Además de la infraestructura AWS global, AWS Transform ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos.

AWS Transform y puntos finales de interfaz (AWS PrivateLink)

Puede establecer una conexión privada entre su VPC y crear un punto final AWS Transform de VPC de interfaz. Los puntos finales de la interfaz funcionan con una tecnología que le permite acceder de forma privada a la AWS Transform consola sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión. [AWS PrivateLink](#) Direct Connect El tráfico entre tu VPC y AWS Transform no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más [interfaces de red elásticas](#) en las subredes.

Para obtener más información, consulte [Puntos de conexión de VPC de interfaz \(AWS PrivateLink\)](#) en la Guía del usuario de Amazon VPC.

Note

Para obtener PrivateLink documentación AWS Transform personalizada, consulte [AWS Transform puntos finales personalizados y de interfaz \(AWS PrivateLink\)](#).

Consideraciones para AWS Transform Puntos de conexión de VPC

Antes de configurar un punto de enlace de VPC de interfaz AWS Transform, asegúrese de revisar las [propiedades y limitaciones del punto de enlace de interfaz](#) en la Guía del usuario de Amazon VPC.

Requisitos previos

Antes de comenzar cualquiera de los procedimientos siguientes, asegúrese de que dispone de lo siguiente:

- Una AWS cuenta con los permisos adecuados para crear y configurar los recursos.
- Ya se ha creado una VPC en su cuenta. AWS
- Familiaridad con AWS los servicios, especialmente Amazon AWS Transform VPC y.

Creación de un punto final de VPC de interfaz para AWS Transform

Puede crear un punto de enlace de VPC para el AWS Transform servicio mediante la consola de Amazon VPC o el (). AWS Command Line Interface AWS CLI Para obtener más información, consulte [Creación de un punto de conexión de interfaz](#) en la Guía del usuario de Amazon VPC.

AWS Transform admite los siguientes servicios de punto final de VPC:

Nombre del servicio	Punto de conexión	Nota
Plano de control	com.amazonaws. <i>region</i> .transform	
API de agencia	com.amazonaws. <i>region</i> .transform-agents	
Aplicación web	com.amazonaws. <i>region</i> .api.transform	Necesaria para la aplicación AWS Transform web. Este punto final debe tener el DNS privado habilitado (la opción Habilitar nombre DNS) para que se api.trans

Nombre del servicio	Punto de conexión	Nota
		form. <i>region</i> .on.aws resuelva en una dirección IP privada de la VPC.

region Sustitúyalo por la AWS región en la que está instalado tu AWS Transform perfil, por ejemplo, com.amazonaws.us-east-1.transform.

Note

Si utilizas la aplicación AWS Transform web, se requiere el punto final. `api.transform`
Para ver la guía de configuración completa, consulte [Acceder al AWS Transform aplicación web desde una VPC](#).

Para obtener más información, consulte [Regiones compatibles para AWS Transform](#) [Acceder a un servicio a través de un punto final de interfaz](#) en la Guía del usuario de Amazon VPC.

Utilizar un ordenador local para conectarse a un AWS Transform punto de conexión

En esta sección se describe el proceso de usar un equipo local al que conectarse a AWS Transform través de un AWS PrivateLink punto final de la AWS VPC.

1. [Cree una conexión de VPN entre el dispositivo en las instalaciones y la VPC.](#)
2. [Cree un punto final de VPC de interfaz para. AWS Transform](#)
3. [Configure un punto de conexión entrante de Amazon Route 53.](#) Esto le permitirá usar el nombre DNS de su AWS Transform punto final desde su dispositivo local.

Acceder al AWS Transform aplicación web desde una VPC

Cuando se utiliza AWS PrivateLink para acceder a la AWS Transform API de forma privada desde la VPC, la aplicación web requiere una configuración de red adicional. Sirve contenido estático (HTML JavaScript, CSS) mediante el cual CloudFront se requiere conectividad a Internet. Las llamadas a la API desde la aplicación web pasan por el punto final de la VPC y permanecen totalmente privadas.

Esta guía le muestra cómo configurar la salida controlada de Internet desde su VPC para que la aplicación web pueda cargarse y, al mismo tiempo, mantener la VPC bloqueada solo en los dominios necesarios.

Funcionamiento

La aplicación AWS Transform web utiliza dos rutas de red:

- Llamadas a la API: cuando interactúas con la aplicación web (al iniciar trabajos, ver los espacios de trabajo, etc.), el navegador envía solicitudes a la API `aapi.transform.region.on.aws`. Con el punto de enlace de la `com.amazonaws.region.api.transform` VPC y el DNS privado habilitados, estas solicitudes se resuelven en una dirección IP privada de la VPC y nunca salen de la red. AWS
- Contenido estático: los archivos HTML y CSS de la aplicación web se envían a través CloudFront de. JavaScript `tenant-id.transform.region.on.aws` La carga de estos archivos requiere conectividad a Internet porque la entrega de CloudFront contenido solo está disponible a través de la Internet pública.
- Autenticación: se utilizan flujos de inicio de sesión en el AWS IAM Identity Center `region.signin.aws`, que también requiere conectividad a Internet.

Para habilitar la aplicación web y, al mismo tiempo, mantener la seguridad, debe crear una ruta de salida controlada mediante AWS Network Firewall con filtrado basado en el dominio. Esto permite que su VPC llegue solo a los dominios específicos que requiere la aplicación web y, al mismo tiempo, bloquea el resto del tráfico de Internet.

Arquitectura

El siguiente diagrama muestra la ruta de red para el tráfico de aplicaciones 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

El Network Firewall debe ver ambas direcciones del tráfico (enrutamiento simétrico) para realizar la inspección TLS SNI. Debe configurar una ruta de retorno en la subred de la puerta de enlace NAT que envíe el tráfico destinado a la subred privada a través del firewall. Sin esto, las reglas de filtrado basadas en el dominio no funcionarán.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una AWS cuenta con permisos para crear recursos de VPC, Network Firewall y pasarelas NAT.
- Una VPC con una subred privada en la que se ejecutan tus instancias o cargas de trabajo.
- Una puerta de enlace de Internet conectada a la VPC (o permisos para crear una).
- Un punto final de AWS Transform VPC para `com.amazonaws.region.api.transform` con el DNS privado habilitado. Este es el punto final que utiliza el cliente del navegador de la aplicación web. Para obtener instrucciones sobre la creación de puntos finales, consulte [AWS Transform y puntos finales de interfaz \(AWS PrivateLink\)](#).

Configuración de la política de puntos finales de la VPC

Si su punto de enlace de `com.amazonaws.region.api.transform` VPC tiene una política de punto de enlace personalizada, debe agregar una declaración que permita AWS Transform las operaciones. Sin esto, la aplicación web no podrá realizar llamadas a la API a través del punto final.

Añada la siguiente declaración a su política de puntos finales de VPC.

AWS_TRANSFORM_PROFILE_ARN Sustitúyalo por el ARN de tu perfil de AWS Transform servicio, que encontrarás en la AWS Transform consola, en la página de configuración.

```
{
  "Statement": [
    {
      "Sid": "AllowAWSTransform",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalArn": [
            "AWS_TRANSFORM_PROFILE_ARN"
          ]
        }
      }
    }
  ]
}
```

Note

Si su punto de conexión de VPC usa la política predeterminada (acceso total), no es necesario realizar cambios y puede omitir este paso.

Configurar la salida controlada de Internet

Complete los siguientes pasos para configurar Network Firewall con filtrado basado en el dominio para la aplicación AWS Transform web.

Paso 1: Cree la subred del firewall

Cree una pequeña subred /28 dedicada al punto final de Network Firewall. Esta subred debe estar en la misma zona de disponibilidad que su subred privada.

```
aws ec2 create-subnet \
  --vpc-id your-vpc-id \
  --cidr-block firewall-subnet-cidr \
  --availability-zone your-az \
  --region region
```

Paso 2: Cree una subred pública para la puerta de enlace NAT

```
aws ec2 create-subnet \  
  --vpc-id your-vpc-id \  
  --cidr-block public-subnet-cidr \  
  --availability-zone your-az \  
  --region region
```

Paso 3: Configurar la tabla de enrutamiento de la subred pública

Cree una tabla de enrutamiento para la subred pública que enruta el tráfico de Internet a la puerta de enlace de 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
```

Paso 4: Cree la puerta de enlace 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
```

Paso 5: Crear el grupo de reglas de Network Firewall

Cree un grupo de reglas con estado que permita el tráfico solo a los dominios requeridos por la aplicación 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 Sustitúyalo por la AWS región en la que está instalado tu AWS Transform perfil (por ejemplo, *us-east-1*). *directory-id* Sustitúyalo por el ID de directorio del IAM Identity Center (por ejemplo, *d-1234567890*). Puede encontrar su ID de directorio en la consola del IAM Identity Center.

En la siguiente tabla se explican los dominios permitidos.

Dominio	Finalidad
.cloudfront.net	CloudFront CDN: proporciona activos estáticos de aplicaciones web (CSS JavaScript, imágenes)
.transform. <i>region</i> .on.aws	URL arrendataria de la aplicación web: el navegador carga la página inicial desde este dominio mediante CloudFront
<i>region</i> .signin.aws	Página de redireccionamiento de inicio de sesión SSO
.s3. <i>region</i> .amazonaws.com	URL prefirmadas de S3: cargas y descargas de artefactos
oidc. <i>region</i> .amazonaws.com	Intercambio de token OIDC para la autenticación de SSO
portal.sso. <i>region</i> .amazonaws.com	Página de inicio de sesión en el portal SSO
assets.sso-portal. <i>region</i> .amazonaws.com	Activos estáticos del portal SSO (CSS,) JavaScript
<i>directory-id</i> .awsapps.com	Portal del centro de identidad de IAM para su organización

Note

El `.cloudfront.net` comodín permite el tráfico a cualquier CloudFront distribución, no solo a la de la aplicación AWS Transform web. No es posible aplicar un filtro de dominio más restringido porque las direcciones IP CloudFront perimetrales se comparten entre las distribuciones y la inspección del SNI mediante TLS no permite distinguir las distribuciones individuales de un mismo dominio.

Note

Las llamadas `api.transform.region.on.aws` a la API son válidas AWS PrivateLink y no requieren la salida de Internet. No se ven afectados por el firewall.

Paso 6: Crear la política de firewall

La política debe utilizar `STRICT_ORDER` la evaluación de reglas `drop_established` como acción predeterminada. Esto garantiza que se elimine cualquier tráfico que no coincida con la lista de permitidos.

```
# 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
```

Paso 7: Crear el Network Firewall

```
# Get the policy ARN
FW_POLICY_ARN=$(aws network-firewall describe-firewall-policy \
  --firewall-policy-name transform-webapp-policy \
  --region region \
  --query 'FirewallPolicyResponse.FirewallPolicyArn' --output text)

# Create the firewall
aws network-firewall create-firewall \
  --firewall-name transform-webapp-firewall \
  --firewall-policy-arn $FW_POLICY_ARN \
  --vpc-id your-vpc-id \
  --subnet-mappings SubnetId=firewall-subnet-id \
  --region region

# Wait for the firewall to become READY (3-5 minutes)
while true; do
  STATUS=$(aws network-firewall describe-firewall \
    --firewall-name transform-webapp-firewall \
    --region region \
    --query 'FirewallStatus.Status' --output text)
  echo "Status: $STATUS"
  if [ "$STATUS" = "READY" ]; then break; fi
  sleep 15
done
```

Paso 8: Obtenga el ID del punto final del 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"
```

Paso 9: Configure la tabla de rutas de subred del firewall

Enrute el tráfico con destino a Internet desde la subred del firewall a la puerta de enlace NAT.

```
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
```

Paso 10: Actualice la tabla de enrutamiento de la subred privada

Enrute todo el tráfico con destino a Internet desde la subred privada a través del 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
```

Si ya existe una ruta predeterminada, `replace-route` utilícela en lugar de `create-route`

Paso 11: Añadir la ruta de retorno simétrica (obligatorio)

⚠ Important

Este paso es fundamental. Network Firewall utiliza la inspección TLS SNI y debe ver las dos direcciones de una conexión TCP. Agregue una ruta en la tabla de rutas de la subred de la puerta de enlace NAT que envíe el tráfico de retorno destinado a la subred privada a través del 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 Sustitúyalo por el bloque CIDR de tu subred privada (por ejemplo,).
`10.0.144.0/20`

Sin un enrutamiento simétrico, el firewall solo ve una dirección del tráfico. El motor de inspección de TLS no puede extraer la indicación del nombre del servidor (SNI) del protocolo de enlace de TLS y todas las reglas basadas en el dominio fallarán silenciosamente.

Paso 12: Eliminar la ruta predeterminada de IPv6 (si existe)

Si la tabla de enrutamiento de la subred privada tiene una ruta IPv6 predeterminada (`:::/0`) que apunta directamente a una puerta de enlace de Internet, pasará por alto el firewall en cuanto a los destinos. IPv6-capable Elimínala:

```
aws ec2 delete-route \  
  --route-table-id private-subnet-route-table-id \  
  --destination-ipv6-cidr-block :::/0 \  
  --region region
```

Verificación

Desde una instancia de la subred privada, verifica la configuración:

```
# 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)
```

Resolución de problemas

El firewall bloquea las llamadas de API a api.transform

El dominio api.transform.region.on.aws debe convertirse en una dirección IP privada a través del punto final de la VPC y no debe llegar al firewall de Internet.

- Comprueba que has creado el com.amazonaws.region.api.transform punto final.
- Compruebe que el DNS privado esté habilitado en el punto final:

```
aws ec2 describe-vpc-endpoints \
  --filters "Name=service-name,Values=com.amazonaws.region.api.transform" \
  --query 'VpcEndpoints[*].[State,PrivateDnsEnabled]' \
  --output table
```

Resultado esperado: available | True

La aplicación web no se carga (se agota el tiempo de espera de la conexión)

- Compruebe que la tabla de rutas de la subred privada tenga una 0.0.0.0/0 ruta que apunte al punto final del firewall.

- Compruebe que la tabla de rutas de subred del firewall tenga una `0.0.0.0/0` ruta que apunte a la puerta de enlace NAT.
- Compruebe que la puerta de enlace NAT esté en un `available` estado.

Non-allowlisted los dominios no están bloqueados

- Compruebe si hay una `::/0` ruta IPv6 que apunte a la puerta de enlace de Internet. Esto evita el firewall. Retírelo (paso 12).
- Verifique que el enrutamiento simétrico esté configurado. La tabla de enrutamiento de subred de NAT Gateway debe tener una ruta de retorno a través del firewall para la subred privada CIDR (paso 11).
- Compruebe las acciones que utiliza la política de firewall `STRICT_ORDER` con `drop_established` y `alert_established` como acciones predeterminadas.

Consideraciones sobre costos

Recurso	Coste aproximado
Network Firewall	~0 \$. 395/hr (~\$288/month) por zona de disponibilidad
Puerta de enlace NAT	~0 \$. 045/hr (~\$33/month) + tarifas de procesamiento de datos
Elastic IP (IPv4 pública)	~0 \$. 005/hr (~3 dólares). 60/month)
Procesamiento de datos de Network Firewall	0\$. 065/GB
Procesamiento de datos de NAT Gateway	0\$. 045/GB

El costo base estimado es de aproximadamente \$ 325/month para una implementación de una sola zona de disponibilidad. Para las implementaciones de producción, implemente el firewall, la puerta de enlace NAT y las subredes asociadas en cada zona de disponibilidad donde existan subredes privadas.

Limpieza

Para eliminar todos los recursos creados en esta guía, ejecute los siguientes comandos en orden inverso. Sustituya los marcadores de posición por los ID de recursos de su implementación. Puede encontrar estos valores en la consola AWS de administración o mediante los `describe` comandos de los pasos de configuración.

```
# 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
```

Supervisión AWS Transformar

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS Transform y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para supervisar AWS Transform, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde instancias de Amazon EC2 y otras fuentes. CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcancen ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la [Guía del usuario CloudWatch de Amazon Logs](#).
- Amazon se EventBridge puede utilizar para automatizar sus AWS servicios y responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios de recursos. Los eventos de AWS los servicios se entregan EventBridge prácticamente en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulta la [Guía EventBridge del usuario de Amazon](#).
- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la [Guía del usuario de AWS CloudTrail](#).

Registro AWS Transforma las llamadas a la API mediante AWS CloudTrail

AWS Transform está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Transform. CloudTrail captura todas las llamadas a la API de AWS Transform como eventos. Las llamadas capturadas incluyen llamadas desde la consola de AWS Transform y llamadas de código a las operaciones de la API de AWS Transform. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de AWS Transform. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a AWS Transform, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

AWS Transforma la información en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS Transform, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de AWS Transform, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)

- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el [elemento userIdentity de CloudTrail](#).

Descripción AWS Transforma las entradas del archivo de registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Notificaciones

AWS Transform proporciona notificaciones por correo electrónico para mantenerte informado sobre los cambios en el acceso al espacio de trabajo, las actualizaciones del estado de los trabajos y las solicitudes pendientes de los colaboradores.

Notificaciones por correo electrónico

Las notificaciones por correo electrónico están habilitadas de forma predeterminada y se envían a los usuarios que tienen permisos de solo lectura o superiores en un trabajo. Los usuarios pueden modificar sus preferencias de notificación. Existen tres categorías de notificaciones por correo electrónico:

- Actualizaciones de acceso a Workspace

Recibirás una notificación cuando te agreguen a un nuevo espacio de trabajo y cuando cambies tu rol dentro de un espacio de trabajo.

- Correos electrónicos con resúmenes diarios

Recibirás un correo electrónico con un resumen diario a las 9:00 a.m., hora del Pacífico, con un resumen de tus trabajos en curso si tienes trabajos activos con una o más solicitudes de colaboración pendientes. El correo electrónico incluye una tabla con el nombre del espacio de trabajo, el nombre del puesto, el estado del puesto, los detalles de la solicitud de colaboración y las acciones necesarias (limitado a 10 filas)

 Note

Los correos electrónicos con resúmenes diarios solo se envían para los trabajos que requieren solicitudes de colaboración. Las solicitudes de colaboración opcionales no generan correos electrónicos resumidos.

- Actualizaciones del estado del trabajo

Recibirás un correo electrónico cuando un trabajo al que tengas acceso se complete o fracase.

- Los colaboradores solicitan actualizaciones

Recibirás un correo electrónico cada vez que una tarea requiera tu entrada, revisión o aprobación.

Administrar las notificaciones por correo electrónico

Para modificar tus preferencias de notificación por correo electrónico en la aplicación web, haz clic en la rueda dentada de configuración situada en la esquina superior derecha de la aplicación y selecciona la configuración de notificaciones.

La página de configuración de notificaciones proporciona los siguientes controles:

Tipo de notificación	Description (Descripción)	Ajuste predeterminado
Actualizaciones de Workspace Access	Recibe correos electrónicos cuando te agregues a un espacio de trabajo o cuando cambies tu rol dentro de un espacio de trabajo	Habilitado

Tipo de notificación	Description (Descripción)	Ajuste predeterminado
Resumen diario de solicitudes de colaboradores	Reciba un resumen diario de las solicitudes de trabajo abiertas de los colaboradores en espacios de trabajo accesibles	Habilitado
Actualizaciones de finalización de trabajos	Reciba correos electrónicos cuando un trabajo se complete o falle	Habilitado
Los colaboradores solicitan actualizaciones	Reciba correos electrónicos cuando se requiera una aportación o aprobación por su parte	Deshabilitado

Puedes usar una configuración general para activar o desactivar todas las notificaciones o configurar los tipos de notificaciones individuales por separado.

Cuotas para AWS Transformar

Tu AWS cuenta tiene cuotas predeterminadas, antes denominadas límites, para cada AWS servicio. A menos que se indique lo contrario, cada cuota es Region-specific. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas de AWS Transform, abra la [consola Service Quotas](#). En el panel de navegación, elija AWS servicios y seleccione AWS Transformar.

Para solicitar un aumento de cuota, consulte [Solicitud de aumento de cuota](#) en la Guía del usuario de Service Quotas. Si la cuota aún no está disponible en Service Quotas, utilice el [formulario de aumento de límite](#).

Tu AWS cuenta tiene las siguientes cuotas relacionadas con AWS Transform.

Carga de trabajo	Dimensión	Cuota	Ajustable	Description (Descripción)
Plataforma	Espacios de trabajo Región de AWS por cuenta AWS Transform habilitada	Se admiten 100 espacios de trabajo para cada uno Región de AWS	Sí	El número máximo de espacios de trabajo por cuenta AWS Transform habilitada por Región de AWS
Migración a VMware	Recuento de servidores para cada oleada	Cada oleada: 150 servidores	No	El número máximo de servidores en una oleada
Computadora central	Trabajos simultáneos para cada cuenta de IAM Identity Center	10 trabajos para cada región compatible	Sí	El número máximo de trabajos simultáneos de Mainframe en una cuenta

Carga de trabajo	Dimensión	Cuota	Ajustable	Description (Descripción)
				de IAM Identity Center
	Líneas de código para cada trabajo	3 000 000 de líneas de código para cada región compatible	No	El número máximo de líneas de código para cada trabajo.
	Analice las líneas de código mensuales	100 000 000 de líneas de código para cada región compatible	Sí	El número máximo de líneas de código para el objetivo del trabajo de Analyze Code en un mes natural
	Líneas de código mensuales para la generación de documentos empresariales	50 000 000 de líneas de código para cada región compatible	Sí	El número máximo de líneas de código para el objetivo de trabajo de generación de documentación empresarial en un mes natural

Carga de trabajo	Dimensión	Cuota	Ajustable	Description (Descripción)
	Líneas de código mensuales para la generación de documentos técnicos	50 000 000 de líneas de código para cada región compatible	Sí	El número máximo de líneas de código para el objetivo de trabajo de generación de documentación técnica en un mes natural
	Transformación de líneas de código	10 000 000 de líneas de código para cada región compatible	Sí	El número máximo de líneas de código transformadas en un mes natural
	Descomposición mensual de líneas de código	50 000 000 de líneas de código para cada región compatible	Sí	El número máximo de líneas de código para el objetivo del trabajo de descomposición en un mes natural
	Reforja las líneas de código mensuales	50 000 000 de líneas de código para cada región compatible	Sí	El número máximo de líneas de código para el objetivo de trabajo de Reforge en un mes natural

Carga de trabajo	Dimensión	Cuota	Ajustable	Description (Descripción)
	Líneas de código extraídas de lógica empresarial mensuales	50 000 000 de líneas de código para cada región compatible	Sí	El número máximo de líneas de código para el objetivo de trabajo de Extracted Business Logic en un mes natural
.NET	Líneas de código mensuales de .NET (web e IDE)	1 000 000 de líneas de código para cada región compatible	Sí	Número máximo de líneas de código de aplicación .NET que se pueden transformar en un mes natural en cada una de las cuentas compatibles Región de AWS del IAM Identity Center

Carga de trabajo	Dimensión	Cuota	Ajustable	Description (Descripción)
	Trabajos concurrentes de.NET con la extensión Microsoft Visual Studio para cada cuenta de IAM Identity Center	10 trabajos para cada región compatible	Sí	El número máximo de trabajos de transformación de .NET simultáneos en cada una Región de AWS de las cuentas del Centro de Identidad de IAM admitidos cuando se utiliza la Extensión Microsoft Visual Studio.
	Trabajos web.NET simultáneos para cada cuenta del IAM Identity Center	5 trabajos para cada región compatible	Sí	El número máximo de trabajos de transformación de .NET simultáneos admitidos en cada una Región de AWS de las cuentas del IAM Identity Center cuando se utiliza la aplicación web AWS Transform.

Carga de trabajo	Dimensión	Cuota	Ajustable	Description (Descripción)
Transformaciones personalizadas	Definiciones de transformación personalizadas	1 000	Sí	El número máximo de definiciones de transformación personalizadas
	Tamaño de definición de transformación personalizada	10 MB	No	El tamaño total máximo de todos los archivos incluidos en la definición de transformación, incluidas las referencias a los documentos.
	Solicitudes de conversación CLI mensuales de transformación personalizada	1 000 000	Sí	El número máximo de solicitudes de conversaciones de transformación personalizadas realizadas en la CLI que se permiten en un mes natural
Evaluación	Límite de recuento de servidores para cada evaluación	Cada evaluación n: 30 000 servidores	No	El número máximo de servidores en un solo trabajo de evaluación

Regiones compatibles para AWS Transform

Note

Si realizas una solicitud que requiera AWS Transform recuperar información de una región que haya optado por participar y que no aparezca en esta página, AWS Transform podrás realizar llamadas a esa región. Para gestionar el acceso a las regiones a las que AWS Transform puede hacer llamadas, consulte [Seguridad en AWS Transformar](#).

En este tema se describe Regiones de AWS dónde puede usarlo AWS Transform. Para obtener más información Regiones de AWS, consulte [Especificar qué Regiones de AWS cuenta puede usar](#) en la Guía de AWS Account Management referencia.

Es posible que sus datos se procesen en una región diferente de la región en la que los utiliza AWS Transform. Para obtener información sobre el procesamiento entre regiones AWS Transform, consulte [Cross-region procesamiento](#). Para obtener información sobre dónde se almacenan los datos durante el procesamiento, consulte [Protección de datos](#).

compatible Regiones de AWS (activado de forma predeterminada)

Puede crear AWS Transform espacios de trabajo de la siguiente Regiones de AWS manera. Estas regiones están habilitadas de forma predeterminada; no es necesario que las habilites antes de usarlas. Para obtener más información, consulte [Regiones que están habilitadas de forma predeterminada](#).

- Este de EE. UU. (Norte de Virginia)
- Europa (Fráncfort)
- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Europa (Londres)
- Asia-Pacífico (Seúl)
- Canadá (Centro)
- Sudamérica (São Paulo): solo agentes de modernización de mainframes

El espacio de trabajo en el que se crea un trabajo determina el Región de AWS del trabajo. Para crear un trabajo en una región diferente, debe usar un espacio de trabajo diferente que se encuentre en la región que desee.

En el caso de los proyectos de VMware, la región del espacio de trabajo se utiliza para la detección. Sin embargo, puede especificar una región diferente como destino de migración. Esa región de destino es donde se alojan sus cargas de trabajo cuando se completa la migración. Para obtener más información sobre Región de AWS las consideraciones a tener en cuenta a la hora de migrar a VMware, incluida la lista de posibles regiones de destino, consulte. [the section called “Regiones de destino compatibles”](#)

AWS soporte para AWS Transform

AWS Transform le permite crear y gestionar casos de AWS Support a través del chat si encuentra problemas durante sus trabajos de transformación. Sus casos se enriquecen automáticamente con el contexto laboral y se envían al equipo de soporte adecuado. Si es un cliente activo de Countdown Premium, el ingeniero designado se pondrá en contacto con usted para gestionar la resolución del problema. Obtenga más información en [AWS Countdown Premium](#). De lo contrario, tu caso será investigado por el equipo de AWS Transform soporte que está en su lista de soporte.

Requisitos previos

Antes de poder utilizar la gestión de casos de soporte, necesitas:

- Un plan de AWS Support activo: Business On-Ramp, Enterprise o Enterprise
- Una AWS Transform aplicación existente

Habilitación de Support Case Management

1. Abra la AWS Transform consola.
2. En el panel de navegación, seleccione Configuración.
3. En Support, selecciona Enable Support case management.
4. Seleccione Save changes (Guardar cambios).

AWS Transform utiliza una función vinculada al servicio (SLR) para crear y gestionar los casos de asistencia en su nombre. No se requieren permisos de IAM adicionales.

Creación de un caso de soporte

Para crear un caso de soporte, usa la interfaz de chat:

1. Solicita crear un caso de soporte. Por ejemplo:
 - «Cree un caso de apoyo para mi fallido trabajo de transformación»
 - «Necesito ayuda con los errores del trabajo, cree un caso»
2. El chat te solicitará la información requerida:

- Una breve descripción del problema
 - Una descripción detallada
3. Confirme la creación del caso cuando se le solicite.

El caso se rellena automáticamente con el contexto de su trabajo de transformación, que incluye:

- ID y estado del trabajo
- Metadatos de trabajo
- Registros de ejecución de trabajos (registros de trabajo)
- Plan de trabajo

El caso se asigna automáticamente en función del tipo de trabajo y la categoría del asunto.

Visualización de casos de soporte

Para ver sus casos de soporte, inicie el chat:

- «Enumere mis casos de soporte»
- «Muéstreme los casos de soporte abiertos»
- «¿Cuál es el estado de mis casos?»

El chat mostrará:

- ID de caso
- Asunto
- Estado, como Abierto, Pendiente, Resuelto o Cerrado
- Fecha de la última actualización
- ID de trabajo asociado

Para ver los detalles de un caso específico:

- «Muéstreme los detalles del caso [case-id]»
- «¿Cuál es la última actualización de case [case-id]?»

Añadir comunicaciones a un caso

Para añadir un mensaje a un caso existente:

1. Pregúntale al chat: «Agrega un mensaje al caso [case-id]»
2. Escribe tu mensaje cuando se te pida.
3. El chat confirmará que se agregó el mensaje.

Recibirás notificaciones cuando AWS Support responda a tu caso.

Resolver un caso

Para resolver un caso de soporte:

1. Pregunta en el chat: «Resolver el caso [identificador del caso]»
2. Confirma la resolución cuando se te pida.

Note

Solo puede resolver los casos que hayan sido abordados por AWS Support.

Desactivación de Support Case Management

1. Abre la AWS Transform consola.
2. En el panel de navegación, seleccione Configuración.
3. En Support, selecciona Disable Support case management.
4. Seleccione Save changes (Guardar cambios).

Note

Al deshabilitar la administración de casos de Support, se elimina la interfaz de administración de casos basada en el chat, pero no se cierran los casos existentes. Aún puede acceder a sus casos a través del AWS Support Center.

Telemetría de uso

El complemento AWS Transform IDE, AWS Transform Agent Skill y AWS Transform Kiro Power recopilan la telemetría de uso de forma predeterminada durante la ejecución de la transformación. La telemetría consta de diferentes puntos de datos, como el nombre del IDE (por ejemplo, VS Code o Kiro), el nombre del agente de IA (por ejemplo, Claude Code u OpenAI Codex) y el modo de ejecución (local o remoto). AWS Transform utiliza estos datos para priorizar las pruebas de compatibilidad, así como la latencia y la fiabilidad.

Para deshabilitar la telemetría, dígame al agente durante la sesión de chat que no desea que se emita la telemetría. Esta opción de exclusión solo se aplica a la sesión de chat actual y debe repetirse en cada nueva sesión. Si ejecuta la CLI de AWS transformación directamente, defina la variable de `ATX_DISABLE_TELEMETRY=true` entorno.

Datos operativos

Es posible que recopilemos señales operativas relacionadas con su uso de AWS Transform, como las funciones que utiliza, los registros de errores y las métricas en función de sus comentarios en lenguaje natural (por ejemplo, si ha aprobado continuar con un plan de transformación o si ha dado instrucciones para seguir adelante con un plan propuesto) para prestar el servicio y evaluar su rendimiento.

Registro de cambios

En la siguiente tabla se describen las versiones y actualizaciones más destacadas de AWS Transform.

Date	Title	Description (Descripción)	Links
16-07-20	AWS Transform for Migrations añade un informe resumido sobre el espacio de trabajo que se puede descargar	AWS Transform for Migrations ahora te permite generar un informe resumido del espacio de trabajo en formato PDF descargable. El informe consolida los datos de todos los trabajos de migración de tu espacio de trabajo, incluidos los estados de los trabajos, el progreso de los pasos del flujo de trabajo, la planificación de oleadas, la migración de la red, la configuración de las zonas de landing zone, el progreso del rehosting y los artefactos producidos.	Descargar un informe resumido del espacio de trabajo
03 de julio de 2026/	AWS La herramienta de descubrimiento de transformaciones añade soporte para	La herramienta de descubrimiento AWS Transform ahora recopila metadatos	Descubrimiento de bases de datos Oracle

Date	Title	Description (Descripción)	Links
	bases de datos Oracle	detallados de Oracle directamente de sus bases de datos en VMware y servidores completos. Hyper-V Puede descubrir las instancias de Oracle a través de conexiones SQL directas. La herramienta recopila la enumeración de Container Database/Pluggable Database (CDB/PDB), el inventario de componentes y el tamaño de los archivos de datos. También captura los indicadores de topología de Real Application Clusters (RAC), Data Guard y la arquitectura multiusuario. Si no ha configurado las credenciales de la base de datos, la herramienta recurre a OS-level la detección. Se admiten todas las versiones de Oracle.	

Date	Title	Description (Descripción)	Links
22-06-2020	Apoyo de la región de Sudamérica (São Paulo) a los agentes de modernización de mainframes	AWS Transform for mainframe Modernization Agents ya está disponible en la región de Sudamérica (São Paulo) (sa-east-1). Se agregó sa-east-1 a las regiones compatibles y a las tablas de inferencia entre regiones.	Regiones compatibles, inferencia Cross-region
22-06-2020	AWS Las migraciones de Transform for VMware admiten la localización	AWS Las migraciones de Transform for VMware ahora admiten la localización. Puede cambiar el idioma de visualización de la aplicación web al trabajar con los flujos de trabajo de migración de VMware. Para ello, seleccione el icono de configuración y el idioma que prefiera.	Configuración de localización

Date	Title	Description (Descripción)	Links
-18 de junio de 2026/	AWS Transform for Migrations apoya a todas AWS las regiones comerciales como objetivos de migración	AWS Las migraciones de Transform for VMware son compatibles con todas las regiones AWS comerciales como objetivos de migración, excepto Oriente Medio (Baréin) y Oriente Medio (Emiratos Árabes Unidos). Una región objetivo de migración es la AWS región en la que se implementan los recursos migrados, incluidas las zonas de destino, la infraestructura de red y el realojamiento de los servidores.	Regiones de destino de migración compatibles

Date	Title	Description (Descripción)	Links
-18 de junio de 2026/	AWS Transform for Migrations le permite adjuntar los ENI existentes a su plantilla de lanzamiento	AWS Transform le permite adjuntar las interfaces de red elásticas (ENI) existentes a la plantilla de lanzamiento para la migración . AWS Transform muestra todos los ENI existentes que se encuentran en su cuenta de destino y puede etiquetar los para que estén disponibles para su uso a través de la configuración de lanzamiento cuando se lancen las instancias.	Etiquetado de recursos de ENI para la migración
-18 de junio de 2026/	AWS Transform for Migrations le permite configurar los ajustes de replicación e inicio	AWS Transform le permite configurar las opciones de replicación y de inicio para la migración. Puede establecer la configuración para su cuenta de destino o para servidores de origen específicos.	Configuración de replicación e inicio

Date	Title	Description (Descripción)	Links
-17 de junio de 2020	Model-to-model evaluación de la migración para cargas de trabajo generativas de IA	AWS Transform ahora ofrece una migración personalizada de modelo a modelo. La transformación evalúa sus cargas de trabajo generativas de IA. Produce un plan de migración para pasar de proveedor externos a Amazon Bedrock. El AI-powered agente escanea tu base de código para identificar todos los modelos y SDK de IA en uso. El agente recopila los requisitos de migración mediante preguntas interactivas. Luego, asigna los modelos a los equivalentes de Amazon Bedrock con comparaciones de costos transparentes y cambios de código listos para la producción. Admite migraciones desde OpenAI, Google Gemini, el uso directo del SDK de	¿Qué hay de nuevo, post, transformaciones personalizadas?

Date	Title	Description (Descripción)	Links
		Anthropic y modelos de código abierto a través de LitellM u Ollama. Gestiona las integraciones directas del SDK y los patrones integrados en marcos, como CrewAI y las capas de enrutamiento de varios proveedores. LangChain LlamaIndex LangGraph Disponibles sin cargo adicional más allá del precio estándar de Transform. AWS	

Date	Title	Description (Descripción)	Links
16-06-20	AWS Transform for mainframe ofrece un flujo de trabajo rediseñado y rastreable	AWS Transform for mainframe ahora ofrece una experiencia de reinversión conectada y rastreable, desde la evaluación hasta la generación del código. Las empresas que z/OS utilizan COBOL y PL/I cargas de trabajo pueden evaluar su cartera para identificar funciones empresariales discretas, extraer reglas empresariales, generar requisitos listos para el desarrollo y producir código rastreable nativo de la nube en un único flujo de trabajo conectado. Todos los requisitos se remontan al código fuente para garantizar una auditabilidad total.	¿Qué hay de nuevo, publicación, documentación

Date	Title	Description (Descripción)	Links
16-06-20	AWS Transform ahora es compatible con Amazon FSx para NetApp ONTAP como almacenamiento de destino (versión preliminar pública)	Ahora puede migrar las cargas de trabajo de almacenamiento en bloque a Amazon FSx NetApp for ONTAP, además de a Amazon EBS, como parte del realojamiento informático. AWS Transform replica los datos de almacenamiento en bloque directamente en FSx para los volúmenes de ONTAP dentro de la misma ola de migración que gestiona la computación y la red.	¿Qué hay de nuevo?: publicación, documentación

Date	Title	Description (Descripción)	Links
2026-06-05	Soporte de evaluación del TCO de Amazon RDS for SQL Server	Ahora puede estimar los costes de la migración de bases de datos de SQL Server locales a Amazon RDS for SQL Server. Utilice la evaluación del AI-powered TCO en AWS Transform para analizar su entorno y obtener recomendaciones óptimas sobre las instancias de bases de datos. La evaluación admite las opciones Bring Your Own Media (BYOM) y License Included (LI) con Database Savings Plans para ahorrar hasta un 20%.	¿Qué hay de nuevo, publicación, documentación

Date	Title	Description (Descripción)	Links
2026-06-04	AWS La herramienta de descubrimiento de transformaciones ahora es compatible como fuente de entrada para la migración de redes	Ahora puede usar la herramienta de descubrimiento AWS Transform como fuente de migración de redes junto con Modelizelt, lo que permite migraciones de redes híbridas para entornos que ejecutan cargas de trabajo tanto de VMware como de otras compañías.	Guía del usuario
27 de mayo de 2026-05-	AWS La documentación personalizada de Transform agrega ejemplos de habilidades y mejores prácticas del lado del cliente	La documentación sobre las habilidades del lado del cliente ahora incluye ejemplos prácticos sobre el cumplimiento de Dockerfile, la seguridad en la migración de las bases de datos, la aplicación de las políticas de Terraform y las ayudas a la obsolescencia de las API, junto con las mejores prácticas para desarrollar y compartir habilidades.	Documentación

Date	Title	Description (Descripción)	Links
22 de mayo de 2026/	Transform ya dispone de nuevas capacidades de evaluación de la migración de los agentes AWS	AWS Transform ahora ofrece capacidades avanzadas de evaluación de la migración, que incluyen escenarios hipotéticos, suposiciones personalizables, compatibilidad flexible con formatos de archivo y varias funciones nuevas de evaluación del costo total de propiedad (TCO).	¿Qué hay de nuevo?: publicación, documentación
2026-05-20	AWS Transform detecta las VPC existentes durante la revisión de la migración de la red	AWS Transform ahora detecta las VPC existentes en su cuenta de destino durante la revisión de la migración de la red. Puede ver las VPC existentes junto con las VPC mapeadas, identificar los conflictos de CIDR y resolverlos antes de la implementación.	Documentación

Date	Title	Description (Descripción)	Links
14 de mayo de 2020	AWS Los agentes de transformación ahora están disponibles en Kiro, Claude, Cursor y Codex	AWS Ahora se puede acceder a los agentes de Transform a través de la tecnología de Kiro, los complementos de agente y el servidor AWS Transform MCP, lo que permite a los desarrolladores utilizar las capacidades de transformación directamente desde su entorno de desarrollo preferido.	¿Qué hay de nuevo, post
14 de mayo de 2026	AWS Transform presenta el kit de herramientas de creación de agentes para crear agentes de transformación personalizados	Los socios y los clientes ahora pueden crear, compartir y registrar agentes de transformación especializados utilizando el kit de herramientas de creación de agentes Kiro power, que integra herramientas y flujos de trabajo personalizados con Transform. AWS	¿Qué hay de nuevo, post

Date	Title	Description (Descripción)	Links
14 de mayo de 2026	AWS Transform añade un asistente de IA agentic al AWS Toolkit for Visual Studio	Los desarrolladores de .NET ahora pueden modernizar las aplicaciones mediante una experiencia conversacional guiada paso a paso directamente en Visual Studio, con todo el contexto conservado en el IDE y la consola web.	¿Qué hay de nuevo en el post
14 de mayo de 2026	AWS Transform ahora es compatible con las tiendas de artefactos propiedad de los clientes	Puede configurar su propio bucket de Amazon S3 y, si lo desea, cifrar los artefactos con su propia clave de AWS KMS, lo que le da un control total sobre dónde se almacenan los artefactos de transformación.	Novedades: publicación , guía del usuario

Date	Title	Description (Descripción)	Links
14 de mayo de 2020	AWS Transform añade recomendaciones de estrategia de migración (7R)	Con AWS Transform , ahora puede analizar el inventario descubierto y obtener una recomendación de estrategia de migración para cada servidor y aplicación. Las recomendaciones siguen las siete estrategias de migración (7R) estándares del sector. Cada recomendación incluye una sugerencia de servicio AWS objetivo, una puntuación de confianza y las razones que la sustentan. Puede generar un panel HTML interactivo, un PDF o una PowerPoint salida de Microsoft.	Recomendaciones de 7R

Date	Title	Description (Descripción)	Links
-11 de mayo de 2022	AWS Transform añade la capacidad de contenerización durante las migraciones	AWS Transform ahora admite el cambio de plataforma de aplicaciones a contenedores durante la migración, la automatización de la generación de archivos Dockerfile, la creación de imágenes de contenedores con escaneo de CVE y la implementación en Amazon ECS o Amazon EKS.	Novedades: publicación, guía del usuario
2026-05-01	AWS Transform ahora ofrece agentes de migración de BI para Power BI y Tableau a Quick	Partner-built Los agentes de Wavicle Data Solutions convierten los paneles de Power BI y Tableau en activos rápidos dentro del flujo de trabajo de Transform. AWS	¿Qué hay de nuevo, post
21 de abril de 2026	AWS La opción Transform Custom ya está disponible en seis regiones adicionales AWS	AWS Transform custom se expande a Asia Pacífico, Canadá y Europa (Londres), hasta alcanzar un total de AWS ocho regiones.	¿Qué es lo nuevo, post

Date	Title	Description (Descripción)	Links
15-04-20	AWS Transform añade la creación de zonas de aterrizaje a los flujos de trabajo de migración	Se agregó la creación de landing zone directamente en los flujos de trabajo de migración. AWS Transform comprueba una base existente, recomienda estructuras de unidades organizativas (OU) y cuentas objetivo, y ofrece un despliegue totalmente automatizado o un resultado de infraestructura como código (IaC) (CloudFormation, AWS CDK o Landing Zone Accelerator (LZA)).	¿Qué hay de nuevo? (publicación, documentación)

Date	Title	Description (Descripción)	Links
15-04-20	AWS Transform añade diagramas e informes de planificación de la migración	Ahora puede generar diagramas interactivos e informes analíticos durante la planificación de la migración . Los tipos de diagramas incluyen mapas de topología de red, gráficos de dependencia de aplicaciones, diagramas de Gantt ondulados y gráficos generales. Los tipos de informes incluyen evaluaciones de riesgos, recomendaciones de las 7 R e informes analíticos personalizados. Los resultados están disponibles como archivos HTML, PDF o Microsoft PowerPoint (.pptx) interactivos.	Diagramación e informes

Date	Title	Description (Descripción)	Links
14 de abril de 2026/	AWS Transform ya está disponible en Kiro y VS Code	AWS Ahora se puede acceder a las transformaciones personalizadas de Transform desde Kiro y VS Code, y el estado del trabajo se comparte en las superficies de IDE, CLI y consolas web.	¿Qué hay de nuevo, post

Date	Title	Description (Descripción)	Links
10-04-20	AWS Transform añade DHCP y mapeo de grupos de seguridad para la migración de la red	Se agregó compatibilidad con DHCP con el mapeo de grupos de seguridad durante la migración de la red. Si tiene cargas de trabajo de DHCP-enabled migración, ahora puede asegurarse de que sus reglas de seguridad sigan siendo válidas después de la migración. Esto se aplica tanto a las referencias a grupos de seguridad dentro de la VPC como a las reglas de salida entre VPC y entre cuentas a través de Transit Gateway.	Documentación

Date	Title	Description (Descripción)	Links
31 de marzo de 2020	AWS Transform custom anuncia la disponibilidad general del análisis automatizado de bases de código	La transformación integral del análisis de la base de código está disponible para el público en general y genera documentos de arquitectura, informes técnicos sobre la deuda y recomendaciones de modernización en cualquier idioma.	¿Qué hay de nuevo, post
31-03-2020	AWS Transform custom presenta nuevas transformaciones gestionadas para modernizar el código a escala	Se agregaron siete nuevas transformaciones gestionadas, incluidas Node.js las actualizaciones (disponibilidad general), la optimización de Java, la migración a Log4j Angular-to-React, las actualizaciones de Angular y las actualizaciones de Vue (acceso anticipado).	¿Qué hay de nuevo en la publicación

Date	Title	Description (Descripción)	Links
2026-03-20	AWS Transform añade API públicas para la migración de la red	Se agregaron API públicas para la migración de la red, lo que permite el acceso programático y de los socios a las capacidades de migración de la red.	Referencia de la API
14 de enero de 2026/	AWS Transform custom añade AWS PrivateLink soporte y se expande a Europa (Frankfurt)	AWS Transform custom ahora admite el acceso a VPC privadas AWS PrivateLink y está disponible en Europa (Fráncfort) además de en EE. UU. Este (Virginia del Norte).	¿Qué hay de nuevo en la publicación
2025-12-23	AWS Transform permite la conversión de redes para migraciones de centros de datos híbridos	AWS Transform for VMware convierte automáticamente las configuraciones de red de los centros de datos híbridos (VLAN, rangos de IP) en AWS VPC, subredes y grupos de seguridad sin necesidad de mapearlas manualmente.	¿Qué hay de nuevo, post

Date	Title	Description (Descripción)	Links
2025-12-01	AWS lanza AWS Transform custom para acelerar la modernización de toda la organización	AWS Transform Custom alcanza la disponibilidad general, lo que permite a las organizaciones automatizar las transformaciones de código repetibles a escala mediante un único comando CLI.	¿Qué hay de nuevo, post
2025-12-01	AWS Transform añade nuevas capacidades de inteligencia artificial para las migraciones empresariales a VMware	AWS El agente VMware de Transform ahora puede descubrir entornos locales, mapear dependencias, generar planes de oleadas de migración y migrar entre HyperV, Nutanix, KVM y objetivos básicos.	¿Qué hay de nuevo, post

Date	Title	Description (Descripción)	Links
2025-12-01	AWS Transform lanza un agente de IA para una modernización completa de Windows	Un nuevo agente completo de Windows automatiza la transformación de aplicaciones de .NET y bases de datos de SQL Server a Aurora PostgreSQL y se despliega en contenedores de Amazon ECS o EC2 Linux.	¿Qué hay de nuevo, post
2025-12-01	AWS Transform amplía las capacidades de transformación de .NET y mejora la experiencia de los desarrolladores	AWS Transform añade compatibilidad con .NET 10, la migración de formularios ASP.NET web a Blazor y una experiencia IDE interactiva mejorada mediante AWS Toolkit for Visual Studio.	¿Qué hay de nuevo, post

Date	Title	Description (Descripción)	Links
2025-12-01	AWS Transform for mainframe ofrece nuevas capacidades de automatización de pruebas	AWS Transform for mainframe introduce la generación automatizada de planes de pruebas, los scripts de recopilación de datos de prueba y la automatización de casos de prueba para acelerar las pruebas de modernización del mainframe.	¿Qué hay de nuevo, post
2025-12-01	AWS Transform for mainframe ahora admite la reinención de las aplicaciones	Los nuevos análisis de datos y actividades, junto con las capacidades de extracción de la lógica empresarial, permiten descomponer las aplicaciones de mainframe heredadas en arquitecturas nativas de la nube.	¿Qué hay de nuevo, post

Date	Title	Description (Descripción)	Links
13-11-2025	AWS Transform automatiza la configuración de la red Landing Zone Accelerator	AWS Transform for VMware genera automáticamente archivos YAML LZA-compatible de red, lo que optimiza la configuración de la infraestructura de nube multicuenta desde los entornos de VMware.	¿Qué hay de nuevo, post
16-07-2025	AWS Transform for mainframe presenta capacidades mejoradas de refactorización de código y lógica empresarial	AWS Transform para mainframe añade la disponibilidad general de la reforja (reestructuración de código) y una extracción ampliada de la lógica empresarial a nivel de aplicación para mejorar la calidad del código.	¿Qué hay de nuevo, post

Date	Title	Description (Descripción)	Links
15-05-2025	AWS Transform for VMware ya está disponible para el público en general	AWS Transform for VMware, un servicio de inteligencia artificial para agencias que automatiza todo el ciclo de vida de la modernización de VMware, desde el descubrimiento hasta la implementación, está disponible para el público en general.	¿Qué hay de nuevo en la publicación
15-05-2025	AWS Transform para mainframe ya está disponible de forma general	AWS Transform for mainframe, el primer servicio de inteligencia artificial para modernizar z/OS las aplicaciones de IBM a gran escala, está disponible para el público en general con nuevas funciones de análisis, descomposición y gestión de trabajos.	¿Qué hay de nuevo, post

[Descarga estos datos.](#)

Historial de documentos del AWS Guía del usuario de Transform

En la siguiente tabla se describe el historial de documentos de la Guía del usuario de AWS Transform.

Cambio	Descripción	Fecha
Análisis y remediación continuos de la cartera de modernización	Se agregó un nuevo capítulo que documenta la función de modernización continua AWS Transform (atx ctsubcomandos) para el análisis y la corrección automatizados del código. Vea la modernización continua.	3 de junio de 2026
Red Brownfield: visibilidad de las VPC existentes	Se agregó la detección de VPC existente durante la revisión de la migración de la red. AWS Transform detecta automáticamente las VPC que ya están desplegadas en la cuenta de destino y detecta los conflictos de CIDR con las VPC mapeadas. Consulta las VPC existentes en tu cuenta de destino.	18 de mayo de 2026
Se agregaron el formato de habilidades, las habilidades del lado del cliente y los registros de subagentes para Transform custom AWS	Las definiciones de transformación ahora usan el formato de habilidades (SKILL.mdcon YAML frontmatter y una carpeta opcional). <code>references/</code> Se han añadido habilidades del lado del cliente	11 de mayo de 2026

para ampliar el agente con capacidades adicionales y registros de subagentes para mejorar la depuración. Requiere CLI versión 2.0 o posterior. Consulte [Definiciones y Client-Side habilidades de transformación](#).

[Se agregó la contenido
rización del código fuente](#)

AWS Transform ahora puede contenerizar sus aplicaciones mediante IA generativa. Proporcione el código fuente de los repositorios de Git o cárguelo en zip y AWS Transform lo analizará, generará artefactos de Docker, publicará imágenes de contenedores en Amazon ECR, generará la infraestructura como código y la implementará en Amazon Elastic Container Service o Amazon Elastic Kubernetes Service. Consulte [Contenido rización del código fuente](#).

7 de mayo de 2026

[Se agregaron operaciones de optimización de red y recomendaciones guiadas](#)

Se agregó el paso 5: revisar y optimizar la red, con las operaciones de VPC y subred (eliminar, excluir, fusionar, dividir, cambiar el tamaño, cambiar el nombre, cambiar la dirección IP) y recomendaciones guiadas para la estandarización de nombres, la revisión del alcance, el dimensionamiento correcto de la capacidad, la revisión de seguridad y la consolidación de la VPC. Consulte [Revisar](#) y optimizar la red.

27 de abril de 2026

[AWS Transform Custom está disponible en 6 nuevas regiones](#)

[Se agregó compatibilidad con ca-central-1, eu-west-2, ap-northeast-1, ap-northeast-2, ap-southeast-2 y ap-south-1 en Transform custom.AWS](#)

21 de abril de 2026

[Documentación actualizada sobre los permisos de los conectores](#)

Se agregó un desglose detallado de los permisos para el Cuenta de AWS conector de destino, que abarca los permisos de S3, MGN, Migration Hub, la migración de la carga de trabajo y el aprovisionamiento de la infraestructura de landing zone. Consulte [Connect target Cuenta de AWS s.](#)

19 de abril de 2026

[Tipos de trabajos de migración a VMware actualizados](#)

Se agregaron los tipos de trabajo de detección y planificación de migración, zona de aterrizaje y zona de aterrizaje, red y migración de servidores. Se cambió el nombre de Network Migration únicamente a Network Migration y Migration Planning to Build Migration Plan. Consulte los [tipos de trabajos de migración de VMware](#).

19 de abril de 2026

[Objetivo Cuenta de AWS de Connect reestructurado](#)

Se reestructuró la configuración del conector en tres pasos: la selección del tipo de migración, el acuerdo de MAP y la configuración del conector, incluidas las regiones de destino compatibles, las funciones de cuenta, la orientación del administrador delegado y las funciones de IAM. Consulte [Connect target Cuenta de AWS s](#).

19 de abril de 2026

[Se agregaron regiones de destino adicionales solo para la migración de servidores](#)

Se documentaron 14 regiones comerciales adicionales disponibles para trabajos de migración de servidores sin migración de red, con el requisito de incluir listas de permitidos hasta el tercer trimestre de 2026. Consulte Regiones de destino [compatibles](#).

19 de abril de 2026

Se agregó el capítulo de servidores de Migrate	Se agregó un nuevo capítulo sobre los servidores de Migrate que abarca todo el flujo de trabajo de realojamiento, incluida la estructura contable, las funciones de IAM, la configuración del administrador delegado, la implementación, las pruebas y la transición de los agentes de replicación.	19 de abril de 2026
Se agregó el capítulo Build landing zone	Se agregó un nuevo capítulo sobre cómo crear una zona de aterrizaje con detalles sobre los permisos de los conectores para el aprovisionamiento de la zona de aterrizaje.	19 de abril de 2026
Mapeo y referencia de grupos de seguridad	Se agregaron estrategias de mapeo de grupos de seguridad (MAP, MAP_DHCP, SKIP) y documentación de referencia de grupos de seguridad a la red de Migrate.	13 de abril de 2026
Auto-conversion para tipos de archivos de red no compatibles	Se agregó soporte para la conversión automática de tipos de archivos de configuración de red no compatibles en la red de Migrate .	6 de abril de 2026
Se agregó una política clave de KMS para la migración de bases de datos	Se agregó la sección de cifrado para la migración de bases de datos.	26 de marzo de 2026

Nueva política AWS gestionada documentada	Se agregó DBModProvisioningAndMigration una sección.	24 de marzo de 2026
Nueva política AWS gestionada documentada	Se agregó DBModDiscoveryAndAssessment una sección.	24 de marzo de 2026
Generación de diagramas de red	Se agregó la generación opcional de diagramas de red (formatos Mermaid y PNG) a la red de Migrate .	18 de marzo de 2026
Soporte para firewalls y archivos de configuración SDN	Se agregó soporte para los archivos de configuración ACI de Palo Alto Networks FortiGate, Fortinet y Cisco para la migración de redes en la red Migrate .	11 de febrero de 2026
Etiquetado personalizado para recursos de red	Se agregó soporte de etiquetado VPC-level personalizado y a nivel de trabajo para la migración de la red en la red de Migrate .	28 de enero de 2026
Documentación de soporte agregada	Se agregó AWS soporte para la sección.	23 de diciembre de 2025
Nuevas políticas AWS gestionadas documentadas	Se agregaron AWSTransformCustomManagementTransformations secciones AWSTransformCustomFullAccessAWSTransformCustomExecuteTransformations , y.	7 de diciembre de 2025

Migración a VMware	Se actualizó la sección de migración a VMware .	1 de diciembre de 2025
Política AWS gestionada actualizada	Se actualizó la AWSServiceRoleForAWSTransformation documentación para reflejar los permisos adicionales.	1 de diciembre de 2025
Regiones admitidas	Se actualizó el tema Regiones compatibles .	1 de diciembre de 2025
Modernización del mainframe	Se actualizó la sección de modernización del mainframe .	1 de diciembre de 2025
¿Cómo empezar	Se actualizó el tema de introducción .	1 de diciembre de 2025
Full-stack Modernización de Windows	Se agregó el tema de modernización de Full-stack Windows , que incluye la sección actualizada de.NET y la nueva sección de modernización de SQL Server .	1 de diciembre de 2025
Herramienta de descubrimiento	Se agregó la sección de herramientas de descubrimiento .	1 de diciembre de 2025
Política AWS gestionada actualizada	Se actualizó AWSTransformApplicationECSEmploymentPolicy con una ampliación de los permisos de inspección de roles de IAM, la creación de roles vinculados al servicio de ECS y los permisos de KMS para admitir el cifrado de ECR.	22 de noviembre de 2025

Política AWS gestionada actualizada	Se actualizó AWSTransformApplicationDeploymentPolicy con permisos adicionales de redes EC2, inspección de roles de IAM, administración de buckets de S3 y cifrado de KMS.	22 de noviembre de 2025
Coleccionista de descubrimientos	Se agregó la documentación sobre la herramienta de descubrimiento AWS Transform .	31 de octubre de 2025
Se agregó el diagrama de la arquitectura de migración de VMware	Se agregó un diagrama de arquitectura de migración de VMware en la red Migrate .	23 de octubre de 2025
Actualización de los resultados de migración a VMware	Información actualizada sobre los resultados de la migración en la red Migrate .	12 de octubre de 2025
Actualización de los resultados de migración a VMware	Información actualizada sobre los resultados de la migración en la red Migrate .	12 de octubre de 2025
Documentación sobre el conector S3	Se agregó la documentación sobre el conector S3 para la aplicación web.NET.	8 de octubre de 2025
Nuevo tema sobre conectores de usuario	Se ha añadido el tema sobre los conectores de usuario .	21 de septiembre de 2025
Política AWS gestionada actualizada	Se actualizó la AWSServiceRoleForAWSTransform documentación.	17 de septiembre de 2025

Soporte para la evaluación del almacenamiento	Se agregó compatibilidad con los archivos NetApp Data Infrastructure Insights (DII) para las evaluaciones del almacenamiento .	2 de septiembre de 2025
Actualización de las regiones objetivo	Se han añadido tres regiones objetivo compatibles .	31 de agosto de 2025
Actualización de la política administrada	Se agregaron permisos de solo lectura del IAM Identity Center para su uso por. AWSServiceRoleForAWSTransform	29 de agosto de 2025
Nueva política gestionada documentada AWS	Se agregó AWSTransformApplicationDeploymentPolicy una sección.	28 de agosto de 2025
puntos finales de la interfaz	Se agregó el tema de puntos finales de la interfaz .	9 de julio de 2025
Versión inicial	Versión inicial de la guía del usuario de AWS Transform.	15 de mayo de 2025

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.