Guide de l’utilisateur

AWS Transformation

AWS Transformation: Guide de l’utilisateur

Table of Contents

Qu'est-ce que AWS Transformer ?

AWS Transform est un service qui vous aide à accélérer et à simplifier la transformation de l'infrastructure, des applications et du code grâce à une expérience d'IA agentique. Il fournit des outils spécialisés pour rationaliser les efforts de modernisation et de migration pour les différentes charges de travail.

Avec AWS Transform, vous pouvez :

- Modernisez et migrez IBM z/OS et Fujitsu GS21 vers AWS
- Migrez les environnements de serveurs virtuels et bare metal vers Amazon EC2, y compris VMware Hyper-V, et d'autres plateformes :
  - Découverte. Collectez et analysez l'inventaire de vos serveurs sur site à partir de différentes sources pour comprendre votre environnement avant de planifier.
  - Planification de la migration. Regroupez les applications, identifiez les dépendances et créez des vagues de migration hiérarchisées.
  - Création d'une zone d'atterrissage. Concevez et déployez une AWS base multi-comptes avec une structure organisationnelle, des contrôles de gouvernance et une configuration de comptes.
  - Migration du réseau. Traduisez la configuration de votre réseau source en une architecture AWS VPC prête pour la production et déployez-la.
  - Réhébergement du serveur. Réhébergez vos serveurs pour qu'ils s'exécutent en mode natif sur Amazon EC2 grâce à des flux de travail guidés de réplication, de test et de basculement.
  - Conteneurisation du code source. Conteneurisez les applications à partir du code source et déployez-les sur Amazon Elastic Container Service ou Amazon Elastic Kubernetes Service.
- Modernisez les applications .NET pour les convertir en .NET Linux-ready multiplateformes
- Evaluer les charges de travail en vue de leur préparation à

AWS Transform vous permet de confier les tâches de transformation complexes et fastidieuses à travers les phases de découverte, de planification et d'exécution à des agents d'IA spécialisés dans les langages, les frameworks et l'infrastructure. Cette approche permet à vos équipes de se concentrer sur l'innovation tout en transformant efficacement des projets complexes à grande échelle grâce à une expérience Web unifiée.

L'utilisation de AWS Transform est gratuite.

Terminologie

Dans cette section, les italiques indiquent un terme officiel dans la définition d'un terme différent.

Connexion au compte

Dans ce contexte, le compte est une référence généralisée à un conteneur appartenant au client ou à une limite de sécurité pour les ressources en service AWS ou à distance, par exemple un compte Compte AWS ou GitHub .

Artefact

Un produit livrable produit par AWS Transform.

Administrateur

Les administrateurs peuvent lire et modifier tout ce qui se trouve dans l'espace de travail. Ils peuvent entamer des discussions avec AWS Transform, démarrer et arrêter des tâches et upload/download des artefacts. Les administrateurs peuvent interagir avec les tâches en cours d'exécution pour les actions HITL (human in-the-loop) et approuver des actions HITL critiques, telles que la fusion avec le serveur principal, la réalisation d'une décomposition graphique ou le déploiement de code dans des environnements de production. Les administrateurs peuvent modifier les espaces de travail, les connecteurs et les utilisateurs.

Agent

Service spécifique à une tâche qui exécute un type de transformation spécifique. Par exemple, les migrations vers VMware.

Approbateur

Les approbateurs disposent d'autorisations similaires à celles des administrateurs, sauf qu'ils ne sont pas autorisés à modifier les espaces de travail, les connecteurs ou les utilisateurs. Les approbateurs ne peuvent pas modifier les espaces de travail, les connecteurs ou les utilisateurs.

Atout

Entrée pour une tâche de transformation. Par exemple, le code source, le serveur, la base de données, le réseau du client. Les actifs sont accessibles via un connecteur.

Demande de collaborateur

Une tâche dans laquelle AWS Transform demande à un humain de faire quelque chose.

connecteur

Les connecteurs sont des fournisseurs d'actifs qui permettent d'accéder aux ressources appartenant au client dans un système externe à AWS Transform.

Lorsque vous configurez un connecteur, l'administrateur du compte auquel vous vous connectez doit accepter la connexion. Pour accepter la connexion, ils doivent disposer des autorisations accordées dans la politique d'acceptation des connecteurs.

Les deux comptes suivants doivent être identiques ou appartenir à la même AWS Organizations organisation :

- Compte à partir duquel l'administrateur de AWS Transform active le service.
- Le compte qui sera le destinataire de votre transformation. Ce compte doit se voir attribuer un rôle IAM lui permettant d'utiliser un connecteur.

Contributeur

Les contributeurs peuvent tout lire dans l'espace de travail. Ils peuvent entamer des discussions avec AWS Transform, démarrer et arrêter des tâches, charger ou télécharger des artefacts et interagir avec les tâches en cours pour les actions HITL. Cependant, ils ne peuvent pas effectuer d'actions HITL critiques, telles que la fusion avec main, la décomposition de graphes ou le déploiement de code dans des environnements de production. Les contributeurs ne peuvent pas non plus modifier les espaces de travail, les connecteurs ou les utilisateurs.

Objectif

État final défini par l'utilisateur que AWS Transform s'efforce d'atteindre. Les utilisateurs écrivent ceci, puis AWS Transform convertit l'objectif en une série de tâches qu'il exécute de concert avec les utilisateurs lorsque cela est nécessaire.

Poste

Processus de longue haleine (weeks/months+) sur lequel AWS Transform travaille afin d'atteindre un objectif défini par un utilisateur. Composé de multiples tâches et demandes de collaborateurs.

Planifier

Liste des tâches que AWS Transform entreprend (avec l'aide d'utilisateurs humains) dans la poursuite d'un objectif.

Lecteur

Les lecteurs peuvent consulter l'état et les résultats des tâches de AWS Transform, mais ne peuvent y apporter aucune modification. Ils peuvent lire tout ce qui se trouve dans l'espace de travail, télécharger des artefacts, consulter les offres d'emploi et visualiser les actions HITL (human in-the-loop). Cependant, les lecteurs ne peuvent pas effectuer d'actions de mutation dans AWS Transform.

Tâche

Unité de travail individuelle qui fait partie d'un travail.

Carnet de travail

Un journal des actions que AWS Transform et les utilisateurs ont effectuées dans le cadre d'une tâche.

Espace de travail

Une ressource AWS Transform qui contient d'autres ressources telles que des connecteurs et des jobs. Un espace de travail sert de limite d'autorisations.

Démarrage avec AWS Transformation

Rubriques

Configuration AWS Transformation

Avant de commencer

Avant de configurer AWS Transform, assurez-vous que vous disposez d'un AWS compte avec accès administrateur.

> **Note**
>
> Si vous souhaitez essayer AWS Transform en tant que preuve de concept ou pour des environnements de test, consultez Démarrage rapide : essai de Transform. AWS

Inscrivez-vous pour Compte AWS

Pour commencer AWS, vous avez besoin d'un Compte AWS. Pour plus d'informations sur la création d'un Compte AWS, consultez la section Démarrage avec un Compte AWS dans le Guide de Gestion de compte AWS référence.

Commencer à utiliser IAM-only Access

Avec IAM-only l'accès, les utilisateurs s'authentifient à l'aide de leurs AWS informations d'identification existantes.

Pour configurer l' IAM-only accès :

1. Dans la AWS console, accédez à AWS Transform et choisissez Commencer.
2. Terminez la configuration des paramètres du compte.
3. Sous Accès utilisateur, sélectionnez IAM-only Accès.
4. Choisissez Activer pour créer votre profil.

Les utilisateurs se connectent à l'application Web AWS Transform via AWS Sign-In. Leur identifiant utilisateur dans l'application Web est basé sur leur principal IAM.

> **Important**
>
> Vous ne pouvez pas ajouter de fournisseur d'identité une fois la configuration terminée. Pour gérer les utilisateurs avec IAM Identity Center ou un fournisseur d'identité existant, choisissez l'une de ces options lors de la configuration initiale.

Avec IAM-only l'accès, tout responsable IAM disposant de l'`transform:AccessTransformProfile`autorisation sur la ressource de profil peut accéder à AWS Transform. Vous gérez l'accès des utilisateurs par le biais de politiques IAM plutôt que par le biais d'attributions d'utilisateurs aux fournisseurs d'identité.

L'`transform:AccessTransformProfile`action donne uniquement accès à AWS Transform. Une fois dans AWS Transform, les rôles de l'espace de travail contrôlent les actions qu'un utilisateur peut effectuer. Ces rôles incluent Administrateur, Contributeur, Approbateur et Read-only. Les rôles de l'espace de travail s'appliquent quel que soit le mode d'authentification de l'utilisateur.

Utilisation des informations d'identification IAM

Gestion des informations sur les utilisateurs

Lorsque les principaux utilisateurs IAM accèdent à AWS Transform, le service gère l'identité des utilisateurs différemment de la manière dont l'accès est basé sur le fournisseur d'identité.

Identité de l'utilisateur

Les utilisateurs IAM sont identifiés par leur responsable IAM.

Double identité

Un utilisateur qui possède à la fois une identité de fournisseur d'identité (comme IAM Identity Center) et une session IAM apparaît comme deux utilisateurs distincts dans AWS Transform. Leur travail n'est pas lié à ces deux identités.

Notifications par e-mail

Les notifications par e-mail ne sont activées que pour les utilisateurs SSO. Les directeurs IAM peuvent toujours être ajoutés aux espaces de travail, mais ils ne recevront pas de notifications par e-mail.

Audit

Les appels d'API IAM sont enregistrés AWS CloudTrail avec l'identité IAM de l'appelant. Les actions effectuées par les utilisateurs IAM dans le cadre d'une tâche sont également traçables dans les worklogs de AWS Transform.

Activation de l'accès IAM aux côtés d'un fournisseur d'identité

Si vous configurez AWS Transform avec IAM Identity Center ou un fournisseur d'identité tiers, vous pouvez également activer l'accès IAM comme moyen supplémentaire d'authentification. Cela permet aux responsables IAM d'accéder à AWS Transform aux côtés des utilisateurs existants de votre fournisseur d'identité.

L'accès IAM est activé par défaut lorsque vous créez un profil auprès d'IAM Identity Center ou d'un fournisseur d'identité tiers. Pour activer ou désactiver l'accès IAM à tout moment :

1. Dans la console AWS Transform, accédez à Paramètres.
2. Sous AWS Transformer l'accès avec les informations d'identification IAM, activez ou désactivez Activer l'accès IAM.

Lorsque l'accès IAM est activé, les utilisateurs du fournisseur d'identité et les responsables IAM peuvent utiliser Transform. AWS Les utilisateurs IAM et les utilisateurs des fournisseurs d'identité peuvent collaborer dans le même espace de travail.

Démarrage avec AWS Organizations

Pour configurer AWS Transform, procédez comme suit :

1. Connectez-vous au compte de gestion de votre AWS organisation.
2. Accédez au service AWS Transform.
3. Choisissez Activer le service pour que votre organisation puisse utiliser AWS Transform.
4. Configurez les autorisations nécessaires pour les comptes des membres de l'organisation.
5. Accédez à l'expérience Web AWS Transform à partir de vos comptes membres.

> **Note**
>
> Pour utiliser la AWS solution Landing Zone Accelerator (LZA) afin de créer votre zone d'atterrissage avec AWS Transform pour les fonctionnalités de migration, votre compte AWS Transform et votre installation LZA doivent se trouver dans la même AWS organisation. L'utilisation d'identifiants d'organisation distincts pour les déploiements LZA et AWS Transform n'est pas prise en charge car cela peut entraîner des incohérences dans la gestion organisationnelle et les déploiements de ressources. Pour savoir comment configurer votre installation LZA à l'aide des organisations, consultez Déployer une base cloud pour prendre en charge des charges de travail hautement réglementées et des exigences de conformité complexes dans le guide de l'utilisateur du Landing Zone Accelerator on AWS Implementation Guide.

Démarrage avec AWS IAM Identity Center

Suivez ces étapes pour utiliser IAM Identity Center for AWS Transform et pour ajouter des utilisateurs et des groupes.

Par défaut, aucun utilisateur n'a accès à AWS Transform lorsque vous l'activez pour la première fois.

> **Note**
>
> IAM Identity Center n'est pas limité à la région dans laquelle il est configuré. Si vous avez déjà configuré IAM Identity Center dans une région qui n'est pas prise en charge par AWS Transform, vous pouvez l'utiliser pour AWS Transform.

1. Configurez IAM Identity Center en suivant les instructions de la section Pour activer une instance d'IAM Identity Center.

Configurez IAM Identity Center pour utiliser un fournisseur d'identité d'entreprise externe et répliquez ses informations sur les utilisateurs et les groupes dans IAM Identity Center.

2. Dans la AWS console, sélectionnez AWS Transformer et choisissez Commencer.
3. Choisissez Activer le service pour que votre organisation puisse utiliser AWS Transform.
4. Sélectionnez une clé de chiffrement. La sélection par défaut est une clé AWS gérée. Pour utiliser une clé personnalisée :

   a. Sous Clé de chiffrement, choisissez Personnaliser les paramètres de chiffrement.

   b. Sélectionnez Utiliser une clé AWS KMS.

   c. Choisissez une clé existante ou créez-en une nouvelle.

   d. Choisissez Soumettre pour appliquer vos modifications, puis choisissez Activer la AWS transformation.

   Choisissez Afficher le profil pour afficher la configuration. L'URL de l'application Web est utilisée par vos utilisateurs pour accéder à l'expérience Web unifiée de AWS Transform.
5. Sélectionnez Utilisateurs dans le volet de navigation, puis sélectionnez Attribuer des utilisateurs ou des groupes.
6. Recherchez le nom de l'utilisateur ou des groupes que vous souhaitez autoriser à utiliser AWS Transform. La recherche fait référence aux utilisateurs et aux groupes propagés par votre fournisseur d'identité.
7. Sélectionnez un groupe ou un utilisateur, sélectionnez Terminé, puis Attribuer. Ces utilisateurs sont autorisés à utiliser l'interface Web unifiée de AWS Transform.

Utilisation de fournisseurs d'identité tiers

AWS Transform prend en charge l'intégration avec des fournisseurs d'identité tiers (IdPs) tels qu'Azure Active Directory (Entra ID) et Okta Workforce Identity. Cela vous permet d'utiliser votre système de gestion des identités existant pour l'authentification des utilisateurs.

Conditions préalables

Avant de configurer l'intégration d'un fournisseur d'identité tiers, assurez-vous que les attributs nom, e-mail et nom d'utilisateur des utilisateurs de votre fournisseur d'identité sont configurés

Informations stockées

Lorsque vous utilisez AWS Transform avec IdPs, AWS stocke un minimum d'informations utilisateur cryptées et sécurisées :

Informations utilisateur stockées

AWS Transform stocke les informations de base du profil utilisateur lors de la première connexion, notamment le nom d'affichage, l'adresse e-mail, le nom d'utilisateur (preferred_username) et un identifiant utilisateur unique. Ces informations sont chiffrées à l'aide d'une clé KMS appartenant au client ou d'une clé appartenant au service, en fonction de la configuration du profil Transform du AWS client. Les données sont stockées dans la base de données d'authentification de AWS Transform et ne sont collectées que lors de la session de connexion initiale. Cela renseigne les résultats de recherche lorsque vous invitez d'autres utilisateurs à rejoindre un espace de travail.

Cycle de vie des données

Les informations utilisateur sont stockées uniquement pour les utilisateurs qui se sont connectés à l'application Web AWS Transform au moins une fois et peuvent devenir obsolètes si les utilisateurs mettent à jour leurs informations dans leur fournisseur d'identité sans se reconnecter à AWS Transform. Toutes les informations utilisateur stockées sont supprimées lors de la suppression du profil AWS Transform.

Stockage secret du client

Le secret client fourni lors de la configuration est stocké AWS Secrets Manager via un Service Linked Secret (SLS) sur votre compte.

Gestion des identificateurs d'utilisateurs

Entrez

Utilise la revendication « oid » (identifiant d'objet) comme identifiant utilisateur unique, qui est immuable et identifie de manière unique les utilisateurs sur l'ensemble du locataire Microsoft. Cette valeur est visible pour les clients dans la console Entra et apparaît dans CloudTrail les journaux.

Identité Okta Workforce

Utilise différentes revendications pour l'identification des utilisateurs en fonction du type de jeton : la « sous-revendication » dans les jetons d'identification et la revendication « uid » dans les jetons

d'accès. AWS Transform confirme que les deux revendications contiennent la même valeur lors de l'authentification. Cette valeur est visible pour les clients dans la console Okta et apparaît dans les CloudTrail journaux.

Configuration d'Azure Active Directory (Entra ID)

Pour configurer l'intégration d'Azure Active Directory à AWS Transform :

1. Accédez au portail Azure et sélectionnez Azure Active Directory.
2. Dans le volet de navigation de gauche, choisissez Gérer > Inscriptions d'applications.
3. Choisissez + Nouvelle inscription.
4. Entrez le nom d'une application, choisissez le type de compte pris en charge, laissez l'URI de redirection vide et choisissez Enregistrer.
5. Dans la navigation de gauche, choisissez Gérer > Manifeste.
6. Effectuez `requestedAccessTokenVersion` la mise `null` à jour 2 de à et choisissez Enregistrer.
7. Choisissez Gérer > Exposer une API, puis choisissez Ajouter une étendue.
8. Créez un URI d'ID d'application à l'aide de la structure par défaut`api://<client-id>`.
9. Ajoutez la lunette`transform:read_write`.
10. Choisissez Ajouter un certificat ou un secret et créez un nouveau secret client. Enregistrez cette valeur car elle est nécessaire à la création du profil.
11. Trouvez l'URL de l'émetteur en choisissant Endpoints et en sélectionnant le document de métadonnées OpenID Connect. Le champ « émetteur » des métadonnées correspond à l'URL de votre émetteur.
12. Créez un profil dans la console AWS Transform à l'aide de l'ID client, du secret client et de l'URL de l'émetteur.
13. Une fois le profil créé, ajoutez un URI de redirection en choisissant Ajouter une plateforme, en sélectionnant Web, puis en saisissant`<web-application-url>/login/callback`.

Configuration d'Okta Workforce Identity

Pour configurer l'intégration d'Okta Workforce Identity à AWS Transform :

1. Accédez à votre console Okta Workforce Identity.

2. Choisissez Applications > Applications, puis sélectionnez Créer une intégration d'applications.
3. Sélectionnez OIDC - OpenID Connect and Web Application, puis choisissez Next.
4. Donnez un nom à votre application, laissez le type de subvention comme code d'autorisation, laissez les URI de redirection vides, configurez les attributions des utilisateurs et choisissez Enregistrer.
5. Accédez à l'onglet Connexion et définissez l'émetteur sur l'URL Okta au lieu de Dynamic.
6. Copiez l'ID client et configurez-le comme audience pour votre serveur d'autorisation en accédant à Sécurité > API et en ajoutant un serveur d'autorisation.
7. Dans le serveur d'autorisation, ajoutez l'étendue `transform:read_write` sous l'onglet Étendues.
8. Ajoutez une politique d'accès qui permet à l'application OIDC d'utiliser ce serveur d'autorisation et configurez une règle pour cette politique.
9. Sur la page Paramètres du serveur d'autorisation, notez l'URL de l'émetteur pour la création du profil dans AWS Transform.
10. Créez un profil dans AWS Transform à l'aide de l'URL de l'émetteur, de l'ID client et de la clé secrète du client dans les paramètres de l'application.
11. Une fois le profil créé, ajoutez-le `<web-application-url>/login/callback` comme URL de redirection dans l'onglet Général de l'application.

> **Note**
>
> Si vous souhaitez être redirigé vers l'application Web AWS Transform après votre déconnexion, vous devez configurer l'URL de votre application Web en tant qu'origine fiable sous Sécurité > API.

Intégration des utilisateurs

Cette section décrit l'expérience des utilisateurs qui ont obtenu l'accès à AWS Transform.

Accepter l'invitation

Lorsqu'un utilisateur est ajouté à AWS Transform, il reçoit une invitation par e-mail contenant :

- Un message d'accueil et des informations sur l'invitation
- URL de l'application Web AWS Transform

- Leur nom d'utilisateur
- Un lien pour accepter l'invitation et configurer leur mot de passe

Pour créer leur compte, procédez comme suit :

1. L'utilisateur clique sur le lien « Accepter l'invitation » figurant dans l'e-mail.
2. Sur la page « Inscription d'un nouvel utilisateur », ils saisissent et confirment un mot de passe.
3. Le mot de passe doit répondre aux exigences de sécurité, notamment :
    - Au moins 8 caractères
    - Au moins une lettre en majuscules
    - Au moins une lettre en minuscules
    - Au moins un chiffre
    - Au moins un caractère spécial
4. Après avoir créé un mot de passe, ils voient une confirmation indiquant que leur compte a été créé avec succès.

Se connecter à AWS Transformation

Pour vous connecter à AWS Transform :

1. Accédez à l'URL de l'application Web AWS Transform fournie dans l'e-mail d'invitation.
2. Entrez le nom d'utilisateur.
3. Choisissez Suivant.
4. Entrez le mot de passe.
5. Choisissez Sign in (Connexion).

Expérience de bienvenue

Lors de la première connexion, les utilisateurs voient la page d'accueil de AWS Transform avec :

- Un message d'accueil personnalisé
- Capacités de transformation disponibles
- Possibilité de créer un espace de travail

La page d'accueil fournit des informations sur les fonctionnalités de transformation disponibles dans AWS Transform, notamment :

- Modernisez z/OS les migrations IBM vers AWS
- Migrer les charges de travail VMware vers Amazon EC2
- Modernisez les applications .NET pour les convertir en .NET Linux-ready multiplateformes
- Evaluer les charges de travail en vue de leur préparation à

Les utilisateurs peuvent commencer par créer un espace de travail ou demander à leur équipe de les ajouter à un espace de travail existant.

Utilisation de votre propre compartiment Amazon S3

Par défaut, AWS Transform utilise un compartiment Amazon S3 géré par un service pour stocker les artefacts de transformation. Vous pouvez choisir d'utiliser votre propre compartiment Amazon S3 à la place pour mieux contrôler le stockage des données, le chiffrement et les politiques d'accès.

> **Note**
>
> Si vous disposez d'un compartiment Amazon S3 pour les transformations de mainframe, vous pouvez continuer à utiliser ce connecteur S3 et vous n'avez pas besoin d'utiliser cette fonctionnalité.

> **Note**
>
> Votre compartiment Amazon S3 ne stocke que les téléchargements et les artefacts de transformation avec lesquels vous interagissez. Les artefacts internes générés par le système ne sont pas stockés dans votre compartiment. En outre, AWS Transform indexe les artefacts de votre compartiment. Il stocke les données indexées dans une base de connaissances gérée par un service qui est utilisée pour vous offrir une expérience de chat enrichie.

Conditions préalables

Avant de configurer votre propre compartiment Amazon S3, assurez-vous que les conditions suivantes sont remplies :

- Le bucket doit se trouver dans la même AWS région que celle où AWS Transform est activé.
- La politique de compartiment requise doit être appliquée à votre compartiment. Pour de plus amples informations, veuillez consulter the section called "Politique en matière de bucket requise".
- Si vous utilisez l'application Web AWS Transform, CORS doit être configuré sur votre bucket. Pour de plus amples informations, veuillez consulter the section called "Configuration CORS requise".
- Si vous utilisez une clé AWS KMS personnalisée, la politique de clé requise doit être appliquée. Pour de plus amples informations, veuillez consulter the section called "Politique relative aux clés KMS (facultatif)".

Configurations de chiffrement compatibles

Votre bucket doit utiliser l'une des configurations de chiffrement suivantes :

- SSE-S3 (AES256) — Laissez le champ clé KMS vide. AWS Transform écrit des objets sans spécifier d'en-tête de chiffrement, et Amazon S3 applique le chiffrement par défaut du compartiment avec des S3-managed clés. Pour plus d'informations, consultez la section Utilisation du chiffrement côté serveur avec les clés gérées Amazon S3 (SSE-S3) dans le guide de l'utilisateur Amazon S3.
- SSE-KMS avec une clé KMS gérée par le client — Fournissez l'ARN de la clé KMS. AWS Transform écrit des objets à `x-amz-server-side-encryption: aws:kms` l'aide de la clé fournie. Suivez the section called "Politique relative aux clés KMS (facultatif)".

Les éléments suivants ne sont pas pris en charge :

- SSE-KMS avec une clé KMS AWS gérée (par exemple,`aws/s3`)
- SSE-C
- DSSE-KMS
- Clés KMS asymétriques ou clés KMS avec une spécification de clé autre que SYMMETRIC_DEFAULT

> **Warning**
>
> AWS-les clés KMS gérées ne sont pas prises en charge. Si votre compartiment est chiffré avec`aws/s3`, migrez vers une clé gérée par le client ou SSE-S3 avant de l'utiliser avec AWS Transform.

Configuration de votre compartiment Amazon S3

Vous pouvez configurer AWS Transform pour utiliser votre propre compartiment Amazon S3 depuis la console AWS Transform.

Pour utiliser votre propre compartiment Amazon S3

1. Dans la console AWS Transform, choisissez Paramètres.
2. Dans Stockage des artefacts, choisissez Utiliser mon propre compartiment S3. Vous pouvez utiliser un compartiment sur votre compte actuel Compte AWS ou sur un autre compte.
3. Pour Bucket, entrez l'URI Amazon S3.
4. (Facultatif) Pour la clé AWS KMS, entrez un ARN de clé KMS pour chiffrer les objets du compartiment. Si vous laissez ce champ vide, AWS Transform écrit des objets sans en-tête de chiffrement et Amazon S3 applique les paramètres de chiffrement par défaut du compartiment. Pour plus d'informations, consultez la section Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3 dans le guide de l'utilisateur Amazon S3.

   Si le cryptage par défaut de votre bucket est SSE-KMS, entrez l'ARN de la clé KMS gérée par le client dans ce champ et mettez à jour votre politique de clé. Pour de plus amples informations, veuillez consulter the section called “Politique relative aux clés KMS (facultatif)”.
5. Choisissez Enregistrer. AWS Transform valide la configuration et les autorisations du bucket avant d'appliquer la configuration.

Après avoir enregistré la configuration, AWS Transform utilise votre compartiment pour stocker les artefacts de transformation.

> **Note**
>
> AWS Transform valide votre configuration uniquement lorsque vous l'enregistrez. Si vous modifiez ultérieurement la politique de compartiment, la configuration CORS ou la politique de clé KMS, enregistrez de nouveau les paramètres de votre profil pour les revalider.

Politique en matière de bucket requise

Vous devez configurer la politique de compartiment pour accorder l'accès à AWS Transform. Ajoutez la politique de compartiment suivante à votre compartiment Amazon S3 pour permettre au

principal du service AWS Transform de lire, d'écrire, de supprimer et de répertorier les artefacts de transformation.

```
{
    "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"
                }
```

```
            }
        }
    ]
}
```

Remplacez les valeurs suivantes :

- *bucket-name*— Le nom de votre compartiment Amazon S3.
- *profile-account-id*— L' Compte AWS identifiant associé à votre profil AWS Transform.
- *profile-arn*— L'ARN de votre profil AWS Transform.

Configuration CORS requise

Si vous utilisez l'application Web AWS Transform, vous devez configurer le partage Cross-Origin des ressources (CORS) sur votre compartiment Amazon S3. Vous pouvez trouver le domaine de l'application Web après avoir activé AWS Transform. Pour de plus amples informations, veuillez consulter Prise en main.

```
[
    {
        "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
    }
]
```

Remplacez les valeurs suivantes :

- *webapp-domain*— L'URL d'origine de votre application Web (par exemple`https://1a2b3c4d5e6f7a8b9.transform.us-east-1.on.aws`), qui se trouve sur la page des paramètres de AWS transformation. N'incluez pas la barre oblique de fin.

Politique relative aux clés KMS (facultatif)

Cette section s'applique uniquement lorsque votre compartiment est chiffré à l'aide d'une clé KMS gérée par le client. Si votre bucket l'utilise SSE-S3, ignorez cette section.

Si vous spécifiez votre propre clé AWS KMS pour le chiffrement des compartiments, ajoutez l'instruction suivante à votre politique de clé. AWS Transform s'appuie sur les sessions d'accès direct (FAS) pour créer des subventions pour son principal de service. Ces autorisations sont utilisées pour valider votre clé et accéder aux artefacts de votre compartiment 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"
        }
    }
```

```
}
```

Remplacez les valeurs suivantes :

- *key-owner-account-id*— L' Compte AWS ID auquel appartient la clé KMS.
- *region*— La AWS région dans laquelle la AWS transformation est activée (par exemple,`us-east-1`).

Revenir au compartiment par défaut

Vous pouvez revenir au compartiment géré par les services à tout moment.

Pour passer à AWS Transformez le stockage géré

1. Dans la console AWS Transform, choisissez Paramètres.
2. Dans Stockage des artefacts, choisissez Modifier.
3. Choisissez AWS Transform Managed Storage.
4. Choisissez Enregistrer.

> **Warning**
>
> Si vous changez de configuration de stockage alors que des tâches de transformation sont en cours, celles-ci échouent. Tous les artefacts déjà générés par ces tâches en cours ne seraient pas non plus accessibles.

> **Important**
>
> Lorsque vous revenez au compartiment géré par les services :
>
> - Les artefacts de votre bucket ne sont pas automatiquement migrés. Pour conserver tous les artefacts, téléchargez-les depuis votre compartiment Amazon S3 et téléchargez-les à nouveau via l'application Web AWS Transform vers la boutique d'artefacts de l'espace de travail et de la tâche correspondants.

- AWS Transform retire la subvention accordée à votre clé KMS. Les objets écrits dans votre compartiment restent dans votre compartiment ; supprimez-les manuellement s'ils ne sont plus nécessaires.

Téléchargement de fichiers directement dans votre bucket

Vous pouvez télécharger des fichiers directement dans votre compartiment Amazon S3 sans utiliser l'application Web AWS Transform. Pour mettre les fichiers chargés à la disposition des agents de transformation, téléchargez-les `User Uploads` dans le dossier de la tâche. Le chemin du répertoire de ce dossier utilise le format suivant :

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

Remplacez les valeurs suivantes :

- *`workspace-id`*— L'ID de votre espace de travail AWS Transform.
- *`job-id`*— L'ID de la tâche de transformation.

Dans AWS Transform, chaque tâche possède son propre `User Uploads` dossier. Les fichiers que vous chargez vers ce chemin apparaissent dans l'application Web et sont mis à la disposition des agents de transformation pendant qu'ils terminent la tâche.

Les chemins d'accès aux fichiers ne doivent pas contenir `..` d'espaces de début ou de fin. Les fichiers qui enfreignent ces contraintes ne sont pas visibles pour les agents. `//`

⚠ La suppression du contenu du bucket peut entraîner l'échec des tâches

La suppression `job_objective` entraînera l'échec des tâches actives ou si la session est rétablie. Pour tous les autres fichiers, leur suppression peut entraîner un comportement inattendu de l'agent ou des échecs de travail.

⚠ Important

Si votre bucket l'utilise SSE-KMS, incluez les en-têtes suivants à chaque téléchargement direct :

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

Les objets doivent être chiffrés à l'aide de la clé KMS enregistrée dans votre profil AWS Transform. Les objets chiffrés avec une autre clé ne sont pas accessibles à AWS Transform.

Matrice de compatibilité

Le tableau suivant récapitule la compatibilité de AWS Transform avec les fonctionnalités courantes des compartiments Amazon S3.

Fonctionnalité	Compatibilité	Remarques
Création de versions du compartiment	Pris en charge	Gérez les versions non actuelles à l'aide d'une règle de cycle de vie.
Propriétaire de l'objet	Obligatoire : le propriétaire du bucket est obligatoire	Le propriétaire du bucket est préféré et Object Writer ne sont pas pris en charge.
ACL	Non pris en charge	Les ACL doivent être désactivées sur le bucket.
Object Lock (mode de gouvernance)	Partiellement pris en charge	Les suppressions peuvent être bloquées par les paramètres de rétention.
Object Lock (mode de conformité)	Non pris en charge	—
Blocage de l'accès public	Pris en charge	—
paiement par le demandeur	Non pris en charge	—
Points d'accès S3	Non pris en charge	Utilisez le nom du compartiment.

Fonctionnalité	Compatibilité	Remarques
Points d'accès S3 Object Lambda	Non pris en charge	Utilisez le nom du compartiment.
S3 sur Outposts	Non pris en charge	—
S3 Express One Zone (compartiments de répertoires)	Non pris en charge	—
Cross-Region seaux	Non pris en charge	—
Cross-account seaux	Pris en charge	—
Cross-account Clés KMS	Non pris en charge	—
Règles de cycle de vie	Pris en charge	—
CloudTrail événements liés aux données	Pris en charge	—

Enable AWS Transformation

Pour activer AWS Transform :

1. Connectez-vous à la console AWS de gestion.

2. Dans la barre de recherche en haut de la console, recherchez AWS Transform.
3. Sélectionnez AWS Transformer dans les résultats de recherche.
4. Choisissez Commencer pour activer le service dans votre région actuelle.
5. Facultatif : configurez IAM Identity Center. Vous pourrez également choisir de faire appel à un fournisseur d'identité tiers (IdP) ultérieurement.
6. Sélectionnez une clé de chiffrement : clé AWS gérée par défaut ou Personnalisez les paramètres de chiffrement.

7. Facultatif : utilisez votre propre compartiment Amazon S3. Par défaut, AWS Transform utilise un compartiment Amazon S3 géré par un service pour stocker les artefacts de transformation. Vous pouvez choisir d'utiliser votre propre seau à la place. Pour de plus amples informations, veuillez consulter Utilisation de votre propre compartiment Amazon S3.
8. Choisissez les fonctionnalités de AWS transformation que vous souhaitez activer :
   - Interface de ligne de commande (CLI), nécessaire pour créer et exécuter des transformations personnalisées. Pour activer la CLI, consultez et suivez les instructions de téléchargement.
   - Application Web, l'interface utilisateur agentique pour la modernisation. Choisissez Activer l'application Web pour l'utiliser.
9. Choisissez Activer la AWS transformation.
10. Facultatif : choisissez Activer l'affichage du profil pour accéder aux onglets AWS Transformer les utilisateurs , les paramètres et les connecteurs, ou Gérer les utilisateurs pour gérer les utilisateurs.

    Vous pouvez accéder aux onglets Utilisateurs , Paramètres et Connecteurs à tout moment en choisissant l'icône de menu dans le coin supérieur gauche de la console.
11. Configurez l'accès utilisateur en choisissant l'une des options suivantes :
    - IAM Identity Center
    - Un fournisseur d'identité tiers (IdP)
    - IAM-only accès

    > **Note**
    >
    > Ce choix est finalisé et ne peut pas être modifié lorsque vous activez AWS Transform.
12. Choisissez Activer l'application Web.
13. Le système affiche « Enabling AWS Transform » pendant qu'il crée les ressources nécessaires.

Une fois AWS Transform activé, l'onglet Paramètres affiche les informations suivantes :

- URL de l'application Web : URL permettant d'accéder à l'application Web AWS Transform
- URL de démarrage pour l'IDE : URL permettant d'accéder à AWS Transform dans les environnements de développement intégrés

- Région : AWS région dans laquelle AWS Transform est activé

Démarrage rapide : Essayer AWS Transformation

Le moyen le plus simple d'essayer AWS Transform est d'utiliser un AWS compte autonome. Vous souhaiterez peut-être le faire à titre de preuve de concept ou pour des environnements de test. Utilisez cette procédure :

1. Connectez-vous à la console AWS de gestion.
2. Accédez au service AWS Transform.
3. Choisissez Commencer pour activer le service.
4. Sélectionnez et configurez votre fournisseur d'identité.
5. Attribuez des utilisateurs au service AWS Transform.
6. Une fois le service activé, l'URL de l'application Web AWS Transform s'affiche.
7. Ouvrez cette URL dans une nouvelle fenêtre de navigateur pour accéder à l'expérience Web AWS Transform.

Vous êtes maintenant prêt à configurer votre espace de travail.

Gestion des utilisateurs

La façon dont vous gérez l'accès des utilisateurs à AWS Transform dépend du modèle d'accès que vous avez choisi lors de la configuration. Si vous avez configuré IAM Identity Center, vous ajoutez des utilisateurs via IAM Identity Center. Si vous avez configuré un fournisseur d'identité tiers, vous gérez les utilisateurs de ce fournisseur. Si vous avez choisi IAM-only l'accès, l'accès des utilisateurs est géré par le biais de politiques IAM.

Ajouter des utilisateurs dans IAM Identity Center

Pour ajouter des utilisateurs dans IAM Identity Center, procédez comme suit :

1. Accédez à la console IAM Identity Center.
2. Dans le panneau de navigation, choisissez utilisateurs.
3. Sélectionnez Ajouter un utilisateur.
4. Entrez les informations requises :

- Nom d'utilisateur : identifiant unique pour l'utilisateur (ne peut pas être modifié ultérieurement)
- Adresse e-mail : adresse e-mail de l'utilisateur
- Prénom et nom de famille - Le nom de l'utilisateur
- Nom d'affichage : nom qui apparaît dans la liste des utilisateurs

5. Pour Mot de passe, choisissez la manière dont l'utilisateur reçoit son mot de passe :
   - Envoyer un e-mail - Envoyer les instructions de configuration par e-mail
   - Générer un mot de passe à usage unique - Créez un mot de passe à partager manuellement
6. Cliquez sur Suivant pour consulter les informations utilisateur.
7. Vérifiez les détails et choisissez Ajouter un utilisateur.

Une fois l'utilisateur ajouté, il reçoit un e-mail l'invitant à configurer son compte IAM Identity Center. Le lien d'invitation est valide pendant 7 jours.

Vous pouvez également découvrir comment travailler avec IAM Identity Center et AWS Transform dans cette vidéo :

VideoTitle

Ajouter des utilisateurs à AWS Transformation

Après avoir ajouté des utilisateurs à IAM Identity Center, vous pouvez leur accorder l'accès à AWS Transform :

1. Revenez à la console AWS Transform.
2. Dans le volet de navigation, choisissez Utilisateurs et groupes.
3. Sélectionnez l'onglet Utilisateurs ou l'onglet Groupes.
4. Recherchez et sélectionnez les utilisateurs ou les groupes que vous souhaitez ajouter depuis IAM Identity Center.
5. Choisissez Attribuer des utilisateurs et des groupes pour autoriser les utilisateurs ou les groupes sélectionnés à accéder à AWS Transform.

Après avoir ajouté des utilisateurs, ceux-ci apparaissent dans la liste des utilisateurs avec le statut « En attente » jusqu'à ce qu'ils acceptent l'invitation et se connectent.

Gestion des utilisateurs ayant IAM-only accès

Si vous avez configuré AWS Transform avec IAM-only accès, l'accès des utilisateurs est géré par le biais de politiques IAM. Tout responsable IAM disposant de l'`transform:AccessTransformProfile`autorisation sur la ressource de profil peut accéder à AWS Transform.

Pour accorder à un utilisateur ou à un rôle l'accès à AWS Transform :

1. Accédez à la console IAM.
2. Joignez une politique qui inclut l'`transform:AccessTransformProfile`action à l'utilisateur ou au rôle IAM. Pour un exemple de politique, voir Autoriser les utilisateurs à accéder à AWS Transform avec des informations d'identification IAM.

Pour révoquer l'accès, supprimez la politique de l'utilisateur ou du rôle IAM.

Comprendre les autorisations des collaborateurs

AWS Transform utilise un modèle d'autorisation basé sur l'espace de travail pour contrôler l'accès aux ressources et aux actions. Chaque utilisateur se voit attribuer un rôle spécifique dans un espace de travail, qui détermine les actions qu'il peut effectuer. Un utilisateur peut avoir différents rôles dans différents espaces de travail.

Rôles utilisateurs

AWS Transform prend en charge cinq rôles d'utilisateur dans chaque espace de travail. Ces rôles s'appliquent dans le contexte d'un espace de travail, et un utilisateur se verra attribuer des rôles dans chaque espace de travail dont il est membre. Les autorisations d'accès définies pour chaque rôle sont indépendantes de l'espace de travail, de sorte que l'utilisateur A avec le rôle Administrateur dans l'espace de travail A dispose des mêmes autorisations que l'utilisateur B avec le rôle Administrateur dans l'espace de travail B.

Autorisations du rôle

Autorisations détaillées pour chaque rôle :

Action	ResourceType	Admin	Approbateur	Participant	ReadOnly
Créer	Espace de travail	✓	✓	✓	✓
List	Espace de travail	✓	✓	✓	✓
Get	Espace de travail	✓	✓	✓	✓
Mettre à jour	Espace de travail	✓	✗	✗	✗
Suppression	Espace de travail	✓	✗	✗	✗
Créer	ChatMessage	✓	✓	✓	✗
Lecture	ChatMessage	✓	✓	✓	✓
Créer	RoleAssociation	✓	✗	✗	✗
Lecture	RoleAssociation	✓	✓	✓	✓
Mettre à jour	RoleAssociation	✓	✗	✗	✗
Suppression	RoleAssociation	✓	✗	✗	✗
Lecture	Tâche CriticalHitl	✓	✓	✓	✓
Mettre à jour	Tâche CriticalHitl	✓	✓	✗	✗
Suppression	Tâche CriticalHitl	✓	✓	✗	✗
Lecture	Appuyez sur Tâche	✓	✓	✓	✓

Action	ResourceType	Admin	Approbateur	Participant	ReadOnly
Mettre à jour	Appuyez sur Tâche	✓	✓	✓	✗
Suppression	Appuyez sur Tâche	✓	✓	✓	✗
Créer	Tâche	✓	✓	✓	✗
Lecture	Tâche	✓	✓	✓	✓
Mettre à jour	Tâche	✓	✓	✓	✗
Suppression	Tâche	✓	✓	✓	✗
Lecture	Worklog	✓	✓	✓	✓
Créer	Artefact	✓	✓	✓	✗
Lecture	Artefact	✓	✓	✓	✓
Mettre à jour	Artefact	✓	✓	✓	✗
Suppression	Artefact	✓	✓	✓	✗
Créer	Connecteur	✓	✓	✓	✗
Lecture	Connecteur	✓	✓	✓	✓
Mettre à jour	Connecteur	✓	✓	✓	✗
Suppression	Connecteur	✓	✓	✓	✗

Human-in-the-loop Actions (HITL)

AWS Transform propose deux types d'actions HITL : standard et critique :

Actions HITL standard

Il s'agit d'actions de routine qui peuvent être effectuées par des utilisateurs dotés des rôles de contributeur, d'approbateur ou d'administrateur.

Actions HITL critiques

Ces actions ont un impact significatif et nécessitent donc des niveaux d'autorisation plus élevés. En voici quelques exemples :

- Fusion du code avec les branches principales
- Exécution d'une décomposition graphique
- Déploiement de code dans des environnements de production

Les actions HITL critiques ne peuvent être effectuées que par des utilisateurs ayant des rôles d'approbateur ou d'administrateur.

Pour garantir une différenciation entre les actions HITL standard et les actions HITL critiques dans les politiques AuthZ, AWS Transform fournit deux API HITL distinctes, l'une pour effectuer une action HITL standard et l'autre pour effectuer une action HITL critique.

AWS Transformez l'environnement

AWS Transform est un service d'agence qui utilise le traitement du langage naturel pour vous aider à planifier et à exécuter les transformations de votre charge de travail. Vous interagissez avec AWS Transform principalement par le biais d'une interface conversationnelle, dans laquelle le service s'adapte et répond en fonction du contexte de votre discussion. Par exemple, vous pouvez commencer par décrire votre architecture actuelle et vos objectifs de transformation dans un langage courant, par exemple « Je dois migrer mes machines virtuelles sur site vers EC2 ».

Lorsque vous discutez avec AWS Transform, le service élabore un plan de travail personnalisé adapté à vos besoins spécifiques. Le flux de conversation est dynamique et piloté par vous, ce qui vous permet d'affiner votre plan de transformation de manière itérative. Vous pouvez modifier le plan de travail au cours de la conversation en faisant des demandes telles que « ajouter une phase de

test avant la mise en production » ou « supprimer l'étape de sauvegarde car nous avons déjà une solution ». Vous pouvez également revenir à une tâche précédente et l'exécuter de nouveau. AWS Transform met continuellement à jour le plan en fonction de vos commentaires, en veillant à ce que la stratégie de transformation finale réponde à vos besoins techniques et commerciaux.

Voici ce que vous voyez lorsque vous ouvrez AWS Transform.

- Afficher le volet de configuration : il s'agit du volet étroit situé à gauche de AWS Transform. Vous pouvez choisir l'une des icônes pour choisir la vue qui s'affiche à droite du panneau de configuration de l'affichage. Passez la souris sur chaque icône pour afficher une info-bulle expliquant la vue. Les cinq vues standard, de haut en bas, sont les suivantes :
  - Plan d'emploi
  - Tableau de bord
  - Agréments
  - Artefacts
  - Carnet de travail

  Certains flux de travail fournissent des vues supplémentaires.

  Lorsque vous travaillez sur un plan d'emploi, les points de vue sont les suivants :
  - Chat
  - Agréments
  - Boutique d'artefacts
  - Carnet de travail

  Lorsque vous êtes dans un espace de travail, les vues sont affichées en haut :
  - Tâches
  - Artefacts
  - Collaborateurs (utilisateurs)
  - Connecteurs
  - Paramètres
- Le volet Affichage se trouve à côté des commandes d'affichage.
- Le volet Chat se trouve au centre. C'est ici que vous menez votre conversation avec AWS Transform.

> **Note**
>
> Les utilisateurs disposant d'autorisations de lecture seule ne peuvent pas envoyer de messages dans le chat.

- À droite se trouve le volet Collaboration. Cela apparaît lorsque des activités HITL (human in the loop) sont effectuées, telles que :
  - Téléchargement de fichiers de données
  - Révision des informations et des plans fournis par AWS Transform

Paramètres de langue

AWS Transform prend en charge la localisation pour certains flux de travail. Vous pouvez modifier la langue d'affichage de l'application Web en choisissant l'icône Paramètres dans le coin supérieur droit et en sélectionnant la langue de votre choix dans le menu Langue.

Les langues suivantes sont prises en charge :

- Anglais (États-Unis)
- Anglais (Royaume-Uni)
- Deutsch (allemand)
- Espanol (espagnol)
- English (Français)
- (japonais)
- Bahasa Indonesia (indonésien)
- Italiano (italien)
- Português (Portugais)
- (coréen)
- () ((chinois simplifié)
- () (Chinois traditionnel)
- Türkçe (Turc)

Les flux de travail suivants prennent en charge la localisation :

- Migrations (y compris VMware)

> **Note**
>
> Les autres flux de travail AWS Transform sont actuellement disponibles en anglais uniquement. La prise en charge de la localisation pour des flux de travail supplémentaires pourrait être ajoutée dans les prochaines mises à jour.

Démarrez votre projet

AWS Transform vous accompagne dans vos projets de modernisation et de migration. Mise en route :

1. Créez un espace de travail pour héberger votre projet. Sur la page Espaces de travail, choisissez Créer un espace de travail. Suivez les instructions, puis ouvrez l'espace de travail.
2. Dans le volet Chat, tapez « créer une tâche »
3. Choisissez une tâche et suivez les instructions fournies par AWS Transform. Si votre saisie est requise, le volet Collaboration apparaît et explique ce qui est requis.

Flexibilité du workflow

L'environnement de flux de travail AWS Transform offre une certaine flexibilité dans la progression de vos projets de modernisation. En utilisant le langage naturel dans le volet de discussion, vous pouvez :

- Réessayez une tâche que AWS Transform a déjà effectuée, en fournissant différentes entrées humaines en cours de route.
- Réexécutez une tâche, par exemple, si des modifications ont été apportées à vos sources de modernisation.

Discuter avec AWS Transformation

AWS Le chat Transform est disponible à chaque étape de votre projet. Pour ouvrir le chat, cliquez sur l'icône hexagonale violette dans le coin inférieur droit de la console Web.

Le chat est là pour que tu puisses demander quoi que ce soit. Par exemple, vous pouvez demander au chat d'expliquer des concepts, de vous guider tout au long d'un processus, d'expliquer une demande ou une réponse de AWS Transform, ou d'expliquer un rapport AWS Transform.

> **Note**
>
> Les utilisateurs disposant d'autorisations de lecture seule ne peuvent pas envoyer de messages dans le chat.

AWS Transformez les intégrations de chat

AWS Transform chat est intégré à :

Experience-Based Accélération

Experience-BasedL'accélération (EBA) est proposée via le chat AWS Transform. Il vous permet d'effectuer une évaluation EBA pour les charges de travail Windows et de générer un plan. Vous pouvez commencer par importer les résultats de l'évaluation depuis CAST. Il vous aide à découvrir votre portefeuille d'applications, après quoi vous pouvez utiliser le chat AWS Transform pour sélectionner les applications qui répondent aux besoins de votre entreprise (par exemple, le filtrage des applications en fonction de leur complexité ou de lignes de code). Vous pouvez ensuite effectuer une évaluation plus approfondie de l'application sélectionnée et générer un plan de modernisation.

AWS Compte à rebours Premium

AWS Countdown Premium (CDP) intégré à AWS Transform fournit des conseils d'experts soutenus avec un support AWS technique désigné. Votre ingénieur CDP désigné explore en profondeur votre infrastructure technologique et fournit une assistance personnalisée et contextuelle en cas de problème. Les utilisateurs peuvent utiliser AWS Transform pour enregistrer un ticket d'assistance directement depuis son interface de chat. Le ticket d'assistance intègre les détails du carnet de travail et du plan de travail pour aider le support à comprendre le contexte du client. Si un client ou un partenaire fait partie du programme CDP, le ticket d'assistance est automatiquement acheminé vers l'ingénieur CDP désigné qui peut aider à déboguer les problèmes, à interpréter les résultats des transformations et à faire avancer les choses pour accélérer la résolution des problèmes. Par exemple :

- Pour les charges de travail .NET, le CDP peut vous aider à résoudre les problèmes liés aux connecteurs de référentiel, à résoudre les dépendances et à les déployer après la transformation.

- Dans les scénarios de mainframe, le CDP peut vous aider à résoudre les problèmes liés au code Java remanié, à configurer les outils de migration de bases de données et à créer des pipelines. CI/CD
- Dans les migrations vers VMware, le CDP peut accélérer la configuration du réseau, la configuration MGN et l'installation des agents.

AWS Générateur de compétences

AWS Skill Builder propose des modules d'apprentissage pertinents via le chat. Vous pouvez demander à AWS Transform chat quels sont vos besoins en matière d'apprentissage, et il vous présentera un catalogue de cours pertinent. Skill Builder propose des expériences de micro-apprentissage contextuelles au fur et à mesure que vous franchissez les étapes de transformation.

AWS Connecteurs Transform

AWS Les connecteurs Transform vous permettent d'accéder en toute sécurité aux ressources au-delà des limites de vos comptes pour les flux de migration et de modernisation. Cela vous permet d'accéder aux ressources et de les gérer au-delà des limites de votre compte tout en maintenant les contrôles de sécurité et les autorisations. Un connecteur représente une connexion entre votre compte AWS Transform-enabled source et des ressources externes dans des comptes AWS cibles ou dans des systèmes tiers.

Les connecteurs nécessitent des demandes d'accès depuis le connecteur source et l'approbation du propriétaire du compte cible. Vous faites cette demande lorsque vous configurez un connecteur source. De même, vous pouvez recevoir des demandes d'approbation des connecteurs de destination afin de permettre à d'autres comptes d'accéder à votre compte.

- Création de connecteurs : créez des connecteurs dans votre compte AWS Transform-enabled source, en spécifiant le compte cible et les autorisations requises
- Configuration des autorisations : AWS Transform nécessite des rôles et des autorisations IAM spécifiques sur le compte de destination pour effectuer des actions de migration, notamment :
  - Gestion des données de migration avec AWS KMS
  - Effectuer des appels d'API interrégionaux
  - Installation d'agents de réplication sur des serveurs VMware
  - Création d'une infrastructure réseau (VPC, sous-réseaux, routage)
  - Lancement d'instances Amazon EC2 et déploiement de piles CloudFormation

  - Exécution des flux de migration via Migration Hub
- Processus d'approbation : vous devez approuver les demandes de connecteur de destination AWS pour que Transform puisse accéder à vos ressources.
- Connexion active : une fois que vous avez approuvé un connecteur, il permet à AWS Transform jobs d'accéder aux ressources du compte cible et de les gérer en toute sécurité.

Traçabilité des utilisateurs pour les opérations des agences

Par défaut, AWS CloudTrail enregistre les actions des agents sur vos AWS ressources sous l'identité du service AWS Transform. La traçabilité des utilisateurs attribue ces actions à l'utilisateur AWS IAM Identity Center qui a initié la tâche ou qui a interagi avec elle, ce qui permet un audit de sécurité et une enquête sur les incidents au niveau de chaque utilisateur.

> **Note**
>
> La traçabilité des utilisateurs est prise en charge uniquement pour les utilisateurs d'IAM Identity Center (IDC).

Pour activer la traçabilité des utilisateurs, activez la session en arrière-plan dans les paramètres de votre profil AWS Transform. Lorsque cette option est activée, AWS Transform crée automatiquement une session d'arrière-plan IAM Identity Center lorsque vous interagissez avec une tâche et l'utilise pour créer des sessions de rôles IAM à identité améliorée pour les opérations du connecteur. Ces sessions intègrent votre identité d'utilisateur dans les appels de AWS service et les AWS CloudTrail événements en aval. Lorsque les sessions en arrière-plan sont désactivées, AWS Transform revient aux sessions standard avec rôle assumé sans contexte d'identité utilisateur.

Les nouveaux connecteurs sont automatiquement configurés pour permettre la traçabilité des utilisateurs. Pour les connecteurs existants, vous devez ajouter manuellement `sts:SetContext` à la politique de confiance du rôle de connecteur :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": ["transform.amazonaws.com"] },
      "Action": ["sts:AssumeRole", "sts:SetContext"],
```

```
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "your-account-id" }
      }
    }
  ]
}
```

Vous pouvez consulter et révoquer vos sessions d'arrière-plan actives à partir de l'onglet Sessions d'arrière-plan de la page des tâches. La révocation d'une session l'invalide immédiatement, ainsi que toutes les sessions de connecteur qui en découlent.

Pour plus d'informations, consultez la section Présentation de la propagation d'identité sécurisée dans le Guide de l'utilisateur d'AWS IAM Identity Center.

Gestion des connecteurs

Sur la page Connecteurs, vous pouvez voir les éléments suivants :

- Onglet Connecteurs source : répertorie tous les connecteurs que vous avez créés pour vous connecter à d'autres comptes, en indiquant les comptes cibles et l'état du connecteur
- Onglet Connecteurs de destination : affiche les demandes de connecteur entrantes provenant d'autres comptes souhaitant accéder à vos ressources et nécessitant votre approbation ou votre rejet

AWS Transform nécessite une confirmation pour les actions critiques telles que l'approbation, le rejet ou la suppression de connecteurs, afin d'éviter des modifications accidentelles susceptibles de perturber vos flux de migration actifs.

Pour créer un connecteur

1. Accédez à l'onglet Connecteurs source.
2. Spécifiez le compte cible et le type de ressource.
3. Configurez les autorisations et l'étendue d'accès requises.

Pour configurer les autorisations

1. Choisissez de créer un nouveau rôle IAM avec les autorisations requises, ou
2. Sélectionnez un rôle existant que vous avez créé précédemment pour les connecteurs.

3. Assurez-vous que le rôle dispose de toutes les autorisations nécessaires pour les opérations de AWS transformation.

Pour gérer les demandes entrantes

1. Consultez les demandes de connecteur dans l'onglet Connecteurs de destination.
2. Approuvez les demandes légitimes pour permettre l'accès entre comptes.
3. Rejetez les tentatives de connexion non autorisées ou inutiles.

Pour gérer vos connecteurs

1. Surveillez la sécurité et la conformité de vos connecteurs actifs.
2. Supprimez les connecteurs lorsque vous n'en avez plus besoin. Notez que cela entraînera l'échec des tâches en cours d'exécution utilisant le connecteur.
3. Mettez à jour les autorisations en fonction de l'évolution de vos besoins.

Outils pour développeurs

Vous pouvez accéder aux agents AWS Transform à partir des IDE d'agence, des plug-ins d'agent et du serveur MCP. Choisissez la surface qui convient à votre flux de travail.

> **Note**
>
> Les plugins Kiro Power et agent installent automatiquement le serveur MCP. Vous n'avez besoin d'installer le serveur MCP manuellement que si vous souhaitez l'utiliser sans Kiro Power ni plug-in d'agent.

Kiro Power

Le AWS Transform Kiro Power fournit un accès complet aux agents AWS Transform depuis l'IDE Kiro.

Pour installer la AWS Transformez Kiro Power

1. Ouvrez Kiro IDE et accédez au panneau Powers.
2. Recherchez AWS Transform dans la liste et installez-le.
3. Ouvrez Kiro Chat, cliquez sur Power, puis sélectionnez Try Power.

Sinon, dans le panneau Pouvoirs, choisissez Ajouter une alimentation personnalisée > Importer de l'énergie depuis GitHub et collez : `https://github.com/kirodotdev/powers/tree/main/aws-transform`

Plug-in d'agent

Le plug-in de l'agent AWS Transform est disponible à l'awslabs/agentadresse -plugins on GitHub, dans le `plugins/aws-transform` répertoire. Le plugin prend en charge Claude Code, Codex et Cursor.

Le plugin inclut `.claude-plugin.codex-plugin`, et les `.mcp.json` configurations. Il donne accès à tous les agents de AWS transformation, tels que .NET, mainframe, VMware, SQL Server et aux transformations personnalisées.

Pour installer dans Claude Code

Exécutez les commandes suivantes :

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

Pour installer dans Codex ou Cursor

Suivez les instructions du README du référentiel agent-plugins.

Plug-in IDE

Le plugin AWS Transform IDE est disponible sur les éditeurs compatibles VS Code et Open VSX. Il présente les fonctionnalités personnalisées de AWS Transform, notamment la création et l'exécution de définitions de transformation. Il présente également les fonctionnalités du mainframe, notamment la traçabilité entre les exigences de modernisation, les règles métier et le code source, ainsi que la possibilité de générer de la documentation technique à la demande. Pour commencer, procédez à l'installation à l'aide de l'une des méthodes suivantes :

- VS Code : installez depuis VS Code Marketplace.
- Ouvrez VSX : installez à partir du registre Open VSX.

Serveur MCP

Utilisez le serveur MCP pour intégrer AWS Transform par programmation à n'importe quel client. MCP-compatible Vous pouvez installer le serveur MCP à partir de PyPI en tant que. `awslabs.aws-transform-mcp-server` Il fournit 19 outils pour la gestion de l'espace de travail, la gestion des tâches, les tâches HITL (human in-the-loop), la gestion des artefacts, la gestion des connecteurs, le chat et la navigation dans les ressources.

Conditions préalables

- Python 3.10 ou version ultérieure

Installation

Claude Code

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

Kiro

Ajouter à `~/.kiro/settings/mcp.json` :

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

Pour plus de détails sur la configuration de votre client MCP spécifique, consultez le fichier README du serveur https://github.com/awslabs/mcp/tree/main/src/aws-transform-mcp-server aws-transform-mcp-server sur. GitHub

Authentification

AWS Transform prend en charge l'authentification SSO (Gestion des identités et des accès AWS Identity Center) et l'authentification basée sur les rôles IAM.

SSO (Centre d'identité IAM)

Demandez à votre assistant IA de « configurer AWS Transform avec SSO ». L'assistant fournit une URL de démarrage et ouvre votre navigateur pour vous connecter.

Rôle IAM

Votre environnement fournit automatiquement des AWS informations d'identification. Définissez `AWS_PROFILE` dans le `env` bloc de configuration de votre client MCP pour sélectionner un profil spécifique.

Pour plus d'informations sur la configuration de l'authentification pour AWS Transform, consultezDémarrage avec AWS Transformation.

Créez des agents personnalisés pour AWS Transformation

La boîte à outils de création d'agents permet aux AWS partenaires et aux clients de créer des agents adaptés à leurs besoins de modernisation spécifiques qui fonctionnent au sein de AWS Transform.

Pour installer la boîte à outils de création d'agents

1. Ouvrez Kiro IDE et accédez au panneau Powers.
2. Recherchez AWS Transform Agent Toolkit dans la liste et installez-le.

Sinon, dans le panneau Pouvoirs, choisissez Ajouter une alimentation personnalisée > Importer de l'énergie depuis GitHub et collez : `https://github.com/kirodotdev/powers/tree/main/aws-transform-agent-toolkit`

La boîte à outils de création d'agents permet aux partenaires compétents en matière de migration et de modernisation, aux ISV ou aux clients de créer des solutions de transformation pour des cas d'utilisation spécifiques. Vous pouvez intégrer des agents, des outils, des bases de connaissances et des flux de travail spécialisés grâce aux fonctionnalités d'IA agentic de AWS Transform.

Cycle de vie des agents

Génération

Utilisez le Kiro Power pour combiner l'agent de base et le SDK afin de créer votre propre agent personnalisé.

Partager

Répartissez les agents au sein des équipes ou entre les réseaux de partenaires.

Enregistrement

Enregistrez des agents auprès de AWS Transform pour qu'ils soient découverts par d'autres utilisateurs.

Personnalisé

Qu'est-ce que AWS Transformer la personnalisation ?

AWS Transform Custom utilise l'IA agentique pour moderniser à grande échelle les logiciels, le code, les bibliothèques et les frameworks afin de réduire la dette technique. Il gère divers scénarios, notamment les mises à niveau des versions linguistiques, les migrations d'API et de services, les mises à niveau et les migrations du framework, la refactorisation du code et les transformations spécifiques à l'organisation.

Grâce à un apprentissage continu, l'agent s'améliore grâce à chaque exécution et aux commentaires des développeurs, fournissant des transformations reproductibles de haute qualité sans avoir besoin d'une expertise spécialisée en automatisation.

Capacités clés

AWS Transform Custom fournit les fonctionnalités suivantes :

- Définition de la transformation basée sur le langage naturel - Créez des transformations personnalisées à l'aide du langage naturel, de la documentation et d'exemples de code
- Exécution des transformations : appliquez des transformations de manière cohérente et fiable sur plusieurs bases de code
- Apprentissage continu : améliorez automatiquement la qualité de la transformation à chaque exécution
- AWS-transformations gérées - Utilisez des transformations prêtes à l'emploi et AWS approuvées pour les scénarios courants

Schémas de transformation

AWS Transform Custom prend en charge divers modèles de transformation pour répondre à vos besoins de modernisation. Chaque modèle présente des caractéristiques de complexité différentes en fonction de la portée et de la nature des modifications requises.

Modèle	Description	Complexité	Exemples
Migrations d'API et de services	Migration entre les versions d'API ou des services équivalents tout en préservant les fonctionnalités	Moyenne	AWS SDK v1→v2 (Java, Python,), Boto2→Boto3, JUnit JavaScript 4→5, Javax→Jakarta
Mises à niveau des versions linguistiques	Mise à niveau vers de nouvelles versions du même langage de programma tion, adoption de nouvelles fonctionn alités et remplacem ent des fonctionnalités obsolètes	Low-Medium	Java 8→17, Python 3.9→3.13, 12→22, mises à niveau de version Node.js TypeScript
Améliorations du framework	Mise à niveau vers des versions plus récentes du même framework, en tenant compte des modificat ions majeures	Moyenne	Spring Boot 2.x → 3.x, React 17→18, mises à niveau Angular, mises à niveau Django
Migrations de cadres	Migration vers des frameworks totalemen t différents ayant des objectifs similaires	Élevée	Angular→React, Redux→Zustand, →React Vue.js
Mises à niveau des bibliothèques et des dépendances	Mise à niveau de bibliothèques tierces vers des versions plus récentes tout en conservant le même langage et le même framework	Low-Medium	Pandas 1.x → 2.x, mises à niveau, mises à niveau de la bibliothèque, NumPy Hadoop/HBase/Hive mises à niveau de Lodash

Modèle	Description	Complexité	Exemples
Refactorisation du code et modernisation des modèles	Moderniser les modèles de code et adopter les meilleures pratiques sans modifier les fonctionnalités externes	Low-Medium	Frameworks Print→Logging, concaténation de chaînes→chaînes f, adoption d'indices de type, instrumentation d'observabilité
Script et File-by-File traductions	Traduction de scripts indépendants ou de fichiers de configuration dont les fichiers sont pour la plupart autonomes	Low-Medium	AWS CDK→Terraform, Terraform →, Excel→Carnets Python, CloudFormation Bash→ PowerShell
Migrations architecturales	Migration entre des architectures matérielles ou des environnements d'exécution avec un minimum de modifications de code	Medium-High	x86 →AWS Graviton (ARM), sur site → Lambda, serveur traditionnel → conteneurs
Language-to-Language Migrations	Traduire des bases de code d'un langage de programmation à un autre	Très élevé	Java→Python, →, C→Rust, JavaScript TypeScript Python→Go
Personnalisation et Organization-Specific transformations	Des exigences organisationnelles uniques et des besoins de modernisation spécialisés	Varie	Migrations de bibliothèques internes personnalisées, normes de codage spécifiques à l'organisation, migrations de frameworks propriétaires

> **Note**
>
> Pour les COBOL/mainframe langues, utilisez AWS Transform for Mainframe. Pour les mises à niveau de .NET Framework vers .NET Core, pensez à AWS Transform pour Windows. Pour les migrations vers VMware AWS, pensez à AWS Transform for VMware.

Comment ? AWS Transformez des œuvres personnalisées

AWS La transformation personnalisée est généralement utilisée dans les projets à grande échelle dans lesquels plusieurs bases de code ou modules sont transformés. Les équipes suivent généralement un flux de travail en quatre phases :

Définir la transformation : fournissez des instructions en langage naturel, de la documentation et des exemples de code à l'agent, qui génère une définition initiale de la transformation. Cette définition peut être affinée de manière itérative par le biais du chat ou de modifications directes. Cette phase peut être ignorée lors de l'utilisation de transformations AWS gérées par -managed.

Pilote ou Proof-of-Concept : testez la transformation sur des exemples de bases de code et affinez-la en fonction des résultats. Cette phase de validation permet d'estimer le coût et les efforts de la transformation complète. L'apprentissage continu améliore la qualité au cours de cette phase.

Exécution échelonnée : configurez l'exécution groupée automatisée à l'aide de l'interface de ligne de commande, les développeurs examinant et validant les résultats. Surveillez les progrès à l'aide de l'application Web et suivez les transformations dans plusieurs référentiels.

Surveillance et révision : l'apprentissage continu améliore automatiquement la qualité de la transformation. Passez en revue les leçons tirées des séries précédentes pour vous assurer qu'elles répondent aux normes de qualité, et archivez celles qui ne sont pas utiles.

Comprendre les concepts clés

Cette section explique les concepts clés relatifs à l'utilisation de AWS Transform custom.

Définitions des transformations

Une définition de transformation contient les instructions et les connaissances nécessaires pour effectuer une transformation de code spécifique. Elle est représentée comme une compétence et comprend :

- `SKILL.md`(obligatoire) - Instructions en Markdown avec une interface YAML (`name`et des `description` champs) contenant la logique de transformation de base et les instructions d'exécution
- `references/`dossier (facultatif) - Documentation chargée selon les besoins lors de l'exécution de la transformation
- `scripts/`dossier (facultatif) - Scripts que la transformation télécharge et exécute pendant l'exécution

AWS Transform CLI télécharge automatiquement les définitions de transformation dans le répertoire actuel lorsque cela est nécessaire pour l'exécution, l'inspection ou la modification.

> **Important**
>
> Lors de la publication d'une transformation, le répertoire doit contenir uniquement `SKILL.md` et éventuellement le `references/` dossier, le `scripts/` dossier ou les deux. Aucun autre fichier ou sous-répertoire n'est autorisé.

> **Note**
>
> Les versions 2.0 et ultérieures de la CLI utilisent le format de compétences. Les définitions de transformation existantes sont automatiquement gérées par l'interface de ligne de commande.

Registre des transformations

Le registre des transformations est le référentiel centralisé de votre AWS compte pour le stockage et la gestion des définitions de transformation. Les transformations dans le registre peuvent être les suivantes :

- Listé en utilisant `atx custom def list`
- Exécuté sur plusieurs bases de code
- Partagé avec d'autres utilisateurs de votre AWS compte
- Version-controlled

> **Important**
>
> Les définitions de transformation sont spécifiques au compte. Si vous souhaitez utiliser une transformation dans un autre AWS compte, vous devez la publier séparément dans ce compte.

Transformations provisoires et transformations publiées

AWS Transform custom prend en charge deux états pour les transformations dans le registre :

Les projets de transformation sont des définitions de transformation en cours ou non testées. Ils sont enregistrés en tant que versions spécifiques et peuvent être récupérés, mis à jour et exécutés par les utilisateurs se référant à cette version spécifique. Les brouillons sont utiles pour le développement itératif, les tests et le raffinement avant que la transformation ne soit prête à être partagée avec votre équipe. Les brouillons sont également associés à une conversation spécifique. Si vous redémarrez la CLI, vous pouvez l'utiliser `atx --conversation-id {id}` pour restaurer une précédente.

Les transformations publiées sont disponibles dans le registre des transformations de votre compte pour être exécutées par d'autres utilisateurs disposant des autorisations IAM requises. Les transformations publiées peuvent être découvertes à l'aide de`atx custom def list`.

Le flux de travail typique est le suivant :

1. Créez une transformation au niveau local
2. Enregistrer en tant que brouillon pour les tests (`atx custom def save-draft`)
3. Affiner et valider
4. Publiez pour partager avec votre équipe (`atx custom def publish`)

Vous pouvez également publier une transformation directement sans l'enregistrer en tant que brouillon.

Références et leçons

AWS Transform Custom utilise deux types de connaissances pour améliorer la qualité de la transformation :

Les références sont de la documentation fournie par l'utilisateur et stockée dans le `references/` dossier d'une définition de transformation. Les références ne prennent en charge que les

fichiers texte (maximum 10 Mo au total pour tous les fichiers) et contiennent généralement de la documentation, des spécifications d'API, des guides de migration et des exemples de code. Les références sont chargées selon les besoins lors de l'exécution de la transformation. Vous ajoutez des références lors de la création ou de la mise à jour d'une définition de transformation en mode interactif.

Les leçons sont automatiquement extraites des exécutions précédentes d'une transformation. Le système d'apprentissage continu les génère à partir des trajectoires d'exécution, des commentaires des développeurs et des corrections de code rencontrées lors des transformations. Il regroupe les leçons connexes en catégories afin que vous puissiez les réviser ensemble. Contrairement aux références, que vous fournissez dès le départ, les leçons s'accumulent au fil du temps au fur et à mesure que vous exécutez la transformation sur différentes bases de code, et le système les applique automatiquement pour améliorer les exécutions futures. Vous révisez et gérez les leçons de manière interactive avec`atx custom def learnings`.

Commandes de création et de validation

La commande de génération ou de validation est un paramètre facultatif qui indique comment valider votre code pendant le processus de transformation. Cette commande est exécutée à différents moments de la transformation pour garantir l'intégrité du code.

Il est très important de fournir une commande qui valide les résultats et renvoie les problèmes en cas d'échec de la validation pour améliorer la qualité de la transformation grâce à un apprentissage continu. Si aucune compilation ou validation n'est nécessaire, omettez cette information de votre saisie.

Pour obtenir des exemples et des conseils détaillés, consultez la section Commandes de création et de validation dans la section Workflows.

Apprentissage continu

L'apprentissage continu est le système qui capture automatiquement les commentaires de chaque exécution de transformation et améliore la qualité de la transformation au fil du temps. Le système recueille des informations par le biais de :

- Feedback explicite - Commentaires et corrections de code fournis en mode interactif
- Observations implicites : problèmes rencontrés par l'agent lors de la transformation et du débogage du code

Le système d'apprentissage continu traite ces informations pour créer des leçons qu'il ajoute à la définition de la transformation afin d'améliorer les transformations futures. Le système exécute automatiquement le processus d'apprentissage une fois les transformations terminées, sans aucune intervention supplémentaire de votre part.

> **Important**
>
> Les leçons sont spécifiques à la transformation et ne sont pas partagées entre différentes transformations ou différents comptes clients.

Gestion des leçons

Le système génère des leçons automatiquement, mais vous restez maître de celles qu'il applique aux prochaines courses. La `atx custom def learnings` commande ouvre une session de terminal interactive pour passer en revue et organiser les leçons qu'une transformation a accumulées.

Au cours de cette session, vous pouvez :

- Parcourez les leçons regroupées par catégories et voyez combien de leçons actives chaque catégorie contient.
- Ouvrez une leçon pour en lire tous les détails, y compris le corps de la leçon, son impact et le nombre de courses précédentes qui l'ont consultée.
- Archivez une leçon pour empêcher le système de l'appliquer à de futures exécutions, et restaurez-la ultérieurement si nécessaire.
- Supprimez définitivement une leçon archivée qui n'est plus utile.

Pour obtenir des instructions détaillées, consultez the section called “Apprentissage continu”.

Client-Side Compétences

Client-side les compétences sont des capacités supplémentaires qui étendent l'agent lors des exécutions de transformation. Contrairement aux définitions de transformation qui définissent la transformation à effectuer, les compétences côté client fournissent des outils, des scripts et des instructions supplémentaires que l'agent peut utiliser en plus de ses fonctionnalités intégrées lors de toute transformation.

Client-side les compétences sont découvertes à partir de répertoires au niveau du projet et au niveau des utilisateurs. Placez les compétences au niveau du projet lorsqu'elles appliquent des normes spécifiques à un référentiel, et au niveau de l'utilisateur lorsqu'elles s'appliquent à tous vos projets. Project-level les compétences ne sont disponibles que lorsqu'un chemin de dépôt de code est fourni. Pour une configuration et une utilisation détaillées, consultezthe section called "Client-Side Compétences".

Démarrage

Cette section explique comment configurer AWS Transform custom et exécuter votre première transformation.

Conditions préalables

Avant d'installer AWS Transform custom, assurez-vous de disposer des éléments suivants :

Plateformes prises en charge

AWS Transform Custom prend en charge les systèmes d'exploitation suivants :

- Linux - Support complet pour toutes les distributions Linux
- macOS - Support complet pour les systèmes macOS
- Windows - Prise en charge complète de Windows natif à l'aide de Windows Terminal et PowerShell (les `atx ct` commandes ne sont pas encore prises en charge sous Windows)
- Sous-système Windows pour Linux (WSL) - Supporté lors de l'exécution sous WSL

Logiciel requis

- Node.js 22 ou version ultérieure - Télécharger depuis https://nodejs.org/en/download
- Git - Doit être installé et le répertoire de travail doit être un dépôt Git valide pour exécuter une transformation. Exécutez `git init; git add .; git commit -m "Initial commit"` pour initialiser un dépôt Git dans votre répertoire de travail.

Exigences réseau

Une connexion Internet avec accès aux terminaux suivants est requise :

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

Si vous travaillez dans un environnement où Internet est restreint, mettez à jour les règles de pare-feu pour autoriser ces URL.

Installation de la AWS Transformer la CLI

La méthode d'installation recommandée consiste à utiliser le script d'installation. Choisissez l'onglet correspondant à votre système d'exploitation.

Pour installer la CLI AWS Transform

1. Exécutez le script d'installation :

   Linux and macOS

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

   Windows (PowerShell)

   Sur Windows natif, exécutez le script d'installation depuis Windows Terminal à l'aide de PowerShell.

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

2. Vérifiez l'installation :

   ```
   atx --version
   ```

   La commande doit afficher la version installée de la CLI AWS Transform.

Configuration de l'authentification

AWS Transform Custom nécessite des AWS informations d'identification pour s'authentifier auprès du service. Configurez l'authentification à l'aide de l'une des méthodes suivantes.

Variables d'environnement

Définissez les variables d'environnement suivantes.

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"
```

Vous pouvez également spécifier un profil à l'aide de la variable d'`AWS_PROFILE`environnement.

Linux and macOS

```
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

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

> **Note**
>
> Les variables d'environnement définies avec `$env:` in PowerShell s'appliquent uniquement à la session en cours. Pour les conserver d'une session à l'autre, définissez-les via Propriétés du système > Variables d'environnement, ou utilisez`[System.Environment]::SetEnvironmentVariable()`.

AWS Fichier d'informations d'identification

Configurez les AWS informations d'identification dans le fichier d'informations d'identification, situé sous Linux et macOS, ou `%USERPROFILE%\.aws\credentials` sous Windows : `~/.aws/credentials`

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

Autorisations IAM

Vos AWS informations d'identification doivent disposer des autorisations nécessaires pour appeler le service personnalisé AWS Transform. Nous vous recommandons d'associer la politique `AWSTransformCustomFullAccess` AWS gérée à votre utilisateur ou à votre rôle IAM. Cette politique fournit un accès complet à AWS Transform custom, y compris l'autorisation de créer le rôle lié au service requis pour l'émission de CloudWatch métriques sur votre compte.

Pour un contrôle plus précis, AWS Transform custom fournit également les politiques AWS gérées suivantes :

- `AWSTransformCustomExecuteTransformations`— Permet d'exécuter des transformations.
- `AWSTransformCustomManageTransformations`— Permet de créer, de mettre à jour, de lire et de supprimer des ressources de transformation, ainsi que d'exécuter des transformations.

Pour plus d'informations sur ces politiques, consultez la section Politiques AWS gérées pour AWS Transform. Pour les politiques IAM personnalisées avec des autorisations au niveau des ressources, consultez le guide de référence d'autorisation du service AWS Transform Custom IAM.

> **Note**
>
> - Les définitions de transformation sont AWS des ressources dotées d'ARN (Amazon Resource Names). Vous pouvez utiliser des politiques IAM pour contrôler l'accès à des transformations ou à des groupes de transformations spécifiques en spécifiant l'ARN de transformation dans vos instructions de ressources de stratégie IAM. Les balises peuvent être utilisées pour le contrôle d'accès groupé.

- AWS IAM Identity Center est requis pour accéder à AWS Transform, mais pas pour utiliser l'interface de ligne de commande.

Configuration AWS Région

AWS Transform custom est disponible dans des AWS régions spécifiques et détecte automatiquement la configuration de votre région à l'aide de la priorité AWS CLI standard.

Régions prises en charge

AWS Transform custom est disponible dans les AWS régions suivantes :

- `us-east-1`(États-Unis Est - Virginie du Nord)
- `eu-central-1`(Europe - Francfort)
- `eu-west-2`(Europe - Londres)
- `ca-central-1`(Canada - Centre)
- `ap-northeast-1`(Asie-Pacifique - Tokyo)
- `ap-northeast-2`(Asie-Pacifique - Séoul)
- `ap-southeast-2`(Asie-Pacifique - Sydney)
- `ap-south-1`(Asie-Pacifique - Mumbai)

Comment la région est déterminée

La CLI vérifie ces sources par ordre de priorité pour déterminer la région à utiliser :

1. `AWS_REGION`variable d'environnement (priorité la plus élevée)
2. variable d'environnement `AWS_DEFAULT_REGION`
3. Profil sélectionné dans le fichier de AWS configuration (via une variable d'`AWS_PROFILE`environnement)
4. Profil par défaut dans le fichier de AWS configuration
5. Solution de repli par défaut `us-east-1` si aucune configuration n'est trouvée

> **Note**
>
> Le fichier de AWS configuration se trouve `~/.aws/config` sur Linux et macOS, ou `%USERPROFILE%\.aws\config` sur Windows.

> **Note**
>
> Si elle `ATX_CUSTOM_ENDPOINT` est définie, la région est extraite de l'URL du point de terminaison et remplace tous les autres paramètres.

Configuration de votre région

Choisissez l'une des méthodes suivantes pour configurer votre région :

Option 1 : variable d'environnement (recommandée pour une utilisation temporaire) :

Linux and macOS

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

Windows (PowerShell)

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

Option 2 : configuration AWS CLI (recommandée pour une configuration permanente) :

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

Option 3 : Profile-specific configuration :

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"
```

Option 4 : édition directe des fichiers :

Modifiez directement le fichier de AWS configuration (`~/.aws/config`sous Linux et macOS, ou `%USERPROFILE%\.aws\config` sous Windows) :

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

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

Vérification de la configuration de votre région

Pour vérifier quelle région AWS Transform custom utilisera :

Vérifiez le réglage actuel de la région :

```
aws configure get region
```

Vérifiez les variables d'environnement :

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"
```

Afficher la résolution détaillée des régions dans les journaux de débogage :

Linux and macOS

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

Windows (PowerShell)

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

Exemple de sortie de journal indiquant la source de la région :

```
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"
}
```

Le `regionSource` champ indique d'où provient la région (par exemple, « aws-config (profile : default) », « AWS_REGION », « default »).

> **Important**
>
> Si la configuration de votre région pointe vers une région non prise en charge, l'interface de ligne de commande affiche un message d'erreur clair contenant des instructions pour mettre à jour votre configuration vers une région prise en charge.

Exécutez votre première transformation

La méthode la plus rapide pour démarrer est d'utiliser une transformation AWS gérée. AWS-les transformations gérées sont des transformations pré-construites et AWS approuvées qui sont prêtes à être utilisées sans aucune configuration.

Pour exécuter une transformation AWS gérée de manière interactive :

```
atx
```

Demandez ensuite à l'agent d'exécuter une transformation :

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

Pour exécuter une transformation de manière non interactive :

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

Pour des informations détaillées sur les modes d'exécution, les options de configuration et les indicateurs de commande, consultezthe section called “Référence de commande”.

Comprendre les résultats de la transformation

Lorsqu'une transformation est terminée, AWS Transform custom fournit un rapport décrivant les résultats. Si la transformation n'a pas été validée (par exemple, compilation réussie pour une application Java), le rapport fournit des recommandations pour d'autres actions.

La plupart des transformations sont effectuées en plusieurs étapes, en utilisant Git pour valider les transformations intermédiaires. Vous pouvez consulter les modifications apportées par la transformation à l'aide des commandes Git standard :

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

Création d'une transformation personnalisée

Lorsque les transformations AWS gérées ne répondent pas à vos besoins, vous pouvez créer des transformations personnalisées adaptées à vos besoins spécifiques.

Pour créer une transformation personnalisée

1. Démarrez la CLI AWS Transform en mode interactif :

   ```
   atx
   ```

2. Dites à l'agent que vous souhaitez créer une nouvelle transformation et décrivez vos besoins.
3. Fournissez des matériaux de référence tels que de la documentation et des exemples de code pour améliorer la qualité.

4. Testez et affinez la transformation de manière itérative.
5. Publiez-le dans le registre des transformations de votre organisation.

Pour obtenir des instructions détaillées sur la création de transformations personnalisées, consultezthe section called "Flux de travail".

AWS Transformer l'application Web (facultatif)

L'application Web AWS Transform est une interface optionnelle permettant de surveiller les campagnes de transformation à grande échelle sur plusieurs référentiels. Avant d'utiliser l'application Web AWS Transform, vous devez disposer d'une identité utilisateur activée pour accéder à AWS Transform dans votre organisation. Pour plus d'informations sur l'activation de AWS Transform, voir Configuration de AWS Transform.

Pour utiliser l'application Web AWS Transform, procédez comme suit :

1. Visitez https://aws.amazon.com/transform/ et connectez-vous à l'aide des informations d'identification AWS IAM Identity Center.
2. Sélectionnez le type de tâche « Personnalisé/code » dans l'application Web AWS Transform.
3. Indiquez à l'agent le nom de la définition de transformation que vous souhaitez utiliser.
4. L'application Web fournit une commande AWS Transform CLI qui peut être partagée avec votre équipe. Cette commande appelle la définition de transformation et enregistre les résultats d'exécution dans l'application Web.
5. Une fois les résultats de transformation saisis, consultez les statistiques, les mesures de gain de temps et posez des questions sur l'avancement de votre travail dans le tableau de bord.

L'application Web est conçue pour les opérations à l'échelle de l'entreprise nécessitant une surveillance centralisée des transformations sur plusieurs bases de code.

> **Note**
>
> AWS IAM Identity Center est requis pour accéder à l'application Web AWS Transform. La CLI ne nécessite pas IAM Identity Center. Seules les AWS informations d'identification standard sont nécessaires.

Présentation des commandes de transformation personnalisées

Voici quelques-unes des commandes que vous pouvez utiliser pour les transformations personnalisées. La liste complète des commandes se trouve dans la référence des commandes AWS Transform custom transformations.

- `atx custom`
  - Exécute une expérience interactive de transformation personnalisée, permettant la création, la découverte, l'exécution et l'affinement des transformations.
  - Il s'agit de la commande par défaut pour`atx`.
  - `--trust-all-tools`(`-t`) est facultatif et autorise implicitement toutes les demandes d'outils demandées par l'agent. À utiliser avec prudence, en particulier dans les environnements de production. Vous pouvez configurer la confiance des outils pour des outils et des commandes spécifiques à l'aide du fichier de paramètres de confiance.
- `atx custom --help` | `atx custom -h`
  - Affiche le menu d'aide.
  - Chaque commande inclut également un menu d'aide, par exemple`atx custom def exec --help`.
- `atx --version` | `atx -v`
  - Montre la version.
  - Le numéro de version change à chaque version.
- `atx custom def list`
  - Imprime la liste des transformations disponibles dans le registre des transformations.
- `atx custom def exec`
  - Exécute une transformation
- `atx custom def learnings`
  - Ouvre une session interactive pour visualiser et gérer les leçons qu'une transformation a tirées des précédentes exécutions
- `atx mcp`
  - Utilisé pour gérer les configurations des serveurs MCP

Flux de travail

Exécution de transformations

Cette section décrit les différentes manières d'exécuter des transformations et les options permettant de contrôler le comportement d'exécution.

Modes d'exécution

AWS Transform Custom prend en charge trois modes d'exécution pour s'adapter à différents flux de travail.

Mode conversationnel interactif

Démarrez la CLI avec `atx` et demandez à l'agent d'exécuter une transformation en langage naturel. Ce mode vous permet d'avoir une conversation complète avec l'agent, d'interrompre l'exécution à tout moment et de fournir des commentaires pendant le processus de transformation.

Utilisez ce mode lorsque vous souhaitez un contrôle maximal et la possibilité de guider l'agent dans des scénarios complexes.

Exécution interactive directe

Permet `atx custom def exec -n <transformation-name> -p <path>` de démarrer une transformation spécifique de manière interactive. Ce mode vous permet de consulter l'agent et d'interagir avec lui au début, pendant ou à la fin de l'exécution. L'agent fera une pause aux principaux points de décision et vous demandera votre avis.

C'est idéal pour tester et affiner les transformations avant de les exécuter de manière autonome.

Vous pouvez exécuter des transformations en mode non interactif ou en mode headless. Non-interactive mode supprime les invites lors d'une transformation nommée. Le mode Headless vous permet d'exécuter l'agent à l'aide d'une invite en texte brut, en contournant complètement l'interface interactive.

Non-interactive mode

À utiliser `atx custom def exec -n <transformation-name> -p <path> -x -t` pour une automatisation complète. Ajoutez `-x` pour exécuter en mode non interactif et `-t` pour faire confiance à tous les outils automatiquement sans y être invité.

Ce mode est conçu pour l'intégration des CI/CD pipelines et l'exécution en masse lorsqu'aucune intervention humaine n'est disponible ou souhaitée.

Mode sans tête

Pour effectuer des tâches sans interagir avec l'agent, exécutez `atx -x "<prompt>" -t` et fournissez vos instructions en texte brut.

Exécution de transformations sans interface

Utilisez ce mode pour appliquer une définition de transformation existante à votre base de code. La transformation s'exécute automatiquement à chaque étape sans votre approbation.

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

Développement de la transformation sans tête

Créez ou modifiez des définitions de transformation.

Pour convertir une ancienne définition de transformation au nouveau format de compétence (SKILL.md + references/), exécutez la commande suivante :

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

Pour créer une nouvelle définition de transformation, exécutez la commande suivante :

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

Drapeaux de commande communs

Lors de l'exécution de transformations avec`atx custom def exec`, les indicateurs suivants sont couramment utilisés :

- `-n`ou `--transformation-name` - Spécifie le nom de la transformation à exécuter
- `-p`ou `--code-repository-path` - Spécifie le chemin d'accès à votre base de code (utilisez «. » pour le répertoire actuel)
- `-c`ou `--build-command` - Spécifie la commande de génération ou de validation à exécuter

- `-x` ou `--non-interactive` - Active le mode non interactif (aucune invite utilisateur)
- `-t` ou `--trust-all-tools` - Fait confiance automatiquement à tous les outils sans y être invité
- `-d` ou `--do-not-learn` - Empêche l'extraction des leçons à partir de cette exécution
- `--tv` ou `--transformation-version` - Spécifie une version spécifique de la transformation
- `-g` ou `--configuration` : fournit un fichier de configuration ou une configuration en ligne

> **Important**
>
> L'`--trust-all-tools` indicateur `-t` ou approuve automatiquement toutes les exécutions d'outils sans y être invité et contourne la plupart des dispositifs de sécurité (les commandes correspondant à votre `alwaysPromptCommands` liste nécessitent toujours une autorisation explicite, sauf si elles sont remplacées par). `trustedShellCommands` La transmission `--trust-all-tools` est obligatoire pour une expérience totalement autonome, mais pas obligatoire pour exécuter la transformation. `--non-interactive` À utiliser avec prudence dans les environnements de production.

Utilisation des fichiers de configuration

AWS Transform custom prend en charge les fichiers de configuration facultatifs au format YAML ou JSON. Les fichiers de configuration vous permettent de spécifier les paramètres d'exécution et de fournir un contexte supplémentaire à l'agent.

Pour utiliser un fichier de configuration :

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

Vous pouvez également fournir la configuration sous forme de paires clé-valeur en ligne :

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

Exemple de fichier de configuration (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
```

Le `additionalPlanContext` paramètre fournit un contexte supplémentaire pour le plan d'exécution de l'agent. Cela est particulièrement utile pour les transformations AWS gérées afin de personnaliser leur comportement en fonction de vos besoins spécifiques.

Commandes de création et de validation

La commande de génération ou de validation est un paramètre facultatif qui indique comment valider votre code pendant le processus de transformation. AWS Transform custom tentera de déduire la meilleure commande de compilation en fonction de la transformation si elle n'est pas spécifiée, bien qu'il soit recommandé d'être spécifique pour des raisons de qualité.

Exemples de commandes de génération et de validation :

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

Même pour les langages ou les transformations qui ne nécessitent pas de construction, il est très important de fournir une commande qui valide les résultats et renvoie les problèmes en cas d'échec de la validation pour améliorer la qualité de la transformation.

Si aucune compilation ou validation n'est nécessaire, omettez cette information de votre saisie.

Contrôler le comportement d'apprentissage

Par défaut, AWS Transform custom extrait les leçons de chaque exécution de transformation. Vous pouvez empêcher l'apprentissage pour des exécutions spécifiques.

Pour empêcher l'apprentissage d'une exécution :

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

L'`--do-not-learn`indicateur `-d` ou permet de ne pas autoriser l'extraction des leçons de l'exécution en cours.

Reprise des conversations

AWS Transform custom vous permet de reprendre les conversations précédentes dans les 30 jours suivant la création.

Pour reprendre la conversation la plus récente :

```
atx --resume
```

Pour reprendre une conversation spécifique :

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

> **Important**
>
> Les conversations ne peuvent être reprises que dans les 30 jours suivant leur création. Après 30 jours, la conversation ne peut plus être reprise.

Suivi des minutes des agents

AWS Transform Custom effectue le suivi des minutes consacrées par les agents au cours d'une session de transformation. Les minutes des agents s'accumulent tout au long du cycle de vie de la conversation et sont affichées à la fin de la conversation :

```
Agent minutes used: 12.50
```

Les minutes des agents persistent malgré les interruptions. Si vous interrompez une session avec Ctrl+C et que vous la reprenez ultérieurement, les minutes précédemment accumulées sont reportées et continuent à s'accumuler lors de la reprise de la session.

Pour consulter les minutes des agents au cours d'une session interactive, procédez comme suit :

Tapez `/usage` à l'invite de saisie pour afficher les minutes d'agent cumulées en cours sans mettre fin à la conversation.

Pour définir une limite budgétaire pour les minutes des agents :

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

L'`--limit`option définit un budget maximum de minutes d'agent pour la session. Les minutes des agents reflètent le temps de travail actif de l'agent, et non l'heure de l'horloge murale. Lorsque la limite est atteinte, la CLI affiche un message et sort avec des instructions pour reprendre :

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

Vous pouvez reprendre la conversation ultérieurement en augmentant la limite :

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

Apprentissage continu

Cette section décrit comment réviser et gérer les leçons créées par l'apprentissage continu.

Comprendre les leçons

Le système d'apprentissage continu extrait automatiquement les leçons des exécutions précédentes d'une transformation. Le système les crée de manière asynchrone en fonction des éléments suivants :

- Feedback des développeurs fourni en mode interactif
- Problèmes de code rencontrés lors des transformations

Les leçons s'accumulent au fil du temps au fur et à mesure que vous exécutez la transformation sur différentes bases de code. Le système les applique automatiquement pour améliorer les courses à venir. Chaque leçon appartient à une catégorie contenant toutes les leçons d'un domaine similaire afin que vous puissiez revoir les leçons connexes ensemble. Pour les leçons que vous ne souhaitez pas utiliser, vous pouvez archiver ou supprimer complètement la leçon.

Afficher et gérer les leçons

Utilisez la `learnings` commande pour ouvrir une session interactive permettant de parcourir et de gérer les leçons d'une définition de transformation.

Pour ouvrir le visualiseur de leçons :

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

Le visualiseur s'ouvre sur une liste de catégories de leçons, chacune indiquant le nombre de leçons actives qu'elle contient. Sélectionnez une catégorie pour voir ses leçons, puis sélectionnez une leçon pour afficher tous ses détails, y compris le corps de la leçon, son impact et le nombre de courses précédentes qui l'ont consultée.

Archivage et restauration des leçons

Le système applique les leçons automatiquement. Si vous ne souhaitez pas que le système applique une leçon, vous pouvez l'archiver. Le système conserve les leçons archivées mais ne les applique pas aux prochaines séries. Toutes les leçons archivées sont regroupées afin que vous puissiez les consulter et les remettre en état d'utilisation active.

Supprimer des leçons

Supprimez définitivement une leçon qui n'est pas utile. La suppression ne peut pas être annulée et le système peut réapprendre une leçon supprimée lors des prochaines exécutions.

Une leçon doit être archivée avant de pouvoir être supprimée.

Configuration avancée

Cette section décrit les fonctionnalités avancées et les options de configuration de AWS Transform custom.

Variables d'environnement

Vous pouvez personnaliser le comportement de la CLI à l'aide de variables d'environnement.

> **Note**
>
> Les exemples suivants montrent la syntaxe Linux et macOS (`export`). Sous Windows, définissez les variables d'environnement dans PowerShell using`$env:NAME="value"`. Consultez les onglets Windows (PowerShell) pour les commandes équivalentes.

ATX_SHELL_TIMEOUT

Remplacez le délai d'attente par défaut pour les commandes shell (900 seconds/15 minutes).

Linux and macOS

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

Windows (PowerShell)

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

Ceci est utile pour les bases de code volumineuses ou les processus de construction de longue durée.

ATX_DISABLE_UPDATE_CHECK

Désactivez les vérifications de version automatiques et mettez à jour les notifications lors de l'exécution des commandes.

Linux and macOS

```
export ATX_DISABLE_UPDATE_CHECK=true
```

Windows (PowerShell)

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

ATX_GIT_COMMITTER_NAME et ATX_GIT_COMMITTER_EMAIL

Configurez l'identité de l'auteur utilisée pour les validations de points de contrôle que AWS Transform custom crée dans votre référentiel lorsqu'il applique les modifications lors d'une transformation. Lorsque ces variables ne sont pas définies, les validations des points de contrôle sont attribuées à une identité par défaut (`ATX Bot <checkpoint@atx.bot>`). Définissez les deux variables pour attribuer des points de contrôle à un auteur spécifique.

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"
```

Paramètres de confiance

Les paramètres de confiance vous permettent de pré-approuver des outils et des commandes spécifiques à exécuter sans invite. Vous pouvez également exiger une autorisation explicite pour des commandes shell spécifiques, quel que soit le niveau de confiance. Ces paramètres sont configurés dans le `~/.aws/atx/trust-settings.yaml` fichier.

Le fichier contient trois listes :

- `trustedTools`- Outils qui peuvent être exécutés sans être invités
- `trustedShellCommands`- Commandes shell qui peuvent être exécutées sans être demandées
- `alwaysPromptCommands`- Modèles de commandes Shell qui nécessitent une autorisation explicite à moins qu'ils ne soient remplacés par`trustedShellCommands`, quel que soit l'`-t`indicateur ou la confiance de session. Ces modèles ne sont pas appliqués en mode non interactif (`-x`).

Outils fiables par défaut :

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

Modification des paramètres de confiance :

Vous pouvez modifier manuellement le fichier trust-settings.yaml pour ajouter ou supprimer des outils et des commandes fiables. À la fois `trustedShellCommands` et `alwaysPromptCommands` prenez en charge les modèles génériques globaux en utilisant. *

> **Note**
>
> Si une commande correspond aux deux listes, elle `trustedShellCommands` est prioritaire.

La section suivante décrit chaque liste de commandes et fournit des exemples :

- `trustedShellCommands`- Les commandes correspondant à ces modèles s'exécutent sans invite, en contournant toutes les autres barrières. Les modèles sont comparés à la chaîne de commande complète.

  Exemples :

  - `cd *`- Correspond aux commandes composées commençant par cd
  - `*&&*`- Fait confiance à toutes les commandes avec les opérateurs &&
- `alwaysPromptCommands`- Les commandes correspondant à ces modèles nécessitent une autorisation explicite à moins qu'elles ne soient remplacées par`trustedShellCommands`, quel que soit l'`-t`indicateur ou la confiance de session. Ces modèles ne sont pas appliqués en mode non interactif (`-x`). Les modèles sont comparés à chaque sous-commande dans les expressions composées (&&, | |, substitutions de commandes).

  Exemples :

  - `rm -rf *`- Demande toujours des commandes de suppression forcée récursives
  - `sudo *`- Demande toujours les commandes exécutées avec sudo
  - `find * -exec *`- Demande toujours des commandes de recherche avec -exec

Session-level confiance :

Au cours des invites interactives, vous pouvez choisir :

- `(y)es`- Exécuter une fois
- `(n)o`- Refuser
- `(t)rust`- Confiance pour la session en cours uniquement

Session-level les paramètres de confiance sont temporaires et réinitialisés au redémarrage de l'interface de ligne de commande, fournissant une approbation temporaire sans modifier définitivement trust-settings.yaml.

> **Note**
>
> La confiance de session n'est pas disponible pour les commandes correspondant à votre `alwaysPromptCommands` liste.

Serveurs MCP (Model Context Protocol)

La CLI AWS Transform prend en charge les serveurs MCP (Model Context Protocol), qui étendent ses fonctionnalités grâce à des outils supplémentaires.

Configuration :

Configurez les serveurs MCP dans le `~/.aws/atx/mcp.json` fichier. La CLI AWS Transform prend en charge deux types de serveurs MCP : les serveurs locaux basés sur des commandes et les serveurs HTTP distants.

Serveurs locaux basés sur des commandes :

Les serveurs locaux s'exécutent en tant que processus enfants sur votre machine. Configurez-les avec la `command` propriété :

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

Serveurs HTTP distants :

Les serveurs distants se connectent aux serveurs MCP hébergés via une URL HTTP ou HTTPS. Configurez-les avec la `url` propriété :

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

La `headers` propriété est facultative et prend en charge l'expansion des variables d'environnement à l'aide de `${VAR_NAME}` la syntaxe. Cela vous permet de stocker des valeurs sensibles telles que des jetons d'API dans des variables d'environnement plutôt que dans le fichier de configuration.

Propriétés de configuration :

Les serveurs locaux basés sur des commandes prennent en charge les propriétés suivantes :

- `command`(obligatoire) - La commande pour exécuter le serveur
- `args`(facultatif) - Tableau d'arguments de ligne de commande
- `env`(facultatif) - Variables d'environnement à transmettre au processus serveur

Les serveurs HTTP distants prennent en charge les propriétés suivantes :

- `url`(obligatoire) - L'URL HTTP ou HTTPS du serveur MCP distant
- `headers`(facultatif) - en-têtes HTTP à inclure dans les requêtes, avec prise en charge de l'extension des variables d'`${VAR_NAME}`environnement

Gestion des serveurs MCP :

Afficher la liste des serveurs MCP configurés :

```
atx mcp tools
```

Répertoriez les outils disponibles proposés par un serveur MCP spécifique :

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

Suivi de l'utilisation :

La CLI suit automatiquement l'utilisation de l'outil MCP lors des exécutions de transformation. Les statistiques d'utilisation sont conservées comme `mcp_usage.json` dans le répertoire des conversations situé à côté`metadata.json`. Le fichier enregistre les métriques par outil pour chaque exécution, notamment :

- Nombre d'invocations par outil
- Nombre d'erreurs par outil
- Temps d'exécution total par outil

- Détails de la dernière erreur (le cas échéant)

Client-Side Compétences

Client-side les compétences sont des capacités supplémentaires qui étendent l'agent lors des exécutions de transformation. Ils vous permettent de fournir des outils, des scripts et des instructions personnalisés que l'agent peut utiliser en plus de ses fonctionnalités intégrées.

Répertoires de découverte de compétences :

Les compétences sont découvertes à partir de quatre répertoires par ordre de priorité. Si une compétence portant le même nom existe dans plusieurs répertoires, le premier répertoire de la liste est prioritaire :

1. `<project>/.aws/atx/skills/`- Project-level, AWS Transformer CLI-specific
2. `<project>/.agents/skills/`- Project-level, cross-client (disponible pour tous les outils d'agent compatibles)
3. `~/.aws/atx/skills/`- User-level, AWS Transformer CLI-specific
4. `~/.agents/skills/`- User-level, cross-client (disponible pour tous les outils d'agent compatibles)

Les `.aws/atx/skills/` répertoires sont spécifiques à la CLI AWS Transform. Les `.agents/skills/` répertoires sont inter-clients, ce qui signifie que les compétences qui y sont placées sont disponibles pour tout outil d'agent compatible au-delà de la CLI AWS Transform.

Structure du répertoire des compétences :

Chaque compétence est un répertoire contenant un `SKILL.md` fichier avec le frontmatter YAML :

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

SKILL.md format :

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

Instructions for the agent...
```

Le `name` champ doit correspondre au nom du répertoire parent.

Désactivation d'une compétence :

Pour empêcher le chargement d'une compétence sans avoir supprimé ses fichiers, ajoutez `disable-model-invocation: true` à la page d'accueil :

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

Lorsque cette propriété est définie, la CLI ignore la compétence lors de la découverte. L'agent ne peut ni voir ni utiliser la compétence à moins qu'une définition de transformation ne lui demande explicitement de lire le fichier de compétences. Utilisez-le pour désactiver temporairement une compétence, la marquer comme étant en cours de développement ou conserver des documents de référence destinés uniquement aux lecteurs humains.

> **Note**
>
> Les fichiers d'une compétence désactivée restent sur le disque. Si une définition de transformation demande à l'agent de lire un chemin de fichier spécifique, l'agent peut toujours accéder au contenu. La `disable-model-invocation` propriété empêche la découverte automatique et l'injection de contexte, mais pas l'accès au système de fichiers.

Disponibilité des compétences par mode d'exécution :

- Mode Exec (`atx custom def execavec--code-repository-path`) - Découvre les compétences à la fois dans les répertoires au niveau de l'utilisateur et au niveau du projet.

- Mode interactif (`atx`) - Seules les compétences de niveau utilisateur sont découvertes initialement. Lorsque vous fournissez un chemin de dépôt de code au cours de la session, les compétences au niveau du projet sont également chargées.

Vérification de la découverte des compétences :

Consultez le journal de débogage de la CLI après une exécution pour vérifier quelles compétences ont été découvertes :

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
```

Les compétences dont la validation échoue sont ignorées avec un avertissement dans les journaux de débogage.

> **Note**
>
> Client-side les compétences nécessitent la version 2.0 ou ultérieure de la CLI.

Choisir entre Project-Level et User-Level compétences

L'endroit où vous placez une compétence détermine qui en bénéficie et quand elle est activée.

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

Consignez-les au contrôle de version afin que chaque membre de l'équipe effectuant des transformations dans le référentiel les découvre automatiquement. Utiliser les compétences au niveau du projet pour :

- Repository-specific contrôles de conformité (règles Dockerfile, politiques Terraform, validateurs de sécurité des migrations)

- Normes de codage organisationnel qui s'appliquent à cette base de code (modèles d'observabilité, gestion des erreurs, conventions de dénomination)
- Créez ou testez des scripts spécifiques au projet (linters personnalisés, fonctions de fitness de l'architecture)
- Guides de migration d'API pour les bibliothèques internes utilisées dans ce référentiel

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

Ils restent sur votre machine et s'activent pendant toutes les transformations, quel que soit le référentiel que vous ciblez. Utilisez les compétences de niveau utilisateur pour :

- Outils de flux de travail personnels (générateurs de journaux des modifications, formateurs de messages de validation)
- Cross-project préférences (modèles de test préférés, rappels de style de documentation)
- Contrôles de conformité des licences dont votre organisation a besoin pour tous les référentiels
- Seuils de couverture ou barrières de qualité que vous appliquez à chaque base de code avec laquelle vous travaillez

Conseils pour des compétences efficaces :

- Écrivez `description` des champs clairs dans votre page `SKILL.md` d'accueil. L'agent utilise ce champ pour décider quand une compétence est pertinente.
- Quittez les scripts de validation avec le code 0 en cas de succès et différent de zéro en cas d'échec. L'agent interprète les codes de sortie pour déterminer la conformité.
- Imprimez des messages d'erreur clairs et exploitables dans des scripts. L'agent lit les résultats pour comprendre ce qu'il faut corriger.
- Placez les compétences dans le répertoire inter-clients (`.agents/skills/`) à chaque niveau pour les partager avec d'autres outils de développement d'IA au-delà de la CLI AWS Transform.

Client-Side Exemples de compétences

Ces exemples montrent deux modèles courants : une compétence de validation basée sur un script et une compétence basée uniquement sur des références.

Exemple : Dockerfile Compliance Checker () Script-Based

Cette compétence permet de valider Dockerfiles par rapport aux meilleures pratiques opérationnelles et de sécurité. Il utilise un script de validation que l'agent exécute avant et après les modifications.

Structure du répertoire :

```
.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.
```

Le script de validation vérifie la présence de balises d'image de base non épinglées, exécutées en tant que root, de secrets codés en dur dans les ENV directives et de définitions manquantes. HEALTHCHECK L'agent exécute le script, corrige les violations à l'aide des modèles du fichier de référence et réexécute le script pour confirmer la conformité.

Exemple : API Deprecation Helper () Reference-Only

Cette compétence guide l'agent dans le remplacement des appels d'API obsolètes lors des transformations de mise à niveau. Il utilise uniquement des fichiers de référence sans script.

Structure du répertoire :

```
.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
```

Les fichiers de référence contiennent des exemples de code avant/après. Par exemple, `aws-sdk-v2-to-v3.md` mappe les modèles `s3.putObject(params).promise()` à l'équivalent modulaire v3 en utilisant `S3Client` et`PutObjectCommand`.

Tags et organisation

Vous pouvez organiser les transformations à l'aide de balises pour le contrôle d'accès et la catégorisation.

> **Note**
>
> Certaines de ces commandes nécessitent la spécification de l'Amazon Resource Name (ARN) pour une définition de transformation. La structure de l'ARN est la suivante : `arn:aws:transform-custom:<region>:<account-id>:package/<td-name>`

Pour répertorier les balises d'une transformation :

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

Pour ajouter des balises à une transformation :

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

Pour supprimer des balises d'une transformation, procédez comme suit :

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

Les balises peuvent être utilisées pour le contrôle d'accès groupé dans les politiques IAM. Vous pouvez créer des politiques qui accordent des autorisations à toutes les transformations comportant des balises spécifiques (par exemple, toutes les transformations marquées avec `team:frontend` ou`environment:production`).

Journaux

AWS La CLI Transform gère trois types de journaux pour le dépannage et le débogage.

Journaux de conversations :

Linux and macOS

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

Windows

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

Ces journaux contiennent l'historique complet des conversations pour une session spécifique.

Journaux des sous-agents :

Linux and macOS

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

Windows

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

Ces journaux contiennent les résultats des sous-agents générés par l'agent principal lors des transformations. Il n'est pas nécessaire de gérer directement les sous-agents.

Journaux de débogage des développeurs :

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
```

Ces journaux fournissent des informations de dépannage avancées pour la CLI elle-même.

> **Note**
>
> Le répertoire des journaux de débogage peut contenir plusieurs fichiers journaux de débogage (par exemple, debug1.log, debug2.log). Consultez et fournissez tous les journaux

pertinents, par exemple ~/. aws/atx/custom/ <conversation-id>/* et ~/. aws/atx/logs/ *, lors de l'ouverture des tickets d'assistance pour une résolution plus rapide.

Mises à jour de

Maintenez votre interface de ligne de commande à jour pour accéder aux nouvelles fonctionnalités et améliorations.

Pour vérifier les mises à jour :

```
atx update --check
```

Pour effectuer la mise à jour vers la dernière version :

```
atx update
```

Pour effectuer une mise à jour vers une version spécifique :

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

Créez des transformations personnalisées

Cette section explique comment créer, modifier et gérer des définitions de transformation personnalisées.

Créer une nouvelle transformation

Utilisez l'interface de ligne de commande interactive pour créer une nouvelle définition de transformation.

Pour créer une définition de transformation

1. Démarrez la CLI AWS Transform :

   ```
   atx
   ```

2. Dites à l'agent que vous souhaitez créer une nouvelle transformation.

3. Fournissez une description claire et détaillée de l'objectif de transformation. Inclure :
    - L'état source et cible (par exemple, « mise à niveau de la version X vers la version Y »)
    - Modifications spécifiques requises (par exemple, « mettre à jour les instructions d'importation, remplacer les méthodes obsolètes »)
    - Toute considération ou contrainte particulière
4. Lorsque l'agent demande des éclaircissements ou des informations supplémentaires, fournissez des exemples spécifiques et des documents de référence.
5. Passez en revue la définition de transformation initiale créée par l'agent.
6. Testez la transformation sur un exemple de base de code.
7. Effectuez une itération en fournissant des commentaires, des corrections de code ou des exemples supplémentaires.
8. Enregistrez la transformation localement ou publiez-la dans le registre.

Meilleures pratiques pour créer des transformations :

- Commencez par des transformations simples et bien définies avant de tenter des transformations complexes
- Fournir des documents de référence complets, y compris des guides de migration et des exemples de code
- Testez sur plusieurs exemples de bases de code avant de publier
- Utilisez des commandes de génération ou de validation déterministes pour permettre un apprentissage continu
- Envisagez de diviser les transformations complexes en plusieurs étapes plus petites
- Marquez les informations cruciales avec « CRITIQUE : » ou « IMPORTANT : » dans vos définitions de transformation pour vous assurer que l'agent donne la priorité à ces exigences
- Lorsque vous devez respecter des exigences précises (comme utiliser une commande ou une valeur de chaîne spécifique), spécifiez explicitement la chaîne complète dans vos définitions de transformation. Vous pouvez les placer entre guillemets bash pour indiquer clairement qu'il s'agit de commandes de terminal ou de chaînes littérales, ce qui réduit la variabilité et garantit une exécution cohérente

Fourniture de matériaux de référence

Vous pouvez fournir des fichiers de référence à AWS Transform custom en spécifiant les chemins des fichiers au cours de la conversation. Ces fichiers sont stockés dans le `references/` dossier de la définition de transformation.

Types de fichiers de référence recommandés :

- Before/after exemple de code
- Documentation sur les API, les bibliothèques ou les fonctionnalités impliquées
- Human-readable guides de migration

Pour fournir un fichier de référence :

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

Vous pouvez également fournir un répertoire contenant plusieurs fichiers de référence :

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

> **Note**
>
> Seuls les fichiers texte (.md, .html, .txt, fichiers de code) sont pris en charge. Les fichiers binaires, les images et les fichiers de texte enrichi (par exemple, .pdf, .png, .docx) ne sont pas pris en charge actuellement. Il est souvent possible d'extraire le contenu du texte et de l'utiliser comme référence. Si vous possédez de nombreux petits fichiers texte, pensez à les concaténer en quelques fichiers portant un nom descriptif. Il y a une limite de 10 Mo au total pour tous les fichiers.

Modifier une transformation existante

Vous pouvez modifier les transformations personnalisées avant et après les avoir enregistrées en tant que brouillons ou les avoir publiées. Vous ne pouvez pas modifier les transformations AWS gérées. Si vous devez les personnaliser, vous pouvez fournir un contexte supplémentaire à l'aide du fichier de configuration.

Pour modifier une transformation existante

1. Démarrez la CLI AWS Transform :

```
atx
```

2. Indiquez à l'agent que vous souhaitez modifier une transformation existante.
3. Choisissez si vous souhaitez :
   - Fournissez un chemin de fichier vers une transformation stockée localement (c'est-à-dire qu'il ne s'agit pas d'un brouillon enregistré ou publié)
   - Demandez la liste des transformations depuis le registre
4. Si vous choisissez dans le registre, sélectionnez la transformation que vous souhaitez modifier.
5. Collaborez avec l'agent pour décrire les modifications que vous souhaitez apporter.
6. Testez la transformation mise à jour sur un exemple de base de code.
7. Publiez vos mises à jour dans le registre si vous le souhaitez.

Publication et gestion des transformations

Vous pouvez publier et gérer vos transformations à l'aide de l'expérience interactive ou à l'aide des commandes suivantes.

Pour enregistrer une transformation en tant que brouillon :

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

Pour publier une transformation :

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

Pour répertorier les transformations disponibles :

```
atx custom def list
```

Pour télécharger une définition de transformation :

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

Cela télécharge la définition de la transformation dans votre répertoire de travail actuel. Vous pouvez spécifier un répertoire cible avec l'`--td`indicateur et une version avec l'`--tv`indicateur.

Pour supprimer une définition de transformation :

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

> **Important**
>
> Cela supprime définitivement la définition de transformation spécifiée de votre compte.

Gestion des versions de transformation

AWS Transform Custom gère les versions de vos définitions de transformation. Vous pouvez spécifier une version lors de l'exécution ou du téléchargement d'une transformation.

Pour exécuter une version spécifique :

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

Pour télécharger une version spécifique :

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

Si aucune version n'est spécifiée, la dernière version est utilisée.

Référence de commande

Cette section fournit une référence complète de toutes les commandes CLI personnalisées de AWS Transform.

Commandes interactives

taxe

Démarrez une conversation interactive avec l'interface de ligne de commande 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
```

Commandes de session interactives

Les commandes suivantes peuvent être saisies à l'invite de saisie au cours d'une session interactive :

- `/usage`- Afficher les minutes d'agent accumulées pour la session en cours

Commandes de définition de transformation

atx custom def exec

Exécutez une définition de transformation dans un référentiel de code.

Option	Forme longue	Paramètre	Description
`-p`	`--code-repository-path`	`<path>`	Chemin d'accès au référentiel de code à transformer. Pour le répertoire actuel, utilisez «. »
`-c`	`--build-command`	`<command>`	Commande à exécuter lors de la création du référentiel
`-n`	`--transformation-name`	`<name>`	Nom de la définition de transformation dans le registre
`-x`	`--non-interactive`	`-`	Exécute la transformation sans assistance de l'utilisateur

Option	Forme longue	Paramètre	Description
`-t`	`--trust-all-tools`	-	Fait confiance à tous les outils (aucune invite d'outil)
`-d`	`--do-not-learn`	-	Ne pas autoriser l'extraction de leçons à partir de cette exécution
`-g`	`--configuration`	`<config>`	Chemin vers le fichier de configuration (JSON ou YAML) ou les paires clé=valeur
`--tv`	`--transformation-version`	`<version>`	Version de la définition de transformation à utiliser
`--limit`	`--limit`	`<limit>`	Définissez la limite budgétaire des minutes consacrées aux agents. La transformation se termine lorsque la limite est atteinte et peut être reprise avec une limite augmentée
`-h`	`--help`	-	Afficher l'aide pour les commandes

liste de définitions personnalisée atx

Répertoriez les définitions de transformation disponibles.

```
atx custom def list
```

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

ATX Custom Def Get

Obtenez les détails d'une définition de transformation spécifique.

Option	Forme longue	Paramètre	Description
`-n`	`--transformation-name`	`<name>`	Le nom de la définition de transformation à récupérer
`--tv`	`--transformation-version`	`<version>`	La version de la définition de transformation à récupérer
`--td`	`--target-directory`	`<directory>`	Le répertoire cible dans lequel enregistrer la définition de transformation (par défaut : «. »)
`--json`	`--json`	-	Réponse de sortie au format JSON
`-h`	`--help`	-	Afficher l'aide pour les commandes

suppression de la définition personnalisée atx

Supprimez définitivement une définition de transformation.

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

publication avec définition personnalisée ATX

Publiez une définition de transformation dans le registre.

Option	Forme longue	Paramètre	Description
`-n`	`--transformation-name`	`<name>`	Le nom de la définition de transformation à publier
`--tv`	`--transformation-version`	`<version>`	La version de la définition de transformation à utiliser (non applicable avec --description ou --source-directory)
`--sd`	`--source-directory`	`<directory>`	Le répertoire source à partir duquel lire les fichiers de définition de transformation locaux (non applicable avec --transformation-version)
`--description`	`--description`	`<description>`	Une description de la définition de la transformation (non applicable avec --transformation-version)
`--json`	`--json`	-	Réponse de sortie au format JSON
`-h`	`--help`	-	Afficher l'aide pour les commandes

fichier de sauvegarde personnalisé ATX

Enregistrez une définition de transformation en tant que brouillon dans le registre. Les brouillons expirent au bout de 30 jours et n'apparaissent pas dans le registre. Cette commande renvoie le numéro de version du brouillon. Vous devez exécuter et récupérer les brouillons de manière explicite en utilisant le nom de la transformation et le numéro de version.

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

Commandes de leçon

Apprentissages ATX Custom Def

Ouvrez une session interactive pour visualiser et gérer les leçons qu'une définition de transformation a tirées des précédentes exécutions. Parcourez les leçons par catégorie, consultez les détails des leçons et archivez, restaurez ou supprimez des leçons.

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

Commandes de balises

balises de liste de définition personnalisées atx

Répertoriez les balises pour une définition de transformation.

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

tag de définition personnalisé atx

Ajoutez des balises à une définition de transformation.

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

Atx Custom Def Untag

Supprimez les balises d'une définition de transformation.

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

Mettre à jour les commandes

mise à jour fiscale

Mettez à jour la CLI AWS Transform.

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

Commandes MCP

outils ATX MCP

Autorise les clients à view/confirm configurer leurs outils MCP. Les mises à jour des configurations doivent être gérées directement via le fichier ~/. aws/atx/mcp.json

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

AWS-Transformations gérées

AWS Les transformations gérées sont des transformations prédéfinies et AWS approuvées pour les cas d'utilisation courants, prêtes à être utilisées sans aucune configuration supplémentaire.

Présentation de

AWS-les transformations gérées présentent les caractéristiques suivantes :

- Validé par AWS - Ces transformations sont contrôlées AWS pour être de haute qualité
- Prêt à l'emploi : aucune configuration supplémentaire n'est requise
- Croissance continue - Des transformations supplémentaires sont continuellement ajoutées
- Personnalisable : Pre-built les transformations peuvent être personnalisées en fournissant des conseils ou des exigences supplémentaires spécifiques aux besoins de votre organisation à l'aide du paramètre `additionalPlanContext` de configuration
- Prise en charge de l'accès anticipé - Certaines transformations peuvent être considérées comme étant en accès anticipé au fur et à mesure qu'elles sont soumises à des tests et à des améliorations supplémentaires

Available AWS-Transformations gérées

Le catalogue suivant répertorie les transformations AWS gérées actuellement disponibles, regroupées par cas d'utilisation. Chaque tableau indique le nom de la transformation, la langue ou la pile à laquelle elle s'applique et son statut. Pour trouver rapidement une transformation, utilisez le champ de recherche en haut de cette page pour effectuer une recherche par nom, langue ou cas d'utilisation.

Ce catalogue est la liste canonique des transformations AWS gérées. Le Kiro Power, le plug-in d'agent, le plug-in VS Code et la CLI exécutent tous les mêmes transformations. Pour répertorier les transformations disponibles dans votre registre, exécutez`atx custom def list`.

> **Note**
>
> Les transformations marquées « Accès anticipé » sont fonctionnelles mais peuvent être mises à jour fréquemment en fonction des commentaires des clients.

Mises à niveau de

Mettez à niveau une langue ou un environnement d'exécution vers une version plus récente, ou modifiez la distribution de l'environnement d'exécution.

Transformation	Langage/pile	Statut	Description
`AWS/java-version-upgrade`	Java	Généralement disponible	Mettez à niveau les applications Java à l'aide de n'importe quel système de compilation, de n'importe quelle version JDK source vers n'importe quelle version JDK cible, en modernisant les dépendances, notamment la migration vers Jakarta

Transformation	Langage/pile	Statut	Description
			EE, les pilotes de base de données, les frameworks ORM et les mises à jour de l'écosystème Spring. Spécifiez la version cible du JDK dans le chat ou à l'aide du `additionalPlanContext` paramètre.
`AWS/python-version-upgrade`	Python	Généralement disponible	Migrez les projets Python de Python 3.8 ou 3.9 vers Python 3.11, 3.12 ou 3.13 tout en préservant les fonctionnalités et les performances. Spécifiez la version cible de Python dans le chat ou à l'aide du `additionalPlanContext` paramètre.

Transformation	Langage/pile	Statut	Description
`AWS/nodejs-version-upgrade`	Node.js	Généralement disponible	Mettez à niveau Node.js les applications depuis n'importe quelle Node.js version source vers n'importe quelle Node.js version cible. Spécifiez la version cible dans le chat ou avec le `additionalPlanContext` paramètre.
`AWS/lambda-nodejs-runtime-upgrade`	Node.js (Lambda)	Accès anticipé	Mettez à niveau les fonctions AWS Lambda des anciens environnements d' Node.js exécution (nodejs4.3 à nodejs22.x) vers nodejs24.x, en corrigeant les modifications majeures apportées au client d'interface d'exécution Lambda (RIC) et à l'environnement d'exécution en 24 langues. Node.js

Transformation	Langage/pile	Statut	Description
`AWS/oracle-java-to-corretto`	Java (distribution JDK)	Accès anticipé	Migrez des projets Java depuis Oracle JDK vers Amazon Corretto. Remplace les API Oracle-specific internes par des équivalents Java standard, met à jour les configurations de build (Maven et Gradle) et les images de base des conteneurs, supprime les indicateurs JVM commerciaux et génère un rapport de licence.

Transformation	Langage/pile	Statut	Description
`AWS/ruby-upgrade`	Ruby	Accès anticipé	Mettez à niveau les applications Ruby de Ruby 2.x vers Ruby 4.0, et leurs frameworks vers Rails 8.0 ou Sinatra 4.1. Vous pouvez utiliser cette transformation avec Rails et les ActiveRecord applications, les applications Sinatra et les gemmes autonomes. La transformation associe chaque modification de version de Ruby à la mise à niveau du framework correspondant et exécute la suite de tests. Il isole ensuite les défaillances avant de passer à la version suivante.

Transformation	Langage/pile	Statut	Description
`AWS/dotnet-version-upgrade`	.NET	Généralement disponible	Migrez les solutions .NET Framework vers un .NET moderne (net10.0 par défaut ; net8.0 ou version ultérieure pris en charge) avec une interaction utilisateur contrôlée. Évalue la complexité et les dépendances, présente un plan de migration, transforme les projets avec validation et génère un résumé des étapes suivantes.

Migrations du SDK

Migrez entre les principales versions d'un AWS SDK.

Transformation	Langage/pile	Statut	Description
`AWS/java-aws-sdk-v1-to-v2`	Java	Généralement disponible	Mettez à niveau le AWS SDK de la v1 à la v2 pour les projets Java utilisant Maven ou Gradle.
`AWS/python-boto2-to-boto3`	Python	Généralement disponible	Migrez les applications Python de boto2 vers boto3, en vous basant sur la

Transformation	Langage/pile	Statut	Description
			documentation officielle de migration. AWS
`AWS/nodejs-aws-sdk-v2-to-v3`	Node.js	Généralement disponible	Mettez à niveau les Node.js applications du AWS SDK pour la JavaScript v2 vers la v3 pour bénéficier d'une architecture modulaire, d'un TypeScript support de premier ordre et de meilleures performances, sans changer de Node.js version.

Mises à niveau et migrations du framework

Mettez à niveau un framework vers une version plus récente ou migrez vers un autre framework.

Transformation	Langage/pile	Statut	Description
`AWS/spring-boot-version-upgrade`	Démarrage Java/Spring	Généralement disponible	Migrez les projets Spring Boot 3.x vers Spring Boot 4.x (ciblant la version 4.1.0 GA). Couvre les mises à niveau de version, les renommages du démarreur, la migration de Jackson 3, Spring Security 7 DSL, la MockBean suppression de @,

Transformation	Langage/pile	Statut	Description
			les renommage s de propriétés, les relocalisations de packages, la consolidation de l'observabilité, Spring AI 2.0, Spring Cloud 2025.1, Spring Batch, Kafka, AMQP, gRPC, Jersey, JSpecify, les modifications apportées aux serveurs intégrés Native/AOT, la compatibilité avec des tiers et la vérification.
`AWS/JBoss-to-Spring-Boot`	Java (JBoss ou WildFly Spring Boot)	Accès anticipé	Migrez les applicati ons d'entreprise Java EE ou Jakarta EE exécutées sur JBoss EAP ou WildFly vers Spring Boot, en éliminant les dépendances aux serveurs d'applica tions pour un modèle de déploiement conteneurisé natif du cloud.
`AWS/early-access-angular-to-react-mi gration`	Angular vers React	Accès anticipé	Transformez une application Angular en React.

Transformation	Langage/pile	Statut	Description
`AWS/angular-version-upgrade`	Angular (Angulaire)	Accès anticipé	Mettez à niveau une ancienne application Angular vers une version Angular cible, y compris les composants, les services, les modèles et le routage.
`AWS/vue.js-version-upgrade`	Vue.js	Accès anticipé	Effectuez une mise à niveau majeure de la version Vue.js 2 à la version Vue.js 3, en modernisant les composants, la gestion des états, le routage et les API globales. Les mises à jour mineures et les correctifs ne sont pas concernés.

GenAI et migrations de modèles

Migrez les charges de travail génératives d'IA vers.

Transformation	Langage/pile	Statut	Description
`AWS/GenAI-to-Bedrock-Migration-Assessment`	Charges de travail d'IA génératives	Accès anticipé	Évaluez les charges de travail d'IA génératives à migrer depuis des fournisseurs tiers (OpenAI, Google Gemini, Anthropic direct et

Transformation	Langage/pile	Statut	Description
			modèles open source) vers. Découvre l'utilisation et les modèles du SDK, clarifie les exigences , conçoit un mappage de modèles, estime les coûts et les risques et génère des artefacts d'évaluat ion. Assessmen t-only; ne modifie pas le code source. Couvre également les frameworks agentique s tels que CrewAI et Strands. LangGraph

Language-to-language migrations

Traduisez une base de code d'un langage de programmation à un autre.

Transformation	Langage/pile	Statut	Description
`AWS/vba-t o-python- migration`	VBA vers Python	Accès anticipé	Migrez les macros, les modules et la logique intégrée Excel VBA vers des scripts et modules Python équivalen ts, en utilisant openpyxl, pandas, tkinter ou PyQt 6 et des bibliothèques standard. UserForms

Transformation	Langage/pile	Statut	Description
			Le langage cible est Python 3.8 ou version ultérieure. À utiliser lors de la conversion de code VBA .bas, .cls, .frm ou .xlsm-embedded.

Migrations de bases

Aucune transformation AWS gérée spécifique à la base de données n'est actuellement disponible. Pour moderniser les bases de données Microsoft SQL Server et leurs applications .NET associées vers Amazon Aurora PostgreSQL, consultez. the section called “Modernisation de SQL Server”

Observabilité

Modernisez la journalisation et la surveillance vers des services AWS natifs.

Transformation	Langage/pile	Statut	Description
`AWS/early-access-log4j-to-slf4j-migration`	Java (journalisation)	Accès anticipé	Migrez les applications Java de Log4j (1.x ou 2.x) vers SLF4J avec un backend Logback. Gère le code source, la gestion des dépendances (Maven et Gradle) et la journalisation des fichiers de configuration, et valide par compilation, test et analyse des importations résiduelles.

Transformation	Langage/pile	Statut	Description
`AWS/datadog-monitors-to-cloudwatch-alarms`	Infrastructure en tant que code/surveillance	Accès anticipé	Migrez les moniteurs de DataDog métriques qui suivent les mesures de AWS service et les mesures personnalisées vers des CloudWatch alarmes natives sous forme d'infrastructure sous forme de code. Génère CloudFormation YAML, CDK TypeScript et Terraform HCL.

Architecture

Re-architect, reconfigurez la plateforme ou optimisez les applications pour AWS.

Transformation	Langage/pile	Statut	Description
`AWS/java-performance-optimization`	Java (performances)	Généralement disponible	Optimisez les performances des applications Java en analysant les données de profilage JFR pour détecter les points chauds et les anti-modèles du processeur et de la mémoire, puis en appliquant des corrections de code ciblées. Pour obtenir

Transformation	Langage/pile	Statut	Description
			des instructions sur la collecte des données JFR, consultez le guide d'exécution JFR.
`AWS/early-access-java-x86-to-graviton`	Java (Arm64/Graviton)	Accès anticipé	Validez la compatibilité des applications Java avec l'architecture Arm64 pour les processeurs AWS Graviton et résolvez les incompatibilités en mettant à jour les dépendances, en détectant les modèles de code spécifiques à l'architecture et en recompilant les bibliothèques natives lorsque le code source est disponible. De nombreuses applications Java modernes le sont déjà Arm64-compatible.

Transformation	Langage/pile	Statut	Description
`AWS/oracle-service-bus-to-aws`	Java/intégration au sans serveur	Accès anticipé	Migrez les configurations de processus Oracle Service Bus (OSB) et BPEL vers une architecture sans AWS serveur native, en générant un TypeScript projet CDK déployable avec Amazon API Gateway, AWS Lambda et Step Functions. AWS

Transformation	Langage/pile	Statut	Description
`AWS/mulesoft-to-aws-native-java`	Java/ MuleSoft vers sans serveur	Accès anticipé	Transformez les applications MuleSoft Mule 3.x et 4.x en architectures AWS sans serveur (Amazon API Gateway, AWS Lambda et AWS Step Functions) ciblant Java 17 sur Lambda avec. AWS SnapStart Mappe les déclencheurs de flux aux sources d' AWS événements, convertit DataWeave et MEL en AWS équivalen ts hiérarchisés (VTL, Step Functions, Lambda), remplace les connecteurs par un AWS SDK pour les appels Java v2 et orchestre les flux avec Step Functions. Produit des modèles SAM, du code de gestionna ire Java Lambda, Maven pom.xml, des documents d'archite cture et des tests JUnit 5.

Transformation	Langage/pile	Statut	Description
`AWS/payshield-hsm-to-aws-payment-cryptography`	Java (HSM vers cryptographie des AWS paiements)	Généralement disponible	Migrez les applications Java du protocole de commande basé sur PayShield socket HSM de Thales vers le SDK v2 du AWS Payment Cryptography Service (APC). Couvre le mappage des commandes, la migration des clés (TR-31 et TR-34 importation, vérification KCV), la configuration des dépendances du SDK (Maven, Gradle et Ant), la suppression de l'infrastructure (pools de sockets, analyseurs de réponses), la mise à jour de l'infrastructure de test et les tests de parité.

Transformation	Langage/pile	Statut	Description
`AWS/websphere-jaxrs-to-bedrock-agentcore`	Java (WebSphere pour AgentCore)	Accès anticipé	Générez des définitions d' AgentCore outils à partir des points de terminaison REST d'une application WebSphere ou d'une application Liberty, afin que la logique métier existante puisse être appelée par les agents d'IA. La transformation lit votre code source et écrit de nouveaux fichiers dans un répertoire de sortie sans rien modifier sur place. Il trouve les points de terminaison utilisés JAX-RS à la fois dans les espaces de noms javax.ws.rs et jakarta.ws.rs, y compris EJB exposé à travers une façade. JAX-RS Pour chaque point de terminaison, il associe les paramètres et les types Java à un schéma JSON, résout la méthode HTTP et évalue sa fiabilité afin que vous sachiez ce

Transformation	Langage/pile	Statut	Description
			qu'il faut examiner. La sortie inclut un rapport de découverte, un schéma JSON par point de terminaison, des implémentations d'outils en Python et un manifeste pour les enregistrer auprès d'une AgentCore passerelle.

Analyse de la base de code

Analysez les bases de code et les portefeuilles pour planifier la modernisation. Ces transformations produisent des rapports et ne modifient pas votre code.

Transformation	Langage/pile	Statut	Description
`AWS/comprehensive-codebase-analysis`	Plusieurs langues	Généralement disponible	Effectuez une analyse statique approfondie d'une base de code pour générer une documentation hiérarchique et référencée qui combine l'analyse comportementale, la documentation architecturale et l'intelligence d'affaires, en mettant l'accent sur les informations sur la dette technique.

Transformation	Langage/pile	Statut	Description
`AWS/agentic-readiness-analysis`	Plusieurs langues	Accès anticipé	Évaluez si les systèmes sont prêts à être appelés en toute sécurité par des agents d'IA, notamment en ce qui concerne les API, l'identité, la gestion des états, l'interaction humaine et l'observabilité.
`AWS/modernization-readiness-analysis`	Plusieurs langues	Accès anticipé	Analysez les portefeuilles pour détecter les écarts de maturité liés au cloud et associez les résultats aux voies de AWS modernisation.
`AWS/portfolio-agentic-readiness-analysis`	Portfolio	Accès anticipé	Regroupez les rapports d'analyse de l'état de préparation des agents individuels sur un portefeuille d'applications afin d'identifier les blocages transversaux, les modèles de remédiation partagés et les recommandations hiérarchisées.

Transformation	Langage/pile	Statut	Description
`AWS/portfolio-modernization-readiness-analysis`	Portfolio	Accès anticipé	Regroupez les rapports d'analyse de modernisation individuels d'un portefeuille dans une feuille de route consolidée avec des vagues de migration hiérarchisées et des voies de modernisation recommandées.

Transformation	Langage/pile	Statut	Description
`AWS/business-rules-extraction`	Plusieurs langues	Accès anticipé	Cette transformation analyse statiquement une base de code monolithique afin de produire une documentation prête à être réécrite sans nécessiter de compilation, d'exécution ou de modifications du code source. Il décompose le système en domaines délimités et extrait les règles métier par domaine, les flux de travail, les préoccupations transversales et la structure de la base de données. Le résultat comprend un manifeste lisible par machine, un tableau de bord interactif et des spécifications d'implémentation indépendantes du langage par domaine pour guider la modernisation ou les réécritures complètes.

Sécurité

Corrigez les failles de sécurité dans le code source en vous basant sur les résultats du scanner.

Transformation	Langage/pile	Statut	Description
`AWS/security-issue-fixer`	Plusieurs langues	Généralement disponible	Corrigez les failles de sécurité dans le code source en vous basant sur les résultats d'un scanner tiers (résultats SARIF, JSON, CSV ou en texte brut avec des identifiants CWE, des chemins de fichiers et des numéros de ligne). N'effectue pas d'analyse ni de découverte ; il corrige uniquement les résultats fournis tout en préservan t le comportement fonctionnel. Couvre l'injection, l'authent ification défaillan te, les défaillances cryptographiques, l'autorisation, le CSRF, la désériali sation non sécurisée, le SSRF, la traversée de chemin, XXE, etc. Supporte Python JavaScript, TypeScrip

Transformation	Langage/pile	Statut	Description
			t, Java, Go, C#, .NET, C, C++ et Ruby.

Personnalisation AWS-Transformations gérées

Vous pouvez personnaliser les transformations AWS gérées pour répondre aux besoins spécifiques de votre organisation en fournissant un contexte supplémentaire via le paramètre `additionalPlanContext` de configuration.

Exemple : Personnalisation de la mise à niveau de la version 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.
```

Exemple : personnalisation de la migration du AWS SDK

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

Cas d'utilisation courants

Cette section fournit des conseils étape par étape pour les scénarios de transformation courants à l'aide de l'interface de ligne de commande AWS Transform.

Mises à niveau de l'environnement d'exécution

Lambda rend régulièrement obsolète les environnements d'exécution des anciens langages, obligeant les équipes à mettre à niveau leurs fonctions Lambda vers les versions prises en charge.

AWS Transform Custom peut automatiser ces mises à niveau à l'aide des transformations de mise à niveau des versions linguistiques AWS gérées. Par exemple, pour mettre à niveau une fonction Lambda écrite en Python 3.9 vers Python 3.13, vous devez utiliser la `AWS/python-version-upgrade` transformation. Des transformations similaires sont disponibles pour Java (`AWS/java-version-upgrade`) et Node.js (`AWS/nodejs-version-upgrade`), couvrant les langages d'exécution Lambda les plus courants.

Pour mettre à niveau une seule fonction Lambda de manière interactive, accédez à la racine du référentiel source de votre fonction et démarrez la CLI AWS Transform avec. `atx` Dans la session interactive, décrivez la mise à niveau dont vous avez besoin, par exemple, « Mettez à niveau cette fonction Lambda Python 3.9 vers Python 3.13 ». L'agent sélectionnera la transformation AWS gérée appropriée, analysera votre code, mettra à jour la syntaxe du langage, ajustera les dépendances et modernisera les appels d'API obsolètes. Vous pouvez fournir une commande de génération ou de validation telle que `pytest` l'agent `python -m py_compile *.py` puisse vérifier que le code transformé est compilé et passe les tests avec succès. Tout au long de la session interactive, vous pouvez consulter les modifications proposées par l'agent, fournir des commentaires et demander des ajustements avant d'accepter le résultat final.

Lorsque vous devez mettre à niveau les environnements d'exécution Lambda sur de nombreux référentiels, utilisez le mode non interactif pour exécuter des transformations à grande échelle. Pour chaque référentiel, appelez la CLI avec les indicateurs appropriés pour qu'elle s'exécute sans intervention de l'utilisateur. Par exemple, pour mettre à niveau une fonction Node.js 16 Lambda vers la fonction 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
```

L'`-x`indicateur exécute la transformation de manière non interactive et `-t` fait confiance à toutes les exécutions d'outils, aucune invite n'est donc requise. Vous pouvez écrire cette commande dans des dizaines ou des centaines de référentiels à l'aide d'une simple boucle shell. Une fois chaque transformation terminée, examinez le diff Git pour vérifier les modifications et exécutez votre suite de tests pour confirmer que la fonction mise à niveau fonctionne correctement. Vous pouvez également intégrer AWS Transform custom à votre CI/CD pipeline afin d'identifier en permanence les fonctions Lambda obsolètes. Cette approche permet non seulement de résoudre le problème immédiat des

environnements d'exécution obsolètes, mais également d'établir un processus continu pour détecter et mettre à niveau les fonctions avant qu'elles n'atteignent le statut de fin de support.

Les équipes de la plateforme centrale peuvent créer des campagnes via l'application Web AWS Transform pour définir la transformation, spécifier les référentiels Lambda cibles et suivre les progrès au sein de l'organisation. Pour une présentation détaillée de la création d'une solution de déploiement évolutif de niveau production à l'aide de AWS Batch, voir Création d'une solution de modernisation de code évolutive avec Transform custom. AWS

AWS Transform points de terminaison personnalisés et d'interface (AWS PrivateLink)

Vous pouvez établir une connexion privée entre votre VPC et un VPC AWS Transform personnalisé en créant un point de terminaison VPC d'interface. Les points de terminaison de l'interface sont alimentés par AWS PrivateLinkune technologie qui vous permet d'accéder en privé à des services AWS Transform personnalisés sans passerelle Internet, périphérique NAT, connexion VPN ou Direct Connect connexion. Le trafic entre votre VPC et le AWS Transform custom ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux.

Pour de plus amples informations, consultez Points de terminaison VPC (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

> **Note**
>
> - Vous devez activer AWS PrivateLink l'intégration pour Amazon S3 car AWS Transform Custom effectue des appels d'API S3. Pour obtenir des instructions détaillées, consultez la AWS PrivateLink documentation relative à Amazon S3. Si vous rencontrez des problèmes d'accès S3 lors de l'utilisation de la AWS Transform personnalisation, consultez notre guide de dépannage.
> - Si vous n'utilisez pas la fonctionnalité DNS AWS PrivateLink privé (voir DNS privé), vous devez :
>   - Configurer le routage vers les points de terminaison de l'interface VPC (voir la documentation du routage vers les points de terminaison de l'interface VPC)

- Définissez la variable d'`ATX_CUSTOM_ENDPOINT`environnement pour spécifier votre domaine personnalisé, par exemple :

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

Considérations relatives à AWS Transform points de terminaison VPC personnalisés

Avant de configurer un point de terminaison VPC d'interface à des fins AWS Transform personnalisées, assurez-vous de consulter les propriétés et les limites du point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

AWS Transform custom prend en charge les appels à toutes ses actions d'API via le point de terminaison de l'interface.

Conditions préalables

Avant de commencer toute procédure ci-dessous, vérifiez que vous disposez des éléments suivants :

- Un AWS compte doté des autorisations appropriées pour créer et configurer des ressources.
- Un VPC déjà créé dans votre AWS compte.
- Connaissance des AWS services, en particulier Amazon VPC AWS Transform et Custom.

Création d'un point de terminaison VPC d'interface pour AWS Transform personnalisé

Vous pouvez créer un point de terminaison VPC pour le service AWS Transform personnalisé à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez les points de terminaison VPC suivants à AWS Transform personnaliser à l'aide de ce nom de service :

- com.amazonaws. *region*.transform-personnalisé

Remplacez *region* par AWS Region dans laquelle vous souhaitez utiliser une CLI AWS Transform personnalisée, par exemple com.amazonaws.us-east-1.transform-custom.

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour AWS Transform personnalisé

Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès aux AWS Transform paramètres personnalisés. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : politique de point de terminaison VPC pour AWS Transform personnaliser les actions

Voici un exemple de politique de point de terminaison AWS Transform personnalisée. Lorsqu'elle est attachée à un point de terminaison, cette politique accorde l'accès aux actions AWS Transform personnalisées répertoriées pour tous les principaux sur toutes les ressources.

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

Utilisation d'un ordinateur local pour se connecter à un AWS Transform point de terminaison personnalisé

Cette section décrit le processus d'utilisation d'un ordinateur sur site pour établir une connexion AWS Transform personnalisée via un AWS PrivateLink point de terminaison de votre AWS VPC.

1. Créez une connexion VPN entre votre appareil sur site et votre VPC.
2. Créez un point de terminaison VPC d'interface à AWS Transform personnaliser.
3. Configurez un point de terminaison Amazon Route 53 entrant. Cela vous permettra d'utiliser le nom DNS de votre point de terminaison AWS Transform personnalisé à partir de votre appareil local.

Résolution des problèmes

Cette section fournit des conseils pour résoudre les problèmes courants liés à AWS Transform custom.

Emplacements des journaux

AWS La CLI Transform gère les journaux aux emplacements suivants :

Journaux de conversations :

Linux and macOS

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

Windows

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

Ces journaux contiennent l'historique complet des conversations pour le débogage d'exécutions de transformations spécifiques.

Journaux des sous-agents :

Linux and macOS

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

Windows

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

Ces journaux contiennent les résultats des sous-agents générés par l'agent principal lors des transformations. Il n'est pas nécessaire de gérer directement les sous-agents.

Journaux de débogage des développeurs :

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
```

Ces journaux fournissent des informations détaillées sur les opérations et les erreurs de la CLI. Chaque fichier journal est limité à 5 Mo avant d'être transféré. Ce répertoire peut contenir plusieurs journaux de débogage, tels que debug1.log et debug2.log.

Problèmes courants

Problèmes d'installation :

Si l'installation échoue, assurez-vous d'avoir installé Node.js 22 ou une version ultérieure :

```
node --version
```

Node.js Téléchargez-le depuis https://nodejs.org/en/download si nécessaire.

Problèmes d'authentification :

Vérifiez que vos AWS informations d'identification sont correctement configurées :

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

Assurez-vous que votre utilisateur ou votre rôle IAM dispose des `transform-custom:*` autorisations requises.

Problèmes de connectivité réseau :

Si vous rencontrez des erreurs de connexion, vérifiez l'accès réseau aux terminaux requis :

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

Si vous travaillez dans un environnement où Internet est restreint, mettez à jour les règles de pare-feu pour autoriser ces URL.

Problèmes de configuration des régions :

Si vous rencontrez des erreurs liées à la région :

- Vérifiez que votre région est prise en charge
- Vérifiez les variables d'environnement susceptibles de remplacer votre configuration : `echo $AWS_REGION $AWS_DEFAULT_REGION`
- Vérifiez la configuration de votre région : `aws configure get region`
- Mettez à jour votre région si nécessaire : `aws configure set region <your-region>`
- Consultez les journaux de débogage pour plus de détails sur la résolution des régions

Problèmes liés à Git :

Assurez-vous que Git est installé et que votre dépôt est sous le contrôle de source git :

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

AWS Transform custom nécessite que les référentiels soient sous le contrôle de source git.

Problèmes liés à l'exécution de la transformation :

Si une transformation échoue :

1. Consultez les journaux de conversation sur `~/.aws/atx/custom/<conversation_id>/logs/`
2. Vérifiez les échecs de génération ou de test dans la sortie de transformation
3. Vérifiez que la commande build est correcte pour votre projet
4. Essayez d'exécuter la transformation en mode interactif pour fournir des commentaires

Problèmes de reprise de conversation :

Si vous ne pouvez pas reprendre une conversation :

- Vérifiez que la conversation date de moins de 30 jours
- Vérifiez que l'identifiant de conversation est correct
- Assurez-vous de disposer d'une connectivité réseau

Obtention de support

Pour obtenir de l'aide supplémentaire, consultez la section AWS Support via la AWS console.

Lorsque vous ouvrez un ticket d'assistance, incluez :

- Journaux de conversation provenant de `~/.aws/atx/custom/<conversation_id>/logs/`
- Le sous-agent se connecte depuis `~/.aws/atx/custom/<conversation_id>/logs/subagents/`
- Journaux de débogage à partir de `~/.aws/atx/logs/`
- Étapes à suivre pour reproduire le problème
- AWS Transformer la version de la CLI (`atx --version`)

Problèmes d'accès à S3

Le service personnalisé AWS Transform distribue des URL pré-signées S3 pour faciliter le chargement et le téléchargement des fichiers to/from de transformation potentiellement volumineux sur les machines clientes. Cela signifie que non seulement la CLI interagit avec les points de terminaison du service AWS Transform, mais qu'elle interagit également avec les points de

terminaison du service S3. Ces interactions utilisent des URL pré-signées, de sorte que les informations d'identification IAM de votre client ne nécessitent aucune autorisation S3, mais parfois, les configurations du serveur proxy de votre machine locale et les politiques des terminaux VPC S3 de votre réseau peuvent restreindre ce trafic.

Consultez les messages d'erreur the section called “Emplacements des journaux” pour plus de détails afin d'aider à provoquer toute défaillance de l'outil ou tout refus d'accès S3 lié au téléchargement et au chargement de fichiers de transformation.

Si vous utilisez un VPN/Proxy serveur qui exploite les variables d'`no_proxy`environnement `https_proxy` et, pensez à ajouter les valeurs suivantes à la valeur de votre variable d'`no_proxy`environnement afin de contourner le proxy pour les points de terminaison des services personnalisés S3 et AWS Transform, par exemple :

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 vous utilisez un AWS PrivateLink pour Amazon S3 dans votre VPC, il se peut qu'une politique soit définie pour restreindre le trafic S3. Assurez-vous que votre politique relative aux points de terminaison S3 VPC autorise `GetObject` et `PutObject` gère les compartiments appartenant au service personnalisé AWS Transform. Cela peut être accompli en ajoutant la déclaration suivante à votre politique de point de terminaison VPC :

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

`Deny`Les déclarations explicites contenues dans les politiques ont priorité sur `Allow` les déclarations. Consultez les politiques S3 VPC Endpoint pour `Deny` détecter les déclarations susceptibles de restreindre l'accès.

AWS Modifier l'historique des versions de la CLI

Consultez le tableau suivant pour plus de détails sur les versions actuelles et passées de la CLI AWS Transform. Le tableau inclut la version, la date de publication et les notes de publication pour chaque version.

Version	Date de publication	Notes de mise à jour
3.11.0 (dernière version)	19 août 2026	• Ajouté `--repos` `atx ct remediation create` pour la correction de plusieurs dépôts en une seule commande. • Ajouté `--transformation-name` `atx ct remote remediation` pour exécuter une correction directement à partir d'une définition de transformation sans nécessiter les résultats existants. • Ajout d'`--json`une sortie `atx ct analysis run` pour obtenir des résultats lisibles par machine. • Ajout d'un récapitulatif des coûts des minutes d'agent à `atx ct analysis get` et`atx ct remediation status` . • Ajout d'une exportation de fichiers locale pour le mode d'exécution `atx ct remote provision` à sec : les AWS CloudFormation modèles générés sont désormais écrits dans un fichier local (remplacez l'emplacement par`--out-dir`) pour être révisés avant le déploiement. • Correction d'un problème à cause duquel les commandes kill-family émises par l'agent pouvaient mettre fin au propre processus de la CLI. Les commandes concernées incluent `pkill -f` `nodexargs kill`, et`find -exec kill`. L'`shell`outil les compare désormais au processus de la CLI et à sa chaîne ancêtre avant de les exécuter. • Correction d'un problème à cause duquel la découvert e des GitLab sources utilisait les rubriques du référentiel comme champ de langue. Cela pourrait entraîner l'échec de l'enregistrement des référentiels dont les rubriques

Version	Date de publication	Notes de mise à jour
		contiennent des caractères spéciaux. La langue n'est plus déduite des sujets. • Correction d'un problème à cause duquel `atx ct` les commandes qui échouaient pouvaient se fermer silencieu sement avec une sortie vide. La CLI affiche désormais des messages d'erreur exploitables. • Correction d'un problème à cause duquel la finalisation d'une analyse locale pouvait entraîner une erreur lorsque le service signalait que l'exécution était déjà terminée. • Correction d'un problème en raison duquel `atx ct remote update` l'infrastructure du répartiteur partagé n'était pas mise à jour. Par conséquent, la mise à niveau de la CLI et l'exécution `remote update` ont continué à utiliser le répartiteur précédemment déployé. `remote update`réconcilie maintenant le répartiteur. • Correction d'un problème à cause duquel les exécution s d'analyses à distance (Amazon EC2 ou AWS Batch) pouvaient signaler un faux échec. Cela s'est produit alors que tous les référentiels d'une exécution limitée étaient déjà terminés sur le service. • Correction d'un problème à cause duquel la découverte de `atx ct` référentiels pouvait supprimer silencieusement les référentiels rejetés par le service. L'interface de ligne de commande compte et signale désormais les référenti els ignorés (« N référentiels ont été ignorés »), avec un récapitulatif des dépassements pour les grandes entrepris es. • Les messages d'erreur et d'avertissement destinés à l'utilisa teur ont été modifiés pour faire référence à AWS Transform et indiquer clairement la prochaine étape (actualiser les informations d'identification, réessayer ou contacter le

Version	Date de publication	Notes de mise à jour
		support). Les messages ne font plus référence à des noms de services internes.

Version	Date de publication	Notes de mise à jour
3.10.0	10 août 2026	• Ajout de la prise en charge `background=true` dans l'`shell`outil des commandes de longue durée ou non terminales (serveurs de développement, observateurs de build,). `tail -f` Il revient immédiatement avec un identifia nt de processus au lieu d'attendre la fin de la commande. Il est possible de suivre jusqu'à 5 processus en arrière-plan à la fois. • Ajout de nouveaux `check_background_shell` `stop_background_shell` outils pour surveiller et mettre fin aux processus en arrière-plan. • Ajouté `llmConfig` à la liste des autorisations de configura tion de la CLI, permettant aux utilisateurs de personnaliser les paramètres LLM via des fichiers de configuration. • Ajouté `--mode aws-managed` à `atx ct schedule create` et pour exécuter des analyses `atx ct remote analysis` à l'aide d'une AWS infrastructure entièrement gérée sans provisionner vos propres ressources Amazon EC2 ou AWS Batch. • Ajout `--schedule-id` `--display-name` d'options permettant de filtrer `atx ct analysis` les résultats par calendrier et d'identifier les analyses à l'aide d'une étiquette lisible par l'homme. • Ajout de la prise en `--region` charge `--mode aws-managed` des opérations, vous permettant de cibler une AWS région spécifique pour les analyses gérées. • Fiabilité améliorée des `delete` commandes `atx ct schedule get` `enabledisable`,, et. • Amélioration de la précision et de la cohérence des `atx ct schedule list` résultats. • Ajouté `--stack-name` à `atx ct schedule create` pour épingler un calendrier à une pile cible spécifique.

Version	Date de publication	Notes de mise à jour
		• Ajout de nouvelles `atx ct analysis get-artifact` commandes `atx ct analysis list-artifacts` et permettant de récupérer les artefacts de sortie des analyses d'infrastructure AWS gérées. • Correction d'un problème en raison duquel les processus d'arrière-plan suivis par la CLI n'étaient pas correctement interrompus à la sortie de la CLI, ce qui pouvait laisser des processus orphelins en cours d'exécution. • Correction d'un problème à cause duquel les `--batch-name` indicateurs `--workers` et `atx ct schedule create` ne étaient pas rejetés lorsqu'ils étaient utilisés avec`--mode aws-managed` . • Correction d'un libellé incohérent dans les messages d'erreur « Impossible de trouver le calendrier ». • Correction d'un problème en raison duquel les remplacem ents de terminaux n'étaient pas résolus de manière cohérente dans toutes les commandes de l'interface de ligne de commande. • Amélioration de la précision de la détection des noms de calendrier dupliqués. • Correction d'un problème qui `atx ct remote analysis --resume` empêchait la reprise d'un traitement par lots partiellement terminé. L'indicateur est maintenant`--resume-incomplete` , qui réexécute uniquement les référentiels qui ne se sont pas terminés (échec, interruption ou pas encore démarré) et ignore ceux qui sont terminés. • Mise à jour `atx ct schedule --help` pour inclure les offres d'exécution de AWS Managed Analysis.

Version	Date de publication	Notes de mise à jour
3.9.0	31 juillet 2026	• Amélioration des performances des définitions `atx custom def export-ki-markdown` de transformation contenant de nombreux éléments de connaissances. La commande n'effectue plus d'appel de service redondant pour chaque élément de connaissance. Elle s'exécute donc beaucoup plus rapidement et n'expire plus sur les définitio ns volumineuses. Des cas où une exportation pouvait omettre des éléments de connaissance ou signaler un total incohérent ont également été corrigés. • Correction d'un problème à cause duquel les analyses de préparation des agents et de préparation à la modernisa tion exécutées `atx ct analysis run` pouvaient ne rapporter aucun résultat pour certains formats de rapports. Les résultats sont désormais récupérés de manière fiable. • Correction d'un problème en raison duquel les analyses planifiées créées avec `atx ct schedule create` against GitLab, Bitbucket ou des sources locales pouvaient échouer à chaque exécution lors de la tentative de récupération des informations d'identification. Le fournisseur source est désormais déterminé automatiquement à partir de votre source enregistrée, et l'`--provider` option n'est plus requise. • Correction d'un problème à cause duquel les analyses de sécurité exécutées dans des environnements distants (AWS Batch ou EC2) pouvaient indiquer à tort que l'agent de sécurité n'était pas configuré. La CLI détecte désormais correctement un agent de sécurité configuré et signale plus facilement les erreurs d'identification ou de limitation transitoires.

Version	Date de publication	Notes de mise à jour
3.8.0	29 juillet 2026	• L'`--recurrence` option à `atx ct schedule create` a été ajoutée afin que vous puissiez définir la cadence d'un planning en termes simples (`dailyweekly:<MONDAY..SUNDAY>` , ou`monthly:<1..28>`) au lieu d'écrire une expression cron brute. • L'`--existing-scheduler-role-arn` option a été ajoutée à`atx ct remote provision` , afin que vous puissiez réutiliser un rôle IAM que votre administrateur a déjà créé pour le planificateur au lieu de demander à la CLI d'en créer un lors du provisionnement. • L'`--existing-instance-profile-name` option a été ajoutée à`atx ct remote provision --mode ec2`, afin que vous puissiez joindre un profil d'instance IAM que votre administrateur a déjà créé au lieu de laisser la CLI créer le rôle de transformation et le profil d'instance. • Amélioration des instructions de sélection des transformations, de sorte qu'elles utilisent désormais les métadonnées de détection, telles que la gravité et les critères de correspondance, lorsqu'elles sont disponibles. Cela permet de mettre en évidence les transformations les mieux adaptées à votre projet et leur priorité relative. • Correction d'un problème en raison duquel l'annulation d'une analyse à distance planifiée arrêtait les conteneurs en cours d'exécution mais pouvait laisser l'analyse bloquée`running`. L'annulation marque désormais de manière fiable l'analyse comme étant annulée. • Correction d'un problème `atx ct schedule delete` qui pouvait laisser un enregistrement d'analyse persistant. La suppression d'une planification supprime désormais également l'analyse planifiée sous-jacente.

Version	Date de publication	Notes de mise à jour
3.7.0	22 juillet 2026	• Ajout du groupe de `atx ct remote` commandes pour exécuter des analyses et des corrections à distance sur EC2 ou AWS Batch. Vous pouvez provisionner, mettre à jour et démanteler l'infrastructure d'exécution à distance, vérifier l'état des soumissions, détecter les piles déployées et gérer les informations d'identification des sources dans AWS Secrets Manager. • Ajout du groupe de `atx ct schedule` commandes pour les tâches récurrentes d'analyse et de correction planifiée s. Vous pouvez créer, répertorier, activer, désactiver et supprimer des planifications (les options de tâche reflètent `remote analysis` et`remote remediation`), en plus `setup` et `teardown` pour l'infrastructure du planificateur. Les plannings capturent les ensembles de sources locales au moment de leur création. • Amélioration `atx ct analysis run` pour utiliser les règles de correspondance tech-debt-quick à partir du registre des packages de transformation. • `atx ct`Commandes de longue durée améliorées pour afficher les résultats de progression, y compris la progressi on par dépôt pendant les exécutions d'analyse (y compris les analyses de sécurité) et les raisons d'échec par dépôt dans l'état de la correction. • Correction de plusieurs problèmes de fiabilité de l'exécuti on à distance. L'état EC2 affiche désormais les résultats et les résultats des demandes d'extraction, correspondant à Batch ; les mises à jour EC2 n'échouent plus sur les piles dépourvues de nouveaux paramètres ; et des correctifs supplémentaires concernent les codes de sortie, la gestion des transformations, la détection basée sur les balises et la sortie JSON.

Version	Date de publication	Notes de mise à jour
3.6.0	17 juillet 2026	• Ajout de la `atx custom def learnings` sous-commande, qui ouvre une session TUI interactive pour afficher et gérer les apprentissages générés automatiquement pour une définition de transformation basée sur les exécutions précédentes. • Ajout de la collecte de télémétrie d'utilisation lors de l'exécution de la transformation. Pour désactiver la télémétrie, définissez la variable d'`ATX_DISABLE_TELEMETRY=true` environnement. Pour de plus amples informations, veuillez consulter Télémétrie d'utilisation. • Correction d'un problème sous Windows où les opérations sur les fichiers utilisant des chemins ~ (répertoire de base) étaient résolues vers un répertoire inattendu. Cela a provoqué des read/write défaillances de fichiers au cours d'une session. • Correction d'un problème à cause duquel les noms de serveurs et d'outils MCP contenant des caractères spéciaux pouvaient provoquer des échecs de connexion. La CLI nettoie désormais automatiquement les noms pour n'utiliser que des caractères valides.

Version	Date de publication	Notes de mise à jour
3.5.0	8 juillet 2026	• Ajout de la prise en charge native de Windows. Vous pouvez désormais exécuter les commandes AWS Transform Custom directement sous Windows. (Les `atx ct` commandes ne sont pas encore prises en charge sous Windows) • Ajout d'entrées de pilotage pour `atx ct analysis run` que les analyses de préparation des agences et de préparation à la modernisation reflètent vos préférences. Utilisez-le `--context` pour le cadrage stratégique, `--agent-scope` pour configurer l'accès des agents afin qu'ils soient prêts à devenir des agents, `--prefer` et/ou pour orienter les recommandations `--avoid` de modernisation vers des technologies spécifiques ou les éloigner de celles-ci. • Les définitions de transformation au format skill peuvent désormais inclure un `scripts/` dossier, ce qui vous permet de regrouper des scripts d'assistance avec vos références `SKILL.md` et vos références. • Ajouté `--wait` à`atx ct remediation create` , qui attend la fin de la correction. • Ajout du mode headless pour une exécution en un seul coup. Exécutez `atx -x "prompt" -t` pour transmettre une invite, obtenir une réponse et quitter sans aucune invite interactive. Le mode Headless nécessite de faire confiance à tous les outils.

Version	Date de publication	Notes de mise à jour
3.4.1	2 juillet 2026	• Correction d'un problème de session interactive introduit par la version 3.4.0. Une fois que l'agent a fini de répondre, l'interface de ligne de commande peut rester sur l'invite « Thinking » (représentée par des points de suspension dans l'interface utilisateur) au lieu de revenir à l'invite de saisie. La CLI vous renvoie désormais à l'invite de saisie après chaque réponse.

Version	Date de publication	Notes de mise à jour
3.4.0 (non recommandé)	29 juin 2026	⚠ Problème connu Dans les sessions interactives, l'interface de ligne de commande peut rester activée sur l'invite « Réfléchir » (représentée par des points de suspension dans l'interface utilisateur) une fois que l'agent a fini de répondre. Cela vous empêche de saisir votre prochain message. Pour résoudre ce problème, passez à la version 3.4.1 ou ultérieure en exécutant`atx update`. • Ajout `atx ct schema` d'un manifeste lisible par machine de la surface de `atx ct` commande complète pour la création de scripts et l'automatisation. • Ajout de la validation de l'étendue des jetons lorsque vous ajoutez ou mettez à jour une source, ce qui permet de faire apparaître immédiatement des problèmes d'identification ou d'autorisation au lieu d'échouer plus tard lors de l'analyse. • Amélioration des pull requests de remédiation automatique pour inclure la recherche de contexte et prendre en charge le mode brouillon pour des PR plus révisables. • Amélioration du feedback de progression de l'interface de ligne de commande avec un contexte en temps réel sur l'activité en cours, les minutes estimées des agents et l'activité des sous-agents. • Ajout de l'identité de l'auteur de la validation des points de contrôle configurables via les variables d'`ATX_GIT_COMMITTER_EMAIL` environnement `ATX_GIT_COMMITTER_NAME` et. • Diverses petites corrections de bugs et améliorations.

Version	Date de publication	Notes de mise à jour
3.3.0	18 juin 2026	• Ajout d'une cohérence `--json` et d'`--help`un support pour toutes `atx ct` les commandes. • Correction de la configuration de l'agent de sécurité, de sorte que l'espace agent soit créé lors de la configuration et supprimé lors du démontage. • Diverses petites corrections de bugs et améliorations.
3.2.0	15 juin 2026	• Ajout de commandes de modernisation continue (`atx ct`) à la distribution CLI standard pour tous les utilisateurs. • Amélioration de l'exécution des sous-agents pour afficher un spinner « Thinking... » en attendant les réponses du serveur, fournissant un retour visuel clair indiquant que le travail est en cours. • Spinner amélioré permettant de redémarrer automatiq uement avec « Working on it... » après 3 secondes de silence après la sortie de l'agent, afin que le terminal n'apparaisse jamais figé entre les étapes de traitement. • Spinner intelligent amélioré avec une animation scintillante subtile pour une apparence visuelle plus soignée.

Version	Date de publication	Notes de mise à jour
3.1.0	3 juin 2026	• Ajout d'une variable d'`ATX_MAX_VALIDATION_LOOPS` environnement pour configurer un maximum de boucles de validation. • La vérification des mises à jour corrigées n'affiche plus de faux avertissements « mise à jour disponible » lorsque la version installée est déjà plus récente que la version du registre. • Le correctif `delete --transformation-name ""` n'affiche plus d'invite de confirmation absurde ; les valeurs vides sont désormais rejetées avec une erreur de validation claire. • Les sous-commandes non reconnues corrigées affichent désormais une « commande inconnue » au lieu d'un message d'erreur interne confus. • Comparaison de versions fixe pour utiliser la comparais on numérique au lieu de l'inégalité des chaînes pour les contrôles de mise à jour.

Version	Date de publication	Notes de mise à jour
3.0.0	21 mai 2026	• Ajout d'une validation des noms par transformation avant le vol qui suggère des noms similaires dans votre registre lorsqu'aucun nom n'est trouvé, ce qui permet de détecter les fautes de frappe sans avoir besoin d'une commande de liste distincte. • Ajout d'explications facultatives pour les commandes shell, montrant ce qu'elles font et pourquoi. • Bannière des paramètres de confiance améliorée pour inclure plus d'informations sur les autorisations des outils. • Ajout d'une bannière désactivant l'apprentissage lors de l'utilisation de l'indicateur Ne pas apprendre, donnant de la visibilité à la fonctionnalité d'apprentissage et à la manière de l'activer. • Changement de rupture : Node.js 22 ou version ultérieure est désormais requise. Effectuez la mise à niveau https://nodejs.org/ si vous utilisez une ancienne version.

Version	Date de publication	Notes de mise à jour
2.0.0	14 mai 2026	• Ajout de la prise en charge des serveurs MCP distants : connexion aux serveurs MCP HTTP et HTTPS avec repli SSE automatique, authentification par jeton Bearer avec extension des variables d'environnement dans les en-têtes et prise en charge du proxy (). HTTP_PROXY/HTTPS_PROXY • Ajout d'`atx resume`une sous-commande comme alias pour`atx --resume`. • Ajout d'`grep`un outil pour la recherche de texte dans plusieurs fichiers avec contrôle de sortie : prend en charge les modèles regex, le filtrage global des fichiers, la recherche sans distinction majuscules/minuscules, les depth/result limites configurables et la troncature de sortie. • Implémentation améliorée du MCP pour utiliser le SDK MCP standard pour un comportement plus cohérent et une prise en charge plus facile des futures fonctionnalités du MCP. • Amélioration de la gestion des sorties du shell : la sortie est désormais tronquée gracieusement à 30 000 caractères par flux au lieu de provoquer une erreur matérielle, préservant ainsi le début et la fin de la sortie pour le contexte. • Correction d'un problème à cause duquel les touches Ctrl +C pouvaient quitter prématurément l'interface de ligne de commande au Linux/macOS lieu d'abandonner l'opération en cours et de revenir à l'invite. • Message de rejet de confiance fixe pour afficher une raison spécifique pour laquelle la confiance n'est pas disponible, distincte de la raison pour laquelle la commande nécessitait une autorisation. • Correction d'un avertissement de commande dangereuse qui ne mentionnait plus la confiance lorsque la commande est entrée. `alwaysPromptCommands`

Version	Date de publication	Notes de mise à jour
1.10.0	29 avril 2026	• Des descriptions d'outils améliorées avec des conseils multi-outils, aidant l'agent à choisir l'outil le mieux adapté à chaque tâche et réduisant l'utilisation inutile de l'interpréteur de commandes. • Ajouté `alwaysPromptCommands` `trust-settings.yaml` : configurez les modèles de commandes shell qui nécessitent toujours une autorisation explicite, quels que soient les paramètres de confiance. Supporte les caractères génériques et les correspondances avec chaque sous-commande dans les expressions composées . `trustedShellCommands` peut annuler ces modèles. Non appliqué en mode non interactif pour éviter de casser les pipelines automatisés. • Les chemins relatifs fixes ne sont pas résolus en chemins absolus.
1.9.0	23 avril 2026	• Amélioration des instructions d'approbation des outils : chaque option indique désormais ce qu'elle fait en ligne, un message « Pourquoi » explique pourquoi une approbation est nécessaire et la confirmation de confiance inclut un indice sur la `trust-settings.yaml` nécessité d'une confiance permanente.
1.8.0	16 avril 2026	• Le préfixe de sortie de l'agent a été modifié, passant de `>` à `ATX:` pour une distinction visuelle plus claire entre l'entrée utilisateur et la sortie de l'agent. • Correction de l'affichage de la commande de reprise lorsque les nouvelles tentatives de la CLI sont épuisées. • CV fixe à partir d'un répertoire de travail différent. En mode interactif, demande le chemin à corriger ; en mode non interactif, échoue rapidement avec une erreur descriptive.

Version	Date de publication	Notes de mise à jour
1.7.1	9 avril 2026	• Correction d'un échec de connexion SSO (« Jeton de session introuvable ou non valide ») lorsque la région du fournisseur d'informations d'identification diffère de celle du profil. `sso_region` • Correction de la mise en cache des informations d'identif ication afin que les sessions de longue durée n'échouent plus lors de la rotation des informations d'identification sur le disque.
1.7.0	2 avril 2026	• Correction d'une `exec` commande pour quitter avec le code 1 en cas d'erreur de validation d'entrée, ce qui rend la CLI fiable dans les scripts et les CI/CD pipelines. • Ajout de l'affichage des messages d'avertissement du service. • Ajout de la prise en charge rapide du MFA pour les profils AWS d'identification. • Correction des appels d'identification STS pour respecter les paramètres du proxy HTTP (S).
1.6.0	18 mars 2026	• Ajout d'une `--limit <minutes>` option permettant de définir un budget de minutes `exec` et de `interactive` commandes pour les agents. Lorsque la limite est atteinte, la CLI affiche l'utilisation et sort avec des instructions de reprise. • Correction de l'enregistrement du message initial de l'utilisa teur dans les journaux de conversation.
1.5.0	11 mars 2026	• Ajout de la prise en charge de l'exécution simultanée de tâches, permettant des transformations plus rapides. • Ajout d'un affichage des minutes d'utilisation des agents à la fin de chaque conversation et d'une `/usage` commande en mode interactif pour vérifier l'utilisation à tout moment.

Version	Date de publication	Notes de mise à jour
1.4.0	2 mars 2026	• Amélioration des messages d'erreur lors de l'enregistrement de définitions de transformation avec des fichiers non pris en charge. • Ajout d'un délai d'attente aux appels de service pour éviter que la CLI ne se bloque lorsque la connexion est interrompue. • Le processus CLI fixe se bloque une fois terminé avec succès. • Correction de la validation de la région lors de la reprise des conversations.
1.3.0	19 février 2026	• Suppression de la restriction pour les chemins de serveur MCP : les utilisateurs peuvent désormais spécifier n'importe quel chemin pour la `command` propriété dans la configuration MCP. • Amélioration de la stabilité des connexions aux serveurs MCP.
1.2.0	9 février 2026	• Ajout de la prise en charge de la configuration du proxy via des variables d'environnement (`https_proxy no_proxy`,, etc.). • Améliorations générales de la stabilité et corrections de bugs.
1.1.1	16 janvier 2026	Corrections de bogues et améliorations de la stabilité.
1.1.0	13 janvier 2026	Ajout de la prise en charge de la configuration des régions AWS CLI, de vérifications précoces de validation des informations d'identification et d'une fonctionnalité de reprise de campagne fixe.
1.0.1	18 décembre 2025	Des arrêts en douceur, des journaux d'erreurs plus propres et des améliorations générales.

Version	Date de publication	Notes de mise à jour
1.0.0	1er décembre 202	Version initiale de la CLI AWS Transform.

AWS Transformez la modernisation continue

Qu'est-ce que AWS Transformer la modernisation continue ?

AWS La modernisation continue de Transform permet d'analyser et de corriger vos référentiels de code source. Vous pouvez connecter GitHub des organisations, des GitLab groupes, des espaces de travail Bitbucket et des référentiels locaux, puis exécuter des analyses automatisées pour identifier la dette technique, les failles de sécurité, les opportunités de modernisation et l'état de préparation des agents sur l'ensemble de votre base de code.

Toutes les analyses et mesures correctives sont exécutées sur votre ordinateur à Compte AWS l'aide de vos informations d'identification. Votre code source reste sous votre contrôle.

> **Note**
>
> Nous vous recommandons de commencer par le plug-in Kiro Power ou agent. La compétence de l'agent orchestre la configuration, l'intégration et l'utilisation continue de la modernisation continue, y compris le provisionnement de l'infrastructure, la configuration des sources, l'exécution des analyses, le triage des résultats et la correction. Pour obtenir des instructions d'installation, consultez Outils pour développeurs.

Principales fonctionnalités

AWS La modernisation continue de Transform fournit les fonctionnalités suivantes :

- Analyse de la dette technologique : analysez les référentiels pour détecter les dépendances obsolètes, les failles de sécurité, les problèmes de qualité du code et les opportunités de modernisation. Effectuez des analyses rapides des métadonnées des manifestes de packages ou effectuez une analyse complète au niveau du code. Définissez des critères d'analyse personnalisés à l'aide de définitions de transformation adaptées à votre environnement.
- Remédiation autonome : générez des pull requests validées à grande échelle. Chaque résultat peut être corrigé automatiquement à l'aide de la définition de transformation qui lui est associée. La correction crée des branches et les ouvre PRs/MRs automatiquement sur GitHub GitLab, et Bitbucket.

- Rapports : générez des rapports HTML présentant les résultats par gravité, référentiel et type d'analyse. Suivez les progrès de la remédiation et trouvez des solutions au fil du temps.
- Surveillance continue — Planifiez des analyses récurrentes pour surveiller en permanence votre portefeuille afin de détecter de nouveaux problèmes. Exécutez-les sur une AWS Transform-managed infrastructure sans configuration, ou sur une pile Amazon EC2 ou Batch provisionnée à l'aide d'Amazon EventBridge Scheduler. Configurez des cadences quotidiennes, hebdomadaires ou mensuelles.

Types d'analyses

AWS La modernisation continue de Transform prend en charge les types d'analyse suivants pour répondre à vos besoins de modernisation.

Type	Description
`rapid-techdebt-analysis`	Analyse rapide des manifestes de packages (`pom.xml`,, `package.json requirements.txt`) uniquement basée sur les métadonnées pour identifier les versions obsolètes et les dépendances obsolètes. N'analyse pas le code source.
`tech-debt-comprehensive`	Analyse approfondie de la dette technique au niveau du code à l'aide de l'agent AWS Transform. Examine le code source pour identifier les modèles d'endettement, les problèmes de qualité du code, les problèmes d'architecture et les opportunités d'amélioration.
`security`	Vulnérabilité de sécurité et détection du CVE à l'aide du AWS Security Agent. Analyse le code source et les dépendances à la recherche de vulnérabilités connues, de modèles de codage non sécurisés et de faiblesses exploitables. Nécessite une configuration d'infrastructure unique.

Type	Description
`agentic-readiness`	Évaluation de l'état de préparation à l'intégration de l'IA et des agents Note 56 critères répartis dans cinq catégories : infrastructure et plateforme, architecture des applications, fondements des données Identity/Security/Governance, et opérations et observabilité.
`modernization-readiness`	Évaluation des opportunités de modernisation du cloud. Évalue l'état de préparation sur les plans de l'infrastructure, des applications, des données, de la sécurité et des opérations. Identifie les candidats pour la conteneurisation, la migration sans serveur et les mises à niveau de la plateforme.
`custom`	Exécutez n'importe quelle définition de transformation (TD) en tant qu'analyse. Utilisez ce type pour définir vos propres critères d'analyse ou pour exécuter des transformations AWS gérées non couvertes par les types intégrés.

Comprendre les concepts clés

Sources

Une source indique la localisation de vos référentiels en cours de modernisation. Types de sources pris en charge :

- GitHub— Organisations disposant de jetons d'accès personnels (classique)
- GitLab— Groupes ou utilisateurs, y compris les instances auto-hébergées
- Bitbucket — Espaces de travail (cloud) ou projets (centre de données)
- Local — Répertoires parents contenant des dépôts git

Référentiels

Les référentiels sont découverts en scannant les sources. Après la découverte, vous pouvez filtrer par source, étiquettes ou autres critères, appliquer des libellés pour l'organisation (équipe, priorité, vague de migration) et cibler des référentiels spécifiques à des fins d'analyse ou de correction.

Analyses

Une analyse est une analyse d'un ou de plusieurs référentiels à l'aide d'un type d'analyse spécifique. Chaque analyse produit des résultats qui permettent d'identifier les problèmes liés à votre code. Vous pouvez exécuter des analyses à la demande ou les programmer pour qu'elles s'exécutent automatiquement. Les types d'analyse incluent l'analyse rapide de la dette technologique, l'analyse complète de la dette technologique, la sécurité, la préparation des agences, la préparation à la modernisation et la personnalisation. Chaque analyse suit son statut (en attente, en cours, terminée, annulée ou échouée) et les référentiels qu'elle a analysés.

Résultats

Les résultats sont les résultats de l'analyse. Chaque découverte inclut la gravité (élevée, moyenne ou faible), l'état (ouvert, ignoré ou obsolète) et la transformation qui peut y remédier (si elle est réparable automatiquement). Les nouvelles découvertes commencent comme ouvertes. Les utilisateurs peuvent rejeter les résultats en indiquant une raison. Re-analysis marque automatiquement les résultats résolus comme obsolètes.

Remédiations

Les mesures correctives appliquent des définitions de transformation pour corriger les résultats. Trois modes : basé sur les résultats (chaque résultat utilise sa propre transformation fixe), TD override (remplace la définition de la transformation pour des résultats spécifiés) et TD direct (exécute une transformation sur un référentiel sans résultats). La sortie dépend du fournisseur source (GitHub PR, GitLab MR, Bitbucket PR ou branche locale).

Définitions des transformations

Une définition de transformation contient les instructions et les connaissances nécessaires pour effectuer une transformation de code spécifique. La modernisation continue utilise des définitions de transformation pour l'analyse personnalisée (`--type custom --transformation-name` *`name`*) et la correction (`--transformation-name` *`name`*). Répertoriez les définitions de transformation disponibles avec`atx custom def list`.

Comment ? AWS Transformez les travaux de modernisation continue

AWS La modernisation continue de Transform est généralement utilisée dans les projets à grande échelle où plusieurs bases de code nécessitent une analyse et une correction continues. Les équipes suivent généralement ce flux de travail :

1. Connecter des sources : ajoutez GitHub des organisations, GitLab des groupes, des espaces de travail Bitbucket ou des annuaires locaux en tant que sources. Fournissez des jetons d'authentification avec des étendues appropriées.
2. Découverte de référentiels — Exécutez des analyses de découverte pour énumérer tous les référentiels de vos sources. Utilisez des étiquettes pour organiser les référentiels par équipe, priorité ou vague de migration.
3. Exécuter une analyse — Exécutez des analyses sur l'ensemble de votre portefeuille. Choisissez des scans rapides pour des résultats rapides ou une analyse complète pour des résultats détaillés. L'analyse de sécurité nécessite une configuration unique de l'infrastructure.
4. Résultats du triage : examinez les résultats par gravité, par référentiel ou par type d'analyse. Rejetez les faux positifs avec des raisons documentées. Re-runanalyse pour marquer les problèmes résolus comme obsolètes.
5. Corriger : créez des correctifs pour corriger les résultats. La modernisation continue crée automatiquement des branches et ouvre pull/merge des demandes avec les correctifs. Suivez l'état des mesures correctives et réessayez les échecs.
6. Configurer l'analyse continue : planifiez des analyses récurrentes à l'aide des `atx ct schedule` commandes, qui utilisent Amazon EventBridge Scheduler. Configurez la cadence d'analyse (quotidienne, hebdomadaire ou mensuelle) pour surveiller en permanence votre portefeuille afin de détecter de nouveaux problèmes. Associez-le à une correction automatique pour préserver l'intégrité du code au fil du temps.

Options de calcul

La modernisation continue prend en charge plusieurs options de calcul pour exécuter des analyses et des mesures correctives. Les analyses peuvent être exécutées localement, sur une infrastructure que vous provisionnez et gérez dans votre Compte AWS (Amazon EC2 ou AWS Batch), ou sur une AWS Transform-managed infrastructure ne nécessitant aucune configuration. Les compétences des agents présentes dans le module Kiro Power et le plug-in d'agent vous aident à configurer chaque option.

> **Note**
>
> Quelle que soit l'option de calcul, vous créez et possédez toutes les ressources que vous utilisez à Compte AWS l'aide de vos informations d'identification, et votre code source reste sous votre contrôle. L'infrastructure qui exécute les analyses et les mesures correctives est soit gérée par le client (une pile que vous provisionnez dans votre compte) soit gérée par le client AWS Transform-managed, soit AWS elle gère le calcul pour vous et il n'y a rien à provisionner.

Local (par défaut)

Par défaut, les analyses s'exécutent sur votre machine locale. Cette option ne nécessite aucune infrastructure supplémentaire. Le serveur s'exécute localement et exécute des analyses à l'aide de ressources de calcul locales. Idéal pour essayer l'outil, de petits référentiels ou pour une utilisation individuelle.

AWS Transform-managed (aucune infrastructure à fournir)

Exécutez des analyses sur AWS Transform-managed l'infrastructure sans provisionner ni gérer de pile. Avec`--mode aws-managed`, vous soumettez l'analyse à AWS Transform, qui l'exécute sur une infrastructure AWS gérée. Il n'y a aucune instance Amazon EC2, aucune pile AWS Batch, aucun VPC ou sous-réseau à configurer. Il n'y a rien à mettre en place ou à démolir : la soumission est la solution. Il s'agit du moyen le plus rapide de fonctionner à distance lorsque vous ne souhaitez gérer aucune infrastructure.

Cette option nécessite une source hébergée sur un fournisseur SCM pris en charge (GitHubGitLab, ouBitbucket). AWS Transform-managed l'infrastructure ne prend pas en charge les sources locales car elle ne peut pas accéder aux référentiels de votre machine. Vous pouvez choisir la AWS région dans laquelle s'exécute la charge de travail à l'aide de l'`--region`option.

AWS Transform-managed l'infrastructure exécute uniquement des analyses. Pour y remédier ou pour exécuter une définition de transformation personnalisée (`--type custom`), utilisez AWS Batch ou Amazon EC2.

Pour exécuter sur l' AWS Transform-managed infrastructure, utilisez la `atx ct remote analysis --mode aws-managed` commande (voirExécution à distance), ou installez le plug-in Kiro Power ou agent (voirOutils pour développeurs) et demandez à l'agent : « Exécutez mon analyse AWS sans

infrastructure ». Une analyse récurrente sur AWS Transform-managed l'infrastructure nécessite un rôle d'exécution (voirPlanifier une analyse récurrente).

Vous pouvez également démarrer une analyse de l' AWS Transform-managed infrastructure depuis la page de modernisation continue de l'application Web AWS Transform (voirAWS Transformez les applications Web).

AWS Lot (Fargate) (recommandé)

Pour la plupart des portefeuilles, vous pouvez exécuter des analyses sur AWS Batch avec Fargate, qui est l'option de calcul recommandée. Chaque analyse s'exécute comme une tâche isolée dans son propre conteneur avec calcul sans serveur. Il n'y a donc aucune infrastructure persistante à gérer, et les tâches sont évolutives pour permettre l'analyse parallèle de plusieurs sources ou types d'analyses.

Le provisionnement déploie l'infrastructure requise, notamment :

- AWS File d'attente de tâches par lots et environnement de calcul
- Définition du poste avec l'image du conteneur de modernisation continue
- Rôles IAM pour l'exécution de tâches par lots
- Une fonction Lambda pour la soumission de tâches

Le provisionnement de l'infrastructure nécessite des autorisations d'administrateur. Pour exécuter des analyses et des corrections sur une pile de commandes déjà provisionnée avec le minimum de privilèges, joignez la politique gérée. AWS `AWSTransformInfrastructureExecutorAccessBatch`

Pour configurer l'exécution par lots, utilisez directement les `atx ct remote` commandes (voirExécution à distance), ou installez le plug-in Kiro Power ou agent (voirOutils pour développeurs) et demandez à l'agent : « Exécutez mon analyse sur Fargate » ou « Configurer l'exécution par lots pour une modernisation continue ». L'agent déploie la pile, stocke vos informations d'identification source dans Secrets Manager et soumet les tâches d'analyse à AWS Batch.

Amazon Amazon EC2

Exécutez des analyses sur une instance Amazon EC2 persistante dans votre Compte AWS. Cette option décharge le calcul de votre machine locale, prend en charge des analyses plus importantes et permet des analyses planifiées récurrentes. L'instance continue de fonctionner entre les soumissions.

Le provisionnement déploie une AWS CloudFormation pile qui inclut :

- Une instance Amazon EC2 (Amazon Linux 2023) avec Docker et le conteneur de modernisation continue
- Un rôle IAM avec des autorisations pour AWS Transform, Amazon S3, AWS KMS, Secrets Manager et l'agent de sécurité
- `AmazonSSMManagedInstanceCore`pour l'accès au shell via SSM (aucune paire de clés SSH ni aucun port entrant requis)
- Un groupe de sécurité sans règles entrantes

L'infrastructure de provisionnement nécessite des autorisations d'administrateur pour la gestion du cycle de vie d'Amazon EC2, les opérations de AWS CloudFormation pile, la création de rôles IAM, les opérations de compartiment Amazon S3, la gestion des secrets Secrets Manager et les commandes SSM. Pour exécuter des analyses et des corrections sur une pile Amazon EC2 déjà provisionnée avec le minimum de privilèges, joignez la politique gérée. AWS `AWSTransformInfrastructureExecutorAccessEC2`

Pour configurer l'exécution d'Amazon EC2, utilisez les `atx ct remote` commandes directement (voirExécution à distance), ou installez le plug-in Kiro Power ou agent (voirOutils pour développeurs) et demandez à l'agent : « Configurer une instance EC2 pour une analyse de modernisation continue ». L'agent approvisionne l'infrastructure, vérifie que le conteneur est en bon état et soumet vos analyses via SSM, aucun SSH n'est requis.

Configuration de l'agent de sécurité

Le type `security` d'analyse utilise le service AWS Security Agent pour la détection des vulnérabilités et des CVE. Contrairement aux autres types d'analyse, elle nécessite une configuration d'infrastructure unique dans votre Compte AWS.

> **Note**
>
> Le type d'`security`analyse n'est pas disponible dans les régions suivantes : Canada (Centre`ca-central-1`) (), Europe (Londres`eu-west-2`) () et Asie-Pacifique (Séoul) (`ap-northeast-2`). Les autres types d'analyse ne sont pas affectés.

La commande setup fournit une AWS CloudFormation pile qui inclut :

- Un compartiment Amazon S3 pour le téléchargement du code source
- Un rôle IAM assumé par `securityagent.amazonaws.com`
- Une politique gérée pour le rôle d'agent de sécurité

Pour exécuter des analyses de sécurité avec le moins de privilèges possible après la configuration, associez la politique AWS gérée `AWSTransformSecurityAgentExecutorAccess` à votre utilisateur ou à votre rôle IAM.

Votre utilisateur ou rôle IAM doit disposer des autorisations supplémentaires suivantes pour exécuter la configuration :

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

Utilisez les commandes suivantes pour gérer l'infrastructure des agents de sécurité :

```
# 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
```

Une fois la configuration terminée, vous pouvez exécuter des analyses de sécurité de la même manière que les autres types d'analyses.

Prise en main

Conditions préalables

Pour utiliser efficacement la modernisation continue, vous devez avoir une connaissance de base du contrôle de version de Git, une bonne connaissance de votre plate-forme de code source (GitHub

GitLab, ou Bitbucket), une connaissance pratique des autorisations AWS IAM et une expérience des outils de ligne de commande.

Avant d'utiliser la modernisation continue, vérifiez que vous disposez des éléments suivants :

- AWS Transform CLI est installé :

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

- Node.js 22 ou version ultérieure
- AWS Informations d'identification valides (`AWS_PROFILE`ou variables d'environnement)
- La politique AWS gérée `AWSTransformCustomFullAccess` associée à votre utilisateur ou à votre rôle IAM

> **Note**
>
> L'exécution d'analyses et de mesures correctives sur une infrastructure distante ou avec l'agent de sécurité nécessite des politiques gérées supplémentaires. Consultez les options de calcul et la configuration des agents de sécurité dansComment ? AWS Transformez les travaux de modernisation continue.

Démarrage rapide

> **Note**
>
> Il n'est plus nécessaire de démarrer un serveur local. La `atx ct server` commande est obsolète.

1. Ajoutez une source :

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

Où *`name`* se trouvent l'identifiant descriptif de votre source, *`provider`* la plateforme (`github`, `gitlabbitbucket`, ou`local`), *`org-or-group`* le nom de votre organisation ou de votre groupe et *`token`* votre jeton d'authentification.

2. Découvrez les référentiels :

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

3. Exécutez une analyse :

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

4. Explorez les résultats :

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

5. Corriger les résultats :

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

Travailler dans le cadre d'une modernisation continue

Gestion des sources

Utilisez `atx ct source` des commandes pour connecter des référentiels. Fournisseurs pris en charge : GitHub GitLab, Bitbucket, local.

GitHub organisations

Jeton : jeton d'accès personnel (classique) avec `repo` scope. Read-only pour l'analyse, dépôt complet pour la correction.

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

GitLab groupes et utilisateurs

Jeton : jeton d'accès personnel avec `api` scope.

```
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
```

Espaces de travail et projets Bitbucket

Bitbucket Cloud — domaines d'application :`read:repository:bitbucket`,,`write:repository:bitbucket`,`read:pullrequest:b` `write:pullrequest:bitbucket` A également besoin `--email` de et`--username`.

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

Centre de données Bitbucket :

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

Référentiels locaux

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

> **Important**
>
> `--path`doit pointer vers un répertoire parent contenant des dépôts git en tant que sous-répertoires, et non vers un seul dépôt.

Gestion des sources

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

Découverte et gestion du référentiel

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

Après la découverte :

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

Analyse en cours

Le `--type` drapeau indique le type d'analyse à exécuter :

- `rapid-techdebt-analysis`— Dépendances obsolètes et gains faciles.
- `tech-debt-comprehensive`— AI-powered Analyse approfondie portant sur les dépendances, la sécurité, les modèles, les performances, la maintenabilité, l'architecture, la qualité du code et les résultats de l'infrastructure.
- `security`— Vulnérabilités et expositions en matière de sécurité.
- `agentic-readiness`— Préparation de vos référentiels pour les agents d'IA (frameworks, API, documentation).
- `modernization-readiness`— Des opportunités de modernisation dans tous les domaines de votre infrastructure, de vos applications, de vos données, de votre sécurité et de vos opérations.

```
atx ct analysis run --type type --source name [--repo source::repo] [--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]
```

Analyse personnalisée

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

Configuration avec `-g` indicateur : clé-valeur, JSON ou chemin de fichier.

Liste des TD : `atx custom def list`

Gestion des résultats

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

Trouver des statuts

- `open`— Actif
- `dismissed`— Rejeté manuellement (nécessite une raison)
- `obsolete`— System-set lorsque la nouvelle analyse ne produit plus le résultat

```
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
```

Trouver l'obsolescence

Re-analysis marque les résultats résolus comme étant obsolètes. Ne peut pas être rouvert. Conservé à des fins d'audit.

Création de mesures correctives

Trois modes : basé sur les résultats, remplacement TD, TD direct.

```
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::repo
```

Sortie par fournisseur : GitHub PR, GitLab MR, Bitbucket PR, succursale locale.

> **Note**
>
> Le jeton doit disposer d'un accès en écriture pour être PR/MR créé.

Exécution locale avec `--local` drapeau.

```
atx ct remediation create --transformation-name TD --repo source::repo -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 cancel --id id
atx ct remediation delete --id id
```

Exécution à distance

Par défaut, les analyses et les corrections s'exécutent sur votre machine locale. Pour les portefeuilles plus importants, vous pouvez déléguer le travail à une infrastructure distante. Vous pouvez fonctionner sur une AWS Transform-managed infrastructure sans rien à provisionner (analyses uniquement), ou sur Compte AWS une infrastructure que vous provisionnez et gérez dans votre instance Amazon EC2 persistante ou des tâches AWS Batch (Fargate). Les `atx ct remote` commandes approvisionnent, exécutent, surveillent et démantelent l'infrastructure gérée par le client. Quel que soit l'endroit où l'exécution a lieu, vous créez toutes les ressources dans votre ordinateur Compte AWS et votre code source reste sous votre contrôle.

> **Note**
>
> Le provisionnement, la mise à jour et le démantèlement de l'infrastructure créent et modifient des AWS CloudFormation piles et des rôles IAM, et nécessitent des autorisations d'administrateur. Passez `--ack` pour en accuser réception et ignorez l'invite interactive. L'exécution d'analyses et de corrections sur une infrastructure déjà provisionnée utilise des politiques d'exécution dotées du moindre privilège. Consultez la section Marquage et contrôle d'accès et les options de calcul pour les politiques gérées concernées. Comment ? AWS Transformez les travaux de modernisation continue

En cours d'exécution AWS Transform-managed infrastructure (pas de provisionnement)

Pour exécuter une analyse à distance sans rien provisionner, utilisez`--mode aws-managed`. La soumission est envoyée à AWS Transform, qui effectue l'analyse de l' AWS Transform-managed infrastructure. Il n'y a aucune pile à provisionner, aucun réseau à configurer et aucune information

d'identification à stocker dans AWS Secrets Manager. La soumission est définitive. Choisissez la AWS région dans laquelle s'exécute la charge de travail`--region`.

```
# Run an analysis on AWS Transform-managed infrastructure
atx ct remote analysis --type type --mode aws-managed --sources name [--
repos repo1,repo2] [--region region]

# Poll the submission (there is no remote status command in this mode)
atx ct analysis get --id id --json
```

Ce mode exécute uniquement des analyses. Il ne prend pas en charge la correction, le type `custom` d'analyse ou les sources locales. Comme il n'y a pas de pile`--stack-name`, les `--batch-name` options `--tags``--existing-instance`,, et ne s'appliquent pas. Une seule soumission couvre jusqu'à 100 référentiels. Pour couvrir des domaines plus larges, répartissez-les sur plusieurs soumissions avec`--repos`. Contrairement à Amazon EC2 et aux exécutions par lots, vous pouvez suivre la progression avec `atx ct analysis get` plutôt que`atx ct remote status`.

Mise en réseau

Le calcul à distance doit être exécuté dans des sous-réseaux privés. Découvrez le réseau existant ou créez un nouveau VPC avant de procéder au provisionnement :

```
# List VPCs, private subnets, and security groups in the current account and Region
atx ct remote network discover
atx ct remote network discover --vpc vpc-id --json

# Create a new VPC with private subnets, a NAT gateway, and a security group
atx ct remote network create --cidr 10.1.0.0/16 --ack
```

Provisionnement de l'infrastructure

Déployez la pile Amazon EC2 ou Batch. Omettez `--execute` de prévisualiser le modèle ou l'ensemble de modifications ; ajoutez-le `--execute` pour appliquer.

Le provisionnement crée la pile de calcul pour le mode que vous choisissez, ainsi qu'une pile de planificateur :

- Batch : une file d'attente de tâches et un environnement de calcul AWS par lots, une définition de tâche avec l'image du conteneur de modernisation continue, des rôles IAM pour l'exécution

des tâches et une fonction Lambda pour la soumission des tâches. Batch nécessite un groupe de sécurité.

- Amazon EC2 : instance Amazon EC2 persistante dotée d'un profil d'instance IAM et d'un groupe de sécurité. Si vous omettez`--securityGroup`, la pile crée un groupe de sécurité sans règles entrantes ; l'accès se fait via SSM.
- Planificateur : `atx-scheduler` pile (un groupe de EventBridge planification Amazon Scheduler et un rôle d'invocation) utilisée par les analyses récurrentes. Laissez-passer `--skip-scheduler` pour vous désinscrire.

```
# Preview, then deploy an EC2 stack
atx ct remote provision --mode ec2 --vpc vpc-id --subnets subnet-a,subnet-b
atx ct remote provision --mode ec2 --vpc vpc-id --subnets subnet-a,subnet-b --execute
 --ack

# Deploy a Batch stack
atx ct remote provision --mode batch --vpc vpc-id --subnets subnet-a,subnet-b --
securityGroup sg-id --execute --ack

# Update an existing stack to the latest template, or tear it down
atx ct remote update --mode ec2|batch --execute --ack
atx ct remote teardown --mode ec2|batch --execute --ack
```

Image de conteneur

Lorsque vous exécutez des analyses et des corrections à distance, elles s'exécutent dans une image de conteneur. Par défaut, lorsque vous provisionnez un environnement distant, celui-ci utilise l'image publique AWS Transform,`public.ecr.aws/d9h8z6l7/aws-transform:latest`. Batch la définit comme image de définition de tâche. Amazon EC2 l'utilise comme image du coureur.

Pour exécuter une autre image (par exemple, une image Amazon ECR privée qui regroupe des langues ou des outils `--image-uri` supplémentaires), vous devez procéder à la mise en service :

```
# Batch: provision with a custom image
atx ct remote provision --mode batch --vpc vpc-id --subnets subnet-a,subnet-b --
securityGroup sg-id --image-uri account-id.dkr.ecr.region.amazonaws.com/repo:tag --
execute --ack

# EC2: provision with a custom image
```

```
atx ct remote provision --mode ec2 --vpc vpc-id --subnets subnet-a,subnet-b --image-
uri account-id.dkr.ecr.region.amazonaws.com/repo:tag --execute --ack
```

Stockage des informations d'identification source

Les conteneurs distants clonent vos référentiels à l'aide de jetons stockés dans AWS Secrets Manager. Enregistrez un jeton pour chaque source SCM avant d'exécuter une analyse ou une correction à distance :

```
atx ct remote credentials --source name --token token
atx ct remote credentials --source name --remove
```

Courir à distance

L'analyse à distance exécute un conteneur pour chaque référentiel ; la correction à distance exécute un conteneur pour chaque découverte. Utilisez `--sources``--repos`, et `--labels` pour contrôler le fan-out, `--stack-name` et/ou `--tags` pour sélectionner la pile provisionnée à utiliser.

```
# Run analysis across a source on Batch
atx ct remote analysis --type type --mode batch --sources name [--repos repo1,repo2]
 [--labels "team:frontend"]

# Run remediation for specific findings on EC2
atx ct remote remediation --mode ec2 --ids id1,id2
atx ct remote remediation --mode ec2 --sources name --min-severity high
```

Surveillance et gestion des courses

```
# Check whether infrastructure is deployed
atx ct remote detect --mode ec2|batch

# Track a submission (Batch by batch ID, EC2 by group ID)
atx ct remote status --batch batch-id --stack-name name
atx ct remote status --group ec2-group-id --wait

# Resume a partially-failed Batch run (re-submits only incomplete repos).
# On resume, --batch-name takes the existing batch ID reported by "remote status --
batch".
atx ct remote analysis --type type --mode batch --sources name --resume-incomplete --
batch-name batch-id
```

```
# Cancel a running submission
atx ct remote cancel --mode batch --batch batch-id --stack-name name
atx ct remote cancel --mode ec2 --group ec2-group-id
```

Planifier une analyse récurrente

Permet `atx ct schedule` d'exécuter des analyses automatiquement à une cadence récurrente. Vous pouvez planifier des analyses mais pas des mesures correctives. Miroir des options d'emploi`atx ct remote analysis`. Les horaires sont exécutés à distance, de deux manières différentes :

- AWS Transform-managed(`--mode aws-managed`) : un calendrier côté serveur qui déclenche des analyses sur AWS Transform-managed l'infrastructure. Il n'y a pas de EventBridge calendrier Amazon et il n'y a rien à prévoir. Cela nécessite un rôle d'exécution (`--execution-role`) que AWS Transform assume à chaque exécution (voirRôle d'exécution pour AWS Transform-managed horaires).
- Customer-managed(`--mode ec2|batch`) : un calendrier Amazon EventBridge Scheduler intégré à votre compte répartit chaque exécution vers une instance Amazon EC2 persistante ou une pile de AWS lots que vous provisionnez en premier (voir). Exécution à distance

La `--recurrence` valeur acceptedaily, `weekly:`*DAY* (par exemple,`weekly:MONDAY`), ou `monthly:`*N* où *N* est un jour compris entre 1 et 28. Les horaires relatifs à AWS Transform-managed l'infrastructure sont exécutés en UTC.

```
# AWS Transform-managed schedule (no infrastructure; requires an execution role)
atx ct schedule create --name name --mode aws-managed --execution-role role-arn --
recurrence daily --type type --sources name [--repos repo1,repo2]

# Customer-managed schedule (EventBridge Scheduler dispatching to your EC2 or Batch
 stack)
atx ct schedule create --name name --mode ec2|batch --recurrence weekly:MONDAY --
type type --sources name [--repos repo1,repo2]

# Manage schedules of either type by their schedule ID (from schedule list)
atx ct schedule list
atx ct schedule get schedule-id
atx ct schedule disable schedule-id
atx ct schedule enable schedule-id
atx ct schedule delete schedule-id
```

Pour afficher les analyses exécutées par un calendrier, utilisez`atx ct analysis list --schedule-id` *`schedule-id`*, qui renvoie les exécutions déclenchées par le calendrier, les plus récentes en premier.

Pour supprimer le rôle de planificateur et le groupe de planification utilisés par les planifications gérées par le client, exécutez. `atx ct schedule teardown --execute`

Rôle d'exécution pour AWS Transform-managed horaires

Un planning créé avec `--mode aws-managed` nécessite un `--execution-role` ARN que AWS Transform assume à chaque exécution du planning. Configurez le rôle comme suit :

- L'identité qui crée le planning doit disposer d'une `iam:PassRole` autorisation sur le rôle d'exécution.
- La politique de confiance du rôle doit permettre au `transform-custom.amazonaws.com` responsable du service de l'assumer.
- Au minimum, le rôle doit être `AWSTransformCustomFullAccess` associé à la politique AWS gérée, ainsi que des `secretsmanager:DescribeSecret` autorisations sur `secretsmanager:GetSecretValue` les secrets sous le `atx/*` préfixe afin que les exécutions planifiées puissent récupérer les informations d'identification du clone source.

La politique en ligne suivante accorde au AWS Secrets Manager l'accès dont les exécutions planifiées ont besoin pour récupérer les informations d'identification du clone source. Attachez-le au rôle d'exécution à côté de la politique `AWSTransformCustomFullAccess` gérée, en *`account-id`* remplaçant *`region`* et par la AWS région et le compte dans lesquels le calendrier s'exécute.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AtxSourceCredentials",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": "arn:aws:secretsmanager:region:account-id:secret:atx/*"
    }
  ]
```

```
}
```

Marquage et contrôle d'accès

Vous pouvez appliquer des balises (`key=value`paires séparées par des virgules) aux sources, aux analyses et aux corrections à l'aide de cette option. `--tags` Les balises sont également prises en charge sur l'infrastructure distante, les informations d'identification stockées et les ressources réseau. Les balises vous permettent d'organiser les ressources. Combinées aux conditions des balises IAM, les balises implémentent le contrôle d'accès basé sur les attributs (ABAC) afin que les équipes n'accèdent qu'aux ressources qui contiennent leurs balises.

```
atx ct source add --name name --provider github --org org --token pat --
tags team=platform,env=prod
atx ct analysis run --type type --source name --tags team=platform
atx ct remediation create --ids id1,id2 --tags team=platform
```

Par défaut, les ressources sont balisées avec les balises que vous définissez dans`~/.aws/atx/settings.json`. Ajoutez les balises que vous souhaitez appliquer à chaque ressource ci-dessous`applyTags`, et elles deviendront vos balises par défaut.

```
{
  "applyTags": [
    { "team": "alpha" }
  ]
}
```

> **Note**
>
> Les balises transmises `--tags` sont fusionnées avec toutes les balises par défaut configurées, et chaque clé est `--tags` gagnante aux deux endroits.

AWS Transformez les applications Web

Utilisez l'application Web AWS Transform pour créer et exécuter des analyses, examiner les résultats, créer des solutions et suivre les demandes d'extraction générées dans vos sources de code.

Avant d'utiliser l'application Web, votre organisation doit activer votre identité d'utilisateur pour accéder à AWS Transform. Pour plus d'informations sur la configuration de AWS Transform, voir Configuration de AWS Transform.

Connexion

Pour accéder à l'application Web AWS Transform, procédez comme suit.

1. Ouvrez `https://aws.amazon.com/transform/` et connectez-vous à l'aide des informations d'identification AWS IAM Identity Center.
2. Si la modernisation continue n'apparaît pas, connectez-vous plutôt avec des informations d'identification IAM :
   a. Dans la console AWS de gestion, ouvrez AWS Transform et choisissez Paramètres.
   b. Activez Access AWS Transform à l'aide des informations d'identification IAM.
   c. Copiez l'URL de l'application Web (avec IAM) et collez-la dans la même fenêtre de navigateur que celle où la console est ouverte.
3. Ouvrez le menu de navigation de gauche et choisissez Modernisation continue.

Modes d'infrastructure

Lorsque vous créez une analyse, choisissez l'un des modes d'infrastructure suivants :

- AWS géré — Exécuté sur une infrastructure gérée par AWS Transform. Vous n'avez pas besoin de provisionner d'infrastructure.
- Appartenant au client — Exécutez sur une pile déployée dans votre propre environnement Compte AWS. Utilisez ce mode lorsque vous avez besoin de contrôler le calcul, la mise en réseau ou la configuration de sécurité.

> **Note**
>
> Pour effectuer une analyse de sécurité, utilisez l'infrastructure appartenant au client. L'analyse de sécurité s'exécute sur l'agent de sécurité déployé sur votre compte.

Pour utiliser l'infrastructure appartenant au client, ouvrez l'onglet Paramètres. Utilisez les liens de AWS CloudFormation création rapide pour déployer les piles suivantes dans l'ordre :

1. `AtxDispatcherStack`— Répartiteur de messages (toujours obligatoire).
2. Pile de calcul : `AtxInfrastructureStack` (AWS Batch) ou `atx-runner` (Amazon EC2).
3. `atx-scheduler`— Nécessaire pour les analyses programmées récurrentes.
4. `AtxSecurityAgentStack-<region>`— Nécessaire uniquement pour l'analyse de sécurité.

Pour le CLI-based provisionnement et la configuration réseau, consultezExécution à distance.

Démarrage du flux de travail

1. Connecter des sources : ouvrez l'onglet Sources et ajoutez des référentiels depuis GitHubGitLab, ouBitbucket.
2. Exécuter ou planifier une analyse : ouvrez l'onglet Analyses, sélectionnez des référentiels, choisissez un type d'analyse, sélectionnez un mode d'infrastructure, puis choisissez Exécuter. Pour exécuter selon une cadence récurrente (quotidienne, hebdomadaire ou mensuelle), choisissez Planifier à la place.
3. Examiner les résultats — Ouvrez l'onglet Résultats pour afficher les résultats par niveau de gravité.
4. Créer une correction : sélectionnez les résultats et choisissez Créer une correction.
5. Passez en revue les pull requests : ouvrez l'onglet Corrections pour afficher les liens PR générés par référentiel.

Discutez avec AWS Transform directement depuis l'application Web pour poser des questions sur vos analyses, vos résultats ou les mesures correctives.

Outils pour développeurs

Vous pouvez accéder à la modernisation continue à partir des IDE d'agence à l'aide du plug-in AWS Transform Power et de l'agent. L'agent orchestre la configuration, l'intégration et l'utilisation continue de la modernisation continue grâce à une interaction conversationnelle.

- Kiro IDE — Installez le AWS Transform Kiro Power. Ouvrez Kiro Chat et demandez à l'agent de vous aider à gérer les flux de travail de modernisation continue.
- Claude Code, Codex, Cursor — Installez le `plugins/aws-transform` répertoire awslabs/agent-plugins. Le plug-in d'agent fournit les mêmes fonctionnalités que le Kiro Power.

Compétences des agents

Le plug-in Kiro Power and Agent inclut des compétences qui permettent d'orchestrer les flux de travail de modernisation continue grâce à une interaction conversationnelle :

Compétence	Description
Guide	Intégration interactive qui vous guide étape par étape tout au long du flux de travail
Source	Ajouter, répertorier et supprimer des connexion s sources
Découverte	Scannez les sources pour découvrir les référentiels
Analyse	Exécutez et gérez des analyses de tous types
Résultats	Interrogez, filtrez et gérez les résultats des analyses
Correction	Créez et gérez des mesures correctives pour corriger les résultats
Exécution EC2	Provisionnez et gérez une instance Amazon EC2 pour une analyse à distance
Exécution par lots	Soumettre des tâches d'analyse à AWS Batch avec Fargate
Planning	Configurez une analyse récurrente selon un calendrier cron à l'aide d'Amazon Scheduler EventBridge
Reporting	Générez des rapports HTML autonomes avec des graphiques montrant les résultats, la distribution de la gravité et les progrès de la correction

référence de l'interface de ligne de commande

Le tableau suivant récapitule toutes les `atx ct` sous-commandes.

Sous-commande	Description
`atx ct status`	Afficher l'état du système, y compris les sources, les référentiels, les analyses, les résultats et les mesures correctives
`atx ct source add`	Ajouter une source (GitHub GitLab, Bitbucket ou locale)
`atx ct source list`	Liste des sources configurées
`atx ct source get`	Afficher les détails d'une source unique
`atx ct source update`	Mettre à jour le jeton d'une source existante
`atx ct source remove`	Supprimer une source
`atx ct discovery scan`	Découvrez des référentiels à partir d'une source
`atx ct discovery status`	Vérifier l'état du scan de découverte
`atx ct repository list`	Répertorier les référentiels avec des filtres optionnels
`atx ct repository get`	Obtenez un référentiel unique
`atx ct repository update`	Mettre à jour les étiquettes du référentiel
`atx ct repository delete`	Supprimer un référentiel
`atx ct analysis run`	Exécuter une analyse sur les référentiels
`atx ct analysis get`	Obtenir les détails de l'analyse
`atx ct analysis list`	Analyses de listes avec filtres de statut et de type facultatifs

Sous-commande	Description
`atx ct analysis cancel`	Annuler une analyse en cours
`atx ct analysis delete`	Supprimer une analyse
`atx ct findings list`	Répertoriez les résultats avec des filtres pour le dépôt, la source, la gravité, le type, l'état et l'analyse
`atx ct findings count`	Compter les résultats agrégés par gravité, par dépôt ou par type d'analyse
`atx ct findings get`	Obtenez une seule découverte
`atx ct findings update`	Mettre à jour le statut de la recherche (ouverte ou rejetée)
`atx ct findings batch-update`	Mise à jour par lots de plusieurs résultats
`atx ct findings delete`	Supprimer une constatation rejetée ou obsolète
`atx ct remediation create`	Créer une solution à partir des résultats ou d'une définition de transformation
`atx ct remediation list`	Répertorier toutes les mesures correctives
`atx ct remediation status`	Vérifier l'état des mesures correctives et afficher les liens PR/MR
`atx ct remediation retry`	Réessayer une correction qui a échoué
`atx ct remediation cancel`	Annuler une correction en cours
`atx ct remediation delete`	Supprimer une correction
`atx ct remote provision`	Déployez une infrastructure d'exécution à distance (Amazon EC2 ou Batch AWS CloudFormation stack)

Sous-commande	Description
`atx ct remote analysis`	Exécutez une analyse à distance sur Amazon EC2 ou Batch
`atx ct remote remediation`	Exécutez la correction à distance sur Amazon EC2 ou Batch
`atx ct remote status`	Afficher l'état d'une soumission à distance
`atx ct remote detect`	Vérifiez si l'infrastructure distante est déployée
`atx ct remote update`	Mettre à jour l'infrastructure d'exécution à distance avec le modèle le plus récent
`atx ct remote credentials`	Gérez les jetons sources dans Secrets Manager pour une exécution à distance
`atx ct remote cancel`	Annuler une course à distance en cours
`atx ct remote teardown`	Détruisez l'infrastructure d'exécution à distance
`atx ct remote network`	Découvrez ou créez un VPC, des sous-réseaux et des groupes de sécurité pour le provision nement à distance
`atx ct schedule create`	Créez un calendrier d'analyse récurrent (Amazon EventBridge Scheduler)
`atx ct schedule list`	Lister les horaires
`atx ct schedule get`	Afficher un seul calendrier
`atx ct schedule enable`	Activer un calendrier
`atx ct schedule disable`	Désactiver un calendrier
`atx ct schedule delete`	Supprimer un calendrier
`atx ct schedule teardown`	Supprimer le rôle de planificateur et le groupe de planification

Sous-commande	Description
`atx ct setup security-agent`	Provisionner ou gérer l'infrastructure des agents de sécurité
`atx ct mcp`	Démarrez le serveur MCP en exposant les outils de modernisation continue
`atx ct schema`	Imprimez un manifeste JSON lisible par machine reprenant l'intégralité de la surface de `atx ct` commande (chaque commande, option et argument) afin que les agents et l'automatisation puissent découvrir l'interface de ligne de commande sans analyser le texte d'aide

Résolution des problèmes

Vérification de l'état du système

Il n'est plus nécessaire de démarrer un serveur local ; la `atx ct server` commande est obsolète. Vérifiez que le système est joignable avec`atx ct status --health`.

Discovery Scan ne renvoie aucun référentiel

Pour les sources locales, vérifiez que cela `--path` pointe vers un répertoire parent contenant des référentiels sous forme de sous-répertoires (par exemple`/home/user/repos`), et non vers un référentiel directement (par exemple,`/home/user/repos/my-app`). Le scanner recherche les répertoires enfants qui contiennent un `.git` dossier.

Erreur SETUP_REQUIRED

La source existe dans votre compte mais les informations d'identification ne sont pas configurées sur cette machine. Exécutez `atx ct source add --name` *`name`* pour configurer les informations d'identification localement.

Erreur AUTH_REQUIRED

Aucun jeton valide n'a été trouvé pour la source. Vérifiez que votre jeton est correct et qu'il possède les étendues requises. Pour GitHub, assurez-vous que le jeton a une `repo` portée. Pour GitLab, assurez-vous de `api` la portée.

Erreur INVALID_INPUT

Vérifiez que vous utilisez le nom de type d'analyse correct. Les valeurs valides sont: `rapid-techdebt-analysis`, `tech-debt-comprehensive`, `security`, `agentic-readiness`, `modernization-readiness`, `custom`.

Erreurs d'autorisation lors de la correction

La correction crée des branches et des pull/merge requêtes, ce qui nécessite un accès en écriture au référentiel. Mettez à jour votre jeton avec des autorisations d'écriture. Pour GitHub, assurez-vous de la `repo` portée complète. Pour GitLab, assurez-vous de `api` la portée. Pour Bitbucket, assurez-vous `write:repository:bitbucket` et définissez la `write:pullrequest:bitbucket` portée.

La configuration de l'agent de sécurité échoue

Vérifiez que votre utilisateur ou rôle IAM possède les autorisations requises AWS CloudFormation, IAM et Amazon S3 répertoriées dans la section Configuration de l'agent de sécurité de. Comment ? AWS Transformez les travaux de modernisation continue Vérifiez le statut avec`atx ct setup security-agent --status`.

L'analyse de sécurité ou la configuration d'un agent de sécurité ne sont pas disponibles dans une région

Le type d'`security`analyse n'est pas disponible au Canada (Centre`ca-central-1`) (), en Europe (Londres`eu-west-2`) () ou en Asie-Pacifique (Séoul) (`ap-northeast-2`). Exécutez `security` des analyses et `atx ct setup security-agent` depuis une région prise en charge. Les autres types d'analyse ne sont pas affectés. Consultez la section Configuration de l'agent de sécurité deComment ? AWS Transformez les travaux de modernisation continue.

Le provisionnement à distance échoue avec une erreur d'autorisations

Le provisionnement, la mise à jour et le démantèlement de l'infrastructure distante (`atx ct remote provision`,`update`,`teardown`) créent et modifient des AWS CloudFormation piles et des rôles IAM, et nécessitent des autorisations d'administrateur. Pour exécuter des analyses et des corrections sur une infrastructure déjà provisionnée avec le minimum de privilèges, connectez ou. `AWSTransformInfrastructureExecutorAccessEC2`

`AWSTransformInfrastructureExecutorAccessBatch` Pour plus de détails, consultez les options de calcul dansComment ? AWS Transformez les travaux de modernisation continue.

La découverte de réseau à distance ne renvoie aucun sous-réseau

Le calcul à distance doit être exécuté dans des sous-réseaux privés et `atx ct remote network discover` exclut les sous-réseaux publics. S'il n'existe aucun sous-réseau privé, créez un réseau avec`atx ct remote network create`.

L'exécution à distance ne peut pas cloner les référentiels

Les conteneurs distants utilisent des jetons stockés dans AWS Secrets Manager. Enregistrez un jeton pour chaque source `atx ct remote credentials --source` *`name`* `--token` *`token`* avant d'exécuter une analyse ou une correction à distance.

Le calendrier ne s'exécute pas

Les plannings sont exécutés sur une infrastructure distante. Provisionnez une pile Amazon EC2 ou Batch avec `atx ct remote provision` avant de créer une planification, et confirmez que la planification est activée avec`atx ct schedule get` *`name`*.

Modernisation continue non visible dans l'application Web

Si la modernisation continue n'apparaît pas une fois que vous vous êtes connecté à l'application Web AWS Transform, connectez-vous avec les informations d'identification IAM de l' Compte AWS endroit où AWS Transform est activé au lieu d' AWS IAM Identity Center. Pour les étapes, consultez AWS Transformez les applications Web.

Évaluations de la migration

AWS Les évaluations Transform vous aident à évaluer le coût, la faisabilité et la valeur commerciale de la migration de l'infrastructure sur site vers. AWS Les évaluations fournissent des recommandations automatisées sur la bonne taille, des comparaisons entre plusieurs scénarios et des améliorations interactives par chat.

Vous pouvez utiliser les évaluations de migration pour :

- Obtenez des estimations de coûts pour Amazon RDS pour SQL Server, Amazon EC2, Amazon EBS, Amazon S3 et Amazon FSx
- Recevez des recommandations automatisées sur la bonne taille
- Évaluez la valeur commerciale et l'impact sur le développement durable
- Comparez plusieurs scénarios de migration côte à côte
- Affinez les évaluations de manière interactive via le chat
- Générez des présentations exécutives et des rapports détaillés

Conditions préalables

Avant de créer une évaluation de migration, vérifiez que vous disposez des éléments suivants :

- Un espace de travail AWS transformé
- Données d'inventaire dans un format compatible, ou vous pouvez utiliser une estimation approximative par chat
- Autorisations appropriées pour créer et exécuter des évaluations

Comment fonctionnent les évaluations de la migration

Les évaluations de migration suivent un flux de travail structuré qui vous guide depuis le téléchargement initial des données jusqu'à la génération finale des livrables.

Pour effectuer une évaluation de la migration

1. Créez une tâche d'évaluation de la migration dans votre espace de travail AWS Transform.

2. Téléchargez vos données d'inventaire sur site.
3. Passez en revue les résultats de découverte générés par AWS Transform à partir de vos données.
4. Gérez l'étendue de l'inventaire en excluant les serveurs ou en ajustant les regroupements.
5. Configurez votre scénario d'évaluation avec des hypothèses de tarification et d'infrastructure.
6. Exécutez l'évaluation.
7. Passez en revue et affinez les résultats par chat.

Après avoir examiné les résultats, vous pouvez créer des scénarios supplémentaires, comparer des scénarios et générer des livrables tels que des présentations et des rapports.

Téléchargement des données d'inventaire

AWS Transform accepte les données d'inventaire provenant de sources multiples. Le tableau suivant répertorie les formats de données pris en charge.

Source de données	Description
AWS Exportation de l'outil Transform Discovery	Inventaire automatique des serveurs découvert par l'outil de découverte AWS Transform
Outils pour camping-cars	Exportations depuis des environnements VMware au format Excel ZIP/CSV ou au format Excel. Les exportations complètes et les Info-only exportations v sont prises en charge.
Données CMDB	Exportations de bases de données de gestion
Outils de découverte de partenaires	Données issues des outils de découverte des AWS partenaires
Évaluateur de migration	Fichier Quick Insights depuis la console Migration Evaluator
Format MPA	Fichier d'importation de l'évaluation du portefeuille de migration
AWS Modèle de données de transformation	Fichier Microsoft Excel créé à partir du modèle AWS Transform Assessment Data

AWS Transform identifie automatiquement le format de fichier lors de l'ingestion. Le processus d'ingestion valide vos données, accepte les données partielles lorsque certains champs sont manquants et prend en charge les téléchargements incrémentiels. Vous pouvez télécharger des fichiers supplémentaires à tout moment pour compléter votre inventaire.

Révision des résultats de découverte

Une fois que AWS Transform a traité vos données d'inventaire, il génère un résumé des découvertes. Le résumé comprend les informations suivantes :

- Nombre de serveurs par système d'exploitation
- Panne des serveurs physiques et virtuels
- Détection de SQL Server
- Résumés du stockage
- Avertissements concernant la qualité des données

Passez en revue les résultats de la découverte pour confirmer que AWS Transform a correctement identifié votre infrastructure avant de procéder à l'évaluation.

Gestion de l'étendue de l'inventaire

Après avoir examiné les résultats de la découverte, vous pouvez affiner la portée de votre évaluation. Utilisez les actions suivantes pour gérer l'étendue de votre inventaire :

- Inventaire des requêtes pour des serveurs ou des charges de travail spécifiques
- Exclure les serveurs du périmètre d'évaluation
- Passez en revue les groupements de serveurs et les dépendances des applications
- Identifiez les charges de travail SQL Server pour une évaluation spécialisée

Configuration de scénarios d'évaluation

Avant d'exécuter une évaluation, configurez les hypothèses utilisées par AWS Transform pour générer des recommandations. Vous pouvez modifier ces hypothèses à tout moment et exécuter de nouveaux scénarios avec différentes configurations.

Le tableau suivant répertorie les catégories d'hypothèses disponibles.

Hypothèse	Description
Modèle de tarification	Database Savings Plans (pour Amazon RDS for SQL Server) On-Demand ou instances réservées
Cible Région AWS	L' Région AWS endroit où vous prévoyez d'héberger les charges de travail migrées
Exclusions de types d'instances	Familles ou types d'instances Amazon EC2 à exclure des recommandations
Configuration d'Amazon EBS	Type de volume et paramètres de performance pour le stockage
Licences SQL Server	Bring Your Own Media (BYOM) ou licence incluse (LI) pour Amazon RDS for SQL Server ; licence incluse (LI) ou licence Bring Your Own (BYOL) pour SQL Server sur EC2

Capacités d'évaluation

AWS Les évaluations Transform couvrent plusieurs aspects de votre migration. Les sections suivantes décrivent chaque capacité d'évaluation.

Taille correcte d'Amazon EC2

AWS Transform analyse les spécifications de votre serveur sur site et recommande des instances Amazon EC2 de taille appropriée. Les recommandations tiennent compte des exigences en matière de processeur, de mémoire et de performances.

Stockage Amazon EBS

AWS Transform recommande les types de volumes et les configurations Amazon EBS en fonction de votre utilisation actuelle du stockage et de vos exigences en matière de performances.

Amazon FSx

AWS Transform évalue les charges de travail liées au stockage de fichiers et fournit des recommandations pour la migration vers Amazon FSx, notamment des estimations de coûts pour les types de systèmes de fichiers Amazon FSx pris en charge.

Amazon RDS for SQL Server

AWS Transform évalue le coût de la migration des bases de données SQL Server locales vers Amazon RDS for SQL Server. À l'aide d' AI-powered agents, AWS Transform analyse votre environnement SQL Server sur site et fournit une analyse de rentabilisation complète en quelques minutes, avec des recommandations en matière de calcul et de mémoire adaptées à vos exigences en matière de charge de travail afin d'éviter le surprovisionnement et de ne payer que pour ce dont vous avez besoin.

L'évaluation de RDS pour SQL Server inclut les fonctionnalités suivantes :

- Licence Bring Your Own Media (BYOM), qui vous permet d'utiliser vos licences SQL Server existantes
- Options de licence incluses (LI)
- Optimisation des coûts grâce aux Database Savings Plans, qui offrent jusqu'à 20 % d'économies par rapport à la On-Demand tarification
- Évaluation de l'éligibilité au AWS Migration Acceleration Program (MAP), qui fournit des crédits et un soutien pour compenser les coûts de migration

Vous pouvez démarrer votre évaluation de RDS pour SQL Server avec n'importe quel format de données pris en charge, y compris les exportations RVTools, les données de la base de données de gestion de la configuration (CMDB), les exportations depuis l'outil de découverte AWS Transform et d'autres outils de découverte tiers. Créez des scénarios hypothétiques pour comparer plusieurs modèles de coûts avec des hypothèses personnalisées, notamment la région, l'utilisation des ressources et les conditions de tarification.

Exemples d’invites :

- « Estimez le coût de la migration de mes bases de données SQL Server vers RDS for SQL Server »
- « Comparez les tarifs BYOM et les tarifs avec licence incluse pour RDS for SQL Server »
- « Montrez-moi les options de Database Savings Plans pour mes charges de travail RDS »

Serveur SQL Amazon EC2

AWS Transform évalue les charges de travail SQL Server et fournit des recommandations pour exécuter SQL Server sur Amazon EC2, notamment une analyse des licences et des mappages d'hôtes dédiés.

On-premises tarification

AWS Transform estime vos coûts actuels sur site afin de fournir une base de référence pour la comparaison avec les AWS prix. Vous pouvez ajuster les coûts globaux par chat. On-premises les ajustements de coûts sont reflétés dans le rapport PDF et les réponses au chat, mais pas dans l'exportation PPTX.

Exemples d’invites :

- « Mettre à jour le coût du serveur sur site à 500$ par serveur et par mois »
- « Ajouter les coûts annuels d'installation du centre de données de 50 000$ »

Durabilité

AWS Transform estime la réduction de l'empreinte carbone résultant de la migration vers. AWS Vous pouvez explorer les indicateurs de durabilité par chat.

Essayez des instructions telles que :

- « Montrez-moi la réduction de carbone estimée pour cette migration »
- « En quoi consiste l'amélioration de l'efficacité énergétique de mes charges de travail AWS ? »

Évaluation de la valeur commerciale

AWS Transform évalue la valeur commerciale globale de la migration au-delà des économies de coûts d'infrastructure. L'évaluation couvre la productivité du personnel, la résilience et l'agilité de l'entreprise.

Voici quelques exemples d'instructions :

- « Estimez les gains de productivité du personnel liés à la migration vers » AWS
- « À quelles améliorations de résilience puis-je m'attendre après la migration ? »

- « Montrez-moi les avantages de cette migration en termes d'agilité commerciale »

Coûts du réseau

AWS Transform estime les coûts liés au réseau pour votre migration, y compris les besoins en matière de transfert de données et de connectivité.

Frais de support

AWS Transform inclut les coûts du plan de AWS support dans l'évaluation en fonction du niveau de support que vous avez sélectionné.

Informatique pour utilisateur finaux

AWS Transform évalue les charges de travail informatiques des utilisateurs finaux et fournit des recommandations pour les services informatiques des utilisateurs AWS finaux.

Utilisation d'évaluations basées sur le chat

Vous pouvez interagir avec AWS Transform par chat pour créer et affiner des évaluations. Le chat prend en charge trois modes d'interaction.

Vous pouvez affiner votre évaluation de manière itérative en poursuivant la conversation. AWS Transform gère le contexte des messages et met à jour les résultats de l'évaluation en fonction de vos informations.

Estimation approximative avec des données limitées

Vous pouvez obtenir une estimation approximative des coûts en décrivant votre environnement dans le chat sans télécharger de fichiers d'inventaire détaillés. L'estimation approximative est une fonctionnalité autonome qui ne peut pas être combinée avec les données d'inventaire téléchargées ou l'enrichissement des données par chat.

Vous pouvez utiliser des instructions comme celles-ci :

- « J'ai 200 serveurs Windows et 150 serveurs Linux, estimez mes AWS coûts »
- « Donnez-moi une estimation approximative de la migration de 500 machines virtuelles vers » AWS
- « Estimation des coûts pour 50 serveurs avec une moyenne de 8 processeurs et 32 Go de RAM »

Ajouter un inventaire par chat

Vous pouvez fournir les détails de l'inventaire directement par chat pour compléter ou remplacer les fichiers téléchargés.

Utilisez des instructions telles que les suivantes :

- « Inclure un serveur de base de données exécutant Oracle sur 4 processeurs avec 128 Go de RAM »
- « Ajoutez 20 serveurs Web fonctionnant sous Linux avec 4 processeurs et 16 Go de RAM »

Modification des coûts et ajout de services

Vous pouvez ajuster les coûts sur site et ajouter AWS des services à votre évaluation par chat.

Exemples d'instructions pour les ajustements sur site :

- « Augmenter les coûts sur site de 15 % pour tenir compte de la prochaine actualisation du matériel »
- « Ajoutez des coûts de maintenance annuels de 100 000$ à la base de référence sur site »

Vous pouvez également ajouter des estimations de coûts approximatives pour les AWS services qui ne sont pas entièrement pris en charge par les évaluations AWS Transform. Cela fournit une analyse plus complète, mais ces estimations sont moins précises que les recommandations automatisées.

- « Ajouter les coûts AWS de sauvegarde pour tous les serveurs migrés »
- « Incluez les coûts CloudWatch de surveillance d'Amazon dans l'estimation »
- « Ajoutez les coûts de AWS Direct Connect pour une connexion de 10 Gbit/s »

Comparaison de scénarios

Vous pouvez créer plusieurs scénarios d'évaluation avec différentes hypothèses et les comparer pour identifier la stratégie de migration optimale.

Création de scénarios

Essayez des instructions telles que :

- « Créez un scénario BYOM pour la migration de bases de données SQL Server vers RDS for SQL Server »
- « Créez un scénario avec Database Savings Plans for RDS for SQL Server »
- « Créez un scénario LI pour toutes les charges de travail SQL Server sur EC2 »
- « Créez un scénario avec toutes les charges de travail dans us-west-2 »

Comparaisons en cours

Voici quelques exemples d'instructions :

- « Montrez-moi une comparaison des coûts pour tous les scénarios »
- « Quel scénario présente le coût total de propriété le plus bas ? »

What-if analyse

Modélisez l'impact de modifications spécifiques sans créer de nouveau scénario complet.

Exemples d’invites :

- « Et si je déplaçais mes charges de travail SQL Server vers RDS for SQL Server au lieu d'EC2 ? »
- « Quelle est la différence de coût entre BYOM et licence incluse pour RDS for SQL Server ? »
- « Et si j'exclus les 50 plus petits serveurs de la migration ? »
- « Et si je n'utilisais que des instances optimisées pour le stockage ? »
- « Quel est l'impact du passage des volumes gp3 aux volumes io2 ? »

Génération de livrables

Une fois votre évaluation terminée, vous pouvez générer des livrables dans plusieurs formats. Le tableau suivant décrit les formats de sortie disponibles.

Format	Description	Personnalisation
PPTX () PowerPoint	Présentation exécutive avec résumé des conclusions et des recommandations	Structure fixe

Format	Description	Personnalisation
XLSX (Excel)	Exportation détaillée des données avec recommandations au niveau du serveur et ventilation des coûts	Structure fixe
PDF	Document de rapport	Personnalisable par chat

Rubriques en relation

- Premiers pas
- Tâches personnalisées
- Outil de découverte

Outil de découverte

L'outil de AWS Transform découverte vous permet de découvrir automatiquement l'inventaire des serveurs de votre organisation afin de préparer la migration. L'outil prend en charge VMware vCenter Hyper-V, Microsoft et les serveurs importés. Pour utiliser l'outil de découverte, vous configurez une ou plusieurs sources de découverte, vous laissez l'outil s'exécuter, puis vous examinez les résultats dans le volet Inventaire découvert.

Une fois que vous avez configuré une source de découverte, l'outil de découverte commence à collecter des informations. Le temps nécessaire à l'outil de découverte pour analyser complètement votre réseau dépend de la taille de votre environnement. Pour une analyse de rentabilisation de la migration directionnelle, vous pouvez utiliser les fichiers MPA (Migration Portfolio Assessment) générés par l'outil une fois la collecte des serveurs terminée.

Flux de travail des outils de découverte

Le flux de travail de l'outil de découverte comprend deux types d'activités :

- Activités de configuration
- Examen et utilisation des données

Les étapes suivantes décrivent comment installer et utiliser l'outil de découverte et comment utiliser les données collectées :

1. Installez l'outil de découverte.
2. Configurez les sources de découverte. Vous pouvez configurer un ou plusieurs des éléments suivants : VMware vCenter, Microsoft Hyper-V hosts ou serveurs via une importation de fichier CSV. La découverte des données commence une fois que vous avez configuré une source.
3. Configurez l'accès au système d'exploitation, puis vérifiez l'état de collecte des serveurs, des bases de données et des connexions réseau.
    - Modifiez les informations d'identification du système d'exploitation selon vos besoins.
4. (Facultatif) Configurez les informations d'identification Oracle pour activer la collecte directe de données SQL ou utilisez la détection de OS-level secours via SSH ou WinRM.
5. Pour générer une analyse de rentabilisation de la migration, téléchargez le fichier .zip dans l'évaluation de la migration, ou décompressez-le et chargez les fichiers MPA depuis le répertoire

mpa_exports. L'exportation inclut des données provenant de toutes les sources configurées et contient des fichiers MPA pour VMware et des serveurs importés. Hyper-V

L'outil de découverte prend en charge les chemins de découverte suivants :

- Découverte automatique de VMware vCenter : découvrez automatiquement les serveurs gérés par VMware vCenter.
- Hyper-V découverte automatique — Découvre automatiquement les serveurs gérés par des Hyper-V hôtes Microsoft.
- Importation du serveur : importez manuellement l'inventaire du serveur via un fichier CSV.

Configuration de l'outil de découverte

Conditions préalables

Les conditions requises pour utiliser l'outil de AWS Transform découverte sont les suivantes :

Prérequis généraux

- L'outil nécessite 4 vCPU, 16 Go de RAM et un disque dur de 35 Go.
- Le protocole DHCP doit être disponible sur le réseau pour la machine virtuelle de l'outil de découverte.
- L'outil collecte des données en utilisant une approche centralisée. Les serveurs concernés doivent autoriser la connectivité entrante depuis la machine virtuelle de l'outil de découverte (ports par défaut, la configuration de port personnalisée est prise en charge) :
  - Linux — SSH TCP/22
  - Windows — TCP/5985 pour HTTP, TCP/5986 pour HTTPS
  - SNMP — UDP/161 (utilisé uniquement pour la collecte réseau, pas pour les métriques du système d'exploitation)
- Pour Linux, comptes d'utilisateurs qui peuvent utiliser SSH pour se connecter au serveur. L'outil de découverte exécute des commandes via SSH pour la collecte du réseau et les métriques du système d'exploitation. La plupart des commandes s'exécutent en tant qu'utilisateur normal. Un petit nombre de commandes tentent de recourir à sudo et de revenir automatiquement en cas d'indisponibilité de sudo : `dmidecode` (UUID du serveur et fabricant), `lvdisplay` (détection LVM) et/ou (connexions réseau avec `ss` informations de `netstat` processus). Sans sudo, l'outil de

découverte collecte toujours la majorité des données, mais les informations relatives à l'UUID, au LVM et au réseau au niveau des processus seront absentes. Nous recommandons de configurer un sudo sans mot de passe pour l'utilisateur SSH afin de garantir une collecte complète des données. Pour une analyse complète, voirthe section called “Autorisations requises”.

Prérequis pour VMware

- VMware vCenter Server version 6.5, 6.7, 7.0 ou 8.0.
- Autorisations pour déployer un OVA dans votre VMware vCenter.
- Pour la configuration de VMware vCenter Server, un utilisateur de vCenter dont le Read-Only rôle est attribué au niveau du centre de données racine. Pour en savoir plus, consultez the section called “Autorisations requises”.

Hyper-V prérequis

- Windows Server avec le Hyper-V rôle activé.
- WinRM activé sur Hyper-V les hôtes.
- Un compte utilisateur membre des groupes d'utilisateurs de gestion à distance, d'Hyper-V administrateurs et d'utilisateurs du moniteur de performance sur chaque Hyper-V hôte, avec un accès WMI en lecture à l'espace de `root\cimv2` noms. Pour en savoir plus, consultez the section called “Autorisations requises”.
- Authentification prise en charge : NTLM (HTTPS uniquement) et Kerberos (HTTP ou HTTPS).

Conditions préalables à l'importation du serveur

- Un fichier CSV contenant les noms d'hôte ou les adresses IP du serveur et les noms d'identification (facultatif) qui correspondent aux noms conviviaux des informations d'identification du système d'exploitation configurées ou à configurer dans l'outil de découverte. Le fichier CSV doit utiliser les en-têtes suivants :

```
hostname_or_ip,os_credential_name,oracle_credential_name
```

- Les serveurs doivent être accessibles depuis la machine virtuelle de l'outil de découverte. Ports par défaut : port SSH 22 pour Linux, 5985/5986 port WinRM pour Windows. Les ports personnalisés sont pris en charge.

Prérequis pour le programme d'installation Linux

- Une distribution Linux prise en charge : Amazon Linux 2, Amazon Linux 2023, RHEL 8-9, Rocky Linux 8-9, 9, Ubuntu 20.04—24.04, AlmaLinux Debian 10—12 ou SLES 15 SP5.
- Minimum 4 vCPU, 16 Go de RAM, 35 Go d'espace disque disponible.
- Le port 5000 doit être disponible (non utilisé par un autre service).
- systemd est requis pour la gestion des services.
- La machine virtuelle de l'outil de découverte doit avoir un accès réseau à votre infrastructure cible. Ports par défaut : vCenter sur le port 443, Hyper-V hôtes sur le port 5985/5986, serveurs sur le port 22. Les ports personnalisés sont pris en charge pour SSH, WinRM et SNMP.

Prérequis pour la base de données Oracle

- Accès réseau depuis l'outil de découverte aux hôtes Oracle sur le port 1521 (ou port personnalisé).
- Versions Oracle prises en charge : vous pouvez collecter Oracle Database 12c version 1 (12.1) et versions ultérieures via des connexions SQL directes. OS-level la détection de repli fonctionne avec toutes les versions d'Oracle.
- Un compte de service Oracle en lecture seule doté de l'autorisation SELECT_CATALOG_ROLE. Pour en savoir plus, consultez the section called “Base de données Oracle (SQL)”.
- Pour la OS-level détection des failles : accès SSH ou WinRM à l'hôte Oracle (utilise les informations d'identification du système d'exploitation existantes).

Déploiement sur VMware

Spécifications des machines virtuelles VMware

- Système d'exploitation — Amazon Linux 2023
- RAM — 16 Go
- Processeur : 4 cœurs
- Disques — 35 Go
- Exigences de VMware — Voir les exigences d'hôte VMware pour exécuter AL2023 sur VMware

Déployez le VMware OVA

1. Téléchargez le fichier OVA à partir de cette URL : https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.ova
2. Connectez-vous à vCenter en tant qu'administrateur VMware.
3. Utilisez l'une des méthodes suivantes pour installer le fichier OVA :

   a. Utilisez l'interface utilisateur : choisissez Fichier, choisissez Déployer le modèle OVF, sélectionnez le fichier OVA de l'outil de découverte que vous avez téléchargé à l'étape 1, puis exécutez l'assistant. Assurez-vous que les paramètres du proxy dans le tableau de bord de gestion du serveur sont correctement configurés.

   b. Utilisez la ligne de commande : pour installer le fichier OVA de l'outil de découverte à partir de la ligne de commande, téléchargez et utilisez l'outil VMware Open Virtualization Format Tool (ovftool). Pour télécharger ovftool, sélectionnez une version sur la page de documentation de l'outil OVF. Voici un exemple d'utilisation de l'outil de ligne de commande ovftool pour installer le fichier OVA de l'outil de découverte.

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

   Descriptions des valeurs remplaçables dans l'exemple :

   - Le nom est le nom que vous souhaitez utiliser pour la machine virtuelle de votre outil de découverte.
   - La banque de données est le nom de la banque de données de votre vCenter.
   - Le nom du fichier OVA est le nom du fichier OVA de l'outil de découverte téléchargé.
   - username/password Il s'agit de vos informations d'identification vCenter.
   - Le vcenterurl est l'URL de votre vCenter.
   - Le chemin vi est le chemin d'accès à votre hôte VMware ESXi.
4. Localisez l'outil de découverte déployé dans votre vCenter. Right-click la machine virtuelle, puis choisissez Power, Power On.
5. Après quelques minutes, l'adresse IP de l'outil de découverte s'affiche dans vCenter. Vous utilisez cette adresse IP pour vous connecter à l'outil de découverte.

Déployez sur Hyper-V

Hyper-V spécifications des machines virtuelles

- Système d'exploitation — Amazon Linux 2023
- RAM — Nous recommandons d'allouer au moins 16 Go
- CPU — Nous recommandons d'allouer au moins 4 cœurs
- Disques — 35 Go (inclus dans le VHD)
- Hyper-V exigences — Voir les exigences de Hyper-V l'hôte pour exécuter AL2023 sur Hyper-V

Déployez le Hyper-V VHD

1. Téléchargez le fichier VHD à partir de cette URL : https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.vhd
2. Copiez le fichier VHD sur la machine Windows Server sur laquelle le Hyper-V rôle est activé.
3. Ouvrez le Hyper-V gestionnaire.
4. Choisissez Nouveau, puis Machine virtuelle.
5. Complétez l'assistant de configuration. Sur la page Spécifier la génération, sélectionnez Génération 1. Les machines virtuelles de génération 2 ne prennent pas en charge le format VHD. Sur la page Attribuer de la mémoire, allouez au moins 16 384 Mo. Sur la page Connect Virtual Hard Disk, choisissez Utiliser un disque dur virtuel existant et sélectionnez le fichier VHD que vous avez copié.
6. Démarrez la machine virtuelle. Après quelques minutes, consultez l'onglet Mise en réseau de la machine virtuelle dans le Hyper-V gestionnaire pour trouver l'adresse IP, ou connectez-vous à la console de la machine virtuelle et lancez-la`ip addr`. Vous utilisez cette adresse IP pour vous connecter à l'outil de découverte.

Déploiement sous Linux

L'outil de découverte est disponible en tant qu'installateur Linux autonome à déployer sur des distributions Linux prises en charge. Utilisez cette option lorsque vous souhaitez installer l'outil de découverte directement sur un serveur Linux existant au lieu de déployer une machine virtuelle.

Spécifications du serveur Linux

- RAM — Nous recommandons d'allouer au moins 16 Go
- CPU — Nous recommandons d'allouer au moins 4 cœurs
- Disques — 35 Go

Distributions prises en charge :

- Amazon Linux — Amazon Linux 2, Amazon Linux 2023
- Red Hat Enterprise Linux et ses dérivés : RHEL 8—9, Rocky Linux 8—9, 9 AlmaLinux
- Ubuntu — 20,04, 22,04, 24,04
- Debian — 10, 11, 12
- SUSE — SLES 15 SP5

Installation de l'outil de découverte

Téléchargez le script d'installation à partir de cette URL : https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh

Pour installer l'outil de découverte sous Linux

1. Téléchargez le script d'installation sur votre serveur 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. (Facultatif) Exécutez le contrôle de compatibilité pour vérifier que votre système répond aux exigences.

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

3. Installez l'outil de découverte. Choisissez l'une des options suivantes :

   Option 1 : Installation avec installation automatique des dépendances (recommandée)

   Cette option installe automatiquement toutes les dépendances système manquantes avant d'installer le service.

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

Option 2 : Installation sans installation automatique des dépendances

Cette option vérifie les dépendances manquantes et affiche les erreurs avec les instructions d'installation manuelle si des dépendances critiques sont absentes. Utilisez cette option si votre organisation restreint l'installation automatique des packages et que vous préférez gérer les packages système manuellement.

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

4. Démarrez le service d'outils de découverte.

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

5. Accédez à l'outil de découverte à l'adressehttps://*ip_address*:5000.

Pour désinstaller l'outil de découverte, exécutezsudo ./AWS-Transform-discovery-tool.sh uninstall.

Vous pouvez également utiliser les commandes suivantes pour gérer le service :

- sudo ./AWS-Transform-discovery-tool.sh status— Vérifiez si le service est en cours d'exécution.
- sudo ./AWS-Transform-discovery-tool.sh stop— Arrêtez le service.
- sudo ./AWS-Transform-discovery-tool.sh logs— Afficher les journaux de service.

Dépendances du système

Le programme d'installation vérifie les dépendances système suivantes :

Dépendance	Sévérité	Objectif
OpenSSL	Critique	Génère la clé de chiffrement de la base de données
libcrypt	Critique	Requis par le moteur d'exécution Python

Dépendance	Sévérité	Objectif
Bibliothèques Kerberos	Avertissement	Nécessaire pour l'authentification Kerberos sur les serveurs Windows. Sans cela, le NTLM et l'authentification de base fonctionnent toujours.

Des dépendances critiques sont nécessaires au démarrage de l'outil de découverte. S'ils sont absents et que vous avez choisi l'option 2 (sans`--install-deps`), le programme d'installation affiche un message d'erreur avec des instructions pour les installer manuellement. Warning-level les dépendances sont facultatives : le programme d'installation vous avertit mais poursuit l'installation.

> **Note**
>
> Le programme d'installation vérifie la compatibilité du système, y compris la version de la glibc et la disponibilité de Systemd. Sur les systèmes dotés de systemd 250 ou version ultérieure (Amazon Linux 2023, RHEL 9, Rocky 9, 9, Ubuntu 24.04+, AlmaLinux Debian 12+), la clé de chiffrement de la base de données est chiffrée au repos à l'aide de systemd-creds. Sur les anciens systèmes, la clé de chiffrement est stockée sous forme de fichier protégé par autorisation.

Configuration de l'outil de découverte

Accédez à la console de l'outil de découverte

1. Dans un navigateur Web, accédez à :`https://`*`ip_address`*`:5000`, où se *`ip_address`* trouve l'adresse IP de l'outil de découverte de Deploy Discovery Tool. L'outil de découverte utilise un certificat auto-signé pour la connexion HTTPS, ce qui entraîne un avertissement de sécurité. Choisissez Accepter le risque et passez à la console de l'outil de découverte.
2. Si vous accédez à la console de l'outil de découverte pour la première fois, créez un mot de passe de connexion à l'outil de découverte. Créez un mot de passe que vous utiliserez pour vos futures connexions.

> **Important**
>
> N'oubliez pas ce mot de passe : il n'existe aucun mécanisme de récupération du mot de passe.

Accès à la machine virtuelle de l'outil de découverte

- L'outil de découverte VM est fourni par défaut avec un nom d'utilisateur et un mot de passe (« découverte », « mot de passe »). Pour renforcer la sécurité, nous vous recommandons de mettre à jour le mot de passe en l'utilisant `sudo passwd discovery` après vous être connecté à la machine virtuelle via la console de votre hyperviseur (par exemple, vSphere Client pour VMware Hyper-V ou Manager Hyper-V pour).
- L'accès SSH est désactivé par défaut. Les utilisateurs peuvent utiliser des alias `enablessh` et des `disablessh` alias préconfigurés pour accéder en enable/disable SSH à la machine virtuelle de l'outil de découverte. Les utilisateurs peuvent se connecter à la machine virtuelle via SSH `ssh discovery@<VM-IP>` après avoir activé l'accès SSH. Les utilisateurs sont invités à désactiver l'accès SSH la plupart du temps et à ne l'activer que lorsqu'ils en ont réellement besoin. Le changement de mot de passe est imposé lors de l'exécution`enablessh`.
- Pour accéder au répertoire de données de l'outil de découverte à l'`/home/ec2-user/.local/share/DiscoveryTool`adresse, nous vous recommandons de passer à `ec2-user` en exécutant`sudo su ec2-user`.

Configuration de l'authentification Kerberos

L'authentification Kerberos est la méthode recommandée pour se connecter aux serveurs Windows à partir de l'outil de découverte. L'outil de découverte VM utilise les bibliothèques Kerberos natives d'Amazon Linux 2023 pour s'authentifier auprès de votre domaine Active Directory.

Voici les points clés concernant l'authentification Kerberos sur la machine virtuelle de l'outil de découverte :

- Utilisez la `kinit` commande pour obtenir un ticket Kerberos et `klist` vérifier le ticket.
- Le fichier de configuration Kerberos se trouve à l'adresse. `/etc/krb5.conf`
- Avant de configurer l'outil de découverte, vérifiez qu'il fonctionne correctement `kinit` à partir de la CLI sur la machine virtuelle de l'outil de découverte.

Conditions requises pour Kerberos

Avant de configurer l'authentification Kerberos, vérifiez que vous disposez des informations et de la connectivité réseau suivantes.

1. Obtenez les informations suivantes auprès de votre administrateur Active Directory :
   - Le nom de domaine Kerberos (généralement votre nom de domaine en majuscules, par exemple). `EXAMPLE.COM`
   - Le nom d'hôte ou l'adresse IP du centre de distribution de clés (KDC), qui est généralement un contrôleur de domaine (par exemple,`dc01.example.com`).
   - Un compte de service autorisé à s'authentifier auprès des serveurs Windows cibles.
2. Vérifiez que la machine virtuelle de l'outil de découverte dispose d'une connectivité réseau aux éléments suivants :
   - Le KDC sur le port 88 (TCP et UDP) pour l'authentification Kerberos.
   - Les serveurs Windows cibles sur les ports WinRM (5985 pour HTTP, 5986 pour HTTPS).

Configuration de Kerberos

Procédez comme suit pour configurer l'authentification Kerberos sur la machine virtuelle de l'outil de découverte.

1. SSH vers la machine virtuelle de l'outil de découverte.

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

2. Modifiez le fichier de configuration Kerberos à l'adresse. `/etc/krb5.conf`

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

   Ajoutez la configuration suivante, en remplaçant les valeurs d'espace réservé par les détails de votre environnement.

   ```
   [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 fait la distinction majuscules/majuscules. Le nom du domaine doit être en majuscules (par exemple`EXAMPLE.COM`, non`example.com`). Le nom de domaine de la `[domain_realm]` section doit être en minuscules.

Plusieurs domaines Active Directory

L'outil de découverte prend en charge plusieurs informations d'identification Kerberos pour différents domaines Active Directory. Chaque identifiant s'authentifie indépendamment. Vous pouvez donc configurer plusieurs identifiants normalement et l'isolation est automatique.

Si vous avez des serveurs dans plusieurs domaines, ajoutez des entrées pour chaque domaine de votre `/etc/krb5.conf` fichier :

```
[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. Vérifiez que vous pouvez obtenir un ticket Kerberos en exécutant la `kinit` commande.

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

   Entrez le mot de passe lorsque vous y êtes invité. Si la commande s'exécute sans erreur, l'authentification a réussi.

4. Vérifiez le ticket en exécutant la `klist` commande.

```
klist
```

   Le résultat attendu est similaire à ce qui suit.

```
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. Configurez l'outil de découverte avec le même principe distinguant majuscules et minuscules que celui que vous avez utilisé avec `kinit` (par exemple,`username@REALM.COM`).

Une `krb5.conf` configuration explicite n'est peut-être pas requise si votre environnement possède des enregistrements DNS SRV configurés pour la découverte de services Kerberos. Pour plus d'informations sur les options de configuration de Kerberos, consultez la documentation MIT Kerberos krb5.conf et le fichier d'exemple krb5.conf.

Rechercher la configuration Kerberos à partir de machines jointes à un domaine

Si vous ne disposez pas des détails de configuration de Kerberos, vous pouvez les récupérer à partir d'un ordinateur Windows joint au domaine. Exécutez les commandes suivantes à partir d'une invite de commande sur la machine jointe au domaine.

Pour trouver le nom de domaine, exécutez la commande suivante.

```
echo %USERDNSDOMAIN%
```

Exemple de sortie :

```
EXAMPLE.COM
```

Pour trouver le nom d'hôte du contrôleur de domaine, exécutez la commande suivante.

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

Exemple de sortie :

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

Mappez la sortie à votre `krb5.conf` configuration comme suit :

- Realm — Utilisez la valeur de `%USERDNSDOMAIN%` en majuscules (par exemple,`EXAMPLE.COM`).
- KDC — Utilisez le nom d'hôte DC indiqué dans la `nltest` sortie (par exemple,`dc01.example.com`).

Configuration de l'accès à vCenter

1. Sur la page de l'outil de découverte, sous Étape 1. Configurez les sources de découverte, choisissez Configurer les sources.
2. Sur la page Configurer les sources de découverte, indiquez le nom convivial, le vCenter FQDN/IP, le nom d'utilisateur et le mot de passe.
3. Choisissez Save configuration.

   L'outil de découverte commence à collecter les informations vCenter, comme décrit dans Discovered Inventory.

Après la configuration initiale, choisissez Modifier l'accès au vCenter dans le cadre d'état de l'outil Discovery pour modifier vos paramètres d'accès au vCenter.

L'outil de découverte collecte des données depuis tous les serveurs vCenter configurés en parallèle. Si un serveur vCenter est inaccessible pendant la collecte, l'outil signale un succès partiel et poursuit la collecte à partir des autres serveurs vCenter.

Si une machine virtuelle apparaît sur plusieurs serveurs vCenter (par exemple, en raison d'hôtes ESXi partagés ou de cross-vCenter vMotion), l'outil de découverte déduplique automatiquement les machines virtuelles. Chaque machine virtuelle unique n'apparaît qu'une seule fois dans l'inventaire.

Configuration de Hyper-V l'accès

1. Sur la page de l'outil de découverte, sous Étape 1. Configurez les sources de découverte, choisissez Configurer les sources.
2. Sur la page Configurer les sources de découverte, indiquez un nom convivial, le nom de domaine complet ou l'adresse IP de l'hôte, le type d'authentification (NTLM ou Kerberos), le nom d'utilisateur WinRM et le mot de passe WinRM.
3. Choisissez Save configuration.

   L'outil de découverte commence à collecter des Hyper-V informations, comme décrit dans Inventaire découvert.

La collecte commence automatiquement une fois que vous avez enregistré les informations d'identification.

Pour les clusters de Hyper-V basculement, vous pouvez ajouter plusieurs hôtes dans le même cluster. L'outil déduplique automatiquement les machines virtuelles qui apparaissent sur plusieurs hôtes.

Serveurs d'importation

1. Accédez à la page Serveurs d'importation depuis la page d'accueil de l'outil Discovery.
2. Préparez un fichier CSV avec les colonnes suivantes : `hostname_or_ip` (obligatoire), `os_credential_name` (facultatif) et `oracle_credential_name` (facultatif).

   - La `hostname_or_ip` valeur doit être une adresse IPv4 valide ou un nom de domaine complet (FQDN).
   - La `os_credential_name` valeur, si elle est fournie, doit correspondre au nom convivial d'un identifiant de système d'exploitation que vous avez déjà configuré (SSH, WinRM ou SNMP).

Laissez ce champ vide pour les serveurs sur lesquels vous n'avez pas encore configuré d'identifiant de système d'exploitation.

- La `oracle_credential_name` valeur, si elle est fournie, doit correspondre au nom convivial d'un identifiant Oracle que vous avez déjà configuré.

3. Téléchargez le fichier CSV. L'outil valide toutes les lignes et rejette le fichier si une ligne n'est pas valide.

Une fois l'importation réussie, l'outil lance automatiquement la collecte des métriques de base de données, de réseau et de système d'exploitation pour les serveurs importés, si les informations d'identification du système d'exploitation sont configurées. Si vous chargez un autre fichier CSV, les enregistrements existants sont mis à jour sans créer de doublons et les nouveaux enregistrements sont fusionnés dans l'inventaire.

Importer une autorité de certification autosignée dans l'outil de découverte (facultatif)

Cela est nécessaire lorsque vous utilisez WinRM sur HTTPS et que vous ciblez des serveurs à l'aide de certificats HTTPS WinRM signés par une autorité de certification (CA) autosignée, et que vous souhaitez activer « Valider le certificat SSL du serveur » dans l'outil de découverte.

Conditions préalables

1. Self-signed Certificat CA utilisé pour signer les certificats HTTPS WinRM sur les serveurs cibles
2. Certificat au format PEM (extension .pem ou .crt)

Pour importer une autorité de certification autosignée sur la machine virtuelle de l'outil de découverte :

1. Machine virtuelle de l'outil SSH to Discovery
2. Placez le ou les certificats CA qui ont signé les certificats WinRM de vos serveurs cibles dans le `/etc/pki/ca-trust/source/anchors/` répertoire Trust Store de la machine virtuelle de l'outil de découverte. Par exemple : `sudo cp winrm-ca.pem /etc/pki/ca-trust/source/anchors/winrm-ca.pem`. Remarque : Si vos serveurs cibles utilisent des certificats signés par différentes autorités de certification, copiez tous les certificats d'autorité de certification pertinents dans ce répertoire.
3. Mettez à jour le magasin de certificats de confiance : `sudo update-ca-trust`
4. Redémarrez la machine virtuelle

5. (Facultatif) Pour vérifier que les certificats ont bien été importés, vous pouvez exécuter la commande suivante. `sudo trust list –filter=ca-anchors | grep -A 5 "<certificate_name>"`

Voir Installation et configuration pour la gestion à distance de Windows

Configuration de l'outil de découverte pour l'accès au système d'exploitation

Configurez l'accès au système d'exploitation afin que l'outil de découverte puisse :

- Découvrez les bases de données pour effectuer une évaluation des bases de données et faciliter la migration des machines virtuelles,
- Suivez les connexions réseau entre les serveurs de votre inventaire, y compris le processus associé à chaque connexion, afin de faciliter le mappage des dépendances des applications et la planification des vagues. Seules les connexions dont les deux points de terminaison figurent dans l'inventaire de l'outil de découverte sont incluses.

Activer l'outil de découverte OS Access

1. Accédez à la page Configurer l'accès au système d'exploitation pour fournir les informations d'identification Windows et Linux.
2. Choisissez le protocole pour lequel vous souhaitez ajouter des informations d'identification.
3. Fournissez les informations d'identification requises pour le protocole sélectionné.
4. Sélectionnez cette option Auto-connectpour permettre à l'outil de découverte d'essayer toutes les informations d'identification fournies sur les serveurs découverts jusqu'à ce que les informations d'identification correspondantes soient trouvées pour chaque serveur.

   Consultez the section called “Utilisation de Auto-Connect la fonctionnalité avec prudence” les recommandations de sécurité importantes concernant la fonction de connexion automatique.
5. Choisissez Configurer et connecter.

Lorsque le processus de mise en correspondance du système d'exploitation est terminé, un message indiquant que la collecte de données est en cours s'affiche, ainsi qu'une erreur concernant les serveurs pour lesquels aucune correspondance d'informations d'identification n'a été trouvée.

Configuration des protocoles pris en charge

Vous devez configurer les protocoles WinRM, SSH et SNMP sur les serveurs cibles pour que l'outil de découverte puisse communiquer avec eux.

Configuration de WinRM et WMI

WinRM est automatiquement installé avec toutes les versions actuellement prises en charge du système d'exploitation Windows.

Pour vérifier ou modifier la configuration WinRM, utilisez l'outil de ligne de `winrm` commande :

- Vérifiez les écouteurs WinRM installés : `winrm enumerate winrm/config/listener`
- Vérifiez les configurations WinRM : `winrm get winrm/config`
- Exemple de commande pour configurer WinRM : `winrm quickconfig -transport:https`

Ports d'écouteur

Le port HTTP par défaut est 5985 ; le port HTTPS est 5986. Vous pouvez utiliser d'autres ports selon vos besoins. Les ports doivent être ouverts entre l'outil de découverte et les serveurs cibles.

Chiffrement

L'outil de découverte utilise une communication WinRM cryptée. Nous recommandons que les écouteurs WinRM installés sur les serveurs cibles utilisent également le chiffrement : `winrm set winrm/config/service '@{AllowUnencrypted="false"}'`

NTLM contre Kerberos

Les protocoles d'authentification WinRM Kerberos et NTLM sont pris en charge par l'outil de découverte. NTLM ne peut être utilisé qu'avec HTTPS et Kerberos peut être utilisé à la fois avec HTTP ou HTTPS.

Exigences WMI

L'outil de découverte interroge les espaces de noms WMI suivants. Le compte WinRM a besoin d'un accès en lecture à chaque espace de noms correspondant à vos modules de collection :

espace de noms WMI	Utilisé par
`root\cimv2`	Métriques du système d'exploitation, métadonnées de l' Hyper-V hôte, collection SQL Server
`root\virtualization\v2`	Hyper-V Inventaire des machines virtuelles
`root\StandardCIMV2`	Collection en réseau
`root\Microsoft\SqlServer\ComputerManagement*`	Collection SQL Server
`root\Microsoft\SqlServer\ReportServer\*`	Collection SQL Server (SSRS)

Pour la collecte sur le réseau, assurez-vous que les conditions suivantes sont remplies :

- Autoriser la connectivité réseau via ICMP
- Autoriser la connectivité réseau via le port TCP 135 et une plage de ports TCP éphémères (49152 - 65535)
- Désactiver l'UAC
- Les autorisations DCOM à distance sont configurées
- Créez un compte de service dédié avec les autorisations minimales requises
- Les autorisations d'espace de nommage WMI sont configurées pour les comptes Windows avec des espaces de noms :, class `\\root\\standardcimv2` `MSFT_NetTCPConnection`

Pour la collecte SQL Server, un compte Windows (local ou de domaine) appartenant au groupe d'administrateurs locaux est requis en raison des exigences d'autorisation complexes relatives aux objets WMI.

Configurer SSH

- Le port par défaut est 22. Les ports personnalisés sont pris en charge. Le port configuré doit être ouvert entre l'outil de découverte et les serveurs cibles.
- Pour que la collecte sur le réseau SSH fonctionne correctement, fournissez un utilisateur configuré pour le sudo sans mot de passe.

- Assurez-vous que les commandes suivantes sont disponibles sur les serveurs Linux cibles (installés par défaut sur la plupart des distributions) : `ss` ou `netstat` pour la collecte réseau,,,`lsblk`,,`iostat`,`dmidecode`,`smartctl`, `top` `ps` `freeip`, et `df` pour la collecte des métriques du système d'exploitation.

L'outil de découverte prend en charge deux méthodes d'authentification pour SSH :

Option 1 : nom d'utilisateur et mot de passe

Entrez le nom d'utilisateur et le mot de passe SSH. Il s'agit de la méthode d'authentification par défaut.

Option 2 : clé privée SSH

Fournissez le nom d'utilisateur SSH et une clé privée au format PEM. Pour utiliser cette option, choisissez la clé SSH dans le menu déroulant Type d'authentification lors de la configuration des informations d'identification SSH. Si la clé privée est chiffrée à l'aide d'une phrase secrète, saisissez-la dans le champ facultatif Phrase secrète de la clé.

Les formats clés suivants sont pris en charge :

- RSA
- ECDSA
- Ed25519
- Format OpenSSH
- Format PKCS #8

Les deux méthodes d'authentification prennent en charge la connexion automatique. Les informations d'identification sont stockées cryptées au repos.

Configuration du SNMP

- Le port par défaut est 161/UDP. Les ports personnalisés sont pris en charge. Le port configuré doit être ouvert entre l'outil de découverte et les serveurs cibles.
- Pour SNMP v2 : fournissez une chaîne communautaire en lecture seule qui peut accéder aux OID de connexion TCP.
- Pour SNMP v3 : fournir username/password et auth/privacy détailler une autorisation en lecture seule permettant d'accéder aux OID de connexion TCP

L'outil de découverte nécessite l'accès à :

- `"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)

Configuration de l'accès aux bases de données Oracle

Configurez l'accès à la base de données Oracle pour collecter les métadonnées détaillées de la base de données Oracle directement via des connexions SQL. Les métadonnées collectées incluent la topologie CDB et PDB, l'utilisation des fonctionnalités et les options installées. Ces données vous aident à planifier les migrations de bases de données Oracle avec plus de précision. Vous pouvez collecter Oracle Database 12c version 1 (12.1) et versions ultérieures via des connexions SQL directes. OS-level la détection de repli fonctionne avec toutes les versions d'Oracle.

Configurer les informations d'identification Oracle dans l'outil de découverte

1. Sur la page de l'outil de découverte, dans la barre latérale, choisissez Accès à la base de données.
2. Choisissez Ajouter des informations d'identification Oracle.
3. Saisissez les informations suivantes :
   - Nom convivial : nom descriptif pour cet identifiant (par exemple,`Oracle Production`).
   - Port : port du récepteur Oracle (par défaut 1521).
   - Nom du service : nom du service Oracle pour la base de données cible.
   - Nom d'utilisateur : nom d'utilisateur du compte de service Oracle.
   - Mot de passe : mot de passe du compte de service Oracle.
   - Auto-connect— Activez cette option pour tester les informations d'identification sur tous les serveurs de votre inventaire. Désactivez cette option pour attribuer manuellement les informations d'identification à des serveurs spécifiques.
4. Pour ajouter d'autres informations d'identification (par exemple, pour différents environnements Oracle), sélectionnez à nouveau Ajouter des informations d'identification Oracle.
5. Choisissez Enregistrer.

Modes d'identification

Lorsque vous configurez les informations d'identification Oracle, vous pouvez choisir entre deux modes :

- Manuel — Épinglez un identifiant sur un serveur spécifique. L'outil de découverte utilise ces informations d'identification exclusivement pour ce serveur. En cas d'échec de la connexion, aucune solution de repli ne se produit. Corrigez la configuration des informations d'identification pour résoudre le problème.
- Auto-connect— L'outil de découverte teste chaque identifiant de connexion automatique sur chaque serveur de votre inventaire. Lorsqu'un identifiant réussit pour un serveur, l'outil de découverte utilise cet identifiant pour tous les cycles de collecte suivants.

Flux de détection

Lorsque vous configurez les informations d'identification Oracle, l'outil de découverte essaie d'abord d'établir une connexion SQL directe. Si toutes les informations d'identification de base de données échouent, l'outil revient à la OS-level détection via SSH ou WinRM, afin que vous puissiez toujours découvrir les installations Oracle sans accès à la base de données.

Mise à jour de l'outil de découverte

L'outil de découverte ne possède pas de fonction de mise à jour automatique, mais vous recevrez une notification de rappel après 30 jours d'installation pour effectuer la mise à jour. Il est recommandé de maintenir l'application à jour pour recevoir les dernières fonctionnalités et correctifs de sécurité.

Pour mettre à jour manuellement l'outil

1. Téléchargez le dernier fichier image de l'outil de découverte (OVA pour VMware ou VHD pour Hyper-V) à partir du lien fourni.
2. (Facultatif) Nous vous recommandons de supprimer le fichier image de l'outil de découverte précédent avant de déployer le dernier.
3. Suivez les étapes décrites dans la section Déployer l'outil de découverte pour déployer la version mise à jour.

Révocation de l’accès

Vous pouvez révoquer l'accès à chaque source de découverte indépendamment. Lorsque vous révoquez l'accès à une source, les données des autres sources ne sont pas affectées.

- Révocation de l'accès à vCenter : supprime les informations d'identification et les données de vCenter. VMware-collected Ne supprime pas les Hyper-V données, les données de serveur importées ou les informations d'identification du système d'exploitation.
- Révocation de Hyper-V l'accès : supprime uniquement les Hyper-V informations d'identification et les Hyper-V-collected données.
- Suppression de serveurs importés — Supprime les serveurs importés de l'inventaire. Les données de collecte en aval (réseau, base de données) collectées auprès de ces serveurs sont conservées.

Autorisations requises pour l'outil de découverte

L'outil de découverte se connecte à votre infrastructure à l'aide de plusieurs protocoles. Chaque protocole et module de collecte nécessite des autorisations de compte spécifiques. Cette section décrit les autorisations minimales requises pour une collecte complète des données, ainsi que les données que vous perdez si certaines autorisations ne sont pas disponibles.

VMware vCenter

L'outil de découverte se connecte à VMware vCenter Server sur le port 443 (HTTPS) et effectue des opérations en lecture seule. Aucune modification n'est apportée à votre environnement vCenter.

Rôle minimum requis : Read-Only, attribué au niveau racine du vCenter.

Le Read-Only rôle fournit tous les accès dont l'outil de découverte a besoin pour collecter l'inventaire des machines virtuelles (nom, UUID, processeur, mémoire, disque, réseau, état de l'alimentation, système d'exploitation invité) et les indicateurs de performance (utilisation du processeur, utilisation de la mémoire, IOPS du disque et débit).

Recommandation : créez un utilisateur vCenter dédié doté du Read-Only rôle intégré au niveau du centre de données racine.

Hyper-V hôtes (Windows)

L'outil de découverte se connecte aux Hyper-V hôtes via WinRM (port 5985 pour HTTP, port 5986 pour HTTPS) et exécute des PowerShell commandes pour collecter l'inventaire des machines virtuelles, les métadonnées des hôtes et les performances de stockage.

Nombre minimum d'adhésions à un groupe requis pour chaque Hyper-V hôte :

groupe Windows	Pourquoi c'est nécessaire
Utilisateurs de la gestion à distance	Accès à distance WinRM de base
Hyper-V Administrateurs	Collecte de l'inventaire des machines virtuelles (liste des machines virtuelles, disque, réseau, mémoire, système d'exploitation invité)
Utilisateurs du moniteur de performances	Compteurs de I/O performances de stockage (read/write IOPS et débit par machine virtuelle)

Le compte a également besoin d'un accès WMI en lecture à l'espace de `root\cimv2` noms correspondant à la version du système d'exploitation hôte et à l'UUID matériel. Cet accès est accordé par défaut aux administrateurs locaux mais doit être configuré explicitement pour les comptes non administrateurs.

Recommandation : créez un compte de service de domaine dédié et ajoutez-le aux groupes d'utilisateurs de gestion à distance, d' Hyper-V administrateurs et d'utilisateurs du moniteur de performance sur chaque Hyper-V hôte. Évitez d'utiliser des comptes d'administrateur de domaine.

Serveurs Linux (SSH)

L'outil de découverte se connecte aux serveurs Linux via SSH (port 22) pour collecter les métriques du système d'exploitation, les connexions réseau et l'inventaire des serveurs. La plupart des collectes de données s'effectuent en tant qu'utilisateur normal. Un petit nombre de commandes tentent `sudo` de revenir automatiquement en arrière si sudo n'est pas disponible.

Accès minimum requis : un compte utilisateur SSH qui peut se connecter au serveur cible.

Accès recommandé : le même utilisateur SSH est configuré avec sudo sans mot de passe pour une collecte complète des données.

Qu'est-ce qui nécessite sudo et que se passe-t-il sans sudo :

Données collectées	Besoin de Sudo ?	Ce que vous perdez sans sudo
Nom du serveur, système d'exploitation, processeur, mémoire, IP, nombre de disques	Non	Rien — collecté en tant qu'utilisateur régulier
Utilisation du processeur, de la mémoire et du réseau	Non	Rien — collecté en tant qu'utilisateur régulier
IOPS, débit et espace sur le disque	Non	Rien — collecté en tant qu'utilisateur régulier
Configuration de l'interface réseau	Non	Rien — collecté en tant qu'utilisateur régulier
Processus en cours (nom, PID, commande)	Non	Rien — collecté en tant qu'utilisateur régulier
UUID du serveur et UUID SMBIOS	Oui	Les champs UUID sont vides lors de l'exportation
Fabricant du matériel (détection physique ou virtuelle)	Oui	La détection des types de ressources est moins précise sur les anciennes distributions
Détection de volumes logiques LVM	Oui	Volumes LVM non détectés ; le type de volume peut s'afficher comme « Inconnu »
Connexions réseau avec nom de processus et PID	Oui	Les connexions sont toujours collectées, mais sans attribution de processus (les colonnes PID et nom de processus sont vides)
OS-level Détection de la base de données Oracle (solution de secours lorsque les informations d'identification Oracle ne sont pas configurées)	Oui	La détection de présence Oracle de base (oratab, moniteur de processus) fonctionne sans sudo. La collecte détaillée (opatch, lsnrctl, ASM, Grid Infrastructure) nécessite un accès sans mot de passe `sudo -u oracle` aux fichiers binaires d'Oracle Home.

> **Note**
>
> L'outil de découverte n'échoue jamais complètement en raison de l'absence de sudo. Il collecte ce qu'il peut et rapporte des résultats partiels. Cependant, pour les données les plus complètes, en particulier le mappage des dépendances réseau avec les noms de processus, nous recommandons le sudo sans mot de passe.

Utilitaires requis sur les serveurs cibles : Les commandes suivantes doivent être disponibles (installées par défaut sur la plupart des distributions Linux) : `ss` ou `netstat` `lsblk` `top` `psfree`,`ip`,,`df`,`hostname`,`cat`,`nproc`, et`grep`. Facultatif pour des données supplémentaires : `iostat` (I/O détail du disque), `dmidecode` (UUID matériel), `smartctl` (type d'interface disque), `lvdisplay` (détection LVM).

Serveurs Windows (WinRM) — Métriques du système d'exploitation

L'outil de découverte se connecte aux serveurs Windows via WinRM pour collecter les métriques du système d'exploitation (inventaire des serveurs, performances, stockage, interfaces réseau et processus en cours d'exécution).

Accès minimum requis : compte WinRM-enabled utilisateur avec accès à distance au serveur cible.

Accès recommandé : un utilisateur du groupe d'administrateurs local pour la collecte complète des données.

Niveau d'autorisation	Ce qu'il permet	Ce que vous perdez sans elle
Utilisateurs de gestion à distance (accès WinRM)	Toutes les collectes de données Windows	Aucune donnée collectée depuis le serveur
Accès en lecture WMI à `root\cimv2`	Nom du serveur, version du système d'exploitation, mémoire, UUID, numéro de série du BIOS, espace disque	Les champs d'inventaire du serveur sont vides
Utilisateurs du moniteur de performances	Utilisation du processeur, débit réseau, IOPS du disque et débit	Indicateurs de performance non collectés

Niveau d'autorisation	Ce qu'il permet	Ce que vous perdez sans elle
Administrateur local	Noms du propriétaire du processus en cours d'exécution	Liste des processus collectée mais la user/owner colonne est vide

> **Note**
>
> L'adhésion à un administrateur local accorde implicitement aux utilisateurs de Performance Monitor l'accès et l'accès en lecture au WMI, de sorte qu'elle répond à toutes les exigences ci-dessus.

> **Note**
>
> La détection de OS-level secours d'Oracle Database sous Windows utilise des requêtes de registre `Get-Service` et des `Get-Process` commandes lorsque les informations d'identification Oracle ne sont pas configurées. Ces commandes nécessitent uniquement l'accès standard des utilisateurs de gestion à distance. Aucune autorisation supplémentaire au-delà des exigences relatives aux métriques du système d'exploitation n'est requise.

Serveurs Windows (WinRM) : collection SQL Server

La collection SQL Server découvre les instances SQL Server, Reporting Services (SSRS) et Integration Services (SSIS) sur les serveurs Windows.

Accès recommandé : un utilisateur du groupe d'administrateurs local sur chaque serveur Windows cible.

L'administrateur local est recommandé car la découverte de SQL Server interroge plusieurs espaces de noms WMI et nécessite un accès élevé pour certaines opérations :

Ce qui est découvert	Autorisation requise	Ce que vous perdez sans elle
Instances du moteur de base de données SQL Server (version, édition, état)	Accès en lecture WMI aux espaces de noms `root\Micr`	Instances de SQL Server non découvertes

Ce qui est découvert	Autorisation requise	Ce que vous perdez sans elle
	`osoft\SqlServer\ComputerManagement*`	
Services de création de rapports SQL Server (SSRS)	Accès en lecture WMI aux espaces de noms `root\Microsoft\SqlServer\ReportServer`	Composants SSRS non découverts
Configuration de l'URL et du port SSRS	Privilèges élevés (administrateur local)	Détails de réservation de l'URL SSRS manquants
SQL Server Integration Services (SSIS)	Accès en lecture au registre (HKLM)	Version et édition SSIS manquantes
Port-to-service association	Accès à l'énumération des écouteurs TCP	Impossible d'associer les ports d'écoute aux services SQL Server

> **Note**
>
> La collection SQL Server est Windows-only. L'outil de découverte ignore les serveurs Linux pour la découverte de SQL Server.

Base de données Oracle (SQL)

La collecte de base de données Oracle se connecte directement aux instances Oracle sur le port 1521 (ou un port personnalisé) pour collecter les métadonnées de base de données. L'outil de découverte ne nécessite aucun privilège DBA ou SYSDBA.

Accès minimum requis : un compte de service Oracle en lecture seule doté de la subvention SELECT_CATALOG_ROLE.

L'outil de découverte n'accède pas aux vues du pack de diagnostic ou du pack de réglage. Aucune licence Oracle supplémentaire n'est donc requise pour la collecte de données.

SQL pour créer le compte :

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

OS-level solution de secours : si les informations d'identification de base de données ne sont pas configurées ou si la connexion échoue, l'outil de découverte utilise les informations d'identification du système d'exploitation SSH ou WinRM existantes pour détecter les installations Oracle. Aucune autorisation de Oracle-specific système d'exploitation supplémentaire n'est requise au-delà de celles requises par le module de métriques du système d'exploitation.

Collection en réseau

La collecte réseau utilise différents protocoles en fonction du système d'exploitation du serveur :

Système d'exploitation du serveur	Protocole	Autorisations nécessaires
Linux	SSH	Utilisateur normal pour les données de connexion. Sudo sans mot de passe recommandé pour les détails au niveau du processus (PID et nom du processus).
Linux	SNMPv2	Chaîne communautaire en lecture seule avec accès à la MIB TCP (tcpConnState, tcpConnectionProcess) et à la MIB des ressources hôtes (hr). SWRunName
Linux	SNMP v3	Un utilisateur USM disposant d'un accès en lecture aux mêmes MIB que SNMPv2. Supporte les niveaux de sécurité no AuthNoPrivNoPriv, auth et AuthPriv.
Windows	WinRM	Accès en lecture WMI à l'espace de `root\StandardCIMV2` noms (classe MSFT_NetTcpConnection).

Référence rapide : autorisations minimales par cas d'utilisation

Cas d’utilisation	Account type (Type de compte)	Autorisations minimales
Découverte de machines virtuelles VMware	Utilisateur de vCenter	Read-Only rôle au niveau du centre de données racine
Hyper-V Découverte de machines virtuelles	Domaine Windows ou compte local	Utilisateurs de gestion à distance + Hyper-V Administrateurs + Utilisateurs du moniteur de performance sur chaque hôte
Métriques du système d'exploitation Linux : données complètes	Utilisateur SSH	Sudo sans mot de passe
Métriques du système d'exploitation Linux — données partielles	Utilisateur SSH	Utilisateur régulier (pas de sudo). Les informations sur l'UUID, le fabricant, le LVM et le processus réseau seront manquantes.
Métriques du système d'exploitation Windows : données complètes	Utilisateur WinRM	Administrateur local
Métriques du système d'exploitation Windows : données de base	Utilisateur WinRM	Utilisateurs de gestion à distance et accès en lecture WMI à `root\cimv2`
Découverte de bases de données SQL Server	Utilisateur WinRM	Administrateur local
Découverte de bases de données Oracle (SQL)	compte de service Oracle	SELECT_CATALOG_ROLE (lecture seule, pas de DBA ni de SYSDBA)

Cas d’utilisation	Account type (Type de compte)	Autorisations minimales
Collection réseau — Linux (SSH)	Utilisateur SSH	Sudo sans mot de passe pour les données au niveau du processus ; utilisateur normal pour les données de connexion uniquement
Collection réseau — Linux (SNMP)	Chaîne de communauté SNMP ou utilisateur USM	Accès en lecture aux MIB TCP et aux ressources hôtes
Collection réseau — Windows	Utilisateur WinRM	Accès en lecture WMI à `root\StandardCIMV2`

Collecte des données

Calendrier de collecte des outils Discovery

Après votre collecte de découverte initiale, l'outil de découverte continue de fonctionner selon un calendrier échelonné afin d'éviter toute contention de ressources :

- VMware Discovery : toutes les heures (à 00h00 UTC)
- Hyper-V découverte — toutes les heures (à 20 h UTC)

L'outil de découverte collecte également les métriques du système d'exploitation par le biais des modules indépendants suivants, chacun ayant son propre calendrier échelonné :

- Mesures du réseau : toutes les 15 secondes, cela peut être moins fréquent dans les grands environnements
- Mesures de performance du serveur : toutes les 10 minutes (à :03, :13, :23, :33, :43, :53 UTC)
- Mesures des performances de stockage : toutes les 10 minutes (à :07, :17, :27, :37, :47, :57 UTC)
- Processus en cours : toutes les heures (à 40 UTC)
- Données de mise en service du serveur : tous les jours (à 00h05 UTC)
- Données relatives au provisionnement du stockage : tous les jours (à 00h35 UTC)
- Interfaces réseau — tous les jours (à 01:05 UTC)

- Découverte de SQL Server, tous les jours (à 03:05 UTC)
- Découverte de bases de données Oracle, tous les jours (à 05:05 UTC)

Vous pouvez démarrer, arrêter ou déclencher indépendamment chaque module de métriques du système d'exploitation en utilisant Collect data now.

Pour exécuter manuellement une collection, dans le menu Actions, choisissez :

- Démarrer — Active le module de découverte.
- Arrêter : désactive le module de découverte.
- Collectez des données dès maintenant : lance immédiatement la découverte. Utilisez cette option, par exemple, après avoir apporté une modification à votre réseau.

Ces actions s'appliquent par module. Vous pouvez contrôler les modules de métriques du système d'exploitation individuellement.

Tentatives de collecte de données du système

Lorsqu'un nouveau serveur est découvert, l'outil de découverte tente chaque identifiant configuré pour chaque adresse IP et nom d'hôte. Une fois que l'outil de découverte a trouvé un identifiant valide, il continue de l'utiliser à moins que vous n'en ajoutiez un nouveau.

Après un échec de collecte, l'outil de découverte tente de collecter les données réseau d'un serveur après 3 minutes, 30 minutes, 2 heures, puis 6 heures. Après 4 tentatives infructueuses, l'outil de découverte continue de tester toutes les informations d'identification configurées une fois toutes les 6 heures.

Inventaire découvert

Une fois que vous avez configuré une source de découverte, la valeur Nombre de serveurs découverts dans le cadre d'état de l'outil de découverte commence à augmenter. L'état de découverte de la source configurée passe à Activé dans le cadre du module Collection. La page d'inventaire affiche les serveurs provenant de toutes les sources configurées : machines virtuelles VMware, Hyper-V machines virtuelles et serveurs importés. Chaque serveur affiche l'état de sa source et de sa collection par module.

Accédez à la page Inventaire découvert pour voir les serveurs détectés par l'outil de découverte. Sur cette page, choisissez Télécharger l'inventaire pour télécharger un fichier ZIP

(`discovery_tool_export.zip`) contenant jusqu'à 30 jours de données collectées, y compris les fichiers MPA pour toutes les sources configurées, les données d'utilisation des performances, les informations de base de données et les informations de communication entre serveurs.

Vous pouvez télécharger le fichier ZIP pendant que l'outil de découverte continue de fonctionner et obtenir des résultats partiels. Téléchargez ce fichier dans l'évaluation de la migration pour obtenir une analyse de rentabilisation en faveur de la migration.

Options d'exportation

Lorsque vous exportez des données, vous pouvez personnaliser l'exportation à l'aide des options suivantes :

Plage de dates

Sélectionnez une date de début et une date de fin pour exporter uniquement les données collectées au cours de cette période. Les deux dates sont inclusives. La plage de dates maximale est de 30 jours.

> **Note**
>
> L'outil de découverte stocke jusqu'à 30 jours de données collectées. Si vous avez besoin de données couvrant plus de 30 jours, effectuez des exportations incrémentielles tous les 30 jours pour capturer toutes les données.

Sélection du module

Choisissez les modules de données à inclure dans l'exportation. Vous pouvez exporter tous les modules ou sélectionner des modules spécifiques :

Module	Description
Données VMware	Inventaire des machines virtuelles à partir des serveurs vCenter
Hyper-V données	Inventaire des machines virtuelles à partir des Hyper-V hôtes
Données du réseau	Connexions réseau entre les serveurs

Module	Description
Inventaire des serveurs	Informations sur le matériel du serveur et le système d'exploitation
Mesures de performance du serveur	Utilisation du processeur, de la mémoire et du réseau
Performances de stockage du serveur	IOPS et débit du disque
Configuration du stockage	Configuration du disque et du volume
Interfaces réseau	Détails de l'adaptateur réseau
Métriques de traitement	Processus en cours d'exécution
Données SQL Server	Inventaire des bases de données SQL Server
Données de base de données Oracle	Inventaire des bases de données Oracle : CDB, PDB, fonctionnalités, options et composants

Si vous ne sélectionnez aucun module, l'outil de découverte exporte toutes les données disponibles.

Points de données collectés

L'outil de découverte rassemble des données complètes sur VMware, les métriques du système d'exploitation Hyper-V, les bases de données et les composants réseau. Les sections suivantes détaillent les points de données spécifiques collectés pour chaque composant.

Collecte de données VMware

Ce tableau décrit les informations de machine virtuelle VMware collectées par l'outil de découverte :

Nom	Type	Catégorie	Valeur de l'échantillon
nom_machine	String	Informations sur la	« w2k22-snmpd-v2-fr-us-mssql-2_testcase4-1"

Nom	Type	Catégorie	Valeur de l'échantillon
		machine virtuelle	
vm_id	String	Informations sur la machine virtuelle	« VM-30920 »
vm_uuid	String	Informations sur la machine virtuelle	« 4201ecf8-cc44-ee7e-01da-34dfb2acf6c0"
powerstate	String	Informations sur la machine virtuelle	« Activé »
hôte	String	Informations sur la machine virtuelle	« esxi-70-node1.testlab.local »
adresse_IP principale	String	Informations sur la machine virtuelle	« 192,168,0.52"
unités centrales	Entier	Informations sur la machine virtuelle	2
memory	Entier	Informations sur la machine virtuelle	4096

Nom	Type	Catégorie	Valeur de l'échantillon
capacité_disque_mib totale	Entier	Informations sur la machine virtuelle	32768
os_accord_à_le_fichier_configuration	String	Informations sur la machine virtuelle	« Microsoft Windows Server 2016 ou version ultérieure (64 bits) »
max_cpu_usage_pct_dec	Float	Performance des machines virtuelles	79,33
avg_cpu_usage_pct_dec	Float	Performance des machines virtuelles	45,06
max_ram_usage_pct_dec	Float	Performance des machines virtuelles	63,99
avg_ram_utl_pct_dec	Float	Performance des machines virtuelles	29,27

Hyper-V collecte de données

Ce tableau décrit les informations de machine Hyper-V virtuelle collectées par l'outil de découverte :

Nom	Type	Catégorie	Valeur de l'échantillon
nom_machine	String	Informations sur la machine virtuelle	« win2_hyperv-test-01"

Nom	Type	Catégorie	Valeur de l'échantillon
vm_id	String	Informations sur la machine virtuelle	« a1b2c3d4-e5f6-7890-abcd-ef1234567890 »
powerstate	String	Informations sur la machine virtuelle	« Courir »
unités centrales	Entier	Informations sur la machine virtuelle	4
mémoire_mb	Entier	Informations sur la machine virtuelle	8192
chemins de disque_disque	String	Disk	« C : \ \ VM \ \ disk1.vhdx »
taille_disque_gb	Float	Disk	127,0
adaptateurs_réseau	String	Réseau	« 00:15:5 D:01:02:03 »
Adresse_IP	String	Réseau	« 10.0.1.50"
host_name	String	Host (Hôte)	« hyperv-host-01.exemple.com »
version du système d'exploitation hôte	String	Host (Hôte)	« Centre de données Windows Server 2022"
nom_cluster	String	Host (Hôte)	« FailoverCluster 01 »

Nom	Type	Catégorie	Valeur de l'échantillon
hyperviseur	String	Informations sur la machine virtuelle	"Hyper-V"

Données de serveur importées

Les serveurs importés ne sont pas découverts automatiquement. Ils sont importés par le biais d'un fichier CSV. L'outil de découverte ne collecte pas de données au niveau de l'hyperviseur pour les serveurs importés. Il collecte plutôt les données de métriques de base de données, de réseau et de système d'exploitation en utilisant les informations d'identification du système d'exploitation associées à chaque serveur lors de l'importation.

OS-related Données de l'outil de découverte

L'outil de découverte collecte l'inventaire du serveur, les performances, le stockage, l'interface réseau et les données de processus via SSH (Linux) et WinRM (Windows). Les tableaux suivants décrivent les points de données collectés.

Inventaire du serveur (server_inventory.csv)

Combine le provisionnement des serveurs (configuration matérielle et système d'exploitation) avec les performances de stockage agrégées. Récolté toutes les 24 heures.

Nom	Type	Catégorie	Valeur de l'échantillon
identifiant_serveur	String	Server Info	« serveur web vm-01 »
nom_serveur	String	Server Info	« serveur web-01 »
resource_type	String	Server Info	« machine_virtuelle »
power_state	String	Server Info	« Courir »
type de système d'exploitation	String	Server Info	« Linux »
nom_système	String	Server Info	« Amazon Linux »

Nom	Type	Catégorie	Valeur de l'échantillon
os_version	String	Server Info	« 2023 »
nom_hôte principal	String	Server Info	« web-server-01.exem ple.com »
adresse_IP principale	String	Server Info	« 10.0.2.101"
masque de réseau	String	Server Info	« 255,255,255,0"
nombre total de cartes-réseau	Entier	Server Info	2
nombre total de disques	Entier	Server Info	1
nombre de processeurs	Entier	Server Info	4
memory_total_gb	Float	Server Info	15,88
serveur_uuid	String	Server Info	« 4201ecf8-cc44-ee7e -01da-34dfb2acf6c0"
smbios_uuid	String	Server Info	« 4201ecf8-cc44-ee7e -01da-34dfb2acf6c0"
nom_cluster	String	Server Info	« cluster-01 de production »
hypervisor_objet_id	String	Server Info	« VM-30920 »
type_hyperviseur	String	Server Info	« VMware »
version de l'hyperviseur	String	Server Info	« 8,0.0"
nom d'hôte de l'hyperviseur	String	Server Info	« esxi-node1.exemple.com »
hypervisor_host_id	String	Server Info	« hôte-1234"
identifiant_hyperviseur	String	Server Info	« 4201ecf8-cc44-ee7e -01da-34dfb2acf6c0"

Nom	Type	Catégorie	Valeur de l'échantillon
disk_read_iops_avg	Float	Performances de stockage	12,5
disk_read_iops_peak	Float	Performances de stockage	245,0
disk_write_iops_avg	Float	Performances de stockage	8,3
disk_write_iops_peak	Float	Performances de stockage	180,0
disk_total_iops_avg	Float	Performances de stockage	20,8
disk_total_iops_peak	Float	Performances de stockage	425,0
disk_read_throughput_avg_mbps	Float	Performances de stockage	1.2
disk_read_throughput_peak_mbps	Float	Performances de stockage	24,5
disk_write_throughput_avg_mbps	Float	Performances de stockage	0.8

Nom	Type	Catégorie	Valeur de l'échantillon
disk_write_throughput_peak_mbps	Float	Performances de stockage	18,0
disk_total_throughput_avg_mbps	Float	Performances de stockage	2.0
disk_total_throughput_peak_mbps	Float	Performances de stockage	42,5

Mesures de performance du serveur (server_performance_metrics.csv)

Utilisation du processeur, de la mémoire et du débit réseau. Échantillonné toutes les 10 minutes, agrégé sur 30 jours.

Nom	Type	Catégorie	Valeur de l'échantillon
identifiant_serveur	String	Server Info	« serveur web vm-01 »
data_source	String	Server Info	« NOUS »
utilisation du processeur avg_pct	Float	CPU	45,06
cpu_utilization_peak_pct	Float	CPU	79,33
nombre de processeurs	Entier	CPU	4
mémoire_total_gb	Float	Mémoire	15,88
utilisation_de la mémoire_avg_pct	Float	Mémoire	29,27
memory_utilization_peak_pct	Float	Mémoire	63,99

Nom	Type	Catégorie	Valeur de l'échantillon
network_in_avg_mbps	Float	Réseau	0,52
réseau_in_peak_mbps	Float	Réseau	12.3
sortie réseau avg_mbps	Float	Réseau	0,31
Network_Out_Peak_Mbps	Float	Réseau	8,7
réseau total_avg_mbps	Float	Réseau	0,83
réseau total_peak_mbps	Float	Réseau	21,0

Performances de stockage (server_storage_performance.csv)

Per-volume utilisation du disque I/O et de l'espace. Échantillonné toutes les 10 minutes, agrégé sur 30 jours.

Nom	Type	Catégorie	Valeur de l'échantillon
identifiant_serveur	String	Server Info	« serveur web vm-01 »
data_source	String	Server Info	« NOUS »
identifiant_volume_disque	String	Informations sur le volume	"/dev/nvme0n1p1"
point de montage sur disque	String	Informations sur le volume	"/"
système_fichiers	String	Informations sur le volume	« xfs »
disk_total_gb	Float	Espace disque	30.0
disk_used_gb	Float	Espace disque	12,5

Nom	Type	Catégorie	Valeur de l'échantillon
disk_free_gb	Float	Espace disque	17,5
disk_read_iops_avg	Float	Disque I/O	12,5
disk_read_iops_peak	Float	Disque I/O	245,0
disk_write_iops_avg	Float	Disque I/O	8,3
disk_write_iops_peak	Float	Disque I/O	180,0
disk_total_iops_avg	Float	Disque I/O	20,8
disk_total_iops_peak	Float	Disque I/O	425,0
disk_read_throughput_avg_mbps	Float	Débit du disque	1.2
disk_read_throughput_peak_mbps	Float	Débit du disque	24,5
disk_write_throughput_avg_mbps	Float	Débit du disque	0.8
disk_write_throughput_peak_mbps	Float	Débit du disque	18,0
disk_total_throughput_avg_mbps	Float	Débit du disque	2.0
disk_total_throughput_peak_mbps	Float	Débit du disque	42,5

Configuration du stockage (storage_config.csv)

Informations sur le matériel du disque physique Récolté toutes les 24 heures.

Nom	Type	Catégorie	Valeur de l'échantillon
identifiant_serveur	String	Server Info	« serveur web vm-01 »
identifiant_contrôleur de disque	String	Informations sur le disque	"/dev/sda"
nom_fichier_vmdk_vhd	String	Informations sur le disque	« serveur web 01.vmdk »
type de volume de disque	String	Informations sur le disque	« Virtuel »
disk_provisioned_fr	Float	Informations sur le disque	30.0
type de disque_périphérique	String	Informations sur le disque	« DISQUE DUR SCSI »
type_interface de disque	String	Informations sur le disque	« SCSI »
protocole_disque	String	Informations sur le disque	« LSI Logic SAS »

Interfaces réseau (network_interfaces.csv)

Configuration de l'adaptateur réseau. Récolté toutes les 24 heures.

Nom	Type	Catégorie	Valeur de l'échantillon
identifiant_serveur	String	Server Info	« serveur web vm-01 »
nom_interface	String	Informations sur l'interface	« eth0"
index_interface	Entier	Informations sur l'interface	2

Nom	Type	Catégorie	Valeur de l'échantillon
adresse_mac	String	Informations sur l'interface	« 0 A:1B:2C:3D:4E:5F »
type_adaptateur	String	Informations sur l'interface	« vmxnet3 »
nom_réseau_virtuel	String	Informations sur l'interface	« Réseau de machines virtuelles »
identifiant_réseau virtuel	String	Informations sur l'interface	« dvportgroup-1234 »
commutateur virtuel	String	Informations sur l'interface	« commutateur V 0 »
adresse_IPV4	String	Config IP	« 10.0.2.101"
masque de sous-réseau ipv4	String	Config IP	« 255,255,255,0"
passerelle IPV4	String	Config IP	« 10.0.2.1"
adresse_IPV6	String	Config IP	« fe80 : :a1b:2cff : fe3d : 4e5f »
longueur_du préfixe ipv6	Entier	Config IP	64
passerelle IPV6	String	Config IP	« fe80 : 1 »
serveurs DNS	String	Config IP	« 10,0.0.2"
DHCP_activé	Booléen	Config IP	false
état_de l'interface	String	Informations sur l'interface	« En haut »
identifiant_vlan	Entier	Informations sur l'interface	100

Nom	Type	Catégorie	Valeur de l'échantillon
is_primaire	Booléen	Informations sur l'interface	true

Processus en cours (process_metrics.csv)

Instantané des processus en cours d'exécution. Collectés toutes les heures, dédupliqués pendant 30 jours.

Nom	Type	Catégorie	Valeur de l'échantillon
identifiant_serveur	String	Server Info	« serveur web vm-01 »
nom_processus	String	Informations sur le processus	« shd »
process_id	Entier	Informations sur le processus	1234
ligne de commande du processus	String	Informations sur le processus	«/usr/sbin/sshd-D »
utilisateur_processus	String	Informations sur le processus	« racine »

Collection en réseau

Le module de collecte réseau vous aide à découvrir les dépendances entre les serveurs de votre centre de données sur site. Ces données réseau accélèrent la planification de votre migration en fournissant une visibilité sur la manière dont les applications communiquent entre les serveurs.

Ce module collecte les données réseau pour les serveurs à partir de toutes les sources configurées, y compris VMware Hyper-V, et des serveurs importés. Il utilise WinRM pour collecter des données à

partir de serveurs Windows et utilise SSH, SNMPv2 et SNMPv3 pour collecter des données à partir de serveurs Linux.

Collecte de données réseau

Le module de collecte réseau capture les connexions TCP IPv4 à l'état ESTABLISHED ou TIME_WAIT entre les serveurs de votre inventaire découvert. Une connexion apparaît dans la sortie uniquement lorsque les adresses IP source et cible appartiennent à des serveurs découverts par l'outil de découverte ou que vous avez importés. Les connexions vers ou depuis des adresses IP extérieures à votre inventaire, telles que les services externes, les points de terminaison cloud ou les serveurs qui n'ont pas encore été ajoutés à l'outil de découverte, ne sont pas incluses.

Cette conception concentre les données réseau sur les dépendances de serveur à serveur au sein de votre environnement, qui sont les informations nécessaires au mappage des dépendances des applications et à la planification des vagues de migration.

Ces points de données sont collectés pour chaque connexion :

Nom	Type	Catégorie	Valeur de l'échantillon
IP Source	String	Connexion	« 192,168.1,10 »
Port source	Entier	Connexion	49152
ID du processus source	Entier	Processus	1234
Nom du processus source	String	Processus	"java"
IP cible	String	Connexion	« 192,168.1,20"
Port cible	Entier	Connexion	5432
ID du processus cible	Entier	Processus	5678
Nom du processus cible	String	Processus	« postgres »
State	String	Connexion	« ÉTABLI »
Protocole de transport	String	Connexion	« TCP »

Nom	Type	Catégorie	Valeur de l'échantillon
Versions d'adresses IP	String	Connexion	« IPv4 »
Nombre	Entier	Connexion	42

> **Tip**
>
> Pour optimiser l'exhaustivité de votre carte des dépendances réseau, configurez toutes les sources de découverte (VMware et importation CSV du serveur) et ajoutez les informations d'identification du système d'exploitation avant de consulter les données réseau. Hyper-V Plus votre inventaire comporte de serveurs, plus le module réseau peut capturer de connexions.

Collecte de réseaux d'adresses privés

Par défaut, le module de collecte réseau capture uniquement les connexions dont les deux points de terminaison sont des serveurs figurant dans votre inventaire découvert. Vous pouvez activer la collecte d'adresses privées pour capturer également les connexions vers et depuis les adresses IP privées RFC 1918 (10.0.0). 0/8, 172,16,0. 0/12, 192.168.0. 0/16) qui ne figurent pas dans votre inventaire.

Pour démarrer la collecte d'adresses privées

1. Sur la page de configuration du collecteur, recherchez la section Modules de collection.
2. Recherchez Découverte des connexions réseau sous Découverte des applications.
3. Ouvrez le menu déroulant Actions.
4. Choisissez Commencer la collecte d'adresses privées.
5. Si le statut du module était Activé, vous pouvez le voir passer à Activé · Adresse privée activée.

Pour arrêter la collecte d'adresses privées, ouvrez le menu déroulant Actions et choisissez Arrêter la collecte d'adresses privées. Les données d'adresse privée précédemment collectées sont conservées même après l'arrêt.

Les connexions par adresse privée apparaissent uniquement dans l'export CSV complet (dans le fichier ZIP), pas dans les fichiers CSV MPA. Si une adresse IP appartient à un serveur déjà présent

dans votre inventaire, elle est toujours identifiée par son ID de serveur découvert, quel que soit ce paramètre.

Ce paramètre est conservé au cours des redémarrages. Vous pouvez démarrer ou arrêter la collecte d'adresses privées à tout moment. Les données d'adresse privée précédemment collectées sont exportées quel que soit le paramètre actuel.

Collection SQL Server

Le module de collecte SQL Server collecte les informations SQL Server à partir de serveurs Windows provenant de toutes les sources configurées, y compris VMware Hyper-V, et des serveurs importés. Le module utilise WinRM pour se connecter à distance à chaque serveur Windows et exécuter PowerShell des requêtes. Il collecte des informations sur tous les services SQL Server installés (composants) à l'aide des espaces de noms, du registre et des propriétés de fichier WMI.

Un composant SQL Server est une instance de service ou de fonctionnalité spécifique installée dans le cadre d'un déploiement de SQL Server sur un serveur Windows. L'outil de découverte collecte le moteur de base de données, les services d'analyse, les services de reporting et les services d'intégration.

Collecte de données SQL Server

Le module de collecte de SQL Server collecte des informations sur les composants de SQL Server. Ce tableau décrit les principaux points de données collectés :

Nom	Type	Catégorie	Valeur de l'échantillon
Type de moteur	String	Composant	serveur_SQL
Est un composant du moteur	Booléen	Composant	Y
Statut	String	Service	En cours d'exécution, arrêté, StartPending
Version	String	Service	2015,131,5026,0
Edition	String	Service	Édition Developer (64 bits)
Nom du service SQL	String	Service	MsDtsServer130, MSQL

Nom	Type	Catégorie	Valeur de l'échantillon
Type de service SQL	String	Service	Service SQL Server, service Integration Services
Nom de l'instance	String	Instance	SERVEUR MSSQL
Nom d'affichage	String	Service	SQL Server (MSSQLSERVER2017)
Mode de démarrage	String	Service	Automatique, manuel, désactivé
Nom du compte de service	String	Service	NT Service/MsDtsServer130
Est clusterisé	Booléen	Configuration	N

> **Note**
>
> Le format complet inclut tous les types de services. Le format MPA inclut uniquement les composants du moteur de base de données. Les champs ne sont pas tous disponibles en fonction du type de service SQL et de sa configuration.

Collection de bases de données Oracle

Avec la collection Oracle Database, vous pouvez découvrir les instances de base de données Oracle dans toutes les sources configurées, y compris VMware Hyper-V, et sur les serveurs importés. Le module collecte les données suivantes :

- Énumération des bases de données de conteneurs (CDB) et des bases de données enfichables (PDB)
- Version et édition
- Options installées
- Statistiques d'utilisation des fonctionnalités
- Inventaire des composants (DBA_REGISTRY)
- Dimensionnement des fichiers de données

- Indicateurs de topologie (RAC, Data Guard et architecture mutualisée)

Database-connected (SQL)

Lorsque vous configurez les informations d'identification Oracle, l'outil de découverte se connecte directement à la base de données Oracle à l'aide du compte de service en lecture seule. Cela fournit une SQL-level collection complète, y compris les détails du PDB, l'utilisation des fonctionnalités et les options installées. Tous les fichiers CSV contiennent des données complètes.

OS-level solution de repli

Si vous n'avez pas configuré les informations d'identification de base de données ou si la connexion échoue, l'outil de découverte utilise SSH ou WinRM pour détecter les installations Oracle. Il découvre les maisons, les écouteurs, les correctifs, les versions et les éditions d'Oracle sans accès à la base de données. Pour les OS-detected hôtes, le fichier CSV CDB exporté contient le nom de l'instance, le nom d'hôte, la version et l'édition. Les fichiers CSV du PDB, des fonctionnalités, des options et des composants ne contiennent aucune ligne.

La collection Oracle produit les fichiers CSV suivants dans le fichier ZIP d'exportation. Chaque tableau décrit les points de données collectés par fichier.

Données CDB (oracle_data_cdbs_full.csv)

Une ligne par instance CDB. Ce tableau décrit les points de données CDB collectés :

Nom	Type	Catégorie	Valeur de l'échantillon	Source
Nom de l'instance	String	Identity	« ORQUE »	SQL, SYSTÈME D'EXPLOITATION
Nom d'hôte	String	Identity	« oracledb01.example.com »	SQL, SYSTÈME D'EXPLOITATION
DB Name	String	Identity	« ORQUE »	SQL uniquement

Nom	Type	Catégorie	Valeur de l'échantillon	Source
Nom unique de la base de données	String	Identity	« ORCL_PRIMAIRE »	SQL uniquement
DBID	Entier	Identity	1234567890	SQL uniquement
Version	String	Version	« 19,0.0.0"	SQL, SYSTÈME D'EXPLOITATION
Version complète	String	Version	« 19,21.0.0"	SQL uniquement
Edition	String	Version	« Édition Enterprise »	SQL, SYSTÈME D'EXPLOITATION
Type de base de données	String	Configuration	« CÉLIBATAIRE »	SQL uniquement
Rôle de base de données	String	Configuration	« PRINCIPAL »	SQL uniquement
Mode ouvert	String	Configuration	« LIRE ÉCRIRE »	SQL uniquement
Mode journal	String	Configuration	« JOURNAL D'ARCHIVES »	SQL uniquement
Plateforme	String	Configuration	« Linux x86 64 bits »	SQL uniquement
Drapeau CDB	String	Configuration	« OUI »	SQL uniquement

Nom	Type	Catégorie	Valeur de l'échantillon	Source
Est-ce que RAC	String	Topology (Topologie)	« OUI » ou « NON »	SQL uniquement
Est-ce que Data Guard est en veille ?	String	Topology (Topologie)	« OUI » ou « NON »	SQL uniquement
Mode de protection	String	Topology (Topologie)	« PERFORMANCE MAXIMALE »	SQL uniquement
Data Guard Broker	String	Topology (Topologie)	« ACTIVÉ »	SQL uniquement
Jeu de caractères NLS	String	Configuration	« AL32UTF8 »	SQL uniquement
Nombre de PDB	Entier	Dimension nement	3	SQL uniquement
Flashback activé	String	Configuration	« OUI »	SQL uniquement
Voie de détection	String	Métadonnées	« phase2 » ou « phase1b »	SQL, SYSTÈME D'EXPLOITATION

Données PDB (oracle_data_pdbs_full.csv)

Une ligne par PDB (base de données enfichable). Ce tableau décrit les points de données PDB collectés :

> **Note**
>
> Les données PDB nécessitent des informations d'identification de base de données Oracle (connexion SQL). OS-level fallback ne renseigne pas ce fichier CSV.

Nom	Type	Catégorie	Valeur de l'échantillon	Source
Nom de l'instance CDB	String	Identity	« ORQUE »	SQL uniquement
Nom du PDB	String	Identity	« APPPDB1"	SQL uniquement
Mode ouvert	String	Statut	« LIRE ÉCRIRE »	SQL uniquement
État du cycle de vie	String	Statut	« NORMAL »	SQL uniquement
Nombre de tablespaces	Entier	Dimension nement	5	SQL uniquement
Nombre de fichiers de données	Entier	Dimension nement	12	SQL uniquement
Taille totale en octets	Entier	Dimension nement	5368709120	SQL uniquement
Nombre de schémas utilisateur	Entier	Dimension nement	8	SQL uniquement
Nombre de liens de base de données	Entier	Connectivité	2	SQL uniquement
Composants installés	String	Configuration	« APEX ; JVM ; XML »	SQL uniquement
Nombre de tablespaces chiffrés	Entier	Sécurité	1	SQL uniquement

Données d'utilisation des fonctionnalités (oracle_data_features_full.csv)

Une ligne par entrée d'utilisation des fonctionnalités provenant de DBA_FEATURE_USAGE_STATISTICS. Ce tableau décrit les points de données d'utilisation des fonctionnalités collectés :

> **Note**
>
> Les données d'utilisation des fonctionnalités nécessitent des informations d'identification de base de données Oracle (connexion SQL). OS-level fallback ne renseigne pas ce fichier CSV.

Nom	Type	Catégorie	Valeur de l'échantillon	Source
Nom de l'instance CDB	String	Identity	« ORQUE »	SQL uniquement
Name	String	Fonctionnalité	« Partitionnement (utilisateur) »	SQL uniquement
Utilisations détectées	Entier	Usage	42	SQL uniquement
Actuellement utilisé	String	Usage	« VRAI »	SQL uniquement
Date de première utilisation	DateTime	Usage	« 15/01/2024 T00:00:00 »	SQL uniquement
Date de dernière utilisation	DateTime	Usage	« 01/06/2020 » T00:00:00	SQL uniquement

Données d'options (oracle_data_options_full.csv)

Une ligne par entrée V$OPTION par CDB. Ce tableau décrit les points de données des options installées collectés :

> **Note**
>
> Les données d'options nécessitent des informations d'identification de base de données Oracle (connexion SQL). OS-level fallback ne renseigne pas ce fichier CSV.

Nom	Type	Catégorie	Valeur de l'échantillon	Source
Nom de l'instance CDB	String	Identity	« ORQUE »	SQL uniquement
Nom d'option	String	Option	« Analyses avancées »	SQL uniquement
Est installé	String	Option	« VRAI »	SQL uniquement
ID du conteneur	Entier	Option	0	SQL uniquement

Données des composants (oracle_data_components_full.csv)

Une ligne par composant DBA_REGISTRY. Ce tableau décrit les points de données des composants collectés :

> **Note**
>
> Les données des composants nécessitent des informations d'identification de base de données Oracle (connexion SQL). OS-level fallback ne renseigne pas ce fichier CSV.

Nom	Type	Catégorie	Valeur de l'échantillon	Source
Nom de l'instance CDB	String	Identity	« ORQUE »	SQL uniquement

Nom	Type	Catégorie	Valeur de l'échantillon	Source
Nom PDB	String	Identity	« APPPDB1"	SQL uniquement
ID du composant	String	Composant	« SOMMET »	SQL uniquement
Nom du composant	String	Composant	« Oracle Application Express »	SQL uniquement
Version	String	Composant	« 22.1.0.15.0"	SQL uniquement
Statut	String	Composant	« VALIDE »	SQL uniquement
Schema	String	Composant	« APEX_220100"	SQL uniquement

Considérations sur la sécurité

Sécurisation de la VM de l'outil de découverte

La sécurité des machines virtuelles de l'outil de découverte est cruciale car l'outil de découverte stocke toutes les informations d'identification, les journaux et les données des clients sur la machine virtuelle de l'outil de découverte.

L'accès SSH à la machine virtuelle de l'outil de découverte est désactivé par défaut et n'est accessible que depuis le clientvCenter `UI -> "Launch Web Console"`.

L'outil de découverte VM est fourni avec un mot de passe de connexion par défaut « mot de passe » pour la « découverte » de l'utilisateur.

- Nous vous recommandons de mettre à jour ce mot de passe immédiatement après le déploiement.
- Nous vous demandons de mettre à jour le mot de passe si vous souhaitez activer SSH à l'aide de la commande `enablessh` après vous être connecté à l'aide de vCenter`Launch Web Console`. Veuillez noter que chaque fois que cette commande est appelée, vous devez la réinitialiser.

Sécurisation des identifiants

Bonnes pratiques générales pour la gestion des accréditations

- Stockez vos identifiants en toute sécurité
- Faites régulièrement pivoter toutes les informations d'identification
- Utilisez des gestionnaires de mots de passe ou des coffres-forts sécurisés
- Surveiller l'utilisation des informations d'identification
- Respectez le principe du moindre privilège et n'accordez que les autorisations minimales nécessaires

Informations d'identification SNMP v2

- Utiliser des chaînes communautaires complexes autres que celles par défaut
- Évitez les chaînes communes telles que « public » ou « privé »
- Traitez les chaînes communautaires comme des mots de passe

Informations d'identification SNMP v3

- Activez à la fois l'authentification et la confidentialité
- Utiliser des protocoles d'authentification forts (SHA préféré à MD5)
- Utilisez des protocoles de chiffrement puissants (AES préféré au DES)
- Utilisez des mots de passe complexes à la fois pour l'authentification et la confidentialité
- Utilisez des noms d'utilisateur uniques (évitez les noms communs)

Informations d'identification WinRM

- Évitez de désactiver la vérification des certificats WinRM.
- Nous vous recommandons de créer un compte de service dédié avec les autorisations minimales requises.
- Évitez d'utiliser des comptes d'administrateur de domaine ou d'administrateur local, sauf si vous avez besoin d'une collecte SQL Server. La collecte SQL Server nécessite un accès d'administrateur local car elle interroge plusieurs espaces de noms WMI et utilise des commandes élevées. Pour les métriques du système d'exploitation sans détection de SQL Server, un compte

non administrateur avec des utilisateurs de gestion à distance, des utilisateurs du moniteur de performances et un accès en lecture WMI `root\cimv2` est suffisant. Voir the section called "Autorisations requises" pour les détails par module.

Hyper-V credentials

- Utilisez des comptes de service dédiés avec Hyper-V des autorisations de gestion minimales.
- Évitez d'utiliser des comptes d'administrateur de domaine.
- Hyper-V les informations d'identification prennent en charge l'authentification NTLM (HTTPS uniquement) et Kerberos.
- L'outil de découverte stocke les informations d'identification chiffrées au repos à l'aide de SQLCipher.

Informations d'identification Oracle

- Utilisez un compte de service dédié en lecture seule avec uniquement SELECT_CATALOG_ROLE. N'utilisez pas les privilèges DBA, SYSDBA ou SYSOPER.
- L'outil de découverte effectue uniquement des opérations de lecture et n'écrit jamais dans la base de données Oracle.
- L'outil de découverte n'accède pas aux vues du pack de diagnostic ou du pack de réglage. Aucune licence Oracle supplémentaire n'est donc requise.
- Changez régulièrement le mot de passe du compte de service Oracle et mettez à jour les informations d'identification dans l'outil de découverte.

Stockage des informations d'identification

L'outil de découverte chiffre les informations d'identification stockées au repos à l'aide d'une clé de chiffrement de base de données. Sur les systèmes équipés de systemd 250 ou version ultérieure, cette clé est cryptée à l'aide de systemd-creds. Sur les anciens systèmes, la clé est stockée sous forme de fichier protégé par autorisation. Dans les deux cas, un attaquant disposant d'un accès root à l'hôte de l'outil de découverte pourrait accéder à la clé de chiffrement et déchiffrer les informations d'identification stockées. Limitez l'accès à l'hôte de l'outil de découverte et traitez-le comme un système privilégié dans votre environnement.

Utilisation de Auto-Connect la fonctionnalité avec prudence

L'outil de découverte utilise deux mécanismes pour attribuer des informations d'identification aux serveurs lors de la OS-level collecte : connexion automatique et manuel. OS-level La collection inclut les modules Network, SQL Server, Oracle Database et OS metrics. Ces modules se connectent à des serveurs individuels provenant de toutes les sources, y compris les machines virtuelles VMware, les Hyper-V machines virtuelles et les serveurs importés.

Manuel : un serveur peut être associé manuellement à un identifiant spécifique. Dans ce cas, l'outil de découverte utilise uniquement ces informations d'identification, quel que soit le succès ou l'échec. Vous devez contrôler manuellement l'état de la collecte pour ce serveur et apporter des modifications.

Auto-connect: si aucun identifiant n'est associé manuellement au serveur, l'outil de découverte utilise le mécanisme de connexion automatique pour ce serveur. Cela signifie :

- Au début de chaque cycle de collecte, l'outil de découverte obtient une liste des informations d'identification disponibles pour ce serveur (en fonction du type de système d'exploitation) et est également configurée pour être « auto-connectable ».
- L'outil de découverte teste ensuite en boucle toutes les informations d'identification par rapport au serveur.
  - Si un identifiant de travail est trouvé, le cycle de collecte pour le serveur est réussi. L'outil de découverte s'en souvient et l'essaiera pour la première fois la prochaine fois.
  - Si aucune information d'identification fonctionnelle n'est trouvée, le cycle de collecte pour le serveur a échoué.
    - Module réseau : le serveur utilise un calendrier d'interruption, commençant le cycle de collecte suivant 3 minutes, 30 minutes, 2 heures et 6 heures après chaque panne (similaire à un arrêt exponentiel).
    - Collection SQL Server : l'outil de découverte ne réessaie pas. Il effectue une tentative par serveur chaque jour.

Impacts/Risks:

N'utilisez la connexion automatique que lorsque vous êtes certain que les risques sont atténués dans votre système :

Risque 1 : la connexion automatique étant configurée sur plusieurs informations d'identification erronées, les essayer automatiquement sur des serveurs peut entraîner le verrouillage des comptes dans les environnements de production dans lesquels des politiques de verrouillage sont configurées. Par exemple, un centre de données peut configurer ses machines virtuelles pour qu'elles se verrouillent après 3 tentatives de connexion SSH infructueuses. Dans ce cas, si la connexion automatique est configurée pour 3 informations d'identification SSH erronées, des blocages de compte légitimes se produiront. Si des verrouillages se produisent sur plusieurs systèmes, les processus métier critiques peuvent être affectés, ce qui peut provoquer des défaillances en cascade dans les systèmes dépendants. En outre, les centres d'opérations de sécurité peuvent être confrontés à des tempêtes d'alertes suite à des échecs d'authentification massifs, créant des incidents de sécurité faussement positifs qui épuisent les ressources et peuvent masquer de véritables attaques.

Risque 2 : L'acteur ayant accès à l'outil de découverte (connaît le mot de passe de l'outil de découverte) peut forcer les informations d'identification du système d'exploitation sur tous les serveurs, en configurant un grand nombre d'informations d'identification de test et en utilisant la connexion automatique pour trouver celles qui ont été retenues.

Atténuations :

Suivez ces instructions :

- Assurez-vous que le mot de passe de l'outil de découverte est correctement sécurisé et connu uniquement des acteurs autorisés
- Assurez-vous que les informations d'identification appropriées sont saisies pour l'environnement si des politiques de verrouillage sont en place. Nous recommandons de ne configurer que des informations d'identification opérationnelles connues, même en l'absence de politiques de verrouillage des comptes, afin de garantir une charge opérationnelle minimale sur les machines virtuelles individuelles.
- « Auto-connect » est une fonctionnalité optionnelle. Ne le sélectionnez pas et utilisez l'attribution manuelle des informations d'identification si le verrouillage des comptes est une source de préoccupation pour l'environnement.

Sécurité des importations CSV

Lorsque vous importez des serveurs à l'aide d'un fichier CSV, tenez compte des implications de sécurité suivantes :

- Le fichier CSV peut contenir les noms d'hôte ou les adresses IP de serveurs internes. Traitez-les comme des données sensibles.
- Les `oracle_credential_name` colonnes `os_credential_name` et font référence aux informations d'identification préconfigurées par un nom convivial. Le fichier CSV ne contient aucun secret.
- All-or-nothing validation : si une ligne du CSV n'est pas valide, le téléchargement complet est rejeté. Cela permet d'éviter les importations partielles susceptibles de créer un état confus.
- Les serveurs importés sont immédiatement visibles dans l'inventaire et peuvent être collectés. Assurez-vous que les informations d'identification du système d'exploitation et d'Oracle sont correctement définies avant de procéder à l'importation.

Considérations relatives à la révocation d'accès

Lorsque vous révoquez l'accès, la suppression est limitée à la source spécifique :

- La révocation de l'accès à vCenter supprime uniquement les données de vCenter. Cela n'affecte pas les données du serveur Hyper-V ou ne les importe pas.
- La révocation de Hyper-V l'accès supprime uniquement Hyper-V les données. Cela n'affecte ni VMware ni les données de serveur importées.
- La suppression des serveurs importés les supprime de l'inventaire, mais les données de collecte en aval (réseau, base de données, indicateurs du système d'exploitation) sont conservées.
- Pour supprimer toutes les données d'inventaire spécifiques à une source, vous devez révoquer ou supprimer chaque source indépendamment. Les données de collecte en aval (réseau, base de données, métriques du système d'exploitation) sont conservées même après la révocation de toutes les sources.

Résolution des problèmes

Vérification de la connectivité de l'outil de découverte à vCenter

Lorsque vous rencontrez des erreurs de configuration du module VMware, procédez comme suit pour vérifier la connectivité :

Accédez à la machine virtuelle de l'outil de découverte

- Log-in vers la machine virtuelle de l'outil de découverte, ouvrez la console distante dans vCenter

- Nom d'utilisateur : discovery
- Mot de passe : mot de passe

Testez la connectivité vCenter

1. Testez l'accès à l'API vCenter :

```
curl -v --insecure -u <username>:<password> https://<vcenter-ip-or-hostname>:443/
mob
```

2. Résultat de réussite attendu :

```
[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
```

Tester le certificat SSL

1. Exécutez cette commande :

```
openssl s_client -showcerts -servername <hostname> -connect <hostname>:443
```

2. Résultat de réussite attendu :

- Devrait afficher les détails du certificat vSphere
- Vérifie la SSL/TLS connectivité sur le port 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
---
```

Résolution des problèmes liés à WinRM

Si vous rencontrez des problèmes de connectivité avec WinRM, procédez comme suit pour tester la connexion. Ces étapes s'appliquent également aux problèmes de Hyper-V connectivité, car l'outil de découverte utilise WinRM pour communiquer avec Hyper-V les hôtes.

Testez la connectivité WinRM de base à l'aide des ports 5985 (HTTP) et 5986 (HTTPS). Nous devons nous assurer que la connectivité fonctionne sur le port 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 les tests ci-dessus échouent, essayez d'établir une PowerShell session avec la validation des certificats désactivée :

```
$cred = Get-Credential
$so = New-PsSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
Enter-PSSession -ComputerName <HOST> -Credential $cred -Port 5985 -SessionOption $so
```

Résolution des problèmes liés à Kerberos

Si vous rencontrez des échecs d'authentification Kerberos lors de la collecte de données à partir de serveurs Windows, consultez les sections suivantes pour diagnostiquer et résoudre les problèmes courants.

Vérifiez les exigences du réseau

Avant de résoudre les problèmes d'authentification Kerberos, vérifiez que l'outil de découverte peut atteindre les points de terminaison réseau requis.

Pour vérifier la configuration réseau requise pour Kerberos

1. Vérifiez la résolution DNS auprès du contrôleur de domaine. Exécutez la commande suivante depuis la machine virtuelle de l'outil de découverte :

   ```
   nslookup dc01.example.com
   ```

   Vous pouvez également utiliser `dig` :

   ```
   dig dc01.example.com
   ```

   Si la résolution DNS échoue, vérifiez que la machine virtuelle de l'outil de découverte est configurée pour utiliser un serveur DNS capable de résoudre votre domaine Active Directory. Vérifiez `/etc/resolv.conf` et confirmez que les entrées du serveur de noms pointent vers les serveurs DNS de votre domaine.
2. Vérifiez la connectivité au centre de distribution de clés (KDC) sur le port 88. Exécutez la commande suivante :

   ```
   nc -zv dc01.example.com 88
   ```

   Sortie attendue :

```
Connection to dc01.example.com 88 port [tcp/kerberos] succeeded!
```

Si la connexion échoue, vérifiez qu'aucune règle de pare-feu ne bloque le trafic entre la machine virtuelle de l'outil de découverte et le contrôleur de domaine sur le port 88.

3. Vérifiez la connectivité aux serveurs Windows cibles sur les ports WinRM. Exécutez les commandes suivantes :

```
nc -zv <windows-server> 5985
nc -zv <windows-server> 5986
```

Si la connexion échoue, vérifiez que WinRM est activé sur le serveur cible et que les règles de pare-feu autorisent le trafic entrant sur les ports 5985 et 5986.

Problèmes courants liés à Kerberos

Vous trouverez ci-dessous des problèmes courants liés à Kerberos et leurs solutions.

Erreurs de distinction majuscules/

Symptôme : Vous recevez le message d'erreur « Serveur introuvable dans la base de données Kerberos » lors de l'authentification.

Cette erreur se produit généralement lorsque le nom de domaine Kerberos n'est pas en majuscules. Les domaines Kerberos doivent être spécifiés en majuscules dans votre fichier. `krb5.conf` Par exemple, utilisez `EXAMPLE.COM` plutôt que `example.com`.

Prévention du verrouillage des comptes

L'outil de découverte utilise un mécanisme de temporisation pour empêcher le verrouillage des comptes suite à des tentatives d'authentification infructueuses répétées. Si votre compte de service est verrouillé, vous pouvez réinitialiser le processus de collecte en arrêtant puis en démarrant le module de collecte via l'interface utilisateur Web de l'outil de découverte à l'adresse`https://<discovery-tool-vm-ip>:5000`.

kinit échoue à partir de la CLI

Le tableau suivant répertorie les `kinit` erreurs courantes et leurs solutions.

Erreur	Cause	Solution
Impossible de trouver le KDC pour le domaine	Le nom d'hôte ou l'adresse IP du KDC ne sont pas accessibles, ou le domaine n'est pas configuré dans. `krb5.conf`	Vérifiez que le `krb5.conf` fichier contient le nom d'hôte et le domaine KDC corrects. Vérifiez la résolution DNS et la connectivité réseau au KDC sur le port 88.
Échec de la préauthentification	Le mot de passe du compte de service est incorrect.	Vérifiez le mot de passe et réessayez. Si le compte est verrouillé, déverrouillez-le dans Active Directory avant de réessayer.
Client introuvable dans la base de données Kerberos	Le nom principal ne correspond à aucun compte dans Active Directory.	Vérifiez que le nom principal correspond exactement au nom du compte, majuscule comprise. Utilisez le format `username@REALM` avec le domaine en majuscules.
Impossible de résoudre l'adresse réseau du KDC	Le DNS ne peut pas résoudre le nom d'hôte du KDC.	Vérifiez la configuration DNS dans `/etc/resolv.conf`. Vérifiez que le serveur DNS peut résoudre le nom d'hôte du KDC. Testez avec `nslookup` ou `dig`.

La collecte échoue malgré un kinit réussi

En cas de `kinit` succès mais que la collecte de données échoue toujours, vérifiez les points suivants :

1. Vérifiez que le nom principal utilisé pour la collecte correspond `kinit` exactement au dossier utilisé pendant la collecte.
2. Vérifiez que le compte de service dispose des autorisations requises sur les serveurs cibles.
3. Vérifiez que WinRM est activé sur les serveurs cibles.
4. Vérifiez que le nom d'hôte utilisé pour la collecte correspond au nom d'hôte enregistré dans Active Directory.

Kerberos fonctionne pour certains serveurs mais pas pour d'autres

Si l'authentification Kerberos réussit pour certains serveurs mais échoue pour d'autres, examinez les points suivants :

Si vos serveurs couvrent plusieurs domaines Active Directory, configurez des informations d'identification Kerberos distinctes pour chaque domaine. Assurez-vous que votre `/etc/krb5.conf` fichier inclut des entrées pour tous les domaines. Chaque domaine nécessite ses propres informations d'identification avec le `username@REALM` principal approprié.

Comparez la configuration WinRM sur un serveur en fonctionnement avec celle d'un serveur défaillant. Exécutez la commande suivante sur chaque serveur :

```
winrm get winrm/config
```

Testez la connectivité avec Remote Desktop pour isoler le problème. L'outil de découverte utilise le format`username@DOMAIN`, tandis que Remote Desktop utilise le format`DOMAIN\username`.

Vérifiez que le compte de service est membre du groupe d'administrateurs local sur le serveur défaillant. Exécutez la commande suivante sur le serveur cible :

```
net localgroup Administrators
```

WMI a besoin de privilèges d'administrateur local pour accéder aux informations du système d'exploitation. La collecte SQL Server nécessite également que le compte de service dispose d'un accès administrateur local sur le serveur cible.

Liste de contrôle de configuration de Kerberos

Utilisez la liste de contrôle suivante pour vérifier votre configuration Kerberos avant de commencer la collecte de données.

- Le `krb5.conf` fichier existe sur la machine virtuelle de l'outil de découverte.
- Le nom du domaine est en majuscules dans. `krb5.conf`
- L'exécution `kinit` avec le compte de service réussit sans erreur.
- Running `klist` montre un billet valide et non expiré.
- Le nom principal correspond exactement au nom du compte Active Directory.
- La résolution DNS fonctionne pour le nom d'hôte du KDC.
- La connectivité réseau au KDC sur le port 88 est confirmée.

- La connectivité réseau vers les serveurs Windows cibles sur les ports 5985 et 5986 est confirmée.
- (Multi-domain) Chaque domaine Active Directory possède ses propres informations d'identification configurées dans l'outil de découverte `[realms]` et `krb5.conf` contient des `[domain_realm]` entrées pour tous les domaines.

Résolution des problèmes liés aux bases de

Pour diagnostiquer les problèmes de collecte de la base de données Oracle, tels que des données manquantes ou des erreurs, vérifiez les points suivants.

Connexion refusée ou expiration du délai

Symptôme : L'état de la collection Oracle indique une erreur de connexion pour un serveur.

Pour résoudre ce problème, vérifiez les points suivants :

- Vérifiez que le récepteur Oracle est en cours d'exécution sur l'hôte cible : `lsnrctl status`
- Vérifiez la connectivité réseau entre l'outil de découverte et l'hôte Oracle sur le port 1521 (ou sur votre port personnalisé) : `nc -zv <oracle-host> 1521`
- Vérifiez que les règles de pare-feu autorisent les connexions entrantes sur le port du récepteur Oracle.
- Vérifiez le nom du service en l'exécutant `lsnrctl services` sur l'hôte Oracle. Si le nom du service est incorrect, le récepteur Oracle rejette la connexion.

Défaillances d'authentification (ORA-01017)

Symptôme : La collecte échoue en raison d'une erreur de nom d'utilisateur ou de mot de passe non valide.

Pour résoudre ce problème, vérifiez les points suivants :

- Vérifiez que le compte de service Oracle existe et qu'il n'est pas verrouillé : `SELECT account_status FROM dba_users WHERE username = 'DISCOVERY_USER';`
- Vérifiez que le mot de passe est correct en vous connectant manuellement : `sqlplus discovery_user/<password>@<host>:1521/<service_name>`
- Si le compte est verrouillé, déverrouillez-le : `ALTER USER discovery_user ACCOUNT UNLOCK;`

Privilèges insuffisants (ORA-01031)

Symptôme : la connexion réussit mais la collecte renvoie des données incomplètes.

Pour résoudre ce problème, vérifiez les points suivants :

- Vérifiez que SELECT_CATALOG_ROLE est accordé : `SELECT * FROM dba_role_privs WHERE grantee = 'DISCOVERY_USER';`
- Accordez le rôle requis s'il manque : `GRANT SELECT_CATALOG_ROLE TO discovery_user;`

Les informations d'identification manuelles indiquent une erreur mais la connexion automatique fonctionne

Lorsque vous épinglez manuellement un identifiant à un serveur, l'outil de découverte ne revient pas en cas d'échec de la connexion. Vérifiez que le port et le nom du service que vous avez configurés sur les informations d'identification correspondent à ceux du récepteur Oracle sur ce serveur spécifique. Si le serveur possède un port ou un nom de service non standard, mettez à jour la configuration des informations d'identification en conséquence.

OS-level solution de repli ne détectant pas Oracle

Si aucune information d'identification de base de données n'est configurée et que la OS-level solution de secours ne détecte pas Oracle :

- Vérifiez que les informations d'identification du système d'exploitation SSH ou WinRM sont configurées et fonctionnent pour le serveur (vérifiez l'état de la collecte des métriques du système d'exploitation).
- Pour les hôtes Linux, vérifiez qu'ils `/etc/oratab` existent ou que les processus Oracle Process Monitor (`pmon`) sont en cours d'exécution.
- Pour les hôtes Windows, vérifiez que les entrées de registre Oracle existent `HKLM\SOFTWARE\Oracle` ou que `oracle.exe` les processus sont en cours d'exécution.

Résolution des problèmes SNMP

Accédez à la machine virtuelle de l'outil de découverte

- Log-in vers la machine virtuelle de l'outil de découverte, ouvrez la console distante dans vCenter
  - Nom d'utilisateur : discovery

- Mot de passe : mot de passe

Installez les outils SNMP (si nécessaire)

- `sudo yum install net-snmp-utils -y`

Tester la connexion SNMP aux serveurs Linux

1. `snmptable -v 2c -c <COMMUNITY_STRING> <REMOTE_SERVER_IP> .1.3.6.1.2.1.6.13.1`
2. Exemple :

```
#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
```

Erreurs de collecte sur le réseau

un terminal est nécessaire pour lire le mot de passe

Erreur :

```
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
```

La commande ss demande le mot de passe utilisateur. L'utilisateur ssh configuré doit appartenir au groupe sudoers et être configuré avec sudo sans mot de passe pour la commande. ss/netstat Pour configurer le sudo sans mot de passe :

1. Créez un nouveau fichier sudoers :

```
sudo vi -f /etc/sudoers.d/<username>
```

2. Ajoutez la ligne :

```
<username> ALL=(ALL) NOPASSWD: /usr/sbin/ss, /usr/bin/netstat
```

3. Après cette modification, en cours d'exécution `sudo ss -tnap` et `sudo netstat -tnap` devrait s'exécuter sans demander de mot de passe

La collecte réseau s'est exécutée sans sudo

Si l'avertissement suivant s'affiche sur la page Inventaire découvert :

```
Network collection ran without sudo. Process-level connection data may be missing.
```

Cet avertissement indique que le compte utilisateur SSH ne dispose pas d'un accès sudo sur le serveur cible. Sans sudo, l'outil de découverte peut toujours collecter des données de connexion réseau, mais il ne peut pas déterminer à quel processus appartient chaque connexion. Pour collecter des données de connexion complètes au niveau du processus, assurez-vous que l'utilisateur SSH dispose d'un accès sudo sur le serveur cible.

Erreurs de collecte des métriques du système d'exploitation

UUID de serveur manquant pour les serveurs Linux

Si l'outil de découverte ne parvient pas à collecter l'UUID du serveur (affiché comme vide ou manquant) pour les serveurs Linux, vérifiez que les informations d'identification SSH configurées pour ces serveurs disposent de privilèges sudo. L'outil permet `dmidecode` de lire l'UUID du serveur. S'il n'`dmidecode`est pas installé, l'outil revient à la lecture`/sys/class/dmi/id/product_uuid`, qui nécessite également un accès sudo. Sans sudo, aucune méthode ne peut récupérer l'UUID.

Solution : Assurez-vous que le compte utilisateur SSH fourni à l'outil de découverte dispose d'un accès sudo sur les serveurs Linux cibles.

Problèmes d'accès dans l'inventaire découvert

Si vous voyez un message dans l'état de la collecte du serveur, tel que Informations d'identification manquantes ou Accès refusé :

1. Sélectionnez le serveur dans le tableau des serveurs découverts.
2. Choisissez Gérer les informations d'accès Vous pouvez choisir de :
    a. Sélectionnez d'autres informations d'identification dans le menu déroulant Sélectionner les informations d'identification.
    b. Sélectionnez Utiliser de nouvelles informations d'identification et fournir de nouvelles informations d'identification.
3. Enregistrez.

L'outil de découverte tente à nouveau de se connecter une fois que vous avez enregistré vos modifications.

Résolution des problèmes liés à l'authentification par clé SSH

Test de la connectivité par clé SSH à partir de l'outil de découverte

Si l'authentification par clé SSH échoue, vérifiez la connectivité entre l'outil de découverte et le serveur cible :

1. Connectez-vous à l'outil de découverte (via la console vSphere ou SSH sur l'hôte Linux).
2. Testez la connectivité SSH à l'aide de votre clé privée :

```
ssh -i /path/to/private_key -o StrictHostKeyChecking=no <username>@<target_ip>
```

3. Si la connexion réussit, le problème réside dans la manière dont la clé a été téléchargée dans l'outil de découverte. Re-upload la clé et vérifiez que le nom d'utilisateur correspond.
4. Si la connexion échoue, consultez le message d'erreur dans le tableau suivant.

Message d'erreur	Cause	Résolution
`Permission denied (publickey)`	La clé publique ne se trouve pas dans le `authorized_keys` fichier du serveur cible ou le	Ajoutez la clé publique `~/.ssh/authorized_keys` sur le serveur cible pour le bon utilisateur. Vérifiez les autorisations des fichiers :`chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys` .

Message d'erreur	Cause	Résolution
	nom d'utilisateur est incorrect.	
`Connection timed out after 20s`	Le port 22 n'est pas accessible depuis l'outil de découverte.	Vérifiez que le port 22 est ouvert entre l'outil de découverte et le serveur cible. Vérifiez les pare-feux et les groupes de sécurité.
`Connection refused`	Le service SSH n'est pas en cours d'exécution sur le serveur cible.	Démarrez le service SSH :`sudo systemctl start sshd`.
`Invalid SSH key for credential 'name'`	Le format de clé n'est pas pris en charge, les données clés sont endommagées ou le mot de passe est manquant ou incorrect.	Vérifiez que le format de clé est RSA, ECDSA ou Ed25519 au format PEM, OpenSSH ou PKCS #8. Si la clé est cryptée, assurez-vous que le mot de passe est correct.

Résolution des problèmes d'installation Linux

Le port 5000 est déjà utilisé

Symptôme : Le service de l'outil de découverte ne démarre pas après l'installation.

Résolution : Identifiez et arrêtez le processus à l'aide du port 5000 :

```
sudo ss -tlnp | grep :5000
```

Arrêtez le processus conflictuel, puis redémarrez l'outil de découverte :

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

Messages d'erreur courants

Ce tableau décrit les messages d'erreur courants et leurs explications :

Message	Location	Explication
Un mot de passe a déjà été créé	Créer une page de mot de passe	Condition de course lorsque deux utilisateurs créent des mots de passe en même temps ; actualiser
Échec de l'exportation	Page d'inventaire	Réessayer ou envoyer les journaux
Une collecte à la demande est déjà en cours	Page d'inventaire	Condition de course lorsque deux utilisateurs démarrent des collectes manuelles en même temps ; réessayez une fois la collecte manuelle en cours terminée
`Command timed out after 60s`	État de la collecte du serveur	Une commande sur le serveur cible n'a pas été exécutée dans les 60 secondes. Cela peut se produire sur des serveurs très chargés. Réessayez la collecte ou examinez la charge du serveur cible.
Une ou plusieurs informations d'identif ication contiennent des UUID inconnus	Page d'accès au système d'exploitation	Condition de course lorsque deux utilisateurs modifient les informations d'identification du système d'exploitation en même temps ; réessayez
Mot de passe non valide	Sign-in page	Mot de passe incorrect pour la connexion ; contactez l'administrateur ou contactez
Votre session a expiré. Veuillez vous reconnect er.	Sign-in page	La session a expiré, vous devez vous reconnecter
Une erreur interne s'est produite	Pages diverses	Réessayer ou envoyer les journaux

Notes de mise à jour

Cette section décrit les fonctionnalités, les améliorations et les corrections de bogues de l'outil de AWS Transform découverte, classées par date de sortie.

Date	Version	Notes de mise à jour
30 juin 2026	1,01646	Nouvelles fonctionnalités • Ajout de la découverte de bases de données Oracle. L'outil collecte la topologie, la version, l'édition, les options installées, l'utilisation des fonctionnalités et l'inventaire des composants des CDB et PDB. L'outil de découverte prend en charge les connexions SQL directes (à l'aide de SELECT_CATALOG_ROLE) et la OS-level détection de secours via SSH ou WinRM. • Ajout de la prise en charge de plusieurs informations d'identification Kerberos dans différents domaines Active Directory. Chaque identifiant s'authentifie indépendamment, ce qui permet de collecter des informations auprès de serveurs Windows dans plusieurs domaines sans conflits d'authentification. Améliorations • Collecte améliorée des métriques du système d'exploitation pour les anciens hôtes. Ajout d'une collecte de données de secours pour les anciens systèmes d'exploitation (RHEL 5, SLES 11, Windows Server 2008 R2) où les commandes modernes ne sont pas disponibles. Les données de stockage, de performance et d'interface réseau sont désormais collectées à l'aide d'interfaces système alternatives. Corrections de bugs • Correction d'échecs d'authentification Kerberos pour les serveurs découverts via. Hyper-V L'outil de découverte résout

Date	Version	Notes de mise à jour
		désormais correctement le nom d'hôte (FQDN) du serveur à partir des métadonnées de l' Hyper-V invité, qui sont requises pour la correspondance du SPN Kerberos.

Date	Version	Notes de mise à jour
14 mai 2026	1,01363	Nouvelles fonctionnalités • Ajout d'un programme d'installation Linux pour déployer l'outil de découverte sur les distributions Linux prises en charge (Amazon Linux 2, Amazon Linux 2023, RHEL 8—9, Rocky Linux 8—9, 9, Ubuntu 20.04—24.04, AlmaLinux Debian 10—12, SLES 15 SP5). • Ajout de la prise en charge de la configuration de plusieurs serveurs VMware vCenter avec déduplication automatique des machines virtuelles sur les vCenters. • Ajout de l'authentification par clé privée SSH comme alternative au nom d'utilisateur et au mot de passe pour l'accès au système d'exploitation Linux. Les formats clés pris en charge incluent RSA, ECDSA, Ed25519, OpenSSH et PKCS #8. • Ajout d'une collection réseau d'adresses privées pour capturer les connexions vers et depuis les adresses IP privées RFC 1918 ne figurant pas dans votre inventaire découvert. • Des options d'exportation ont été ajoutées pour sélectionner une plage de dates personnalisée et choisir les modules de données à inclure dans l'exportation. Améliorations • Fiabilité accrue des collectes planifiées en échelonnant les calendriers des collecteurs. • Amélioration des performances de collecte des métriques du système d'exploitation grâce au traitement par lots de commandes SSH. • Les modifications d'informations d'identification réessayent désormais immédiatement les serveurs précédemment défaillants.

Date	Version	Notes de mise à jour
		• La collecte des métriques du système d'exploitation indique désormais un état partiel lorsque certaines commandes renvoient des résultats vides. • Visibilité améliorée des erreurs liées aux problèmes de connexion à vCenter dans le tableau de bord.
7 avril 2026	1,0,1074	Nouvelles fonctionnalités • Ajout de la prise en charge de Hyper-V la découverte Microsoft, notamment de la découverte automatique des machines virtuelles à partir d' Hyper-V hôtes avec déduplica tion des clusters sur incident. • Ajout de la prise en charge de l'importation de serveurs via le téléchargement de fichiers CSV. • Ajout d'une collecte de métriques du système d'exploitation avec six modules indépendants : performances des serveurs, performances de stockage, provisionnement des serveurs, provisionnement du stockage, interfaces réseau et processus en cours d'exécution. • Ajout d'une option de Hyper-V déploiement à l'aide d'un fichier image VHD. • Renforcement de la sécurité sur site en supprimant des EC2-specific services et en bloquant l'accès au point de terminais on des métadonnées de l'instance.

Date	Version	Notes de mise à jour
26 mars 2026	1,01014	Corrections de bogues et améliorations • La validation de la capitalisation du domaine Kerberos a été déplacée du backend vers le frontend. • Basculé de Python-kerberos vers Python-pykerberos et fait du cache basé sur des fichiers la valeur par défaut. • Correction de la validation de l'ID du serveur de modification en bloc sans distinction majuscules/minuscules. • Nom de fichier ZIP d'exportation fixe (maintenant`discovery_tool_export.zip`). • Service fixe l'exécution de la vérification et ajout de journaux de débogage pour les informations d'identification du système. • Ajout d'un script de configuration réseau pour créer un artefact.
16 décembre 2025	1,0718	Nouvelles fonctionnalités et améliorations • Ajout de la prise en charge de l'UUID SMBIOS pour empêcher la duplication des machines virtuelles dans les services en aval. • Nous avons introduit Min/Max/Avg le suivi et étendu les métriques de stockage pour une meilleure surveillance des ressources. • Améliorations apportées à la validation de l'API. • Ajout d'une fonctionnalité de panneau d'aide avec des conseils contextuels. • Terminologie mise à jour de « collecteur » à « outil » dans l'ensemble de l'interface.

Date	Version	Notes de mise à jour
31 octobre 2025	1.0.0	Première version Lancement initial de l'outil de AWS Transform découverte. Cette version inclut : • Collecte hors ligne (aucune dépendance à l'égard d'un AWS compte ou d'Application Discovery Service). • Découverte et surveillance de VMware. • Découverte de bases de données SQL Server. • Server-to-server collecte de communications via SSH, WMI et SNMP.

Migrations (y compris VMware)

AWS Transform peut vous aider à migrer vos environnements de serveurs virtuels et bare metal vers Amazon EC2 en utilisant l'IA générative, notamment VMware Hyper-V, et d'autres sources. Un AI-powered agent accélère chaque étape de votre migration, depuis la découverte et la planification jusqu'à la migration du réseau et au réhébergement des serveurs, réduisant ainsi l'effort manuel traditionnellement requis pour les migrations à grande échelle. Vous interagissez avec l'agent via une interface conversationnelle qui vous guide étape par étape, afin que vous puissiez vous concentrer sur les décisions plutôt que sur leur exécution.

Capacités et fonctionnalités clés

AWS Transform offre les fonctionnalités et fonctionnalités clés suivantes pour la migration de vos environnements de serveurs vers AWS.

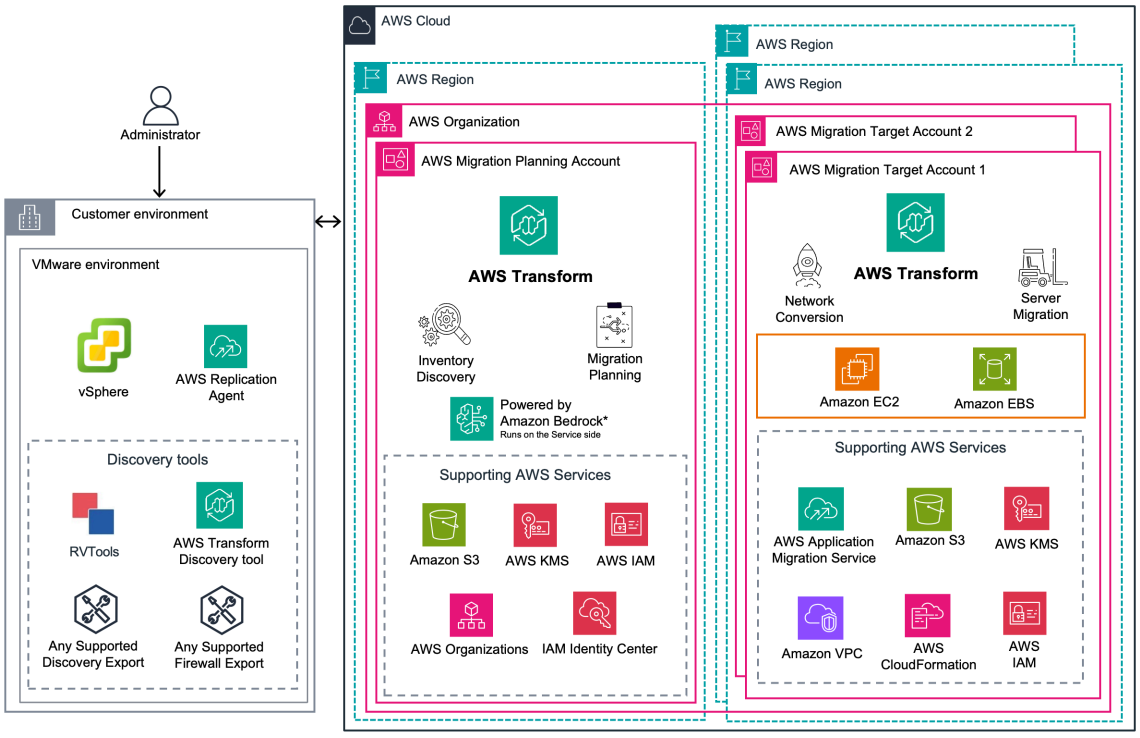
- Une découverte flexible qui vous accompagne où que vous soyez, avec de multiples options pour capturer votre environnement source :
  - Découverte assistée de votre environnement VMware à l'aide de collecteurs provenant de AWS Application Discovery Service.
  - L'outil open source Export for vCenter (environnements VMware).
  - Importation de données de découverte collectées indépendamment (n'importe quel environnement source).
- AI-driven une migration réseau qui traduit la configuration de votre réseau source en une architecture Amazon VPC prête pour la production, de sorte que vous n'ayez pas à la concevoir à partir de zéro.
- Planification intelligente de la migration qui regroupe automatiquement les applications et séquence les vagues de migration, ce qui vous permet d'avancer plus rapidement en réduisant les cycles de planification.
- Réhébergement automatique des serveurs pour faire fonctionner vos serveurs de manière native sur Amazon EC2, avec des tests guidés et des flux de travail de basculement.
- Interface localisée, vous permettant d'utiliser AWS Transform pour les migrations dans la langue de votre choix. Pour de plus amples informations, veuillez consulter Paramètres de langue.

AWS Transform prend en charge la migration des serveurs Windows et Linux des systèmes d'exploitation pris en charge. Pour obtenir la liste complète des systèmes d'exploitation pris en

charge, consultez la section Systèmes d'exploitation pris en charge dans le Guide de AWS Transform MGN l'utilisateur.

AWS Transformez l'architecture de migration

AWS Transform orchestre l'ensemble du cycle de vie de la migration à partir d'une interface unique. Le schéma suivant présente une vue d'ensemble de l'architecture.



Emplois liés à la migration

Pour commencer la migration, créez un espace de travail et lancez une tâche de migration. Un espace de travail est un conteneur logique pour une ou plusieurs tâches de migration, vous offrant un emplacement unique pour gérer l'ensemble de votre migration.

Obtenir un espace de travail

Pour plus d'informations sur la création d'un espace de travail, consultez la section Mise en route.

Votre espace de travail détermine l' Région AWS emplacement de vos tâches, de vos données de découverte et de vos recommandations de AWS transformation. Pour travailler dans une autre région

Région AWS, demandez à votre administrateur de créer un espace de travail dans cette région. Pour plus d'informations sur les Régions AWS pris en charge, veuillez consulter Régions prises en charge.

Vous pouvez spécifier une autre Région AWS cible de migration. Cela signifie que vous pouvez exécuter la découverte dans une région mais déployer votre environnement cible dans une autre. Dans ce cas, certaines de vos données seront transférées Régions AWS. Les données de réplication de serveurs ne sont pas transférées entre les régions et sont directement transférées de votre environnement source vers votre compte cible et votre région. Pour de plus amples informations, veuillez consulter the section called "Connecter la cible Compte AWS s et régions".

Types d'emplois

Que vous ayez besoin d'une migration de bout en bout ou que vous souhaitiez aborder une phase spécifique, AWS Transform propose les types de tâches de migration suivants, parmi lesquels vous pouvez choisir en fonction de vos besoins en matière de migration. Outre ces options prédéfinies, vous pouvez ajouter ou supprimer dynamiquement n'importe quelle étape de votre tâche à tout moment afin de personnaliser votre flux de migration.

End-to-end migration

Idéal pour les migrations complètes où vous souhaitez que AWS Transform gère tout, de la découverte au réhébergement.

1. Effectuez une découverte
2. Élaborez un plan de migration
3. Connectez les comptes cibles
4. Construire une zone d'atterrissage
5. Migrer le réseau
6. Migrer des serveurs

Planification de la découverte et de la migration

Utilisez-le lorsque vous souhaitez évaluer votre environnement et élaborer un plan de vagues avant de vous engager dans son exécution.

1. Effectuez une découverte
2. Élaborez un plan de migration

Migration du réseau

Utilisez-le lorsque votre zone de destination et vos comptes sont déjà configurés et que vous devez migrer la configuration de votre réseau vers AWS.

1. Connectez les comptes cibles
2. Migrer le réseau

Zone d'atterrissage

Utilisez-le lorsque vous devez configurer votre AWS base multi-comptes avant de migrer des charges de travail.

1. Connectez les comptes cibles
2. Construire une zone d'atterrissage

Migration de zones d'atterrissage, de réseaux et de serveurs

Utilisez-le lorsque la découverte et la planification sont déjà terminées et que vous souhaitez que AWS Transform gère la configuration et l'exécution de l'infrastructure.

1. Connectez les comptes cibles
2. Construire une zone d'atterrissage
3. Migrer le réseau
4. Migrer des serveurs

Planification de la migration et migration des serveurs

Utilisez-le lorsque votre réseau est déjà en place et que vous souhaitez passer directement de la découverte au réhébergement.

1. Effectuez une découverte
2. Élaborez un plan de migration
3. Connectez les comptes cibles
4. Migrer des serveurs

Création et démarrage d'un emploi

Pour créer une tâche de migration, procédez comme suit. Pour plus d'informations sur les différents types de tâches, consultezthe section called “Types d'emplois”.

Pour créer et démarrer un nouvel emploi lié à la migration

1. Sur la page d'accueil de votre espace de travail, choisissez Créer une offre d'emploi.
2. Choisissez l'option de migration, puis spécifiez le type de tâche de migration que vous souhaitez créer. Pour plus d'informations sur les étapes incluses dans chacun des types de tâches de migration, consultezthe section called “Types d'emplois”.
3. Après avoir répondu à toutes les questions du chat, choisissez Créer une offre d'emploi.

Téléchargement d'un rapport récapitulatif sur l'espace de travail

Vous pouvez générer un rapport récapitulatif de l'espace de travail sous forme de PDF téléchargeable à tout moment pendant votre migration. Le rapport fournit une vue consolidée de toutes les tâches de migration de votre espace de travail, notamment :

- Statuts des tâches et étapes du flux de travail en cours
- Actions et approbations des utilisateurs
- Détails de la planification des vagues
- Topologie de migration réseau
- Configuration de la zone d'atterrissage
- Réhébergez la progression
- Décisions relatives à la conteneurisation
- Principaux artefacts produits

Pour générer un rapport, demandez à l'agent dans le chat. Par exemple, « Donnez-moi un résumé de l'avancement de ma migration sur l'ensemble des jobs dans mon espace de travail ». L'agent compile les données de toutes les tâches et diffuse le PDF directement dans le chat.

Utiliser le mode expert

Le mode Expert minimise les interactions lors d'une tâche de migration. Vous fournissez des entrées et des préférences avant l'exécution, et l'agent les applique automatiquement au fur et à mesure de

l'avancement de la tâche. L'agent fait une pause uniquement lorsqu'il ne parvient pas à résoudre une question ou lorsqu'une erreur nécessite une action.

Pour utiliser le mode expert

1. Créez la tâche de migration et définissez son plan de travail. Avant de démarrer une étape, activez le mode expert en saisissant « Exécuter cette tâche en mode expert » dans le chat ou en saisissant la commande /expert-mode-on dans l'application Web.
2. Commencez le travail. L'agent ajoute la collecte de données comme première étape et affiche les entrées disponibles pour votre plan de travail.
3. Indiquez vos entrées et vos préférences. Vous pouvez inclure plusieurs valeurs dans un message ou joindre un fichier UTF-8 texte (256 Ko maximum). Par exemple, saisissez « Utiliser la migration multi-comptes, le dimensionnement moyen d'Amazon EC2, la location partagée et un maximum de 20 serveurs par vague ».
4. Vous pouvez éventuellement spécifier des points de contrôle de révision ou des commutateurs de mode. Par exemple, saisissez « Suspendre mon examen après la planification de la migration » ou « Passer en mode standard après la migration du réseau ».
5. Passez en revue les valeurs collectées et corrigez les valeurs que l'agent considère comme non valides, puis demandez à l'agent de continuer.

L'agent traite les étapes et les vagues de manière séquentielle, présentant des résultats intermédiaires sans attendre de confirmation, sauf si vous définissez un point de contrôle de révision. Vous pouvez envoyer des instructions dans le chat à tout moment et passer en mode standard à la demande.

Limitations

- Vous devez activer le mode expert avant de démarrer une étape. Vous ne pouvez pas l'activer en cours de travail.
- L'agent fait une pause lorsqu'il ne parvient pas à résoudre une question à partir des entrées collectées, lorsqu'une entrée n'est pas valide ou lorsqu'une erreur nécessite une action.
- Le mode Expert ne contourne pas les exigences d'approbation. Les opérations nécessitant une approbation attendent toujours l'autorisation dans l'onglet Approbations.
- Les paramètres collectés s'appliquent globalement à toutes les étapes et vagues pertinentes. Wave-specific les instructions sont évaluées lorsque cette onde passe.

- Les fichiers texte d'entrée doivent utiliser un UTF-8 encodage et ne peuvent pas dépasser 256 Ko. Cette limite ne s'applique pas à l'inventaire ou à d'autres artefacts de migration.

Limitations

AWS Transform présente les limites suivantes :

- Si vous arrêtez une tâche de migration en cours, puis demandez à l'agent de la redémarrer, la tâche recommencera depuis le début et vous perdrez tout progrès réalisé dans cette tâche. Cependant, les artefacts créés dans la tâche avant de la redémarrer seront toujours disponibles.
- Vous pouvez spécifier une cible Région AWS par tâche de migration. Pour migrer des applications vers différentes régions cibles, créez plusieurs tâches de migration.
- Multi-account migration — Une seule région uniquement — Vous pouvez migrer vers plusieurs comptes au sein d'un seul Région AWS. Pour les migrations multirégionales, vous devez créer des projets distincts pour chaque région cible.
- Multi-account migration — Un compte par vague — Chaque vague de migration ne peut cibler qu'un seul compte. Les demandes nécessitant différents comptes cibles doivent être placées dans des vagues distinctes.
- Multi-account migration — AWS Organisations requises — Tous les comptes cibles doivent faire partie d'une AWS organisation.

Découvrez les données sources

Téléchargez les données de votre serveur local et AWS Transform détecte automatiquement le format et la structure des fichiers, analyse et extrait les enregistrements d'entités structurés, supprime les doublons dans plusieurs fichiers, valide la qualité des données et signale les problèmes, puis prépare un résumé prêt à être utilisé pour la planification de la migration en aval.

AWS Transform accepte les données provenant des sources suivantes :

- AWS Outil de découverte de transformations (CSV et JSON au format ZIP)
- AWS Collecteur Migration Evaluator
- RVTools (fichier Excel ou fichier ZIP contenant des fichiers CSV)
- ModelizeIt (CSV au format ZIP)
- AWS Exportations au format MPA (Migration Portfolio Assessment) (par exemple, Cloudamize)

Pour chaque source de données, AWS Transform accepte le fichier du serveur principal individuellement. Les fichiers supplémentaires tels que les connexions ne sont traités que s'ils sont inclus dans un fichier ZIP avec les fichiers du serveur ou dans un fichier Excel avec la feuille du serveur.

Téléchargez les données les plus détaillées disponibles. Vérifiez vos fichiers d'exportation avant de les charger pour vous assurer de l'exhaustivité et de l'exactitude des données. Vérifiez que tous les fichiers requis sont inclus dans votre téléchargement et que les données reflètent l'état actuel de votre environnement. Cela permet à AWS Transform de capturer plus précisément votre environnement sur site et de mieux prendre en charge la planification de la migration, y compris le regroupement des applications et la planification des vagues. Vous pouvez ajouter des données de manière incrémentielle au fur et à mesure de leur obtention. AWS Transform déduplique automatiquement les enregistrements lors de plusieurs téléchargements.

Après le téléchargement, passez en revue vos données de découverte en développant les données locales de Discover dans le Job Plan et en sélectionnant Résumé de l'état de préparation de l'inventaire. Vous pouvez poser des questions dans le chat pour vérifier l'ingestion ou identifier les problèmes. Par exemple, vous pouvez poser des questions sur le système d'exploitation et les versions. Pour corriger les erreurs, chargez à nouveau vos données et AWS Transform fusionne automatiquement les enregistrements mis à jour. Vous pouvez également supprimer un fichier précédemment chargé si vous ne souhaitez plus utiliser ces données d'inventaire.

Élaborez un plan de migration

L'étape de planification de la migration de AWS Transform for migrations est une expérience collaborative basée sur le chat pour la planification de migrations importantes. AWS Les agents de Transform appliquent des directives AWS prescriptives pour guider les clients depuis l'analyse des données sur site jusqu'à la finalisation des plans de vague de migration.

Une fois la tâche de découverte de données sur site terminée avec succès, AWS Transform utilise les données de découverte pour regrouper les applications en vagues de migration. AWS Transform vous guide pas à pas pour analyser et définir la portée de vos serveurs, les regrouper dans des applications, générer des groupes de migration et créer des vagues de migration.

AWS Transform prend en charge la planification itérative tout au long du processus :

- Vous pouvez poser des questions pour mieux comprendre comment AWS Transform a analysé les logiciels que vous avez installés, par exemple en ce qui concerne les dépendances des serveurs et l'architecture réseau.

- Vous pouvez ajuster la portée au sein des groupes d'applications et des vagues à tout moment.
- Vous pouvez télécharger à nouveau les données de découverte, et AWS Transform traitera, dédupliquera et fusionnera automatiquement les nouveaux enregistrements avec les données existantes.
- Lorsque des modifications sont détectées, telles que des dépendances récemment découvertes ou des ajouts à l'infrastructure, AWS Transform signale les groupes de dépendances concernés et fournit des recommandations pour les ajustements du plan de vagues.
- La planification de la migration peut également utiliser des données textuelles non structurées pour enrichir le processus de planification.

La planification de la migration comporte quatre étapes :

- Dans Scope and analysis, vous pouvez examiner vos données de découverte, poser des questions sur votre environnement logiciel et réseau et déterminer les ressources concernées par la migration.
- Dans les applications de groupe, vous pouvez fournir une combinaison de règles commerciales et techniques concernant, par exemple, l'analyse des noms d'hôte, les dépendances réseau et les règles métier, afin que la planification de la migration puisse regrouper votre infrastructure en applications. Si vous disposez déjà d'un inventaire de vos applications, la planification de la migration peut l'utiliser à la place.
- Dans Générer des groupes de migration, vous pouvez indiquer à la planification de la migration vos exigences techniques et commerciales afin qu'elle puisse déterminer quelles applications doivent être déplacées ensemble. Les dépendances techniques incluent les bases de données, les files de messages ou d'autres ressources partagées entre plusieurs applications. Les dépendances commerciales et opérationnelles incluent la criticité commerciale, le RPO et le RTO, l'emplacement des centres de données et les propriétaires des applications.
- Enfin, dans Build waves, vous pouvez donner un contexte à la planification de la migration concernant vos délais et vos priorités afin qu'il puisse élaborer un plan de migration que vous pouvez effectuer. Vous pouvez sélectionner des groupes de déplacements à inclure dans une vague en fonction de facteurs tels que le score de priorité, la taille des groupes de déplacements, le nombre d'utilisateurs et la complexité de l'application.

Terminologie de planification de la migration

Vague migratoire

Groupe logique d'applications qui sont migrées ensemble. Les vagues migratoires sont composées d'un ou de plusieurs groupes de déplacements.

Déplacer le groupe

Ensemble d'applications co-dépendantes qui doivent être déplacées ensemble. Ils peuvent présenter des dépendances techniques telles qu'une base de données partagée ou des dépendances commerciales telles que la prise en charge d'une fonction métier partagée.

Dépendance

Relation entre les systèmes. Il existe plusieurs types de dépendances :

- Dépendances critiques ou difficiles. Les systèmes ne peuvent pas fonctionner sans dépendance. Les exemples courants incluent les applications qui dépendent de bases de données, d'autres applications ou de services.
- Dépendances douces. Non critique pour le fonctionnement du système. Les exemples courants incluent les dépendances insensibles à la latence qui peuvent être migrées indépendamment.
- Non-technicaldépendances. Dépendances commerciales, organisationnelles, opérationnelles et de conformité liées à votre organisation et à ses priorités. Les exemples incluent le partage des fonctions commerciales et la propriété organisationnelle.

Flux de travail

La planification de la migration est un flux de travail interactif et itératif. Vous pouvez revenir en arrière et modifier les étapes précédentes à tout moment. Un flux de travail typique de planification de la migration est le suivant :

1. La planification de la migration commence par la synthèse des données de découverte disponibles. Passez en revue les données disponibles et revenez à tout moment à l'étape de découverte pour fournir des données supplémentaires.
2. Au cours de l'étape de cadrage et d'analyse, vous pouvez poser des questions sur votre environnement sur site afin de valider les données que vous avez collectées. Voici quelques exemples de questions :
   a. Répertorier mes serveurs par système d'exploitation

   b. Résumer la topologie de mon réseau local

   c. Répertoriez les technologies les plus courantes utilisées dans mon environnement.

3. Lors de l'analyse de votre environnement, si vous identifiez des serveurs qui ne devraient pas être concernés par la migration, vous pouvez demander à AWS Transform d'exclure ces ressources. En voici quelques exemples :

   a. Supprimez tous les serveurs dont le nom d'hôte contient un ancien nom d'hôte

   b. Supprimez tous les serveurs de la version 10.0.2. 0/24 sous-réseau

   c. Supprimez tous les serveurs exécutant des versions de Windows antérieures à 2022

4. Une fois que vous aurez suffisamment exploré votre environnement et déterminé l'étendue de votre migration, vous pouvez demander à AWS Transform de passer à l'étape suivante de planification de la migration.

5. L'étape suivante consiste à regrouper les demandes. Si vos serveurs sont déjà mappés à des applications, vous pouvez demander à AWS Transform d'utiliser ce mappage et ignorer cette étape. Si vos applications ne sont pas prédéfinies, vous pouvez fournir la logique technique et commerciale qui définit vos applications. AWS Transform vous guidera tout au long du processus de regroupement des applications et vous proposera les points de données que vous pouvez fournir pour regrouper efficacement vos serveurs au sein d'applications. Plus vous pouvez fournir d'informations sur vos applications locales, plus AWS Transform peut regrouper efficacement vos serveurs en applications. Une fois que vous avez fourni suffisamment d'informations, vous pouvez demander à AWS Transform de regrouper les applications.

6. Une fois le regroupement des applications effectué, passez en revue les groupes d'applications. Vous pouvez demander à AWS Transform d'apporter les modifications nécessaires, par exemple :

   a. Déplacer le serveur example-server vers application-5

   b. Renommer l'application-5 « HR App Test Environment »

   c. Supprimer tous les serveurs Linux de la ferme de développement IIS

7. Une fois vos applications regroupées, demandez à AWS Transform de passer à l'étape suivante

8. L'étape suivante consiste à déplacer le regroupement. Lors de l'étape de regroupement des déplacements, vous identifiez les applications qui doivent être déplacées ensemble. Fournissez un contexte concernant vos dépendances techniques et non techniques. AWS Transform vous guidera tout au long du processus et vous proposera des points de données que vous pouvez fournir pour regrouper vos applications. Il y a plusieurs considérations à prendre en compte à ce stade, notamment :

   a. Quelle devrait être la taille cible du groupe de déménagement ?

b. Voulez-vous combiner des environnements, par exemple dev, test et prod, pour chaque application, ou les scinder ?

c. Comment souhaitez-vous prendre en compte les dépendances réseau ? Toutes les dépendances sont-elles critiques ou certaines dépendances peuvent-elles être considérées comme des dépendances douces et être réparties entre les groupes de déménagement ?

9. Une fois que vous avez défini vos règles de regroupement de déplacements, demandez à AWS Transform d'exécuter votre stratégie de regroupement de déplacements. Vous pouvez ensuite consulter et modifier vos groupes de déplacements. Une fois que vous avez examiné vos groupes de déménagements, vous pouvez demander à AWS Transform de passer à l'étape finale de planification de la migration.

10. La planification des vagues est la dernière étape de la planification de la migration. Au cours de cette étape, vous regroupez vos groupes de déplacements en vagues de migration et vous hiérarchisez ces vagues. Au cours de l'étape de planification des vagues, AWS Transform vous guidera en vous fournissant les priorités commerciales nécessaires pour regrouper vos groupes de déménagements en vagues, puis hiérarchiser ces vagues. Les considérations relatives à la planification des vagues incluent :

a. L'importance commerciale de chacun de vos groupes de déménagement

b. Les délais de migration et les délais pour chaque groupe de déménagement

c. Les risques associés à chaque groupe de déménagement

d. Le nombre de serveurs à migrer par vague

11. Une fois que vous avez fourni suffisamment de conseils sur la façon de regrouper en vagues, demandez à AWS Transform d'exécuter la planification des vagues. Vous pouvez ensuite revoir vos vagues et les modifier.

12. Une fois que vous avez finalisé votre plan Wave, vous pouvez terminer la planification de la migration et passer à l'exécution. Vous pouvez revenir à la planification de la migration à tout moment pour peaufiner et modifier votre plan.

13. Pour chaque vague, vous pouvez attribuer une stratégie de migration : réhébergement (migration des serveurs vers Amazon EC2) et conteneurisation (conteneurisation du code source et déploiement sur Amazon Elastic Container Service ou Amazon Elastic Kubernetes Service). Lorsque vous attribuez à une vague la stratégie de conteneurisation, AWS Transform exécute le flux de travail de conteneurisation du code source pour cette vague lors de l'exécution de la migration. Pour de plus amples informations, veuillez consulter Conteneurisation du code source. Pour obtenir les stratégies AWS recommandées dans le cadre des 7R avant de les attribuer, consultez. the section called “Recommandations des 7R”

Recommandations relatives à la stratégie de migration (7R)

Lors de la planification de la migration, AWS Transform peut analyser l'inventaire que vous avez découvert et recommander une stratégie de migration, l'une des 7R standard du secteur, pour chaque serveur et chaque application. Chaque recommandation comprend un service AWS cible suggéré, un score de confiance et le raisonnement qui le sous-tend. Cela vous donne un point de départ défendable pour votre plan de vagues et fait apparaître des opportunités de modernisation que vous pourriez manquer autrement.

Les sept stratégies sont le réhébergement, la replateforme, le refactoring, le rachat, la retraite , la fidélisation et la relocalisation. AWS Transform lit les signaux contenus dans vos données, tels que le système d'exploitation, l'utilisation et le type de charge de travail, afin de formuler des recommandations explicables. Par exemple, il peut recommander de retirer les serveurs inactifs ou en fin de vie, de déplacer SQL Server ou des bases de données open source vers Amazon RDS, de transférer les charges de travail de messagerie et de collaboration vers Microsoft 365, de conserver les anciens systèmes spécialisés et de réhéberger les charges de travail restantes sur Amazon EC2. Les recommandations s'étendent des serveurs individuels aux applications et à l'ensemble de votre portefeuille, avec une vue de la criticité par stratégie et des résumés par niveau de vague.

Pour générer un rapport sur la stratégie de migration (7R), procédez comme suit :

1. Terminez l'étape Discover on-premises data et regroupez vos serveurs en applications. Les deux sont nécessaires pour que AWS Transform puisse fournir des recommandations par serveur et par application.
2. Dans le chat de planification de la migration, demandez à AWS Transform un rapport sur la stratégie de migration (7R). Par exemple, Générez un R-strategy rapport. Une fois le regroupement des applications terminé, AWS Transform propose également de générer le rapport pour vous.
3. AWS Transform analyse votre inventaire, applique le framework 7R et génère le rapport. Vous pouvez fournir des informations telles que le nom de votre organisation et les éventuels filtres permettant de définir la portée de l'analyse.
4. Passez en revue les recommandations. Pour modifier une recommandation, indiquez-le à AWS Transform dans le chat. Vous pouvez modifier un seul serveur ou une seule application, ou appliquer une modification en bloc (par exemple, par système d'exploitation, environnement, vague ou priorité). AWS Transform met à jour le rapport en fonction de vos modifications.

Par défaut, AWS Transform produit un tableau de bord HTML interactif que vous pouvez filtrer et explorer. Sur demande, vous pouvez également générer un document PDF à partager avec les parties prenantes, ou un diaporama Microsoft PowerPoint (PPTX) à présenter ; le PDF et les PowerPoint résultats sont des instantanés instantanés de la même analyse. Le rapport inclut une stratégie recommandée et un service AWS cible pour chaque serveur et application, des scores de confiance et un raisonnement, des opportunités de modernisation mises en évidence, une vue de la criticité par stratégie, des résumés des niveaux de vague et des indicateurs de risque.

La stratégie recommandée dans ce rapport complète la stratégie par vague que vous attribuez lors de la planification des vagues. Pour la conteneurisation du code source, consultez. Conteneurisation du code source

Création de diagrammes et rapports

Lors de la planification de la migration, AWS Transform transforme l'inventaire découvert et les résultats de planification en diagrammes visuels et en rapports analytiques. Vous les générez de manière conversationnelle dans le chat de planification. Par exemple, « Afficher un diagramme de topologie de réseau » ou « Générer un rapport sur les risques ». AWS Transform les crée à partir des données que vous avez déjà fournies, sans aucune configuration requise.

Les diagrammes sont interactifs et vous permettent d'explorer visuellement votre environnement. Les diagrammes disponibles incluent :

- Topologie du réseau : carte interactive de vos serveurs et de leurs relations réseau, conçue pour s'adapter à de grands environnements composés de milliers de nœuds.
- Dépendance des applications : relations orientées entre applications dérivées des connexions réseau que vous avez observées.
- Diagramme de Gantt par vagues : vue chronologique de vos vagues de migration indiquant les calendriers, les dépendances, les jalons et les progrès (disponible après la planification des vagues).
- Graphiques généraux : graphiques à secteurs, graphiques à barres, histogrammes, arborescences et tableaux récapitulatifs reprenant les dimensions des données que vous choisissez.

Les rapports fournissent une analyse narrative et des recommandations concernant vos données de migration. Les rapports disponibles incluent :

- Évaluation des risques : évalue chaque application en fonction de sa complexité technique, de son risque de dépendance, de sa préparation à la migration et de son risque opérationnel, avec des résumés par application, par vague et à l'échelle du portefeuille.
- Stratégie de migration (7R) Per-server et recommandations de stratégie par application. Pour de plus amples informations, veuillez consulter the section called "Recommandations des 7R".
- Rapports généraux et personnalisés : rapports analytiques pour des demandes telles que les résumés de préparation des dirigeants, les compromis coûts-risques et les évaluations des candidats en conteneurisation.

Certains résultats dépendent de l'état d'avancement de votre planification. Par exemple, les diagrammes de dépendance des applications utilisent vos données de connexion réseau. Le diagramme de Gantt sur les vagues et les résumés des rapports sur le niveau des vagues sont disponibles une fois la planification des vagues terminée. Si une condition préalable est manquante, AWS Transform vous indique ce qui est nécessaire et peut d'abord exécuter l'étape requise.

AWS Transform fournit des diagrammes sous forme de code HTML interactif que vous pouvez filtrer et explorer. Par défaut, AWS Transform fournit les rapports sous la forme d'un fichier HTML autonome. Sur demande, AWS Transform peut également générer un document PDF à partager avec les parties prenantes ou un diaporama Microsoft PowerPoint (PPTX) à présenter. Le PDF et les PowerPoint sorties sont des instantanés instantanés de la même analyse.

Connecter la cible Compte AWS s et régions

Connectez AWS Transform à votre AWS environnement cible afin que l'agent puisse déployer l'infrastructure, migrer les réseaux et réhéberger les serveurs en votre nom. Cela implique trois étapes : sélectionnez votre type de migration, fournissez les détails de votre accord MAP (le cas échéant) et configurez le connecteur. Ces paramètres s'appliquent à toutes les étapes de la migration, y compris la migration du réseau, la zone d'accueil et le réhébergement du serveur.

Étape 1 : Sélection du type de migration

AWS Transform prend en charge les migrations à compte unique et à comptes multiples. Choisissez l'option qui correspond à votre environnement cible :

- Single-account migration : toutes les charges de travail sont migrées vers une seule cible Compte AWS. Le compte cible du connecteur et le compte cible sont identiques.

- Multi-account migration — Migrez les charges de travail sur plusieurs comptes de votre organisation à partir d'un seul espace de travail. Le connecteur doit être connecté au compte de gestion de l'organisation ou à un compte d'administrateur délégué (DA) enregistré pour AWS Transform MGN et CloudFormation StackSets.

Étape 2 : accord MAP

Si votre migration s'inscrit dans le cadre du programme d'accélération de la AWS migration (MAP 2.0), indiquez votre identifiant Migration Portfolio Experience (MPE). Il s'agit d'un code à 10 caractères utilisant des lettres majuscules et des chiffres (par exemple, ABCDE12345). Lorsque vous fournissez votre identifiant MPE, la balise MAP est appliquée à toutes les ressources créées lors des étapes de migration du réseau, de zone d'accueil et de réhébergement du serveur. Le format des balises est le suivant :

- Clé : Valeur `map-migrated` : `mig`*`MPE_ID`*

Vous devez appliquer des balises MAP pour recevoir des crédits MAP. Pour plus d'informations sur MAP, consultez la section Programme d'accélération de la AWS migration.

Étape 3 : Configuration du connecteur

Vous utilisez le connecteur de compte cible pour connecter votre tâche de migration à l' AWS environnement dans lequel résideront vos charges de travail après la migration. Avant de commencer, vérifiez que votre cible Compte AWS possède les autorisations, les quotas et les configurations nécessaires pour prendre en charge votre infrastructure migrée.

Lorsque vous approuvez la demande de connecteur, vous accordez des autorisations AWS Transform pour :

- Gérez les opérations de compartiment Amazon S3 (read/write) pour la migration vers VMware, ainsi que l'accès au AWS Migration Hub et au Service de migration des AWS applications (MGN). Cela inclut les autorisations pour les éléments suivants, tous limités aux ressources du compte cible qui sont étiquetées avec `CreatedBy:AWSTransform` ou `CreatedFor:AWSTransform` :
  - Gérez les vagues migratoires.
  - Gérez les configurations réseau (Amazon EC2, VPC, Transit Gateway, Direct Connect, Load Balancers, Network Firewall).
  - Gérez les déploiements de CloudFormation piles.

  - Effectuez des installations automatisées d'agents via Systems Manager.
- Migrez vos charges de travail sur site vers la cible Compte AWS et la région en utilisant les informations stockées dans la région de découverte.
- Fournir et gérer l'infrastructure de la zone d'atterrissage dans la cible Compte AWS et la région. Cela inclut les autorisations pour les éléments suivants, limitées aux ressources qui sont étiquetées avec, le cas `CreatedBy:AWSTransform` échéant :
  - Effectuez des opérations de compartiment Amazon S3 (création, lecture, écriture, suppression) pour les compartiments commençant `transform-vmware-landing-zone-` par.
  - Gérez les déploiements de CloudFormation piles et les ensembles de modifications pour les piles de zones d'atterrissage.
  - Effectuez les opérations AWS de la tour de contrôle. Vous pouvez gérer les zones d'atterrissage, activer les lignes de base et activer les contrôles.
  - Gérez AWS les organisations. Vous pouvez créer et gérer des unités organisationnelles, créer des comptes et déplacer des comptes.
  - Gérez les politiques de contrôle des services (SCP) via AWS Control Tower.
  - Gérez les artefacts de provisionnement du catalogue de AWS services.

> **Note**
>
> Les types de connecteurs peuvent être mis à jour lorsque de nouvelles fonctionnalités nécessitent des modifications d'autorisations. La version actuelle pour le type de connecteur de compte cible est 2.0. Lorsque vous créez un nouveau connecteur, il utilise la dernière version.

Avant de configurer le connecteur, comprenez les rôles de compte impliqués dans votre migration :

Compte	Description
AWS Transformer le compte	Tout compte de membre de votre AWS organisation sur lequel vous avez configuré AWS Transform. C'est là que s'exécute votre espace de travail AWS Transform. Il n'est pas nécessaire qu'il s'agisse du compte de gestion.

Compte	Description
Compte cible Connector	Le compte pour lequel votre connecteur AWS Transform est configuré. Cela dépend de votre type de migration : • Single-accountmigration : connectez-vous au compte vers lequel vous migrez les charges de travail. Le compte cible du connecteur et le compte cible sont identiques. • Multi-accountmigration : connectez-vous au compte de gestion de l'organisation ou à un compte d'administrateur délégué (DA). Le compte DA doit être enregistré en tant qu'administrateur délégué à la fois pour MGN et CloudFormation StackSets pour votre AWS organ isation. AWS Transform vérifie si le compte connecté est le compte de gestion ou un compte DA et ajuste son comportement en conséquen ce.
Compte cible	L' Compte AWS endroit vers lequel vos charges de travail sont migrées. Dans le cas d'une migration à compte unique, il s'agit du compte cible du connecteur. Dans le cas d'une migration multi-comptes, il s'agit des comptes membres individuels qui reçoivent les charges de travail migrées.

Utilisation d'un compte administrateur délégué

Pour les migrations impliquant plusieurs comptes, il est AWS recommandé d'utiliser un compte d'administrateur délégué (DA) plutôt que le compte de gestion de l'organisation directement. Un compte DA suit le principe du moindre privilège en limitant l'étendue des autorisations requises pour les opérations de migration. Le compte DA doit être enregistré en tant qu'administrateur délégué à la fois pour MGN et CloudFormation StackSets pour votre AWS organisation.

La principale différence entre les deux options est la suivante :

- Compte de gestion : peut permettre un accès sécurisé pour MGN et pour l' CloudFormation StackSets ensemble de l'organisation. AWS Transformez les CloudFormation StackSets API d'appels avec`CallAs: SELF`.
- Compte administrateur délégué : impossible d'activer l'accès sécurisé directement (cela doit être effectué à partir du compte de gestion), mais peut gérer les serveurs sources MGN, lancer des

instances et les déployer CloudFormation StackSets sur les comptes membres. AWS Transformez les CloudFormation StackSets API d'appels avec`CallAs: DELEGATED_ADMIN`.

Pour plus d'informations, consultez la section Administrateur délégué pour MGN dans le Guide de l'utilisateur de MGN.

Rôles IAM créés lors de la configuration du connecteur

Lors de la configuration du connecteur, AWS Transform crée le rôle IAM suivant dans votre compte cible :

- `AWSTransform-Connector-role-`— Créé lorsque vous configurez le connecteur de compte cible, dans le compte de gestion ou le compte d'administrateur délégué de votre AWS organisation. Ce rôle permet à AWS Transform de se connecter à votre compte cible et d'agir en votre nom pour exécuter les opérations de migration.

Configuration du connecteur de compte cible

> **Important**
>
> Lors de la configuration du connecteur, un compartiment Amazon S3 est créé dans votre cible Compte AWS. Ce compartiment n'appliquera pas HTTPS-only access (`SecureTransport`) par défaut. Si vous souhaitez que la politique des compartiments inclue le transport sécurisé, vous devez la mettre à jour vous-même. Pour plus d'informations, consultez la section Bonnes pratiques en matière de sécurité pour Amazon S3.

Pour utiliser un connecteur de compte cible existant

1. Dans le volet Job Plan, développez Choisir un compte cible, puis choisissez Créer ou sélectionner des connecteurs.
2. Dans l'onglet Collaboration, sélectionnez un connecteur existant, puis choisissez Utiliser le connecteur. Si un connecteur n'est pas disponible, sa version n'est pas compatible avec le type de tâche que vous avez sélectionné.

> **Important**
>
> Si vous spécifiez un connecteur Région AWS dont la cible est différente de la région de AWS transformation, AWS Transform transfèrera vos données Régions AWS.

3. Sélectionnez Continuer.

Pour créer un nouveau connecteur

1. Dans le volet Job Plan, développez Connect target account, puis choisissez Create ou sélectionnez Connectors.
2. Spécifiez le Compte AWS et Région AWS pour votre cible, puis choisissez Suivant.

> **Important**
>
> Si la cible est Région AWS différente de celle de la découverte Région AWS, AWS Transform transfèrera vos données Régions AWS.

3. Choisissez si vous souhaitez utiliser des clés gérées par Amazon S3 pour le chiffrement. Si vous spécifiez votre propre clé KMS, vous pouvez utiliser la politique de clé par défaut ou une politique moins permissive. Pour plus d'informations sur la création d'une clé KMS, voir Créer une clé KMS dans le Guide du AWS Key Management Service développeur.

   AWS Transform utilise cette `kms:DescribeKey` autorisation pour vérifier l'existence de la clé `kms:GenerateDataKey` et `kms:Decrypt` pour chiffrer et déchiffrer les données des tâches dans le compartiment Amazon S3. Pour plus d'informations, consultez la section Réduire le coût SSE-KMS d'Amazon S3 Bucket Keys.
4. Sélectionnez Continuer.
5. Copiez le lien de vérification, partagez-le avec un administrateur de la cible Compte AWS et demandez-lui d'approuver la demande de connexion.
6. Une fois que l'administrateur a approuvé la demande, sélectionnez le connecteur nouvellement créé dans la liste et choisissez Utiliser le connecteur.
7. Choisissez Envoyer vers AWS Transform.

Si vous envisagez de modifier le AWS Transform MGN modèle pour activer les actions après le lancement, ajoutez l'autorisation suivante au rôle de connecteur cible. Cette déclaration de politique JSON accorde l'`iam:PassRole`autorisation pour le rôle d'actions post-lancement. Le nom du rôle se trouve dans l'onglet Collaboration une fois le connecteur créé. Pour plus d'informations sur l'ajout d'autorisations à un rôle, consultez la section Mettre à jour les autorisations pour un rôle dans le Guide de l'utilisateur IAM.

```
{
      "Sid": "MGNPostLaunchActions",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::target-account-ID:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
}
```

Régions cibles prises en charge

Une région cible de migration est l' Région AWS endroit où les ressources migrées sont déployées, y compris les zones d'atterrissage, l'infrastructure réseau et le réhébergement des serveurs. Lorsque vous créez le connecteur, spécifiez une cible Région AWS. Vous pouvez utiliser l'une des options suivantes Régions AWS :

- USA Est (Virginie du Nord)
- USA Est (Ohio)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Taipei)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Tokyo)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Osaka)

- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Melbourne)
- Asie-Pacifique (Malaisie)
- Asie-Pacifique (Nouvelle Zélande)
- Asie-Pacifique (Thaïlande)
- Canada (Centre)
- Canada-Ouest (Calgary)
- Europe (Francfort)
- Europe (Zurich)
- Europe (Irlande)
- Europe (Londres)
- Europe (Paris)
- Europe (Stockholm)
- Europe (Milan)
- Europe (Espagne)
- Israël (Tel Aviv)
- Mexique (Centre)
- Amérique du Sud (São Paulo)

Important

Si vous spécifiez une cible Région AWS différente de la AWS Transform Région AWS, certaines de vos données sont transférées Régions AWS.
Notez que les données de réplication de votre serveur sont transmises directement de votre environnement source à votre compte et à votre région cibles.

Construire une zone d'atterrissage

AWS Transform vous guide dans la conception et le déploiement d'une zone AWS d'atterrissage dans le cadre de votre projet de migration. Une zone d'accueil est un AWS environnement multi-comptes qui sert de base à vos charges de travail. Les limites organisationnelles, les contrôles de gouvernance et la structure des comptes sont en place avant l'arrivée de toute charge de travail. AWS Transform analyse votre inventaire de migration et vos exigences commerciales pour recommander une unité organisationnelle (OU) et une structure de compte, appliquer les politiques de contrôle des services (SCP) recommandées et générer le and/or déploiement de l'infrastructure sous forme de code (IaC). Ce qui nécessite généralement des semaines de planification et de configuration manuelles, peut être réalisé par AWS Transform en une seule conversation.

L'agent de zone d'atterrissage automatise deux phases :

- Configuration de base — Établissez la structure de base de la zone d'atterrissage : tour de AWS contrôle, unités d'organisation fondamentales et comptes principaux.
- Conception des comptes de charge de travail : concevez et créez des unités d'organisation et des comptes de charge de travail en fonction de vos vagues de migration, de vos unités commerciales et de vos exigences en matière de séparation des environnements.

AWS Transform prend en charge à la fois les environnements entièrement nouveaux (aucune zone d'atterrissage existante) et les environnements désaffectés (unités d'organisation existantes et comptes déjà déployés). Dans les scénarios de friche industrielle, AWS Transform détecte la structure existante de votre organisation et recommande uniquement les modifications nécessaires pour combler les lacunes par rapport aux AWS meilleures pratiques, sans que vous ayez à repartir de zéro ou à effectuer une analyse manuelle des lacunes.

Configuration du connecteur

Avant que l'agent puisse provisionner des ressources, vous devez le connecter au compte de gestion de votre organisation. L'agent de zone d'atterrissage a besoin d'un Compte AWS connecteur cible autorisé à :

- Configurer la tour AWS de contrôle
- Création d'unités organisationnelles et de comptes
- Configuration des politiques de contrôle des services (SCP)

Lorsque vous approuvez la demande de connecteur, vous accordez des autorisations AWS Transform pour :

- Fournir et gérer l'infrastructure de la zone d'atterrissage dans la cible Compte AWS et la région. Cela inclut les autorisations pour les éléments suivants, limitées aux ressources étiquetées avec `CreatedBy:AWSTransform` et par, le cas `ATWorkspace:{workspace-id}` échéant :
  - Opérations sur les compartiments S3 (création, lecture, écriture, suppression) pour les compartiments commençant par `transform-vmware-landing-zone-`
  - CloudFormation déploiements de piles et gestion des ensembles de modifications pour les piles de zones d'atterrissage
  - AWS Opérations de la tour de contrôle (gestion des zones d'atterrissage, activation des lignes de base et des contrôles)
  - AWSGestion des organisations (création et gestion d'unités organisationnelles, création de comptes et transfert de comptes)
  - Gestion de la politique de contrôle des services (SCP) via AWS Control Tower
  - AWSProvisionnement et gestion des artefacts du catalogue de services

Lorsque vous créez le connecteur, vous spécifiez une cible Région AWS. Cette région doit être la même que la région de votre tour de contrôle d'origine. Pour plus d'informations sur les régions de la tour de contrôle, consultez Régions AWS Comment utiliser la tour AWS de contrôle.

Au début de la configuration de la zone d'atterrissage, AWS Transform récupère la configuration de votre connecteur et présente l'ID du compte de gestion de AWS l'organisation et la région cible pour confirmation. Pour de plus amples informations, veuillez consulter the section called “Connecteurs”.

> **Important**
>
> Dépendance de la région IAM Identity Center — AWS Transform nécessite AWS IAM Identity Center (IAM Identity Center), ce qui signifie que la région de votre connecteur doit correspondre à la fois à la région d'origine de votre AWS Control Tower et à votre région IAM Identity Center. Si IAM Identity Center est déjà configuré dans votre organisation, l'initialisation AWS de la tour de contrôle échouera si le connecteur cible une autre région. Pour plus d'informations, consultez la section Considérations destinées aux clients d'IAM Identity Center dans le Guide de l'utilisateur AWS de Control Tower.

Configuration de la fondation

La phase de configuration des fondations établit l'infrastructure de base de la zone d'atterrissage à l'aide AWS de la tour de contrôle. Lorsque AWS Control Tower configure une zone d'atterrissage, elle fournit automatiquement un ensemble de ressources gérées dans votre compte de gestion qui constituent le fondement de la gouvernance pour AWS l'ensemble de votre organisation :

- Root : le parent de niveau supérieur qui contient toutes les unités d'organisation de votre zone d'atterrissage.
- Security OU — Créé automatiquement par Control Tower. Contient deux comptes partagés : le compte Log Archive (journalisation centralisée et immuable de toutes les activités d' AWS API et des modifications de ressources au sein de votre organisation) et le compte Audit (accès en lecture seule à tous les comptes à des fins de contrôle de sécurité et de conformité). Ces comptes ne peuvent pas être renommés ni remplacés après la configuration initiale.
- Contrôles obligatoires (garde-fous) — Control Tower applique automatiquement des contrôles préventifs et de détection dans l'ensemble de votre organisation afin de faire appliquer les politiques de gouvernance de base. Ils ne peuvent pas être désactivés.
- Répertoire IAM Identity Center : Control Tower crée un annuaire natif du cloud avec des groupes préconfigurés et un accès par authentification unique pour les utilisateurs de votre zone de destination. Pour plus d'informations, consultez AWS IAM Identity Center.

Control Tower les utilise CloudFormation StackSets pour déployer et gérer ces ressources de manière cohérente sur tous les comptes et toutes les régions de votre organisation. Vous ne devez pas modifier ou supprimer les ressources gérées par Control Tower en dehors des méthodes prises en charge, car cela peut entraîner le passage de votre zone d'atterrissage à un état inconnu.

Convention relative aux comptes de messagerie

AWS nécessite une adresse e-mail unique pour chaque compte. Ces e-mails reçoivent des notifications importantes concernant le compte. AWS Transform utilise l'adressage Plus pour générer des e-mails de compte uniques à partir d'une seule boîte aux lettres.

Format : `prefix+account-name@domain`

Vous fournissez un préfixe (par exemple`aws-admin`) et un domaine (par exemple,`acme.com`), et AWS Transform extrait automatiquement tous les e-mails du compte. Par exemple :

- Compte d'audit : `aws-admin+audit@acme.com`

- Compte Log Archive : `aws-admin+log-archive@acme.com`
- Compte Sandbox : `aws-admin+sandbox@acme.com`

Dans les scénarios de friche industrielle, AWS Transform inspecte les e-mails des comptes existants pour en déduire la convention d'adressage positive déjà utilisée et propose de continuer avec le même schéma.

Structure de fondation recommandée

Sur la base des AWS meilleures pratiques, AWS Transform recommande la structure d'organisation organisationnelle de base suivante. Vous pouvez le personnaliser avant de le créer.

UO	Objectif	Comptes
Sécurité	Enregistrement et surveillance centralisés des audits. L'isolation de ces services dans des comptes dédiés est conçue pour vous aider à séparer votre piste d'audit de celle des équipes chargées de la charge de travail.	Audit, archivage des journaux
Infrastructures	Réseau partagé (passerelle de transit, VPN), DNS et services communs. Il est recommandé de les centraliser afin de réduire les doublons et de donner à votre équipe réseau un endroit unique pour gérer la connectivité.	Aucun (créé vide)
Sandbox	Expérimentation par les développeurs en matière de limites de dépenses et d'accès restreint. Recommandé pour donner aux développeurs un espace pour expérimenter sans risquer les ressources de production.	Sandbox
Charges de travail	Contient la production et, éventuellement Non-Production, des sous-unités d'organisation réglementées. Les comptes de charge de travail sont conçus lors de la phase suivante	Aucun (créé vide)

UO	Objectif	Comptes
	en fonction de vos besoins en matière de migration.	

> **Note**
>
> L'unité d'organisation de sécurité avec comptes d'audit et d'archivage des journaux est créée dans le cadre de la configuration de base de la Control Tower. Les unités d'organisation Infrastructure, Sandbox et Workloads sont créées séparément une fois que vous avez confirmé la structure.

Dans les scénarios de friches industrielles, AWS Transform compare votre fondation existante à la structure recommandée et ne signale que les lacunes. Par exemple : « Votre fondation possède des unités d'organisation dédiées à la sécurité et à l'infrastructure, mais aucune unité d'organisation Sandbox. »

Politiques de contrôle des services

Les SCP sont des barrières d'autorisation au niveau de l'organisation qui définissent les autorisations maximales pour tous les comptes de votre organisation. AWS Ils n'accordent pas l'accès, mais définissent des limites que personne ne peut dépasser sur le compte, même les administrateurs du compte.

Dans le cadre du déploiement de la tour de contrôle, les garde-corps de référence sont appliqués automatiquement. AWS Transform recommande également des SCP supplémentaires conçus pour renforcer la posture de votre organisation. Elles sont basées sur les AWS meilleures pratiques pour une zone d'atterrissage minimale viable.

Les SCP peuvent être appliqués aux unités d'organisation Infrastructure, Sandbox et Workloads. L'unité d'organisation de sécurité est gérée par Control Tower et ne peut pas être ciblée par les SCP via cet outil.

> **Important**
>
> L'UO Security est une UO de fondation gérée par Control Tower. Vous ne pouvez pas y ajouter de comptes, de SCP ou de ressources via l'agent de zone d'atterrissage.

Dans les scénarios de friches industrielles, AWS Transform vérifie quels SCP sont déjà appliqués et ne recommande que ceux qui combleraient les lacunes.

Déploiement des fondations

Une fois la conception de base terminée, vous choisissez le mode de déploiement :

- Déployez pour moi : AWS Transform déploie les unités d'organisation, les comptes et les SCP de base dans votre AWS organisation.
- Je vais déployer moi-même : AWS Transform génère des artefacts d'infrastructure en tant que code (IaC) à télécharger dans le format de votre choix (voirthe section called “Formats IaC”).
- Concevez d'abord les comptes de charge de travail — Ignorez le déploiement et passez à la phase de conception des comptes de charge de travail. Vous pourrez tout déployer en même temps plus tard.

Initialisation de la tour de contrôle

Si AWS Transform détecte que AWS Control Tower n'est pas encore initialisée dans votre organisation, il fournit à l'utilisateur un lien vers la page de la console AWS Transform. La génération de l'opération dans le lien créera une CloudFormation pile pour démarrer Control Tower. Le processus créera cette pile dans la CloudFormation console pour votre région cible. Une fois la création de la pile terminée, AWS Transform poursuit le déploiement.

Conception du compte de charge de travail

Lors de la phase de conception du compte de charge de travail, AWS Transform conçoit l'unité d'organisation et la structure des comptes pour les charges de travail de vos applications en fonction de votre inventaire de migration, de vos exigences commerciales et de vos préférences de séparation des environnements.

Contexte de planification de la migration

AWS Transform extrait les données de la phase de planification de votre migration, notamment les plans Wave, les mappages serveur-application et le contexte partagé. Si des données de planification de la migration sont disponibles, AWS Transform affiche un résumé et vous demande de le confirmer ou de le modifier. Si aucune donnée de planification de migration n'est disponible, AWS Transform pose directement des questions de découverte.

Découverte

AWS Transform pose des questions pour comprendre vos exigences en matière de charge de travail. Vous pouvez ignorer n'importe quelle question. Les sujets suivants sont notamment abordés :

- Nombre d'unités commerciales ou d'équipes utilisant AWS
- L'industrie et tous les cadres applicables (HIPAA, SOC2 PCI-DSS, FedRAMP)
- Si les charges de travail gèrent des données sensibles (PII, PHI, financières)
- Préférences de séparation des environnements (dev/test/staging/prod en tant que comptes séparés ou partagés)
- Exigences relatives à l'isolation des charges
- Les applications métier et leurs objectifs
- Regroupement de serveurs en applications
- Besoins en matière de suivi et d'allocation des coûts (par unité commerciale, projet, environnement)
- Croissance attendue au cours des 12 à 24 prochains mois
- Stratégie de compte préférée (application unique par compte, groupée ou basée sur l'environnement)

Structure de charge de travail proposée

Sur la base de vos réponses et des données de planification de la migration, AWS Transform propose une unité d'organisation et une structure de comptes dans le cadre de l'unité d'organisation Workloads. La proposition inclut le raisonnement qui sous-tend chaque décision de conception.

AWS Transform suit les principes de conception suivants :

- Tous les serveurs d'une vague de migration sont dirigés vers le même compte. Les vagues ne peuvent pas être réparties entre les comptes. Il s'agit d'une limitation du réhôte lors de l'exécution d'une vague.
- Si vous demandez des environnements isolés, AWS Transform crée un Workloads/Production Workloads/Non-Production sous-UO.
- Si des frameworks applicables sont identifiés, AWS Transform crée un Workloads/Regulated Workloads/Standard sous-UO.

- Si plusieurs unités commerciales nécessitent une gouvernance différente, AWS Transform crée des unités opérationnelles spécifiques à chaque unité commerciale dans le cadre des charges de travail.
- Les applications contenant des données critiques ou sensibles bénéficient d'une seule application par compte. Dans ce cas, il se peut que l'on vous demande de modifier votre plan de vagues.
- Les applications étroitement couplées avec des dépendances partagées sont regroupées dans un seul compte.

Chaque compte proposé comprend : le nom, l'objectif, l'unité d'organisation cible et l'unité commerciale. AWS La transformation indique la convention de dénomination utilisée (par exemple,`<business-unit>-<environment>-<workload>`).

Vous pouvez revoir et modifier la structure proposée avant que AWS Transform n'applique les modifications. Après avoir postulé, vous pouvez recommencer, en apportant des modifications supplémentaires jusqu'à ce que vous soyez satisfait.

Configuration de la charge de travail SCP

Une fois la structure de charge de travail créée, AWS Transform présente les SCP disponibles et vous demande si vous souhaitez en appliquer à vos unités d'organisation de charge de travail. Vous sélectionnez les SCP à appliquer et à quelles UO. AWS Transform applique les SCP et affiche l'arbre d'organisation mis à jour avec un tableau récapitulatif des SCP.

Déploiement des charges

Une fois la conception de la charge de travail terminée, vous choisissez le mode de déploiement :

- Déployez pour moi : AWS Transform déploie les unités d'organisation, les comptes et les SCP de la charge de travail dans votre AWS organisation.
- Je vais le déployer moi-même. AWS Transform génère des artefacts IaC à télécharger dans le format de votre choix (voirthe section called “Formats IaC”).

Formats IaC

Lorsque vous choisissez l'auto-déploiement, AWS Transform génère des artefacts Infrastructure as Code dans les formats suivants :

- Cloud Development Kit AWS (AWS CDK)— TypeScript projet de déploiement d'une infrastructure programmatique.
- HashiCorp Terraform — Génère des modèles HashiCorp de langage de configuration (HCL) pour gérer les ressources de la zone d'atterrissage.
- Landing Zone Accelerator (LZA) — Fichiers de configuration YAML basés sur la version 1.1.0 de LZA Universal Configuration. Ces modèles prêts à l'emploi fonctionnent avec le Landing Zone Accelerator AWS pour créer des environnements AWS multi-comptes. Les fichiers générés incluent des paramètres préconfigurés pour la gouvernance, la structure organisationnelle et la mise en réseau qui correspondent aux AWS meilleures pratiques. Pour en savoir plus, consultez la section Configuration universelle LZA.

> **Note**
>
> Lors d'un déploiement via le pipeline Landing Zone Accelerator (LZA), votre compte AWS Transform et votre installation LZA doivent se trouver dans la même AWS organisation. Le déploiement échouera en cas de non-concordance entre les identifiants d'organisations utilisés dans AWS Transform et LZA. Pour savoir comment configurer votre installation LZA à l'aide des organisations, consultez la section Installation basée sur AWS les organisations.

Une fois que vous avez sélectionné un format, AWS Transform génère les artefacts et les rend disponibles au téléchargement.

Pour vérifier que le fichier téléchargé n'a pas été endommagé ou altéré, générez et téléchargez une somme de contrôle, puis comparez-la à un hachage généré localement en utilisant :

```
openssl dgst -sha256 -binary <file.zip> | base64
```

Processus d'approbation des déploiements

Les demandes de déploiement de zones d'atterrissage nécessitent une approbation explicite avant d'être exécutées. Lorsque vous soumettez une demande de déploiement, celle-ci est automatiquement acheminée vers des approbateurs autorisés via l'onglet AWS Transformer les approbations.

Les approbateurs examinent les CloudFormation modèles et les configurations des zones d'atterrissage. Seuls les utilisateurs ayant le rôle d'administrateur dans AWS Transform peuvent

approuver les demandes de déploiement. Chaque soumission déclenche un nouveau cycle de révision, et les déploiements n'ont lieu qu'après réception de la confirmation.

Si un approbateur refuse votre demande, contactez-le directement pour discuter des modifications nécessaires. Le système assure le suivi de toutes les décisions d'approbation à des fins d'audit et tient à jour l'historique des déploiements.

Tag : ressources relatives à la zone d'atterrissage

AWS Transform étiquette automatiquement toutes les ressources générées `"CreatedBy": "AWSTransform"` avec des identifiants de définition et d'exécution à des fins de suivi.

Tags automatiques

Toutes les ressources de la zone d'atterrissage reçoivent les balises suivantes :

- `CreatedBy`— Transformation AWS
- `ATWorkspace`— Identifiant du poste de travail

> **Note**
>
> Si votre migration fait partie du programme d'accélération de la AWS migration (MAP 2.0), vous pouvez inclure la balise MAP requise : Clé : `map-migrated` Valeur : `migMPE_ID` (où MPE_ID est l'identifiant d'évaluation de votre portefeuille de migration). La balise MAP est demandée lors de la phase de configuration du connecteur. AWS Transform applique ces balises lors du déploiement de la zone d'atterrissage.

Inverser les modifications

Seuls les éléments non déployés peuvent être retirés. Une fois qu'une unité d'organisation ou un compte est déployé, il ne peut pas être supprimé par l'intermédiaire de l'agent de zone d'atterrissage.

Lorsque vous supprimez des éléments, l'ordre est important : vous devez retirer les enfants avant les parents :

1. Supprimez d'abord les comptes (par e-mail).
2. Supprimez les SCP des UO.

3. Supprimer des unités d'organisation enfants : une unité d'organisation ne peut pas être supprimée si elle possède toujours des comptes ou des unités d'organisation imbriquées.

Ressources connexes

- the section called “Connecter la cible Compte AWS s et régions”
- the section called “Migrez votre réseau vers AWS”
- AWS Guide de l'utilisateur de Control Tower
- AWS Guide de l'utilisateur pour les organisations
- AWS Guide de l'utilisateur d'IAM Identity Center
- CloudFormation Guide de l'utilisateur
- Accélérateur de zone d'atterrissage activé AWS
- AWS Well-Architected Cadre
- AWS Directives prescriptives : Construction de zones d'atterrissage

Migrez votre réseau vers AWS

Avec AWS Transform, vous pouvez migrer votre réseau AWS en une fraction du temps nécessaire à la conception et au déploiement manuels. AWS Transform utilise un AI-powered agent pour traduire la configuration de votre environnement source en ressources AWS réseau prêtes pour la production, notamment des VPC, des sous-réseaux, des groupes de sécurité, des passerelles NAT, des passerelles de transit, des adresses IP élastiques, des itinéraires et des tables de routage. Vous passez en revue et modifiez la configuration réseau générée via une interface conversationnelle avant le déploiement. Vous pouvez déployer directement avec AWS Transform ou choisir l'auto-déploiement et recevoir l'infrastructure sous forme de code (IaC) dans le format de votre choix : Cloud Development Kit AWS (AWS CDK) Landing Zone Accelerator (LZA) ou HashiCorp Terraform.

L'agent AWS Transform vous guide à travers les étapes suivantes, en gérant l'analyse et la génération pendant que vous prenez les décisions :

1. Téléchargez votre fichier réseau source.
2. Téléchargez des fichiers de configuration supplémentaires (facultatif, pour les environnements RVTools).
3. Sélectionnez une topologie de réseau.

4. Sélectionnez une stratégie de mappage des groupes de sécurité.
5. Passez en revue et optimisez votre réseau.
6. Générez un diagramme de réseau (facultatif).
7. Configurez le balisage des ressources.
8. Déployez votre réseau.

> **Note**
>
> Pour les déploiements multicomptes, vous devez configurer les rôles IAM entre comptes et l'accès sécurisé pour les AWS organisations avant de commencer la migration du réseau. Pour plus d'informations sur les types de migration, consultezthe section called "Étape 1 : Sélection du type de migration".

Étape 1 : mappage du réseau source

AWS Transform génère une infrastructure réseau cible à partir d'une grande variété de fichiers de configuration réseau sources. Téléchargez un ou plusieurs fichiers de configuration depuis votre environnement source et AWS Transform utilise les informations pour générer des réseaux cibles, notamment des VPC Amazon, des sous-réseaux et des groupes de sécurité. Bien que AWS Transform ne génère pas de ressources de pare-feu ou d'équilibreur de charge, la configuration de ces éléments de réseau peut être utilisée comme entrée pour générer des réseaux cibles.

AWS Transform accepte les fichiers de configuration provenant des types de sources suivants :

- Réseaux définis par logiciel (SDN) : Import/Export pour la virtualisation du réseau VMware NSX ou la configuration Cisco ACI pour l'infrastructure centrée sur les applications Cisco.
- Réseaux VMware vSphere : https://www.dell.com/en-us/shop/vmware/sl/rvtools RVTools. Lorsque vous utilisez des fichiers RVTools, AWS Transform génère uniquement des configurations Amazon VPC. Les configurations des groupes de sécurité nécessitent des informations supplémentaires provenant du pare-feu ou des fichiers réseau définis par logiciel. Pour plus d'informations sur la génération de groupes de sécurité à partir de fichiers supplémentaires, consultez la section Fichiers de configuration supplémentaires.
- Réseaux basés sur les données de configuration du pare-feu : exportez des fichiers depuis Palo Alto Networks Firewall, Fortinet FortiGate Firewall ou Cisco ACI. Pour plus d'informations sur les

versions prises en charge et les instructions d'extraction, consultez la section Extraction du fichier de configuration.

- Réseaux hybrides qui exécutent à la fois des charges de travail VMware et non VMware : outil de découverte AWS Transform ou ModelizeIt.
- Autres types de fichiers : AWS Transform accepte également d'autres fichiers de configuration réseau, tels que les configurations Checkpoint et F5. Si votre fichier de configuration n'est pas l'un des formats répertoriés ci-dessus, AWS Transform le convertit automatiquement et l'utilise pour générer des réseaux cibles. Cette conversion peut prendre jusqu'à deux heures en fonction de la taille et de la complexité du fichier.

> **Note**
>
> La taille maximale de fichier réseau source prise en charge est de 70 Mo.

> **Note**
>
> Pour permettre la suppression des règles de groupe de sécurité obsolètes lors de l'examen du réseau, soumettez les données de trafic réseau observées à partir de l'outil de découverte AWS Transform ou de ModelizeIt en même temps que votre configuration réseau source. Pour plus d'informations, consultez la section Recommandations de réseau guidées.

> **Warning**
>
> Téléchargez RVTools uniquement depuis le site officiel de Dell à https://www.dell.com/en-us/shop/vmware/sl/rvtools l'adresse. Ne téléchargez pas RVTools à partir de sources non officielles.

Chaque segment de réseau source est mappé à son propre VPC distinct. La segmentation du réseau varie selon le type de source :

- Réseau virtuel : AWS transformez les groupes de machines virtuelles par vSwitch et réseau local virtuel (VLAN). Les VLAN peuvent apparaître sous plusieurs commutateurs virtuels (à l'exception du VLAN 0).

- Réseaux NSX : AWS transformez les segments du réseau en fonction des Tier-1 routeurs, en regroupant les routeurs et en collectant leurs segments.

Étape 2 : fichiers de configuration supplémentaires

Pour les environnements sources RVTools, vous pouvez éventuellement télécharger des fichiers de configuration supplémentaires pour permettre la génération de groupes de sécurité. Si vous ne chargez pas de fichiers de configuration supplémentaires, aucun groupe de sécurité n'est généré pour votre RVTools-based migration.

AWS Transform prend en charge les types de fichiers de configuration supplémentaires suivants. Vous ne pouvez télécharger qu'un seul fichier de configuration à partir d'une seule plateforme.

- L'infrastructure centrée sur les applications (ACI) de Cisco fournit des configurations de politique réseau.
- Palo Alto Networks fournit des politiques de sécurité en matière de pare-feu.
- Fortinet FortiGate fournit des politiques de sécurité en matière de pare-feu.

Lorsque vous chargez un pare-feu ou un fichier Cisco ACI, AWS Transform génère une infrastructure réseau et des groupes de sécurité. Lorsque vous chargez un fichier RVTools seul, AWS Transform génère uniquement une infrastructure réseau.

Pour plus d'informations sur les versions prises en charge et les instructions d'extraction, consultez la section Extraction du fichier de configuration.

Étape 3 : topologies du réseau

Au cours de l'étape de définition du réseau, vous sélectionnez une topologie de réseau. Vous pouvez choisir la topologie VPC isolés ou la topologie Hub and Spoke.

VPC isolés

Qu'est-ce qui est déployé

Les VPC isolés sont des environnements réseau indépendants qui fonctionnent comme des unités distinctes au sein AWS de ceux-ci. Vos VPC sont complètement isolés, sans aucune voie de communication intégrée entre eux. Cette séparation fournit le plus haut niveau de protection des limites du réseau.

AWS Transform crée les ressources suivantes :

- Un VPC dédié pour chaque segment de réseau source détecté.
- Sous-réseaux privés en fonction de la configuration de votre réseau source.
- Groupes de sécurité (si vous avez fourni des fichiers de configuration de pare-feu ou SDN).

Terminez votre configuration

AWS Transform déploie l'infrastructure réseau principale pour vous. Vous terminez la configuration finale de connectivité et de sécurité pour répondre aux exigences de votre organisation.

Pour activer l'accès à Internet pour un VPC isolé, procédez comme suit :

1. Créez une passerelle Internet et connectez-la au VPC.
2. Créez des sous-réseaux publics dans chaque zone de disponibilité où vous avez besoin d'un accès Internet. Ajoutez un itinéraire pour `0.0.0.0/0` pointer vers la passerelle Internet. Pour plus d'informations sur la configuration des sous-réseaux, consultez Sous-réseaux pour votre VPC.
3. Créez des passerelles NAT dans les sous-réseaux publics (une par AZ pour une haute disponibilité). Allouez une adresse IP élastique pour chaque passerelle NAT.
4. Mettez à jour les tables de routage de vos sous-réseaux privés. Ajoutez une route pour `0.0.0.0/0` pointer vers la passerelle NAT dans la même zone de disponibilité.
5. Passez en revue les règles de votre groupe de sécurité. Assurez-vous que les règles sortantes autorisent le trafic dont vos charges de travail ont besoin (HTTPS, DNS, etc.).

Pour VPC-to-VPC la communication, configurez le peering VPC ou une passerelle de transit et mettez à jour les tables de routage de chaque VPC pour acheminer le trafic vers la connexion d'appairage ou la pièce jointe TGW.

Hub et rayon

Dans ce modèle, une passerelle de AWS transit fait office de hub central qui connecte plusieurs VPC de charge de travail (les rayons).

Qu'est-ce qui est déployé

AWS Transform crée les ressources suivantes :

- VPC en étoile : un VPC par segment de réseau source détecté, avec des sous-réseaux privés et une pièce jointe Transit Gateway.
- VPC d'inspection : héberge votre dispositif de pare-feu pour l'inspection du trafic. Tout le trafic inter-VPC est acheminé via ce VPC. La pièce jointe Transit Gateway utilise le mode appliance, un paramètre qui garantit que le trafic circule de manière symétrique via la même appliance dans les deux sens d'une connexion.
- VPC entrant : gère le trafic entrant dans votre réseau depuis l'Internet public (entrant nord-sud). Comprend une passerelle Internet et des sous-réseaux publics dans plusieurs zones de disponibilité.
- VPC sortant : gère le trafic sortant de votre réseau vers l'Internet public (trafic sortant nord-sud). Comprend une passerelle Internet, des passerelles NAT avec des adresses IP élastiques dans chaque zone de disponibilité pour une haute disponibilité, et des sous-réseaux privés pour la pièce jointe Transit Gateway.
- Tables de routage de Transit Gateway : deux tables de routage orientent le trafic via le VPC d'inspection. La table Non inspectée est associée aux VPC en étoile, aux VPC entrants et aux VPC sortants. Il achemine tout le trafic (0.0.0. 0/0) à la pièce jointe Inspection VPC et constitue la table de routage d'association par défaut. Le tableau Inspecté est associé au VPC d'inspection. Il contient les routes propagées depuis tous les VPC en étoile et constitue la table de routage de propagation par défaut.

Pour les déploiements multi-comptes, le Transit Gateway est partagé entre les comptes via AWS Resource Access Manager (RAM).

Flux de trafic

Tout le trafic inter-VPC suit le chemin suivant :

1. Le trafic provenant d'un VPC en étoile est envoyé à la passerelle de transit (route par défaut 0.0.0). 0/0).
2. La table de routage Non inspecté achemine le trafic vers le VPC d'inspection.
3. Votre pare-feu du VPC d'inspection inspecte le trafic et le retransmet à la passerelle de transit.
4. La table de routage inspectée achemine le trafic vers le VPC en étoile de destination à l'aide d'itinéraires propagés.

Pour le trafic Internet sortant, la table de routage inspectée achemine le trafic vers le VPC sortant. Les passerelles NAT traduisent les adresses IP privées avant que le trafic ne soit transféré vers la

passerelle Internet. La table de routage publique des VPC sortants inclut des itinéraires spécifiques pour chaque plage de Inter-Domain routage sans classe (CIDR) VPC à rayons vers la passerelle de transit. Ces itinéraires permettent au trafic de retour d'atteindre le VPC à rayons correct.

Le trafic Internet entrant entre par la passerelle Internet du VPC entrant et suit le même chemin d'inspection pour atteindre les VPC en étoile.

Terminez votre configuration

AWS Transform déploie l'infrastructure réseau principale pour vous, y compris la passerelle de transit, les VPC en étoile et le routage du trafic. Vous terminez la configuration du pare-feu et du service entrant en fonction des exigences de sécurité de votre organisation.

> **Note**
>
> Par défaut, le trafic inter-VPC passe par le VPC d'inspection sans inspection. Vous devez déployer un pare-feu pour permettre l'inspection du trafic.

Déployez un pare-feu : créez des sous-réseaux supplémentaires dans le VPC d'inspection pour les points de terminaison du pare-feu. AWS Transform crée des sous-réseaux pour la pièce jointe Transit Gateway uniquement. Acheminez le trafic depuis les sous-réseaux de pièces jointes TGW vers les points de terminaison du pare-feu, et depuis les sous-réseaux du pare-feu vers la passerelle de transit. Vous pouvez déployer un pare-feu AWS réseau ou une appliance tierce. Pour plus d'informations sur le déploiement d'un pare-feu avec une passerelle de transit, voir Création d'un pare-feu avec une passerelle de transit.

Vérifiez la connectivité : après avoir déployé le pare-feu, testez l'accès Internet sortant à partir d'une instance VPC en étoile (par exemple). `curl https://aws.amazon.com` Vous pouvez utiliser Reachability Analyzer pour résoudre les problèmes de connectivité.

Configurer les services entrants : pour héberger des services destinés au public, déployez un équilibreur de charge d'application ou un équilibreur de charge réseau dans les sous-réseaux publics du VPC entrant. Configurez des groupes cibles qui pointent vers des instances de vos VPC satellites via la passerelle de transit et vérifiez que la table de routage inspectée contient des itinéraires de retour vers le VPC entrant.

Si vous souhaitez un contrôle précis de la communication entre les VPC, choisissez l'option VPC isolés et modifiez le réseau généré pour créer les chemins de communication spécifiques dont vous avez besoin.

Étape 4 : mappage des groupes de sécurité

Choisissez la manière dont vos politiques de sécurité des sources sont traduites en groupes AWS de sécurité. AWS Transform crée des groupes de sécurité en fonction des configurations de votre environnement source. Les politiques de sécurité, les règles de politique de sécurité, les politiques de passerelle et les règles de politique de passerelle sont converties en groupes de sécurité.

> **Important**
>
> AWS Transform crée des groupes de sécurité de son mieux pour correspondre à votre environnement source. Passez en revue et modifiez les groupes de sécurité générés pour vous assurer qu'ils répondent aux besoins et aux politiques de sécurité de votre entreprise.

Référencement des groupes de sécurité

Lorsque des groupes de sécurité sont générés, AWS Transform utilise le référencement des groupes de sécurité lorsqu'il est pris en charge. Le référencement des groupes de sécurité définit les règles de sécurité en fonction d'un autre identifiant de groupe de sécurité plutôt que de plages d'adresses IP spécifiques (blocs CIDR). Cette approche fournit des configurations de sécurité plus flexibles et plus faciles à gérer.

Les règles de votre groupe de sécurité peuvent uniquement faire référence à d'autres groupes de sécurité au sein du même VPC ou d'un VPC connecté dans la même région. Cross-account les références sont également prises en charge. Vous ne pouvez pas référencer un groupe de sécurité dans un VPC non connecté ou dans plusieurs régions. Pour les VPC connectés, seules les règles entrantes prennent en charge les références de groupes de sécurité inter-VPC. Les règles sortantes doivent utiliser des CIDR-based règles. La façon dont AWS Transform crée les règles des groupes de sécurité dépend de la topologie de réseau que vous avez choisie :

- Hub and Spoke : Transit Gateway fournit une connectivité réseau entre les VPC. AWS Transform utilise le référencement à la fois pour les règles internes au VPC et pour les règles d'entrée croisée. VPC/cross-account Cross-VPC/cross-account les règles de sortie (sortante) utilisent CIDR-based des règles.
- VPC isolés : vos VPC ne disposent d'aucune connectivité réseau entre eux. AWS Transform utilise le référencement pour les règles internes au VPC uniquement. Toutes les règles inter-VPC et inter-comptes utilisent des règles. CIDR-based

CIDR-based les règles sont également utilisées lorsque les configurations de source ne sont pas symétriques.

Choisissez l'une des stratégies de mappage des groupes de sécurité suivantes :

- MAP : traduit les règles de sécurité de votre environnement source en groupes et règles de AWS sécurité. Utilisez cette option pour les migrations utilisant un adressage IP statique.
- MAP_DHCP (Translate with DHCP support) : traduit les règles de sécurité de votre environnement source avec une compatibilité DHCP. Le DHCP attribue des adresses IP de manière dynamique à partir de la plage d'adresses CIDR du sous-réseau. Par conséquent, les règles de sortie inter-VPC sont étendues pour correspondre au CIDR du sous-réseau de destination complet. Un CIDR plus étroit bloquerait les DHCP-assigned adresses IP qui se situent en dehors de cette plage. Passez en revue ces règles après la migration.

  Utilisez cette option pour la prise en charge DHCP avec la communication entre VPC Transit Gateway. Fonctionne également avec les adresses IP statiques, mais peut produire des règles plus étendues que MAP.
- SKIP : ne traduit pas les règles de sécurité. Configurez les groupes AWS de sécurité manuellement après la migration. Fonctionne à la fois avec les environnements IP statiques et DHCP. Pour les environnements sources RVTools sans fichiers de configuration supplémentaires, AWS Transform utilise automatiquement SKIP.

> **Note**
>
> Votre stratégie de mappage détermine vos options d'attribution IP. MAP ne prend en charge que les adresses IP statiques. MAP_DHCP et SKIP prennent en charge à la fois le mode statique et le DHCP.

Approches de migration IP

Vous avez deux choix de configuration réseau pour votre migration :

Sélection de la plage de réseau

- Conserver les plages existantes (conservation des plages d'adresses IP) : Conservez les plages d'adresses IP d'origine pendant la migration. Idéal pour les migrations dans le cadre desquelles vous déplacez des applications AWS sans les modifier (lift-and-shift), en particulier pour les

applications héritées dont les dépendances IP sont codées en dur ou dont les règles de pare-feu sont déjà en vigueur.

- Mise à jour vers de nouvelles plages IP (mise à jour du CIDR) : vous pouvez modifier chaque plage d'adresses CIDR VPC pendant la migration, et AWS Transform propage automatiquement les modifications aux sous-réseaux, aux tables de routage et aux groupes de sécurité.

Attribution d'adresses IP

- Adresses IP fixes (statiques) : AWS Transform attribue des adresses IP statiques en fonction du CIDR. C'est la solution idéale pour les applications qui nécessitent un comportement réseau prévisible, une gestion DNS ou un contrôle IP-based d'accès. Les adresses IP persistent lors des redémarrages d'instance via les interfaces réseau élastiques (ENI), qui sont des cartes réseau virtuelles connectées à vos instances.
- Attribution dynamique d'adresses IP (AWS DHCP) : attribuez automatiquement des adresses IP à partir de pools de sous-réseaux au lancement de l'instance. Idéal pour les applications conçues pour s'exécuter dans le cloud et les charges de travail à dimensionnement automatique. Réduit les frais opérationnels mais oblige les applications à utiliser le DNS ou la découverte de services.

Vous pouvez combiner l'une ou l'autre sélection de plage avec l'une ou l'autre des méthodes d'attribution IP.

> **Note**
>
> La stratégie d'attribution des adresses IP est définie au niveau de la vague. Vous pouvez attribuer différentes stratégies à des serveurs spécifiques en personnalisant le fichier wave. Par exemple, si vous avez choisi une approche d'adresse IP statique pour la vague mais que vous souhaitez attribuer une approche dynamique à un serveur spécifique, vous devez utiliser la méthode `[RESET_VALUE]` décrite dans la section Modification de votre configuration dans le guide de l'utilisateur MGN.

Étape 5 : Passez en revue et optimisez votre réseau

Une fois que AWS Transform a généré la configuration de votre réseau cible, vous pouvez examiner les segments de réseau locaux qui ont convergé vers l' AWS infrastructure. Utilisez l'interface visuelle pour passer en revue votre réseau et l'interface de discussion pour apporter des modifications

et recevoir des recommandations guidées. AWS Transform effectue une analyse d'impact en cascade et met en œuvre les modifications nécessaires pour maintenir la cohérence du réseau et la conformité aux meilleures pratiques. Vous pouvez également demander à AWS Transform d'analyser votre réseau et de suggérer des optimisations. Pour plus d'informations, consultez la section Recommandations guidées.

VPC existants sur votre compte cible

Si votre compte cible contient déjà des VPC issus de phases de migration précédentes ou de projets d'infrastructure parallèles, AWS Transform les détecte automatiquement et les affiche à côté de vos VPC mappés pendant le processus de révision. Pour les migrations multi-comptes, AWS Transform détecte les VPC existants sur tous les comptes de votre AWS organisation.

Cette visibilité vous permet de comprendre comment votre réseau planifié est lié à votre infrastructure existante, d'identifier les conflits CIDR potentiels et de prendre des décisions éclairées avant le déploiement.

> **Note**
>
> AWS Transform détecte uniquement les VPC existants (pas les sous-réseaux ou autres ressources). La détection est en lecture seule. AWS Transform ne modifie pas vos VPC existants.

Optimisez votre réseau

> **Note**
>
> Ces opérations s'appliquent uniquement aux VPC de charge de travail. Pour les VPC d'appliance dans la topologie Hub and Spoke (inspection, entrée, sortie), seule la modification de l'adresse IP est prise en charge.
> Vous ne pouvez pas annuler les opérations de suppression, de fusion et de fractionnement. Vérifiez attentivement votre configuration avant d'appliquer ces modifications.

Les opérations suivantes sont disponibles pour les VPC :

- Supprimer : supprimez définitivement un VPC de la configuration. Utilisez-le pour les segments de réseau obsolètes vers lesquels il ne faut pas migrer AWS.

- Exclure : supprimez temporairement un VPC de la migration pour les stratégies de migration par étapes. Les VPC exclus ne sont pas déployés mais peuvent être réinclus ultérieurement.
- Inclure : ajoutez à nouveau un VPC précédemment exclu dans la migration.
- Fusionner : combinez deux VPC en un seul. Le premier VPC conserve son identité et absorbe tous les sous-réseaux du second VPC. Les groupes de sécurité sont déplacés vers le VPC fusionné et leurs associations sont reconstruites en conséquence. Le CIDR du premier VPC s'étend jusqu'à la plus petite plage d'adresses CIDR contenant les deux CIDR d'origine, et le routage est mis à jour automatiquement. Le second VPC est supprimé de la configuration.

  Exigences relatives à la fusion :

  - Les CIDR de sous-réseau ne doivent pas se chevaucher entre les deux VPC.
  - Le CIDR fusionné ne doit pas dépasser /16.
  - Pour les déploiements multi-comptes, les deux VPC doivent être affectés au même compte.
- Modifier l'adresse IP : modifiez l'adresse IP de base d'un CIDR VPC tout en conservant la même longueur de préfixe. AWS Transform traduit automatiquement tous les CIDR des sous-réseaux selon le même décalage. Par exemple, la modification d'un VPC de `10.0.0.0/16` à `10.20.0.0/16` déplace un sous-réseau de à`10.0.1.0/24`. `10.20.1.0/24`

  Les règles des groupes de sécurité qui correspondent exactement à l'ancien CIDR du VPC sont mises à jour automatiquement. Les règles qui se chevauchent partiellement ou ne correspondent pas à l'ancien CIDR ne sont pas modifiées. Passez en revue ces règles après la modification.
- Renommer : modifiez le nom d'un VPC pour l'aligner sur les conventions de dénomination de votre organisation en matière de répartition des coûts, de suivi de conformité et de normes opérationnelles.
- Redimensionner : modifiez la longueur du préfixe d'un CIDR VPC pour étendre ou réduire la plage d'adresses IP.
  - Diminution de la longueur du préfixe (plus d'adresses IP, par exemple /20 à /16) : les sous-réseaux restent dans la plage la plus large. Aucune modification de sous-réseau n'est nécessaire.
  - Augmentation de la longueur du préfixe (moins d'adresses IP, par exemple /16 à /20) : les sous-réseaux qui se situent en dehors de la nouvelle plage doivent d'abord être redimensionnés à l'aide de l'opération de redimensionnement des sous-réseaux.

  Les règles des groupes de sécurité qui correspondent exactement à l'ancien CIDR du VPC sont mises à jour automatiquement. Les règles qui se chevauchent partiellement ou ne

correspondent pas à l'ancien CIDR ne sont pas modifiées. Passez en revue ces règles après le redimensionnement.

Exigences de redimensionnement :

- Le nouveau CIDR doit être compris entre /16 et /28.
- Le nouveau CIDR ne doit pas chevaucher les autres VPC du réseau (topologie Hub and Spoke).
- Lors de la réduction du CIDR, tous les sous-réseaux existants doivent correspondre au nouveau CIDR. Redimensionnez d'abord les sous-réseaux si nécessaire.

- Séparer : divisez un VPC en deux VPC en fonction des limites CIDR que vous fournissez. Les sous-réseaux sont attribués au nouveau VPC dont le CIDR les contient. Les groupes de sécurité sont clonés sur les deux nouveaux VPC, mais les CIDR des règles de groupe de sécurité ne sont pas automatiquement mis à jour. Passez en revue vos règles après le fractionnement pour vous assurer que la communication entre VPC fonctionne comme prévu. Le VPC d'origine est remplacé par les deux nouveaux VPC.

  Exigences partagées :

  - Vous devez fournir exactement deux plages CIDR.
  - Les deux CIDR ne doivent pas se chevaucher.
  - Chaque CIDR doit être compris entre /16 et /28.
  - Chaque sous-réseau doit correspondre exactement à l'un des deux CIDR. Si un sous-réseau ne correspond pas, l'opération est rejetée.

Les opérations suivantes sont disponibles pour les sous-réseaux :

- Modifier l'adresse IP : modifiez l'adresse IP de base d'un CIDR de sous-réseau tout en conservant la même longueur de préfixe.
- Supprimer : supprimez définitivement un sous-réseau de la configuration sans affecter le VPC parent.
- Redimensionner : modifiez la longueur du préfixe d'un CIDR de sous-réseau pour étendre ou réduire la plage d'adresses IP.

  Exigences relatives au redimensionnement des sous-réseaux :

  - Le nouveau CIDR doit être compris entre /16 et /28.
  - Le nouveau CIDR ne doit pas chevaucher les autres sous-réseaux du même VPC.
  - Le nouveau CIDR doit se trouver dans le CIDR du VPC parent.

Après chaque opération, AWS Transform réévalue le référencement des groupes de sécurité, ce qui peut convertir CIDR-based les règles en références de groupes de sécurité ou vice versa. Passez en revue les règles de votre groupe de sécurité après avoir apporté des modifications pour vérifier qu'elles répondent à vos exigences.

Recommandations de réseau guidées

AWS Transform analyse automatiquement votre réseau cartographié et propose des recommandations prioritaires via l'interface de discussion, identifiant les optimisations qui nécessitent généralement un examen manuel par les architectes réseau. Les recommandations sont basées sur les données de votre réseau et nécessitent votre confirmation avant que des modifications ne soient appliquées.

AWS Transform peut recommander les optimisations suivantes :

- Résolution des conflits CIDR : signale les plages CIDR qui se chevauchent entre vos VPC mappés et les VPC existants sur tous les comptes de votre organisation. AWS Les VPC en conflit sont affichés en premier. Vous pouvez résoudre les conflits en réadressant le VPC mappé, en l'excluant ou en le supprimant, ou en reconnaissant le conflit et en le résolvant vous-même après le déploiement.
- Standardisation des noms : signale les noms de VPC qui ne suivent pas un modèle cohérent (par exemple, les noms contenant des références matérielles). AWS Transform demande la convention de dénomination de votre cloud avant de proposer des remplacements.
- Examen de la portée : identifie les segments de réseau vers lesquels il n'est peut-être pas nécessaire de migrer AWS, tels que les systèmes existants ou les constructions en attente de mise hors service. AWS Transform demande votre confirmation avant d'exclure toute construction.
- Ajustement de la capacité des VPC : affiche les VPC dont le CIDR semble surdimensionné ou sous-dimensionné pour les sous-réseaux qu'il contient. AWS Transform présente les données de capacité actuelles et vous permet de décider de redimensionner ou non.
- Examen de sécurité : signale les règles des groupes de sécurité qui autorisent un trafic entrant illimité (0.0.0. 0/0) pour votre évaluation.
- Suppression des règles de groupe de sécurité obsolètes : identifie les règles de pare-feu entrantes non utilisées migrées depuis votre environnement sur site et suggère de les supprimer, afin de ne pas reporter une exposition de sécurité qui n'a plus d'utilité. Pour identifier les règles non utilisées, AWS Transform utilise les données de trafic réseau observées collectées par l'outil de découverte AWS Transform ou ModelizeIt. Vous devez soumettre ces données de trafic en même temps que votre entrée réseau source. AWS Transform compare vos règles de pare-feu migrées

au trafic observé sur la fenêtre d'observation capturée dans ces données, et signale une règle comme non utilisée lorsqu'aucun trafic entrant ne correspond à celle-ci. Sans données de trafic, AWS Transform ne peut pas déterminer quelles règles ne sont pas utilisées et ne suggère pas de suppression. AWS Transform supprime uniquement les règles d'entrée (entrantes) non utilisées. L'absence de trafic entrant observé est un signal fiable indiquant qu'une règle n'est pas utilisée. Passez en revue les suppressions suggérées avant de les appliquer pour vous assurer qu'elles sont conformes à vos politiques de sécurité.

- Consolidation des VPC : identifie les VPC fragmentés qui semblent séparés par des limites d'infrastructure physique plutôt que par des exigences d'isolation logique, et suggère de les fusionner.

> **Note**
>
> Toutes les recommandations nécessitent votre confirmation explicite avant que AWS Transform n'applique des modifications. AWS Transform propose des compromis lorsqu'une recommandation affecte plusieurs aspects de votre réseau.

Étape 6 : Schéma du réseau

Après avoir examiné les configurations VPC générées, vous pouvez éventuellement générer un diagramme de réseau pour visualiser la topologie de votre réseau. AWS Transform prend en charge les formats de diagramme suivants :

- Code Mermaid (.mmd) : ce format produit un fichier de définition de diagramme basé sur du texte que vous pouvez afficher à l'aide d'outils. Mermaid-compatible
- Image (.png) : ce format produit une image rendue de la topologie de votre réseau.

Étape 7 : Configuration du balisage des ressources

Vos ressources réseau sont étiquetées pour le lancement et la réplication. Vous pouvez également ajouter des balises personnalisées et des balises MAP (AWS Migration Acceleration Program).

Tags automatiques pour le lancement et la réplication

AWS Transform étiquette automatiquement vos ressources réseau migrées (VPC, sous-réseaux, groupes de sécurité et tables de routage) avec les balises suivantes :

- Clé : Valeur `CreatedBy` : `AWSApplicationMigrationService`
- Clé : Valeur `ATWorkspace` : *`workspace-id`*

Ces balises permettent d'utiliser le VPC et le sous-réseau pour lancer des instances de test et de basculement dans. AWS

> **Note**
>
> Vos VPC et sous-réseaux migrés n'incluent pas de connectivité Internet par défaut. Ils ne sont donc pas adaptés comme zones de transit pour la réplication.

Pour utiliser également le VPC et le sous-réseau comme zone intermédiaire (réplication), ajoutez manuellement les balises suivantes :

- Clé : Valeur `CreatedFor` : `AWSTransform`
- Clé : Valeur `ATWorkspace` : *`workspace-id`*

Vous pouvez également appliquer ces balises à n'importe quelle ressource AWS réseau existante afin de la rendre disponible pour la réplication.

Trouvez l'identifiant de votre espace de travail dans l'URL de l'application Web AWS Transform : https://... *`workspace-id`* /workspace//-id job/job

Balises personnalisées

Outre les balises appliquées automatiquement par AWS Transform, vous pouvez éventuellement ajouter des balises personnalisées pour organiser, suivre les coûts et gérer la conformité de vos ressources réseau migrées. Vous pouvez appliquer des balises personnalisées à deux niveaux :

- Job-level tags : s'appliquent à toutes les ressources créées par cette tâche, y compris à tous les VPC, sous-réseaux, groupes de sécurité et tables de routage.
- VPC-level tags : s'appliquent à un VPC spécifique et se répercutent automatiquement sur toutes ses ressources associées (sous-réseaux, groupes de sécurité, tables de routage).

> **Note**
>
> 40 balises maximum par demande. Chaque étiquette nécessite une clé et une valeur. AWS les conventions de balisage s'appliquent.

AWS Transform applique ces balises lorsqu'elle génère l'infrastructure sous forme de modèles de code.

AWS Programme d'accélération des migrations

Si votre migration s'inscrit dans le cadre du programme d'accélération de la AWS migration (MAP 2.0), AWS Transform applique une balise MAP à vos ressources. Si vous avez fourni votre identifiant MPE plus tôt dans le processus de migration, la balise est appliquée automatiquement. Sinon, une fois que vous avez terminé de passer en revue les configurations VPC générées, AWS Transform vous demande si vous avez un accord MAP et vous invite à fournir votre identifiant MPE. L'identifiant MPE est un code à 10 caractères composé de lettres majuscules et de chiffres (par exemple, ABCDE12345). La balise appliquée utilise le format suivant :

- Clé : Valeur `map-migrated` : `mig`*`MPE_ID`*

Étape 8 : Déployez votre réseau

Après avoir marqué, sélectionnez votre stratégie de déploiement :

- AWS Transform-managed déploiement : AWS Transform utilise des CloudFormation modèles pour déployer votre réseau et exécute Reachability Analyzer pour vérifier la connectivité entre les sous-réseaux de plusieurs VPC et au sein d'un même VPC.

  > **Note**
  >
  > Vous devez obtenir une approbation explicite avant que votre demande de déploiement réseau ne soit exécutée. Consultez la section Processus d'approbation des déploiements.

- Self-deployment: AWS Transform génère des modèles d'infrastructure en tant que code (IaC). CloudFormation les modèles sont générés par défaut. Vous pouvez également sélectionner d'autres formats de sortie :
  - AWS CDK génère un TypeScript projet pour le déploiement d'une infrastructure programmatique.

- HashiCorp Terraform génère des modèles HashiCorp de langage de configuration (HCL) pour gérer les ressources réseau.
- Landing Zone Accelerator (LZA) génère un fichier network-config.yaml pour la configuration réseau LZA.

> **Note**
>
> Lorsque vous effectuez un déploiement via le pipeline Landing Zone Accelerator (LZA), votre compte AWS Transform et votre installation LZA doivent se trouver dans la même AWS organisation. Le déploiement échouera en cas de non-concordance entre les ID d'organisation.

Pour l'auto-déploiement, utilisez le lien fourni pour télécharger un fichier zip contenant les modèles générés. Le dossier zip contient un README.md fichier qui explique comment utiliser les modèles générés.

Pour vérifier que le fichier téléchargé n'a pas été endommagé ou altéré, générez et téléchargez une somme de contrôle, puis comparez-la à un hachage généré localement à l'aide `openssl dgst -sha256 -binary <file.zip> | base64` de la commande.

Processus d'approbation des déploiements

Pour garantir que les modifications apportées au réseau sont conformes aux normes de sécurité et aux exigences architecturales de votre organisation, toutes les demandes de déploiement sont soumises à un flux de travail d'approbation. Vous devez obtenir une approbation explicite avant que votre demande de déploiement réseau ne soit exécutée. Lorsque vous soumettez une demande de déploiement, celle-ci est automatiquement acheminée vers des approbateurs autorisés via l'onglet AWS Transformer les approbations. Les approbateurs valident à la fois les CloudFormation modèles et les configurations réseau pour garantir la conformité aux normes de sécurité et aux exigences architecturales. Chaque soumission déclenche un nouveau cycle de révision, et les déploiements n'ont lieu qu'après réception de la confirmation. Si un approbateur refuse votre demande, contactez-le directement pour discuter des modifications nécessaires. AWS Transform suit toutes les décisions d'approbation à des fins d'audit et tient à jour l'historique des déploiements.

Supprimer les ressources réseau déployées

Si vous devez annuler un déploiement, vous pouvez supprimer les ressources réseau déployées par AWS Transform. Vous pouvez supprimer des ressources immédiatement après la fin du déploiement. Si vous modifiez les ressources réseau déployées après le déploiement, les ressources ne peuvent pas être supprimées automatiquement.

- AWS Transform-managed déploiements : AWS Transform supprime toutes les CloudFormation piles créées lors du déploiement. Cette action nécessite une approbation via l'onglet AWS Transformer les approbations.
- Self-deployments: vous devez supprimer manuellement les ressources déployées via la console de AWS gestion ou l' AWS interface de ligne de commande.

Extraction du fichier de configuration

Si votre environnement source utilise Cisco ACI, Palo Alto Networks ou Fortinet FortiGate, vous devez extraire un fichier de configuration à fournir à Transform. AWS Vous pouvez utiliser ces fichiers comme fichiers sources autonomes pour générer une infrastructure réseau et des groupes de sécurité, ou comme fichiers complémentaires à côté d'un téléchargement RVTools pour ajouter la génération de groupes de sécurité. Le processus d'extraction est le même dans les deux cas.

Pour extraire les fichiers de configuration de votre pare-feu et de votre environnement réseau, procédez comme suit. Consultez la documentation du fournisseur pour obtenir les informations les plus récentes.

Fortinet FortiGate

- La version du microprogramme doit être 7.0 ou ultérieure.
- Vous avez besoin `super_admin` de `super_admin_readonly` nos privilèges au niveau mondial.
- Étapes :
  1. Connectez-vous au pare-feu via SSH ou un client CLI intégré
  2. Exécuter : `show | grep ""` (`| grep ""`désactive la pagination)
  3. Enregistrez toutes les sorties dans un fichier à partir de la `show` commande

Palo Alto Networks

- La version du microprogramme doit être 10.1 ou ultérieure.
- Vous avez besoin du rôle de superadmin.
- Connectez-vous au pare-feu via SSH, exécutez les commandes suivantes pour désactiver la pagination, définir le format de sortie, passer en mode configuration et exporter la configuration et les objets prédéfinis. Enregistrez les sorties :

```
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 version du microprogramme doit être 6.0 ou ultérieure.
- Vous avez besoin du rôle d'administrateur avec tous les privilèges et d'une destination configurée pour le protocole SCP (Secure Copy Protocol), le protocole SFTP (SSH File Transfer Protocol) ou le protocole FTP (File Transfer Protocol).
- Étapes :
  1. Connectez-vous à l'Application Policy Infrastructure Controller (APIC) via votre navigateur
  2. Ouvrez le menu Admin et choisissez Config Rollbacks
  3. Dans la boîte de dialogue Prendre un instantané, sélectionnez l'option de localisation distante et choisissez Créer un instantané maintenant.
  4. Après avoir reçu le message « Transfert réussi », connectez-vous au serveur de localisation distant et récupérez le dernier fichier instantané (fichier .gz)

Migrer des serveurs

AWS Transform automatise le réhébergement de vos serveurs sur Amazon EC2 à grande échelle. L' AI-powered agent vous guide tout au long de chaque vague de migration, de la validation de l'inventaire au déploiement de l'agent de réplication, en passant par les tests et la transition finale. AWS Transform gère l'orchestration sur des centaines de serveurs tout en gardant le contrôle sur les décisions de configuration et d'approbation. Sous le capot, AWS Transform utilise AWS Transform

MGN (MGN) pour la réplication des données. Pour plus d'informations sur le MGN, voir Qu'est-ce que c'est ? AWS Transform MGNdans le guide de l'utilisateur MGN.

Vous pouvez migrer des serveurs depuis pratiquement n'importe quel environnement source, y compris des centres de données sur site, d'autres fournisseurs de cloud ou d'autres AWS régions. AWS Transform prend en charge à la fois les serveurs physiques et les serveurs virtuels exécutés sur VMware Hyper-V, KVM ou d'autres plateformes de virtualisation. L'infrastructure source et l'hyperviseur ne sont pas importants tant que le système d'exploitation source est pris en charge.

La migration des serveurs est organisée par vagues. Chaque vague représente un groupe de serveurs qui sont migrés ensemble. Pour chaque vague, l'agent vous guide à travers les phases suivantes :

Pour les vagues dotées d'une stratégie de migration conteneurisée, AWS Transform exécute le flux de travail de conteneurisation du code source au lieu des étapes de réhébergement décrites ci-dessous. Le flux de travail de conteneurisation vous guide dans le clonage du code source, la génération d'artefacts Docker, la publication d'images de conteneurs et le déploiement sur Amazon Elastic Container Service ou Amazon Elastic Kubernetes Service. Pour le flux de travail complet de conteneurisation, consultez. Conteneurisation du code source

1. Conditions préalables et configuration des paramètres de migration par défaut. Configurez vos comptes cibles et configurez la manière dont les instances sont lancées. AWS Transform fournit des paramètres par défaut intelligents pour vous permettre de démarrer rapidement.
2. Étape 1 : Configurez la vague de migration. L'agent configure votre compte cible, valide les autorisations et configure automatiquement le balisage des ressources.
3. Étape 2 : Validez et confirmez l'inventaire. Passez en revue les configurations de vos serveurs, les recommandations relatives aux types d'instances et les attributions réseau avant de commencer la migration.
4. Étape 3 : Déploiement des agents de réplication L'agent peut déployer des agents sur tous les serveurs en une seule vague sans avoir besoin d'accéder manuellement à chaque serveur individuellement.
5. Étape 4 : réplication des données La réplication continue au niveau des blocs permet de synchroniser votre environnement cible avec les serveurs sources jusqu'à ce que vous soyez prêt pour le basculement.
6. Étape 5 : Tester. Lancez des instances de test pour valider vos serveurs migrés avant de passer à la version finale.

7. Étape 6 : Découpe. Terminez la migration avec un minimum de temps d'arrêt. L'agent coordonne le passage final et vérifie le succès.

Conditions préalables et configuration des paramètres de migration par défaut

Conditions préalables

Si vous avez effectué toutes les étapes d'une tâche de migration de bout en bout dans AWS Transform, vos comptes cibles, votre fichier d'inventaire et votre infrastructure réseau sont déjà prêts. Vous pouvez passer à la section Configurer les paramètres de migration par défaut.

Si vous lancez la migration de serveurs de manière indépendante, assurez-vous que les éléments suivants sont en place :

- Systèmes d'exploitation pris en charge : les serveurs sources doivent exécuter un système d'exploitation pris en charge. Pour la liste complète, consultez la section Systèmes d'exploitation pris en charge dans le guide de l'utilisateur MGN.
- Comptes cibles pour la migration : Compte AWS ID sur lesquels vous souhaitez que vos serveurs soient migrés. Vous pouvez utiliser AWS Transform landing zone ou tout autre outil pour configurer votre infrastructure.
- Infrastructure réseau en place : VPC, sous-réseaux et groupes de sécurité déployés et configurés. Vous pouvez utiliser AWS Transform Network Migration ou tout autre outil pour configurer votre infrastructure réseau.
- Fichier d'inventaire — Préparé avec les détails du serveur, les attributions des vagues, les informations du compte cible et les préférences de type d'instance Amazon EC2. Vous pouvez utiliser la planification de migration de AWS Transform pour générer ce fichier.

Configurer les paramètres de migration par défaut

AWS Transform fournit des paramètres par défaut intelligents pour votre configuration de migration, notamment la manière dont les instances Amazon EC2 sont lancées et la configuration de la réplication. Vous pouvez accepter ces paramètres par défaut et commencer à migrer immédiatement, ou les personnaliser via l'interface de discussion ou un examen visuel. Les valeurs par défaut s'appliquent à tous vos comptes cibles et peuvent être modifiées au niveau de la vague lors de la configuration de la vague.

Préférences de recommandation Amazon EC2

AWS Transform analyse l'utilisation de votre serveur source et recommande des instances Amazon EC2 de taille optimale, ce qui vous permet d'éviter le surprovisionnement dès le premier jour. Vous pouvez configurer vos préférences de recommandation Amazon EC2 pour contrôler la manière dont les types d'instance sont sélectionnés pour vos serveurs migrés.

Pour plus d'informations sur la génération de recommandations Amazon EC2, consultez la section Génération de recommandations Amazon EC2 dans. AWS Migration Hub

> **Note**
>
> Vous pouvez modifier les types d'instances Amazon EC2 suggérés pour inclure les recommandations issues de l'évaluation de la migration, de l'évaluation de AWS l'optimisation et des licences (OLA) ou d'une tâche d'évaluation AWS Transform.

Initialisation de la migration

AWS Transform configure automatiquement l'infrastructure de migration requise dans vos comptes cibles avant le début de la migration. Cela inclut l'initialisation de MGN pour chaque Région AWS compte vers lequel vous prévoyez de migrer, ainsi que pour tous les comptes cibles. Au cours du processus d'initialisation :

- Les rôles et politiques IAM requis sont créés.
- Les modèles par défaut requis sont configurés.

Pour plus d'informations sur le processus d'initialisation, consultez la section Initialisation à l' AWS Transform MGN aide de la console dans le guide de l'utilisateur MGN.

Modèle de lancement Amazon EC2

Les paramètres de lancement comprennent deux parties : les paramètres de lancement généraux et le modèle de lancement Amazon EC2, qui détermine comment une instance de test ou de basculement est lancée pour chaque serveur source dans. AWS

Les paramètres de lancement, y compris le modèle de lancement Amazon EC2, peuvent être définis au niveau du compte et sont ensuite appliqués automatiquement à chaque serveur source chaque fois que vous ajoutez un serveur source à AWS Transform MGN. Les paramètres de lancement par défaut définis dans cette section peuvent être appliqués automatiquement à tous vos comptes cibles.

AWS Transform présente la liste des paramètres de modèle de lancement disponibles. Vous pouvez choisir de continuer avec les paramètres par défaut ou de configurer votre modèle de lancement. Si vous choisissez de configurer, AWS Transform fournit un lien vers une revue HITL (human in-the-loop) contenant tous les paramètres des paramètres du modèle de lancement. Vous pouvez également apporter des modifications directement via l'interface de discussion pour les paramètres de votre choix.

https://docs.aws.amazon.com/mgn/latest/ug/source-servers.htmlLes serveurs sources sont créés avec les paramètres du modèle de lancement de compte. Une fois les serveurs sources créés avec ces paramètres par défaut, vous pouvez les modifier au niveau des paramètres de lancement du serveur source. Vous pouvez modifier les paramètres du serveur source sur n'importe quel paramètre à l'aide de l'interface de discussion ou, pour les opérations groupées, à l'aide du fichier d'inventaire Excel pendantÉtape 2 : Valider et confirmer l'inventaire.

Pour consulter la liste complète des paramètres et des détails du modèle de lancement, consultez la section Paramètres généraux de lancement dans le guide de l'utilisateur MGN.

Modifications supplémentaires du modèle de lancement d'Amazon EC2

Pour apporter d'autres modifications au modèle de lancement d'Amazon EC2, vous devez les effectuer sur l'ID du modèle de chaque compte cible. Cette option est disponible dans la configuration des vagues. AWS Transform vous y guide et vous fournit le lien approprié.

Post-launch actions

Post-launch les actions automatisent les tâches de modernisation et de validation qui s'exécutent sur chaque serveur source immédiatement après son lancement en tant qu'instance de test ou de basculement dans. AWS AWS Transform Rehost exécute les actions post-lancement disponibles dans MGN et fournit ces fonctionnalités afin que l'agent puisse les recommander, les configurer et les exécuter en votre nom dans le cadre du flux de migration. Les actions sont exécutées via AWS Systems Manager (Systems Manager) et peuvent être l'une des actions prédéfinies disponibles dans MGN ou une action personnalisée créée à partir d'un document Systems Manager existant.

Post-launch les actions peuvent être définies au niveau du compte et sont ensuite appliquées automatiquement à chaque serveur source chaque fois que vous ajoutez un serveur source à MGN. Les paramètres d'action par défaut définis dans cette section peuvent être appliqués automatiquement à tous vos comptes cibles.

AWS Transform présente d'abord la liste des actions disponibles après le lancement sur vos comptes cibles. Il vous propose ensuite de définir une nouvelle action après le lancement et de

l'appliquer à la migration de votre compte cible. AWS Transform fournit également AI-powered des recommandations basées sur le système d'exploitation et les meilleures pratiques pour votre inventaire. Vous pouvez choisir de continuer avec les valeurs par défaut ou de configurer vos propres actions.

Vous pouvez également choisir une action post-lancement qui est déjà définie dans MGN. Demandez à l'agent d'afficher la liste des actions prédéfinies disponibles après le lancement. Pour plus d'informations sur cette liste, consultez la section Actions prédéfinies après le lancement dans le guide de l'utilisateur MGN.

Création d'une nouvelle action après le lancement

Si vous choisissez de créer une nouvelle action après le lancement, l'agent vous invite à fournir le nom du document Systems Manager ou l'ARN de Systems Manager avec lequel créer l'action après le lancement. Le document Systems Manager doit être créé à l'avance via la AWS Systems Manager console. Pour plus d'informations sur la création d'un document Systems Manager, voir Création de documents Systems Manager dans le Guide de AWS Systems Manager l'utilisateur.

L'agent génère ensuite une interface HITL (human in-the-loop) dans laquelle vous fournissez les champs obligatoires :

- Post-launch nom de l'action : l'agent fournit un nom par défaut, que vous pouvez modifier.
- Post-launch ordre des actions : la valeur de commande par défaut est 1001, sauf si le compte a déjà défini des actions après le lancement, auquel cas la nouvelle action est placée en dernier dans l'ordre d'exécution. Vous pouvez modifier l'ordre. Pour plus d'informations sur l'ordre des actions après le lancement, consultez Post-launch les paramètres du guide de l'utilisateur MGN.
- Valeurs de paramètres de Systems Manager requises : indiquez les valeurs de tous les paramètres requis par le document Systems Manager.

Vous pouvez également apporter des modifications directement via l'interface de discussion pour les paramètres de votre choix.

Les serveurs sources sont créés avec les paramètres d'action du compte après le lancement. Une fois les serveurs sources créés avec ces paramètres par défaut, vous pouvez les modifier au niveau du serveur source. Vous pouvez modifier les paramètres du serveur source pour n'importe quelle action à l'aide de l'interface de discussion, ou pour les opérations groupées à l'aide du fichier Excel d'inventaire pendantÉtape 2 : Valider et confirmer l'inventaire.

Post-launch actions dans le fichier d'inventaire

L'agent Rehost étend le fichier d'inventaire avec un modèle d'action post-lancement défini pour chaque serveur source. Cela permet aux clients de mettre à jour ou d'ajouter des actions après le lancement par serveur source lors du processus de réhébergement vers MGN. Pour supprimer des actions spécifiques après le lancement sur un serveur source, utilisez la `active` colonne correspondante. `FALSE` Post-launch les actions du fichier d'inventaire utilisent la convention de dénomination suivante :

`mgn:launch:post-actions:<ACTION_NAME>:<FIELD_NAME>`

Une bascule globale permet de contrôler si les actions sont exécutées après le lancement :

`mgn:launch:post-actions:enabled` (`TRUE`/`FALSE`)

Champs par action

- `ssmDocumentName`(Chaîne, obligatoire) — Le document Systems Manager à exécuter.
- `order`(Nombre entier, obligatoire) — Ordre d'exécution ; doit être compris entre 1 000 et 10 000. Les actions sont exécutées dans l'ordre croissant : les valeurs inférieures sont exécutées en premier.
- `active`(`TRUE`/`FALSE`, facultatif) — Indique si l'action est active.
- `mustSucceedForCutover`(`TRUE`/`FALSE`, facultatif) — Indique si l'action doit réussir avant le basculement.
- `timeoutSeconds`(Nombre entier, facultatif) — Délai d'attente en secondes.
- `description`(Chaîne, facultatif) — Human-readable description.
- `parameters`(JSON, facultatif) : paramètres du document Systems Manager.

Structure JSON des paramètres

Le `parameters` champ est fourni sous forme de structure JSON :

```
{
  "parameters": {
    "Operation": [
      {"value": "Scan", "type": "String"}
    ]
  },
  "externalParameters": {
```

```
    "InstanceId": "ec2.InstanceId"
  }
}
```

- `parameters`— Associe les noms des paramètres du document à une liste de références de valeurs (chacune comportant un `value` et une valeur facultative`type`, la valeur par défaut étant`String`).
- `externalParameters`— Associe les noms des paramètres du document à des chaînes de chemin dynamiques (aucun paramètre Systems Manager n'est créé).

Étape 1 : Configuration de la vague de migration

Au cours de cette phase, AWS Transform prépare la vague de migration en configurant le compte cible, en vérifiant les autorisations de service, en configurant des balises de ressources, en ajoutant des données réseau à votre inventaire et en configurant les paramètres de réplication et de lancement.

Mode de migration et configuration du compte

AWS Transform prend en charge deux modes de migration :

- Single-account migration — Tous les serveurs de la vague migrent vers le même compte cible configuré dans votre connecteur.
- Multi-account migration : les serveurs migrent vers différents comptes cibles spécifiés dans votre fichier d'inventaire. Pour les migrations multicomptes, votre fichier d'inventaire doit inclure une `mgn:account-id` colonne contenant l'identifiant du compte cible pour chaque serveur.

AWS Transform confirme la configuration du compte cible et vérifie que MGN est initialisé dans chaque compte cible. Si MGN n'est pas encore initialisé, AWS Transform fournit des instructions pour terminer l'initialisation. Lors de l'initialisation, MGN crée les rôles de service IAM suivants pour les opérations de réplication et de lancement :

- `AWSApplicationMigrationReplicationServerRole`
- `AWSApplicationMigrationConversionServerRole`
- `AWSApplicationMigrationMGHRole`
- `AWSApplicationMigrationLaunchInstanceWithDrsRole`
- `AWSApplicationMigrationLaunchInstanceWithSsmRole`

- `AWSApplicationMigrationAgentRole`

Pour en savoir plus sur ces rôles, consultez Initialisation de MGN à l'aide de la console ou Initialisation de MGN à l'aide de l'API dans le guide de l'utilisateur de MGN.

Pour les migrations multi-comptes, AWS Transform crée également le rôle suivant lors de l'étape d'initialisation :. `AWSTransformRehostSharingRole_<management-or-delegated-admin-account-id>` Ce rôle est déployé sur tous les comptes cibles de migration.

Vérification du balisage des ressources

Une fois les autorisations de service confirmées, AWS Transform vérifie que toutes les ressources requises sont correctement balisées pour que la migration soit effectuée avec succès par l'agent. S'il manque des balises obligatoires à certaines ressources, AWS Transform fournit un lien vers la page de balisage où vous pouvez appliquer les balises manquantes avant de continuer. Les balises suivantes sont obligatoires :

- Les serveurs sources existants doivent comporter des balises `CreatedBy: AWSTransform` et`ATWorkspace: <workspace_id>`. Si vous avez déjà commencé la réplication sur des serveurs sources et que vous les avez créés dans le service AWS Transform MGN, vous devez baliser ces serveurs afin que AWS Transform puisse les corréler avec les serveurs sources découverts dans votre environnement sur site et éviter la création inutile de serveurs sources dupliqués. AWS Transform les met automatiquement en corrélation à l'aide de l'ID, du FQDN ou des clés de nom d'hôte fournis par l'utilisateur.
- Les ressources réseau doivent être correctement balisées pour les instances de réplication (zone de transit) et de lancement. AWS Transform affiche la liste complète des ressources réseau de votre compte cible, en indiquant si chaque ressource est déjà balisée ou non. Vous pouvez consulter la liste et sélectionner les ressources non balisées que vous souhaitez ajouter. Pour chaque ressource que vous sélectionnez, AWS Transform applique la balise appropriée :
  - `CreatedBy: AWSTransformouCreatedFor: AWSTransform`, selon le type de ressource.
  - `ATWorkspace: <workspace_id>`est appliqué à toutes les ressources sélectionnées.

  Les VPC et les sous-réseaux créés par l'agent de migration réseau AWS Transform sont automatiquement balisés.
- Outre les VPC et les sous-réseaux, AWS Transform affiche également toutes les interfaces réseau élastiques (ENI) existantes présentes dans votre compte cible. Si vous souhaitez que AWS Transform les utilise dans le cadre du lancement de votre instance, ils doivent être balisés avec

`CreatedFor: AWSTransform etATWorkspace: <workspace_id>`. Pour plus d'informations sur la manière de joindre ou d'ajouter des ENI au modèle de lancement d'Amazon EC2, consultez les considérations détaillées dans le guide de l'utilisateur MGN.

Ajouter des données réseau à l'inventaire

AWS Transform ajoute les informations réseau issues de la migration de votre réseau au fichier d'inventaire. Cette étape mappe vos serveurs aux sous-réseaux cibles et aux groupes de sécurité appropriés en fonction de la configuration réseau générée lors de la phase de migration du réseau.

Paramètres de réplication et de lancement

Configuration des paramètres de réplication

Les paramètres de réplication déterminent la manière dont les données sont répliquées depuis vos serveurs sources vers AWS. Configurez les paramètres de réplication dans le modèle de réplication avant d'ajouter des serveurs sources à AWS Transform MGN. AWS Transform vous montre tous les paramètres des paramètres de réplication. Vous pouvez les configurer via un HITL dédié ou via l'interface de chat.

Pour plus de détails sur les paramètres des paramètres de réplication, consultez la section Modèle de paramètres de réplication dans le guide de l'utilisateur MGN.

Paramètres du modèle de lancement

Le modèle de lancement vous permet de contrôler la façon dont AWS Transform MGN lance les instances dans AWS. La configuration par défaut définie dans le modèle est automatiquement appliquée à chaque nouveau serveur ajouté. Vous pouvez configurer les paramètres du modèle de lancement via un HITL dédié ou via l'interface de chat.

Pour plus de détails sur les paramètres des paramètres du modèle de lancement, consultez la section Modèle de lancement dans le guide de l'utilisateur MGN.

AWS Transform fournit également un lien vers l'ID du modèle de lancement Amazon EC2 associé au modèle de lancement, vous permettant de modifier des attributs supplémentaires du modèle de lancement Amazon EC2. Pour modifier le modèle de lancement Amazon EC2, suivez les instructions de la section Modèle de lancement du guide de l'utilisateur MGN.

Stratégie d'attribution d'adresses IP

Vous choisissez la manière dont les adresses IP sont attribuées à vos serveurs migrés :

- IP statique : l'adresse IP du serveur source est conservée. Si une transformation CIDR est requise, AWS Transform convertit automatiquement l'adresse IP pour qu'elle corresponde au nouveau CIDR.
- IP dynamique (DHCP) : une nouvelle adresse IP est attribuée à chaque serveur à partir du pool IP du sous-réseau.

> **Note**
>
> Si vous avez sélectionné la stratégie de mappage des groupes de sécurité MAP lors de la migration du réseau, seule l'attribution d'adresses IP statique est disponible. Pour plus de détails, consultez la section Cartographie des groupes de sécurité.

Étape 2 : Valider et confirmer l'inventaire

Avant de charger les données de votre serveur dans MGN, AWS Transform prépare le fichier d'inventaire pour que vous puissiez le consulter. Vous pouvez télécharger le fichier au format CSV ou XLSX, consulter les configurations du serveur et apporter des modifications si nécessaire.

Le fichier d'inventaire inclut des informations telles que les noms des serveurs, les systèmes d'exploitation, les recommandations relatives au type d'instance Amazon EC2, les sous-réseaux cibles, les groupes de sécurité, les attributions IP et les options de licence. Les champs obligatoires incluent :

- Informations sur le serveur : nom du serveur, VMID et spécifications de la source.
- Affectation des vagues — Regroupement des vagues de migration.
- Regroupement d'applications — Associations logiques d'applications.
- Configuration cible : compte cible, région et type d'instance Amazon EC2.
- Configuration réseau : sous-réseau cible et groupes de sécurité.

Vous pouvez modifier le fichier pour ajuster les configurations Amazon EC2, modifier les options de licence du système d'exploitation (BYOL ou licence incluse) et mettre à jour les paramètres de location.

Après avoir consulté l'inventaire, vous pouvez soit l'accepter tel qu'il est indiqué, soit télécharger une version modifiée. AWS Transform charge ensuite les données dans MGN, qui crée des enregistrements de serveur source pour chaque serveur de la vague.

> **Note**
>
> Ne supprimez pas de colonnes et ne modifiez pas les en-têtes de colonne dans le fichier d'inventaire. AWS La transformation nécessite la structure de fichier d'origine pour traiter correctement les données.

> **Note**
>
> AWS Transform permet d'importer une seule fois vers une cible donnée Compte AWS et une cible Région AWS à la fois. Si vous travaillez sur plusieurs vagues simultanément, ou si plusieurs tâches de migration sont en cours d'exécution avec le même compte cible, vous devez attendre la fin d'une importation avant de pouvoir effectuer une autre importation dans une autre vague ou une autre tâche.

Vous pouvez contrôler les options de licence du système d'exploitation (BYOL ou licence incluse) et la location en spécifiant la configuration dans les colonnes `mgn:launch:placement:operating-system-licensing` du fichier d'inventaire et. `mgn:launch:placement:tenancy` Pour plus d'informations, consultez la section Paramètres d'importation dans le guide de l'utilisateur MGN.

Étape 3 : Déploiement des agents de réplication

Pour commencer à répliquer les données de vos serveurs sources vers AWS, vous devez installer l'agent de AWS réplication sur chaque serveur source. AWS Transform propose trois méthodes d'installation :

- Outils d'organisation : utilisez les outils de déploiement existants de votre organisation (tels que SCCM, Ansible ou Chef) pour installer des agents sur vos serveurs. AWS Transform fournit aux commandes d'installation des paramètres supplémentaires pour une installation silencieuse `--no-prompt--aws-access-key-id`, notamment`--aws-secret-access-key`, et`--aws-session-token`.
- Connecteur MGN : utilisez un connecteur MGN pour automatiser l'installation de l'agent. Le connecteur se connecte aux machines sources via SSH (Linux) ou WinRM (Windows) et installe automatiquement l'agent de réplication. Une fois configuré, un connecteur peut être réutilisé sur plusieurs ondes et sur différentes cibles Comptes AWS. Pour plus d'informations sur le connecteur MGN, voir Configuration du connecteur MGN dans le guide de l'utilisateur MGN.

> **Note**
>
> Avant d'utiliser le connecteur MGN avec AWS Transform, vous devez baliser l'instance gérée du connecteur dans AWS Systems Manager Fleet Manager avec les balises suivantes :
>
> - Clé : `CreatedFor` Valeur : `AWSTransform`
> - Clé : `ATWorkspace` Valeur : *`workspace-id`*
>
> Pour baliser l'instance gérée, ouvrez la AWS Systems Manager console, accédez à Fleet Manager sous Node Tools, choisissez l'instance gérée de votre connecteur MGN et appliquez les balises ci-dessus. Trouvez l'ID de votre espace de travail dans l'URL de l'application Web AWS Transform :`https://.../workspace/`*`workspace-id`*`/job/`*`job-id`*.

- Installation manuelle : installez l'agent directement sur chaque serveur source. Cette méthode nécessite un accès direct à chaque serveur mais vous donne un contrôle total sur le processus d'installation.

AWS Configuration du connecteur Transform MGN

Le connecteur AWS Transform MGN automatise le déploiement des agents de réplication sur vos serveurs sources, évitant ainsi de devoir vous connecter à chaque serveur individuellement. Le connecteur est un client léger déployé sur une machine Linux dédiée dans votre environnement local. Il se connecte aux serveurs sources via SSH (Linux) ou WinRM (Windows) pour installer et configurer des agents de réplication, éliminant ainsi la nécessité de coordonner manuellement plusieurs AWS services.

Comment fonctionne le connecteur

Le connecteur fonctionne grâce aux composants suivants :

- Client de connecteur : déployé sur une machine Linux dédiée dans votre environnement.
- Agent SSM : installé sur la même machine pour permettre une communication sécurisée avec AWS.
- Activation hybride SSM : relie la machine connectée à AWS Systems Manager pour une exécution sécurisée des commandes.

- Gestion des informations d'identification : extrait les informations d'identification du serveur source à partir de AWS Secrets Manager.

Lorsque vous déployez des agents, AWS Transform envoie un document SSM à la machine à connecter. Le connecteur récupère ensuite les informations d'identification du serveur source à partir de AWS Secrets Manager, établit une connexion avec chaque serveur source, vérifie que le serveur source répond aux prérequis, installe et configure l'agent de réplication et vérifie la réussite de l'installation.

Exigences relatives à la machine à connecteurs

Exigence	Détails
Système d'exploitation	Système d'exploitation Linux pris en charge. Pour la liste complète, consultez la section Prérequis pour le connecteur MGN dans le Guide de l'utilisateur MGN.
Accès réseau	Doit atteindre tous les serveurs sources (Linux via SSH, Windows via WinRM)
Connectivité Internet	HTTPS sortant (443) vers les AWS terminaux (Systems Manager, Secrets Manager, MGN)
Espace disque	Minimum 200 Mo gratuits
Permissions	Accès root ou sudo

> **Note**
>
> Le connecteur doit être installé sur une machine Linux, mais il peut déployer des agents sur des serveurs sources Linux et Windows.

Processus de configuration

AWS Transform vous guide à travers les étapes suivantes pour configurer le connecteur :

Étape 1 : Configuration du connecteur

Donnez un nom à votre connecteur ou utilisez le nom par défaut généré automatiquement. Le connecteur peut être installé sur le compte de gestion ou sur un compte administrateur délégué dans MGN. Pour les migrations multi-comptes, le connecteur peut déployer des agents sur des serveurs sur l'ensemble des comptes membres.

Étape 2 : configuration AWS des ressources

AWS Transform ouvre une page de configuration qui s'exécute dans votre navigateur à l'aide de vos AWS informations d'identification. Vous devez être connecté à la console AWS de gestion avec votre compte de gestion ou votre compte d'administrateur délégué. Il doit s'agir du même compte auquel votre connecteur cible AWS Transform est connecté.

La page de configuration crée automatiquement les ressources suivantes :

- Rôles IAM (créés par erreur, ignorés s'ils existent déjà) :
  - `AWSApplicationMigrationConnectorManagementRole`— Utilisé lors de l'installation de l'agent pour accéder aux informations d'identification.
  - `AWSApplicationMigrationConnectorSharingRole_<ACCOUNT-ID>`— Contient des autorisations pour l'installation de l'agent.
- Activation hybride SSM — Période d'expiration de 30 jours. Lie la machine connectée à AWS Systems Manager et génère des informations d'activation sécurisées.

Vous pouvez également télécharger un CloudFormation modèle depuis la page de configuration pour déployer vous-même les rôles IAM.

La page de configuration génère une commande d'installation en une ligne contenant toutes les informations d'identification et de configuration nécessaires.

> **Important**
>
> Laissez la page de configuration ouverte jusqu'à ce que l'installation soit terminée. Pour le fermer, il faudra redémarrer le processus. Toutes les informations d'identification existent uniquement dans votre navigateur et ne sont pas stockées par AWS Transform.

Étape 3 : Installation du connecteur

Installez le connecteur sur une machine Linux de votre environnement :

1. Copiez le lien d'installation depuis la page de configuration.
2. Connexion SSH à la machine Linux de votre choix.
3. Collez et exécutez la commande d'installation.
4. Attendez la fin de l'installation (généralement 2 à 3 minutes).

Étape 4 : connecter les serveurs sources

Après l'installation, AWS Transform identifie tous les serveurs sources appartenant à la vague actuelle et les connecte automatiquement au connecteur MGN.

Étape 5 : Configuration des informations d'identification

Fournissez AWS les ARN de Secrets Manager pour les informations d'identification de votre serveur source. AWS Transform propose trois options de configuration des informations d'identification :

- Secret unique pour les serveurs Linux — Un secret partagé contenant des clés SSH ou username/password pour tous les serveurs sources Linux.
- Secret unique pour les serveurs Windows — Un secret partagé contenant le nom d'utilisateur et le mot de passe pour tous les serveurs sources Windows.
- Secrets multiples par serveur — Différents secrets par serveur ou groupe de serveurs. Utilisez-le lorsque les serveurs ont des informations d'identification différentes. AWS Transform génère un fichier CSV prérempli avec votre liste de serveurs. Vous remplissez la `secret_arn` colonne pour chaque serveur et vous chargez le fichier terminé.

> **Note**
>
> Vous pouvez combiner les options de secret unique pour Linux et Windows si les deux types de serveurs disposent chacun d'un secret partagé. L'option de secrets par serveur s'exclut mutuellement des options de secret unique.

Format secret des informations d'identification. Pour en savoir plus, consultez les informations d'identification du connecteur MGN dans le guide de l'utilisateur MGN :

```
{
  "WinConnectionProtocol": "HTTPS",
  "WinUserName": "windows_username",
```

```
  "WinPassword": "windows_password",
  "LinuxUserName": "linux_username",
  "LinuxPrivateKey": "linux_private_key",
  "LinuxHostKeyValidation": false
}
```

Déploiement d'agents

Une fois les informations d'identification configurées et vérifiées, AWS Transform déploie des agents de réplication sur vos serveurs sources. Vous pouvez effectuer un déploiement sur tous les serveurs de la vague actuelle ou sélectionner des serveurs spécifiques.

Le processus de déploiement pour chaque serveur :

1. AWS Transform envoie des commandes de déploiement au connecteur via SSM.
2. Le connecteur récupère les informations d'identification à partir de AWS Secrets Manager.
3. Le connecteur se connecte au serveur source à l'aide des informations d'identification configurées.
4. Le connecteur vérifie que le serveur source répond à toutes les conditions requises pour exécuter l'agent de réplication.
5. Le connecteur installe et configure l'agent de réplication.
6. Le connecteur vérifie la réussite de l'installation et de la connectivité.

Vous pouvez suivre la progression du déploiement en temps réel grâce au suivi de l'état de chaque serveur, y compris l'étape d'installation en cours, le temps écoulé et le temps restant estimé. Si un serveur tombe en panne, AWS Transform affiche la raison de l'échec et propose des options de nouvelle tentative par serveur. Les serveurs déployés avec succès peuvent procéder indépendamment pendant que les serveurs défaillants sont réessayés.

Réutilisation et cycle de vie des connecteurs

Lorsque vous déployez des agents pour les vagues suivantes, vous pouvez réutiliser un connecteur existant ou en créer un nouveau. AWS Transform répertorie tous les connecteurs configurés dans votre compte, en indiquant le nom du connecteur, son état (actif ou expiré), le nombre de serveurs connectés et la date d'expiration de l'activation hybride.

- Connecteur actif : l'activation hybride est toujours valide. AWS Transform vérifie les rôles IAM pour la nouvelle vague et procède à la configuration des informations d'identification. Aucune nouvelle activation hybride n'est nécessaire.

- Connecteur expiré : l'activation hybride SSM a expiré. Les activations expirées ne peuvent pas être renouvelées. Vous devez sélectionner un autre connecteur ou en créer un nouveau.

Les activations hybrides SSM expirent au bout de 30 jours. L'activation n'est requise que pour installer le connecteur sur la machine Linux. Une fois le connecteur installé, vous pouvez continuer à l'utiliser pour installer des agents de réplication sur les serveurs sources même après l'expiration de l'activation. Si vous devez installer le connecteur sur une nouvelle machine après l'expiration de l'activation, vous devez créer un nouveau connecteur via le processus de configuration.

Installation manuelle de l'agent

Pour une installation manuelle, vous devez d'abord générer des AWS informations d'identification (temporaires ou permanentes), puis installer l'agent sur chaque serveur source.

Options de certification :

- Informations d'identification temporaires (recommandé) : créez un rôle IAM avec la politique `AWSApplicationMigrationAgentInstallationPolicy` gérée, puis utilisez-le `aws sts assume-role` pour générer des informations d'identification temporaires. Pour en savoir plus, consultez la section Autorisations d'installation de l'agent dans le guide de l'utilisateur MGN.
- Informations d'identification permanentes : créez un utilisateur IAM avec la politique `AWSApplicationMigrationAgentInstallationPolicy` gérée et générez une clé d'accès.

Étapes d'installation :

Pour les serveurs Linux, téléchargez et exécutez le programme d'installation :

```
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
```

Pour les serveurs Windows, téléchargez et exécutez le programme d'installation approprié en PowerShell tant qu'administrateur :

```
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

Le paramètre `--user-provided-id` est obligatoire. *`server-identifier`*Remplacez-la par la valeur exacte `mgn:server:user-provided-id` figurant dans la colonne de votre fichier de stock. Cet identifiant relie le serveur physique à son enregistrement de serveur source MGN.

Pour plus d'informations sur l'installation de l'agent, consultez les sections Agent Linux et Agent Windows dans le Guide de l'utilisateur MGN.

Après l'installation, AWS Transform vérifie que tous les agents sont correctement connectés en vérifiant que les serveurs affichent un état de réplication égal `INITIATING` ou`INITIAL_SYNC`.

Note

AWS Transform ne prend pas en charge la réplication sans agent MGN. Pour plus d'informations sur la réplication sans agent, consultez la section Présentation de la réplication sans agent dans le guide de l'utilisateur MGN.

Note

Vous devez installer l'agent de réplication sur tous les serveurs en une seule vague. Déconnectez et archivez les serveurs sur lesquels vous n'installez pas l'agent de réplication. Vous pouvez utiliser la `disconnect-from-service` commande pour déconnecter les serveurs et la `mark-as-archived` commande pour archiver les serveurs déconnectés. La commande d'archivage ne fonctionne que pour les serveurs sources dont l'état du cycle de vie est `DISCONNECTED` défini.

Pour les quotas liés à la réplication, consultez la section Limites de quotas de service MGN dans le Guide de l'utilisateur MGN.

Étape 4 : réplication des données

Une fois les agents de réplication installés, la réplication des données démarre automatiquement. AWS Transform utilise la réplication continue au niveau des blocs pour synchroniser les données des serveurs sources vers. AWS

Le processus de réplication comprend deux phases :

- Synchronisation initiale : copie complète des données du serveur source vers AWS. Les données sont stockées sous forme de snapshots Amazon Elastic Block Store (Amazon EBS) ou sur des volumes Amazon FSx for NetApp ONTAP (FSx for ONTAP) dans le compte cible, en fonction du type de stockage cible que vous avez configuré. Pour plus d'informations, consultez la section Type de stockage cible dans le guide de l'utilisateur MGN. La durée dépend du volume de données et de la bande passante du réseau.
- Réplication continue : synchronisation continue des blocs modifiés avec un impact minimal sur les performances du serveur source. Conserve une copie à jour dans AWS.

Les serveurs de réplication sont des instances Amazon EC2 temporaires déployées dans le sous-réseau de la zone de transit. Ils reçoivent des données répliquées depuis les serveurs sources et sont gérés automatiquement par MGN. Pour en savoir plus, consultez la section Paramètres du serveur de réplication dans le guide de l'utilisateur MGN.

AWS Transform surveille la progression de la réplication et fournit des mises à jour de statut, notamment l'état de la réplication, le décalage de réplication (différence de temps entre les données source et les données répliquées) et l'utilisation de la bande passante.

Au cours de la réplication, chaque serveur passe par les états suivants :

- Pas prêt : le serveur est en cours de synchronisation initiale et n'est pas encore prêt pour les tests.
- Prêt pour les tests : le serveur a été ajouté avec succès et la réplication des données a commencé. Les instances de test ou de basculement peuvent désormais être lancées.

Une fois que tous les serveurs de la vague ont dépassé l'`NOT_READY`état, la phase de réplication des données est terminée et vous pouvez passer aux tests.

Vous pouvez contrôler la réplication pour des serveurs individuels ou pour l'ensemble de la vague à tout moment :

- Suspendre la réplication : interrompez temporairement la réplication pour des serveurs spécifiques ou pour l'ensemble de la vague.
- Reprendre la réplication : reprend la réplication précédemment suspendue.
- Arrêter la réplication : arrête définitivement la réplication. La réplication arrêtée peut être redémarrée, mais elle recommence à partir de la synchronisation initiale.

Étape 5 : Tests

Une fois la réplication des données terminée, vous pouvez lancer des instances de test pour valider vos serveurs migrés avant d'effectuer le basculement final. Pour en savoir plus, consultez la section Lancer des instances de test dans le guide de l'utilisateur MGN. AWS Transform prend en charge deux options de test :

- Test en pleine vague : lancez des instances de test pour tous les serveurs de la vague.
- Tests sélectifs : lancez des instances de test pour des serveurs spécifiques que vous sélectionnez en fournissant leurs identifiants fournis par l'utilisateur à partir du fichier d'inventaire.

AWS Transform lance des instances Amazon EC2 à partir des données répliquées et fournit les ID d'instance afin que vous puissiez vous connecter aux instances de test et les valider. Après le test, vous pouvez :

- Procédez au passage en mode automatique si le test est réussi.
- Lancez de nouvelles instances de test pour effectuer un nouveau test.
- Mettez fin aux instances de test et corrigez tout problème avant de recommencer le test.

Étape 5b : Marquer les demandes comme étant prêtes à être transférées

Lorsque les tests sont terminés et que vous êtes satisfait des résultats, marquez vos applications comme étant prêtes à être transférées. AWS Transform examine l'état de réplication de chaque application et résout les éventuelles alertes de réplication avant de vous autoriser à poursuivre. Seules les applications dont l'état de réplication est propre peuvent être marquées pour le basculement.

Étape 6 : Découpe

Le cutover est l'étape finale de la migration vers laquelle vos charges de travail de production sont déplacées. AWS Pour en savoir plus, consultez la section Lancer des instances de basculement dans le guide de l'utilisateur MGN. Comme pour les tests, AWS Transform prend en charge la coupure complète ou la coupure sélective pour des serveurs spécifiques.

Lors de la transition, AWS Transform lance des instances Amazon EC2 à partir des dernières données répliquées et fournit les ID d'instance pour chaque serveur. Après avoir vérifié les instances de basculement, vous finalisez le basculement, ce qui arrête la réplication en cours de la machine source.

Le processus de découpage comprend les étapes suivantes :

1. Lancer des instances de basculement : AWS Transform lance des instances Amazon EC2 pour les serveurs sélectionnés. Vous pouvez choisir la coupure complète ou la coupure sélective.
2. Vérifier les instances coupées : connectez-vous aux instances lancées et vérifiez qu'elles fonctionnent correctement.
3. Finaliser le basculement : confirmez le basculement pour arrêter la réplication de la machine source. Vous pouvez finaliser tous les serveurs de la vague ou sélectionner des serveurs spécifiques. La finalisation empêche les agents de réplication d'envoyer des données, supprime les agents de réplication des serveurs sources et verrouille l'état du cycle de vie du serveur. Cette action ne peut pas être facilement annulée. Pour en savoir plus, consultez la section Finaliser le découpage dans le guide de l'utilisateur MGN.
4. Serveurs sources d'archivage (facultatif) — Une fois la finalisation terminée, vous pouvez marquer les serveurs sources comme archivés pour libérer un quota de serveurs source sur votre compte.

> **Important**
>
> La finalisation du basculement arrête la réplication en cours de la machine source. Assurez-vous d'avoir vérifié vos instances de basculement avant de finaliser.

> **Note**
>
> Un temps d'arrêt survient entre l'arrêt de la source et la disponibilité de l'instance de basculement. Planifiez votre fenêtre de découpe en conséquence.

États du cycle de vie des serveurs

Au cours de la migration, chaque serveur passe par les états de cycle de vie suivants. Pour en savoir plus, consultez la section Cycle de vie du serveur source dans le guide de l'utilisateur MGN.

- Pas prêt : le serveur est en cours de synchronisation initiale et n'est pas encore prêt pour les tests.
- Prêt pour les tests : la réplication des données a commencé et des instances de test ou de basculement peuvent être lancées.
- Test en cours : une instance de test est en cours de lancement.
- Prêt pour le basculement : le serveur a été testé et est prêt pour le basculement.
- Cutover en cours : une instance de basculement est en cours de lancement.
- Transition terminée : le serveur a été coupé. Toutes les données ont été migrées vers l'instance de AWS transfert.
- Déconnecté — Le serveur a été déconnecté de MGN.

Vous pouvez demander à AWS Transform quel est l'état de vos serveurs à tout moment pendant la migration. AWS Transform fournit un tableau d'état interactif des vagues qui affiche toutes les informations pertinentes sur les serveurs, notamment le cycle de vie de la migration, l'état de la réplication et les prochaines étapes recommandées. Vous pouvez également demander en langage naturel, par exemple :

- Quel est l'état de mes serveurs ?
- Quel est l'état de ma vague ?
- Quel est le statut de l'étape dans laquelle je me trouve actuellement ?

Pendant la migration par vagues, vous pouvez demander à AWS Transform de mettre à jour ou de modifier l'état de chaque serveur. Par exemple, si 9 des 10 serveurs de votre vague ont réussi la phase de test mais que l'un d'entre eux a échoué, vous pouvez autoriser AWS Transform à continuer à déplacer les 9 serveurs vers la phase suivante tout en relançant le test sur le serveur défaillant.

Approbations de déploiement

AWS Transform inclut des flux de travail d'approbation intégrés pour garantir que les modifications de production passent par le processus de révision de votre organisation. Lorsqu'une opération nécessite une approbation, AWS Transform achemine la demande vers les approbateurs autorisés via l'onglet Approbations. Seuls les utilisateurs ayant le rôle d'administrateur dans AWS Transform

peuvent approuver les demandes de déploiement. Les déploiements n'ont lieu qu'après réception de la confirmation.

Notes de mise à jour

Les notes de version suivantes couvrent les dernières modifications apportées àMigrations (y compris VMware). Pour obtenir la liste des modifications apportées à l'ensemble du service AWS Transform, consultez le journal des modifications. Pour les régions AWS Transform prises en charge, voir Régions prises en charge. Pour les régions cibles prises en charge, consultez la page de configuration du connecteur de compte.

Août 2026

- AWS Transform for migrations identifie désormais les règles de pare-feu entrantes non utilisées migrées depuis votre environnement sur site et suggère de les supprimer dans le cadre des recommandations réseau guidées. Cela vous permet d'éviter de reporter une exposition à la sécurité, telle que l'accès entrant ouvert, qui ne sert plus à rien. La suppression est limitée aux règles d'entrée non utilisées. En savoir plus sur les recommandations de réseau guidées.

Juillet 2026

- AWS Transform for migrations prend désormais en charge la migration d'environnements de serveurs virtuels et bare metal depuis pratiquement toutes les sources, y compris VMware et d'autres plateformes. Hyper-V Les fonctionnalités de migration, notamment la découverte, la planification de la migration, la création de zones d'atterrissage, la migration du réseau et le réhébergement des serveurs, sont disponibles quelle que soit votre infrastructure source. Le flux de travail des applications Web a été renommé de « VMware Migrations » en « Migrations (y compris VMware) ». En savoir plus sur les migrations.
- AWS Transform vous permet désormais de générer un rapport récapitulatif sur l'espace de travail au format PDF téléchargeable. Le rapport consolide les données de toutes les tâches de migration de votre espace de travail, y compris les statuts des tâches, la progression des étapes du flux de travail, la planification des vagues, la migration du réseau, la configuration de la zone d'atterrissage, la progression du réhôte et les artefacts produits. En savoir plus sur les rapports récapitulatifs sur l'espace de travail.
- L'outil de découverte AWS Transform collecte désormais des métadonnées Oracle détaillées directement à partir de vos bases de données sur VMware et sur des serveurs bare metal. Hyper-

V Vous pouvez découvrir des instances Oracle via des connexions SQL directes. L'outil collecte l'énumération de la Database/Pluggable base de données de conteneurs (CDB/PDB), l'inventaire des composants et le dimensionnement des fichiers de données. En savoir plus sur la découverte des bases de données Oracle.

- AWS Transform for migrations fournit désormais des fonctionnalités améliorées pour les actions post-lancement. Vous pouvez désormais définir des actions après le lancement au niveau du compte et les appliquer automatiquement à tous les serveurs sources, ou les personnaliser par serveur source lors de la validation de l'inventaire. Post-launch les actions automatisent les tâches de modernisation et de validation sur chaque serveur source immédiatement après son lancement en tant qu'instance de test ou de basculement. En savoir plus sur les actions à effectuer après le lancement.

juin 2026

- AWS Transform for migrations prend désormais en charge la localisation. Vous pouvez modifier la langue d'affichage de l'application Web lorsque vous utilisez des flux de migration. En savoir plus sur les paramètres de langue.
- AWS Transform vous permet désormais de configurer vos paramètres de réplication et de lancer les paramètres de votre migration. Vous pouvez définir la configuration en fonction de votre compte cible ou en fonction de serveurs sources spécifiques. En savoir plus sur les paramètres de réplication et de lancement.
- AWS Transform vous permet désormais d'associer des interfaces réseau élastiques (ENI) existantes à votre modèle de lancement. Vous pouvez identifier les ENI dans votre compte cible afin qu'ils puissent être utilisés lors du lancement des instances. En savoir plus sur le balisage des ressources réseau.
- AWS Transform for migrations prend désormais en charge toutes les régions AWS commerciales en tant que cibles de migration, à l'exception du Moyen-Orient (Bahreïn) et du Moyen-Orient (Émirats arabes unis). En savoir plus sur les régions cibles prises en charge.
- Vous pouvez désormais utiliser l'outil de découverte AWS Transform comme source de migration réseau aux côtés de ModelizeIT, permettant ainsi des migrations de réseaux hybrides pour les environnements exécutant à la fois des charges de travail VMware et non VMware. En savoir plus sur les sources d'entrée de migration réseau.

mai 2026

- AWS Transform détecte désormais les VPC existants dans votre compte cible lors de l'examen de la migration du réseau. Vous pouvez voir les VPC existants à côté de vos VPC mappés, identifier les conflits CIDR et les résoudre avant le déploiement. En savoir plus sur la détection des VPC existante.
- AWS Transform prend en charge le reformatage des référentiels de code source vers des conteneurs lors de la migration vers. AWSEn savoir plus sur la conteneurisation.
- AWS Transform peut désormais analyser l'inventaire que vous avez découvert et fournir une recommandation de stratégie de migration pour chaque serveur et chaque application. Les recommandations suivent les sept stratégies de migration (7R) standard du secteur. Chaque recommandation comprend un service AWS cible suggéré, un score de confiance et le raisonnement qui le sous-tend. En savoir plus sur les recommandations des 7R.

Avril 2026

- Ajout de la création de zones d'atterrissage directement dans les flux de migration. AWS Transform vérifie la présence d'une base existante, recommande des structures d'unités organisationnelles (OU) et des comptes cibles, et propose un déploiement automatisé ou une sortie d'infrastructure en tant que code (IaC) (formats CloudFormation AWS CDK, ou Landing Zone Accelerator (LZA)). En savoir plus sur la création de zones d'atterrissage.
- Ajout de la prise en charge du protocole DHCP avec mappage des groupes de sécurité lors de la migration du réseau. En savoir plus sur la création de groupes de sécurité.
- Vous pouvez désormais générer des diagrammes interactifs et des rapports analytiques lors de la planification de la migration. Les types de diagrammes incluent les cartes de topologie du réseau, les graphiques de dépendance des applications, les diagrammes de Gantt ondulatoires et les diagrammes généraux. Les types de rapports incluent les évaluations des risques, les recommandations 7R et les rapports analytiques personnalisés. Les sorties sont disponibles sous forme de fichiers HTML, PDF ou Microsoft PowerPoint (.pptx) interactifs. En savoir plus sur les diagrammes et les rapports de planification de la migration.

Mars 2026

- Ajout d'API publiques pour la migration du réseau, permettant aux partenaires et aux programmeurs d'accéder aux fonctionnalités de migration du réseau. Consultez la référence de l'API de migration réseau.

Février 2026

- La migration réseau prend désormais en charge l'ingestion de fichiers de configuration de pare-feu ou de Software-Defined réseau (SDN) sans nécessiter de données de découverte RVTools. Vous pouvez utiliser les fichiers de configuration du pare-feu ou du SDN indépendamment, ou les combiner avec les exportations RVTools.

janvier 2026

- Ajout de la prise en charge du balisage du programme d'accélération de la migration (MAP) et du balisage défini par l'utilisateur sur les éléments de migration du réseau, ce qui vous permet de suivre les ressources de migration à des fins de crédit MAP et d'organisation.

Décembre 2025

- Ajout d'une nouvelle expérience de migration avec un flux de travail repensé et une facilité d'utilisation améliorée. Pour plus d'informations, consultez Accélérer la migration vers VMware : la nouvelle expérience de AWS Transform.
- Ajout de la configuration réseau de l'accélérateur de zone d'atterrissage (LZA) pour la configuration automatique de la zone d'atterrissage.
- Ajout de la prise en charge de plusieurs AWS comptes cibles lors de l'exécution de la migration, ce qui vous permet de migrer les charges de travail entre les comptes.
- Ajout de la prise en charge de la migration réseau pour les formats source Cisco ACI FortiGate, Palo Alto et ModelizeIT.

Octobre 2025

- L'exécution de la migration a été étendue à 16 régions cibles avec l'ajout de l'Asie-Pacifique (Osaka).

septembre 2025

- Ajout de la prise en charge de la configuration des licences dans les vagues de réhébergement, vous permettant de spécifier Bring Your Own License (BYOL) ou des options incluses dans la licence par vague.
- Ajout de la prise en charge de Terraform dans la migration réseau, vous permettant de déployer une infrastructure réseau à l'aide de modèles Terraform.
- Ajout de la prise en charge de la mise à jour de la configuration du sous-réseau de réplication, supprimant ainsi la nécessité d'un VPC par défaut dans le compte cible.

août 2025

- Exécution étendue de la migration (migration du réseau et réhébergement) à 15 régions cibles avec l'ajout des États-Unis de l'Est (Ohio), de l'Europe (Stockholm) et de l'Europe (Irlande).
- Ajout de fonctionnalités de plage CIDR flexibles pour la migration du réseau, vous permettant de personnaliser les plages d'adresses IP lors du déploiement du réseau.

Mai 2025

- Lancement du service initial deMigrations (y compris VMware), fournissant des fonctionnalités de migration de bout en bout, notamment la découverte, l'évaluation, la planification de la migration, la migration du réseau et le réhébergement des serveurs.
- Exécution de la migration prise en charge dans 12 régions cibles : États-Unis Est (Virginie du Nord), États-Unis Ouest (Oregon), Canada (Centre), Amérique du Sud (São Paulo), Europe (Francfort), Europe (Londres), Europe (Paris), Asie-Pacifique (Mumbai), Asie-Pacifique (Séoul), Asie-Pacifique (Tokyo), Asie-Pacifique (Singapour) et Asie-Pacifique (Sydney).

Conteneurisation du code source

AWS Transform prend en charge le reformatage des applications vers des conteneurs lors de la migration vers. AWS Ce chapitre décrit les fonctionnalités d'IA agentic de AWS Transform pour automatiser la conteneurisation de votre code source. Vous pouvez migrer et vous moderniser en parallèle, réduisant ainsi le temps et la complexité liés au passage d'une architecture sur site à une architecture cloud native. Vous pouvez conteneuriser le code source à partir de GitHub fichiers Bitbucket ou .zip GitLab, générer des images Docker, publier sur Amazon Elastic Container Registry (Amazon ECR) et déployer sur Amazon Elastic Container Service (Amazon ECS) ou Amazon Elastic Kubernetes Service (Amazon EKS). La conteneurisation est ainsi intégrée au même flux de travail que celui que vous utilisez pour planifier et exécuter les migrations de réhébergement.

Capacités et fonctionnalités clés

AWS Transform offre les fonctionnalités suivantes pour conteneuriser vos applications.

- AI-driven analyse du code source. Analyse le code source de votre application et génère automatiquement des artefacts Docker, notamment des Dockerfiles et des fichiers de configuration associés. Aucune expertise Docker n'est requise.
- Création et publication d'images de conteneurs. Crée et teste automatiquement des images de conteneurs, puis les publie sur Amazon Elastic Container Registry grâce à une analyse automatique des vulnérabilités.
- L'infrastructure en tant que génération de code. Génère une infrastructure de déploiement prête pour la production pour Amazon Elastic Kubernetes Service (Helm charts) ou Amazon Elastic Container Service (modules Terraform), avec validation et analyse de sécurité automatisées. Pas besoin d'écrire IaC à partir de zéro.
- Aide privée aux personnes dépendantes. Vous pouvez éventuellement configurer AWS CodeArtifact des référentiels (Maven, PyPI, npm) et des images de base Amazon ECR privées comme sources de dépendance pour vos builds.
- Test itératif et déploiement de cutover. Déploie l'infrastructure de test à des fins de validation, puis déploie l'infrastructure finalisée pour le passage en production.

> **Note**
>
> La conteneurisation du code source est conçue pour les applications qui ne sont pas encore conteneurisées. Il nécessite l'accès au code source de votre application et ne prend pas en charge la migration des charges de travail conteneurisées existantes. Pour migrer des conteneurs existants vers AWS, utilisez des méthodes de déploiement standard pour Amazon Elastic Container Service ou Amazon Elastic Kubernetes Service.

Comment fonctionne la conteneurisation

AWS Transform fait appel à un AI-powered agent pour vous guider tout au long du processus de conteneurisation dans un flux de travail basé sur le chat. L'agent gère l'ensemble du processus, de l'analyse du code au déploiement du conteneur, réduisant ainsi à plusieurs heures les journées consacrées à la création manuelle de Dockerfile et à la configuration de l'infrastructure. AWS Transform coordonne des tâches spécialisées telles que l'analyse du code source, la génération d'images Docker et la création d'infrastructures. À des moments clés du flux de travail, vous examinez et approuvez le résultat avant de poursuivre.

Vous accédez à la conteneurisation du code source en créant une tâche de migration. Dans le cadre du job, vous pouvez exécuter la conteneurisation en tant que flux de travail autonome ou dans le cadre d'une migration de bout en bout lorsque la stratégie de migration d'une vague est définie sur la conteneurisation. Pour de plus amples informations, veuillez consulter Migrations (y compris VMware).

Conditions préalables

Avant de commencer, vérifiez que vous disposez des éléments suivants :

- Un espace de travail AWS Transform. Pour plus d'informations sur l'obtention d'un espace de travail, consultez la section Mise en route.
- Le code source de votre application se trouve dans un dépôt Git accessible via AWS CodeConnections ou compressé sous forme de fichiers zip à télécharger. Les fichiers individuels ne doivent pas dépasser 1 Go et la taille totale de l'ensemble du code source ne doit pas dépasser 8 Go.

- (Facultatif) Un référentiel Amazon ECR pour la publication d'images de conteneurs. Vous pouvez configurer l'accès à Amazon ECR ultérieurement dans le flux de travail lorsque vous serez prêt à publier.
- Pour les déploiements Amazon EKS : un cluster Amazon EKS existant ou des autorisations pour créer l'infrastructure requise.
- Pour les déploiements Amazon ECS : autorisations pour créer des clusters, des services et des ressources associées Amazon ECS à l'aide de Terraform, AWS CloudFormation ou. Cloud Development Kit AWS (AWS CDK)

Flux de travail de conteneurisation

Le flux de travail de conteneurisation comprend les étapes suivantes. L'agent AWS Transform vous guide à chaque étape de l'interface de chat.

1. the section called "Étape 1 : Avertissement de sécurité". Lisez et acceptez la clause de non-responsabilité de sécurité.
2. the section called "Étape 2 : Cloner le code source". Fournissez le code source de votre application.
3. the section called "Étape 3 : conteneuriser". Un agent IA analyse votre code et génère des artefacts Docker.
4. the section called "Étape 4 : Examiner les artefacts". Passez en revue les artefacts générés et approuvez les modifications de code.
5. the section called "Étape 5 : Publier des images". Publiez des images de conteneurs sur Amazon ECR.
6. the section called "Étape 6 : Générer du iAc". Générez des modèles de déploiement Amazon EKS ou Amazon ECS.
7. the section called "Étape 7 : Déploiement de l'infrastructure de test". Déployez et validez l'infrastructure de test.
8. the section called "Étape 8 : Nettoyer l'infrastructure de test". Détruisez les ressources de test.
9. the section called "Étape 9 : Déployer une infrastructure de transition". Déployez une infrastructure de production.

Démarrage d'une tâche de conteneurisation

Pour conteneuriser vos applications, vous devez d'abord créer une tâche de migration VMware dans votre espace de travail AWS Transform. Depuis le job, vous pouvez choisir d'exécuter un flux de conteneurisation autonome ou un flux de migration de bout en bout incluant la conteneurisation.

- Conteneurisation autonome : conteneurisez votre code source sans effectuer de migration complète vers VMware. Choisissez cette option si vous souhaitez conteneuriser des applications indépendamment de toute migration d'infrastructure.
- End-to-end migration avec conteneurisation : exécutez le flux de migration complet de VMware avec une stratégie de migration conteneurisée affectée à une ou plusieurs vagues. Le flux de travail de conteneurisation s'exécute dans le cadre de la migration de ces vagues. Pour plus d'informations sur la migration vers VMware, consultezMigrations (y compris VMware).

Pour démarrer une tâche de conteneurisation

1. Sur la page d'accueil de votre espace de travail, choisissez Créer une offre d'emploi.
2. Choisissez VMware Migration.
3. Choisissez d'exécuter un flux de conteneurisation autonome ou un flux de migration de bout en bout incluant la conteneurisation.
4. AWS Transform vous guide tout au long des étapes du flux de travail, en commençant parthe section called “Étape 1 : Avertissement de sécurité”.

Autorisations de conteneurisation

Au cours du flux de travail de conteneurisation, AWS Transform déploie sur vous un rôle IAM Compte AWS qui permet de créer des images de conteneur et de déployer une infrastructure. Il vous est demandé de vérifier et d'approuver la création de ce rôle avant que le flux de travail ne se poursuive.

Le rôle est nommé `AWSTransformCodeBuildExecutionRole` et est déployé par le biais d'une AWS CloudFormation pile. Il inclut les politiques gérées suivantes.

Politique de base

Fournit des autorisations de base pour le flux de travail de conteneurisation :

- Amazon S3 — Lecture et écriture d'objets dans des `aws-transform-*` compartiments
- Amazon ECR — Authentifier, extraire des images (étiquetées avec`Project: atx-migration`) et envoyer des images vers des référentiels étiquetés avec `CreatedBy: AWSTransform`
- AWS CodeArtifact — Lisez les référentiels marqués avec`Project: atx-migration`, listez les référentiels, obtenez des jetons d'autorisation et lisez les points de terminaison des référentiels. Ces autorisations prennent en charge à la fois la résolution des dépendances publiques et les sources de dépendances privées configurées pendant le flux de travail.
- Amazon CloudWatch Logs : créez des groupes de journaux et des flux, et rédigez des événements de journal pour les groupes de journaux Amazon ECS
- AWS KMS — Décrire et déchiffrer les clés (limité à Amazon S3 via les conditions de service)
- Amazon EC2 — Création et gestion d'interfaces réseau pour des projets VPC-enabled
- AWS CodeConnections — Utilisez des connexions pour accéder aux référentiels de code source via l'ARN configuré CodeConnections

Politique de mise en réseau

Gère les ressources réseau pour les applications déployées :

- Elastic Load Balancing — Créez, décrivez et gérez des équilibreurs de charge, des groupes cibles, des écouteurs et des règles (étiquetés avec) `CreatedBy: AWSTransform`
- Route 53 — Création et gestion de zones hébergées et d'enregistrements DNS
- AWS Cloud Map — Créez et gérez des espaces de noms et des services pour la découverte de services (étiqueté avec`CreatedBy: AWSTransform`)

Politique de stockage

Gère les ressources de stockage pour les applications déployées :

- Amazon S3 — Créez et gérez des compartiments, notamment en matière de chiffrement, de gestion des versions, de cycle de vie et de politiques d'accès
- Amazon EFS — Création et gestion de systèmes de fichiers, de cibles de montage et de points d'accès (étiquetés avec`CreatedBy: AWSTransform`)
- Amazon EBS — Créez et gérez des volumes et des instantanés (étiquetés avec) `CreatedBy: AWSTransform`

AWS KMS policy

Gère les opérations liées aux clés de chiffrement :

- Décrire les clés, répertorier les alias et lire les politiques relatives aux clés
- Chiffrer, déchiffrer et générer des clés de données (dans le cadre d'Amazon Logs CloudWatch , Amazon EFS, Amazon EC2 et Amazon S3 via les conditions de service)

Politique Amazon ECS

Gère les ressources Amazon Elastic Container Service pour les déploiements de conteneurs :

- Création et gestion de clusters, de services et de définitions de tâches (étiquetés avec`CreatedBy: AWSTransform`)
- Enregistrer et désenregistrer les définitions de tâches, exécuter des tâches
- Transférer des rôles IAM aux tâches et services Amazon ECS
- Lire les informations sur le rôle IAM et les certificats ACM
- Décrire les VPC, les sous-réseaux, les groupes de sécurité et les interfaces réseau Amazon EC2

Politique Amazon EKS

Gère les ressources Amazon Elastic Kubernetes Service pour les déploiements de Kubernetes :

- Accédez à l'API Kubernetes, décrivez les clusters et listez les modules complémentaires
- Transférer des rôles IAM à Amazon EKS

> **Note**
>
> Toutes les autorisations sont limitées à votre Compte AWS et. Région AWS Les ressources créées par AWS Transform sont étiquetées avec`CreatedBy: AWSTransform`, et les opérations d'écriture sont limitées aux ressources portant cette balise, le cas échéant.

Étape 1 : Consultez la clause de non-responsabilité relative à la sécurité

Avant le début du processus de conteneurisation, AWS Transform présente une clause de sécurité que vous devez consulter et accepter.

Ce que couvre la clause de non-responsabilité

Le processus de conteneurisation nécessite un accès à Internet pour télécharger les dépendances des applications (telles que les packages provenant de registres publics tels que npm, PyPI ou Maven Central). La clause de sécurité vous informe que :

- Les environnements de génération disposeront d'un accès Internet sortant pour résoudre et télécharger les dépendances spécifiées dans la configuration de compilation de votre application.
- Il vous incombe de vérifier les dépendances requises par votre application et de vous assurer qu'elles sont conformes aux politiques de sécurité de votre entreprise.
- Vous pouvez éventuellement configurer des sources de dépendance privées (telles que AWS CodeArtifact des référentiels ou des images de base Amazon ECR privées) ultérieurement pour éviter le téléchargement depuis des registres publics.

Ce que vous devez faire

Pour consulter et accepter la clause de non-responsabilité en matière de sécurité

1. Lisez l'avertissement de sécurité présenté par AWS Transform.
2. Acceptez la clause de non-responsabilité pour poursuivre le flux de travail de conteneurisation.

Après avoir accepté la clause de non-responsabilité, AWS Transform passe à l'étape suivante où vous fournissez votre code source.

> **Note**
>
> La configuration du connecteur pour AWS CodeConnections Amazon ECR n'est plus requise dès le départ. AWS Transform vous invite à configurer l'accès à ces services ultérieurement dans le flux de travail, uniquement lorsque cela est nécessaire. Par exemple, vous configurez

le CodeConnections moment où vous choisissez de cloner à partir de référentiels Git, et vous configurez l'accès Amazon ECR lorsque vous êtes prêt à publier des images de conteneur.

Étape 2 : Cloner le code source

Au cours de cette étape, vous devez fournir le code source de votre application à AWS Transform. Vous pouvez fournir du code source à partir des référentiels Git ou en téléchargeant des fichiers zip.

Option 1 : référentiels Git

Vous pouvez fournir votre code source à partir des référentiels Git. Si vous n'avez pas encore configuré AWS CodeConnections, AWS Transform vous invite à fournir votre CodeConnections ARN à ce stade. Vous pouvez spécifier vos référentiels de deux manières :

- Télécharger un fichier CSV — Préparez un fichier CSV avec des colonnes `repo_name` et`branch`. Ils `repo_name` doivent être au `owner/repo-name` format. La `branch` colonne est facultative ; laissez-la vide pour utiliser la branche par défaut du dépôt. Exemple :

```
repo_name,branch
owner/my-app,main
owner/api-service,develop
owner/another-repo,
```

- Fournissez les détails du référentiel dans le chat : indiquez à AWS Transform le ou les noms des branches du référentiel directement dans le chat au lieu de télécharger un fichier CSV.

AWS Transform vérifie que chaque référentiel existe et est accessible via votre CodeConnections configuration, puis clone les référentiels.

> **Note**
>
> Les fichiers individuels ne doivent pas dépasser 1 Go et la taille totale de tous les référentiels ne doit pas dépasser 8 Go. AWS Transformez des clones plusieurs référentiels simultanément pour accélérer le traitement.

> **Important**
>
> Les applications qui s'étendent sur plusieurs référentiels ne sont pas prises en charge par l'option Git clone. Si votre application nécessite du code source provenant de plusieurs référentiels, regroupez-les sous forme de fichier zip et utilisez plutôt l'option de téléchargement zip.

Option 2 : téléchargement du fichier zip

Si vous n'avez pas configuré CodeConnections ou si vous préférez télécharger directement votre code source, vous pouvez télécharger des fichiers zip.

Pour télécharger le code source sous forme de fichiers zip

1. Lorsque vous y êtes invité, chargez un fichier zip par application. Vous pouvez faire glisser des fichiers dans le chat ou utiliser le bouton de pièce jointe.
2. Chaque fichier zip doit contenir le code source d'une application.
3. Les fichiers individuels ne doivent pas dépasser 1 Go et la taille totale de tous les téléchargements ne doit pas dépasser 8 Go.

Facultatif : configurer les dépendances privées

Si votre application dépend de packages provenant de registres privés, vous pouvez configurer des sources de dépendances privées au cours de cette étape. AWS Transform prend en charge les types de dépendances privées suivants :

- AWS CodeArtifact référentiels — Configurez les référentiels Maven, PyPI ou npm hébergés dans. AWS CodeArtifact AWS Transform présente une liste des référentiels disponibles dans votre compte parmi lesquels vous pouvez sélectionner.
- Images de base Amazon ECR privées : si vos Dockerfiles utilisent des images de base provenant d'un référentiel Amazon ECR privé, fournissez les détails du référentiel afin que l'environnement de création puisse extraire ces images.

Lorsque vous configurez des dépendances privées, AWS Transform vous invite à vous connecter à l' Compte AWS endroit où ces ressources sont hébergées. Cette configuration de connecteur n'est requise que si vous utilisez des dépendances privées.

Confirmation des préférences de conteneurisation

Une fois que votre code source est disponible, AWS Transform vous demande si vous avez des instructions spécifiques sur la manière dont la conteneurisation doit être effectuée. Vous pouvez éventuellement spécifier :

- Qu'il s'agisse de générer un nouveau Dockerfile ou de réutiliser un Dockerfile existant.
- Qu'il s'agisse de traiter un service spécifique dans un monorepo ou tous les services.
- Toute autre préférence pour le processus de conteneurisation.

Les valeurs par défaut sont les suivantes :

1. Utilisez l'image de base Amazon Linux 2023 (`public.ecr.aws/amazonlinux/amazonlinux:latest`).
2. Traitez toutes les demandes du référentiel.
3. Réutilisez un Dockerfile existant s'il est présent, avec des modifications mineures si nécessaire.

Vous pouvez confirmer que vous souhaitez continuer avec les valeurs par défaut ou fournir des instructions spécifiques.

Étape 3 : conteneuriser

Au cours de cette étape, l'agent AWS Transform AI analyse le code source de votre application et génère des artefacts Docker. AWS Transform examine la structure, les dépendances et les exigences d'exécution de votre application afin de produire les Dockerfiles appropriés et les fichiers de configuration associés.

Que se passe-t-il lors de la conteneurisation

L'agent de conteneurisation exécute les tâches suivantes :

1. Analyse du code source : AWS Transform examine les fichiers de projet, les dépendances, la configuration de build et les exigences d'exécution de votre application. AWS Transform remplace également les valeurs codées en dur (telles que les adresses IP de base de données ou les noms DNS), identifie les variables d'environnement, détecte les volumes et tente de rediriger les journaux vers la sortie standard.

2. Génération de Dockerfile — Sur la base de l'analyse, AWS Transform génère un Dockerfile adapté à votre application.
3. Création et test de l'image du conteneur — AWS Transform crée l'image du conteneur et exécute un test pour vérifier que le Dockerfile produit une image fonctionnelle. Si la compilation échoue, AWS Transform itère automatiquement sur le Dockerfile.
4. Analyse de sécurité : AWS Transform analyse les artefacts générés à la recherche de valeurs codées en dur telles que des informations d'identification, des clés d'API ou d'autres données sensibles, et signale les résultats pour examen.

Si vous avez fourni plusieurs référentiels ou un monorepo avec plusieurs services, chaque service est traité en parallèle.

Types d'applications pris en charge

AWS Transform prend en charge la conteneurisation des types d'applications suivants :

- .NET 7 et versions ultérieures : conteneurisation optimisée pour les applications .NET exécutées sur la version 7 ou ultérieure.
- Applications générales — Conteneurisation pour les applications créées avec n'importe quel langage ou framework, y compris Java, Python Node.js, Go, etc.
- Applications non prises en charge : Windows, Xcode ou tout autre environnement de construction propriétaire ne sont pas pris en charge.

Ce que vous devez faire

Cette étape s'exécute automatiquement. AWS Transform affiche les mises à jour de progression lors de l'analyse et de la conteneurisation de chaque application. Si AWS Transform rencontre des problèmes, elle peut vous demander des éclaircissements ou des informations supplémentaires.

Lorsque la conteneurisation est terminée, AWS Transform passe à l'étape suivante où vous passez en revue les artefacts générés. Les sorties sont enregistrées dans l'Artifact Store.

Étape 4 : examiner les artefacts Docker et les modifications de code

Au cours de cette étape, vous passez en revue les artefacts Docker et les modifications de code générées par AWS Transform lors de la conteneurisation.

Révision des modifications apportées par les référentiels Git

Si vous avez fourni du code source à partir de référentiels Git, AWS Transform valide les modifications de conteneurisation dans une nouvelle branche de chaque référentiel. Si vous disposez de plusieurs référentiels, AWS Transform présente toutes les modifications sous forme de lot pour une révision consolidée.

Pour examiner et approuver les modifications

1. Passez en revue les liens de différence de code fournis par AWS Transform. Chaque différence montre tous les fichiers ajoutés ou modifiés, y compris les Dockerfiles, les fichiers de configuration et les modifications du code source.
2. Lorsque AWS Transform présente la boîte de dialogue d'approbation, approuvez ou rejetez les modifications. Pour plusieurs référentiels, vous approuvez toutes les modifications en une seule opération par lots.
3. Si vous approuvez, AWS Transform transmet les modifications aux nouvelles branches de vos référentiels.
4. Confirmez que vous êtes prêt à passer à l'étape suivante.

Révision des modifications apportées à la suite de téléchargements au format zip

Si vous avez chargé le code source sous forme de fichiers zip, AWS Transform fournit des liens de téléchargement pour les artefacts conteneurisés. Téléchargez et examinez les artefacts, y compris les Dockerfiles générés et toute modification du code source.

Demande de modifications

Si les artefacts générés doivent être modifiés, vous pouvez fournir des commentaires à AWS Transform, redémarre l'étape de conteneurisation avec vos instructions mises à jour et génère de nouveaux artefacts pour votre examen.

Étape 5 : Publier des images

Au cours de cette étape, AWS Transform publie les images de vos conteneurs sur Amazon Elastic Container Registry. Si vous n'avez pas encore configuré l'accès à Amazon ECR, AWS Transform vous invite à fournir les détails de votre référentiel Amazon ECR à ce stade.

Que se passe-t-il lors de la publication

AWS Transform exécute les tâches suivantes pour chaque image de conteneur :

1. Configuration du connecteur — Si vous n'avez pas encore configuré l'accès à Amazon ECR, AWS Transform présente un formulaire de connecteur dans lequel vous fournissez l'ARN de votre référentiel Amazon ECR et vous connectez à votre. Compte AWS
2. Demande d'approbation — AWS Transform présente la liste des images à publier et demande votre approbation. Vous pouvez approuver ou rejeter l'opération de publication.
3. Image push — Après approbation, AWS Transform publie les images du conteneur dans votre référentiel Amazon ECR à l'aide de. Si vous disposez de plusieurs services, AWS Transform publie toutes les images en une seule opération par lots.
4. Analyse des vulnérabilités : Amazon ECR analyse automatiquement les images publiées pour détecter les vulnérabilités connues. AWS Transform rapporte les résultats de l'analyse. Pour une analyse plus complète, activez le scan amélioré AWS ECR et la surveillance du temps AWS GuardDuty d'exécution.

> **Note**
>
> La publication d'images s'exécute de manière asynchrone à l'aide de. Si votre session est interrompue pendant la publication, AWS Transform rétablit automatiquement l'opération lorsque vous vous reconnectez.

Ce que vous devez faire

- Consultez la liste des images à publier.
- Approuver ou rejeter l'opération de publication. Si vous refusez, AWS Transform ignore la publication d'images et vous pouvez passer à l'étape suivante sans publier d'images.
- Passez en revue les résultats de l'analyse des vulnérabilités une fois la publication terminée.

Après la publication, AWS Transform fournit les URI d'image qui sont utilisés dans les étapes de déploiement de l'infrastructure.

Étape 6 : Génération de l'infrastructure sous forme de code

Au cours de cette étape, AWS Transform génère AWS des modèles d'infrastructure pour le déploiement de votre application conteneurisée. Vous avez le choix entre Amazon Elastic Kubernetes Service et Amazon Elastic Container Service comme plate-forme cible.

Amazon Elastic Kubernetes Service (Kubernetes)

Si vous choisissez Amazon EKS, AWS Transform génère des diagrammes Helm avec des manifestes Kubernetes pour votre application. Les modèles générés incluent :

- Déploiements et services
- Règles d'entrée
- ConfigMaps et SecretProviderClass ressources
- Comptes de service
- Réclamations de volume persistantes (EBS et EFS)
- Route 53 enregistrements DNS
- Configurations du bilan de santé

Facultatif : CloudWatch journalisation

AWS Transform vous demande si vous souhaitez inclure la CloudWatch journalisation pour votre déploiement Amazon EKS. Si vous vous y inscrivez, AWS Transform génère une DaemonSet configuration Fluent Bit qui collecte les journaux des pods et les envoie à CloudWatch Logs.

Si vous choisissez la CloudWatch journalisation, votre administrateur de cluster doit remplir les conditions préalables suivantes avant le déploiement :

1. Créez l'`amazon-cloudwatch`espace de noms dans le cluster.
2. Créez un rôle IAM pour le compte de service Fluent Bit avec CloudWatch les autorisations d'écriture des journaux. Vous êtes invité à saisir l'ARN du rôle lors du déploiement.

Amazon Elastic Container Service (Terraform)

Si vous choisissez Amazon ECS, AWS Transform génère des modules Terraform pour déployer votre application. Les modèles générés incluent :

- Cluster ECS
- Service ECS avec définitions de tâches
- Application Load Balancer avec journalisation des accès
- Amazon EFS pour le stockage persistant
- Zones hébergées privées pour la découverte de services
- Configurations du bilan de santé

Validation et analyse de sécurité automatisées

AWS Transform valide automatiquement les modèles d'infrastructure générés avant de vous les présenter. La validation consiste à :

- Pour Terraform : `terraform fmt` et pour vérifier l'exactitude `terraform validate` de la syntaxe et de la configuration.
- Pour Helm : validation du graphique pour vérifier que les manifestes générés sont bien formés.
- Analyse de sécurité à l'aide de Checkov pour identifier les erreurs de configuration de sécurité potentielles dans le code d'infrastructure généré.

AWS Transform signale tous les problèmes de validation et les résout avant de poursuivre.

Génération d'iAc sans images publiées

Vous pouvez générer des modèles d'infrastructure même si vous n'avez pas publié d'images de conteneur à l'étape précédente. Les modèles générés utilisent des URI d'image fictifs que vous pouvez mettre à jour ultérieurement avec l'emplacement réel de vos images.

Ce que vous devez faire

Pour générer des modèles d'infrastructure

1. Lorsque vous y êtes invité, choisissez votre plate-forme cible : Amazon EKS ou Amazon ECS.

2. Si vous avez choisi Amazon EKS, AWS Transform vous demande si vous souhaitez inclure la CloudWatch journalisation. Répondez par oui ou par non.
3. Si vous y êtes invité, fournissez les détails du point de terminaison de vérification de l'état de votre application (par exemple, un `/health` chemin).
4. AWS Transform génère et valide les modèles d'infrastructure. Cette étape s'exécute automatiquement et AWS Transform affiche les mises à jour de progression, y compris les résultats de validation ou d'analyse de sécurité.
5. Passez en revue les modèles générés lorsque AWS Transform les présente.

Étape 7 : Déploiement de l'infrastructure de test

Au cours de cette étape, AWS Transform déploie une infrastructure de test afin que vous puissiez valider votre application conteneurisée avant le passage à la production.

Que se passe-t-il pendant le déploiement des tests

AWS Transform déploie les modèles d'infrastructure générés à l'étape précédente sur votre Compte AWS. Pour les déploiements Amazon EKS, Helm est utilisé. Pour les déploiements Amazon ECS, Terraform est utilisé.

Avant le déploiement, AWS Transform présente un formulaire de valeurs d'infrastructure dans lequel vous pouvez configurer les paramètres de déploiement tels que les noms des ressources, le nombre de répliques et les paramètres spécifiques à l'environnement. AWS Transform génère également un aperçu du déploiement qui indique les ressources qui seront créées, afin que vous puissiez examiner les modifications avant de les approuver.

Ce que vous devez faire

Pour déployer et valider l'infrastructure de test

1. Complétez le formulaire sur les valeurs de l'infrastructure avec votre configuration de déploiement. Le formulaire inclut des paramètres tels que les noms de clusters, les espaces de noms, le nombre de répliques et d'autres paramètres spécifiques à l'environnement.
2. Consultez l'aperçu du déploiement qui indique les ressources qui seront créées ou modifiées.
3. Approuvez le déploiement de l'infrastructure lorsque AWS Transform le demande.
4. Attendez que le déploiement soit terminé. AWS Transform affiche les résultats du déploiement.

5. Testez votre application déployée pour vérifier qu'elle s'exécute correctement dans un conteneur et que l'infrastructure répond à vos exigences.
6. Indiquez à AWS Transform si vous êtes satisfait du déploiement ou si vous souhaitez modifier l'infrastructure et la redéployer.

Itérer sur l'infrastructure

Si vous devez modifier les modèles d'infrastructure, vous pouvez télécharger des modèles mis à jour et les redéployer :

1. Dites à AWS Transform que vous souhaitez modifier l'iAc.
2. Téléchargez un fichier zip contenant vos modèles d'infrastructure modifiés.
3. AWS Transform remplace les modèles et effectue une mise à jour incrémentielle (Terraform apply ou Helm upgrade).
4. Passez en revue les résultats de déploiement mis à jour.

Vous pouvez répéter ce cycle jusqu'à ce que vous soyez satisfait du déploiement.

Récupération de session

Les déploiements d'infrastructure s'exécutent de manière asynchrone à l'aide de. Si votre session est interrompue pendant un déploiement, AWS Transform rétablit automatiquement l'opération lorsque vous vous reconnectez et affiche les résultats du déploiement.

Étape 8 : Nettoyer l'infrastructure de test

Une fois la validation terminée, AWS Transform démonte l'infrastructure de test pour éviter des coûts inutiles.

Ce que vous devez faire

Pour nettoyer l'infrastructure de test

1. AWS Transform vous informe que l'infrastructure de test va être démolie.
2. Approuvez l'opération de destruction lorsque AWS Transform le demande.

3. Attendez que le nettoyage soit terminé. AWS Transform affiche les résultats lorsque toutes les ressources de test ont été supprimées.

Pour les déploiements Amazon ECS, cette étape supprime toutes les ressources créées lors du déploiement de test, notamment les ressources de calcul, les équilibreurs de charge, le stockage et les composants réseau.

Pour les déploiements Amazon EKS, le nettoyage est défini par étiquette en fonction de votre projet spécifique. Seules les ressources étiquetées pour ce flux de travail de conteneurisation sont supprimées. Les autres charges de travail exécutées sur le même cluster Amazon EKS ne sont pas affectées.

Étape 9 : Déployer une infrastructure de transition

Au cours de cette dernière étape, AWS Transform déploie l'infrastructure finalisée pour une utilisation en production. Le déploiement de transition utilise les mêmes modèles d'infrastructure que ceux que vous avez validés lors de l'étape de déploiement de test.

Ce que vous devez faire

Pour déployer une infrastructure de transition

1. Complétez le formulaire des valeurs d'infrastructure avec votre configuration de déploiement en production. Vous pouvez ajuster les paramètres à partir du déploiement du test ou utiliser les mêmes valeurs.
2. Consultez l'aperçu du déploiement qui indique les ressources de production qui seront créées.
3. Approuvez le déploiement de production lorsque AWS Transform le demande.
4. Attendez que le déploiement soit terminé. AWS Transform affiche les résultats du déploiement de la transition.
5. Vérifiez que votre application fonctionne correctement dans l'environnement de production.

> **Important**
>
> Passez en revue les configurations d'infrastructure générées avec votre équipe pour vous assurer qu'elles répondent aux exigences de sécurité, de conformité et commerciales de votre entreprise. Bien que AWS Transform fournisse des recommandations de configuration

automatisées, vous êtes chargé de valider et d'ajuster les paramètres en fonction de vos besoins avant de procéder au déploiement du transfert.

Restauration de session

Les déploiements de production s'exécutent de manière asynchrone à l'aide de. Si votre session est interrompue pendant le déploiement, AWS Transform rétablit automatiquement l'opération lorsque vous vous reconnectez et affiche les résultats du déploiement.

Modernisation des applications mainframe

AWS Transform est conçu pour accélérer la modernisation des applications mainframe existantes. Il orchestre l'analyse des bases de code du mainframe, génère de la documentation, extrait la logique métier, décompose les structures monolithiques, transforme le code existant et gère le parcours global avec des intrants humains (HITL) en cas de besoin. Les fonctionnalités de transformation de AWS Transform pour la modernisation et la migration des applications mainframe vous permettent de moderniser plus rapidement vos applications mainframe critiques, tout en préservant la logique critique de votre entreprise tout au long du processus de transformation.

Rubriques

Capacités et fonctionnalités clés

AWS Transform fournit les fonctionnalités suivantes pour la modernisation du mainframe :

- Prend en charge la modernisation des applications z/OS mainframe écrites en COBOL (Common Business-Oriented Language) et PL/I (Programming Language One) avec les transactions JCL (Job Control Language), CICS (Customer Information Control System), les écrans BMS (Basic Mapping Support), les bases de données DB2 et les fichiers de données VSAM (Virtual Storage Access Method) associés.
- Prend en charge la refactorisation des applications mainframe Fujitsu GS21 avec les fichiers de données PSAM (Presentation Service Access Method), les jeux de caractères japonais et les fichiers de données NDB (base de données réseau).
- Effectue un raisonnement, une analyse, une décomposition, une planification, une génération de documentation et une refactorisation du code axés sur les objectifs.

- Refactorise automatiquement les charges de travail COBOL-based du mainframe en applications Java modernes optimisées pour le cloud.
- Orchestre et intègre parfaitement les outils sous-jacents qui exécutent l'analyse, la documentation, la décomposition, la planification et le refactoring du code.
- Vous aide à configurer des environnements cloud pour des applications mainframe modernisées en fournissant des modèles d'infrastructure en tant que code (IaC) prêts à l'emploi.

High-level procédure pas à pas

Voici une présentation détaillée de AWS Transform pour la modernisation et la migration des applications mainframe.

1. Démarrez une discussion avec AWS Transform et saisissez un objectif.
2. En fonction de votre objectif, AWS Transform propose un plan de modernisation, en divisant l'objectif de haut niveau en étapes intermédiaires.
3. En fonction de l'objectif que vous avez défini, AWS Transform peut :
   - Évaluez et réimaginez la base de code
   - Créez un travail personnalisé en fonction de l'objectif

En cours de route, AWS Transform peut vous demander des informations pour exécuter les tâches.

> **Note**
>
> Pour plus d'informations sur les fonctionnalités de AWS Transform for mainframe refactor, voir Créer un projet dans la documentation AWS Transform for mainframe refactor.

L'humain dans la boucle (HITL)

Tout au long de la transformation des applications mainframe, vous pouvez suivre la progression et le statut des tâches de transformation grâce à l'expérience Web AWS Transform.

AWS Transform collectera des informations supplémentaires auprès de vous dans les scénarios suivants :

- Lorsque des informations supplémentaires sont nécessaires pour exécuter des tâches.

- Lorsque l'approbation est requise pour les artefacts intermédiaires (par exemple, la décomposition des domaines ou la planification des vagues).
- Lorsque des problèmes surviennent que AWS Transform ne peut pas résoudre automatiquement.

Types de fichiers pris en charge pour la transformation d'applications mainframe

Les types de fichiers pris en charge z/OS sont les suivants :

- Artefacts COBOL et CPY (Copybooks) associés
- PL/I fichiers source
- JCL (Job Control Language) et procédure JCL (PROC)
- Définition du système CICS (CSD)
- BMS (Support de cartographie de base)
- Bases de données DB2
- VSAM (méthode d'accès au stockage virtuel)
- IMS TM (gestionnaire de transactions)

Les types de fichiers pris en charge pour Fujitsu GS21 sont les suivants :

- PSAM (méthode d'accès au service de présentation)
- ADL (langage de définition AIM)
- NDB (base de données réseau)

Pour plus d'informations sur le Fujitsu GS21, consultez les rubriques suivantes dans le guide de migration de AWS Transform for mainframe :

- GS21
- Capture et rediffusion - Terminaux GS21
- Mainframe, AS400, Open VMS et GS21

Régions prises en charge et quotas pour AWS Transformez le mainframe

Pour obtenir la liste des régions prises en charge, consultezRégions prises en charge pour AWS Transform.

> **Note**
>
> Vos données peuvent être traitées dans une région différente de celle dans laquelle vous utilisez AWS Transform. Pour plus d'informations sur le traitement interrégional, voirthe section called “Cross-region traitement”.

Pour les limites de quotas, voirQuotas.

High-level vue d'ensemble du parcours de modernisation des ordinateurs centraux

La modernisation des applications mainframe s' AWS effectue généralement en quatre phases : (a) évaluation, (b) mobilisation, (c) migration et modernisation, et (d) exploitation, optimisation et innovation. Chacune de ces phases est décrite plus en détail avec les objectifs et les activités associées pour soutenir votre parcours de modernisation.

Phases

- Phase 1 : Évaluation
- Phase 2 : Mobiliser
- Phase 3 : Migrer et moderniser
- Phase 4 : Exploiter, optimiser et innover

Phase 1 : Évaluation

Objectif : comprendre votre état de préparation à la modernisation et élaborer des plans de modernisation initiaux.

Avec AWS Transform, vous pouvez évaluer les applications, l'infrastructure et les opérations de votre mainframe afin de déterminer l'approche de modernisation adaptée aux besoins de votre entreprise.

> **Note**
>
> Chaque phase contient une liste de toutes les activités possibles que vous pouvez effectuer lors de la modernisation de votre application mainframe. Vous pouvez ignorer certaines activités qui ne correspondent pas à votre cas d'utilisation ou à vos objectifs.

Activités

- Commencez par une conversation informelle sur la modernisation et travaillez sur la qualification des opportunités en recrutant les bonnes personnes dans la salle
- Déterminer la qualification des opportunités
- Faites une présentation au premier appel avec le plan de mappage des dépendances des applications et l'architecture de l'application
- Déterminez le ROM (ordre de grandeur approximatif) qui inclut le coût de l'infrastructure pendant la migration, le travail de migration, les coûts de post-production et la durée du projet
- Détection rapide du portefeuille :
  - Réaliser une évaluation des modèles et du guidage des outils
  - Effectuez une analyse du code source
  - Identifier les candidats à la preuve de concept (POC)
- Créez une formation d'habilitation technique :
  - Journées d'immersion
  - Ateliers sur des sujets généraux
- Créez un rapport d'évaluation de l'état de préparation à la migration (MRA) pour les grands projets de modernisation du mainframe ou pour les nouveaux clients AWS
- Créer un cahier des charges pour la phase de mobilisation

Phase 2 : Mobiliser

Objectif : établir les bases et valider l'approche grâce à une preuve de concept réussie ou à des modernisations pilotes.

Avec la phase de mobilisation, vous pouvez établir les cadres, les outils et les processus nécessaires pour soutenir la modernisation du mainframe à grande échelle.

Activités

- Lancez le plan de modernisation avec un pilote et le POC identifié :
  - Analyser le projet pilote et configurer le code de modernisation
  - Créez et testez les données modernisées du pilote
  - Fournissez des résultats et passez en revue le projet pilote afin de créer une solution détaillée pour une modernisation des données à plus grande échelle
- Pour la plateforme :
  - Créez un plan de sécurité, de conformité et de surveillance
  - Configuration d'environnements de zone d'atterrissage avec zone d'atterrissage sur AWS ordinateur central et structure de compte
  - Déterminez l'architecture, l'infrastructure, l'application, l'intégration, etc.
- Pensez aux personnes et aux processus :
  - Le centre d'excellence du cloud est une bonne ressource
  - Modèle de fonctionnement
- Créez une analyse complète du portefeuille pour différents scénarios d'application :
  - Découverte complète incluant une documentation de haut niveau
  - Plan de décomposition (pour toutes les applications)
  - Guide des modèles et des outils pour toutes les applications
  - Élaborez un plan initial de modernisation et de migration
- Créez une solution détaillée prenant en compte le pilote, la plateforme, les personnes et les processus, ainsi qu'une analyse complète du portefeuille
- Déterminer l'analyse de rentabilisation
- Compléter avec succès le projet pilote avec solution pour le cahier des charges de la phase suivante

Phase 3 : Migrer et moderniser

Objectif : mener à bien la modernisation et la migration dans les délais et le budget prévus.

Au cours de cette phase, vous pouvez migrer et moderniser vos applications et données mainframe vers AWS.

Activités

- Allouez des ressources au code d'application prêt pour la production
- Réviser et analyser la conception à l'aide de la documentation existante ou en interrogeant des experts en la matière (PME)
- Définissez des scénarios de test
- Configurez des environnements de modernisation avec des environnements d'exécution, des bases de données et des logiciels tiers appropriés
- Migrez et modernisez le code source et les données :
  - Vous pouvez moderniser votre application de manière itérative en fonction des domaines commerciaux de la base de code de l'application.
  - Adaptez les environnements de modernisation selon les besoins pour prendre en charge vos charges de travail de modernisation
- Établir un pipeline CI/CD (intégration continue, livraison continue)
- Migrez les charges de travail sélectionnées pour lancer votre modernisation.
- Transférez les programmes d'application et ajustez le dimensionnement de l'environnement selon les besoins :
  - Vous pouvez augmenter ou diminuer les environnements en fonction de vos besoins
  - Modernisez les packages de travail en exécutant des tests de cohérence du code
  - Resynchronisez avec le code source si nécessaire
- Effectuez des tests complets et vérifiez votre migration :
  - Collectez les données d'état initiales
  - Enregistrez les scénarios de test sur le mainframe
  - Environnement de scène, application et données
  - Exécutez des scénarios de test sur le cloud
  - Comparez les résultats des tests source et cible
  - Créez des pipelines d'exécution de scénarios de test automatisés
  - Génération de KPI et de rapports
- Validez vos données pour la configuration de la production
- Validez votre progression en :
  - Exécution de tests d'intégration et de système
  - Exécution de tests de performance

  - Exécution de tests d'acceptation par les utilisateurs
  - HA/DR Tests en cours
- Définissez un plan de déploiement avec le propriétaire de l'application et créez un plan de formation et de transfert de connaissances
- Tenez compte de la transition et exécutez les interruptions de production
- Mettre en place un support soutenu pour les activités de post-production telles que les opérations, la surveillance, la planification des capacités et la garantie des fonctions des applications

Phase 4 : Exploiter, optimiser et innover

Objectif : Soutenir l'excellence opérationnelle et l'amélioration continue des applications modernisées.

Après la modernisation, vous pouvez optimiser les performances, la sécurité et les coûts de vos applications tout en tirant parti AWS des services pour innover.

Activités

- Application de surveillance pour :
  - Métriques de performances
  - Pratiques de sécurité
  - Directives de conformité
  - Coûts
- Détails de journalisation
- Gérez les opérations des applications :
  - Gestion de l'infrastructure
  - Transactions et gestion des tâches
  - Support de l'environnement d'exécution
- Optimisation et modernisation des applications
- Développement et maintenance d'applications :
  - IDE de codage
  - Génération
  - Integration
  - Test

- Déploiement

Transformation des applications mainframe

AWS Transform accélère la transformation de vos applications de modernisation de mainframe. Cette rubrique décrit les fonctionnalités disponibles.

Rubriques

Prérequis : préparer les entrées du projet dans S3

AWS Transform est capable de gérer des bases de code complexes pour mainframe. Pour utiliser la base de code, assurez-vous de disposer de tous les actifs dans votre emplacement S3.

Principaux apports du projet :

- Code source : vous devez télécharger les fichiers de code source de votre mainframe sur S3. Cela inclut les programmes COBOL, les scripts JCL, les copybooks et tout autre fichier source pertinent.
- Fichiers de données : si vous possédez des fichiers VSAM ou d'autres fichiers de données utilisés par vos applications mainframe, ceux-ci doivent être téléchargés vers S3.
- Fichiers de configuration : incluez les fichiers de configuration spécifiques à votre environnement mainframe.

Autres contributions au projet

- Enregistrements SMF (System Management Facility) : le cas échéant, téléchargez les enregistrements SMF dans un nouveau dossier du compartiment S3 où le code source est stocké. Ces enregistrements doivent être au format de fichier .zip.
- Formatage : pour la génération de documentation technique, vous pouvez utiliser un fichier de configuration facultatif pour générer des documents PDF conformes aux formats et normes requis, notamment les en-têtes, les pieds de page, les logos et les informations personnalisées.
- Glossaire : AWS Transform AWS Transform tire parti de l'automatisation grâce à l'IA générative pour la génération de documentation et l'extraction de règles métier. L'inclusion d'un fichier CSV de glossaire contenant des informations sur les abréviations et terminologies importantes dans le répertoire racine de votre fichier zip contribuera à améliorer la qualité de la documentation générée.
- Données de test : si disponibles, téléchargez des ensembles de données de test qui peuvent être utilisés pour valider l'application modernisée. Ces données doivent être stockées dans un nouveau dossier du compartiment S3 où le code source est stocké.

Les détails sur les contributions au projet peuvent être trouvés ici.

Collection d'artefacts provenant des sources du mainframe

Cette rubrique décrit le processus de collecte du code source du mainframe et des artefacts associés afin de soutenir les initiatives de modernisation du mainframe à l'aide AWS de Transform. La collecte et la préparation appropriées des artefacts sources sont essentielles à la réussite de l'analyse, de la planification de la migration et de la mise en œuvre.

Inventaire du code source

Types de code source des applications

Les types de code source d'application suivants sont pris en charge :

- Programmes COBOL
- Scripts JCL
- Programmes d'assemblage
- PL/I programmes
- Transactions CICS
- Programmes naturels
- Scripts REXX

- Programmes Easytrieve
- Copybooks et inclusions
- Bibliothèques Proc

Ressources de base de données

Les actifs de base de données suivants sont pris en charge :

- Scripts DB2 DCLGEN et DDL
- Définitions de base de données IMS (PSB et DBD)
- Définitions de fichiers VSAM
- Schémas de base de données physiques et logiques
- Procédures et déclencheurs de base de données

Extensions de fichiers de code source

Si vous n'êtes pas sûr de l'extension, laissez-la vide ou .txt et AWS Transform la classera pour vous.

Le tableau suivant répertorie les extensions de fichier courantes pour les artefacts sources du mainframe.

Extensions de fichiers de code source du mainframe

Language/Type	Extensions courantes	Description
COBOL	.cbl, .cob, .cobol	Programmes source COBOL
JCL	.jcl	Scripts du langage Job Control
Assembleur	.asm	Programmes en langage assembleur
PL/I	.pl1	PL/I programmes de langue
Définition du CICS	.csd	Définition du système CICS (CSD)
Naturel	.nat	Programmes naturels
REXX	.rex, .rexx	Scripts REXX

Language/Type	Extensions courantes	Description
Easy Trieve	.ezt	Programmes de rapports Easytrieve
Cahiers	.copie	cahiers COBOL
BMS	.bms	Support cartographique de base (BMS)
PL/I cahiers	.pl1_copie	PL/I cahiers
DB2 DCLGEN	.dcl	Générateur de déclarations DB2
Définition de DB2	.sql, .ddl	Définitions de base de données DB2
Définition IMS	.ims	Ensemble de données de définition des ressources IMS (IMS Stage 1)
MFS	.mfs	IMS MFS (service de formatage des messages)
PSB	.psb	IMS PSB (bloc de spécification du programme)
DBD	.dbd	Définitions des données IMS
Procédé JCL	.prc, .proc	Bibliothèques de procédures JCL
JCL inclut	.inc	JCL Inclure des fichiers
Macros	.mac	Macros d'assemblage
Cartes de contrôle	.ctl	Cartes de contrôle JCL Utility

Méthodes de collecte

Extraction du code source

Utilisez des clients FTP sécurisés (WinSCP/FileZilla) pour l'extraction interactive du code source à partir des bibliothèques PDS du mainframe.

Extraction du schéma DB2

Le logiciel client DB2 LUW (Linux, UNIX et Windows) inclut l'`db2look`utilitaire dans son package d'installation. L'`db2look`utilitaire extrait les instructions DDL (Data Definition Language) d'une base de données DB2.

Exécutez la commande suivante :

```
db2look -d DATABASE_NAME -i userid -w password -a -e -m -l -x -f -createdb -printdbcfg
 -o DATABASE_NAME.sql
```

La liste suivante décrit les paramètres :

- `-d` *`DATABASE_NAME`*: Spécifie le nom de la base de données dont le schéma doit être extrait
- `-i` *`userid`*: ID utilisateur pour l'authentification de la base de données
- `-w` *`password`*: mot de passe pour l'authentification de base de données
- `-a`: Extrait les informations d'autorisation (subventions)
- `-e`: extrait tous les objets de base de données (tables, vues, index, etc.)
- `-m`: Extrait les statistiques et les caractéristiques physiques
- `-l`: extrait les commentaires des tables et des colonnes
- `-x`: Des extraits expliquent les tableaux
- `-f`: Formate la sortie pour une meilleure lisibilité
- `-createdb`: inclut les instructions de création de base de données
- `-printdbcfg`: inclut les paramètres de configuration de base de données
- `-o` *`DATABASE_NAME`*`.sql`: Spécifie le nom du fichier de sortie

Extraction des informations de catalogue depuis le mainframe

La commande LISTCAT dans IDCAMS est un utilitaire permettant de récupérer les informations du catalogue concernant les ensembles de données sur le mainframe. Cela est utile lors des projets de modernisation du mainframe pour inventorier les ensembles de données et comprendre leurs caractéristiques.

```
//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
/*
```

Extraire les définitions du CICS

L'utilitaire IBM-provided DFHCSDUP peut extraire les définitions de ressources CICS du fichier CSD (CICS System Definition).

Utilisez le JCL suivant pour décharger les définitions existantes du 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
/*
```

Extraction de définitions IMS

Pour extraire les définitions IMS, vous pouvez générer le fichier de transaction IMS à l'aide de l'utilitaire DFSURDD0. Cet utilitaire crée des instructions de macro de phase 1 que vous pouvez utiliser à des fins de migration. Seul IMS Stage 1 est actuellement pris en charge.

Utilisez le JCL suivant pour extraire les définitions 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
/*
```

Extraction des informations du CA-7 planificateur

CA-7 les informations relatives aux horaires de travail sont incluses dans les rapports LJOB. Utilisez l'utilitaire LJOB avec le `LIST=NODD` paramètre pour générer les rapports sur le mainframe. Les rapports doivent avoir une `.ca7` extension. Chaque rapport doit comporter des caractères de contrôle de chariot ANSI dans la colonne 1. Vous pouvez créer un rapport avec des caractères de commande de chariot dans la colonne 1 en spécifiant `DCB=RECFM=FBA` (ou FA) dans la JCL utilisée pour exécuter l'utilitaire LJOB.

Par exemple : `LJOB,JOB=ZBN*,LIST=ALL`

Pour plus d'informations, consultez la documentation de Broadcom.

Extraction de données SMF

Les enregistrements du System Management Facility (SMF) fournissent les mesures d'activité utilisées par AWS Transform pour analyser l'utilisation des tâches par lots et des transactions CICS. Les types d'enregistrement SMF suivants sont pris en charge : 14, 15, 30 (sous-type 5), 64, 102, 110 (sous-type 1 avec classes de données 1, 3 et 4).

Exigences de format pour les enregistrements SMF :

- Doit inclure les types d'enregistrement 30 et 110 (au minimum)

- Doit être au format binaire brut EBCDIC avec des octets RDW (Record Descriptor Word) inclus
- Doit être fourni sous l'une des formes suivantes :
  - Un fichier jusqu'à 600 Mo compressé au format .zip
  - Un fichier jusqu'à 5 Go compressé au format .tar.gz ou .gz
- Doit être stocké dans un dossier distinct de votre code source dans Amazon S3

Fournissez au moins 13 mois d'enregistrements SMF pour capturer les cycles de lots annuels et les modèles saisonniers susceptibles de ne pas être pris en compte sur des périodes plus courtes.

Option 1 : Extraire et trier les enregistrements SMF

Utilisez l'exemple de JCL suivant pour extraire et trier les enregistrements 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
/*
```

Personnalisez les valeurs suivantes dans la JCL précédente :

1. Job card : Mettre à jour le compte, la classe et le msgclass
2. DUMPIN : pointez vers vos ensembles de données SMF
3. DUMPOUT : Spécifiez le nom du jeu de données en sortie et le HLQ
4. TYPE : Sélectionnez les types d'enregistrement (14, 15, 30, 110 ou autres)
5. DATE : Format yyyy/ddd (par exemple 2026/055,2026/056)
6. ESPACE : Ajustez en fonction du volume de données attendu
7. Supprimer l'étape de tri si elle n'est pas nécessaire

Option 2 : Extraire les données SMF avec DFSORT

Vous pouvez utiliser DFSORT pour consolider et rapporter les données SMF historiques. Cela est utile si vous stockez vos enregistrements SMF dans un GDG par jour ou par semaine. La tâche

suivante utilise DFSORT pour consolider les enregistrements SMF du fichier SORTIN et filtrer en fonction des enregistrements spécifiés dans le paramètre 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')
```

Pour télécharger les données tout en conservant les données RDW, vous pouvez utiliser un serveur FTP pour recevoir le fichier extrait. Assurez-vous que les données sont transférées au format binaire et que l'option RDW est utilisée afin que le RDW soit inclus dans le transfert de données. La tâche suivante montre un exemple de tâche FTP pour transférer ce fichier.

```
//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
```

Téléchargement du rapport SCRT

Vous pouvez également télécharger un Sub-Capacity rapport d'outil de reporting (SCRT) dans AWS Transform.

Téléchargement de l'inventaire des applications

Après avoir collecté tous les artefacts, procédez comme suit :

1. Organisez les fichiers en sous-dossiers par type d'artefact (par exemple, /cobol, /jcl, /copybooks, /db2, /ims, /cics, /ca7).
2. Compressez le dossier de premier niveau dans un seul fichier .zip.
3. Téléchargez le fichier .zip dans le compartiment Amazon S3 connecté à votre espace de travail AWS Transform.

> **Note**
>
> Les enregistrements SMF doivent être placés dans un dossier distinct de votre code source dans le compartiment Amazon S3 et doivent être au format .tar.gz ou .gz.

Pour obtenir des instructions détaillées sur la connexion de votre compartiment Amazon S3 à AWS Transform, consultezthe section called “Configuration d'un connecteur”.

Sign-in et créez un emploi

Pour vous connecter à l'expérience Web AWS Transform, suivez toutes les instructions de la Démarrage avec AWS Transformation section de la documentation.

Pour créer et démarrer une tâche : suivez les étapes décrites dans Démarrer votre projet.

Créer un espace de travail : nommez et décrivez votre espace de travail dans lequel les emplois, les collaborateurs et les artefacts associés seront stockés.

Créer un travail : créez un travail en le sélectionnant parmi des plans de travail préconfigurés, ou personnalisez le plan de travail en fonction de votre objectif en le sélectionnant dans la liste des fonctionnalités prises en charge.

> **Important**
>
> AWS Transform refusera les opérations de votre part si vous ne disposez pas des autorisations appropriées. Par exemple, un contributeur ne peut pas annuler une tâche de transformation d'applications mainframe ou supprimer une tâche. Seul un administrateur peut exécuter ces fonctions.

Lorsque vous créez votre tâche, vous pouvez sélectionner l'une des fonctionnalités ci-dessous, mais l'étape de lancement est toujours requise car c'est là que se trouve le code source du projet. Lors de la première tâche configurée dans un espace de travail, vous devez configurer un connecteur pour votre compartiment Amazon S3.

Suivi de la progression de la transformation

Vous pouvez suivre la progression de la transformation tout au long du processus de deux manières :

- Journal de travail : il fournit un journal détaillé des actions entreprises par AWS Transform, ainsi que des demandes d'intervention humaine et de vos réponses à ces demandes.
- Tableau de bord : il fournit un résumé de haut niveau de la transformation des applications mainframe. Il présente des indicateurs sur le nombre de tâches transformées, les transformations appliquées et le temps estimé pour terminer la transformation des applications mainframe. Vous pouvez également consulter les détails de chaque étape, notamment les lignes de code par type de fichier, la documentation générée par chaque type de fichier, le code décomposé et le plan de migration.

Configuration d'un connecteur

AWS Transform utilise un connecteur pour accéder aux ressources de votre compte nécessaires aux fonctions de modernisation du mainframe. Votre connecteur est automatiquement configuré avec le premier job que vous exécutez dans l'espace de travail. En fonction du plan de travail que vous choisissez, AWS Transform vous guide pour créer votre connecteur.

Connecteur Mainframe Reimagine

Le connecteur de réimagination du mainframe est destiné aux tâches qui exécutent l'évaluation et la refonte des flux de travail. Il utilise un compartiment S3 pour accéder aux ressources de

transformation et les stocker, ainsi qu'un cluster Amazon Neptune pour stocker les artefacts extraits. Le cluster Neptune sert de graphe de connaissances unifié qui stocke tous les artefacts extraits concernant votre travail, et le graphe de connaissances répond à toutes les questions de l'interface de discussion AWS Transform.

Déployez le cluster Amazon Neptune dans un VPC où AWS Transform peut créer des interfaces réseau élastiques (ENI). Il s'agit des connexions réseau qui permettent à AWS Transform de communiquer en toute sécurité avec Neptune dans votre VPC pour charger des données et interroger votre graphe de connaissances.

AWS CloudFormation

Nous vous recommandons d'utiliser le CloudFormation modèle suivant pour créer les ressources nécessaires à votre connecteur Mainframe Reimagine. Utilisez le même compartiment S3 que celui que vous prévoyez d'utiliser pour le connecteur lors de l'exécution du CloudFormation modèle. Pour plus d'informations sur l'utilisation CloudFormation des modèles, consultez la section Utilisation des modèles.

Pour télécharger le CloudFormation modèle, choisissez neptune-kg-setup.yaml.

Le modèle accepte les paramètres suivants :

- BucketName : obligatoire. Nom du compartiment S3 pour l'accès au chargeur en vrac Neptune. Vous devez utiliser le même compartiment S3 que celui que vous prévoyez d'utiliser dans votre connecteur AWS Transform.
- KmsKeyId : facultatif. Clé KMS pour le chiffrement Neptune. Accepte l'ID de clé, l'ARN, le nom d'alias ou l'ARN d'alias. La valeur par défaut est la clé AWS gérée si elle est omise.

Fournissez les informations suivantes lorsque vous configurez votre connecteur :

- ARN de compartiment S3
- ARN du cluster Neptune
- ID de ressource du cluster Neptune
- ID de sous-réseau d'applications
- ID du groupe de sécurité de l'application
- ARN du rôle de chargeur en vrac Neptune S3

> **Important**
>
> L'onglet Sorties du CloudFormation modèle inclut les informations que vous devez fournir à AWS Transform lors de la configuration du connecteur.

Configuration personnalisée

Si vous préférez utiliser un VPC existant ou d'autres outils pour créer l'infrastructure requise, votre environnement doit répondre aux exigences suivantes :

Cluster Neptune

- Amazon Neptune Serverless avec moteur version 1.4.5.1 ou ultérieure
  - Authentification IAM activée
  - Chiffrement du stockage activé (cléAWS gérée ou clé KMS gérée par le client)
- Configuration de dimensionnement sans serveur (recommandée : 1 à 128 NCU)
- (Recommandé) Lisez la réplique dans une deuxième zone de disponibilité pour une haute disponibilité et des performances de lecture améliorées

Réseaux

- Un VPC avec support DNS et noms d'hôte DNS activés
- Au moins deux sous-réseaux dans des zones de disponibilité distinctes. AWS Transform crée des ENI dans ces sous-réseaux pour accéder au cluster Neptune, qui peut résider dans les mêmes sous-réseaux ou dans des sous-réseaux dédiés. Dimensionnez les sous-réseaux à /20 pour s'adapter aux ENI des points de terminaison et des applications VPC.
- Connectivité réseau entre les sous-réseaux et les AWS services suivants via les points de terminaison AWS PrivateLink de l'interface VPC () :
  - AWS API Transform Agents : coordonne les tâches de modernisation du mainframe
  - Amazon Bedrock Runtime — Invoque des modèles de base pour l'analyse et le raisonnement
  - Amazon Relational Database Service (Amazon RDS) — Gestion de clusters Neptune
  - Amazon Elastic Compute Cloud (Amazon EC2) — Gestion des ENI
  - Amazon CloudWatch — Des métriques pour AWS transformer l'observabilité

- Point de terminaison de passerelle S3 attaché aux tables de routage associées à vos sous-réseaux. AWS Transform utilise ce point de terminaison pour charger les données du compartiment S3 vers le cluster Neptune.

Groupes de sécurité

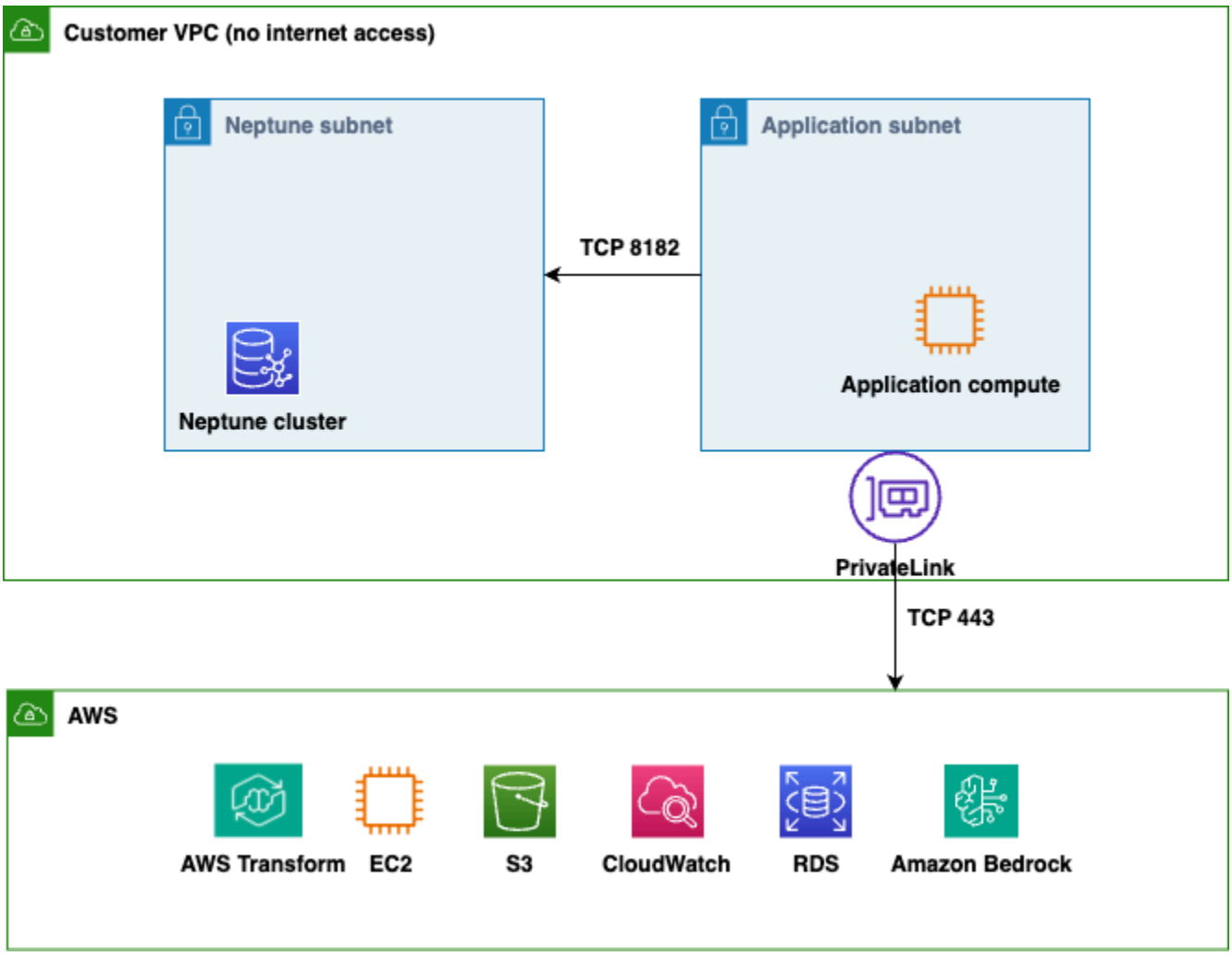
Les groupes de sécurité sont attachés aux ENI, et non aux sous-réseaux. Même lorsque AWS Transform ENI et Neptune résident dans le même sous-réseau, des groupes de sécurité distincts contrôlent l'accès entre eux.

- Un groupe de sécurité (attaché aux ENI créés par AWS Transform) qui permet :
  - TCP 8182 sortant vers le groupe de sécurité Neptune
  - TCP 443 sortant pour atteindre les points de terminaison VPC
- Un groupe de sécurité (attaché au cluster Neptune) qui permet de :
  - TCP 8182 entrant depuis le groupe de sécurité de l'application
- Un groupe de sécurité du point de terminaison VPC (attaché aux ENI du point de terminaison de l'interface) qui permet :
  - TCP 443 entrant depuis le groupe de sécurité de l'application

IAM

- Un rôle IAM avec une politique de confiance `rds.amazonaws.com` qui accorde `s3:GetObjects3:ListBucket`, et `s3:GetBucketLocation` sur votre compartiment S3
- Ce rôle doit être associé au cluster Neptune pour le chargement en bloc de données du Knowledge Graph

Le schéma suivant montre l'architecture recommandée.



Connecteur S3

Pour les tâches avec un plan personnalisé, AWS Transform peut utiliser un connecteur S3. Le connecteur S3 utilise un compartiment S3 pour accéder aux ressources de transformation et les stocker, et un compartiment vectoriel S3 pour les sorties indexées.

> **Important**
>
> Vos données sont stockées et conservées dans le magasin d'artefacts AWS Transform de votre espace de travail et ne sont utilisées que pour exécuter la tâche.

Configuration optionnelle du compartiment vectoriel S3.

Dans les régions où les compartiments vectoriels S3 sont disponibles, AWS Transform stockera les codages vectoriels consultables des résultats des tâches dans ce compartiment vectoriel S3 de votre compte afin de fournir une expérience de recherche et de chat basée sur l'IA. Les données ne sont pas utilisées en dehors de cette tâche et ne sont pas utilisées pour entraîner des modèles. Pour activer cela, vous devez créer et fournir un compartiment vectoriel S3. AWS Transform crée et attache automatiquement un rôle avec les autorisations requises pour écrire dans ce compartiment.

Autorisations CORS du compartiment S3

Une fois votre connecteur configuré, ajoutez la politique CORS suivante à votre compartiment S3 afin de pouvoir visualiser et comparer les artefacts directement dans la console AWS Transform. Si cette politique n'est pas correctement configurée, vous ne pourrez peut-être pas utiliser les fonctionnalités de visualisation en ligne ou de comparaison de fichiers 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
    }
]
```

Évaluez et réimaginez le plan de travail

Le plan de travail Assess and reimagine est un flux de travail prédéfini pour moderniser les applications mainframe. Il vous guide à travers deux phases : évaluer votre base de code pour

identifier les fonctions commerciales et réinventer les fonctions que vous sélectionnez. Pour choisir plutôt des capacités individuelles, utilisez le plan de travail personnalisé.

Évaluation

Les processus de modernisation du mainframe commencent généralement par l'évaluation de la base de code afin d'identifier le contenu et de comprendre les relations et les dépendances. Après cette évaluation, vous pouvez commencer à décomposer et à sélectionner des parties du code source à moderniser. Les limites de la décomposition sont déterminées en fonction des fonctions commerciales.

Le catalogue des fonctions métiers décompose votre base de code en fonctions métiers distinctes, qui reposent sur des chemins de données déterministes qui cartographient chaque fonction métier du début à la fin. Un chemin de données est le chemin emprunté par les données, en commençant par un déclencheur métier jusqu'à l'écriture finale dans le code du mainframe. Plutôt que de limiter l'analyse à un point d'entrée unique, le système couvre les tâches par lots, les transactions CICS et leurs banques de données partagées afin d'identifier des unités de travail commerciales cohérentes.

Une fonction commerciale est un ensemble de travaux qui commence par un déclencheur commercial et se termine par un résultat commercial mesurable. AWS Transform fournit un catalogue de fonctions commerciales sur lesquelles un secteur d'activité peut agir, ce qui permet de prendre des décisions éclairées sur ce qu'il convient de moderniser en premier lieu.

Avantages de l'évaluation de votre base de code pour la moderniser à l'aide de fonctions métiers :

- Full-estate visibilité — Découvrez comment vos tâches par lots, vos transactions en ligne et vos magasins de données se connectent à des fonctions utiles pour votre entreprise.
- Limites réalisables — Chaque fonction commerciale identifiée est une unité autonome que les parties prenantes de votre secteur d'activité peuvent examiner et prioriser dans le cadre des efforts de modernisation.
- Cohérence entre le code et la spécification — Les mêmes blocs de code qui définissent une fonction métier sont utilisés pour générer ses spécifications, sans aucune couche de traduction ni aucun rapprochement requis.
- Temps de découverte réduit : la détection automatisée remplace des mois d'entretiens manuels sur les connaissances tribales par des analyses systématiques et reproductibles.

Résultats de l'évaluation fournis via le chat

Les résultats de l'évaluation fournis par le biais du chat incluent une liste des fonctions commerciales, y compris le nombre de chemins de données, l'étendue de chaque fonction en termes de transactions par lots et CICS, ainsi qu'une description de l'entreprise. Un lien vous est fourni vers les artefacts générés dans le compartiment Amazon S3, et vous pouvez également y accéder via le chat. Deux artefacts sont fournis : les détails des fonctions commerciales et le résumé des fonctions commerciales.

- Résumé des fonctions métiers : fournit une liste des fonctions métiers et une description en langage naturel des fonctions exécutées par les éléments du code.
- Détails des fonctions métiers : fournit un graphique interactif illustrant les relations entre les différents éléments du code source.

Pour interagir avec le graphique, sélectionnez un élément pour afficher des détails supplémentaires à son sujet, ou ouvrez un élément pour en examiner les détails. Chaque page contient un résumé de tous les éléments de ce niveau et une interface graphique permettant d'interagir avec chaque composant et d'en savoir plus sur chacun d'entre eux, notamment les éléments suivants :

- Fonction commerciale — Décrit les fonctions commerciales connectées les unes aux autres et fournit une vue d'ensemble de chaque fonction commerciale. Lorsque vous sélectionnez une fonction commerciale, les informations suivantes sont fournies :
  - Nombre de chemins de données
  - Nombre de lignes de code
  - Description de l'entreprise : aperçu de la fonction métier qui décrit, en langage naturel, les fonctions exécutées par les éléments du code.
  - Interfaces : détaille les relations entre les éléments de données de la fonction métier (par exemple, échange ou écriture).
- Détails des fonctions commerciales : décrit les connexions entre les chemins de données au sein d'une même fonction commerciale, ce qui vous permet d'approfondir la composition de la fonction commerciale. Lorsque vous sélectionnez un élément, vous voyez comment cet élément est connecté à l'ensemble de la fonction métier, ainsi que les détails suivants :
  - Banque de données : rédacteurs et lecteurs pour la banque de données.
  - Autres éléments : un aperçu du chemin de données associé qui décrit, en langage naturel, les actions et les résultats traités dans le chemin de données, une liste de programmes, de lecteurs et de rédacteurs.

- Chemins de données — Décrit les détails d'un chemin de données et la façon dont les éléments du chemin de données sont liés les uns aux autres.
  - Description : une vue d'ensemble du chemin de données qui décrit, en langage naturel, les actions et les résultats traités dans le chemin de données.
  - Contenu du chemin de données :
    - Point d'entrée
    - Lectures
    - Écritures
    - Programmes

Grâce au chat, vous pouvez interroger les résultats pour comprendre les éléments contenus dans chaque fonction commerciale et explorer les limites à l'aide du graphique des fonctions commerciales.

Une fois que vous avez identifié les limites de votre modernisation, le chat vous invite à sélectionner les fonctions commerciales que vous souhaitez réinventer. Vous pouvez sélectionner une ou plusieurs fonctions commerciales. AWS Transform envoie les limites sélectionnées et les résultats d'évaluation requis au flux de réimagination afin de poursuivre le processus de modernisation.

Une fois votre première modernisation terminée, vous pouvez utiliser le chat pour sélectionner un ensemble supplémentaire de fonctions commerciales à moderniser.

Réinventez

Au cours de la phase de refonte, vous pouvez sélectionner une ou toutes les fonctions métier identifiées par l'évaluation et les préparer à la modernisation. Cela déclenche l'extraction de la logique métier suivie de la génération d'exigences pour les fonctions commerciales sélectionnées. Les exigences générées constituent le principal élément d'entrée de l'ingénierie avancée, traduisant la compréhension du système existant en une spécification précise de ce que l'application modernisée doit fournir.

Extraire la logique métier

Une fois que vous avez sélectionné une ou plusieurs fonctions métier, AWS Transform commence à générer une logique métier pour les fonctions métier sélectionnées. Une fois l'extraction terminée, AWS Transform stocke les résultats dans un compartiment Amazon S3 au format JSON pour une utilisation en aval. Vous pouvez suivre la progression de l'extraction et examiner les éventuels problèmes directement dans la console AWS Transform.

Pour consulter les résultats de l'extraction de la logique métier

1. Dans le volet de navigation de gauche, choisissez l'étape Extraire la logique métier pour la développer.
2. Consultez les informations suivantes à partir des détails de l'étape :
   - Lien vers le compartiment S3 : emplacement où les résultats de la logique métier extraits sont stockés au format JSON.
   - Problèmes : liste de tous les problèmes rencontrés au cours du processus d'extraction de la logique métier.

Si des fichiers ont rencontré des problèmes lors de l'extraction, les informations suivantes sont affichées pour chaque fichier concerné :

- Nom du fichier : nom du fichier qui a rencontré un problème.
- Type de fichier : type du fichier (par exemple, COBOL ou JCL).
- Chemin du fichier : emplacement du fichier dans votre application.
- État : état actuel de l'extraction du fichier.
- Détails : description du problème rencontré.

> **Note**
>
> Une fois l'étape d'extraction terminée, AWS Transform commence automatiquement à générer des exigences. Aucune saisie supplémentaire ne vous est demandée avant le début de ce processus.

Générer des exigences

Une fois l'extraction de la logique métier terminée, l'agent Generate Requirements consomme les artefacts extraits (analyse du code, analyse des données, règles métier) et produit des exigences de modernisation. Ces exigences sont des spécifications fonctionnelles formelles qui sont indépendantes de la technologie et incluent des critères d'acceptation testables. AWS Transform produit un `requirements.md` fichier pour chaque fonction métier que vous sélectionnez et stocke le résultat dans un compartiment Amazon S3. Pour afficher l'emplacement de la sortie sur Amazon S3, choisissez l'étape Generate requirements.

Chaque `requirements.md` fichier est organisé selon les parties suivantes :

- Titre : nomme la fonction métier et le flux de travail qu'elle représente.
- Conditions préalables globales : conditions qui doivent rester vraies tout au long du flux de travail avant et pendant le traitement. Les valeurs configurables apparaissent sous forme d'espaces réservés aux paramètres.
- Sections de flux de travail numérotées : chaque section représente une étape distincte de la fonction commerciale. Chaque section contient les éléments suivants :
  - Une histoire utilisateur qui définit l'objectif en tant que rôle, l'action que ce rôle souhaite entreprendre et le résultat qui en résulte.
  - Une liste des exigences au format EARS (Easy Approach to Requirements Syntax), chacune avec un identifiant unique.

> **Note**
>
> La sélection d'un deuxième ensemble de fonctions métiers relance l'étape de réinvention des fonctions nouvellement sélectionnées. La console affiche ensuite les résultats uniquement pour la nouvelle sélection, de sorte que tout problème lié aux règles métier de vos fonctions commerciales précédentes et aux liens Amazon S3 qui stockent les résultats correspondant à la logique et aux exigences métier ne sont plus affichés. Vos sorties précédentes ne sont pas perdues. Vous pouvez toujours y accéder depuis l'onglet Artifacts ou dans votre compartiment Amazon S3.

Traçabilité entre les artefacts de transformation

AWS Transform assure la traçabilité entre les artefacts générés tout au long du flux de travail d'évaluation et de refonte. La traçabilité vous permet de relier chaque exigence à vos règles métier extraites ou directement au code source d'origine qui a produit l'exigence.

Vous pouvez consulter tous les détails de traçabilité pour chaque fonction commerciale à l'aide du `traceability.yaml` fichier. Il décrit comment chaque règle métier correspond à une exigence.

Pour une traçabilité interactive, vous pouvez utiliser le plugin IDE dans les éditeurs compatibles avec VS Code et Open VSX. Pour plus d'informations, consultez la section Outils pour développeurs.

Réinventez le plan d'emploi

Pour les applications dont la modernisation est prévue et que vous êtes prête à repenser, vous pouvez exécuter une tâche de refonte autonome. La tâche analyse votre code et vos données, extrait la logique métier, identifie les domaines commerciaux et génère des exigences de modernisation pour chaque domaine d'activité.

Plan de travail personnalisé

Un plan de travail personnalisé vous permet de créer votre propre flux de travail de modernisation en sélectionnant les fonctionnalités que vous souhaitez exécuter. Il vous donne un contrôle total sur les fonctionnalités incluses. Choisissez parmi les fonctionnalités suivantes en fonction de votre objectif de modernisation. Certaines fonctionnalités dépendent de l'exécution préalable d'autres fonctionnalités. Par exemple, l'analyse du code est requise pour la plupart des autres fonctionnalités.

Analyser le code

Une fois que vous avez partagé le chemin du compartiment Amazon S3 avec AWS Transform, celui-ci analysera le code de chaque fichier avec des détails tels que le nom du fichier, le type de fichier, les lignes de code et leurs chemins.

> **Note**
>
> Vous pouvez télécharger les résultats du code Analyser via l'onglet artefacts au niveau de la tâche ou de l'espace de travail. Au niveau de la tâche, cliquez sur l'option « Artifacts » dans le menu de navigation de gauche et ouvrez le dossier « résultats », ou au niveau de l'espace de travail, recherchez le nom de la tâche et ouvrez le dossier « résultats ». Cela téléchargera un fichier zip contenant le fichier de classification pour le flux de travail de classification manuel, la liste des actifs, le fichier JSON des dépendances et la liste des fichiers manquants.

Dans le plan de travail, sélectionnez Analyser le code dans le volet de navigation de gauche pour afficher vos résultats. Vous pouvez consulter les résultats de votre analyse de code de plusieurs manières :

- Affichage de liste — Tous les fichiers du compartiment Amazon S3 que vous souhaitez transformer pour le mainframe

- Affichage du type de fichier : tous les fichiers du compartiment Amazon S3 sont affichés par type de fichier. Pour obtenir la liste des types de fichiers pris en charge, consultez la section Fichiers pris en charge.
- Vue des dossiers : tous les fichiers du compartiment Amazon S3 sont affichés dans une structure de dossiers.

Dans les résultats du fichier, AWS Transform fournit les informations suivantes en fonction de la vue de fichier que vous choisissez :

- Nom
- Type de fichier
- Nombre total de lignes de code
- Chemin d'accès du fichier
- Lignes de commentaires
- Lignes vides
- Lignes de code efficaces
- Nombre de fichiers
- Complexité cyclomatique - La complexité cyclomatique représente le nombre de chemins linéairement indépendants à travers le code source d'un programme. AWS Transform affichera une complexité cyclomatique pour chacun des fichiers.

Fichiers manquants : fichiers manquants lors de l'analyse du code de modernisation du mainframe. Idéalement, ces fichiers devraient être ajoutés en tant que partie de l'entrée source dans le compartiment Amazon S3, et l'étape d'analyse devrait être réexécutée pour obtenir des résultats meilleurs et cohérents.

Nom identique — AWS Transform fournit une liste de fichiers portant le même nom et éventuellement les mêmes caractéristiques (par exemple, le nombre de lignes de code). Il ne sera pas en mesure de comparer la différence entre le contenu de deux fichiers à la fois.

Identifiants dupliqués — Avec le programme Cobol, le champ Program ID sert d'identifiant unique du fichier. Cet identifiant doit être unique car il est utilisé pour appeler le programme tout au long de votre projet. Cependant, certains projets peuvent comporter des fichiers COBOL portant des noms différents mais portant le même identifiant de programme. L'obtention de la liste de ces fichiers lors de l'évaluation peut aider à comprendre les dépendances entre tous les programmes.

> **Note**
>
> Ceci est spécifique au code et aux fichiers COBOL.

Lorsque vous avez des programmes avec des identifiants dupliqués, il est suggéré de modifier les identifiants de programme de ces fichiers afin d'avoir un identifiant unique pour chacun d'entre eux dans le code COBOL. Vous pouvez ensuite réexécuter votre tâche pour obtenir des résultats d'analyse de code plus précis et plus complets.

En résolvant les identifiants de programme dupliqués, vous pouvez :

- Améliorez la clarté et la maintenabilité du code
- Réduisez les conflits potentiels lors des appels de programmes
- Améliorez la précision du mappage des dépendances
- Simplifier les futurs efforts de modernisation

Problèmes liés à la base de code : problèmes potentiels détectés dans la base de code que vous devez résoudre avant de poursuivre le projet de modernisation. Ces problèmes peuvent inclure des références manquantes avec des instructions associées ou des liens non pris en charge dans le code.

Mettre à jour la classification : avec la reclassification manuelle, vous pouvez reclasser des fichiers à l'aide de la fonctionnalité de mise à jour groupée en chargeant le fichier JSON contenant la nouvelle classification.

> **Important**
>
> Ceci n'est disponible que pour les `TXT` fichiers `UNKNOWN` et.

Après la reclassification, AWS Transform va :

1. Met à jour les résultats du classement
2. Re-runs analyse des dépendances avec les nouveaux types de fichiers
3. Actualise tous les résultats d'analyse concernés

> **Note**
>
> Vous ne pouvez reclasser les fichiers qu'une fois la boucle d'analyse initiale terminée.

Visionneuse en ligne et comparaison de fichiers

Le visualiseur intégré est une fonctionnalité des fonctionnalités de AWS Transform for mainframe qui fournit deux fonctionnalités de visualisation clés :

- Affichage des fichiers : affichage du contenu des anciens fichiers sélectionnés à partir des tâches
- Comparaison de fichiers : comparez le contenu de deux anciens fichiers côte à côte

Affichage du fichier d'entrée

Pour consulter vos fichiers dans Analyser le code step

- Sous Afficher les résultats de l'analyse du code, sélectionnez un fichier à l'aide de la case à cocher de la liste.

  Cliquez sur le bouton d'action Afficher (activé lorsqu'un élément est sélectionné).

  Le contenu du fichier sera affiché à l'écran dans le composant Affichage des fichiers.

Comparaison de fichiers

Pour comparer des fichiers dans Analyser le code step

1. Sous Afficher les résultats de l'analyse du code, sélectionnez deux fichiers à l'aide des cases à cocher de la liste.
2. Cliquez sur le bouton d'action Comparer (activé uniquement lorsque 2 éléments sont sélectionnés).
3. Les fichiers seront affichés côte à côte dans le composant de comparaison de fichiers.

> **Note**
>
> Vous ne pouvez pas sélectionner plus de deux fichiers pour les comparer.

> **Important**
>
> Si vous rencontrez des problèmes avec la visionneuse en ligne ou la comparaison de fichiers, assurez-vous que le compartiment S3 est correctement configuré. Pour plus d'informations sur la politique CORS du compartiment S3, consultezthe section called “Autorisations CORS du compartiment S3”.

Analyse des données

AWS Transform fournit une analyse des données pour aider à comprendre l'impact des relations entre les données et des éléments sur le projet de modernisation du mainframe. Les deux sorties fournies sont les suivantes :

- Lignage des données : trace le cycle de vie des données en cartographiant les relations entre les sources de données, les tâches et les programmes
- Dictionnaire de données : sert de référentiel documentant les métadonnées structurelles des éléments de données existants

Une fois l'analyse terminée, deux onglets seront présents pour chaque sortie, puis plusieurs vues seront disponibles, décrites ci-dessous, pour le lignage des données et le dictionnaire.

> **Note**
>
> Lorsque vous demandez une analyse de données. AWS Transform effectue l'analyse du code, qui est nécessaire pour effectuer l'analyse des données.

Traçabilité des données

AWS Transform fournit plusieurs vues basées sur les relations entre les données qui doivent être comprises dans l'ensemble de la base de code en cours de modernisation. Les quatre vues tabulaires disponibles dans Data Lineage sont les suivantes :

- Ensembles de données : cette vue fournit une analyse d'impact complète, y compris le suivi des opérations pour aider à faire la distinction entre lecture, écriture, mise à jour et suppression
- Tables DB2 : fournissez l'analyse d'impact liée aux tables DB2 et aux opérations

- Program-to-data: Identifiez les programmes COBOL qui font référence à chaque ensemble de données
- JCL-to-data relations : identifiez les scripts JCL qui font référence à chaque ensemble de données

Le résumé fournit une vue d'ensemble des sources de données et de leurs relations avec les programmes et les JCL, ainsi que des informations récapitulatives sur la manière dont les sources de données sont exploitées et le nombre total d'opérations trouvées dans la base de code.

Dictionnaire de données

Comprendre les éléments de données contenus dans les sources de données présentes dans la base de code est l'étape suivante pour comprendre en quoi les différentes sources de données sont dépendantes. Le dictionnaire de données est un catalogue de données fournissant des métadonnées au niveau du terrain avec des descriptions en langage commercial pour une cartographie précise des transformations.

- Structure de données COBOL : fournit des informations sur les champs dans les cahiers COBOL et les références INLINE présentes dans la base de code, y compris les propriétés des champs et la définition commerciale
- Tables DB2 : fournit les propriétés des colonnes et des tables des tables DB2 présentes dans la base de code, y compris les clés primaires et étrangères, les informations de schéma et d'index, ainsi que les types de données

La relation entre le lignage de données et le dictionnaire est disponible en sélectionnant la source de données, puis en utilisant le bouton de lignage de données ou de dictionnaire de données afin d'approfondir la relation entre la source de données et les éléments de données. La navigation entre le lignage des données et le dictionnaire fournit une visibilité intégrée des données, le lignage des données fournissant le « quoi » (structure et signification), ainsi que le « où » - utilisation et relation.

Analyse des métriques d'activité

L'analyse des métriques d'activité vous permet d'analyser les enregistrements SMF (System Management Facility) de type 14, 15, 30, 64, 102 et 110. L'analyse fournit des informations sur la façon dont les éléments sont utilisés dans votre application mainframe. Cela peut aider à retirer le code inutilisé ou à prendre des décisions concernant l'architecture cible de l'application modernisée. Si vous incluez l'analyse des métriques d'activité dans votre travail, l'étape d'analyse du code permet d'abord d'obtenir des résultats SMF plus riches, bien que cela ne soit pas obligatoire.

> **Note**
>
> Lorsque vous négociez le plan de travail pour la modernisation du mainframe, l'exécution des étapes d'analyse et de décomposition du code dans un premier temps permet d'obtenir des résultats plus riches.

Enregistrements SMF intégrés pour analyse

Vous devez fournir l'emplacement de l'enregistrement SMF dans votre compartiment Amazon S3 comme première étape de l'analyse SMF. Fournissez un minimum de 13 mois d'enregistrements pour saisir les événements annuels susceptibles de ne pas être pris en compte sur des périodes plus courtes. Bien que 13 mois soient recommandés, toute période comportant des enregistrements SMF détectables produit des résultats d'analyse.

Votre extrait SMF doit répondre aux exigences de format suivantes :

- Incluez les types 14, 15, 30 (sous-type 5), 64, 102 et 110.
- Utilisez un fichier binaire brut au format EBCDIC.
- Incluez les octets RDW.

Fournissez un lien vers les enregistrements SMF de votre compartiment Amazon S3, en vous assurant que les enregistrements se trouvent dans un dossier distinct de votre code source. Les options de format incluent .zip (jusqu'à 600 Mo) ou .tar.gz (jusqu'à 5 Go) compressé. Si vous fournissez un lien vers un dossier dans lequel aucun enregistrement SMF n'est détecté, vous recevez un message d'erreur et aucune analyse n'est terminée.

Résultat de l'analyse

La sortie d'analyse contient deux composants, selon le type d'enregistrement : une vue tabulaire et une sortie .csv (disponible dans votre compartiment Amazon S3). Dans AWS Transform, les sorties sont affichées pour les types 30 et 110. Grâce aux artefacts de votre compartiment Amazon S3, vous pouvez explorer l'analyse sur d'autres types d'enregistrements. Dans l'interface utilisateur, l'en-tête affiche la plage horaire des enregistrements que vous avez fournis afin que vous puissiez identifier les dates clés manquantes. Par exemple, si vos enregistrements s'étendent du 1er mai au 31 octobre, mais excluent la journée chargée qui suit Thanksgiving, vous pouvez constater que des enregistrements clés sont manquants. Les horodatages de l'application Web reflètent le fuseau horaire de votre système et les enregistrements SMF.

Les artefacts disponibles dans Amazon S3 fournissent une analyse de tout type d'enregistrement trouvé dans les enregistrements fournis.

Vue tabulaire

La vue tabulaire, disponible uniquement pour SMF 30 et 110, contient jusqu'à trois composants principaux pour les tâches par lots et les transactions CICS :

- Résumé — Fournit les principaux travaux et transactions.
- Analyse job/CICS des transactions par lots : fournit une analyse agrégée des tâches et des transactions.
- Comparaison de l'analyse du code (par lots uniquement) : fournit des données de comparaison lorsque l'étape d'analyse du code s'exécute avant l'analyse SMF.

Le résumé des découvertes fournit trois groupes de tâches et de transactions qui vous aident à identifier rapidement les éléments pour une analyse plus approfondie.

L'analyse des tâches par lots et des transactions CICS fournit une analyse agrégée des tâches et des transactions. Certaines colonnes des résultats d'analyse sont masquées par défaut. Cliquez sur l'icône représentant une roue dentée pour afficher des champs supplémentaires.

La clé de transaction génère une agrégation de données unique pour les transactions CICS, combinant quatre champs en une seule valeur de clé :

- Numéro de transaction
- Nom du programme
- SysPlex ID
- ID système

Vous pouvez effectuer une recherche par clé complète ou par n'importe quel composant de la clé dans le résultat de l'analyse.

La comparaison de l'analyse du code met en évidence les tâches trouvées dans les enregistrements SMF ou dans l'étape d'analyse du code, mais absentes dans les deux. Cela montre les tâches qui n'ont pas été exécutées pendant votre période d'enregistrement SMF ou qui n'étaient pas présentes lors de l'étape d'analyse du code. Cette sortie n'est disponible que lorsque vous exécutez l'étape d'analyse du code avant l'analyse SMF dans le cadre de votre tâche.

Bonnes pratiques

Pour obtenir des résultats complets pour les tâches par lots (type 30), assurez-vous que le nom de votre fichier JCL correspond au nom de la tâche afin d'obtenir des résultats significatifs dans la comparaison de l'analyse de code.

Générer de la documentation technique

Vous pouvez générer de la documentation technique pour vos applications mainframe en cours de modernisation. En analysant votre code, AWS Transform peut créer automatiquement une documentation détaillée de vos programmes d'application, y compris des descriptions de la logique du programme, des flux, des intégrations et des dépendances présents dans vos anciens systèmes. Cette fonctionnalité de documentation permet de combler le déficit de connaissances, en vous permettant de prendre des décisions éclairées lors de la transition de vos applications vers des architectures cloud modernes.

> **Note**
>
> Lorsque vous demandez la génération de documentation technique, AWS Transform effectue une analyse de code, y compris une analyse de dépendance du code, qui est requise pour générer la documentation.

Pour générer de la documentation technique

1. Dans le volet de navigation de gauche, sous Générer la documentation technique, choisissez Sélectionner les fichiers et configurer les paramètres.
2. Sélectionnez les fichiers du compartiment Amazon S3 pour lesquels vous souhaitez générer de la documentation, puis configurez les paramètres dans l'onglet Collaboration.

   > **Note**
   >
   > Les fichiers sélectionnés doivent avoir le même type de codage (c'est-à-dire tous dans le même CCSID : UTF8 ou ASCII). Dans le cas contraire, la documentation technique générée peut comporter des champs ou des sections vides.

3. Choisissez le niveau de détail de la documentation :

- Résumé — Fournit une vue d'ensemble de haut niveau de chaque fichier inclus dans le champ d'application. Donne également un résumé d'une ligne de chaque fichier.
- Spécification fonctionnelle détaillée : fournit des informations complètes pour chaque fichier inclus dans le périmètre de transformation de l'application mainframe. Certains détails incluent la logique et le flux, les dépendances, le traitement des entrées et des sorties et divers détails des transactions.

> **Note**
>
> La documentation ne peut être générée que pour les fichiers COBOL et JCL.

4. Sélectionnez Continuer.
5. Une fois que AWS Transform a généré la documentation, passez en revue les résultats de la documentation en suivant le chemin du compartiment Amazon S3 dans la console, où les résultats sont générés et stockés.
6. Une fois la documentation générée, vous pouvez également utiliser le chat AWS Transform pour poser des questions sur la documentation générée et décider des prochaines étapes.

Ajouter des informations utilisateur dans la documentation

```
ARTIFACT_ID.zip
### app/
    ### File1.CBL
    ### File2.JCL
    ### subFolder/
    #   # File3.CBL
### glossary.csv
### pdf_config.json
### header-logo.png
### footer-logo.png
# ...
```

Des fichiers facultatifs peuvent être ajoutés dans le fichier zip pour améliorer la qualité de la documentation générée et fournir une page de couverture PDF personnalisée. Certains d'entre eux peuvent être :

- Fichier glossary.csv : vous pouvez choisir de fournir et de télécharger un glossaire facultatif dans le fichier zip du compartiment S3. Le glossaire est au format CSV. Ce glossaire permet de créer une documentation avec des descriptions pertinentes conformes au vocabulaire du client. Un exemple de `glossary.csv` fichier ressemble à ce qui suit :

```
LOL,Laugh out loud
ASAP,As soon as possible
WIP,Work in progress
SWOT,"Strengths, Weaknesses, Opportunities and Threats"
```

- pdf_config.json : vous pouvez tirer parti de ce fichier de configuration facultatif pour générer des documents PDF conformes aux formats et aux normes de leur entreprise, notamment les en-têtes, les pieds de page, les logos et les informations personnalisées. Un échantillon `pdf_config.json` ressemble à ce qui suit :

```
{
    "header": {
    "text": "Acme Corporation Documentation",
    "logo": "header-logo.png"
  },
  "customSection": {
    "variables": [
      {
        "key": "business Unit",
        "value": "XYZ"
      },
      {
        "key": "application Name",
        "value": "ABC"
      },
      {
        "key": "xxxxxxxxxx",
        "value": "yyyyyyyyyyy"
      },
      {
        "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
  }
}
```

- En-tête :
  - Pour le fichier PDF de la page de couverture, le texte par défaut sera le nom du projet.
  - Pour chaque fichier PDF du programme, le texte par défaut sera le nom du programme.
  - Il n'existe aucun logo par défaut. Si aucun logo d'en-tête n'est configuré, aucun logo ne sera affiché.
  - La taille de police et la taille du logo doivent être modifiées dynamiquement en fonction du nombre de mots ou de la taille du fichier du logo.
- Section personnalisée :
  - Si la section personnalisée n'est pas configurée, elle sera omise du PDF.
  - Le lien doit être cliquable.
- Pied de page :
  - Il n'existe aucun texte ou logo par défaut pour le pied de page.
  - Le numéro de page sera affiché dans le pied de page par défaut, sauf configuration contraire explicite.
  - La taille de police et la taille du logo doivent être modifiées dynamiquement en fonction du nombre de mots ou de la taille du fichier du logo.

Générer un visualiseur de documentation en ligne

Vous pouvez consulter les fichiers PDF à l'étape de génération de la documentation technique.

Pour consulter les fichiers PDF

1. Accédez à l'onglet Consulter les résultats de la documentation.
2. Localisez le PDF dans le tableau répertoriant les PDF générés.
3. Sélectionnez le fichier puis Afficher ou sélectionnez l'élément de lien superposé au nom du fichier.

Le PDF s'ouvre dans AWS Transform, avec la possibilité d'agrandir l'écran en haut à droite.

> **Note**
>
> AWS Transform vous permet également de télécharger une version XML ou PDF de la documentation technique générée.

> **Important**
>
> Si vous rencontrez des problèmes avec l'afficheur de documentation en ligne, assurez-vous que le compartiment S3 est correctement configuré. Pour plus d'informations sur la politique CORS du compartiment S3, consultezthe section called "Autorisations CORS du compartiment S3".

Extraire la logique métier

Vous pouvez extraire la logique métier essentielle de vos applications mainframe en cours de modernisation. AWS Transform analyse automatiquement votre code pour identifier et documenter les éléments commerciaux critiques, notamment les flux de processus détaillés et la logique métier intégrée à vos applications. Cette fonctionnalité est utile à de multiples parties prenantes dans votre parcours de modernisation. Les analystes commerciaux peuvent exploiter la logique extraite pour créer des exigences commerciales précises et identifier les lacunes ou les incohérences dans les implémentations actuelles. Les développeurs sont en mesure de comprendre rapidement les fonctionnalités complexes des anciens systèmes sans avoir à acquérir une expertise approfondie en matière de mainframe.

> **Note**
>
> Lorsque vous demandez l'extraction de la logique métier. AWS Transform effectue l'analyse du code, y compris l'analyse des dépendances du code et l'analyse des points d'entrée, qui sont nécessaires pour effectuer l'extraction de la logique métier.

Pour extraire la logique métier

1. Dans le volet de navigation de gauche, sous Extraire la logique métier, choisissez Configurer les paramètres.
2. Dans l'onglet Collaboration, sélectionnez la manière dont vous souhaitez extraire la logique métier :

   - Niveau de l'application : génère des documents commerciaux pour toutes les fonctions commerciales, les transactions, les traitements par lots et les fichiers. Cela permet de sélectionner tous les fichiers de l'application.
   - Niveau du fichier : génère des documents commerciaux uniquement pour les fichiers que vous sélectionnez dans le tableau des fichiers.

   > **Note**
   >
   > - Pour l'une ou l'autre option, vous pouvez sélectionner Inclure les spécifications fonctionnelles détaillées afin que AWS Transform inclue le flux de contrôle et les règles métier complètes pour les fichiers sélectionnés.
   > - Les fichiers sélectionnés doivent avoir le même type de codage (c'est-à-dire tous dans le même CCSID : UTF8 ou ASCII). Dans le cas contraire, la documentation générée peut comporter des champs ou des sections vides.
   > - La documentation ne peut être générée que pour les fichiers COBOL et JCL.
   > - Au niveau de l'application, les programmes utilisés par les transactions CICS et les tâches par lots sont regroupés, tandis que tous les autres programmes sont classés dans la catégorie « Non assignés ».

3. Sélectionnez Continuer.

4. Une fois que AWS Transform a extrait la logique métier, il stocke les résultats dans un compartiment Amazon S3 au format JSON afin que vous puissiez les consulter en ligne.

> **Note**
>
> Le nombre de fichiers de règles métier générés peut être supérieur à celui que vous avez sélectionné initialement. Certains fichiers sélectionnés peuvent déclencher l'extraction des règles métier afin d'inclure des fichiers dépendants supplémentaires, qui apparaîtront également dans le tableau des résultats.

Consultez la documentation commerciale extraite en ligne

Vous pouvez consulter la logique métier à l'étape Extraire la règle métier. Pour ce faire,

1. Accédez à Examiner les résultats de l'extraction de la logique métier.
2. Sélectionnez le document que vous souhaitez consulter dans le tableau, puis cliquez sur le bouton Afficher le résultat.

La page de documentation commerciale s'ouvre dans un nouvel onglet du navigateur.

Décomposition

Vous pouvez décomposer votre code en domaines qui tiennent compte des dépendances entre les programmes et les composants. Cela permet de regrouper les fichiers et programmes associés de manière appropriée au sein d'un même domaine. Cela permet également de maintenir l'intégrité de la logique de l'application pendant le processus de décomposition.

> **Note**
>
> Lorsque vous demandez une décomposition, AWS Transform effectue une analyse de code, y compris une analyse de dépendance du code, qui est nécessaire pour effectuer la décomposition. Nous vous recommandons également d'effectuer une extraction de la logique métier avant la décomposition pour de meilleurs résultats.

Pour commencer à décomposer votre application :

1. Sélectionnez Décomposer le code dans le volet de navigation de gauche.

> **Note**
>
> Un domaine, Non attribué, est automatiquement créé pour tous les fichiers non associés à un domaine. Lors de la navigation initiale, tous les fichiers doivent être associés à Unassigned, sauf si des domaines ont été proposés à partir de l'extraction de la logique métier au niveau de l'application.

2. Créez un nouveau domaine via le menu Actions, puis choisissez Créer un domaine.
3. Dans Créer un domaine, indiquez le nom de domaine, une description facultative et marquez certains fichiers comme des graines.
   - Les fichiers configurés CICS (CSD) et les fichiers configurés par le planificateur (SCL) peuvent être utilisés pour la détection automatique des semences.
   - Vous pouvez également définir un seul domaine en tant que composant commun. Les fichiers de ce domaine sont communs à plusieurs domaines.
4. Choisissez Créer.

> **Note**
>
> Vous pouvez créer plusieurs domaines avec différents fichiers sous forme de graines.

5. Après avoir confirmé tous les domaines et les graines, choisissez Decompose.
6. AWS Transform vérifiera les fichiers de code source, puis les décomposera en domaines contenant des programmes et des ensembles de données présentant des cas d'utilisation similaires et des dépendances de programmation élevées.

   AWS Transform vous donne une vue tabulaire et graphique des domaines décomposés sous forme de dépendances. La vue graphique comporte trois options :

   - Vue du domaine : permet de voir comment les différents domaines sont liés les uns aux autres dans un format visuel.
   - Vue des dépendances : permet de visualiser tous les fichiers de chaque domaine sous la forme d'un graphe de dépendance complexe. Si un nœud ajouté à un domaine n'a pas reçu d'informations d'une source du même domaine, ce nœud sera soit déclaré non attribué (le nœud n'a reçu aucune information), soit déconnecté (dans un sous-graphe qui n'a pas reçu

d'informations de départ), soit connecté à un autre domaine (le nœud a reçu des informations d'au moins ce domaine).

- Vue des sous-graphes - L'utilisateur peut créer des sous-graphes pour visualiser un sous-ensemble de nœuds afin de mieux comprendre l'impact relationnel et les limites de cet ensemble de nœuds.
  - Pour créer un sous-graphe, sélectionnez un groupe de nœuds et sélectionnez l'option Extraire le sous-graphe dans la barre d'outils.
  - La fusion de sous-graphes est disponible. Lors de la fusion, un troisième sous-graphe est créé en plus des deux sous-graphes que vous fusionnez.

> **Note**
>
> Répétez ces étapes pour ajouter d'autres domaines ou pour reconfigurer vos domaines déjà créés avec un ensemble de graines différent si vous n'aimez pas la structure de domaine actuelle.

7. Lorsque vous avez terminé, choisissez Continuer.

Graines

Les graines sont les entrées fondamentales de la phase de décomposition du code. Chaque composant ou fichier (par exemple, JCL, COBOL, tables DB2, CSD et fichiers de planificateur) peut être attribué en tant que point de départ à un seul domaine, ce qui garantit des limites et un alignement clairs pendant le processus de décomposition.

L'identification des semences dépend de la structure de l'application ou du portefeuille. Dans le cas d'une ancienne application mainframe typique, les bases peuvent souvent être déterminées en respectant les conventions de dénomination établies, en groupant par lots dans le planificateur et en groupant au niveau des transactions défini dans le système CICS. En outre, les tables de base de données peuvent également servir de base de données, fournissant ainsi une couche de structure supplémentaire pour la décomposition.

Importer des fichiers de dépendances de and/or mise à

Pendant la décomposition, vous pouvez télécharger un fichier JSON pour les dépendances qui remplace les fichiers existants générés par l'analyse des dépendances effectuée par AWS Transform.

La fonction d'exportation des dépendances vous permet de télécharger le fichier json des dépendances généré lors de l'étape de décomposition. Après le téléchargement, vous pouvez modifier le fichier selon vos besoins. Vous pouvez ensuite importer des dépendances à l'aide de la fonctionnalité de téléchargement de AWS Transform qui vous permet de télécharger le nouveau fichier JSON des dépendances qui remplace le fichier généré par l'analyse des dépendances. Ensuite, le graphique de l'étape de décomposition sera mis à jour.

Pour exporter, modifier et importer des dépendances

1. Sur la page Afficher les résultats de la décomposition, sélectionnez Actions.
2. Dans la liste déroulante, choisissez l'option Mettre à jour le fichier de dépendances sous Autres actions.
3. Dans le modal du fichier de mise à jour des dépendances,

    a. Téléchargez le fichier de dépendance AWS Transform créé à partir des résultats d'analyse existants.

    b. Dans le fichier téléchargé, modifiez les dépendances en fonction de ce que vous souhaitez obtenir.

    c. Après avoir modifié, enregistrez et téléchargez ce fichier à l'aide du bouton Télécharger le fichier de dépendance.

    > **Note**
    >
    > Le seul format de fichier accepté est le fichier JSON.

4. Ensuite, choisissez Importer.

AWS Transform importera le fichier de dépendances et créera un nouveau graphe de dépendances en fonction de vos entrées.

Importer des domaines de and/or mise à

Pour les clients dont les domaines, les graines et les relations entre les and/or fichiers ont été mappés avant l'étape de décomposition, vous pouvez télécharger cette définition de domaine via la fonction Importer un fichier de domaines disponible dans le menu Actions. Voici quelques exemples de cas dans lesquels cette fonction peut être utilisée :

- Procéder à la décomposition à partir d'une autre tâche

- Des experts en la matière fournissant cette cartographie

Une fois le fichier de domaines importé, l'utilisateur peut soit exécuter la décomposition par rapport à la définition du domaine, soit, s'il est satisfait, enregistrer puis soumettre la définition de domaine.

Parent/child/neighbor fichiers

Dans un graphe de dépendances, les programmes sont liés les uns aux autres par le biais de différents types de connexions. La compréhension de ces relations vous permet d'analyser les dépendances entre les programmes lors de la transformation de vos applications mainframe. Cela aide également à comprendre les limites d'un domaine. Par exemple, si vous sélectionnez un domaine, puis le niveau parent 1, les nœuds connectés seront affichés.

Relations parentales : un fichier parent appelle ou contrôle d'autres programmes. Dans la hiérarchie, les parents se situent au-dessus de leurs programmes dépendants. Vous pouvez sélectionner un parent à un niveau ou à tous les niveaux.

Relations avec les enfants : un fichier enfant est appelé ou contrôlé par le programme parent. Les enfants sont placés en dessous de leur parent dans la hiérarchie des fichiers.

Relations de voisinage : les voisins sont des fichiers situés au même niveau hiérarchique. Ils partagent le même programme parent et peuvent interagir directement entre eux.

Reforger le code

Reforge utilise des modèles de langage de grande taille (LLM) pour améliorer la qualité du code refactorisé. La COBOL-to-Java transformation initiale préserve l'équivalence fonctionnelle tout en conservant COBOL-influenced les structures de données et les noms de variables du système existant. Reforge restructure ce code pour suivre les pratiques et expressions idiomatiques modernes de Java, en remplaçant les COBOL-style constructions par des collections Java natives et des conventions de dénomination. Cela rend le code plus lisible et plus facile à maintenir pour les développeurs Java.

> **Note**
>
> Les quotas pour le reforge sont les suivants :
>
> - 3 000 000 lignes de code par tâche
> - 50 000 000 lignes de code par utilisateur et par mois

Reforgez votre code après le refactoring en suivant ces étapes :

1. Choisissez Reforge le code Java dans le volet de navigation de gauche, puis sélectionnez Configurer la reforge du code.
2. Indiquez l'emplacement S3 de votre projet source à compiler compressé et choisissez Continuer. Utilisez cette structure zip :

   ```
   input.zip
           ### PROJECT-pom
           ### PROJECT-entities
           ### PROJECT-service
           ### PROJECT-tools
           ### PROJECT-web (optional)
           ### pom.xml
   ```

   AWS Transform analyse votre package zip pour localiser les fichiers dans le PROJECT-service répertoire afin de fournir une liste sélectionnable de classes que vous pouvez reforger. Ces classes ont le suffixe`ProcessImpl.java`.
3. Complétez la page Sélectionner les classes à reforger et choisissez Continuer. Suivez l'état de la reforge dans l'onglet Worklog.
4. Consultez les résultats de votre reforge terminée sur la page Afficher les résultats, qui affiche l'état de la reforge par classe. Il indique également où trouver le résultat de Reforge dans votre compartiment S3.

Une fois que AWS Transform reçoit cette entrée de votre part, il vous fournit un fichier téléchargeable contenant les résultats de Reforge.

Voici la structure zip issue d'une reforge réussie :

```
reforge.zip
### maven_project
### reforge.log
###tokenizer_map.json
```

- maven_project contient le code source reforgé.
  - Les fichiers qui ont été refactorisés mais dont la compilation n'a pas été finalisée avec succès se trouvent dans `/src/main/resources/reforge/originalClassName.java.incomplete`

et sont nommés. `originalClassName.java.incomplete` Comparez-les aux versions originales des fichiers pour choisir les fonctions reforgées que vous souhaitez enregistrer.

- Les fichiers source fournis à AWS Transform qui ont été refactorisés avec succès sont sauvegardés `src/main/resources/reforge/originalClassName.java.original` et nommés. `originalClassName.java.original` Les versions refactorisées des fichiers remplacent les fichiers source fournis à Transform. AWS

> **Note**
>
> Les `originalClassName.java` fichiers sont remplacés par les fichiers reforgés uniquement si le processus de reforgeage est réussi. Dans le cas contraire, ils conservent le contenu original.

- reforge.log contient des journaux que vous pouvez utiliser pour diagnostiquer les échecs de tâches ou fournir au AWS support en cas de problème.
- tokenizer_map.json contient un mappage des identifiants de token vers vos données, tels que les chemins et les class/method noms de fichiers, qui sont tokenisés dans les journaux pour protéger la confidentialité. Vous pouvez fournir ce fichier au AWS support en cas de problème.

Planifiez les tests de vos applications modernisées

Vous pouvez créer et gérer des plans de test pour les applications modernisées de votre mainframe en fonction des attributs du code extrait, de la complexité des tâches et des chemins du planificateur. AWS Transform permet de hiérarchiser les tâches à tester et d'identifier les artefacts spécifiques nécessaires pour chaque scénario de test. Le processus de planification des tests est divisé en trois phases principales : configuration, cadrage et révision.

Pour créer un plan de test

1. Configuration des paramètres du plan de test

   a. Dans le volet de navigation de gauche, sous Planifiez vos tests, choisissez Configurer les paramètres.

   b. (Facultatif) Fournissez des chemins S3 pour votre extraction de logique métier (BLE). Ces artefacts améliorent la qualité du plan de test. Sans artefacts BLE, certains champs du plan de test peuvent rester incomplets.

2. Définition de la portée du plan de test

a. Sélectionnez les points d'entrée, tels que les tâches par lots, à inclure dans votre plan de test.

b. Filtrez et triez les tâches en fonction de plusieurs attributs :

- Fonctions commerciales (extraites de BRE BLE)
- Domaines (à partir de la phase de décomposition)
- Chemins et emplacements des fichiers
- Critères de recherche personnalisés

c. Sélectionnez des tâches individuelles ou des groupes entiers à tester.

d. Passez en revue les relations professionnelles et les dépendances.

3. Vérifiez et ajustez le plan de test

Le plan de test généré fournit des informations complètes, notamment :

- Ordre d'exécution préféré basé sur les dépendances
- Attributions de groupes de tâches depuis le planificateur
- Les scores de complexité, qui sont des scores agrégés pour les cas de test
- Associations de domaines commerciaux
- Mesures de complexité cyclomatique
- Dépendances entre les ensembles de données et
- Lignes de code, métriques
- Mappages des fonctions métiers

Options de personnalisation du plan de test

Votre plan de test peut être personnalisé pour répondre à des besoins spécifiques. Par exemple, vous pouvez effectuer les actions suivantes :

- Créez de nouveaux scénarios de test en sélectionnant plusieurs points d'entrée
- Fusionnez les cas de test existants pour combiner les fonctionnalités associées
- Divisez les cas de test pour des tests plus précis
- Supprimer les scénarios de test inutiles
- Ajouter ou supprimer des points d'entrée pour les scénarios de test existants

- Modifier les descriptions et les attributs des scénarios de test
- Ajuster l'ordre d'exécution

Informations détaillées sur le cas de test

Chaque cas de test fournit des détails qui décrivent son contenu et l'ensemble de données ou les fichiers de données associés :

- Description complète de l'étendue du test
- Liste complète des points d'entrée incluse
- Mesures agrégées indiquant la complexité et la taille
- Règles commerciales et conseils automatisés pour les scénarios de test
- Dépendances des ensembles de données et des tables avec direction (input/output)
- Visualisation interactive du graphe de dépendances
- Prérequis et exigences d'exécution

Fonctionnalités de gestion des données

Ces informations vous aident à comprendre les données relatives au scénario de test. Vous pouvez effectuer les actions suivantes :

- Filtrer les ensembles de données par input/output direction
- Identifier les artefacts nécessaires à l'exécution des tests
- Suivez les dépendances des données entre les scénarios de test
- Surveillez l'utilisation des ensembles de données dans l'ensemble des plans de test

> **Note**
>
> AWS Transform analyse automatiquement les dépendances du planificateur et attribue des scores de complexité pour aider à hiérarchiser les efforts de test. Des scores de complexité plus élevés indiquent des tâches qui peuvent nécessiter des tests plus approfondis ou une isolation pendant le processus de test.

Règles commerciales et conseils relatifs aux scénarios de test

Le plan de test AWS Transform fournit des recommandations pour votre plan de test basées sur l'extraction des règles métier :

- Traitement automatique des règles métier à l'aide du LLM
- Génération de scénarios de test synthétiques
- Conseils de test pour des scénarios commerciaux spécifiques
- Traçabilité entre les règles et les cas de test

Le plan de test final est stocké dans l'emplacement S3 spécifié et inclut toutes les informations nécessaires pour exécuter efficacement votre stratégie de test. Vous pouvez exporter le plan de test pour l'intégrer à d'autres outils de test ou systèmes de documentation.

> **Note**
>
> Bien que des instructions synthétiques sur les scénarios de test soient fournies, les artefacts de test réels doivent être créés séparément en fonction des directives. Le plan de test sert de modèle complet pour votre stratégie de test, mais ne génère pas les données de test ni les scripts d'exécution.

Règles de création de scénarios de test - Résumé

Règles générales

- Un cas de test contient 1 à plusieurs JCL dans l'ordre d'exécution du calendrier
- Les cas de test sont créés à partir de planificateurs compatibles valides (CA7 et) Control-M
- Le test exécute les JCL, et non le planificateur lui-même ou les tâches planifiées
- Une tâche planifiée est unique et n'exécute qu'une seule JCL
- Une seule JCL peut être exécutée par plusieurs tâches planifiées
- Une seule JCL peut exister sans figurer dans un calendrier

Règles de création de scénarios de test par défaut

- Si un seul JCL se trouve dans un scénario de test :

  - JCL n'est pas impliqué dans un calendrier
  - JCL est exécuté par une tâche planifiée qui diverge en plusieurs branches
  - Une branche du planning contient uniquement cette JCL
- Si plusieurs JCL dans un cas de test : représente une séquence de chemins d'exécution linéaire dans une branche de planification
- Si JCL exécute une tâche planifiée divergente : JCL devient son propre cas de test distinct
- Si JCL exécute une tâche planifiée convergente : JCL peut démarrer un nouveau scénario de test mais ne sera pas inclus dans les branches précédentes
- Les JCL manquants sont ignorés et l'exécution continue (avec une future amélioration prévue pour réduire le scénario de test au point JCL manquant)

Règles relatives aux opérations des utilisateurs

- Créer un cas de test : l'utilisateur sélectionne parmi les JCL disponibles
  - Succès si les JCL existent dans la séquence de branches d'exécution du planning
  - Suit l'ordre d'exécution du calendrier
- Ajouter une JCL au scénario de test : l'utilisateur sélectionne parmi les JCL disponibles
  - Succès si JCL peut exister dans l'exécution planifiée du scénario de test branch/path
- Supprimer le JCL du scénario de test : l'utilisateur peut supprimer n'importe quel JCL d'un scénario de test
  - Autorisé même s'il entraîne des écarts dans le chemin d'exécution
- Fusionner les cas de test : l'utilisateur sélectionne deux cas de test à combiner
  - Succès si les JCL peuvent exister ensemble dans la même branche d'exécution du calendrier
  - Maintient l'ordre d'exécution du calendrier
- Scénario de test fractionné : l'utilisateur sélectionne une JCL dans un scénario de test pour le fractionnement
  - Crée un nouveau scénario de test à partir du point de partage
  - Scénario de test original modifié pour exclure le point de division passé par JCL
- Supprimer le scénario de test : l'utilisateur peut supprimer n'importe quel scénario de test créé

> **Note**
>
> Vous ne pouvez pas créer, ajouter ou fusionner des scénarios de test à partir d'un planificateur branches/path différent. Une future amélioration est prévue pour permettre des opérations allant au-delà divergent/convergent des tâches du planificateur.

Génération de scripts de collecte de données de test

Vous pouvez générer des scripts JCL pour collecter des données de test à partir de vos systèmes mainframe sur la base du plan de test créé à l'étape précédente. AWS Transform crée automatiquement des scripts de collecte de données pour les ensembles de données, les tables de base de données et les fichiers séquentiels nécessaires à des tests complets. Le processus de collecte de données est divisé en quatre phases principales : configuration des entrées, sélection des scénarios de test, configuration des scripts et génération de scripts.

Pour générer des scripts de collecte de données de test

1. Fournir des informations sur le plan de test
    a. Dans le volet de navigation de gauche, sous Collecte de données de test, choisissez Fournir une entrée de plan de test.
    b. Spécifiez le chemin S3 vers le fichier JSON de plan de test dans Planifier vos tests d'applications modernisés.
    c. Le champ de saisie est prérempli si le plan de test a été généré lors d'une étape de travail précédente.
    d. Vous pouvez également sélectionner un plan de test parmi d'autres tâches en spécifiant l'emplacement S3 approprié.
2. Sélectionnez des cas de test pour la collecte de données
    a. Consultez la liste complète des cas de test figurant dans votre plan de test.
    b. Filtrez et triez les cas de test en fonction de plusieurs attributs :
        - Fonctions et domaines commerciaux
        - dépendances des tables de base de données
        - Exigences relatives aux ensembles de données
        - Indicateurs de complexité

- Critères de recherche personnalisés

c. Sélectionnez des cas de test individuels ou utilisez les options de sélection groupée.

d. Consultez les détails des scénarios de test, notamment les points d'entrée, les indicateurs et les règles commerciales, en cliquant sur un cas de test pour voir les détails.

3. Configuration des scripts de collecte de données

a. Téléchargez des exemples de modèles et de fichiers de configuration pour référence.

- AWS Transform fournit des exemples de modèles pour le déchargement de bases de données DB2, le fichier VSAM REPRO et le traitement séquentiel des ensembles de données à utiliser comme guide sur les types de modèles attendus par le processus.
- Les normes peuvent varier d'un site à l'autre. Les clients s'attendent donc à ce qu'ils modifient ou remplacent ces modèles conformément à leurs propres normes.
- Ces modèles modifiés doivent être téléchargés dans un compartiment S3 où la collecte de données de test peut les traiter.

b. Fournissez un fichier de configuration variable (format JSON) contenant :

- Préfixes utilisateur et constantes spécifiques à l'environnement
- Paramètres de configuration de base de données
- Paramètres du point de terminaison de destination et paramètres de transfert de données
- Autres paramètres requis définis par l'utilisateur et à utiliser dans les modèles JCL

c. Téléchargez des modèles JCL pour différentes méthodes de collecte de données :

- Modèle DB2 : pour le déchargement des tables de base de données (personnalisable pour BMC, IBM DSN ou d'autres utilitaires de déchargement)
- Modèle VSAM : pour le traitement de fichiers VSAM (utilise généralement l'utilitaire REPRO)
- Modèle d'ensembles de données séquentiels : pour traiter des ensembles de données séquentiels, des ensembles de données partitionnés, des GDG, etc.

4. Vérifiez et gérez les scripts générés

Les scripts générés fournissent des fonctionnalités complètes de collecte de données, notamment :

- Scripts distincts pour la collecte de données « avant » et « après » l'exécution des tests

- Structure de script organisée par cas de test et type de données
- Les scripts sont automatiquement stockés dans le compartiment S3 pour un accès et un transfert faciles
- Les scripts JCL générés sont prêts à être exécutés sur le mainframe
- La substitution de variables est basée sur la configuration utilisateur définie dans les modèles

Fonctionnalités de génération de scripts

Les scripts générés sont automatiquement personnalisés en fonction de vos modèles et de votre configuration :

- Template-based génération : Utilise les modèles JCL que vous avez fournis avec une substitution de variables
- Environnement : intègre la configuration spécifique de votre mainframe
- Gestion des types de données : crée des scripts appropriés pour les ensembles de données séquentiels, les fichiers VSAM et les tables de base de données
- Collecte pour les cas de test : génère des scripts de collecte de données « avant » et « après »
- Traitement séquentiel des ensembles de données : l'exemple AWS fourni fournit une fonction de transfert de fichiers, mais celle-ci peut être personnalisée en fonction des utilitaires de compression disponibles sur votre site ou des utilitaires tels que Connect Direct ou le transfert de fichiers géré, etc.

Stratégie de collecte de données

Les scripts générés prennent en charge des stratégies complètes de collecte de données :

- Collecte de jeux de données séquentiels : utilitaires REPRO et de copie pour VSAM et fichiers plats
- Déchargement des tables de base de données : processus de déchargement DB2 personnalisables
- Traitement séquentiel des ensembles de données : post-traitement personnalisable des ensembles de données séquentiels tels que la compression, les services de transfert de fichiers gérés, etc.
- Gestion des dépendances : collecte coordonnée basée sur la définition du cas de test

> **Note**
>
> AWS Transform génère des scripts basés sur vos modèles et votre configuration. Passez en revue tous les fichiers JCL générés avant de les exécuter sur votre environnement mainframe afin de garantir leur compatibilité avec la configuration spécifique de votre système et les exigences de sécurité.

Personnalisation des modèles et meilleures pratiques

La collecte de données de test ATX fournit des fonctionnalités flexibles de personnalisation des modèles :

- Multi-utility support : Adapter les modèles aux différents utilitaires du mainframe (BMC, IBM, DSN)
- Variable-driven configuration : utilisez des constantes pour les paramètres spécifiques à l'environnement
- Modèles réutilisables : créez des modèles standardisés pour une génération de script cohérente
- Traitement des données : intégrer les exigences de traitement des données spécifiques à l'organisation
- Intégration de la sécurité : inclure des contrôles de sécurité et d'accès appropriés
- Optimisation des performances : configuration pour une collecte et un transfert de données efficaces

Structure de sortie générée

Les scripts générés sont organisés dans votre compartiment S3 selon la structure suivante :

- Organisation des cas de test : scripts regroupés par cas de test associés
- Calendrier de collecte : dossiers séparés pour la collecte de données « avant » et « après »
- Classification des types de données : scripts organisés par ensembles de données séquentiels, tables de base de données et transferts
- Fichiers de métadonnées : informations récapitulatives et conseils d'exécution
- Ready-to-transfer format : format JCL pour un déploiement direct sur mainframe

La collection de scripts finale est stockée dans l'emplacement S3 spécifié et inclut tout le JCL nécessaire pour exécuter efficacement votre stratégie de collecte de données. Vous pouvez

télécharger les scripts pour les transférer vers votre environnement mainframe ou les intégrer à des processus de déploiement automatisés.

> **Note**
>
> Bien que des scripts JCL complets soient générés, leur exécution réelle doit être effectuée sur votre environnement mainframe. Les scripts servent d'outils de collecte de données prêts à l'emploi, mais nécessitent un accès au mainframe et des autorisations d'exécution appropriés.

Génération de scripts d'automatisation des tests

Vous pouvez générer des scripts d'automatisation des tests pour exécuter des scénarios de test sur votre application modernisée en fonction du plan de test créé à l'étape précédente. AWS Transform crée automatiquement des scripts de test complets qui utilisent les données collectées lors du processus de collecte des données de test. Le processus de génération de scripts d'automatisation des tests comprend trois phases principales : la configuration des entrées, la sélection des scénarios de test et les résultats de génération des scripts.

Pour générer des scripts de test

1. Fournir des informations sur le plan de test
    a. Dans le volet de navigation de gauche, sous Génération de scripts d'automatisation des tests, sélectionnez Fournir une entrée de plan de test.
    b. Spécifiez le chemin S3 vers le fichier JSON de plan de test dans Planifier vos tests d'applications modernisés.
    c. Le champ de saisie est prérempli si le plan de test a été généré lors d'une étape de travail précédente.
    d. Vous pouvez également sélectionner un plan de test parmi d'autres tâches en spécifiant l'emplacement S3 approprié.
    e. Le système utilise ce plan de test comme base pour générer des scripts d'automatisation.
2. Sélectionnez les scénarios de test pour la génération de scripts
    a. Consultez la liste complète des cas de test figurant dans votre plan de test.
    b. Filtrez et triez les cas de test en fonction de plusieurs attributs :

- Fonctions et domaines commerciaux
- dépendances des tables de base de données
- Exigences relatives aux ensembles de données
- Indicateurs de complexité
- Critères de recherche personnalisés

c. Sélectionnez des cas de test individuels ou utilisez les options de sélection groupée à l'aide des boutons Tout cocher et Tout décocher.

d. Consultez les détails des scénarios de test, notamment les points d'entrée, les indicateurs et les règles commerciales, en cliquant sur des cas de test individuels.

   Les scénarios de test sélectionnés comporteront des scripts d'automatisation générés pour être exécutés sur l'application modernisée.

3. Passez en revue et gérez les scripts d'automatisation des tests générés :

- Le système affiche un message de réussite confirmant que la génération du script est terminée.
- Les scripts de test générés sont automatiquement stockés dans l'emplacement du compartiment S3 que vous avez spécifié.
- Accédez à la liste complète des scripts de test générés avec leurs emplacements S3 respectifs.
- Le script d'automatisation correspondant à chaque cas de test est stocké dans des emplacements S3 individuels.
- Les scripts sont prêts à être déployés et exécutés dans votre environnement applicatif modernisé.

Fonctionnalités du script d'automatisation des tests

Les scripts d'automatisation générés fournissent des fonctionnalités de test complètes :

- Tests d'applications modernisés : les scripts sont spécialement conçus pour exécuter des cas de test sur votre application transformée
- Intégration des données : utilise les données de test collectées lors de l'étape de collecte des données de test précédente, ces données doivent être copiées dans des dossiers pour chaque cas de test

- Exécution automatisée : les scripts peuvent être utilisés pour configurer des récepteurs de données, exécuter des scénarios de test et comparer les résultats. Certains paramètres devront être définis en fonction de votre environnement de déploiement
- Structure organisée : les scripts sont systématiquement organisés par cas de test dans votre compartiment S3
- Ready-to-deploy format : les scripts sont formatés pour un déploiement direct dans votre environnement de test

Structure de sortie générée

Les scripts d'automatisation des tests générés sont organisés dans votre compartiment S3 selon la structure suivante :

- Organisation des cas de test : chaque scénario de test possède son script dédié stocké dans un dossier S3 individuel
- Execution-ready format : les scripts sont formatés pour un déploiement et une exécution immédiats après avoir configuré une variable en fonction de votre environnement
- Accès centralisé : tous les scripts sont accessibles à partir d'un emplacement de compartiment S3 unique pour une gestion simplifiée

Stratégie d'exécution des tests

Les scripts générés prennent en charge des flux de travail complets d'exécution des tests :

- Configuration de l'environnement : les scripts incluent des fonctionnalités permettant de configurer les données initiales pour exécuter le test
- Préparation des données : intégration avec les données de test collectées lors de l'étape de collecte des données du cas de test
- Exécution de cas de test : exécution automatisée de cas de test individuels sur l'application modernisée
- Comparaison des résultats : Built-in fonctionnalités permettant de comparer les résultats des tests et de valider le comportement des applications

> **Note**
>
> AWS Transform génère des scripts d'automatisation des tests en fonction de votre plan de test et des cas de test sélectionnés. Les scripts sont conçus pour être exécutés sur votre environnement applicatif modernisé et utilisent les données de test collectées à l'étape précédente. Passez en revue tous les scripts générés avant le déploiement afin de garantir la compatibilité avec la configuration et les exigences de test spécifiques de votre application.

Bonnes pratiques pour l'automatisation des tests

- Validation de l'environnement : assurez-vous que votre environnement d'application modernisé est correctement configuré avant l'exécution du script
- Vérification des données : vérifier que les données de test requises lors de la phase de collecte sont disponibles et accessibles
- Personnalisation des scripts : passez en revue et personnalisez les scripts générés en fonction de vos besoins de test spécifiques
- Surveillance de l'exécution : implémentez une surveillance et une journalisation appropriées lors de l'exécution du script de test
- Analyse des résultats : établir des processus pour analyser les résultats des tests et identifier les problèmes liés aux applications

La collection finale de scripts d'automatisation des tests fournit un cadre de test complet pour valider les fonctionnalités de votre application modernisée. Les scripts peuvent être intégrés dans vos processus de test continu ou exécutés dans le cadre de votre flux de travail de validation des applications.

Capacités de déploiement dans AWS Transformation

AWS Transform vous aide à configurer des environnements cloud pour des applications mainframe modernisées en fournissant des modèles d'infrastructure en tant que code (IaC) prêts à l'emploi. Grâce à l'interface de chat AWS Transform, vous pouvez accéder à des modèles prédéfinis qui créent des composants essentiels tels que les ressources informatiques, les bases de données, le stockage et les contrôles de sécurité. Les modèles sont disponibles dans des formats courants tels que CloudFormation (CFN) et Terraform Cloud Development Kit AWS (AWS CDK), ce qui vous donne la flexibilité de déployer votre infrastructure.

Ces modèles constituent des éléments de base qui réduisent le temps et l'expertise nécessaires à la configuration des environnements pour vos applications mainframe modernisées. Vous pouvez personnaliser ces modèles en fonction de vos besoins, ce qui constitue une base solide pour créer votre environnement de déploiement.

Pour récupérer les modèles iAc, demandez dans le chat AWS Transform les Infrastructure-as-Code modèles précisant votre modèle de modernisation préféré (comme AWS Transform pour le refactorage des mainframes), votre topologie préférée (autonome ou haute disponibilité) et votre format préféré (par rapport à Cloud Development CloudFormation Kit ou à Terraform).

Créez et déployez votre application modernisée après le refactoring

Après avoir terminé le processus de refactorisation avec AWS Transform, vous pouvez créer et déployer votre application Java modernisée. Ce guide vous explique comment récupérer votre code modernisé, configurer votre environnement, déployer et tester votre application.

> **Note**
>
> Outre les conseils fournis ici, le package de code généré par AWS Transform inclura un document Set up the AWS Automated Refactor Development Environment qui fournit des instructions pour configurer un IDE (environnement de développement intégré) avec Developer Runtime.

Rubriques

Conditions préalables

Avant de commencer, assurez-vous d'avoir :

- Vous avez terminé avec succès un travail de refactorisation avec AWS Transform.
- Accédez à votre code modernisé.
- Une pile d'outils logiciels de génération installée et configurée sur votre machine de développement, telle qu'Apache Maven ou Apache Tomcat. Pour plus d'informations sur le versionnement de Runtime, consultez les notes de version de AWS Transform for mainframe Runtime.
- Amazon Corretto ou une version de Java Runtime installé et configuré. Pour plus d'informations sur l'installation d'Amazon Corretto, consultez Amazon Corretto 24.
- Accès pour créer et configurer des bases de données Amazon Aurora PostgreSQL pour les composants Runtime, si nécessaire. Pour plus d'informations sur la création de la base de données Aurora PostgreSQL, consultez la section Utilisation d'Amazon Aurora PostgreSQL.
- Accès administratif pour déployer des applications dans votre environnement d'exécution.
- Nous avons examiné les concepts d'exécution de AWS Transform for mainframe pour les concepts fondamentaux relatifs aux applications modernisées grâce à une solution de refactorisation AWS automatisée.

Étape 1 : récupérer le code modernisé

Pour récupérer le code modernisé

1. Téléchargez et extrayez le package de code généré.
2. Ouvrez `codebase/app-pom/pom.xml` et notez la version du moteur d'exécution requise. Par exemple `<gapwalk.version>4.6.0</gapwalk.version>`.
3. Localisez le document Configurer l'environnement de développement de refactorisation AWS automatique dans le package de code téléchargé à titre de référence.

Étape 2 : Création de l'application modernisée

Pour créer votre application modernisée

1. Accédez au Runtime depuis la boîte à outils AWS Transform for mainframe.
2. Téléchargez et installez la version d'exécution appropriée (identifiée dansthe section called "Étape 1 : récupérer le code modernisé") sur votre machine de développement locale.

> **Note**
>
> Des informations supplémentaires sur l'installation des dépendances d'exécution sur votre machine locale sont disponibles dans la section 3.1 du document Configurer l'environnement de développement de refacteurs AWS automatisés.

3. Ouvrez l'invite de commande et accédez au répertoire racine de votre application.
4. Pour créer des packages déployables pour l'application modernisée, exécutez la commande Maven build :

```
mvn package
```

Reportez-vous à la page Organisation de l'application pour plus de détails sur l'organisation de base du code modernisé. Par exemple, pour une application modernisée contenant une application Web frontale, vous pouvez vous attendre à au moins les `.war` agrégats déployables suivants en plus des composants d'exécution :

- Projet de service : contient des éléments de modernisation de la logique métier existante

```
<business-app>-service.*.war
```

- Projet Web : contient la modernisation des éléments liés à l'interface utilisateur

```
<business-app>-web.*.war
```

Étape 3 : Configuration de l'environnement de test

Pour configurer votre environnement de test

1. Configurez le runtime de votre application modernisée. Pour plus d'informations, consultez la section Configurer la configuration pour Runtime dans le guide de AWS Mainframe Modernization l'utilisateur.

> **Note**
>
> Reportez-vous à la section 5 du guide Set up the AWS Automated Refactor Development Environment pour des exemples de configuration spécifiques aux composants d'exécution.

2. Préparez des ensembles de données d'entrée et de sortie (I/O) pour les applications modernisées. Les applications modernisées peuvent traiter des ensembles de I/O données séquentiels, des ensembles de données VSAM ou autres.

> **Note**
>
> Reportez-vous à la section 6 de la section Configuration de l'environnement de développement de refactorisation AWS automatique pour des exemples.

3. Un environnement d'exécution : vous pouvez utiliser votre environnement d'exécution existant ou créer un nouvel environnement d'exécution.
   - Pour configurer un environnement d'exécution non géré, voir Configuration d'une application non gérée.
   - Pour configurer un environnement d'exécution géré, voir Configuration d'une application gérée.

Après avoir configuré l'environnement de test, vous passez à l'étape suivante qui consiste à déployer l'application modernisée.

Étape 4 : Déploiement de l'application modernisée

Déployez les artefacts de l'application dans l'environnement d'exécution que vous avez créé et and/or configuré dans les the section called “Étape 3 : Configuration de l'environnement de test” sections the section called “Étape 2 : Création de l'application modernisée” et.

Des instructions supplémentaires pour le déploiement de l'application modernisée sont disponibles à l'aide des liens suivants :

- Déploiement sur Amazon EC2
- Déploiement sur des conteneurs sur Amazon ECS et Amazon EKS
- Création d'une AWS Mainframe Modernization application

Étape 5 : Testez l'application modernisée

Après le déploiement,

1. Consultez les API d'exécution disponibles pour savoir comment interagir avec les applications modernisées.
2. Testez votre application pour aligner son équivalence fonctionnelle avec l'ancienne application. Par exemple, voir Tester un exemple d'application dans le guide de AWS Mainframe Modernization l'utilisateur.

Autre exemple

Pour un exemple spécifique de modernisation d'une application mainframe avec AWS Transform, voir Moderniser l'application CardDemo mainframe.

Full-stack Modernisation de Windows

AWS Transform assure une modernisation complète de Windows, y compris la modernisation du .NET et de SQL Server.

L'agent de AWS transformation pour .NET peut vous aider à moderniser vos applications .NET afin qu'elles soient compatibles avec le .NET multiplateforme. Vous pouvez moderniser .NET à l'aide de l'application Web .NET ou de l'IDE .NET.

AWS Transform for SQL Server Modernisation est un AI-powered service qui automatise la modernisation complète des bases de données Microsoft SQL Server et de leurs applications .NET associées vers Amazon Aurora PostgreSQL. Le service orchestre l'ensemble du processus de migration, de la conversion du schéma à la migration des données, en passant par la modification du code de l'application pour l'adapter à la nouvelle cible PostgreSQL, afin de rendre vos équipes plus productives en automatisant des tâches complexes et exigeantes en main-d'œuvre.

Rubriques

- Modernisation de .NET avec AWS Transformation
- Modernisation de SQL Server

Modernisation de .NET avec AWS Transformation

L'agent de AWS transformation pour .NET peut vous aider à moderniser vos applications .NET afin qu'elles soient compatibles avec le .NET multiplateforme. Cette fonctionnalité s'appelle la modernisation du .NET. Une fois AWS Transformez l'environnement dans AWS Transform, vous pouvez créer une tâche de transformation de modernisation .NET.

Expériences

AWS Transform est disponible dans plusieurs versions :

- Console Web : pour la transformation à grande échelle de 500 référentiels à la fois.
- Visual StudioIDE : transformation d'une solution ou d'un projet dirigée par le développeur en collaboration avec un agent de manière interactive et itérative. Recommandé pour les projets de moyenne à grande envergure.

Vous pouvez passer librement de la console Web à l'IDE pour travailler sur une tâche de transformation.

Vous pouvez également invoquer AWS Transform à partir d'autres IDE et compagnons de code AI :

- Kiro : transformez-vous à partir de Kiro en utilisant le pouvoir AWS Transform for Kiro.
- Autres compagnons de code AI : transformez-vous à partir de vos assistants de codage AI préférés à l'aide des agents AWS Transform MCP.

Capacités et fonctionnalités clés

- Analysez les bases de code .NET Framework à partir de vos systèmes de contrôle de source, ce qui inclut le NuGet support privé, l'identification des dépendances entre référentiels et la fourniture d'un rapport d'analyse.
- Transformation automatisée des anciennes applications .NET Framework en .NET multiplateforme, notifications par e-mail et rapport récapitulatif de transformation.
- Intégration facile avec les plateformes de contrôle de source (BitBucket, GitHub, et GitLab) pour ingérer le code existant et valider le code transformé dans une nouvelle branche.
- Validation du code transformé par des tests unitaires.

Versions et types de projets pris en charge

AWS Transform prend en charge la transformation pour les versions suivantes de .NET :

- .NET Framework 3.5 et versions ultérieures
- .NET Core 3.1
- .NET 5.x et versions ultérieures
- .NET 8

AWS Transform peut être transformé vers les versions .NET cibles suivantes :

- .NET 8
- .NET 10

AWS Transform prend en charge la transformation de ces types de projets (C# uniquement) :

- Bibliothèques de classes
- Applications de console
- ASP.NET:
  - Model View Controller (MVC), y compris le Razor Views frontal
  - Backends d'applications monopages (SPA) (couches de logique métier)
  - API Web
  - Formulaires Web
- Projets de tests unitaires (NUnit, xUnit et MSTest)
- Services de Windows Communication Foundation (WCF)
- Projets avec des versions multiplateformes fournies pour des NuGet packages tiers ou privés. Si un équivalent multiplateforme est manquant ou indisponible, AWS Transform for .NET tentera une conversion dans la mesure du possible.

AWS Transform peut également transformer les types de projets suivants en .NET moderne. Il s'agit d'une fonctionnalité de prévisualisation qui risque de ne pas se transformer aussi complètement que les types de projets pris en charge.

- WinForms projets de bureau.
- Projets de bureau WPF.
- Projets mobiles Xamarin.
- Projets écrits en VB.NET.

Limitations

Pour plus d'informations sur les quotas et les limites de AWS Transform, consultezQuotas pour AWS Transformation.

AWS La transformation ne transforme pas les éléments suivants :

- Composants de l'interface utilisateur Blazor
- DLL Win32 qui ne possèdent pas de bibliothèques compatibles de base
- Référentiels ne contenant aucune solution.

AWS Transform ne modifiera pas les branches du dépôt d'origine et ne pourra écrire que dans une branche cible distincte spécifiée dans votre plan de transformation.

Intervention humaine

Lors du portage des applications .NET Framework vers le .NET multiplateforme, il peut vous être demandé de fournir des informations ou des approbations dans les scénarios suivants :

- Configurez un connecteur pour votre code source et vos autorisations
- Valider le plan de modernisation proposé
- Téléchargez les dépendances de package manquantes en tant que NuGets
- Vérifiez et acceptez le code transformé

En savoir plus

Vous pouvez moderniser votre code .NET à l'aide de l'application Web AWS Transform ou du AWS Toolkit forVisual Studio.

- Modernisation de votre code .NET à l'aide du AWS Transformer une application Web
- Modernisation du .NET dans l'IDE
- Bonnes pratiques pour les transformations .NET

Modernisation de votre code .NET à l'aide du AWS Transformer une application Web

AWS Transform for .NET est un nouvel AI-powered agent génératif conçu pour moderniser les applications .NET existantes. Vous pouvez moderniser votre ancien code .NET à l'aide de l'application Web AWS Transform ou de l'extension Visual Studio AWS Toolkit.

Pour moderniser votre code .NET à l'aide de l'application Web AWS Transform, accédez à l'application Web en suivant ces étapes détaillées :

1. Création du AWS Transformez le plan de travail .NET
2. Création d'un connecteur de référentiel de code source
3. Confirmation de vos référentiels pour préparer la transformation
4. Résolution des dépendances entre les packages pour préparer la transformation

5. Révision de votre plan pour préparer la transformation
6. Transformation de votre code .NET

Création du AWS Transformez le plan de travail .NET

Après avoir créé votre espace de travail, dans l'onglet Tâches, sélectionnez Créer une tâche. Suivez ensuite les instructions de AWS Transform dans le volet de discussion en langage naturel. Voici les étapes typiques de création d'une tâche de modernisation .NET.

1. AWS Transform vous demandera quel type de travail de transformation vous souhaitez créer. Dans le chat, entrez dans la modernisation du .NET.
2. AWS Transform vous proposera un nom de travail et vous demandera si vous souhaitez le modifier. Si vous souhaitez modifier le nom de la tâche, indiquez à AWS Transform en langage naturel, par exemple, remplacez le nom de la tâche par ExampleCorpDotNet1. Sinon, dans le chat, vous pouvez accepter le nom de poste suggéré. Une fois que vous avez accepté le nom de la tâche, AWS Transform vous informe dans la fenêtre de discussion qu'elle est en train de créer la tâche.
3. AWS Transform crée le travail de transformation.

Composantes du AWS Transformez le plan de travail .NET

L'affichage des tâches AWS Transform .NET comporte 5 onglets que vous pouvez sélectionner parmi les icônes verticales situées à l'extrême gauche : tâches, tableau de bord, approbations, artefacts et journal de travail. Chaque onglet possède un volet gauche et un volet de discussion central. Un volet de collaboration approprié peut parfois apparaître pour afficher des détails supplémentaires et demander une contribution humaine.

Tâches (Job Plan)

Cet onglet affiche votre plan de travail dans le volet de gauche. Une tâche .NET comporte 5 étapes :

1. Obtenez des ressources à transformer : Dans cette phase, vous créez un connecteur vers votre référentiel de code à l'aide de AWS CodeConnections. En fonction des autorisations de votre référentiel, un administrateur du référentiel de code devra peut-être approuver le connecteur et autoriser AWS Transform à accéder au référentiel.

2. Découvrez les ressources nécessaires à la transformation : au cours de cette phase, AWS Transform découvre les référentiels dans le contrôle de source, et vous les sélectionnez en partie ou en totalité à des fins d'évaluation.
3. Évaluer le code pour la transformation : les référentiels sélectionnés sont évalués et vous pouvez consulter les rapports d'évaluation.
4. Préparation à la transformation : au cours de cette phase, AWS Transform vous avertit si des dépendances sont absentes de vos référentiels. Vous pouvez télécharger les dépendances manquantes ou les ignorer. Si vous n'êtes pas administrateur du dépôt, un administrateur devra peut-être approuver le plan de transformation final.
5. Transformation : Au cours de cette phase, AWS Transform transforme votre dépôt et vous fournit le statut continu pendant la transformation jusqu'à ce qu'elle soit terminée. Vous pouvez consulter les rapports de transformation pour comprendre ce qui a été modifié et pourquoi.

Vous pouvez voir le statut de chaque étape :

- Non démarré
- Attendre la saisie de l'utilisateur
- En cours
- Terminé

Tableau de bord

L'onglet Tableau de bord fournit un résumé de haut niveau de la transformation. Il affiche des mesures relatives au nombre de tâches transformées, à la transformation appliquée et au temps estimé pour terminer la transformation. Sous le tableau de bord se trouve un tableau des référentiels et de leur statut (échec ou réussite). In-progress

Approbations

Les demandes d'approbation pour le travail sont affichées et traitées dans cet onglet.

Artefacts

Jjob-related les artefacts sont chargés ou téléchargés à partir de cet onglet.

Worklog

AWS Transform enregistre ses actions dans l'onglet Worklog. Le Worklog fournit un journal détaillé des actions entreprises par AWS Transform, ainsi que les demandes d'intervention humaine et vos réponses à ces demandes.

Création d'un connecteur de référentiel de code source

EnsuiteCréation du AWS Transformez le plan de travail .NET, dans l'onglet Tâches, le volet gauche de la fenêtre de AWS transformation répertorie les phases du travail de transformation. La première phase consiste à obtenir des ressources à transformer. Au cours de cette phase, vous pouvez inviter des collaborateurs et connecter un référentiel de code source. Le volet droit de la fenêtre de AWS transformation permet de définir les détails.

Chaque tâche de transformation doit disposer d'un seul connecteur de référentiel de code source. L'agent de AWS transformation utilise ce connecteur pour télécharger votre base de code .NET depuis GitHub GitLab, ou Bitbucket en utilisant. AWS CodeConnections Vous devez effectuer l'installation AWS CodeConnections dans la même région que votre tâche de AWS transformation. Vous pouvez également vous connecter au code source dans Amazon S3 au lieu d'un référentiel de code source.

> **Note**
>
> Si vous disposez d'un connecteur de référentiel de code source existant, AWS Transform vous en informera. Sélectionnez Utiliser un connecteur existant pour utiliser ce connecteur. Si vous ne souhaitez pas utiliser le connecteur existant, voir Supprimer un connecteur existant ci-dessusAjouter un nouveau connecteur. Vous ne pouvez avoir qu'un seul connecteur de référentiel source par tâche.

Ajouter un nouveau connecteur

Pour créer un nouveau connecteur de référentiel de code source :

1. Entrez le numéro de AWS compte que vous souhaitez utiliser pour le AWS CodeConnections connecteur.
2. Si vous n'avez pas configuré AWS CodeConnections le même AWS compte, cliquez sur Configurer AWS CodeConnections.

3. Utilisez la console AWS Developer Tools pour créer une connexion à votre Bitbucket GitHub, GitHub Enterprise Server ou à votre AzureDevOpsréférentiel. GitLab
4. Copiez le nom de ressource Amazon (ARN) de la connexion que vous avez créée.
5. Retournez dans AWS Transform et collez l'ARN de la connexion que vous avez créée.
6. Entrez un nom pour le connecteur.

> **Note**
>
> Ne saisissez pas d'informations personnelles dans le nom du connecteur.

7. Sélectionnez Lancer la création du connecteur.
8. AWS Transform demande la création d'un connecteur pour le AWS compte que vous avez saisi, dans la même région que le travail de transformation en cours, et vous informe qu'une demande d'approbation est prête à être approuvée par votre AWS administrateur dans la console de AWS gestion. Sélectionnez Copier le lien de vérification.
9. Si vous êtes l' AWS administrateur, connectez-vous au AWS compte et cliquez sur le lien de vérification pour approuver la demande de connexion. Si vous n'êtes pas l' AWS administrateur, fournissez le lien de vérification à votre AWS administrateur.
10. Une fois que l' AWS administrateur a approuvé la demande de connecteur, sélectionnez Finaliser le connecteur pour terminer le processus de création du connecteur. Si vous souhaitez utiliser un autre connecteur, sélectionnez Redémarrer pour relancer le processus de création du connecteur.

L'onglet Collaboration inclut également des informations sur votre connecteur, notamment :

- État : Approuvé ou en attente d'approbation
- AWS ID de compte
- AWS Région
- ARN de connexion

Supprimer un connecteur existant

> **Note**
>
> Si vous disposez d'un connecteur de référentiel de code source existant, AWS Transform vous en informera. Sélectionnez Utiliser le connecteur existant ou Supprimer et créer un nouveau connecteur.

Si vous choisissez de supprimer une connexion au référentiel de code source existante, AWS Transform vous avertira avant de supprimer réellement le connecteur.

1. Vous pouvez supprimer un connecteur existant de plusieurs manières :
   a. Si AWS Transform vous y invite, vous pouvez sélectionner Supprimer et créer un nouveau connecteur.
   b. Vous pouvez également sélectionner redémarrer dans l'invite. Pour modifier ce connecteur, vous devez le redémarrer.
2. AWS Transform vous avertit que le redémarrage supprimera le connecteur. Pour supprimer le connecteur, sélectionnez Redémarrer à nouveau.
3. AWS Transform vous avertit à nouveau que la suppression du connecteur supprimera la connexion à votre référentiel tiers, tel que Bitbucket GitHub, et GitLab. En outre, toutes les tâches de AWS transformation utilisant ce connecteur échoueront si le connecteur est supprimé. Pour confirmer la suppression, tapez Supprimer, puis sélectionnez Supprimer.
4. Pour ajouter un nouveau connecteur de référentiel de code source, consultezAjouter un nouveau connecteur.

Connectez-vous au code source dans Amazon S3

Vous pouvez connecter AWS Transform au code source dans Amazon S3 au lieu de connecter un dépôt de code source.

Organisation du compartiment S3

Le code source original et le code transformé sont stockés dans un compartiment S3 commun, organisé comme indiqué ci-dessous. Vous devez configurer votre compartiment S3 dans la même région que votre tâche de AWS transformation. Téléchargez votre code source dans le bucket sous

forme de fichier zip au niveau de la racine. Le fichier zip doit contenir un dossier de premier niveau pour chaque dépôt.

Au cours de la AWS transformation, Transform crée un dossier de sortie de transformation et stocke les résultats de transformation dans ce dossier. La transformation crée un fichier zip nommé transformed-code.zip contenant le code transformé. Cela inclut un rapport sur les différences de code nommé diff.txt qui met en évidence les modifications apportées au fichier au niveau du projet.

```
<customer-bucket>/
### source-code.zip
         ### repo 1
         ### repo 2
         ### ......
         ### repo n
### transform-output/
      ### transformed-code.zip
```

Ajouter un nouveau connecteur S3

Pour créer un nouveau connecteur de référentiel de code source S3 :

1. Dans la AWS console, créez un compartiment S3.
2. Téléchargez votre code source sous forme de fichier zip dans le compartiment S3.
3. Dans l'application Web AWS Transform, lancez une tâche de transformation .NET. À l'étape Connecter un référentiel de code source, sélectionnez Connecter votre code source dans le compartiment S3 et choisissez Enregistrer.
4. Sur la page suivante, entrez les détails de votre compartiment S3 et choisissez Soumettre.
   a. Nom du connecteur
   b. AWS Identifiant du compte
   c. Arne à godets S3
   d. Clé de chiffrement du compartiment S3 (facultatif)
5. Approuvez le connecteur :
   a. Sur la page suivante, copiez le lien de vérification.
   b. Demandez à un approbateur de parcourir le lien pour accéder à la page de demande de création du connecteur AWS Transform.

c. Choisissez de créer un nouveau rôle ou d'utiliser un rôle existant.

d. Après avoir examiné la demande, choisissez Enregistrer et approuver pour l'approuver.

6. Spécifiez l'emplacement du fichier zip S3 :

a. Dans l'application Web AWS Transform, attendez que le statut indique Approuvé.

b. Sur la page Spécifier l'emplacement de la ressource, entrez une URL S3 pour le fichier de code zip au format `s3://bucket-name/zip-file-name` et choisissez Envoyer pour AWS transformer.

c. La tâche passe à l'étape Découverte pour poursuivre la transformation.

Supprimer un connecteur S3

Pour supprimer un connecteur S3 existant :

1. Dans l'application Web AWS Transform, sélectionnez Gérer les connecteurs en haut à droite.
2. Dans la fenêtre Gérer les connecteurs, sélectionnez le connecteur.
3. Sélectionnez Delete (Supprimer).

Confirmation de vos référentiels pour préparer la transformation

EnsuiteCréation d'un connecteur de référentiel de code source, confirmez vos référentiels comme première étape de préparation à la transformation. Vous pouvez effectuer les actions suivantes :

- Passez en revue et modifiez Paramètres par défaut le contenu du plan.
- Passez en revue les référentiels découverts et sélectionnez ceux à évaluer en vue de leur transformation.
- Consultez le rapport d'évaluation du référentiel et discutez de son contenu avec AWS Transform.
- Utilisez le plan généré par AWS Transformation.
- Personnalisez le plan de transformationà l'aide de l'application Web ou en téléchargeant un fichier JSON, en le modifiant et en le chargeant dans AWS Transform.

Paramètres par défaut

Dans la section Détails du Job de l'onglet Collaboration, vous pouvez définir les paramètres suivants :

Dans l'onglet Tâches, à l'étape Préparer la transformation - Confirmer les référentiels à transformer, vous pouvez définir les paramètres suivants :

- Définissez le nom de la branche cible dans laquelle le code transformé est écrit dans votre référentiel.
- Définissez la version .NET cible :
  - .NET 8 : transformer tous les projets en .NET 8
  - .NET 10 : transformer tous les projets en .NET 10
- Vous pouvez mettre à jour les paramètres du Job par défaut ou les laisser tels quels. Il s’agit des licences suivantes :
  - Exclure les projets .NET Standard du plan de transformation Ce paramètre est sélectionné par défaut. Lorsque cette option est sélectionnée, AWS Transform exclut tous les projets .NET Standard du plan de transformation. Si vous désélectionnez ce paramètre, les projets .NET Standard seront transformés, ce qui les rendra incompatibles avec le .NET Framework.
  - Vérifiez les NuGet sources et obtenez les versions de package compatibles .NET AWS Autorisez Transform à rechercher et à obtenir des versions de package compatibles .NET pour le code que vous souhaitez transformer.

Consultez le rapport d'évaluation du référentiel

Le rapport d'évaluation du référentiel fournit une vue tabulaire des informations relatives à chaque référentiel détecté par AWS Transform. Cela inclut notamment les éléments suivants :

- Propriétaire du référentiel
- Branche évaluée
- Nombre de solutions
- Nombre de projets
- Nombre total de lignes de code
- Versions .NET détectées
- Types de projets détectés
- Nombre de dépendances Nuget privées
- Nombre de dépendances Nuget publiques
- Complexité de transformation

Pour télécharger le fichier :

1. Dans votre espace de travail, sélectionnez l'onglet Collaboration.
2. Dans le volet Choisir les référentiels, sélectionnez Télécharger, puis sélectionnez Télécharger au format HTML ou Télécharger au format JSON

Discuter du rapport récapitulatif du dépôt

Le résumé de votre dépôt peut être très long. Utilisez le chat pour mieux comprendre son contenu. Votre rapport est disponible pour le chat lorsque vous voyez ce message dans l'onglet Worklog : le rapport d'évaluation est désormais disponible dans le chat pour les requêtes. Pour ouvrir le chat, cliquez sur l'icône hexagonale violette dans le coin inférieur droit de la console Web. Voici quelques exemples d'instructions :

- Répertoriez tous les référentiels découverts ou évalués.
- Combien de projets .NET 6 ont été découverts lors de l'évaluation ?
- Quels sont les projets les plus complexes ?

Utilisez le plan généré par AWS Transformation

Vous pouvez choisir d'utiliser le plan de AWS transformation créé à partir de la découverte de référentiels présentant une probabilité de réussite de transformation plus élevée, qui inclut les référentiels les plus récents, les référentiels root et les référentiels interdépendants.

AWS Transform répertorie quelques détails de haut niveau sur le plan de transformation, notamment :

- Nombre total de référentiels découverts Nombre de référentiels .NET existants découverts par AWS Transform à l'aide de votre connecteur de référentiel de code source. AWS Transform peut scanner un maximum de 1 000 référentiels par tâche. Si vous avez d'autres référentiels à scanner ou à transformer, vous pouvez créer plusieurs tâches de transformation.
- Référentiels sélectionnés Nombre de référentiels .NET hérités sélectionnés par AWS Transform pour la transformation.
- Dépendances sélectionnées Nombre de dépendances requises par les référentiels sélectionnés, que AWS Transform a détectées automatiquement et ajoutées au plan de transformation.

Le tableau Référentiels sélectionnés répertorie les référentiels sélectionnés. Vous pouvez rechercher des référentiels par nom, accéder à des pages supplémentaires de référentiels et télécharger un fichier au format JSON répertoriant les référentiels sélectionnés et leurs dépendances. Vous pouvez apporter des modifications dans cette vue.

Le tableau Référentiels sélectionnés répertorie les informations suivantes concernant les référentiels sélectionnés par AWS Transform pour la transformation :

- Nom du référentiel
- Branche source
- Date et heure de dernière modification
- Lignes de code Cela vous permet de voir si vous approchez de vos limites de quotas. Pour de plus amples informations, veuillez consulter Quotas pour AWS Transformation.
- Référentiels dépendants Vous pouvez cliquer sur le nombre de référentiels dépendants pour afficher plus de détails sur ces dépendances.

Si vous êtes satisfait du plan de AWS transformation généré par Transform, sélectionnez Confirmer les référentiels.

Si vous souhaitez apporter des modifications au plan de AWS transformation généré par Transform, sélectionnezPersonnalisez le plan de transformation.

Personnalisez le plan de transformation

Si vous choisissez de ne pas le faireUtilisez le plan généré par AWS Transformation, vous pouvez personnaliser la liste des référentiels à transformer à l'aide de l'une des options suivantes :

1. Sélectionnez les référentiels dans le tableau Référentiels sélectionnés.
   a. Lorsque vous ajoutez un référentiel au plan, AWS Transform sélectionne pour vous les dépendances du référentiel et les ajoute automatiquement au plan de transformation.
   b. Vous pouvez également désélectionner les référentiels dans le tableau.
2. Téléchargez la liste JSON des dépôts et des branches générée par AWS Transform.
   a. Sélectionnez Télécharger, puis sélectionnez Télécharger au format JSON.
   b. Vérifiez et modifiez le JSON. Vous pouvez supprimer des référentiels, ou des solutions au sein de référentiels, que vous ne souhaitez pas transformer.
   c. Téléchargez le JSON révisé en sélectionnant Télécharger un plan personnalisé.

d. Si le téléchargement du fichier JSON est réussi, le tableau des référentiels sélectionnés affiche les sélections que vous avez effectuées.

3. Vous pouvez sélectionner Afficher les dépôts dépendants pour afficher la liste des référentiels dont AWS Transform a découvert qu'ils étaient des dépendances pour les référentiels que vous avez sélectionnés.
4. Vous pouvez répéter ces étapes si nécessaire. Lorsque vous êtes satisfait de votre plan personnalisé, sélectionnez Confirmer les référentiels.

Résolution des dépendances entre les packages pour préparer la transformation

EnsuiteConfirmation de vos référentiels pour préparer la transformation, si AWS Transform trouve des dépendances de package manquantes, vous devez effectuer cette étape. Vous pouvez exécuter un PowerShell script Windows pour récupérer les dépendances de package manquantes sur le même appareil que votre environnement de Visual Studio développement, ou vous pouvez récupérer les packages manquants manuellement. Ensuite, téléchargez les packages manquants.

Les dépendances de package manquantes peuvent être mises à jour de deux manières :

- Résolution à l'aide du connecteur Artifact : résolvez en configurant un référentiel d'artefacts (NuGet connecteur ADO) via un flux de travail HITL dédié à Connect Artifact Repository, qui s'affiche lorsqu'un connecteur d'artefacts n'est pas configuré et que des packages sont manquants.
- Mettre à jour le package manquant : AWS Transform répertorie les packages manquants dans le tableau des dépendances des packages manquants. Vous pouvez rechercher un package manquant par son nom dans le champ de recherche. Ce tableau contient les informations suivantes concernant les packages manquants :
  - Nom
  - Référentiels associés
  - État de la version du framework
  - État de la version principale

Pour résoudre les dépendances de package manquantes,Téléchargez les packages manquants.

Téléchargez les packages manquants

1. Si vous le souhaitez, vous pouvez télécharger un script d' PowerShell assistance Windows pour récupérer les dépendances de package manquantes dans votre environnement de Visual Studio développement. Vous pouvez également rechercher les packages manquants manuellement.

   Pour utiliser le PowerShell script Windows, procédez comme suit :

   a. Sélectionnez Télécharger le PowerShell script Windows.
   b. Exécutez le script localement avec une connexion active aux référentiels contenant les fichiers de dépendance des packages manquants.
   c. Ce script vous permet de télécharger les dépendances de package manquantes dans votre environnement local.
2. Le script créera un fichier zip unique que vous pourrez télécharger, qui inclut toutes les dépendances dans une seule archive. Vous pouvez également télécharger des fichiers individuels `.nupkg` ou des fichiers zip pour chaque dépendance.
3. Sélectionnez Charger les fichiers du package.
4. Dans le mode Télécharger les fichiers de dépendance, sélectionnez Choisir les fichiers et accédez à l'emplacement des fichiers de package manquants compressés sur votre appareil.
5. Sélectionnez Téléverser.
6. AWS Transform valide les fichiers que vous avez chargés. Pendant la validation, vous ne pouvez effectuer aucune mise à jour. AWS Transform indique l'état de validation au-dessus du tableau des dépendances des packages manquants.
7. AWS Transform met également à jour les colonnes d'état du tableau des dépendances de package manquantes de Missing à Resolved. Si la validation d'un package échoue, son statut devient invalide. Pour les fichiers non valides, procédez comme suit :

   a. Dans le tableau Dépendances de package manquantes, sélectionnez le package non valide à l'aide de la case à cocher.
   b. Sélectionnez Supprimer le fichier téléchargé.
   c. Cela ramène son statut à Disparu.
8. Une fois que vous avez chargé les packages manquants et résolu les dépendances des packages, sélectionnez Procéder à la révision.

   Si vous sélectionnez Procéder à la révision sans résoudre les dépendances de package manquantes, AWS Transform vous demande si vous souhaitez démarrer le travail de transformation sans les packages manquants. Si vous sélectionnez Ignorer les dépendances de

package manquantes, AWS Transform utilisera des références d'assemblage pour transformer le code. La poursuite de cette action peut affecter les ressources associées.

Exigences relatives à la structure des dossiers

Pour les NuGet téléchargements, AWS Transform nécessite soit :

- Le `.nuspec` fichier à placer à la racine pour les packages chargés manuellement, ou
- Utilisation du PowerShell script fourni pour générer la structure correcte

Exigences relatives à la correspondance des versions

- État du framework : AWS Transform tente de faire correspondre la version de la dépendance spécifiée dans le `.csproj` fichier (code source) à la version de la dépendance téléchargée. Une correspondance exacte se traduit par un statut de réussite.
- État de base : AWS Transform attend une spécification de version de base dans la section des dépendances du `.nuspec` fichier téléchargé. Si l'un d'entre eux est trouvé, le statut de base est Succès.

  Exemple de format :

  ```
  <dependencies>
      <group targetFramework="net8.0" />
  </dependencies>
  ```

  Les versions courantes incluent :

  - .NET 5.0 (net5.0)
  - .NET 6.0 (net6.0)
  - .NET 7.0 (net 7.0)
  - .NET 8.0 (net 8.0)

Révision de votre plan pour préparer la transformation

Ensuite Confirmation de vos référentiels pour préparer la transformationRésolution des dépendances entre les packages pour préparer la transformation, l'administrateur du AWS compte doit revoir le plan de transformation et l'approuver dans AWS Transform.

AWS Transform affiche la liste des référentiels, des référentiels dépendants et des packages dépendants sélectionnés pour la transformation de la tâche.

Révision du plan de transformation

AWS Transform affiche la liste des référentiels, des référentiels dépendants et des packages dépendants sélectionnés pour la transformation de la tâche.

> **Note**
>
> AWS Transform peut transformer un maximum de 100 dépendances et référentiels par plan de transformation.

1. Si vous n'êtes pas l'administrateur du AWS compte, consultez le plan de travail et, si vous l'acceptez, sélectionnez Envoyer pour approbation.
2. Si vous êtes l'administrateur du AWS compte, vous devez revoir le plan et, une fois prêt, l'approuver pour démarrer la transformation. Après avoir examiné le plan de travail, sélectionnez l'une des options suivantes :
   a. Rejeter Si la tâche a été créée par un utilisateur qui n'est pas l'administrateur du AWS compte, nous vous suggérons de demander au créateur de la tâche de redémarrer la tâche.
   b. Approuvez et lancez la transformation.

L'évaluation du poste inclut les détails suivants :

1. Résumé du poste Cela inclut :
   a. Branche cible dans laquelle AWS Transform placera le code transformé.
   b. La version .NET cible, .NET 8.0 ou .NET 10.
   c. Les paramètres de la tâche :
      i. Exclure les projets standard .NET
   d. Nombre de référentiels sélectionnés pour la transformation
   e. Nombre de référentiels dépendants
   f. Nombre de NuGet forfaits privés
   g. Nombre total de lignes de code pour la tâche
2. Référentiels sélectionnés Il s'agit des référentiels sélectionnés pour la transformation. Il doit s'agir de MVC, Web, Windows Communication Foundation (WCF), console, bibliothèque de classes,

framework d'interface utilisateur (pages Razor) ou packages de tests unitaires. Ce tableau contient les informations suivantes :

a. Nom

b. Branche source

c. Projets soutenus

d. Lignes de code

e. Projets détectés

f. Projets ignorés

g. Dépendances détectées

3. Référentiels dépendants ajoutés Il s'agit des référentiels dépendants ajoutés pour la transformation. Il doit s'agir de MVC, Web, Windows Communication Foundation (WCF), console, bibliothèque de classes, framework d'interface utilisateur (pages Razor) ou packages de tests unitaires. Ce tableau contient les informations suivantes :

   a. Nom

   b. Nécessaire par

   c. Branche source

   d. Projets soutenus

   e. Lignes de code

   f. Projets détectés

   g. Projets ignorés

4. Packages dépendants Il s'agit des packages dépendants ajoutés pour la transformation. Il doit s'agir de MVC, Web, Windows Communication Foundation (WCF), console, bibliothèque de classes, framework d'interface utilisateur (pages Razor) ou packages de tests unitaires. Ce tableau contient les informations suivantes :

   a. Nom

   b. Référentiels associés

   c. État de la version du framework

   d. État de la version principale

Transformation de votre code .NET

Une fois que l'administrateur du AWS compte a terminéRévision de votre plan pour préparer la transformation, vous pouvez consulter la progression de la transformation dans l'onglet Tableau de bord de votre tâche de transformation.

> **Note**
>
> Outre la transformation des référentiels et des dépendances, AWS Transform peut exécuter des projets de tests unitaires entièrement transformés (aucune erreur de construction). AWS Transform n'a pas accès aux résultats des tests unitaires avant la transformation et ne peut partager que les résultats après la transformation. Vous pouvez ensuite comparer vos données de référence, avant la transformation, avec les résultats obtenus après la transformation afin de comprendre les éventuelles lacunes.

Dans le coin supérieur droit, vous pouvez voir le statut de la tâche, qui possède l'une des valeurs suivantes :

- En attente de saisie par l'utilisateur
- Temps écoulé
- En cours d'exécution

Vous pouvez également voir les icônes suivantes :

- Une icône d'arrêt de la transformation
- Une icône d'actualisation
- Une icône de paramètres

Le tableau de bord fournit un résumé de haut niveau de la transformation. Il indique les indicateurs du nombre d'emplois transformés et de transformations appliquées, ainsi que le temps estimé pour terminer la transformation.

Le tableau de bord inclut :

1. La section Détails du travail de transformation, qui répertorie les paramètres par défaut et les détails du travail de transformation, notamment :

   a. Destination de la branche cible Pour transformer votre code, AWS Transform crée une nouvelle branche pour le code transformé dans votre dépôt de code.
   b. Version .NET cible, .NET 8.0 ou .NET 10
   c. L'ID de la tâche AWS Transform.
   d. Les paramètres de la tâche :
      i. Exclure les projets standard .NET
2. La section Récapitulatif de la transformation contient :
   a. Le nombre de référentiels sélectionnés pour la transformation
   b. Le nombre de projets à transformer
   c. Le nombre total de lignes de code dans ces référentiels et projets

Une fois la transformation lancée, des diagrammes circulaires apparaissent dans les sections État du référentiel, État du package et statut des tests unitaires pour afficher la progression en temps réel. L'état des tests unitaires indique l'état des tests unitaires situés dans vos référentiels que AWS Transforms exécute après la transformation pour tester le code transformé. AWS Transform partage les résultats des tests exécutés, ainsi que le nom de chaque test, afin que les clients puissent consulter la liste des tests unitaires réussis et échoués.

> **Note**
>
> La section Référentiels répertorie les référentiels recommandés par AWS Transform ou que vous avez sélectionnés pour la transformation. Sélectionnez Télécharger le JSON pour télécharger la liste des référentiels, des dépendances et des packages de votre plan de transformation.

Consultez les rapports de transformation

Une fois le travail de transformation terminé, vous pouvez télécharger les rapports de transformation :

- Rapport de synthèse de la transformation : ce rapport fournit une vue d'ensemble de la transformation au format HTML ou JSON. Téléchargez le rapport récapitulatif de transformation depuis l'onglet Tableau de bord. Sélectionnez Télécharger, puis choisissez Télécharger au format HTML ou Télécharger au format JSON.
- Rapport détaillé de transformation : ce rapport fournit des informations détaillées sur une transformation au format HTML. Téléchargez les rapports détaillés des transformations depuis

l'onglet Tableau de bord. Sélectionnez le lien Télécharger le rapport détaillé dans la liste des référentiels pour télécharger un rapport détaillé.

Discutez avec AWS Transformation à propos du rapport de transformation

Vous pouvez discuter avec AWS Transform du rapport de transformation une fois qu'un référentiel a été complètement traité ou une fois le travail de transformation terminé. L'onglet Worklog affiche ce message pour chaque référentiel disponible pour le chat : les détails de *`repository_name`* transformation du référentiel sont désormais disponibles dans le chat pour les requêtes. Il affiche ce message lorsque le travail de transformation est terminé : Le travail de AWS transformation est terminé.

Pour ouvrir le chat, cliquez sur l'icône hexagonale violette dans le coin inférieur droit de la console Web.

Voici quelques exemples d'instructions :

- Quels projets ont été transformés avec succès ?
- Quels projets ont été partiellement portés ?
- Quelles modifications ont été apportées au `repo_name` référentiel ?
- Quels packages ont été mis à niveau dans le `project_name` cadre du projet ?

Modernisation du .NET dans l'IDE

AWS Transform inclut un assistant d'intelligence artificielle agentique et interactif dans le AWS kit d'outils pour. Visual Studio Il vous permet de moderniser les applications grâce à une expérience conversationnelle guidée étape par étape directement dans votre IDE. Pour transformer une solution ou un projet .NET, l'agent AWS Transform analyse votre base de code, détermine les mises à jour nécessaires pour porter votre application et génère un rapport d'évaluation et un plan de transformation avant le début de la transformation.

L'expérience Visual Studio IDE prend uniquement en charge l'authentification par IAM Identity Center. Pour de plus amples informations, veuillez consulter Ajouter des utilisateurs dans IAM Identity Center.

L'expérience IDE propose des modes autonomes et interactifs. Utilisez le mode autonome pour une transformation sans surveillance, adapté aux tâches nocturnes ou de longue durée. Utilisez le mode interactif pour travailler aux côtés de l'agent dans le chat, avec une grande visibilité sur la

transformation, un plan de transformation personnalisable et un examen étape par étape de chaque projet. Vous pouvez itérer pour affiner les résultats ou changer de direction jusqu'à ce que vous soyez satisfait.

Lorsqu'une tâche de transformation est active, vous pouvez interagir avec trois fenêtres :

- La fenêtre de discussion est votre principal point d'interaction avec l'agent de transformation. Utilisez le chat pour poser des questions, discuter des options, piloter la transformation et itérer.
- La fenêtre AWS Transform Job Plan indique les étapes de progression et vous permet de télécharger ou de charger des artefacts ou de consulter les différences de modification du code.
- La fenêtre Worklog affiche un journal des activités de transformation en langage naturel.

AWS Transform exécute quatre tâches principales pour porter des applications .NET vers Linux :

- Met à niveau les versions .NET et linguistiques : met à niveau l'ancien code .NET C# vers les versions .NET et linguistiques actuelles.
- Migration du .NET Framework vers le .NET multiplateforme : migre les projets et les packages du .NET Framework dépendant de Windows vers un .NET multiplateforme compatible avec Linux.
- Réécrit le code pour assurer la compatibilité avec Linux : refactorise et réécrit les composants de code obsolètes et inefficaces.
- Génère un rapport de compatibilité Linux : pour les tâches ouvertes nécessitant l'intervention de l'utilisateur pour créer et exécuter le code sous Linux, AWS Transform fournit un rapport détaillé des actions nécessaires pour configurer votre application après la transformation.

Pour plus d'informations sur la manière dont AWS Transform exécute les transformations .NET, consultezComment ? AWS Transform modernise les applications .NET.

Pour moderniser votre code .NET à l'aide de AWS Transform from Visual Studio IDE, reportez-vous à ce qui suit :

- Modernisation de .NET à l'aide de AWS Transformez-vous en Visual Studio
- Comment ? AWS Transform modernise les applications .NET
- Résolution des problèmes liés aux transformations .NET dans l'IDE

Quotas

Pour les quotas de transformation de AWS Transform .NET dans l'IDE, consultezQuotas pour AWS Transformation.

Modernisation de .NET à l'aide de AWS Transformez-vous en Visual Studio

Procédez comme suit pour porter une application Windows-based .NET vers une application .NET Linux-compatible multiplateforme avec AWS Transform en Visual Studio 2026 ou 2022.

Étape 1 : Prérequis

Avant de continuer, assurez-vous d'avoir téléchargé et installé l'extension AWS Toolkit avec Amazon Q depuis Visual Studio Marketplace. Passez en revue les fonctionnalités et les limites de AWS transformation pour la modernisation du .NET afin de vous assurer que votre code peut être transformé.

Étape 2 : Authentification dans Visual Studio

Pour vous connecter à vos AWS comptes depuis le Toolkit for Visual Studio, ouvrez l'interface utilisateur Getting Started with the AWS Toolkit (interface utilisateur de connexion) :

1. Dans le menu principal de Visual Studio, accédez à Extensions > AWS Boîte à outils > Getting Started pour ouvrir la page Getting Started : AWS Toolkit.
2. Sélectionnez AWS Transformer l'authentification.
3. Choisissez un profil existant ou créez-en un nouveau. Lorsque vous créez un nouveau profil, entrez le nom du profil et l'URL de démarrage de la AWS transformation, qui vous a été envoyée par e-mail après votre ajout à IAM Identity Center par votre administrateur.
4. Choisissez Se connecter. Suivez les instructions pour vous connecter et accorder des autorisations d'accès via votre navigateur Web. Dans Visual Studio, vous devriez voir Connected with IAM Identity Center.
5. Une fois connecté, vous êtes redirigé vers le tableau de bord AWS Transform. À partir de cette page de destination, vous pouvez effectuer les opérations suivantes :

   - Sélectionnez un profil de AWS transformation (région)
   - Sélectionnez ou créez un espace de travail
   - Afficher l'état des tâches de transformation

Étape 3 : Transformez votre application

Pour transformer votre solution ou votre projet .NET, procédez comme suit :

Commencer la transformation

1. Ouvrez n'importe quelle solution ou projet C# ou VB.NET basé sur le langage C# Visual Studio que vous souhaitez transformer.
2. Dans l'Explorateur de solutions, cliquez avec le bouton droit sur une solution ou un projet que vous souhaitez transformer, puis choisissez Port with AWS Transform.
3. La boîte de dialogue Port with AWS Transform apparaît.

    a. Dans le menu déroulant Choisissez un espace de travail, créez un espace de travail ou sélectionnez-en un existant. Les espaces de travail rendent votre activité visible dans l'application Web AWS Transform, où vous pouvez inviter des collaborateurs à consulter les tâches de transformation et à discuter à ce sujet.

    b. Dans le menu déroulant Choisir une cible .NET, sélectionnez la version .NET vers laquelle vous souhaitez effectuer la mise à niveau.

    c. Pour le mode de transformation, sélectionnez Autonome pour une transformation sans assistance ou Interactif pour une transformation interactive.

    d. Choisissez Démarrer pour commencer la transformation.
4. Une fois le travail de transformation démarré, les fenêtres AWS Transform Job Plan, Chat et Worklog apparaissent.

Plan d'évaluation et de transformation

1. Une fois que AWS Transform a analysé votre code, un rapport d'évaluation et un plan de transformation sont affichés dans le chat. En mode interactif, le chat s'interrompt pour que vous puissiez les consulter. Si vous préférez ne pas donner de commentaires dans le chat, vous pouvez utiliser les alternatives suivantes :

    - Pour consulter l'évaluation ou le plan dans l'éditeur de code, choisissez Afficher l'évaluation ou Afficher le plan de transformation dans la fenêtre AWS Transform Job Plan.
    - Pour télécharger l'évaluation ou le plan, utilisez l'icône de téléchargement dans la fenêtre Job Plan.
2. Modifiez éventuellement le plan de transformation. Vous pouvez discuter du plan par chat, par exemple en explorant d'autres options. Vous pouvez modifier le plan en donnant des instructions dans le chat ou en téléchargeant un plan de transformation révisé à l'aide de l'icône de téléchargement dans la fenêtre Job Plan. Vous pouvez librement ajouter, supprimer ou modifier des étapes. Chat confirmera qu'il a bien compris vos instructions avec un plan révisé.

3. Téléchargez éventuellement les documents de pilotage. Dans la fenêtre de discussion, utilisez l'icône de téléchargement pour télécharger des documents de pilotage tels que les spécifications de l'application, les préférences et conventions technologiques de l'organisation, ou des exemples de codage. Après avoir téléchargé un document de pilotage, décrivez-le dans la fenêtre de discussion pour donner du contexte à l'agent.
4. Une fois que vous êtes satisfait du plan, approuvez-le par chat et la transformation commencera.
5. En mode interactif, vous pouvez définir des points de contrôle pour qu'ils s'arrêtent une fois qu'un projet est transformé pour révision. Les étapes décrites dans la section Transformation du code dans la fenêtre Job Plan comporteront des icônes de point de contrôle rondes. Tous les projets ont des points de contrôle activés par défaut. Utilisez les cases à cocher pour effacer ou définir un point de contrôle.

Transformation et examens des points de contrôle

1. AWS Transform commence à transformer votre code. Vous pouvez suivre la progression des étapes de transformation dans la fenêtre AWS Transform Job Plan. La fenêtre Job Plan affiche le temps maximum estimé restant et votre numéro de Job.
2. Au fur et à mesure que les projets sont transformés, les résumés sont affichés dans le chat et les modifications de code sont appliquées.
3. En mode interactif, lorsqu'un point de contrôle est atteint, l'agent fait une pause pour que vous puissiez consulter les résultats. Dans la fenêtre Job Plan, vous verrez un bouton Afficher les résultats correspondant à l'étape pendant laquelle il est suspendu et où vous pouvez examiner les différences de code. Après avoir examiné les modifications, vous pouvez demander d'autres modifications dans le chat ou apporter vous-même des modifications au codeVisual Studio.
4. Vous pouvez itérer au point de contrôle autant que vous le souhaitez. Lorsque vous êtes satisfait, demandez au chat de continuer, et il passera au projet suivant.

Fin de la transformation

1. Après avoir transformé vos projets, l'agent .NET déclenchera une intégration locale pour confirmer que le code est correctement généré sur votre machine locale. Visual Studio S'il y a des erreurs, il s'efforcera de les résoudre.
2. Une fois la transformation terminée, des étapes supplémentaires peuvent être nécessaires, telles que des tâches de transformation que AWS Transform n'a pas pu effectuer ou des modifications nécessaires pour assurer la compatibilité avec Linux. Un fichier Markdown pour les prochaines

étapes (NextSteps.md) est disponible en téléchargement et vous pouvez l'utiliser comme guide pour accéder à un compagnon de code AI. Utilisez l'icône de téléchargement de la fenêtre Job Plan pour le télécharger NextSteps.md.

3. Vous pouvez continuer à interagir dans le chat pour poser des questions ou demander des modifications supplémentaires.
4. Dites au chat quand vous êtes prêt à terminer votre travail de transformation.

Comment ? AWS Transform modernise les applications .NET

Consultez les sections suivantes pour en savoir plus sur le fonctionnement de la transformation .NET avec AWS Transform.

Analyse de votre application et génération d'un plan de transformation

Avant le début d'une transformation, AWS Transform crée votre code localement pour vérifier qu'il est compilable et correctement configuré pour la transformation. Si le code n'est pas compilé, AWS Transform vous demandera s'il convient de poursuivre la transformation. AWS Transform télécharge ensuite votre code dans un environnement de génération sécurisé et crypté AWS, analyse votre base de code et détermine les mises à jour nécessaires pour porter votre application

Au cours de cette analyse, AWS Transform divise votre solution ou projet .NET en groupes de codes. Un groupe de code est un projet et toutes ses dépendances qui, ensemble, génèrent une unité de code constructible telle qu'une bibliothèque de liens dynamiques (DLL) ou un exécutable. Même si vous n'avez pas sélectionné toutes les dépendances du projet à AWS transformer, Transform détermine les dépendances nécessaires pour créer les projets que vous avez sélectionnés et les transforme également, afin que votre application transformée puisse être créée et prête à être utilisée.

Après avoir analysé votre code, AWS Transform génère un plan de transformation qui décrit les modifications proposées, y compris une liste des groupes de codes et de leurs dépendances qui seront transformés.

Transformation de votre application

Pour démarrer la transformation, AWS Transform crée à nouveau votre code dans l'environnement de génération sécurisé afin de vérifier s'il peut être créé à distance. AWS Transform commence ensuite le portage de votre application. Cela fonctionne de façon ascendante, en commençant par le niveau de dépendance le plus bas. Si AWS Transform rencontre un problème lors du portage d'une dépendance, il arrête la transformation et fournit des informations sur la cause de l'erreur.

La transformation inclut les mises à jour suivantes de votre application :

- Remplacement des versions obsolètes du code C# par des versions Linux-compatible C#
- Mise à niveau de .NET Framework vers .NET multiplateforme, y compris :
  - Identification et remplacement itératif des packages, des bibliothèques et des API
  - Mise à niveau et remplacement de NuGet packages et d'API
  - Transition vers un environnement d'exécution multiplateforme
  - Configuration de l'intergiciel et mise à jour des configurations d'exécution
  - Remplacement de packages privés ou tiers
  - Gestion des composants IIS et WCF
  - Débogage des erreurs de compilation
- Réécriture de code pour la compatibilité avec Linux, notamment refactorisation et réécriture de code obsolète et inefficace pour porter le code existant

Examen du rapport de transformation et acceptation des modifications

Une fois la transformation terminée, AWS Transform fournit un rapport de transformation contenant des informations sur les mises à jour proposées pour votre application, notamment le nombre de fichiers modifiés, de packages mis à jour et d'API modifiées. Il signale toute transformation infructueuse, y compris les fichiers ou parties de fichiers concernés, ainsi que les erreurs rencontrées lors d'une tentative de compilation. Vous pouvez également consulter un résumé de build avec les journaux de build pour en savoir plus sur les modifications apportées.

Le rapport de transformation fournit également un état du portage Linux, qui indique si une intervention supplémentaire de l'utilisateur est nécessaire pour rendre l'application compatible avec Linux. Si l'un des éléments d'un groupe de codes nécessite une saisie de votre part, vous téléchargez un rapport de préparation à Linux qui contient des Windows-specific considérations que AWS Transform n'a pas pu prendre en compte au moment de la création. Si des informations sont nécessaires pour des groupes de code ou des fichiers, consultez le rapport pour plus de détails sur le type de modification qui doit encore être apporté et, le cas échéant, pour obtenir des recommandations sur la manière de mettre à jour votre code. Ces modifications doivent être effectuées manuellement avant que votre application puisse être exécutée sous Linux.

Vous pouvez consulter les modifications proposées par AWS Transform dans une vue diff avant de les accepter en tant que mises à jour sur place de vos fichiers. Après avoir mis à jour vos fichiers et

traité tous les éléments du rapport de préparation à Linux, votre application est prête à fonctionner sur .NET multiplateforme.

Vous pouvez télécharger un fichier de balisage Next Steps contenant des instructions pour poursuivre la transformation avec AWS Transform ou un compagnon de code AI. Pour télécharger le fichier, cliquez sur le bouton Télécharger les étapes suivantes en haut à droite du rapport.

Résolution des problèmes liés aux transformations .NET dans l'IDE

Utilisez les sections suivantes pour résoudre les problèmes courants liés aux transformations .NET dans l'IDE avec AWS Transform.

Comment savoir si une tâche progresse ?

Vous devriez voir une activité régulière dans la fenêtre Worklog. Si AWS Transform semble consacrer beaucoup de temps à une étape de la fenêtre AWS Transform Job Plan, vous pouvez vérifier si la tâche est toujours active dans les journaux de sortie. Si des messages de diagnostic sont générés, la tâche est toujours active.

Pour vérifier les sorties, choisissez l'onglet Sortie dansVisual Studio. Dans le menu Afficher la sortie depuis :, choisissez Client de langage Amazon Q.

La capture d'écran suivante montre un exemple des sorties générées par AWS Transform lors d'une transformation.

Pourquoi certains projets ne sont-ils pas sélectionnés pour la transformation ?

AWS Transform ne peut transformer que les types de projets .NET pris en charge. Pour obtenir la liste des types de projets pris en charge et les autres conditions préalables à la transformation de vos projets .NET, consultez Étape 1 : Prérequis.

Comment puis-je obtenir de l'aide si mon projet ou ma solution ne se transforme pas ?

Si vous n'êtes pas en mesure de résoudre les problèmes vous-même, vous pouvez contacter votre Compte AWS équipe pour Support soumettre un dossier d'assistance.

Pour obtenir de l'aide, fournissez l'identifiant de la tâche de transformation afin de AWS pouvoir enquêter sur une tâche ayant échoué. Pour trouver un identifiant de tâche de transformation, cliquez sur l'onglet Sortie dansVisual Studio. Dans le menu Afficher la sortie depuis :, choisissez Client de langage Amazon Q.

Comment puis-je empêcher mon pare-feu d’interférer avec les tâches de transformation ?

Si votre entreprise utilise un pare-feu, celui-ci peut interférer avec les transformations dansVisual Studio. Vous pouvez désactiver temporairement les contrôles de sécurité Node.js pour résoudre les problèmes ou tester les facteurs qui empêchent l'exécution de la transformation.

La variable d’environnement `NODE_TLS_REJECT_UNAUTHORIZED` contrôle les contrôles de sécurité importants. Le réglage `NODE_TLS_REJECT_UNAUTHORIZED` sur « 0 » désactive Node.js le rejet des certificats non autorisés TLS/SSL . Autrement dit :

- Self-signed les certificats seront acceptés
- Les certificats expirés seront autorisés
- Les certificats dont les noms d’hôtes ne correspondent pas seront autorisés
- Toute autre erreur de validation du certificat sera ignorée

Si votre proxy utilise un autocertificat, vous pouvez définir les variables d’environnement suivantes au lieu de désactiver `NODE_TLS_REJECT_UNAUTHORIZED` :

```
NODE_OPTIONS = –use-openssl-ca
NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs
```

Sinon, vous devez spécifier les certificats CA utilisés par le proxy pour désactiver `NODE_TLS_REJECT_UNAUTHORIZED`.

Pour désactiver NODE_TLS_REJECT_UNAUTHORISED sous Windows :

1. Ouvrez le menu Démarrer et recherchez les variables d’environnement.
2. Choisissez Modifier les variables d’environnement système.
3. Dans la fenêtre Propriétés du système, choisissez Variables d’environnement.
4. Sous Variables du système, sélectionnez Nouveau.
5. Définissez Nom de la variable sur NODE_TLS_REJECT_UNAUTHORISED et Valeur de la variable sur 0.

6. Choisissez OK pour enregistrer les modifications.
7. Redémarrez Visual Studio.

Portage du code de couche d'interface utilisateur

AWS Transform peut porter la couche d'interface utilisateur des ASP.NET sites Web vers des frameworks d'interface utilisateur compatibles avec ASP.NET Core, qui peuvent fonctionner sous Linux. Les transformations suivantes sont disponibles :

- Portage de l'interface utilisateur MVC Razor
- Portage de formulaires Web vers l'interface utilisateur Blazor

Portage de l'interface utilisateur MVC Razor

ASP.NET Les projets MVC avec l'interface utilisateur Razor Views peuvent être portés vers MVC Razor Views on ASP.NET Core, en restant sur le même framework d'interface utilisateur. Bien que les points de vue de Razor soient similaires entre ceux de ASP.NET Core ASP.NET et ceux de Razor, certaines différences nécessitent des modifications du code de portage :

- ASP.NET Les vues MVC Razor utilisent l'espace de System.Web.Mvc noms et sont étroitement liées au .NET Framework.
- ASP.NET Les Core Razor Views sont modulaires, intégrés Microsoft.AspNetCore.Mvc, avec une injection de dépendance améliorée.
- ASP.NET Core propose de nouvelles fonctionnalités, notamment Tag Helpers et View Components.

AWS Transform détecte et porte les composants et constructions incompatibles courants dans Razor Views.

Portage de formulaires Web vers l'interface utilisateur Blazor

ASP.NET L'interface utilisateur de Web Forms n'a pas d'équivalent sur ASP.NET Core. AWS Transform peut porter le code de la couche d'interface utilisateur Web Forms vers Blazor Server on ASP.NET Core. Le code de la couche d'interface utilisateur est réécrit pour le framework d'interface utilisateur cible.

Pour activer ou désactiver le portage des formulaires Web vers l'interface utilisateur Blazor, cochez ou décochez le paramètre de tâche Transform UI ASP.NET Web Forms to Blazor.

Détails de la transformation

Votre projet Web Forms est converti en projet Blazor avec hébergement côté serveur. Les modifications de projet et de fichier suivantes sont apportées au cours de la transformation :

Cartographie des transformations de fichiers

De	À	Description
*.aspx, *.ascx	*.rasoir	Les pages .aspx et les contrôles personnal isés .ascx deviennent des fichiers .razor
Web.config	appsettings.json	Web.config les paramètres deviennent les paramètres appsettings.json
Global.asax	Program.cs	Global.asax le code devient Program.cs code
*.maître	*layout.razor	Les fichiers principaux deviennent des fichiers layout.razor

Post-transformation structure du projet

Après la transformation, les fichiers transformés se trouvent dans les emplacements de projet suivants :

- Dossier Components : tous les composants Razor (*.razor) sont placés dans un dossier Components créé au même niveau que le fichier .csproj du projet.
- Mappage des pages : les pages Web Forms (*.aspx) sont converties en structure de Components/ Pages dossiers.
- Cartographie des contrôles : les contrôles Web Forms (*.ascx) sont placés directement sous le dossier Components.

Limitations et fonctionnalités non prises en charge

Les fonctionnalités suivantes ne sont pas prises en charge actuellement. Si vos charges de travail utilisent ces fonctionnalités, ce code devra être porté manuellement ou à l'aide d'un code AI associé à la transformation.

- fichiers .svc (fichiers de service)
- fichiers .ashx (fichiers de gestion génériques)
- Références de services et références Web (fichiers de référence .map, reference.cs, .wsdl)
- Mélanges de fichiers .aspx (Web Forms) et de fichiers .cshtml (Razor) dans le même projet
- Dépendances relatives aux types de projets qui ne sont pas encore pris en charge par AWS Transform for .NET
- Third-party interface utilisateur du fournisseur libraries/controls
- Projets de sites Web

Seuls les projets d'applications Web (contenant un fichier .csproj) sont pris en charge. Pour convertir un projet de site Web en projet d'application Web, consultez les instructions de Microsoft relatives à la conversion d'un projet de site Web en projet d'application Web.

Rapports de transformation

Une fois votre tâche de transformation .NET terminée, ces rapports de transformation sont disponibles :

- Rapport de synthèse sur la transformation
- Rapport détaillé sur la transformation

Rapport de synthèse sur la transformation

Une fois le travail de transformation terminé, un rapport récapitulatif de transformation est disponible dans la console Web. Téléchargez le rapport récapitulatif de transformation depuis l'onglet Tableau de bord. Sélectionnez Télécharger le rapport récapitulatif de transformation, puis choisissez Télécharger au format HTML ou Télécharger au format JSON.

Le rapport de synthèse de la transformation fournit une vue d'ensemble de la transformation et des informations spécifiques à chaque référentiel transformé, notamment :

- Détails d'une tâche
  - Vue d'ensemble des tâches de transformation
  - Vue d'ensemble des résultats de transformation
  - Vue d'ensemble des fichiers
- Liste des référentiels, et pour chaque dépôt :
  - Vue d'ensemble du nom du référentiel
  - Résumé de la transformation de la solution
  - Détails du projet, y compris le statut, le type, la version .NET, le nombre total de lignes de code, les lignes de code transformées et les fichiers modifiés

Rapport détaillé sur la transformation

Une fois le travail de transformation terminé, les rapports détaillés de transformation sont disponibles pour les utilisateurs de la console Web et de l'IDE.

- Utilisateurs de la console Web : un rapport détaillé est disponible pour chaque dépôt transformé. Dans l'onglet Tableau de bord, utilisez les liens Télécharger le rapport détaillé dans la liste des référentiels pour télécharger un rapport détaillé.
- Utilisateurs de l'IDE : téléchargez le rapport de transformation depuis la fenêtre AWS Transform Job Plan à l'aide de l'icône de téléchargement.

Le rapport détaillé de transformation est un rapport HTML interactif. Il contient des informations détaillées sur la transformation, notamment les raisons des modifications apportées aux fichiers et des informations détaillées sur les erreurs exploitables. Les informations sont organisées selon la hiérarchie suivante :

- Informations sur le poste
- Pour chaque solution :
  - Résumé de la transformation de la solution
  - Aperçu de la transformation
  - Projets
  - Pour chaque projet :
    - Résumé du projet
    - Récapitulatif des erreurs de construction

    - NuGet modifications apportées au package
    - Modifications apportées aux fichiers
    - Erreurs de construction
- Résultats des tests unitaires
- Rapport de préparation à Linux

Pour une présentation des sections du rapport détaillé de transformation avec des exemples, reportez-vous au billet de blog Annunching Transform for .NET Detailed AWS Transform for .NET pour les rapports de transformation.

Bonnes pratiques pour les transformations .NET

Suivez ces instructions pour obtenir de meilleurs résultats en matière de modernisation .NET avec AWS Transform. Ces meilleures pratiques s'appliquent à l'assistant d'IA conversationnelle .NET, actuellement disponible pour l'Visual StudioIDE.

Rubriques

- Avant de transformer
- Évaluation et planification
- Transformez de manière interactive ou autonome
- Validation et finalisation

Avant de transformer

Consultez les recommandations suivantes avant de démarrer une tâche de transformation .NET.

Utiliser l'assistant d'IA conversationnelle .NET

Utilisez le nouvel agent .NET pour de meilleurs résultats de transformation. L'assistant d'intelligence artificielle conversationnelle est disponible Visual Studio via le AWS Toolkit for Visual Studio. Il est également disponible pour Kiroou d'autres IDE grâce à la Kiro puissance des agents AWS Transform et AWS Transform MCP. Le nouvel agent .NET n'est pas encore disponible dans la console Web.

Utilisez d'autres outils si l'objectif n'est pas la transformation de .NET en .NET

AWS Transform for .NET convient à la modernisation du code .NET Framework vers .NET et aux mises à niveau de .NET vers des versions ultérieures. Il ne convient pas aux transformations qui

incluent des langages autres que .NET, tels que Java, ou des frameworks autres que .NET, tels que React. Il ne fournit pas non plus de refactorisation de l'architecture des applications. Utilisez AWS Transform custom ou Kiro pour ce type de modernisation.

Utilisez une édition stable de Visual Studio, de préférence VS2026

Utilisez une édition GA Visual Studio plutôt qu'une version préliminaire ou une édition Insiders pour éviter les complications liées à la prévisualisation du logiciel. La AWS boîte à outils peut être utilisée en Visual Studio 2026 ou 2022. Le VS2026 est recommandé car il fonctionne mieux avec une consommation de mémoire réduite.

Utilisez la dernière version AWS Boîte à outils pour Visual Studio

Restez sur la dernière version de AWS Toolkit Visual Studio pour les corrections de bogues et les mises à jour des fonctionnalités. Vous pouvez vérifier la version de votre boîte à outils et effectuer la mise à niveau dans Extensions > Gérer les extensions > Installées.

Travaillez dans Visual Studio IDE pour les projets de complexité moyenne ou élevée

L'expérience IDE vous donne une vision approfondie de la transformation, grâce à laquelle vous pouvez travailler aux côtés de l'agent .NET lors de la transformation des projets. Pour les projets de complexité moyenne, élevée ou critique, utilisez l'IDE plutôt que la console Web.

Disposer d'un plan de validation

Décidez de la manière dont vous validerez l'exactitude de votre demande après sa transformation. Post-transformation, vous devez vérifier qu'il se comporte et s'affiche correctement lorsqu'il est exécuté, et que les contrôles de sécurité, la logique métier et le stockage des données sont intacts. La validation sera-t-elle effectuée manuellement à and/or l'aide de l'automatisation des tests ? Si votre solution contient des tests unitaires, AWS Transform les transférera pour vous et les exécutera, et les résultats apparaîtront dans le rapport de transformation.

Fournir NuGet dépendances des packages privés

Si votre solution repose sur des packages privés, assurez-vous qu'ils sont disponibles sur votre machine locale afin que l'IDE et AWS Transform puissent les trouver.

Spécifiez les emballages de remplacement ou demandez des recommandations à un agent

Pour les packages qui ne disposent pas de versions .NET modernes, vous pouvez soit personnaliser le plan de transformation pour spécifier les substitutions de packages que vous souhaitez, soit demander des recommandations à l'agent.

Ne mettez pas fin à votre travail tant que vous n'êtes pas sûr de vouloir d'autres modifications

Une fois la transformation terminée, ne mettez pas fin à votre travail immédiatement au cas où vous souhaiteriez des modifications supplémentaires. La transformation n'est pas complète tant que vous ne le dites pas. Vous pouvez demander des modifications jusqu'à ce que vous marquiez la tâche comme terminée.

Après la transformation, confiez-vous à un compagnon de code AI pour finaliser votre application

Attendez-vous à combiner AWS Transform avec un compagnon de code AI tel queKiro. Il est courant de procéder d'abord à la transformation avec AWS Transform pour .NET, puis de passer à un compagnon de code AI pour finaliser l'application. Ce travail de finalisation peut inclure l'identification et la correction des erreurs d'exécution, des problèmes de comportement et du style UX.

Dans le cadre du processus de modernisation, imaginez AWS Transform comme le voyage express qui vous emmène le plus loin possible vers votre objectif, et un compagnon utilisant un code AI comme le voyage local qui vous emmène à votre destination finale.

Pour faciliter le passage de AWS Transform à des compagnons de code AI, AWS Transform fournit un rapport de transformation HTML et un document de balisage sur les prochaines étapes à la fin de la transformation.

Évaluation et planification

Une fois que vous avez démarré une tâche de transformation, AWS Transform analyse votre code et produit un rapport d'évaluation et un plan de transformation. Utilisez les meilleures pratiques suivantes pour tirer le meilleur parti de cette phase.

Passez en revue l'évaluation et posez des questions pour définir vos attentes

Examinez attentivement les résultats de l'évaluation pour comprendre quels projets seront difficiles à transformer et pourquoi. L'agent présente les projets présentant un niveau de complexité (faible, moyen, élevé, critique) et explique pourquoi ils ont obtenu cette note.

Posez des questions pour mieux comprendre les domaines difficiles. Par exemple :

- Demandez à l'agent quel est son niveau de confiance dans une transformation de projet ou un cas d'utilisation.
- Demandez à l'agent quelles tâches post-transformation seront probablement nécessaires avec un compagnon de code AI.

Passez en revue le plan et discutez des options avec l'agent

L'agent vous fournit un plan de transformation pour examen. Vous pouvez discuter de ce plan et le modifier. Commencez par comprendre les options qui s'offrent à vous. Demandez à l'agent quelles sont les alternatives à l'une ou l'autre des parties du plan.

Par exemple, le plan de transformation peut proposer de transformer les services WCF en API ASP.NET Web. Toutefois, votre organisation préfère s'en tenir à la WCF. Vous demandez à l'agent des options et vous apprenez qu'une alternative consiste à les transformer enCoreWCF.

Téléchargez des documents de pilotage pour adapter un plan à votre organisation

Le plan de transformation d'origine est créé sans que l'on connaisse les exigences et les préférences de votre organisation. Vous pouvez informer l'agent des conventions organisationnelles, des spécifications des applications, de la pile technologique préférée et des exemples de modèles de codage préférés.

Après avoir téléchargé un document de pilotage, expliquez-le pour donner du contexte à l'agent. Grâce aux informations supplémentaires contenues dans les documents de pilotage, l'agent peut préparer un plan adapté à la façon dont votre organisation aime travailler.

Personnalisez librement le plan

L'agent .NET est flexible et vous pouvez personnaliser librement le plan de transformation, dans le domaine de la transformation .NET vers .NET. Vous pouvez demander des modifications de plan dans le chat, ou si vous préférez, vous pouvez travailler avec des fichiers Markdown. Passez en revue et affinez le plan jusqu'à ce que vous soyez satisfait.

Si un plan doit être examiné par plusieurs parties prenantes, vous pouvez le télécharger sous forme de fichier Markdown, le partager, puis télécharger un plan personnalisé.

Par exemple, vous examinez le plan de transformation et décidez que vous souhaitez que les projets de bibliothèque de classes soient transformés en .NET Standard au lieu de .NET 10. Dans le chat, vous dites « Révisez le plan pour transformer toutes les bibliothèques de classes en .NET Standard 2.0 » et l'agent vous présente un plan révisé.

Transformez de manière interactive ou autonome

L'expérience Visual Studio IDE propose des modes autonomes et interactifs pour contrôler le degré d'interactivité lors de la transformation.

Utilisez des modes interactifs et autonomes pour contrôler le degré d'interactivité

Vous sélectionnez le mode lorsque vous démarrez une transformation, et vous pouvez le modifier à tout moment via une liste déroulante en haut de la fenêtre de discussion.

- Utilisez le mode autonome pour une transformation sans surveillance, adapté aux tâches nocturnes ou de longue durée. Vous avez toujours la possibilité de consulter les résultats et de demander des modifications à la fin du travail.
- Utilisez le mode interactif pour travailler aux côtés de l'agent dans le chat tout au long du processus de transformation grâce à un plan de transformation personnalisable, à une grande visibilité sur les détails de la transformation et à un examen étape par étape de chaque projet. Vous pouvez itérer pour affiner les résultats ou changer de direction jusqu'à ce que vous soyez satisfait.

Vous pouvez combiner les modes. Par exemple, commencez en mode interactif pour revoir et ajuster le plan de transformation, puis passez en mode autonome pour transformer automatiquement les projets.

Demandez à l'agent d'expliquer les modifications apportées au code

Si vous constatez des modifications de code que vous ne comprenez pas, demandez à l'agent de les expliquer.

Utilisez les points de contrôle pour vous arrêter sur les projets à des fins de révision ou de modification

En mode interactif, après avoir approuvé votre plan, vous pouvez définir ou effacer des points de contrôle pour chaque projet. Lorsqu'un projet avec un point de contrôle a été transformé, le code transformé est appliqué au projet dans l'IDE et l'agent fait une pause pour votre révision. Vous pouvez consulter les résultats et, s'ils ne vous plaisent pas, vous pouvez demander d'autres modifications.

Lorsque vous êtes arrêté à un point de contrôle, vous pouvez :

- Passez en revue les résultats tels qu'ils sont présentés dans le chat et posez des questions dans le chat. Par exemple : « Pourquoi avez-vous modifié l'API de cryptographie dans le fichier X ? »
- Affichez les modifications du code en cliquant sur le bouton Afficher les résultats du projet dans la fenêtre AWS Transform Job Plan.

- Affinez la transformation en demandant des modifications supplémentaires. Par exemple : « Changez ceci pour utiliser l'enregistreur X » ou « Modifiez ceci pour utiliser le package X au lieu du package Y ».
- Réessayez la transformation en suivant des instructions différentes. Par exemple : « Modifiez cette bibliothèque de classes pour cibler .NET Standard au lieu de .NET 10 » ou « Réessayez cette transformation et remplacez la cible par Blazor MVC Razor Pages ».
- Apportez vos propres modifications de code dans l'IDE.
- Dites à l'agent de passer au point de contrôle suivant du projet.

Itérer jusqu'à satisfaction

La modernisation est intrinsèquement itérative, et vous pouvez vous attendre à ce qu'elle soit itérée avec l'agent. Vous pouvez apporter des modifications aux points de contrôle du projet, ainsi qu'à la fin de la transformation. Répétez autant de fois que nécessaire jusqu'à ce que vous soyez satisfait. La transformation n'est pas complète tant que vous ne le dites pas.

Codez à côté de l'agent lorsqu'il est arrêté à un point de contrôle

Vous pouvez apporter vos propres modifications de code pendant que vous travaillez avec l'agent. Lorsque vous êtes arrêté à un point de contrôle, vous pouvez modifier les fichiers de code dansVisual Studio. Vos modifications seront synchronisées lorsque vous demanderez à l'agent de continuer.

Validation et finalisation

Une fois la transformation terminée, validez votre application transformée et finalisez-la pour une utilisation en production.

Consultez le rapport de transformation et les prochaines étapes pour comprendre ce qui est fait et ce qui reste à faire

Consultez le rapport de transformation HTML pour comprendre ce qui a été fait. Consultez le fichier de balisage Prochaines étapes pour savoir quelles tâches restent à accomplir. Demandez à l'agent de clarifier tout ce qui n'est pas clair.

Utilisez un compagnon de code AI pour valider, déboguer et finaliser votre application

Vérifiez que votre application transformée est correcte. Utilisez un compagnon de code AI, par exemple Kiropour résoudre les problèmes.

Valider les tests unitaires

Si votre solution contient des projets de tests unitaires (NUnitxUnit,, ouMSTest), AWS Transform les portera vers le .NET moderne et exécutera les tests pour vous. Consultez le rapport de transformation HTML pour les résultats des tests unitaires. Corrigez les tests qui échouent à l'aide d'un code AI associé.

Valider les fonctionnalités des applications

Lancez votre application et vérifiez que ses fonctionnalités correspondent à celles d'origine. Notez les problèmes fonctionnels et les erreurs d'exécution. Corrigez avec un code AI associé.

Validation de l'interface utilisateur

Exécutez votre application et vérifiez qu'elle ressemble et se comporte comme l'original, y compris en ce qui concerne la navigation et le routage. Si votre application n'a aucun style, il se peut que les fichiers .css ne soient pas au bon emplacement. Corrigez avec un code AI associé.

Modernisation de SQL Server

AWS Transform for SQL Server Modernization est un AI-powered service qui automatise la modernisation complète des bases de données Microsoft SQL Server et de leurs applications .NET associées vers Amazon Aurora PostgreSQL. AWS Transform convertit désormais les objets de stockage SQL Server, alimentés par AWS DMS, et les objets de code (procédures stockées) à l'aide d'une expérience interactive agentique. Le service orchestre l'ensemble du processus de migration, depuis la conversion du schéma, la migration des données et la modification du code de l'application pour l'adapter à la nouvelle cible PostgreSQL, ce qui accroît la productivité de vos équipes en automatisant les tâches complexes et fastidieuses.

Régions prises en charge

AWS Transform for SQL Server est disponible dans l'est des États-Unis (Virginie du Nord) - us-east-1

Cross-Region Utilisation : pour les bases de données situées dans des régions non prises en charge, vous pouvez cloner la base de données dans une région prise en charge à des fins de transformation, puis redéployer les résultats dans votre région cible.

Capacités et fonctionnalités clés

Transformation de la base

- Conversion de schéma : convertit automatiquement les schémas SQL Server en Aurora PostgreSQL, y compris les tableaux, les vues, les index, les contraintes et les relations
- Transformation des procédures stockées : convertit les procédures T-SQL stockées en procédures stockées PL/pgSQL avec AI-enhanced précision
- Migration des données : migre les données avec validation de l'intégrité à l'aide du service AWS de migration de base de données (DMS)
- Objets de base de données : prend en charge les déclencheurs, les fonctions, les vues, les colonnes calculées et les colonnes d'identité
- Validation : vérification automatique de l'intégrité des données et contrôles d'intégrité référentielle

Transformation des applications

- Transformation d'Entity Framework : mise à jour des configurations Entity Framework 6.3-6.5 et EF Core 1.0-10.0 pour PostgreSQL
- ADO.NET transformation : convertit le code d'accès aux ADO.NET données de SQL Server vers les fournisseurs PostgreSQL.
- Mises à jour des chaînes de connexion : met automatiquement à jour toutes les chaînes de connexion à la base de données vers la nouvelle base de données PostgreSQL cible
- Modifications apportées au fournisseur de base de données : remplace les fournisseurs SQL Server par Npgsql (fournisseur PostgreSQL)
- Mises à jour de la configuration ORM : modifie les mappages de types de données, les colonnes d'identité et les configurations spécifiques à la base de données

Validation de l'orchestration &

- Wave-based modernisation : organise les grands domaines en phases de migration logiques
- Cartographie des dépendances : identifie les relations entre les applications et les bases de données
- Human-in-the-loop Points de contrôle (HITL) : fournit des points de contrôle et d'approbation aux étapes critiques

- Validation automatique : teste la compatibilité des schémas, l'intégrité des données et les fonctionnalités de l'application
- CI/CD intégration : s'intègre aux pipelines de développement existants

Déploiement

- Déploiement d'Amazon ECS et Amazon EC2 : déploiement conteneurisé automatisé avec prise en charge de la mise à l'échelle automatique
- Infrastructure-as-code génération : crée CloudFormation des modèles de AWS CDK
- Validation automatique du déploiement : vérifie la réussite du déploiement à l'aide de bilans de santé
- Capacités de restauration : prend en charge les procédures de restauration en cas de problème

Versions et types de projets pris en charge

Versions de SQL Server

AWS Transform prend en charge les versions de SQL Server suivantes :

SQL Server Version	État du support
SQL Server 2#022	Pris en charge
SQL Server 2019	Pris en charge
SQL Server 2017	Pris en charge
SQL Server 2016	Pris en charge
SQL Server 2014	Pris en charge
SQL Server 2012	Pris en charge
SQL Server 2008 R2	Pris en charge

> **Note**
>
> Toutes les éditions de SQL Server sont prises en charge (Express, Standard, Enterprise). SQL Server peut être hébergé sur AWS (Amazon RDS pour SQL Server ou SQL Server sur Amazon EC2) ou hébergé en dehors de AWS celui-ci.

Versions de .NET

Version .NET	État du support
.NET 10	Pris en charge
.NET 8	Pris en charge
.NET 7	Pris en charge
.NET 6 (Noyau)	Pris en charge
.NET Framework 4.x et versions antérieures	Non pris en charge

> **Important**
>
> Les anciennes versions de .NET Framework 4.x et antérieures ne sont pas prises en charge. Si votre application utilise .NET Framework, vous devez d'abord effectuer une mise à niveau vers .NET Core 6+ à l'aide de AWS Transform for .NET Modernization avant d'utiliser les fonctionnalités de transformation de SQL Server.

Versions du framework Entity

Cadre	Versions prises en charge
Entity Framework 6	6,3, 6,4 et 6,5
Entity Framework Core	1,0 à 10,0
ADO.NET	Toutes les versions (GA)

Référentiels de code source

AWS Transform prend en charge les plateformes de code source suivantes :

- GitHub et GitHub Enterprise Server
- GitLab.com et GitLab Self-Managed
- Bitbucket Cloud et centre de données Bitbucket
- Azure DevOps et Azure DevOps Server
- Amazon S3

Base de données cible

AWS Transform cible Amazon Aurora PostgreSQL (compatible avec PostgreSQL 15+) en prenant en charge les dernières fonctionnalités et optimisations d'Aurora.

Exigences techniques

Exigences de base de données

- Microsoft SQL Server, version 2008 R2 jusqu'en 2022
- SQL Server hébergé sur AWS (Amazon RDS pour SQL Server ou SQL Server sur Amazon EC2) ou hébergé en dehors de AWS
- Pour les bases de données AWS hébergées, la base de données et AWS Transform doivent se trouver dans la même AWS région.
- Pour les bases de données hébergées en dehors de l'établissement AWS, une connectivité réseau au service AWS Transform est requise.
- Utilisateur de base de données disposant des autorisations VIEW DEFINITION et VIEW DATABASE STATE
- Mots de passe de base de données utilisant uniquement des caractères ASCII imprimables (à l'exception des caractères '/', '@', "" et des espaces)
- Le VPC contenant le SQL Server source doit disposer de sous-réseaux dans au moins 2 zones de disponibilité différentes (obligatoire pour les groupes de sous-réseaux de réplication DMS)

Exigences relatives à la candidature

- Applications .NET 6, 7, 8 ou 10

- Entity Framework 6.3-6.5 ou Entity Framework Core 1.0-10.0, ou ADO.NET
- Connexions à la base de données détectables dans le code source
- Les applications sont créées et exécutées avec succès
- Code source sur les plateformes de dépôt prises en charge

AWS exigences relatives au compte

- AWS compte avec accès administrateur
- IAM Identity Center activé
- Les rôles de service requis ont été créés (voir les instructions de configuration ci-dessous)
- VPC avec configuration réseau appropriée

Traitement et stockage des données

Lieu de traitement

- Le traitement du schéma s'effectue dans une instance DMS de votre VPC
- La migration des données est facultative et peut être exclue si nécessaire
- Les artefacts de transformation sont stockés dans la région de service AWS Transform

Artefacts entreposés

Les articles suivants sont stockés dans la zone de service :

- Journaux de l'agent
- Résultats de l'évaluation
- Fichiers de schéma SQL
- Artefacts de sortie DMS

> **Important**
>
> Important pour la résidence des données : même lorsque la migration des données est désactivée, les métadonnées et les artefacts de traitement sont stockés dans la région de

service. Ceci est important pour les organisations qui ont des exigences strictes en matière de résidence des données.

Gestion des artefacts

- Option client pour le chiffrement à l'aide de vos propres clés KMS
- Période TTL (durée de vie) définie pour tous les artefacts
- Les artefacts peuvent être téléchargés pour être stockés hors ligne

Commencer un travail de modernisation

Une fois que vous avez créé une tâche de modernisation de SQL Server dans AWS Transform et que l'agent a démarré, l'agent vous demande comment vous souhaitez que AWS Transform accède à votre schéma SQL Server source. Votre réponse à ce premier message détermine le flux de travail à exécuter pour le reste de la tâche. Sélectionnez l'une des méthodes suivantes :

- Connexion à la base de données : AWS Transform se connecte directement à votre serveur SQL en cours d'exécution. Choisissez cette option lorsqu'une connexion réseau en direct à la base de données est disponible et que vous souhaitez que AWS Transform migre des données réelles.
- Charger des fichiers DDL : vous extrayez vos fichiers de définition de schéma (DDL) à l'aide d'un script fourni et vous les chargez dans Transform. AWS Choisissez cette option lorsqu'une connexion directe à la base de données n'est pas disponible ou n'est pas souhaitée. Aucune connexion en direct n'est requise et les données réelles ne sont pas migrées.

Les deux flux de travail ciblent Amazon Aurora PostgreSQL et partagent les mêmes versions prises en charge, les mêmes limites et le même comportement de gestion des données décrits ailleurs sur cette page. Choisissez le flux de travail qui correspond à votre environnement.

> **Note**
>
> Lorsque vous choisissez Se connecter à la base de données, le flux de travail en ligne démarre. Lorsque vous choisissez Charger des fichiers DDL, le flux de travail hors ligne démarre.

Connexion à la base de données (flux de travail en ligne)

Dans ce flux de travail, AWS Transform se connecte directement à votre serveur SQL source et utilise le service AWS de migration de base de données (DMS) pour convertir le schéma et migrer les données vers Amazon Aurora PostgreSQL. Il s'agit du flux de travail standard de bout en bout lorsqu'une connexion à une base de données en direct est disponible.

Le flux de travail se déroule selon les phases suivantes :

1. Prérequis : AWS Transform confirme que les prérequis du DMS sont en place (rôles IAM, secrets et accès réseau à la base de données source).
2. Connexion : vous fournissez les détails de connexion et AWS Transform établit une connexion avec la base de données source.
3. Valider : AWS Transform valide la connectivité et les autorisations.
4. Découverte et évaluation : AWS Transform découvre les bases de données sur le serveur, vous choisissez celles à moderniser et AWS Transform les évalue.
5. Per-database transformation : pour chaque base de données sélectionnée, AWS Transform fournit une cible Aurora PostgreSQL, convertit le schéma et migre les données. Choisissez de migrer des données réelles, de générer des données synthétiques ou d'ignorer la migration des données.
6. Évaluation et transformation du code (facultatif) : si un référentiel de code source est connecté, AWS Transform évalue et transforme l'application .NET associée.
7. Déployer (facultatif) : AWS Transform déploie l'application transformée.

> **Note**
>
> Ce flux de travail permet de migrer vos données réelles à l'aide de AWS DMS. Assurez-vous que les prérequis en matière de réseau et d'IAM sont satisfaits avant de commencer. Consultez les exigences techniques dans la section précédente.

Configuration requise pour SQL Server

Exigences de base de données

bases de données hébergées en externe

Les bases de données hébergées en dehors de AWS sont prises en charge. Pour utiliser une base de données hébergée en externe, vous devez garantir la connectivité réseau entre la base de données et le service AWS Transform.

Charges de travail SSIS

- Limitation : la transformation de SQL Server Integration Services (SSIS) n'est pas prise en charge.
- Solution : utilisez AWS Glue ou d'autres services ETL pour la migration SSIS.

Serveurs liés

- Limitation : les connexions aux bases de données externes via des serveurs liés nécessitent une configuration humaine.
- Solution : reconfigurez les serveurs liés après la migration ou utilisez d'autres approches telles que les liens de base de données ou l'intégration au niveau des applications.

T-SQL Motifs complexes

- Limite : Certains T-SQL modèles avancés peuvent nécessiter une intervention humaine.
- Solution : utilisez l'interface de ligne de commande Amazon Kiro pour les conversions SQL complexes. AWS Transform les signale pour examen au cours du processus de transformation.

Exigences relatives à la candidature

Framework .NET hérité

- Limitation : .NET Framework 4.x et les versions antérieures ne sont pas prises en charge.
- Solution : utilisez AWS Transform for .NET pour passer d'abord à .NET Core 6+, puis utilisez la transformation SQL Server.

Versions du framework Entity

- Limitation : seuls Entity Framework 6.3-6.5 et EF Core 1.0-10.0 sont pris en charge.
- Solution : effectuez une mise à niveau vers une version d'Entity Framework prise en charge avant la transformation.

VB.NET candidatures

- Limitation : n' VB.NET est pas prise en charge.
- Solution : convertissez en C# ou utilisez la fonction AWS Transform custom pour effectuer la conversion en C#. VB.NET

Cross-database dépendances

- Limite : Difficultés rencontrées lorsque des schémas de base de données interagissent entre plusieurs bases de données.
- Solution : passez en revue et remaniez les requêtes entre bases de données avant la migration. Envisagez de consolider les bases de données ou d'utiliser des schémas PostgreSQL.
- Impact : peut nécessiter une intervention humaine pour des scénarios complexes impliquant plusieurs bases de données.

Repository-database accouplement

- Limite : Difficultés rencontrées lorsqu'un seul référentiel dessert plusieurs bases de données.
- Solution : envisagez une restructuration du référentiel ou une approche de migration progressive.
- Impact : peut nécessiter une planification supplémentaire pour les migrations basées sur les vagues.

Exigences en matière d'infrastructure

Une seule account/region par tâche

- Limite : chaque tâche de transformation cible un AWS compte et une région.
- Solution : créez plusieurs tâches de transformation pour les déploiements multicomptes ou multirégions.

Cibles de déploiement

- Limitation : les déploiements Amazon ECS et Amazon EC2 sont pris en charge.

Exigences relatives au référentiel

NuGet Packages privés

- Limitation : les NuGet packages privés nécessitent une configuration supplémentaire.
- Solution : configurez les NuGet flux privés dans les paramètres de transformation avant de démarrer la tâche.

Configuration de SQL Server

Effectuez ces étapes dans votre environnement SQL Server pour activer la modernisation de AWS Transform.

Installation et configuration de la base de données

Étape 1 : Création d'un utilisateur de base de données avec les autorisations requises

Créez un utilisateur de base de données dédié pour AWS Transform avec les autorisations nécessaires. Si vous avez déjà un utilisateur DMS Schema Conversion, vous pouvez le réutiliser.

Connectez-vous à votre instance SQL Server et exécutez les commandes suivantes :

```
-- 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**
>
> Répétez les commandes spécifiques à la base de données (USE, CREATE USER, GRANT) pour chaque base de données que vous souhaitez moderniser.

Le rôle db_datareader n'est nécessaire que pour la migration des données, pas uniquement pour la conversion de schémas.

- Le rôle db_datareader accorde un accès en lecture à toutes les tables de la base de données
- Ce rôle est requis UNIQUEMENT lors de la migration des données.
- Pour la conversion de schéma uniquement (sans migration de données), le rôle db_datareader n'est PAS requis
- Les autres autorisations (VIEW DEFINITION, VIEW DATABASE STATE, etc.) sont suffisantes pour la conversion du schéma

Étape 2 : Stockez les informations d'identification dans AWS Secrets Manager

Stockez les informations d'identification de votre base de données en toute sécurité dans AWS Secrets Manager. Ignorez cette étape si vous avez déjà créé un secret pour DMS.

1. Accédez à AWS Secrets Manager dans la console
2. Choisissez Stocker un nouveau secret
3. Configurez le secret :
   - Type de secret : informations d'identification pour une autre base de données
   - Base de données : Microsoft SQL Server
   - Nom d'utilisateur : atx_user (ou nom d'utilisateur que vous avez choisi)
   - Mot de passe : le mot de passe que vous avez créé
   - Nom du serveur : votre point de terminaison SQL Server
   - Nom de la base de données : nom de votre base de données
   - Port : 1433 (ou votre port personnalisé)
4. Choisissez Next (Suivant)

5. Entrez le nom secret : atx-db-modernization-sqlserver
6. Ajoutez les balises requises (ces balises sont obligatoires) :
   - Clé : Projet, Valeur : atx-db-modernization
   - Clé : Owner, Valeur : database-connector
7. Choisissez Suivant dans les autres écrans
8. Choisissez Store
9. Notez l'ARN secret à utiliser à l'étape suivante

> **Important**
>
> Les mots de passe de base de données doivent utiliser uniquement des caractères ASCII imprimables, à l'exception des caractères «/», « @ », et des espaces. Les secrets dont la suppression est programmée peuvent entraîner des échecs de transformation.

Étape 3 : Création des rôles DMS requis

AWS Transform nécessite des rôles IAM spécifiques pour les opérations DMS. Déployez ces rôles à l'aide du CloudFormation modèle ci-dessous.

> **Note**
>
> Si votre AWS compte possède déjà DMS-related des rôles, modifiez ce modèle pour réutiliser ces ressources plutôt que de créer des doublons.

Créez un fichier nommé dms-roles.yaml avec le contenu suivant :

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'DMS Service Roles for AWS Transform SQL Server Modernization'

Resources:
  DMSCloudWatchLogsRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-cloudwatch-logs-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
```

```
      Statement:
        - Effect: Allow
          Principal:
            Service:
              - dms.amazonaws.com
              - schema-conversion.dms.amazonaws.com
          Action: sts:AssumeRole
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

DMSS3AccessRole:
  Type: AWS::IAM::Role
  Properties:
    RoleName: dms-s3-access-role
    AssumeRolePolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Principal:
            Service:
              - dms.amazonaws.com
              - schema-conversion.dms.amazonaws.com
          Action: sts:AssumeRole
    Policies:
      - PolicyName: S3TaggedAccess
        PolicyDocument:
          Version: '2012-10-17'
          Statement:
            - Effect: Allow
              Action:
                - s3:GetBucketLocation
                - s3:GetBucketVersioning
                - s3:PutObject
                - s3:PutBucketVersioning
                - s3:GetObject
                - s3:GetObjectVersion
                - s3:ListBucket
                - s3:DeleteObject
              Resource: arn:aws:s3:::atx-db-modernization-*
              Condition:
                StringEquals:
                  aws:ResourceAccount: !Ref AWS::AccountId

DMSSecretsManagerRole:
```

```
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-secrets-manager-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
            Action: sts:AssumeRole
      Policies:
        - PolicyName: SecretsManagerTaggedAccess
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action:
                  - secretsmanager:GetSecretValue
                  - secretsmanager:DescribeSecret
                Resource: '*'
                Condition:
                  StringEquals:
                    secretsmanager:ResourceTag/Project: atx-db-modernization
                    secretsmanager:ResourceTag/Owner: database-connector

  DMSVPCRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-vpc-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
            Action: sts:AssumeRole
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

  DMSServerlessRole:
```

```
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: dms.amazonaws.com
      Description: 'Service Linked Role for AWS DMS Serverless'

Outputs:
  DMSCloudWatchLogsRoleArn:
    Description: ARN of the DMS CloudWatch Logs Role
    Value: !GetAtt DMSCloudWatchLogsRole.Arn
  DMSS3AccessRoleArn:
    Description: ARN of the DMS S3 Access Role
    Value: !GetAtt DMSS3AccessRole.Arn
  DMSSecretsManagerRoleArn:
    Description: ARN of the DMS Secrets Manager Role
    Value: !GetAtt DMSSecretsManagerRole.Arn
  DMSVPCRoleArn:
    Description: ARN of the DMS VPC Role
    Value: !GetAtt DMSVPCRole.Arn
    Export:
      Name: !Sub ${AWS::StackName}-VPCRole

  DMSServerlessRoleArn:
    Description: ARN of the DMS Serverless Role
    Value: !Sub 'arn:aws:iam::${AWS::AccountId}:role/aws-service-role/
dms.amazonaws.com/AWSServiceRoleForDMSServerless'
    Export:
      Name: !Sub ${AWS::StackName}-ServerlessRole
```

Déployez la CloudFormation pile à l'aide de la AWS CLI :

```
aws cloudformation create-stack \
  --stack-name dms-roles \
  --template-body file://dms-roles.yaml \
  --capabilities CAPABILITY_NAMED_IAM \
  --region us-east-1
```

Ou déployez à l'aide de la AWS console :

1. Accédez CloudFormation à la AWS console
2. Choisissez Créer une pile
3. Sélectionnez Charger un fichier modèle
4. Téléchargez le fichier dms-roles.yaml

5. Entrez le nom de la pile : dms-roles
6. Reconnaître les capacités IAM
7. Choisissez Créer une pile

Étape 4 : Configuration de la sécurité du réseau

Assurez une connectivité réseau adéquate entre AWS Transform, votre base de données SQL Server et les autres AWS services.

Configuration du groupe de sécurité (approche recommandée)

Approche recommandée : utilisez un contrôle d'accès basé sur les groupes de sécurité plutôt que IP-based des règles. Cela permet une meilleure sécurité, une gestion plus facile et fonctionne parfaitement avec l'architecture de AWS Transform.

Pourquoi le contrôle Group-Based d'accès sécurisé ?

- La conversion de schéma DMS crée des interfaces réseau élastiques (ENI) au sein de votre VPC
- Vos bases de données n'ont pas besoin d'être accessibles au public
- AWS Transform n'expose pas les adresses IP privées, ce qui IP-based complique les règles
- Les références aux groupes de sécurité fournissent des mises à jour dynamiques et automatiques à mesure que les ressources évoluent

Configuration de votre groupe de sécurité SQL Server

Lorsque vous configurez le profil d'instance de conversion de schéma DMS dans AWS Transform, vous spécifiez un groupe de sécurité pour l'instance DMS SC. Le groupe de sécurité de votre base de données doit autoriser le trafic entrant provenant de ce groupe de sécurité DMS SC.

Step-by-step configuration :

1. Identifiez le groupe de sécurité de conversion de schéma DMS :
   - Ceci est spécifié lors de la création du profil d'instance dans AWS Transform
   - Notez l'ID du groupe de sécurité (par exemple, sg-0123456789abcdef0)
2. Mettez à jour les règles entrantes de SQL Server Security Group :
   - Type : TCP personnalisé

- Port : 1433 (ou votre port SQL Server personnalisé)
- Source : ID du groupe de sécurité de conversion de schéma DMS
- Description : « Autoriser l'accès à la conversion du schéma DMS »

3. Pour la cible Aurora PostgreSQL (après sa création) :
   - Type : PostgreSQL
   - Port : 5432 (ou votre port PostgreSQL personnalisé)
   - Source : ID du groupe de sécurité de conversion de schéma DMS
   - Description : « Autoriser l'accès à la conversion du schéma DMS »

> **Important**
>
> Important pour les modèles de sécurité les moins privilégiés : si votre organisation utilise un modèle de sécurité « moins privilégié » qui bloque tout le trafic par défaut, vous devez autoriser explicitement le trafic entrant depuis le groupe de sécurité de conversion de schéma DMS vers le port de votre base de données. N'ouvrez pas le port 1433 pour toutes les sources ou plages IP.

Obligatoire AWS connectivité du service

Assurez-vous que votre VPC peut communiquer avec :

- AWS Transformez les terminaux de service
- AWS DMS points de terminaison
- Points de terminaison Aurora PostgreSQL
- Points de terminaison S3 pour le stockage des artefacts
- AWS Secrets Manager points de terminaison
- AWS CodeConnections points de terminaison

Points de terminaison VPC : pour les réseaux privés, configurez les points de terminaison VPC pour les AWS services requis afin d'éviter toute dépendance à la passerelle Internet.

Exigences relatives aux bases de données hébergées en externe

Si votre base de données SQL Server est hébergée en dehors de AWS, assurez-vous que les conditions suivantes sont remplies, puis effectuez les étapes de configuration avant de commencer la modernisation.

Conditions préalables

- Un AWS compte avec un VPC
- Connectivité réseau entre le VPC et la base de données externe. Pour plus d'informations sur la configuration de la connectivité réseau, voir Configuration de la connectivité réseau dans le Guide de AWS DMS l'utilisateur.

Étapes de configuration

1. Créez un secret AWS Secrets Manager avec les informations de connexion pour la base de données externe. Pour de plus amples informations, veuillez consulter the section called "Étape 2 : Stockez les informations d'identification dans AWS Secrets Manager".
2. Lorsque vous y êtes invité, indiquez l'ID VPC et l'ID du groupe de sécurité pour la connexion à la base de données externe. AWS Transform vous invite à fournir ces informations car le nom d'hôte de la base de données contenu dans le secret ne peut pas être résolu dans le AWS compte.

AWS Transformez la configuration

Commencez votre parcours de modernisation en accédant à la console AWS Transform et en lançant un nouveau projet de modernisation. Cette étape définit votre espace de travail et met en place la configuration de base pour votre transformation complète.

Actions à effectuer :

- Accédez au service AWS Transform dans la console AWS de gestion
- Sélectionnez Microsoft Modernization dans les options de service
- Choisissez Créer un nouveau projet de modernisation
- Indiquez le nom et la description du projet
- Sélectionnez votre AWS région cible (doit correspondre à l'emplacement de votre serveur SQL)
- Vérifiez et confirmez les paramètres du projet

> **Note**
>
> Bonne pratique : utilisez des noms de projet descriptifs qui incluent le nom de l'application et l'environnement cible (par exemple, « CustomerPortal-Production-Modernization ») pour identifier facilement les projets dans les scénarios à plusieurs vagues.

Création d'une tâche de modernisation de SQL Server

Connecter la base de données et le dépôt de code source

Configuration du connecteur de base de données

Établissez une connectivité sécurisée à vos bases de données SQL Server en configurant des connecteurs de base de données. Le connecteur effectue une analyse de l'environnement, découvre les dépendances et permet à AWS Transform d'accéder aux schémas et aux métadonnées de votre base de données à des fins d'évaluation et de conversion.

Actions à effectuer :

- Sélectionnez Configurer le connecteur de base de données dans l'assistant de configuration
- Choisissez la méthode de connexion : nouvelle connexion ou connexion existante
- Fournissez les détails de connexion à SQL Server (point de terminaison, port, noms de base de données)
- Configurer l'authentification et tester la connectivité
- Passez en revue les bases de données découvertes et confirmez la sélection

> **Note**
>
> Connectivité réseau : assurez-vous que vos groupes de sécurité et vos NACL SQL Server autorisent les connexions entrantes depuis les points de terminaison du service AWS Transform.

Référentiel de code source Connect

Activez AWS Transform pour accéder au code source de votre application .NET. AWS Transform prend en charge trois méthodes pour fournir du code source : un connecteur PAT (Personal Access

Token) (recommandé) ou Amazon S3. AWS CodeConnections Cette intégration permet au service d'analyser le code de votre application, d'identifier les dépendances des bases de données et d'effectuer des transformations de code automatisées pour assurer la compatibilité avec PostgreSQL.

Actions à effectuer :

- Accédez à la section Connect Source Code Repository
- Choisissez votre méthode d'authentification : connecteur PAT (recommandé) ou Amazon S3 AWS CodeConnections
- Sélectionnez des référentiels contenant des applications .NET
- Spécifier la branche pour l'analyse (généralement main/master pour le développement)
- Valider l'accès au référentiel et la structure du code

> **Note**
>
> Découverte des référentiels : AWS Transform analyse automatiquement vos référentiels pour identifier les projets .NET, les configurations Entity Framework, les chaînes de connexion à la base de données et les dépendances SQL.

> **Note**
>
> Note de sécurité : AWS Transform nécessite uniquement un accès en lecture à vos référentiels et crée de nouvelles branches de fonctionnalités pour le code transformé. Votre branche principale reste intacte.

L'humain au courant

AWS Transform utilise des mécanismes HITL (human in-the-loop) pour garantir la qualité et vous permettre de revoir et d'approuver les décisions de transformation critiques. Les points de contrôle suivants requièrent votre attention :

Examen et approbation du plan Wave

Ce que vous passez en revue : Les vagues de migration proposées, y compris les bases de données et les applications qui sont regroupées et la séquence des vagues.

Vous pouvez effectuer les actions suivantes :

- Approuver le plan de vagues
- Personnalisez les vagues en déplaçant les bases de données entre les vagues
- Modifier la séquence d'ondes
- Séparer ou fusionner des vagues

Après approbation, AWS Transform procède à la conversion du schéma.

Révision de la conversion du schéma

Ce que vous examinez : objets de base de données convertis, notamment des tables, des procédures stockées, des fonctions et des déclencheurs. Les actions mettent en évidence les objets qui nécessitent une attention particulière.

Vous pouvez effectuer les actions suivantes :

- Accepter le code converti
- Modifier le code converti
- Drapeau pour l'évaluation humaine après la transformation
- Afficher la comparaison côte à côte du code d'origine et du code converti

Que se passe-t-il après approbation : AWS Transform applique le schéma à Aurora PostgreSQL et procède à la migration des données (si configuré).

Révision du code de l'application

Ce que vous examinez : Toutes les modifications apportées au code de l'application, y compris les configurations Entity Framework, les chaînes de connexion, le code d'accès aux données et les appels de procédure stockés.

Vous pouvez effectuer les actions suivantes :

- Accepter les modifications pour chaque fichier
- Modifier le code transformé
- Refuser les modifications (non recommandé)

- Ajoutez des commentaires pour votre équipe
- Téléchargez le code transformé pour une révision locale

Que se passe-t-il après l'approbation : AWS Transform valide les modifications dans une nouvelle branche de votre référentiel et procède à la validation.

Examen des résultats de validation

Ce que vous examinez : résultats de validation automatisés, notamment la compatibilité des schémas, les contrôles d'intégrité des données et l'état de création de l'application.

Vous pouvez effectuer les actions suivantes :

- Passez en revue les tests réussis
- Étudier les tests qui ont échoué
- Avertissements relatifs aux adresses
- Procéder au déploiement ou revenir pour résoudre les problèmes

Que se passe-t-il une fois l'approbation AWS terminée : Transform prépare le déploiement dans votre environnement cible.

Approbation du déploiement

Ce que vous examinez : Configuration du déploiement, y compris les modèles d'infrastructure en tant que code, la configuration du service ECS et les paramètres de déploiement.

Vous pouvez effectuer les actions suivantes :

- Vérifiez et personnalisez les paramètres de déploiement
- Approuver le déploiement pour continuer
- Retarder le déploiement pour des tests supplémentaires
- Télécharger le code d'infrastructure pour révision

Après approbation, AWS Transform déploie votre application et votre base de données modernisées dans l'environnement cible.

Évaluation et planification des vagues

Configurer la zone d'atterrissage

Configurez l'environnement d'infrastructure cible dans lequel vos applications modernisées seront déployées. La configuration de la zone d'atterrissage inclut le provisionnement Aurora PostgreSQL, la configuration réseau et les configurations de déploiement de référence.

Actions à effectuer :

- Sélectionnez Configurer la zone d'atterrissage dans le menu de configuration
- Configurer la cible Aurora PostgreSQL (version, classe d'instance,) Multi-AZ
- Configuration des paramètres réseau et de sécurité (VPC, sous-réseaux, groupes de sécurité)

> **Note**
>
> Prise en compte des coûts : les instances Aurora PostgreSQL entraînent des coûts permanents. Envisagez d'utiliser Aurora Serverless v2 pour les development/testing environnements.

Évaluation

Effectuez une analyse complète de vos schémas de base de données, de votre code d'application et de vos dépendances. La phase d'évaluation fournit des évaluations de la complexité de la transformation, identifie les défis potentiels et génère des rapports détaillés.

Actions à effectuer :

- Sélectionnez la branche du référentiel pour l'analyse du code
- Sélectionnez les référentiels et les bases de données à transformer
- Examiner les résultats de l'évaluation et les cotes de complexité
- Générer un rapport d'évaluation avec des projections d'effort
- Rapport d'exportation pour examen et approbation par les parties prenantes

> **Note**
>
> Informations sur l'évaluation : L'évaluation fournit une analyse détaillée des objets du schéma, des procédures stockées, des dépendances entre les applications et estime le niveau d'intervention humaine requis.

Planification des vagues

Organisez votre modernisation en étapes gérables en fonction de la complexité de la transformation, des priorités de l'entreprise et des dépendances entre les applications. AWS Transform génère des recommandations de vagues intelligentes que vous pouvez personnaliser.

Actions à effectuer :

- Revoir le plan AI-Generated Wave et ses recommandations
- Personnalisez la configuration Wave en fonction des priorités de l'entreprise
- Valider les dépendances entre les applications et les bases de données
- Finaliser le plan Wave à l'aide d'une interface conversationnelle
- Définissez les priorités d'exécution des vagues et attribuez les responsabilités

> **Note**
>
> AI-Powered Recommandations : vous pouvez interagir avec l'IA via le langage naturel pour ajuster les recommandations : « Déplacer CustomerDB vers la vague 1 » ou « Combiner ces deux applications dans la même vague ».

> **Note**
>
> Meilleure pratique : Commencez par une vague pilote contenant 1 à 2 bases de données peu complexes afin d'établir des processus et de renforcer la confiance de l'équipe.

Migration des données pour chaque vague

Conversion de schéma pour chaque vague

Transformez les schémas de base de données SQL Server en PostgreSQL-compatible équivalents à l'aide des fonctionnalités AI-enhanced de conversion. Ce processus convertit les tables, les procédures stockées, les fonctions, les déclencheurs et d'autres objets de base de données.

Actions à effectuer :

- Fournissez des cibles de conversion de schéma et configurez les préférences
- Exécuter une conversion automatique à l'aide du service de conversion de schéma DMS
- Examiner les résultats de conversion et identifier les éléments d'intervention humaine
- Gérez les interventions manuelles à l'aide des instructions HITL
- Validez les corrections humaines et relancez la conversion si nécessaire

> **Note**
>
> Interventions manuelles courantes : les serveurs liés, les types définis par l'utilisateur, T-SQL les modèles avancés et les fonctionnalités SQL spécifiques aux fournisseurs nécessitent généralement une révision et une correction humaines.

Migration des données pour chaque vague

Transférez des données de SQL Server vers Aurora PostgreSQL à l'aide de l'intégration AWS Database Migration Service (AWS DMS). Choisissez entre la migration des données de production ou la génération de données synthétiques à des fins de test.

Actions à effectuer :

- Choisissez la migration des données de production ou la génération de données synthétiques
- Configuration de l'instance de réplication DMS pour le transfert de données
- Surveillez la progression de la migration et gérez les incohérences dans les données
- Valider l'intégrité des données et les contraintes référentielles
- Confirmez que vous avez terminé avec succès avant de continuer

> **Note**
>
> Intégration automatisée du DMS : AWS Transform résume la complexité de la configuration du DMS en gérant automatiquement la création des terminaux, la configuration des tâches et les mappages des types de données.

> **Note**
>
> Validation des données : le service effectue des tests empiriques en exécutant des requêtes identiques sur les bases de données source et cible afin de garantir la cohérence des données.

Migration de code pour chaque vague

Transformez le code de l'application .NET pour qu'il fonctionne avec Aurora PostgreSQL, notamment en mettant à jour la configuration d'Entity Framework, en modifiant les chaînes de connexion, en adaptant les requêtes SQL et en ajustant les paramètres spécifiques au framework.

Actions à effectuer :

- Exécuter une analyse de code automatisée pour les dépendances de SQL Server
- Procéder à une transformation du framework (mises à jour du fournisseur Entity Framework)
- Adapter la syntaxe des requêtes SQL à PostgreSQL-compatible SQL
- Configuration de la gestion des branches cibles pour le code transformé
- Gérez les interventions manuelles pour des modèles complexes

Workflow de modernisation de SQL Server

Cette section décrit étape par étape le processus complet de modernisation de SQL Server à l'aide de AWS Transform.

Étape 1 : Création d'une tâche de modernisation de SQL Server

Commencez votre parcours de modernisation en créant une nouvelle tâche de transformation dans la console AWS Transform.

1. Connectez-vous à la console AWS Transform
2. Choisissez Créer une tâche de modernisation
3. Sélectionnez la tâche de modernisation de Windows, puis sélectionnez Modernisation de SQL Server
4. Entrez les détails du poste :
   - Nom du poste : nom descriptif de votre projet
   - Description : description facultative
   - Région cible : AWS région de déploiement
5. Choisissez Create job (Créer un travail).

> **Important**
>
> N'incluez pas d'informations personnelles identifiables (PII) dans le nom de votre poste.

Étape 2 : connexion à la base de données SQL Server

Connectez AWS Transform à votre base de données SQL Server pour activer l'analyse et la conversion des schémas.

Création d'un connecteur de base de données

1. Dans votre tâche de modernisation de SQL Server, accédez à Connexion aux ressources
2. Choisissez Se connecter à la base de données SQL Server
3. Choisissez Créer un nouveau connecteur
4. Entrez les informations du connecteur :
   - Nom du connecteur C : nom descriptif
   - AWS ID de compte : compte sur lequel SQL Server est hébergé
5. Une fois confirmé, vous recevrez un lien d'approbation. Copiez le lien d'approbation pour obtenir l'approbation de votre compte auprès de votre AWS administrateur. Une fois qu'ils ont été approuvés, vous pouvez passer à l'étape suivante.
6. Une fois que votre administrateur a approuvé la demande de connecteur, cliquez sur Soumettre pour procéder à la configuration de la connexion au code source.

Étape 3 : connecter le référentiel de code source

AWS Transform a besoin d'accéder au code source de votre application .NET pour analyser et transformer le code qui interagit avec votre base de données SQL Server. AWS Transform prend en charge trois méthodes pour fournir du code source.

Choisissez votre méthode d'authentification

Connecteur PAT (Personal Access Token) (recommandé)

> Idéal pour les équipes qui ont besoin de domaines d'autorisation personnalisés, d'une assistance auto-hébergée pour les fournisseurs ou d'un accès à des API spécifiques au fournisseur, telles que Secrets. GitHub Vous créez un PAT dans votre fournisseur de code source avec des autorisations personnalisées, vous le stockez et AWS Transform le récupère en AWS Secrets Manager cas de besoin. Vous êtes responsable de la gestion de la rotation et de l'expiration des jetons.

AWS CodeConnections

> Idéal pour les équipes qui souhaitent une gestion automatisée des informations d'identification. AWS CodeConnections utilise une intégration de fournisseur géré qui gère l'authentification via un flux d'autorisation OAuth 2.0. AWS gère l'ensemble du cycle de vie des informations d'identification, y compris l'actualisation et la rotation automatiques des jetons. Aucune gestion manuelle des informations d'identification n'est requise.

Amazon S3

> Téléchargez votre code source directement dans un compartiment Amazon S3. AWS Transform accède au code depuis le bucket pendant la tâche de transformation.

Fonctionnalité	Connecteur PAT (recommandé)	AWS CodeConnections
Gestion des informations d'identification	Manuel (géré par le client)	Automatique (AWS géré)
Cycle de vie des jetons	Rotation manuelle requise	Actualisation automatique
Flexibilité des autorisations	Des oscilloscopes entièrement personnalisables	Autorisations fixes

Fonctionnalité	Connecteur PAT (recommandé)	AWS CodeConnections
Self-hosted soutien aux fournisseurs	Pris en charge	Non disponible
Complexité de configuration	Modéré (création et stockage manuels de jetons)	Faible (autorisation unique)
Stockage de jetons	Du client AWS Secrets Manager	Géré par AWS

Configurer un connecteur PAT (recommandé)

Avec un connecteur PAT, vous créez un jeton d'accès personnel dans votre fournisseur de code source avec des autorisations personnalisées, vous le stockez en AWS Secrets Manager toute sécurité et AWS Transform le récupère en cas de besoin. Vous êtes responsable de la gestion du cycle de vie des jetons, y compris la rotation et l'expiration. AWS Transform crée automatiquement le rôle IAM nécessaire avec les autorisations nécessaires pour accéder à votre secret.

Le connecteur PAT prend en charge les fournisseurs suivants, y compris les DNS/URL versions auto-hébergées et personnalisées :

- GitHub et GitHub Enterprise Server
- GitLab.com et GitLab Self-Managed
- Bitbucket Cloud et centre de données Bitbucket
- Azure DevOps et Azure DevOps Server

Créez un jeton d'accès personnel

Créez un PAT dans votre fournisseur de code source. Les autorisations requises varient selon le fournisseur. Choisissez l'onglet correspondant à votre fournisseur.

> **Important**
>
> Copiez le jeton immédiatement après sa création. Vous ne pouvez pas le consulter à nouveau. Définissez l'expiration pour la durée de la tâche de transformation. Ne définissez pas l'expiration pour qu'elle n'expire jamais.

> **Warning**
>
> Ne validez jamais les jetons PAT dans des référentiels de code et ne les partagez jamais via des canaux non sécurisés. Rangez-les toujours dedans AWS Secrets Manager.

GitHub

Accédez à Paramètres, Paramètres du développeur, Jetons d'accès personnels, Fine-grained Jetons. Sélectionnez les référentiels à transformer et accordez les autorisations suivantes.

Autorisations du référentiel

Autorisation	Accès	Objectif
Table des matières	Lisez et écrivez	Lit le code source et réécrit le code transformé dans le référentiel
Métadonnées	Read-only	Permet d'accéder aux informations de base du référentiel

Autorisations de l'organisation (requises pour les référentiels de l'organisation)

Autorisation	Accès	Objectif
Members	Read-only	Répertorie les organisations auxquelles le jeton a accès pour la découverte du référentiel

GitLab

Accédez à Modifier le profil, puis Accédez aux jetons. Sélectionnez les domaines suivants.

Scope	Objectif
`read_api`	Lit les métadonnées du référentiel, les informations sur le projet, les informations sur les utilisateurs et répertorie les groupes et les branches

Scope	Objectif
`read_repository`	Lit les fichiers de code source et la structure du référentiel à des fins d'analyse
`write_repository`	Réécrit le code transformé dans le référentiel

Bitbucket

Accédez aux paramètres du compte, à la sécurité , à la création et à la gestion des jetons d'API. Les étendues requises dépendent du type de votre jeton.

Workspace/Repository Jeton (ATCT — Authentification du porteur, aucun nom d'utilisateur requis)

Autorisation	Accès	Objectif
Référentiels	Lisez et écrivez	Répertorie les dépôts, lit les branches et écrit le code transformé via git push

Jeton d'API de compte (ATAT — Authentification de base avec e-mail) ou mot de passe d'application (ATBB — Authentification de base avec nom d'utilisateur)

Scope	Objectif
`read:account`	Identifie l'utilisateur authentifié pour résoudre la question de l'appartenance au référentiel
`read:workspace:bitbucket`	Répertorie les espaces de travail auxquels le jeton peut accéder afin que AWS Transform puisse énumérer leurs référentiels. Non obligatoire si vous spécifiez une liste d'espaces de travail dans le secret.
`read:repository:bitbucket`	Répertorie les référentiels et lit les métadonnées et les informations sur les branches
`write:repository:bitbucket`	Réécrit le code transformé dans le référentiel via git push

Azure DevOps

Accédez aux paramètres utilisateur, puis aux jetons d'accès personnels. Sélectionnez Étendue personnalisée. Pour la portée de l'organisation, choisissez Toutes les organisations accessibles (recommandé) ou spécifiez une seule organisation.

Scope	Accès	Objectif
Code	Lire et écrire	Lit le code source, répertorie les référentiels et les branches, et réécrit le code transformé
Profil de l'utilisateur	Lecture	Valide l'accès par jeton et découvre l'identité de l'utilisateur pour la recherche de l'organisation
Gestion des droits des membres	Lecture	Répertorie les organisations auxquelles le jeton a accès pour la découverte du référentiel

Conservez le PAT dans AWS Secrets Manager

1. Ouvrez la AWS Secrets Manager console.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Pour Secret type (Type de secret), choisissez Other type of secret (Autre type de secret).
4. Ajoutez des paires clé-valeur en fonction de votre fournisseur et de votre type d'hébergement :
   - Cloud-hosted providers : ajoutez une clé nommée `token` avec votre PAT comme valeur.
     - Pour Azure DevOps avec une organisation spécifique, ajoutez également une clé `organization` portant le nom de votre organisation.
     - Pour les mots de passe des applications Bitbucket (ATBB), ajoutez également une clé nommée `username` avec votre nom d'utilisateur Bitbucket. Pour les jetons d'API de compte Bitbucket (ATAT), ajoutez une clé nommée `email` avec votre adresse e-mail Bitbucket.
   - Self-hosted et DNS/URL fournisseurs personnalisés : ajoutez les clés suivantes : `host` (URL de votre serveur, par exemple`https://github.mycompany.com`)`github`, `provider_type` (`gitlab`,`bitbucket`, ou`ado`) et `token` (votre PAT).

- Pour Azure DevOps avec une organisation spécifique, ajoutez également une clé `organization` portant le nom de votre organisation.
- Pour les mots de passe des applications Bitbucket (ATBB), ajoutez également une clé nommée `username` avec votre nom d'utilisateur Bitbucket. Pour les jetons d'API de compte Bitbucket (ATAT), ajoutez une clé nommée `email` avec votre adresse e-mail Bitbucket.

L'exemple suivant montre comment se présente un secret AWS Secrets Manager pour un fournisseur GitHub hébergé dans le cloud :

```
{
  "token": "your-github-personal-access-token"
}
```

L'exemple suivant montre le mot de passe d'une application Bitbucket (ATBB) :

```
{
  "token": "your-bitbucket-app-password",
  "username": "my-bitbucket-username"
}
```

L'exemple suivant montre une GitLab instance auto-hébergée :

```
{
  "host": "https://gitlab.mycompany.com",
  "provider_type": "gitlab",
  "token": "your-gitlab-personal-access-token"
}
```

5. Choisissez Suivant.
6. Entrez un nom secret, par exemple`github-pat-myproject`.
7. (Facultatif) Sélectionnez une clé KMS gérée par le client pour le chiffrement.
8. Terminez l'assistant et choisissez Store.
9. Copiez l'ARN secret. Vous avez besoin de cette valeur lorsque vous configurez la tâche AWS Transform.

Si vous utilisez une clé KMS gérée par le client pour chiffrer votre secret (au lieu de la clé AWS gérée par défaut), vous devez mettre à jour la politique de clé KMS pour permettre à AWS Transform de déchiffrer le secret. Ajoutez la déclaration suivante à votre politique de clé KMS gérée par le client :

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

Remplacez *REGION* par votre AWS région (par exemple`us-east-1`) et *YOUR-SECRET-ARN* par l'ARN de votre secret. Cette `kms:ViaService` condition garantit que la clé KMS ne peut être utilisée que via le AWS Secrets Manager service. La `kms:EncryptionContext:SecretARN` condition limite le déchiffrement à votre secret spécifique.

Pour mettre à jour votre politique relative aux clés KMS :

1. Ouvrez la console AWS KMS à l'adresse`https://console.aws.amazon.com/kms`.
2. Dans le panneau de navigation, choisissez Clés gérées par le client.
3. Sélectionnez votre clé KMS.
4. Dans l'onglet Stratégie de clé choisissez Modifier.
5. Ajoutez la déclaration de politique à la politique existante.
6. Sélectionnez Enregistrer les modifications.

> **Note**
>
> Si vous utilisez la clé AWS gérée par défaut (`aws/secretsmanager`), vous n'avez pas besoin de modifier la politique de clé KMS.

Configurez le AWS Transformer le travail

1. Dans votre tâche AWS Transform, accédez à Se connecter aux ressources.
2. Choisissez Connect source code repository.
3. Sélectionnez PAT Connector comme méthode d'authentification.
4. Entrez l'ARN secret de l'étape 2.
5. (Facultatif) Entrez l'ARN de la clé KMS si vous avez utilisé une clé KMS gérée par le client.
6. Sélectionnez votre référentiel et votre branche.
7. Sélectionnez Continuer.

AWS Transform crée automatiquement un rôle IAM avec les autorisations requises pour accéder à votre secret.

Rotation et maintenance des jetons

Vous êtes responsable de la rotation des jetons PAT avant leur expiration. Pour faire pivoter un jeton :

1. Générez un nouveau PAT dans votre fournisseur de code source avec les mêmes autorisations.
2. Mettez à jour la valeur secrète dans AWS Secrets Manager.
3. Vérifiez que votre tâche AWS Transform peut accéder au référentiel avec le nouveau jeton.
4. Révoquez l'ancien PAT dans votre fournisseur de code source.

Résoudre les problèmes liés au connecteur PAT

Accès refusé — PAT non valide

Vérifiez que le PAT n'a pas expiré. Vérifiez que le PAT possède les étendues requises pour votre fournisseur. Vérifiez que le PAT est correctement enregistré AWS Secrets Manager.

Impossible de récupérer le secret

Vérifiez que l'ARN secret est correct. Consultez les journaux des tâches pour vous assurer que AWS Transform a créé le rôle IAM. Si vous utilisez une clé KMS gérée par le client, vérifiez la politique de clé.

Autorisations insuffisantes

Le PAT n'a peut-être pas les étendues requises pour l'opération. Régénérez le PAT avec les étendues requises et mettez à jour la valeur secrète dans. AWS Secrets Manager

Configuration AWS CodeConnections

AWS CodeConnections utilise une intégration de fournisseur géré qui récupère automatiquement les informations d'identification OAuth temporaires via un flux d'autorisation OAuth 2.0. Les autorisations sont configurées dans l'application du fournisseur et gérées entièrement par AWS. Vous autorisez l'application une seule fois et vous gérez l'ensemble AWS de la gestion des informations d'identification.

1. Dans votre tâche de modernisation de SQL Server, accédez à Connexion aux ressources.
2. Choisissez Connect source code repository.
3. Si vous n'avez pas de connexion existante, choisissez Créer une connexion.
4. Sélectionnez le fournisseur de votre référentiel :
   - GitHub / GitHub Entreprise
   - GitLab.com
   - Bitbucket Cloud
   - Référentiels Azure
5. Suivez le flux d'autorisation de votre fournisseur.
6. Après autorisation, choisissez Connect.

Sélectionnez votre référentiel et votre branche

1. Sélectionnez votre référentiel dans la liste.
2. Choisissez la branche que vous souhaitez transformer (généralement principale, principale ou développer).

3. (Facultatif) Spécifiez un sous-répertoire si votre application .NET ne se trouve pas à la racine du référentiel.
4. Sélectionnez Continuer.

> **Note**
>
> AWS Transform crée une nouvelle branche pour le code transformé. Vous pouvez revoir et fusionner les modifications dans le cadre de votre processus normal de révision du code.

Approbation de l'accès au référentiel

Pour GitHub et certaines autres plateformes, l'administrateur du référentiel doit approuver la demande de connexion :

1. AWS Transform affiche un lien de vérification.
2. Partagez ce lien avec l'administrateur de votre référentiel.
3. L'administrateur examine et approuve la demande dans les paramètres de son référentiel.
4. Une fois que l'administrateur a approuvé la demande, l'état de la connexion passe à Approuvé.

> **Important**
>
> Le processus d'approbation peut prendre du temps en fonction des politiques de votre organisation. Planifiez en conséquence.

Étape 4 : Création d'un connecteur de déploiement (facultatif)

Si vous souhaitez déployer les applications transformées sur votre AWS compte, vous pouvez sélectionner un connecteur de déploiement.

Configurer le connecteur de déploiement

1. Sélectionnez Oui si vous souhaitez déployer vos applications. Si vous sélectionnez Non, cette étape sera ignorée.
2. Ajoutez votre AWS compte à l'endroit où vous souhaitez déployer les applications transformées.
3. Ajoutez un nom qui vous permettra de vous souvenir facilement du connecteur

4. Soumettez la demande de connecteur pour approbation.

Approbation du connecteur de déploiement

L'administrateur de votre AWS compte doit approuver la demande de connexion pour le connecteur de déploiement.

1. AWS Transform affiche un lien de vérification
2. Partagez ce lien avec l'administrateur de votre AWS compte
3. L'administrateur examine et approuve la demande dans les paramètres de son référentiel
4. Une fois approuvée, le statut de la connexion passe à Approuvé

> **Important**
>
> Le processus d'approbation peut prendre du temps en fonction des politiques de votre organisation. Planifiez en conséquence.

Étape 5 : Confirmez vos ressources

Une fois connecté à votre base de données et à votre référentiel, AWS Transform vérifie que toutes les ressources requises sont accessibles et prêtes à être transformées.

Quoi AWS Transform vérifie

- Connectivité à la base de données : la connexion est active, l'utilisateur dispose des autorisations requises, les bases de données sont accessibles, la version est prise en charge
- Accès au référentiel : le référentiel est accessible, une branche existe, des fichiers de projet .NET ont été détectés, des connexions à la base de données peuvent être détectées
- Préparation à l'environnement : la configuration VPC prend en charge le DMS, les rôles de AWS service requis existent, la connectivité réseau est établie, la compatibilité régionale est confirmée

Consultez la liste de contrôle avant le vol

1. Accédez à Confirmer vos ressources dans le plan de travail
2. Passez en revue les éléments de la liste de contrôle :

- # Connexion à la base de données vérifiée
- # Accès au référentiel confirmé
- # Version .NET prise en charge
- # Entity Framework ou ADO.NET détecté
- # Configuration réseau valide
- # Autorisations requises accordées

3. Si tous les éléments apparaissent comme complets, choisissez Continuer
4. Si des éléments comportent des avertissements ou des erreurs, corrigez-les avant de continuer

Étape 6 : Découverte et évaluation

AWS Transform analyse votre base de données SQL Server et votre application .NET pour comprendre l'étendue et la complexité de la modernisation.

Ce qui est découvert

- Objets de base de données : tables, vues, index, procédures stockées, fonctions, déclencheurs, contraintes, types de données, colonnes calculées, colonnes d'identité, relations par clé étrangère
- Code de l'application : structure du projet .NET, modèles et configurations Entity Framework, code d'accès aux ADO.NET données, chaînes de connexion à la base de données, appels de procédures stockées, requêtes SQL dans le code
- Dépendances : quelles applications utilisent quelles bases de données, dépendances entre bases de données, procédures stockées partagées, modèles d'accès aux données communs

Processus de découverte

- AWS Transform commence la découverte automatiquement après confirmation de la ressource
- La découverte prend généralement 5 à 15 minutes, selon la taille de la base de données et la complexité de l'application
- Suivez les progrès dans le journal de travail
- AWS Transform affiche des mises à jour en temps réel à mesure que des objets sont découverts

Examiner les résultats des découvertes

Une fois la découverte terminée, accédez à Découverte et évaluation pour passer en revue :

Analyse de base de données :

- Nombre d'objets : nombre de tables, de vues, de procédures stockées, de fonctions, de déclencheurs
- Score de complexité : évaluation de la complexité de la transformation (faible, moyenne, élevée)
- Mesures à prendre : objets pouvant nécessiter l'attention de l'homme
- Fonctionnalités prises en charge : fonctionnalités de base de données qui seront converties automatiquement
- Fonctionnalités non prises en charge : fonctionnalités nécessitant des solutions de contournement

Analyse des applications :

- Type de projet : ASP.NET Core, application console, bibliothèque de classes, etc.
- Version .NET : version .NET Core détectée
- Cadre d'accès aux données : version Entity Framework ou ADO.NET
- Connexions à la base de données : nombre de chaînes de connexion trouvées
- Complexité du code : évaluation de la complexité de la transformation

Carte des dépendances :

- Représentation visuelle des relations entre l'application et la base de données
- Cross-database dépendances
- Composants partagés

Comprendre l'évaluation de la complexité

AWS Transform classe votre modernisation en trois catégories :

Complexité	Caractéristiques	Résultat attendu
Faible (classe A)	Modèles SQL standard (ANSI SQL), procédures stockées simples, types de données de base, Entity Framework avec configurations standard	Intervention humaine minimale attendue, taux de réussite élevé en matière d'automatisation

Complexité	Caractéristiques	Résultat attendu
Moyen (classe B)	T-SQL Modèles avancés, procédures stockées complexes avec logique métier, fonctions définies par l'utilisateur, colonnes calculées	Une certaine intervention humaine est requise, un examen par un expert est recommandé
Élevé (classe C)	assemblages CLR, serveurs liés, Service Broker, recherche complexe en texte intégral	Une importante refactorisation humaine est requise, envisagez une approche par étapes

Rapport d’évaluation

AWS Transform génère un rapport d'évaluation détaillé qui inclut :

- Résumé avec vue d'ensemble de haut niveau
- Inventaire complet des bases de données
- Inventaire des applications
- Pourcentage de préparation à la transformation
- Estimation de l'effort
- Stratégies d'évaluation et d'atténuation des risques
- Approche recommandée

Vous pouvez télécharger le rapport d'évaluation pour le consulter hors ligne et le partager avec les parties prenantes.

Étape 7 : Générer et réviser le plan de vagues

Pour les grands parcs dotés de multiples bases de données et applications, AWS Transform génère un plan d'onde qui organise la modernisation en groupes logiques.

Qu'est-ce qu'un plan de vagues ?

Un plan ondulatoire organise votre modernisation en phases (vagues) en fonction de :

- Dépendances entre les bases de données et les applications
- Priorités commerciales

- Tolérance au risque
- Disponibilité des ressources
- Complexité technique

Chaque vague contient un groupe de bases de données et d'applications qui peuvent être modernisées ensemble sans rompre les dépendances.

Passez en revue le plan des vagues

1. Accédez à la planification des vagues dans le plan de travail
2. Passez en revue les vagues proposées
3. Pour chaque vague, passez en revue :
   - Bases de données incluses
   - Applications incluses
   - Dépendances vis-à-vis d'autres vagues
   - Durée de transformation estimée
   - Niveau de complexité
   - Applications déployables

Personnalisez le plan des vagues

Vous pouvez personnaliser le plan Wave en fonction des besoins de votre entreprise de deux manières :

À l'aide de JSON :

1. Choisissez Télécharger toutes les vagues pour obtenir un fichier JSON contenant toutes les vagues
2. Modifiez les vagues dans le JSON en :
   - Déplacer des bases de données entre les vagues
   - Diviser les vagues en petits groupes
   - Fusionner des vagues
   - Séquence d'ondes changeante
   - Ajouter ou supprimer des bases de données du périmètre

3. Rechargez le fichier JSON sur la console en choisissant Upload wave plan
4. AWS Transform valide vos modifications et vous avertit en cas de violation des dépendances
5. Choisissez Confirmer les vagues pour mettre à jour le plan des vagues

À l'aide du chat :

Vous pouvez modifier les plans de vagues en discutant avec l'agent et en lui demandant de déplacer les référentiels et les bases de données vers des vagues spécifiques. Cette approche fonctionne bien si vous devez apporter des modifications mineures aux vagues.

> **Important**
>
> Assurez-vous que les dépendances sont respectées lors de la personnalisation des vagues. La transformation d'une application dépendante avant sa base de données peut entraîner des problèmes.

Modernisation des bases de données

Si vous modernisez une seule base de données et une seule application, AWS Transform crée un plan simple en une seule vague. Vous pouvez passer directement à la transformation sans planification des vagues.

Approuver le plan de vagues

1. Après avoir révisé et personnalisé (si nécessaire), choisissez Approuver le plan Wave
2. AWS Transform verrouille le plan de vague et procède à la transformation
3. Vous pouvez toujours modifier le plan ultérieurement en choisissant Modifier le plan de vagues

Étape 8 : Conversion du schéma

AWS Transform convertit le schéma de votre base de données SQL Server en Aurora PostgreSQL, y compris les tables, les vues, les procédures stockées, les fonctions et les déclencheurs.

Comment fonctionne la conversion de schéma

AWS Transform utilise la conversion de schéma AWS DMS améliorée par l'IA générative pour :

- Analyser les schémas et les relations SQL Server

- Mapper les types de données de SQL Server aux équivalents PostgreSQL
- Transformer T-SQL en PL/pgSQL
- Gérez les colonnes d'identité, les colonnes calculées et les contraintes
- Valider la conversion et l'intégrité référentielle
- Générez des actions pour les objets nécessitant une révision humaine

Conversions prises en charge

Conversion automatique :

- Tableaux, vues et index
- Clés primaires et clés étrangères
- Vérifiez les contraintes et les valeurs par défaut
- Types de données les plus courants
- Procédures mémorisées simples
- Fonctions de base et déclencheurs
- Colonnes d'identité (converties en SERIAL ou GENERATED)
- Colonnes les plus calculées

Peut nécessiter un examen humain :

- Procédures stockées complexes avec des fonctionnalités avancées T-SQL
- Server-specific Fonctions SQL (GETUTCDATE, SUSER_SNAME, etc.)
- Colonnes calculées avec des expressions complexes
- Full-text index de recherche
- Opérations sur les types de données XML
- Type de données HIERARCHYID (nécessite l'extension LTREE)

Pas automatiquement converti :

- Assemblages CLR
- Serveurs liés
- Courtier de services

- Tâches de SQL Server Agent

Démarrer la conversion du schéma

1. Accédez à la conversion de schéma dans le plan de travail
2. Vérifiez les paramètres de conversion :
   - Version cible de PostgreSQL
   - Options d'extension (ltree, PostGIS, etc.)
   - Convention d'appellation
3. Choisissez Commencer la conversion
4. Suivez les progrès dans le journal de travail
5. La conversion prend généralement 10 à 30 minutes selon le nombre d'objets de base de données

Passez en revue les résultats de conversion

Une fois la conversion terminée, accédez à Revoir la conversion du schéma :

Résumé de la conversion :

- Objets convertis : nombre d'objets convertis avec succès
- Mesures à prendre : objets nécessitant une attention humaine
- Avertissements : problèmes potentiels à examiner
- Erreurs : objets qui n'ont pas pu être convertis

Révision par type d'objet :

- Tableaux : mappages de types de données, contraintes, index
- Procédures stockées : T-SQL vers la PL/pgSQL conversion
- Fonctions : signature des fonctions et modifications de logique
- Déclencheurs : modifications de syntaxe et de synchronisation des déclencheurs

Réviser les mesures à prendre

1. Choisissez Afficher les actions
2. Pour chaque action, passez en revue :

- Nom de l'objet : objet de base de données
- Type de problème : Ce qui nécessite une attention particulière
- Gravité : critique, avertissement ou information
- Recommandation : résolution suggérée
- Code d'origine : version de SQL Server
- Code converti : version PostgreSQL

3. Pour chaque action, vous pouvez :
   - Accepter : utilisez le code converti
   - Modifier : modifiez le code converti
   - Drapeau pour plus tard : Marquer pour examen humain après transformation

Exemple : conversion de procédures stockées

Serveur SQL T-SQL :

```
CREATE PROCEDURE GetProductsByCategory
    @CategoryId INT,
    @PageSize INT = 10
AS
BEGIN
    SET NOCOUNT ON;

    SELECT TOP (@PageSize)
        ProductId,
        Name,
        Price,
        DATEDIFF(DAY, CreatedDate, GETUTCDATE()) AS DaysOld
    FROM Products
    WHERE CategoryId = @CategoryId
    ORDER BY Name
END
```

PostgreSQL PL/pgSQL converti :

```
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;
```

Modifications apportées :

- Procédure convertie en fonction renvoyant TABLE
- Noms de paramètres préfixés par p_
- TOP converti en LIMIT
- DATEDIFF converti en EXTRACT
- GETUTCDATE () converti en NOW ()
- Noms de colonnes convertis en minuscules (convention PostgreSQL)

Approuver la conversion du schéma

1. Après avoir examiné toutes les mesures à prendre et apporté les modifications nécessaires
2. Choisissez Approuver la conversion du schéma
3. AWS Transform prépare le schéma converti pour le déploiement sur Aurora PostgreSQL

> **Note**
>
> Vous pouvez télécharger le schéma converti sous forme de scripts SQL pour une révision hors ligne ou un contrôle de version.

Étape 9 : Migration des données (facultatif)

AWS Transform propose des options pour migrer les données de SQL Server vers Aurora PostgreSQL. La migration des données est facultative et peut être ignorée si vous n'avez besoin que d'une transformation de schéma et de code.

Options de migration des données

Option 1 : Migration des données de production

Migrez vos données de production réelles à l'aide de AWS DMS :

- Chargement initial complet de toutes les données
- Réplication continue pendant les tests (CDC)
- Interruption minimale des temps d'arrêt
- Validation des données et contrôles d'intégrité

Option 2 : Ignorer la migration des données

Transformez le schéma et le code uniquement :

- Utile pour les development/testing environnements
- Quand les données seront migrées séparément
- Pour les projets de validation de concept

Configuration de la migration des données

1. Accédez à Migration des données dans le plan de travail
2. Choisissez votre option de migration :
   - Migrer les données de production
   - Ignorer la migration des données

3. Si vous migrez des données de production, configurez :
   - Type de migration : chargement complet ou chargement complet + CDC
   - Validation : activer la validation des données
   - Performances : taille de l'instance DMS
   - Choisissez >Commencer la migration

Processus de migration des données de production

Si vous choisissez de migrer les données de production :

1. Synchronisation initiale : AWS DMS charge complètement toutes les tables
2. Réplication continue : (si le CDC est activé) Maintient la synchronisation des données
3. Validation : vérifie le nombre de lignes et l'intégrité des données
4. Préparation du découpage : prépare la synchronisation finale

Chronologie de la migration :

- Bases de données de petite taille (< 10 Go) : 30 minutes à 2 heures
- Bases de données moyennes (10 à 100 Go) : 2 à 8 heures
- Bases de données volumineuses (> 100 Go) : plus de 8 heures

Validation des données

AWS Transform valide les données migrées à l'aide des vérifications suivantes :

- Comparaison du nombre de lignes (source et cible)
- Intégrité de la clé primaire
- Relations clés avec l'étranger
- Compatibilité des types de données
- Résultats des colonnes calculés
- Gestion des valeurs nulles

Étape 10 : Transformation du code de l'application

AWS Transform transforme le code de votre application .NET pour qu'il fonctionne avec Aurora PostgreSQL au lieu de SQL Server. Il demande un nom de branche cible dans vos référentiels pour valider le code source transformé. Une fois que vous avez saisi le nom de la branche, AWS Transform crée une nouvelle branche et lance la transformation pour qu'elle corresponde à la base de données PostgreSQL.

Qu'est-ce qui se transforme

Changements apportés à la structure des entités :

- Fournisseur de base de données : UseSqlServer () → UseNpgsql ()
- Chaînes de connexion : format SQL Server → format PostgreSQL
- Mappages de types de données : types SQL Server → types PostgreSQL
- DbContext configurations : SQL Server-specific → PostgreSQL-specific
- Fichiers de migration : mis à jour pour assurer la compatibilité avec PostgreSQL

ADO.NET Changements :

- Classes de connexion : SqlConnection → NpgsqlConnection
- Classes de commandes : SqlCommand → NpgsqlCommand
- Lecteur de données : SqlDataReader → NpgsqlDataReader
- Paramètres : SqlParameter → NpgsqlParameter
- Syntaxe SQL S : T-SQL → PostgreSQL SQL

Changements de configuration :

- Chaînes de connexion dans appsettings.json
- NuGet Packages pour les fournisseurs de bases
- Configurations d'injection de dépendances
- Startup/Program.cs configurations

Démarrer la transformation du code

1. Accédez à la section Transformation des applications dans le plan de travail

2. Vérifiez les paramètres de transformation :
   - Version .NET cible (en cas de mise à niveau)
   - Version du fournisseur PostgreSQL
   - Préférences de style de code
3. Choisissez Commencer la transformation
4. Suivez les progrès dans le journal de travail
5. La transformation prend généralement 15 à 45 minutes selon la taille de la base de code

Étape 11 : Examiner les résultats de la transformation

Avant de procéder au déploiement, examinez les résultats complets de la transformation pour vous assurer que tout est prêt pour les tests.

Vous pouvez télécharger le code transformé depuis la branche du référentiel pour :

- Tests et validation locaux
- Révision du code dans votre IDE
- Intégration à votre CI/CD pipeline
- Commit de contrôle de version

Vous pouvez également télécharger le résumé de la transformation pour consulter les modifications en langage naturel apportées par AWS Transform dans le cadre de la transformation.

Résumé de la transformation

1. Accédez au résumé de la transformation dans le plan de travail
2. Passez en revue les résultats globaux :
   - Conversion de schéma : objets convertis, actions, avertissements
   - Migration des données : tables migrées, lignes transférées, état de validation
   - Transformation du code : fichiers modifiés, lignes modifiées, problèmes résolus
   - Score de préparation : état de préparation global au déploiement

Générer un rapport de transformation

AWS Transform génère un rapport de transformation complet :

1. Choisissez Générer un rapport
2. Sélectionnez le type de rapport :
   - Résumé : High-level aperçu pour les parties prenantes
   - Détails techniques : documentation complète sur la transformation
   - Mesures à prendre : Liste des tâches humaines requises
3. Choisissez Télécharger le rapport

Le rapport inclut :

- Portée et objectifs de la transformation
- Objets et code transformés
- Problèmes rencontrés et solutions
- Résultats de la validation
- Évaluation de la préparation au déploiement
- Recommandations pour les tests

Étape 12 : Validation et tests

Avant le déploiement en production, vérifiez que l'application transformée fonctionne correctement avec Aurora PostgreSQL.

Types de validation

Validation automatique : AWS Transform effectue des contrôles automatisés :

- Validation du schéma sur la base de données source
- Vérification de l'intégrité des données
- Test d'équivalence des requêtes
- Validation des chaînes de connexion
- Validation de configuration

Validation humaine : vous devez effectuer des tests supplémentaires :

- Tests fonctionnels des fonctionnalités de l'application

- Tests d'intégration avec d'autres systèmes
- Tests de performance et analyses comparatives
- Tests d'acceptation par les utilisateurs
- Tests de sécurité

Exécuter une validation automatique

1. Accédez à Validation dans le plan de travail
2. Choisissez Exécuter la validation
3. AWS Transform exécute des tests de validation :
   - Connectivité à la base
   - Compatibilité des schémas
   - Intégrité des données
   - Création de l'application
   - Fonctionnalité de base
4. Passez en revue les résultats de validation :
   - Réussi : tests réussis
   - Échec : tests nécessitant une attention particulière
   - Avertissements : problèmes potentiels à examiner

Liste de contrôle des tests

Fonctionnalité de base de données :

- Toutes les tables sont accessibles
- Les procédures stockées s'exécutent correctement
- Les fonctions renvoient les résultats attendus
- Les déclencheurs se déclenchent correctement
- Contraintes appliquées correctement
- Les index améliorent les performances des requêtes

Fonctionnalité de l'application :

- L'application démarre correctement
- Connexions aux bases de données établies
- Les opérations CRUD fonctionnent correctement
- Les appels de procédures stockées aboutissent
- Transactions commit/rollback correctement
- La gestion des erreurs fonctionne comme prévu

Intégrité des données :

- Le nombre de lignes correspond à la source
- Clés primaires uniques
- Clés étrangères valides
- Colonnes calculées correctes
- Gestion des valeurs nulles appropriée
- Types de données compatibles

Performances :

- Temps de réponse aux requêtes acceptables
- Regroupement de connexions configuré
- Indices optimisés
- Aucun problème de requête N+1
- Efficacité des opérations par lots
- Utilisation des ressources raisonnable

Étape 13 : Déploiement

Une fois la validation réussie, déployez votre application et votre base de données modernisées en production.

Options de déploiement

- Amazon ECS et Amazon EC2 Linux

Pre-deployment liste de contrôle

Avant le déploiement en production :

- Tous les tests de validation ont été réussis
- Test de performance terminé
- Examen de sécurité terminé
- Plan de sauvegarde et de restauration documenté
- Configuration de la surveillance et des alertes
- Équipe formée au nouvel environnement
- Les parties prenantes informées du déploiement
- Fenêtre de maintenance planifiée

Déploiement sur Amazon ECS

1. Accédez à Déploiement dans le plan de travail
2. Choisissez Deploy to ECS
3. Configurez les paramètres de déploiement :
   - Cluster : sélectionnez ou créez un cluster ECS
   - Service : Configuration du service ECS
   - Définition de tâche : revoir la définition de tâche générée
   - Équilibreur de charge : configurer ALB/NLB
   - Auto-scaling: définissez des politiques de dimensionnement
4. Réviser l'infrastructure en tant que code (CloudFormation modèle ou AWS code CDK)
5. Choisissez Deploy

Surveillez le déploiement

AWS Transform déploie votre application :

1. Crée un cluster Aurora PostgreSQL
2. applique le schéma de base de données
3. Charge les données (le cas échéant)
4. Déploie des conteneurs d'applications

5. Configure l'équilibreur de charge
6. Configure la mise à l'échelle automatique

Surveillez la progression du déploiement et vérifiez :

- Provisionnement de l'infrastructure
- Initialisation de la base de données
- Déploiement de l'application
- Contrôles de santé réussis
- Application accessible
- Les connexions aux bases de données fonctionnent
- Journaux indiquant un fonctionnement normal

Post-deployment validation

Après le déploiement :

Test de fumée :

- Vérifiez les fonctionnalités critiques
- Testez les flux de travail des principaux utilisateurs
- Vérifiez les points d'intégration
- Surveiller les taux d'erreur

Surveillance des performances :

- Suivez les temps de réponse
- Surveillance des requêtes de base de données
- Vérifier l'utilisation des ressources
- Consulter les journaux des applications

Validation par l'utilisateur :

- Réaliser des tests d'acceptation par les utilisateurs

- Recueillez des commentaires
- Résolvez tous les problèmes
- Documenter les leçons apprises

Procédures de restauration

Si des problèmes surviennent après le déploiement :

Annulation immédiate :

- Revenir à la version précédente de l'application
- Revenez à SQL Server (s'il est toujours disponible)
- Restaurez à partir d'une sauvegarde si nécessaire

Annulation partielle :

- Restaurer des composants spécifiques
- Conserver les modifications de la base
- Rétablir le code de l'application uniquement

Correctif avancé :

- Appliquer le correctif à la version Aurora PostgreSQL
- Déployez le code d'application mis à
- Moniteur pour la résolution

> **Important**
>
> Gardez votre base de données SQL Server disponible pendant un certain temps après la mise en service afin de permettre la restauration si nécessaire.

Post-deployment optimisation

Après un déploiement réussi :

Réglage des performances :

- Optimisez les requêtes lentes
- Régler les paramètres du pool de connexions
- Fine-tune Paramètres Aurora PostgreSQL
- Passez en revue et optimisez les index

Optimisation des coûts :

- Right-size Instance Aurora
- Configuration appropriée de la mise à l'échelle automatique
- Vérifiez les paramètres de stockage
- Optimisez la conservation des sauvegardes

Configuration de la surveillance :

- Configuration des CloudWatch tableaux de bord
- Configurer les alertes
- Activer la surveillance améliorée
- Configurer les informations sur les performances

Documentation :

- Mettre à jour les runbooks
- Modifications de l'architecture des documents
- Équipe chargée des opérations de formation
- Création de guides de résolution des problèmes

Testez et déployez après la transformation

Déployez vos applications transformées dans la zone d'atterrissage et validez la connectivité entre vos applications et la base de données transformée, et configurez éventuellement des CI/CD pipelines. Des exemples de configurations de CI/CD pipeline sont générés à titre de référence pour

vous aider à implémenter l'automatisation de votre déploiement. Cette dernière phase valide la modernisation complète.

Configuration des ressources

Vous devez configurer les ressources utilisées lors du déploiement, telles que les rôles IAM, les profils d'instance et le compartiment S3. AWS Transform n'est pas autorisé à créer des compartiments S3 ou à apporter des modifications à votre IAM. Cette action doit être effectuée par un utilisateur autorisé à créer de nouveaux rôles. Il s'agit généralement de l'administrateur du compte.

Pour simplifier le processus, nous fournissons un script de configuration qui permet automatiquement de :

- Exécute les modèles nécessaires CloudFormation
- Crée le Service-Linked rôle ECS
- Configure toutes les ressources IAM requises

> **Important**
>
> Exécutez le script de configuration fourni tel quel. Ne modifiez aucun nom de ressource dans les modèles ou le script car cela pourrait avoir un impact sur le processus de déploiement.

Pour Linux :

```
./setup.sh --region <YOUR-Region>
```

Pour Windows :

```
./setup.ps1 -Region <YOUR-Region>
```

Vérifiez les groupes de sécurité dans votre VPC

AWS Transform déploie les applications sur le même sous-réseau et le même groupe de sécurité que l'instance Aurora PostgreSQL.

Pour que l'application puisse se connecter à l'instance Aurora, assurez-vous que ce groupe de sécurité possède des règles sortantes autorisant la connexion au même groupe de sécurité et des règles entrantes autorisant la connexion depuis le même groupe de sécurité.

Sélection et configuration des applications

L'interface utilisateur de AWS Transform affiche la liste des applications qui peuvent être déployées. Sélectionnez l'application et cliquez sur Configurer et valider pour ouvrir une fenêtre de configuration dans laquelle vous pouvez spécifier :

- Infrastructure cible pour les applications : sélectionnez ECS ou l'une des instances EC2
- Paramètres de l'application ou de l'instance

Une fois que vous avez terminé et fermé la fenêtre de configuration, AWS transformez :

- Génère des artefacts de déploiement en fonction de votre configuration
- Commet ces artefacts dans votre référentiel, notamment :
  - Scripts de déploiement
  - CloudFormation modèles
  - Exemples de configurations de CI/CD pipeline (que vous pouvez utiliser comme référence pour configurer l'automatisation de votre déploiement)

Une fois la validation terminée, le statut de l'application passe à Configuré et validé. Vous pouvez ensuite sélectionner les applications et utiliser le bouton Déployer en haut à droite pour lancer le déploiement.

Déploiement ECS

Toutes les applications avec ECS cible sont déployées dans un nouveau cluster ECS créé dans votre compte. Chaque application est déployée dans son propre conteneur dédié ; plusieurs applications par conteneur ne sont pas prises en charge. Vous configurez les paramètres du conteneur pour chaque application individuellement, tels que le processeur et la mémoire requis.

Déploiement d'EC2

Vous pouvez sélectionner l'une des instances EC2 proposées et configurer ses paramètres tels que le type d'instance. Plusieurs applications peuvent être déployées sur la même instance EC2 :

- Pour déployer plusieurs applications sur une seule instance, sélectionnez la même instance EC2 cible pour chacune de ces applications lors de la configuration.
- Toutes les applications dont la même instance est sélectionnée comme cible sont déployées sur cette instance et des ports aléatoires différents lui sont attribués.

- Notez que si vous modifiez les paramètres d'instance d'une application, puis que vous modifiez une autre application ciblant la même instance, les modifications concernent toutes les applications déployées sur cette instance.

Déploiement réussi

Une fois le déploiement réussi, vos applications s'exécutent sur Aurora PostgreSQL avec des coûts de licence réduits, des performances améliorées et une évolutivité native du cloud. La tâche reste ouverte sauf si elle est explicitement arrêtée. Cela permet d'envisager un éventuel redéploiement avec des paramètres de déploiement mis à jour.

Charger des fichiers DDL (flux de travail hors ligne)

Dans ce flux de travail, AWS Transform modernise entièrement votre schéma à partir de fichiers DDL chargés. Aucune connexion directe à votre base de données n'est requise. Vous exécutez un script d'extraction fourni sur votre serveur SQL, vous chargez les fichiers de schéma qui en résultent, et AWS Transform découvre, évalue, convertit et déploie le schéma sur Amazon Aurora PostgreSQL. Choisissez ce flux de travail lorsque votre base de données ne peut pas être exposée à une connexion directe ou lorsque vous souhaitez une évaluation de faisabilité et une conversion de schéma avant d'accorder l'accès au réseau.

> **Important**
>
> Le flux de travail hors ligne convertit et déploie uniquement votre schéma. Il ne migre pas de données réelles. Le cas échéant, vous pouvez générer des données de test synthétiques pour valider la cible. Si vous devez migrer des données réelles, utilisez la console AWS DMS pour créer un nouveau projet de migration de données.

Prérequis pour le flux de travail hors ligne

- Une version de SQL Server prise en charge (2008 R2 à 2022, toutes éditions confondues).
- PowerShell 7 ou version ultérieure pour exécuter le script d'extraction. PowerShell est préinstallé sur Windows. Sur macOS ou Linux, installez PowerShell 7+ et exécutez le script avec`pwsh`. Consultez le guide d'installation de Microsoft.
- L'`sqlcmd`utilitaire disponible sur le PATH. Voir l'utilitaire sqlcmd.

- Un identifiant d'authentification SQL Server (nom d'utilisateur et mot de passe) avec au moins `VIEW SERVER STATE` et `VIEW ANY DEFINITION` des autorisations. Le script ne prend pas en charge l'authentification Windows ou de domaine.
- Un AWS compte pour les phases ultérieures (création de la cible Aurora PostgreSQL et déploiement du schéma converti), avec IAM Identity Center ou l'authentification IAM activée.
- Aucune connectivité de base de données entrante ou sortante n' AWS est requise pour les phases d'analyse du schéma et de conversion.

Étapes du workflow

1. Charger des fichiers DDL — AWS Transform propose un bouton de téléchargement pour un script d'extraction dans le chat. Téléchargez et exécutez le script sur votre serveur SQL. Limitez éventuellement l'extraction à des bases de données spécifiques avec une liste d'inclusion séparée par des virgules (sans distinction majuscules/minuscules). Le script produit un horodatage `.zip` des fichiers SQL DDL. Téléchargez le `.zip` (ou les `.sql` fichiers individuels) à l'aide du bouton de téléchargement du chat.
2. Discovery — AWS Transform analyse les fichiers chargés et catalogue les objets de base de données (tables, procédures stockées, vues, déclencheurs, index, contraintes, séquences, etc.), regroupés par base de données. Vous examinez un résumé par base de données et vous choisissez les bases de données à évaluer. Si certaines instructions ne peuvent pas être analysées, AWS Transform signale les problèmes et vous permet de continuer avec les objets analysés, de choisir des bases de données spécifiques ou de télécharger des fichiers corrigés.
3. Évaluation — AWS Transform évalue la faisabilité de la conversion pour les bases de données sélectionnées et produit un rapport téléchargeable contenant un résumé, un résumé par objet de base de données et une estimation du niveau d'effort (LOE). Personnalisez les scores LOE, téléchargez des fichiers supplémentaires ou procédez à la conversion.
4. Conversion de schéma : AWS Transform convertit le schéma SQL Server (y compris les procédures T-SQL stockées) en Aurora PostgreSQL, une base de données à la fois. Une seule base de données est convertie automatiquement ; dans le cas de plusieurs bases de données, vous choisissez laquelle convertir. Les bases de données sont converties indépendamment et en parallèle.
5. Provisionnement cible : pour chaque base de données convertie, AWS Transform crée ou réutilise un cluster Amazon Aurora PostgreSQL dans votre compte. AWS Vous choisissez le réseau et la configuration cible à l'aide d'instructions guidées.

6. Déploiement du schéma : AWS Transform applique le schéma converti au cluster Aurora. Après le déploiement, corrigez les objets restants dans le chat ou dans un IDE, générez des données de test synthétiques (le cas échéant) ou terminez.
7. Modernisation du code d'application (facultatif) — AWS Transform peut mettre à jour les applications .NET 6+ associées pour qu'elles fonctionnent avec Aurora PostgreSQL. Le service met à jour les connexions à la base de données dans le code source et modifie le code ORM dans Entity Framework ADO.NET pour être compatible avec Aurora PostgreSQL dans un flux de travail unifié sous supervision humaine. Connectez votre référentiel de code source à l'aide AWS CodeConnections d'un jeton d'accès personnel (PAT) pour GitHub et GitLab, ou fournissez un URI S3 pour un fichier zip contenant le code source.

> **Note**
>
> Amazon Aurora PostgreSQL est le seul moteur cible pris en charge pour ce flux de travail.

Limites de service pour le flux de travail hors ligne

Les limites par défaut suivantes s'appliquent au flux de travail hors ligne. Certaines limites sont configurables par compte ; contactez l'équipe chargée de votre AWS compte pour demander une augmentation.

Limite	Par défaut	S'applique à
Taille du téléchargement par tâche	1 024 Mo (1 Go), cumulés sur tous les téléchargements de la tâche	Télécharger des fichiers DDL
Bases de données converties par mois	10 par compte	Conversion du schéma
Procédures stockées par base de données	250	Conversion du schéma

Limite	Par défaut	S'applique à
Conversions de schémas simultanées	5 bases de données à la fois	Conversion du schéma
Tâches exécutées simultanément	5	Par compte

- La limite de taille de téléchargement est un budget cumulé par tâche. Si vous réinitialisez la configuration des entrées, le budget est effacé (les fichiers déjà chargés sont supprimés et la découverte et l'évaluation sont relancées dans la même tâche).
- Lorsque vous choisissez plus de 5 bases de données à convertir, les bases de données supplémentaires sont mises en file d'attente et démarrent automatiquement à la fin des conversions en cours.
- L'évaluation n'est jamais bloquée par la limite du nombre de procédures stockées par base de données ; seule la conversion du schéma est affectée.

Résolution des problèmes liés au workflow hors ligne

Script d'extraction

- **`pwsh: command not found`**(macOS/Linux) — PowerShell 7+ n'est pas installé. Installez-le et lancez-le`pwsh ./ExtractDatabaseMetadata.ps1`.
- Erreurs de référencement **`sqlcmd`** : l'`sqlcmd`utilitaire ne figure pas dans le PATH. Installez-le et assurez-vous qu'il se trouve sur le PATH.
- Erreurs de connexion ou d'autorisation : utilisez une connexion d'authentification SQL Server avec `VIEW SERVER STATE` et`VIEW ANY DEFINITION`. Windows/domain l'authentification n'est pas prise en charge.
- Seules certaines bases de données ont été exportées — La liste d'inclusion a réduit la portée. Re-run sans elle, ou spécifiez les noms de base de données séparés par des virgules corrects.

Charger

- Téléchargement rejeté avec un message de taille — Le budget de téléchargement par tâche est dépassé. Téléchargez un fichier plus petit ou demandez à l'agent de réinitialiser la configuration

des entrées pour effacer le budget pour la même tâche. Demandez à l'agent le budget restant actuel plutôt que de l'estimer.

- Fichier non accepté — Téléchargez les fichiers `.zip` produits par le script ou des `.sql` fichiers individuels. Compressez plusieurs fichiers dans une seule archive.

Découverte

- Problèmes de syntaxe SQL détectés — Téléchargez le rapport sur les problèmes. Les objets des sections exemptes d'erreurs sont toujours catalogués. Choisissez de continuer avec les objets analysés, de choisir des bases de données spécifiques ou de télécharger les fichiers corrigés.
- Objets regroupés sous un nom générique — L'analyseur n'a pas pu trouver d'`USE [Database]`instruction. Lorsque vous y êtes invité, indiquez le nom de base de données correct.
- Aucun objet trouvé : les fichiers ne contenaient aucune instruction`CREATE`, ou tous n'ont pas pu être analysés. Re-upload DDL valide.

Évaluation

- Les estimations de la LOE sont annulées : choisissez de personnaliser les scores de LOE, modifiez le modèle et téléchargez-le à nouveau pour régénérer l'évaluation.
- Objets manqués : choisissez de télécharger des fichiers SQL supplémentaires ; la découverte et l'évaluation sont automatiquement relancées.

Conversion du schéma

- Une conversion de base de données échoue : AWS Transform en indique la raison. Répondez en demandant de réessayer ; la conversion redémarre pour cette base de données.
- Une réponse est dirigée vers la mauvaise base de données — Lorsque plusieurs bases de données sont en attente de saisie, spécifiez à quelle base de données votre message est destiné. Vous pouvez vous adresser à une base de données spécifique avec`@DatabaseName:`.

Approvisionnement et déploiement de cibles

- Impossible de créer le cluster Aurora — Répondez aux instructions d'identification et de mise en réseau guidées, et assurez-vous que le compte est autorisé à créer Aurora PostgreSQL.

- Certains objets n'ont pas été déployés : utilisez les options de post-déploiement pour corriger les objets restants dans le chat ou dans un IDE, puis redéployez.

Bonnes pratiques et dépannage

Les meilleures pratiques, les problèmes courants et leur résolution au cours du processus de modernisation.

Journaux des applications ECS

CloudWatch journaux

- Tous les journaux de conteneurs ECS sont automatiquement envoyés à CloudWatch Logs
- Accédez aux journaux dans la CloudWatch console sous Log Groups
- Format de dénomination des groupes de journaux :/aws/ecs/{application-name}
- Chaque instance de conteneur crée un nouveau flux de journaux au sein du groupe

Affichage des journaux

Par le biais AWS de la console :

- Accédez à CloudWatch > Groupes de journaux
- Sélectionnez le groupe de journaux de votre application
- Choisissez le flux de journaux approprié pour afficher les journaux des conteneurs

En utilisant la AWS CLI :

```
aws logs get-log-events --log-group-name /aws/ecs/your-app-name --log-stream-name your-
stream-name
```

Emplacements courants des journaux

- Journaux des applications : CloudWatch journaux
- Événements de service ECS : console ECS > Cluster > Service > onglet Événements
- Conteneur health/status : ECS Console > Cluster > Service > onglet Tâches

Gestion des connexions aux bases de données

Les applications utilisent des variables d'environnement pour les paramètres de connexion à la base de données

Si vous rencontrez des problèmes de connectivité :

- Vérifiez les paramètres de connexion actuels dans vos variables d'environnement
- Mettez à jour les variables d'environnement pour modifier les chaînes de connexion à la base de données si nécessaire
- Les modifications de la chaîne de connexion peuvent être effectuées par le biais de mises à jour des variables d'environnement sans redéploiement de l'application

Problèmes de connexion aux bases de données

Problème : Impossible de connecter AWS Transform à SQL Server

Solutions :

- Vérifiez la connectivité réseau entre AWS Transform et SQL Server
- Vérifiez les règles du groupe de sécurité pour un accès correct aux ports (1433)
- Vérifiez les informations d'identification de la base de données dans Secrets
- Testez les autorisations de base de données avec l'utilisateur créé
- Assurez-vous que SQL Server est configuré pour l'authentification en mode mixte
- Vérifier que le secret possède les balises requises (Projet : atx-db-modernization, propriétaire : database-connector)

Problèmes liés au pare-feu et aux groupes de sécurité

Problème : expiration du délai de connexion ou erreur « Impossible d'accéder à la base de données »

Cause principale : groupes de sécurité ou ACL réseau bloquant le trafic

Solutions :

1. Vérifiez la configuration du groupe de sécurité :

- Vérifiez que votre groupe de sécurité SQL Server dispose d'une règle entrante autorisant le port 1433 depuis le groupe de sécurité DMS Schema Conversion
- Vérifiez que la source est l'ID du groupe de sécurité (par exemple, sg-0123456789abcdef0), et non une adresse IP
- Vérifiez que le groupe de sécurité DMS Schema Conversion est correctement spécifié dans le profil d'instance
- Assurez-vous qu'il n'y a pas de règles de refus contradictoires

2. Vérifiez les ACL réseau :
   - Vérifiez que les ACL réseau au niveau du sous-réseau autorisent le trafic entrant sur le port 1433
   - Assurez-vous que les ACL réseau autorisent les ports éphémères sortants pour le trafic de retour
   - Vérifiez à la fois le sous-réseau de la base de données et le sous-réseau DMS (ACL) réseau
3. Vérifiez la configuration du VPC :
   - Vérifiez que l'instance de conversion de schéma DMS et SQL Server se trouvent dans le même VPC ou disposent d'un peering VPC approprié
   - Vérifiez que les tables de routage autorisent le trafic entre les sous-réseaux
   - Vérifiez qu'aucune appliance de pare-feu ne bloque le trafic
4. Testez la connectivité :
   - Lancer une instance EC2 de test dans le même sous-réseau que DMS Schema Conversion
   - Attachez le même groupe de sécurité que DMS Schema Conversion
   - Testez la connexion à SQL Server à l'aide de Telnet ou de SQL Server Management Studio
   - Si le test réussit, le problème provient de la configuration de AWS Transform ; s'il échoue, le problème est network/firewall

Erreur courante : ouverture du port 1433 à 0.0.0. 0/0 (toutes sources confondues) constitue un risque pour la sécurité. Utilisez toujours le contrôle d'accès basé sur les groupes de sécurité pour limiter l'accès au seul groupe de sécurité DMS Schema Conversion.

Problèmes de conversion de schéma

Problème : la conversion de schéma affiche de nombreuses actions

Solutions :

- Passer en revue les mesures à prendre dans le rapport de conversion
- Prioriser en fonction de l'impact
- Utilisez Amazon Q Developer pour les conversions SQL complexes
- Consultez le AWS support pour obtenir des conseils
- Envisagez une approche par étapes pour les bases de données complexes

Problèmes liés à la transformation des applications

Problème : la transformation de l'application ne parvient pas à être créée

Solutions :

- Examiner les erreurs de génération dans le rapport de transformation
- Configurez NuGet les flux privés si nécessaire
- Mettre à jour les références des packages si nécessaire
- Vérifiez les Windows-specific dépendances
- Consultez les journaux de transformation pour détecter les erreurs détaillées

Problèmes liés à la migration des données

Problème : échec de la validation de la migration des données

Solutions :

- Examiner le rapport de validation pour détecter des défaillances spécifiques
- Vérifiez les mappages de types de données
- Vérifier la configuration de la colonne d'identité (GÉNÉRÉ PAR DÉFAUT ou GÉNÉRÉ TOUJOURS)
- Passez en revue les expressions de colonnes calculées
- Contactez le AWS support pour les problèmes complexes liés aux données

Problèmes de nettoyage des ressources

Problème : échec de la tâche de transformation en raison d'erreurs liées aux ressources

Solutions :

- Vérifiez les ressources DMS existantes (projets de migration, fournisseurs de données, profils d'instance)
- Nettoyez les ressources échouées ou incomplètes des tentatives précédentes
- Vérifiez que la suppression des secrets n'est pas programmée
- Vérifiez les quotas de service pour DMS et Aurora PostgreSQL
- Contactez AWS le support si le nettoyage ne résout pas le problème

Problèmes de déploiement

Problème : l'application transformée ne peut pas se connecter à Aurora PostgreSQL

Solutions :

- Vérifier le format de chaîne de connexion pour PostgreSQL
- Vérifiez les règles des groupes de sécurité
- Vérifiez les informations d'identification de base de données dans Secrets Manager
- Assurez-vous qu' SSL/TLS il est correctement configuré
- Testez la connexion à l'aide de psql ou pgAdmin

Aide supplémentaire

Lorsque vous contactez AWS le support, veuillez fournir :

- ID de tâche de transformation
- AWS ID de compte
- Région
- Messages d'erreur et captures d'écran
- Journaux de transformation (disponibles dans la console AWS Transform)

Sécurité dans AWS Transformation

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Transform, voir AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS Transform. Les rubriques suivantes expliquent comment configurer AWS Transform pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources AWS Transform.

Rubriques

Protection des données dans AWS Transform

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans AWS Transform. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble des AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable de la configuration de la sécurité et des tâches de gestion de Services AWS ce que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) relatives à la confidentialité des données. Pour plus d'informations sur la protection des données en Europe, consultez l'article intitulé AWS Shared Responsibility Model and GDPRAWS sur le blog sur la sécurité .

Pour des raisons de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous vous recommandons le certificat TLS 1.2 ou une version ultérieure.
- Configurez l'API et la journalisation des activités des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS cryptage, ainsi que tous les contrôles de sécurité par défaut qui s'y trouvent Services AWS.
- Utilisez des services de sécurité gérés avancés tels que Amazon Macie, qui vous aident à découvrir et à sécuriser les données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons vivement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec AWS Transform ou Services AWS utilisez l' Console de gestion AWS API () ou les kits de développement logiciel AWS Command Line Interface

(AWS SDK AWS CLI). Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Pour plus d'informations sur l' AWS Transform utilisation du contenu, consultezAWS Transform amélioration du service.

AWS Transform stocke vos questions, leurs réponses et un contexte supplémentaire, tel que les métadonnées et le code de la console dans votre IDE, pour générer des réponses à vos questions. Pour plus d'informations sur le mode de chiffrement des données, consultez Chiffrement des données dans AWS Transform. Pour plus d'informations sur la manière dont certaines questions que vous posez AWS Transform et leurs réponses AWS peuvent être utilisées pour améliorer nos services, consultezAWS Transform amélioration du service.

Dans AWS Transform, vos données sont stockées dans la AWS région où votre AWS Transform profil a été créé.

Grâce à l'inférence croisée, vos demandes AWS Transform peuvent être traitées dans une région différente de la zone géographique où vos données sont stockées. Pour plus d'informations, voir Cross-Region inférence.

Rubriques

- Cross-region traitement dans AWS Transform
- Chiffrement des données dans AWS Transform
- AWS Transform amélioration du service

Cross-region traitement dans AWS Transform

Les sections suivantes décrivent comment l'inférence interrégionale et les appels interrégionaux sont utilisés pour fournir le service. AWS Transform

Cross-region inférence

AWS Transform est alimenté par Amazon Bedrock et utilise l'inférence entre régions pour répartir le trafic entre différentes régions afin d'améliorer les performances et la fiabilité Régions AWS de l'inférence selon un modèle de langage étendu (LLM). Grâce à l'inférence entre régions, vous obtenez :

- Débit et résilience accrus pendant les périodes de forte demande
- Amélioration des performances

- Accès aux nouvelles AWS Transform capacités et fonctionnalités qui s'appuient sur les LLM les plus puissants hébergés sur Amazon Bedrock

Cross-region les demandes d'inférence sont conservées dans la Régions AWS zone géographique où se trouvent les données à l'origine. Par exemple, une demande effectuée à partir d'une AWS Transform configuration aux États-Unis est conservée Régions AWS aux États-Unis. Bien que l'inférence entre régions ne modifie pas l'endroit où vos données sont stockées, vos demandes et les résultats de sortie peuvent être déplacés en dehors de la région dans laquelle les données se trouvent à l'origine. Toutes les données sont chiffrées lors de leur transmission sur le réseau sécurisé d'Amazon. L'utilisation de l'inférence entre régions n'entraîne aucun coût supplémentaire.

L'inférence entre régions n'affecte pas l'endroit où vos données sont stockées. Pour plus d'informations sur l'endroit où les données sont stockées lorsque vous les utilisez AWS Transform, consultezProtection des données dans AWS Transform.

Régions prises en charge pour AWS Transform inférence entre régions

Certaines demandes que vous envoyez AWS Transform peuvent nécessiter des appels interrégionaux. Le tableau suivant décrit les régions vers lesquelles vos demandes peuvent être acheminées en fonction de la zone géographique d'origine de la demande.

Région source	Régions de destination
USA Est (Virginie du Nord) (us-east-1)	USA Est (Virginie du Nord) (us-east-1) USA Est (Ohio) (us-east-2) USA Ouest (Oregon) (us-west-2)
Europe (Francfort) (eu-central-1)	Europe (Francfort) (eu-central-1) Europe (Stockholm) (eu-north-1) Europe (Milan) (eu-south-1) Europe (Espagne) (eu-south-2) Europe (Irlande) (eu-west-1) Europe (Paris) (eu-west-3)

Région source	Régions de destination
Asie-Pacifique (Mumbai) (ap-south-1)	Asie-Pacifique (Tokyo) (ap-northeast-1) Asie-Pacifique (Séoul) (ap-northeast-2) Asie-Pacifique (Osaka) (ap-northeast-3) Asie-Pacifique (Mumbai) (ap-south-1) Asie-Pacifique (Hyderabad) (ap-south-2) Asie-Pacifique (Singapour) (ap-southeast-1) Asie-Pacifique (Sydney) (ap-southeast-2) Asie-Pacifique (Melbourne) (ap-southeast-4)
Asie-Pacifique (Tokyo) (ap-northeast-1)	Asie-Pacifique (Tokyo) (ap-northeast-1) Asie-Pacifique (Osaka) (ap-northeast-3)
Asie-Pacifique (Séoul) (ap-northeast-2)	Asie-Pacifique (Tokyo) (ap-northeast-1) Asie-Pacifique (Séoul) (ap-northeast-2) Asie-Pacifique (Osaka) (ap-northeast-3) Asie-Pacifique (Mumbai) (ap-south-1) Asie-Pacifique (Hyderabad) (ap-south-2) Asie-Pacifique (Singapour) (ap-southeast-1) Asie-Pacifique (Sydney) (ap-southeast-2) Asie-Pacifique (Melbourne) (ap-southeast-4)
Asie-Pacifique (Sydney) (ap-southeast-2)	Asie-Pacifique (Sydney) (ap-southeast-2) Asie-Pacifique (Melbourne) (ap-southeast-4)

Région source	Régions de destination
Europe (Londres) (eu-west-2)	Europe (Francfort) (eu-central-1) Europe (Stockholm) (eu-north-1) Europe (Milan) (eu-south-1) Europe (Espagne) (eu-south-2) Europe (Irlande) (eu-west-1) Europe (Londres) (eu-west-2) Europe (Paris) (eu-west-3)
Canada (Centre) (ca-central-1)	Commercial Régions AWS + Canada (Centre) (ca-central-1)
Amérique du Sud (São Paulo) (sa-east-1)	Commercial Régions AWS + Amérique du Sud (São Paulo) (sa-east-1)

Pour une liste complète des régions que vous pouvez utiliser AWS Transform, consultezRégions prises en charge pour AWS Transform.

Cross-Region connaissances

Lorsque vous posez une question générale sur les AWS Transform services, les flux de transformation ou la AWS documentation associée, vous AWS Transform pouvez envoyer des demandes interrégionales à l'est des États-Unis (Virginie) (us-east-1) pour les régions des États-Unis ou à l'Europe (Francfort) (eu-central-1) pour toutes les autres régions afin de récupérer de la documentation et de répondre à votre demande. Par exemple, lorsque vous posez des questions sur l'utilisation d'autres AWS services tels que Lambda, vous AWS Transform pouvez effectuer un appel interrégional pour récupérer la AWS documentation pertinente répondant à votre question. Le tableau suivant décrit les régions vers lesquelles vos demandes peuvent être acheminées en fonction de la zone géographique d'origine de la demande.

Région source	Régions de destination
USA Est (Virginie du Nord) (us-east-1)	USA Est (Virginie du Nord) (us-east-1)
Europe (Francfort) (eu-central-1)	Europe (Francfort) (eu-central-1)
Europe (Londres) (eu-west-2)	Europe (Francfort) (eu-central-1)
Asie-Pacifique (Tokyo) (ap-northeast-1)	Europe (Francfort) (eu-central-1)
Asie-Pacifique (Sydney) (ap-southeast-2)	Europe (Francfort) (eu-central-1)
Asie-Pacifique (Séoul) (ap-northeast-2)	Europe (Francfort) (eu-central-1)
Asie-Pacifique (Mumbai) (ap-south-1)	Europe (Francfort) (eu-central-1)
Canada (Centre) (ca-central-1)	Europe (Francfort) (eu-central-1)
Amérique du Sud (São Paulo) (sa-east-1)	Europe (Francfort) (eu-central-1)

Ce paramètre est activé par défaut. Un administrateur de compte peut modifier ce paramètre. La désactivation de cette fonctionnalité entraîne la perte de l'accès aux fonctionnalités qui nécessitent de AWS Transform récupérer des connaissances provenant d'autres régions. Cela peut entraîner des réponses moins précises.

Pour désactiver les appels interrégionaux effectués par AWS Transform :

1. Lors de la première configuration AWS Transform, accédez à la page Get Started et terminez la configuration. Pour une AWS Transform configuration existante, accédez à la page Paramètres.
2. Activez les appels interrégionaux pour répondre aux questions générales AWS liées à la position Off.

AWS Transform pour l'inférence entre régions Windows

Le tableau suivant indique les régions source à partir desquelles vous pouvez appeler le profil d'inférence et les régions de destination vers lesquelles les demandes peuvent être acheminées :

Région source	Régions de destination d'inférence
USA Est (Virginie du Nord) (us-east-1)	USA Est (Virginie du Nord) (us-east-1) USA Est (Ohio) (us-east-2) USA Ouest (Oregon) (us-west-2)
Europe (Francfort) (eu-central-1)	Europe (Francfort) (eu-central-1) Europe (Stockholm) (eu-north-1) Europe (Milan) (eu-south-1) Europe (Espagne) (eu-south-2) Europe (Irlande) (eu-west-1) Europe (Paris) (eu-west-3)
Asie-Pacifique (Tokyo) (ap-northeast-1)	Asie-Pacifique (Tokyo) (ap-northeast-1) Asie-Pacifique (Osaka) (ap-northeast-3)
Asie-Pacifique (Sydney) (ap-southeast-2)	Asie-Pacifique (Sydney) (ap-southeast-2) Asie-Pacifique (Melbourne) (ap-southeast-4)
Asie-Pacifique (Séoul) (ap-northeast-2)	Toutes les régions commerciales
Asie-Pacifique (Mumbai) (ap-south-1)	Toutes les régions commerciales
Canada (Centre) (ca-central-1)	Toutes les régions commerciales

AWS Transform pour l'inférence interrégionale sur les migrations

Le tableau suivant indique les régions source à partir desquelles vous pouvez appeler le profil d'inférence et les régions de destination vers lesquelles les demandes peuvent être acheminées :

Région source	Régions de destination d'inférence
USA Est (Virginie du Nord) (us-east-1)	Toutes les régions commerciales
Europe (Francfort) (eu-central-1)	Toutes les régions commerciales
Europe (Londres) (eu-west-2)	Toutes les régions commerciales
Asie-Pacifique (Tokyo) (ap-northeast-1)	Asie-Pacifique (Tokyo) (ap-northeast-1) Asie-Pacifique (Osaka) (ap-northeast-3)
Asie-Pacifique (Sydney) (ap-southeast-2)	Asie-Pacifique (Sydney) (ap-southeast-2) Asie-Pacifique (Melbourne) (ap-southeast-4)
Asie-Pacifique (Séoul) (ap-northeast-2)	Toutes les régions commerciales
Asie-Pacifique (Mumbai) (ap-south-1)	Toutes les régions commerciales
Canada (Centre) (ca-central-1)	Toutes les régions commerciales

AWS Transform pour l'inférence entre régions du mainframe

AWS Transform pour mainframe utilise l'inférence géographique entre régions d'Amazon Bedrock. Cela signifie que certains de vos appels peuvent être routés Régions AWS en dehors de votre région d'origine. Le tableau suivant indique les régions source à partir desquelles vous pouvez appeler le profil d'inférence et les régions de destination vers lesquelles les demandes peuvent être acheminées :

Région source	Régions de destination d'inférence
USA Est (Virginie du Nord) (us-east-1)	USA Est (Virginie du Nord) (us-east-1) USA Est (Ohio) (us-east-2) USA Ouest (Oregon) (us-west-2)
Europe (Francfort) (eu-central-1)	Europe (Francfort) (eu-central-1)

Région source	Régions de destination d'inférence
	Europe (Stockholm) (eu-north-1) Europe (Milan) (eu-south-1) Europe (Espagne) (eu-south-2) Europe (Irlande) (eu-west-1) Europe (Paris) (eu-west-3)
Europe (Londres) (eu-west-2)	Europe (Francfort) (eu-central-1) Europe (Stockholm) (eu-north-1) Europe (Milan) (eu-south-1) Europe (Espagne) (eu-south-2) Europe (Irlande) (eu-west-1) Europe (Londres) (eu-west-2) Europe (Paris) (eu-west-3)
Asie-Pacifique (Tokyo) (ap-northeast-1)	Asie-Pacifique (Tokyo) (ap-northeast-1) Asie-Pacifique (Osaka) (ap-northeast-3)
Asie-Pacifique (Sydney) (ap-southeast-2)	Asie-Pacifique (Sydney) (ap-southeast-2) Asie-Pacifique (Melbourne) (ap-southeast-4)
Asie-Pacifique (Séoul) (ap-northeast-2)	Toutes les régions commerciales
Asie-Pacifique (Mumbai) (ap-south-1)	Toutes les régions commerciales

Région source	Régions de destination d'inférence
Canada (Centre) (ca-central-1)	Canada (Centre) (ca-central-1) USA Est (Virginie du Nord) (us-east-1) USA Est (Ohio) (us-east-2) USA Ouest (Oregon) (us-west-2)
Amérique du Sud (São Paulo) (sa-east-1)	Toutes les régions commerciales

AWS Transform Personnalisé

AWS Transform custom utilise l'inférence géographique interrégionale d'Amazon Bedrock. Cela signifie que certains de vos appels peuvent être routés Régions AWS en dehors de votre région d'origine. Le tableau suivant indique les régions source à partir desquelles vous pouvez appeler le profil d'inférence et les régions de destination vers lesquelles les demandes peuvent être acheminées :

Région source	Régions de destination d'inférence
USA Est (Virginie du Nord) (us-east-1)	USA Est (Virginie du Nord) (us-east-1) USA Est (Ohio) (us-east-2) USA Ouest (Oregon) (us-west-2)
Europe (Francfort) (eu-central-1)	Europe (Francfort) (eu-central-1) Europe (Stockholm) (eu-north-1) Europe (Milan) (eu-south-1) Europe (Espagne) (eu-south-2) Europe (Irlande) (eu-west-1) Europe (Paris) (eu-west-3)

Région source	Régions de destination d'inférence
Europe (Londres) (eu-west-2)	Europe (Francfort) (eu-central-1) Europe (Stockholm) (eu-north-1) Europe (Milan) (eu-south-1) Europe (Espagne) (eu-south-2) Europe (Irlande) (eu-west-1) Europe (Londres) (eu-west-2) Europe (Paris) (eu-west-3)
Asie-Pacifique (Tokyo) (ap-northeast-1)	Toutes les régions commerciales
Asie-Pacifique (Sydney) (ap-southeast-2)	Asie-Pacifique (Sydney) (ap-southeast-2) Asie-Pacifique (Melbourne) (ap-southeast-4)
Asie-Pacifique (Séoul) (ap-northeast-2)	Toutes les régions commerciales
Asie-Pacifique (Mumbai) (ap-south-1)	Toutes les régions commerciales
Canada (Centre) (ca-central-1)	Canada (Centre) (ca-central-1) USA Est (Virginie du Nord) (us-east-1) USA Est (Ohio) (us-east-2) USA Ouest (Oregon) (us-west-2)

Chiffrement des données dans AWS Transform

Cette rubrique fournit des informations spécifiques AWS Transform sur le chiffrement en transit et le chiffrement au repos.

AWS Transform fournit un chiffrement par défaut pour protéger les données sensibles des clients au repos grâce à un chiffrement à l'aide de clés AWS détenues.

Types de chiffrement

Chiffrement en transit

La communication entre les clients AWS Transform et entre eux AWS Transform et ses dépendances en aval est protégée à l'aide de connexions TLS 1.2 ou supérieures.

> **Important**
>
> Lorsque vous connectez un compte de découverte, AWS Transform crée un compartiment Amazon S3 en votre nom sur ce compte. Ce compartiment n'est pas `SecureTransport` activé par défaut. Si vous souhaitez que la politique des compartiments inclue le transport sécurisé, vous devez la mettre à jour. Pour plus d'informations, consultez la section Meilleures pratiques en matière de sécurité pour Amazon S3.

Chiffrement au repos

AWS Transform stocke les données au repos à l'aide d'Amazon DynamoDB et d'Amazon Simple Storage Service (Amazon S3). Les données au repos sont cryptées par défaut à l'aide de solutions de AWS cryptage. AWS Transform chiffre vos données à l'aide de clés AWS détenues par AWS Key Management Service (AWS KMS). Vous n'avez aucune action à entreprendre pour protéger les clés AWS gérées qui chiffrent vos données. Pour plus d'informations, consultez Clés détenues par AWS dans le Guide du développeur AWS Key Management Service .

Type de données	AWS chiffrement par clé détenue	Chiffrement par clé gérée par le client (facultatif)
Données relatives au compartiment client Entrées et sorties des clients, telles que le code et la documentation stockés dans un compartiment Amazon S3	Activé	Activé
Boutique d'artefacts	Activé	Activé

Type de données	AWS chiffrement par clé détenue	Chiffrement par clé gérée par le client (facultatif)
Artefacts intermédiaires faisant partie de la transform ation du code stockés dans un compartiment S3		
Objectif du poste L'intention du client concernan t la tâche stockée dans un compartiment Amazon S3	Activé	Activé
Messages de chat Messages échangés entre le client et AWS Transform stockés dans un compartiment Amazon S3	Activé	Activé
Base de connaissances sur le chat Données indexées relatives au chat client AWS Transform et stockées sur Amazon OpenSearch et traitées via AWS Bedrock	Activé	Activé

Remarque : Le client peut enregistrer sa propre clé gérée par le client (CMK) à utiliser pour chiffrer tous les types de données ci-dessus.

Les clés gérées par le client sont des clés KMS de votre AWS compte que vous créez, possédez et gérez pour contrôler directement l'accès à vos données en contrôlant l'accès à la clé KMS. Seules les clés symétriques sont prises en charge. Pour plus d'informations sur la création de votre propre clé KMS, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

Lorsque vous utilisez une clé gérée par le client, AWS Transform utilise les autorisations KMS, permettant aux utilisateurs, rôles ou applications autorisés d'utiliser une clé KMS. Lorsqu'un AWS Transform administrateur choisit d'utiliser une clé gérée par le client pour le chiffrement lors de la configuration, une autorisation est créée pour lui. Cette autorisation permet à l'utilisateur final d'utiliser la clé de chiffrement pour le chiffrement des données au repos. Pour plus d'informations sur les autorisations, consultez Utilisation des octrois dans AWS KMS.

AWS Clés détenues (par défaut)

> **Note**
>
> AWS clés détenues : AWS Transform utilise ces clés par défaut pour crypter automatiquement les données personnelles identifiables. Vous ne pouvez pas afficher, gérer ou utiliser les clés AWS détenues, ni auditer leur utilisation. Toutefois, vous n'avez pas besoin de prendre de mesure ou de modifier les programmes pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez la section AWS relative aux clés détenues dans le Guide du développeur du service de gestion des AWS clés.

Le chiffrement des données au repos par défaut permet de réduire les frais opérationnels et la complexité liés à la protection des données sensibles. Dans le même temps, il vous permet de créer des applications sécurisées qui répondent aux exigences réglementaires et de conformité strictes en matière de chiffrement.

Bien que vous ne puissiez pas désactiver cette couche de cryptage ou sélectionner un autre type de cryptage, vous pouvez ajouter une deuxième couche de cryptage aux clés de chiffrement AWS détenues existantes en choisissant une clé gérée par le client lorsque vous créez votre transformation :

Clés gérées par le client (facultatif)

Clés gérées par le client : AWS Transform prend en charge l'utilisation d'une clé gérée par le client symétrique que vous créez, possédez et gérez pour ajouter une deuxième couche de cryptage au cryptage existant à l'aide de clés AWS détenues. Étant donné que vous avez le contrôle total de cette couche de chiffrement, vous pouvez effectuer les tâches suivantes :

- Établissement et gestion des stratégies de clé
- Établissement et gestion des politiques IAM et des octrois

- Activation et désactivation des stratégies de clé
- Rotation des matériaux de chiffrement de clé
- Ajout de balises
- Création d'alias de clé
- Rotation des matériaux de chiffrement de clé
- Ajout de balises
- Création d'alias de clé
- Planification des clés pour la suppression
- Pour plus d'informations, consultez Clé gérée par le client dans le Guide du développeur AWS Key Management Service.

> **Note**
>
> AWS Transform active automatiquement le chiffrement au repos à l'aide de clés AWS détenues pour protéger gratuitement les données personnelles identifiables. L'utilisation d'une clé gérée par le client entraîne toutefois des AWS KMS frais. Pour plus d'informations sur la tarification, consultez la rubrique AWS Key Management Service Tarification.

Pour plus d'informations AWS KMS, voir Qu'est-ce que c'est AWS Key Management Service ?

Comment ? AWS Transform utilise des subventions dans AWS Key Management Service

AWS Transform nécessite une subvention pour utiliser votre clé gérée par le client.

Lorsque vous créez un [Nom de la ressource] chiffré avec une clé gérée par le client, vous AWS Transform créez une subvention en votre nom en envoyant une CreateGrant demande à AWS Key Management Service. AWS Key Management Service Les autorisations sont utilisées pour donner AWS Transform accès à une clé KMS dans un compte client.

AWS Transform nécessite l'autorisation d'utiliser votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez des requêtes [API KMS] AWS KMS à pour vérifier que l'ID de clé KMS géré par le client symétrique saisi lors de la création de [Nom de la ressource] est valide.

- Envoyez des requêtes [KMS API] AWS KMS à pour générer des clés de données chiffrées par la clé gérée par votre client.
- Envoyez des requêtes [KMS API] AWS KMS à pour déchiffrer les clés de données cryptées afin qu'elles puissent être utilisées pour crypter vos données.

Vous pouvez révoquer l'accès à l'octroi ou supprimer l'accès du service à la clé gérée par le client à tout moment. Si vous le faites, vous AWS Transform ne pourrez accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affectera les opérations qui dépendent de ces données. Par exemple, si vous tentez d'obtenir [Nom de la ressource] à partir d'un [Nom de la ressource] chiffré auquel il n'est pas AWS Transform possible d'accéder, l'opération renverra une AccessDeniedException erreur.

Création d'une clé gérée par le client

Vous pouvez créer une clé gérée par le client symétrique à l'aide de la console AWS de gestion ou des AWS Key Management Service API.

Pour créer une clé symétrique gérée par le client, suivez les étapes de la section Création d'une clé gérée par le client symétrique dans le Guide du AWS Key Management Service développeur.

Pour utiliser votre clé gérée par le client avec vos AWS Transform ressources, les opérations d'API suivantes doivent être autorisées dans la politique relative aux clés :

kms : CreateGrant — Ajoute une autorisation à une clé gérée par le client. Accorde l'accès de contrôle à une clé KMS spécifiée, ce qui permet d'accéder aux autorisations requises par les opérations AWS Transform . Pour plus d'informations à propos de l'Utilisation des octrois, consultez le Guide du développeur AWS Key Management Service .

Cela permet AWS Transform d'effectuer les opérations suivantes :

- Appelez [KMS API (GenerateDataKeyWithoutPlainText/GenerateDatakey) pour générer une clé de données chiffrée et la stocker, car la clé de données n'est pas immédiatement utilisée pour chiffrer.
- Appelez [KMS API (Decrypt)] pour utiliser la clé de données cryptée stockée afin d'accéder aux données chiffrées.
- Configurer un principal sortant pour permettre au service de RetireGrant.
- kms : DescribeKey — Fournit les informations relatives à la clé gérée par le client pour permettre à [Nom du service] de valider la clé.

Chiffrement pour la modernisation de SQL

Au cours du processus de modernisation de SQL Server, AWS Transform créez des ressources dans votre compte, telles que des instances EC2, des clusters ECS, des images ECR et des objets S3. Vous avez la possibilité de fournir une clé gérée par le client pour crypter les données de votre compte. Vous devrez étiqueter votre clé KMS avec la clé CreatedFor et la valeur AWSTransform. Cet exemple de politique répertorie les autorisations minimales requises dans votre politique clé si vous n'avez pas de stratégie clé par défaut. Si vous avez une politique de clé par défaut, vous devez tout de même mettre à jour manuellement la clé KMS en plus de votre politique de clé par défaut pour permettre à ECS d'utiliser votre clé.

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

Cryptage pour la migration de bases de données

Pendant le processus de migration de base de données, AWS Transform utilise le service AWS de migration de base de données (DMS) pour migrer les données de votre base de données. Vous pouvez éventuellement fournir une clé gérée par le client pour chiffrer les données de votre base de données lors de la migration.

La politique suivante contient trois déclarations. La première instruction accorde les autorisations du compte root pour la AWS KMS clé. La deuxième instruction permet au rôle du connecteur de valider la clé lors de la découverte. La troisième instruction permet au rôle de connecteur d'utiliser la clé pour les opérations 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"
        }
      }
    }
  ]
```

Utilisation des clés KMS gérées par le client

Après avoir créé une clé KMS gérée par le client, un AWS Transform administrateur doit fournir la clé dans la AWS Transform console pour l'utiliser pour chiffrer les données.

Pour configurer une clé gérée par le client dans laquelle chiffrer les données AWS Transform, les administrateurs ont besoin d'autorisations d'utilisation AWS KMS.

Pour utiliser les fonctionnalités chiffrées à l'aide d'une clé gérée par le client, les utilisateurs ont besoin d'autorisations leur permettant AWS Transform d'accéder à la clé gérée par le client.

Si vous voyez une erreur liée aux autorisations KMS lors de l'utilisation AWS Transform, vous devrez probablement mettre à jour vos autorisations pour AWS Transform permettre de créer des autorisations. Pour configurer automatiquement les autorisations nécessaires, accédez à la AWS Transform console et choisissez Mettre à jour les autorisations dans la bannière en haut de la page. Pour autoriser la création AWS Transform de subventions, vous devez mettre à jour les autorisations sur la page de AWS Transform console.

Allow AWS Transform accès aux clés gérées par le client

L'exemple de déclaration de politique suivant accorde aux utilisateurs l'autorisation d'accéder aux fonctionnalités chiffrées avec une clé gérée par le client en autorisant l' AWS Transform accès à la clé. Cette politique doit être utilisée AWS Transform si un administrateur a configuré une clé gérée par le client pour le chiffrement.

> **Note**
>
> Ces informations ne s'appliquent pas au flux de travail de déploiement de la modernisation de SQL Server à l'aide de 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 amélioration du service

Afin de AWS Transform fournir les informations les plus pertinentes, nous pouvons utiliser certains contenus AWS Transform, tels que les questions que vous posez AWS Transform et leurs réponses,

afin d'améliorer le service. Cette page explique le contenu que nous utilisons et comment nous désinscrire.

AWS Transform contenu utilisé pour améliorer le service

Nous pouvons utiliser certains contenus AWS Transform pour améliorer le service. AWS Transform peuvent utiliser ce contenu, par exemple, pour fournir de meilleures réponses aux questions courantes, résoudre des problèmes AWS Transform opérationnels, pour le débogage ou pour la formation de modèles.

Le contenu AWS susceptible d'être utilisé pour améliorer le service inclut, par exemple, vos questions, les réponses et le code AWS Transform généré. AWS Transform

Comment se désinscrire

La manière dont vous choisissez de ne pas AWS Transform utiliser le contenu pour améliorer le service dépend de l'environnement dans lequel vous utilisez AWS Transform.

Pour AWS Transform configurer une politique de désactivation des services d'IA dans AWS Organizations. Pour plus d’informations, consultez Politiques de désactivation des services IA dans le Guide de l’utilisateur AWS Organizations .

Pour refuser le partage de votre contenu dans l'Visual StudioIDE, procédez comme suit.

Accédez à Outils -> Options -> AWS Toolkit -> Amazon Q

Définissez Partager le contenu Amazon Q avec AWS sur Vrai ou Faux.

Pour ne pas partager vos données de télémétrie dans la AWS boîte à outils pourVisual Studio, procédez comme suit :

1. Sous Outils, choisissez Options.
2. Dans le volet Options, choisissez AWS Toolkit, puis Général.
3. Désélectionnez Autoriser la AWS boîte à outils pour collecter des informations d'utilisation.

Gestion des identités et des accès pour AWS Transformation

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM

contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources AWS Transform. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes AWS Transformez l'identité et l'accès)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment ? AWS Transform fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Identity-based exemples de politiques pour AWS Transformation)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations

sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle IAM (console) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités).

Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques intégrées qui se trouvent dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment ? AWS Transform fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Transform, découvrez quelles fonctionnalités IAM peuvent être utilisées avec AWS Transform.

Fonctionnalité IAM	AWS Transformez le support
Identity-based politiques	Oui
Resource-based politiques	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Service-linked rôles	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS Transform et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Identity-based politiques pour AWS Transformation

Prend en charge les politiques basées sur l'identité : oui

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. Ces politiques

contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Identity-based exemples de politiques pour AWS Transformation

Pour consulter des exemples de politiques basées sur l'identité AWS Transform, consultez. Identity-based exemples de politiques pour AWS Transformation

Resource-based politiques au sein de AWS Transformation

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour AWS Transformation

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions de AWS transformation, consultez la section Actions, ressources et clés de condition pour AWS Transform dans la référence d'autorisation de service.

Pour consulter la liste des actions pour AWS Transform custom, voir Actions, ressources et clés de condition pour AWS Transform custom dans la référence d'autorisation de service.

Les actions de politique dans AWS Transform utilisent le préfixe suivant avant l'action :

```
transform
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "transform:action1",
      "transform:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité AWS Transform, consultez. Identity-based exemples de politiques pour AWS Transformation

Ressources politiques pour AWS Transformation

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les

actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources AWS Transform et de leurs ARN, ainsi que les actions à l'aide desquelles vous pouvez spécifier l'ARN de chaque ressource, consultez la section Actions, ressources et clés de condition pour AWS Transform dans la référence d'autorisation de service.

Pour consulter la liste des types de ressources et leurs ARN, ainsi que les actions avec lesquelles vous pouvez spécifier l'ARN de chaque ressource pour AWS Transform custom, voir Actions, ressources et clés de condition pour AWS Transform custom dans la référence d'autorisation de service.

Pour consulter des exemples de politiques basées sur l'identité AWS Transform, consultez. Identity-based exemples de politiques pour AWS Transformation

Clés de conditions de politique pour AWS Transformation

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition de AWS transformation et les actions et ressources avec lesquelles vous pouvez utiliser une clé de condition, consultez la section Actions, ressources et clés de condition pour AWS Transform dans la référence d'autorisation de service.

Pour consulter la liste des clés de condition et les actions et ressources avec lesquelles vous pouvez utiliser une clé de condition pour AWS Transform custom, voir Actions, ressources et clés de condition pour AWS Transform custom dans la référence d'autorisation de service.

Pour consulter des exemples de politiques basées sur l'identité AWS Transform, consultez. Identity-based exemples de politiques pour AWS Transformation

ACL dans AWS Transformation

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec AWS Transformation

Prend en charge ABAC (identifications dans les politiques) : partiellement

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AWS Transformation

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au

lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Cross-service autorisations principales pour AWS Transformation

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour AWS Transformation

Prend en charge les rôles de service : oui

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut interrompre la fonctionnalité de AWS transformation. Modifiez les rôles de service uniquement lorsque AWS Transform fournit des instructions à cet effet.

Service-linked rôles pour AWS Transformation

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre fichier Compte AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés au service AWS Transform, consultez. Utilisation de rôles liés à un service pour AWS Transform

Identity-based exemples de politiques pour AWS Transformation

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources AWS Transform. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS Transform, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition pour AWS Transform dans la référence d'autorisation de service.

Rubriques

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer, accéder ou supprimer des ressources AWS Transform dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à

vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de AWS Transformer la console

Pour accéder à la console AWS Transform, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des ressources AWS Transform de votre Compte AWS. Si vous créez une politique basée sur l'identité

qui est plus restrictive que l’ensemble minimum d’autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l’accès à uniquement aux actions qui correspondent à l’opération d’API qu’ils tentent d’effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d’afficher les politiques en ligne et gérées attachées à leur identité d’utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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": "*"
```

```
        }
    ]
}
```

Autoriser les administrateurs à accepter une demande de connecteur provenant du compte avec AWS Transformation

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-*"
        }
    ]
}
```

Permettre aux administrateurs d'attribuer des utilisateurs IAM Identity Center existants et de créer de nouveaux utilisateurs IAM Identity Center auxquels attribuer AWS Transformation

La politique suivante accorde les autorisations dont un administrateur a besoin pour gérer les utilisateurs et les groupes IAM Identity Center dans la console AWS Transform. Grâce à cette politique, un administrateur peut attribuer et supprimer des utilisateurs et des groupes, afficher les noms d'affichage, créer de nouveaux utilisateurs IAM Identity Center, gérer les attributions des applications et configurer les paramètres de session des applications.

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

Autoriser les administrateurs à activer AWS Transformation

La politique suivante accorde les autorisations dont un administrateur a besoin pour activer et administrer AWS Transform via la AWS console. Cela inclut la gestion des profils, la configuration des agents et la gestion des connecteurs. Cette politique s'adresse uniquement aux administrateurs et doit s'appliquer aux personnes de confiance associées à votre compte.

```
{
  "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": "*"
    }
  ]
}
```

Autoriser les utilisateurs à accéder AWS Transformez avec les informations d'identification IAM

La politique suivante accorde à un IAM principal un accès à l'application Web et aux API AWS Transform à l'aide des informations d'identification IAM. Cette politique est requise pour IAM-only l'accès et pour l'accès IAM activé conjointement avec un fournisseur d'identité.

Remplacez *`regionaccount-id`*, et *`profile-id`* par vos valeurs. Vous trouverez l'ID du profil dans la console AWS Transform sous Paramètres.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccess",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/profile-id"
    }
  ]
}
```

Pour autoriser l'accès à tous les profils d'un compte, utilisez un caractère générique comme identifiant de profil :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowTransformAccessAllProfiles",
      "Effect": "Allow",
      "Action": "transform:AccessTransformProfile",
      "Resource": "arn:aws:transform:region:account-id:profile/*"
    }
  ]
}
```

> **Note**
>
> L'`transform:AccessTransformProfile`action donne accès à AWS Transform uniquement. Les actions au sein des espaces de travail sont contrôlées par les rôles de l'espace de travail AWS Transform (administrateur, contributeur, approbateur Read-only), et non par les politiques IAM. Les rôles de l'espace de travail déterminent ce qu'un utilisateur peut faire, par exemple créer des emplois, gérer des collaborateurs ou approuver des tâches.

Résolution des problèmes AWS Transformez l'identité et l'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de AWS Transform et d'IAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans AWS Transformation

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `AWS Transform:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: AWS
 Transform:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `AWS Transform:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à AWS Transform.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans AWS Transform. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mon AWS Transformez les ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si AWS Transform prend en charge ces fonctionnalités, consultezComment ? AWS Transform fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.

- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de rôles liés à un service pour AWS Transform

AWS Transform utilise des Gestion des identités et des accès AWS rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Transform Service-linked les rôles sont prédéfinis par AWS Transform et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Utilisation de rôles liés à un service pour AWS Transform

AWS Transform utilise des Gestion des identités et des accès AWS rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Transform Service-linked les rôles sont prédéfinis par AWS Transform et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Transform car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Transform définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Transform peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS Transform ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la Service-linked colonne des rôles. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Service-linked autorisations de rôle pour AWS Transform

AWS Transform utilise le rôle lié au service nommé AWSServiceRoleForAWSTransform— Ce Service-Linked rôle permet à AWS Transform de fournir des informations d'utilisation.

Le rôle AWSServiceRoleForAWSTransform lié à un service fait confiance aux services suivants pour assumer le rôle :

- `transform.amazonaws.com`

La politique d'autorisations de rôle nommée AWSServiceRoleForAWSTransform AWS Transform permet d'effectuer les actions suivantes sur les ressources spécifiées :

- surveillance des nuages : PutMetricData
  - Envoyer des métriques personnalisées à CloudWatch pour les AWS Transform opérations
  - Suivez la progression de la transformation, les taux de réussite et les indicateurs de performance
  - Activez la surveillance et les alertes sur les flux de travail de transformation
- SSO : DescribeApplication
  - Afficher les détails d'une application spécifique dans Identity Center
  - Obtenez les métadonnées de l'application telles que le nom, la description, le statut et la configuration
- SSO : GetApplicationAssignmentConfiguration
  - Récupérer les paramètres de configuration des affectations pour une application
  - Découvrez comment users/groups sont configurés pour être affectés à l'application
- SSO : ListApplicationAssignmentsForPrincipal
  - Répertorier toutes les applications attribuées à un utilisateur ou à un groupe spécifique (principal)
  - Afficher les applications auxquelles une identité donnée a accès
- Permet le déchiffrement des KMS-encrypted données en cas d'accès via IAM Identity Center. Fonctionne uniquement lorsque le contexte de chiffrement contient un ARN d'instance IAM Identity Center valide et doit être accessible via les points de terminaison du service IAM Identity Center.
- Permet le déchiffrement des KMS-encrypted données en cas d'accès via Identity Store. Fonctionne uniquement lorsque le contexte de chiffrement contient un ARN Identity Store valide et doit être accessible via les points de terminaison du service Identity Store.
- responsable des secrets : GetSecretValue
  - Accédez aux secrets AWS Transform liés aux services utilisés pour stocker les secrets des clients pour les fournisseurs d'identité externes
  - Ressource : arn:aws:secretsmanager :*:*:secret:transform-preprod ! *
  - Condition : Doit appartenir au service transform-preprod et être accessible depuis le même compte
- support :CreateCase, support :DescribeCases, support :DescribeCommunications, support :AddCommunicationToCase, support : ResolveCase

- Créez et gérez des dossiers de support premium à partir de l'application AWS Transform Web
- Afficher les détails du dossier et les communications
- Ajoutez des communications et résolvez les demandes d'assistance

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez les autorisations relatives aux Service-linked rôles dans le guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Transform

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un profil pour AWS Transform dans le Console de gestion AWS, AWS Transform crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous mettez à jour les paramètres, le rôle lié au service est à nouveau AWS Transform créé pour vous.

Vous pouvez également utiliser la console IAM ou la AWS CLI pour créer un rôle lié à un service avec le nom du `transform.amazonaws.com` service. Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour AWS Transform

AWS Transform ne vous permet pas de modifier le rôle AWSServiceRoleForAWSTransform lié au service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Transform

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le AWS Transform service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForAWSTransform service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour AWS Transform Rôles liés à un service

AWS Transform ne prend pas en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Vous pouvez utiliser le AWSServiceRoleForAWSTransform rôle dans les régions suivantes. Pour plus d'informations, consultez Régions et points de terminaison AWS.

Nom de la région	Identité de la région	Support dans AWS Transform
USA Est (Virginie du Nord)	us-east-1	Oui
Europe (Francfort)	eu-central-1	Oui

Utilisation de rôles liés à un service pour AWS Transformer sur mesure

AWS Transform Custom utilise le rôle lié au service nommé AWSServiceRoleForAWSTransformCustompour publier des statistiques et des journaux sur votre compte en votre nom. Ces indicateurs vous permettent de surveiller le nombre de transformations, les latences et les codes d'état directement dans vos tableaux de bord. Les journaux fournissent une visibilité sur les problèmes rencontrés lors des transformations.

Ce rôle lié au service est prédéfini par AWS Transform Custom et inclut uniquement les autorisations dont le service a besoin. Il n'est pas nécessaire d'ajouter manuellement des autorisations, et le rôle ne peut être assumé que par AWS Transform Custom. Pour obtenir des informations générales sur les rôles liés à un service, consultez la section Utilisation des rôles liés à un service dans le guide de l'utilisateur IAM.

Service-linked autorisations de rôle pour AWS Transformer sur mesure

Le rôle AWSServiceRoleForAWSTransformCustom lié à un service fait confiance aux services suivants pour assumer le rôle :

- `transform-custom.amazonaws.com`

La politique d'autorisation de rôle nommée AWSServiceRoleForAWSTransformCustom permet à AWS Transform Custom d'effectuer les actions suivantes sur les ressources spécifiées :

- `cloudwatch:PutMetricData`sur toutes les AWS ressources
  - Publier les métriques opérationnelles sous l'espace de `AWS/TransformCustom` noms
  - Suivez le nombre de transformations, les latences et les codes d'état
  - Délimité à l'espace de `AWS/TransformCustom` noms via la clé de condition `cloudwatch:namespace`
- `logs:CreateLogGroup`et `logs:PutRetentionPolicy` sur le groupe de `/aws/TransformCustom` logs
  - Création du groupe de CloudWatch journaux pour publier les journaux de transformation
  - Définissez des politiques de conservation des journaux sur le groupe de journaux
  - Limité par `arn:aws:logs:*:*:log-group:/aws/TransformCustom` une `aws:ResourceAccount` condition garantissant l'accès uniquement à votre compte
- `logs:CreateLogStream`et `logs:PutLogEvents` sur les flux de journaux au sein du groupe de `/aws/TransformCustom` journaux
  - Création de flux de journaux et publication d'événements de journal pour les opérations de transformation
  - Limité par `arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*` une `aws:ResourceAccount` condition garantissant l'accès uniquement à votre compte

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez les autorisations relatives aux Service-linked rôles dans le guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Transformer sur mesure

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous exécutez une transformation à l'aide de la CLI AWS Transform Custom, AWS Transform Custom crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous exécutez une transformation à l'aide de la CLI AWS Transform Custom, AWS Transform Custom crée à nouveau le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec le AWSServiceRoleForAWSTransformCustomcas d'utilisation. Dans l'API AWS CLI ou dans l' AWS API, créez un rôle lié à un service avec le nom du `transform-custom.amazonaws.com` service. Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour AWS Transformer sur mesure

AWS Transform Custom ne vous permet pas de modifier le rôle AWSServiceRoleForAWSTransformCustom lié au service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Transformer sur mesure

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement.

Le rôle AWSServiceRoleForAWSTransformCustom lié au service ne crée pas de ressources persistantes dans votre compte. Vous pouvez le supprimer directement sans avoir à nettoyer les ressources.

Si vous supprimez ce rôle et que vous exécutez ultérieurement une transformation à l'aide de la CLI AWS Transform Custom, le rôle lié au service est automatiquement recréé.

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForAWSTransformCustom service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour AWS Transformez les rôles personnalisés liés à un service

AWS Transform Custom prend en charge l'utilisation de rôles liés à un service dans toutes les régions où AWS Transform Custom est disponible. Pour obtenir la liste des régions prises en charge, consultez la section Régions prises en charge.

AWS politiques gérées pour AWS Transformation

Une politique AWS gérée est une politique autonome qui est créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou que de nouvelles opérations d'API deviennent disponibles pour des services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS Transformez les mises à jour pour AWS stratégies gérées

Consultez les détails des mises à jour des politiques AWS gérées pour AWS Transform depuis le 1er mars 2021.

Modifier	Description	Date
AWSTransformInfrastructureExecutorAccessBatch— Politique mise à jour	Autorisations AWS Lambda restreintes à une liste d'autorisations de fonctions explicites, ajout de l'accès en écriture à Amazon S3 pour la sortie par lots par lots, élargissement de la portée des ressources Amazon EventBridge Scheduler pour les déploiements multipiles CloudFormation et ajout de la prise en charge des variantes d'alias de clé régionales. AWS Key Management Service	27 juillet 2026
AWSTransformInfrastructureExecutorAccessEC2— Politique mise à jour	Élargissement CloudFormation de la portée d'Amazon EventBridge Scheduler et Gestion des identités et des accès AWS PassRole des ressources pour les déploiements multistack, amélioration de la visibilité de l'infrastructure des agents de sécurité et prise en charge des variantes d'alias clés régionales. AWS Key Management Service	27 juillet 2026
AWSTransformSecurityAgentExecutorAccess— Politique mise à jour	Ajout d' CloudFormation autorisations permettant de découvrir et de décrire la pile d'infrastructure de Security Agent, et migration du préfixe du compartiment Amazon S3 de `kct-security-agent`	27 juillet 2026

Modifier	Description	Date
	`-*` vers. `atx-security-agent-*`	
AWSTransformInfrastructureExecutorAccessBatch : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui accorde les autorisations nécessaires pour exécuter les évaluations et les transformations de la modernisation continue de AWS Transform à l'aide de AWS Batch, y compris le téléchargement du code source, la récupération des résultats, la surveillance de l'état des tâches Batch, la lecture des journaux et la gestion des calendriers de transformation.	20 juillet 2026
AWSTransformInfrastructureExecutorAccessEC2 : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui accorde les autorisations nécessaires pour exécuter les évaluations et les transformations de la modernisation continue de AWS Transform à l'aide d'Amazon EC2, notamment le téléchargement du code source, la récupération des résultats, le suivi de l'état des tâches et la gestion des calendriers de transformation.	20 juillet 2026

Modifier	Description	Date
AWSTransformSecurityAgentExecutorAccess : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui accorde à AWS Transform Continuous Modernization les autorisations nécessaires pour invoquer le service AWS Security Agent afin d'automatiser les révisions de sécurité du code et la correction, y compris le téléchargement des artefacts de numérisation et la récupération des résultats.	30 juin 2026
AWSServiceRoleForAWSTransformCustom— Politique mise à jour	Ajout d'autorisations relatives aux CloudWatch journaux pour permettre à AWS Transform custom de publier des journaux dans le `/aws/TransformCustom` groupe de journaux de votre compte.	5 mai 2026
AWSTransformCustomExecuteTransformations— Politique mise à jour	Ajout de l'autorisation de créer le rôle personnalisé lié au service AWS Transform (`AWSServiceRoleForAWSTransformCustom`) afin de permettre l'émission de CloudWatch métriques vers les comptes clients.	27 avril 2026

Modifier	Description	Date
AWSTransformCustomManageTransformations— Politique mise à jour	Ajout de l'autorisation de créer le rôle personnalisé lié au service AWS Transform (`AWSServiceRoleForAWSTransformCustom`) afin de permettre l'émission de CloudWatch métriques vers les comptes clients.	27 avril 2026
AWSTransformCustomFullAccess— Politique mise à jour	Ajout de l'autorisation de créer le rôle personnalisé lié au service AWS Transform (`AWSServiceRoleForAWSTransformCustom`) afin de permettre l'émission de CloudWatch métriques vers les comptes clients.	7 avril 2026
AWSServiceRoleForAWSTransformCustom : nouvelle politique	Ajout d'une nouvelle politique AWS gérée pour le rôle personnalisé lié aux services AWS Transform. Cette politique permet à AWS Transform custom de publier CloudWatch des statistiques sur votre compte.	23 mars 2026
DBModProvisioningAndMigration : nouvelle politique	Cette politique confère des fonctionnalités de provision nement et de migration des bases de données.	24 mars 2026

Modifier	Description	Date
DBModDiscoveryAndAssessment : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui fournit des fonctionnalités complètes de découverte et d'évaluation de la modernisation des bases de données.	24 mars 2026
AWSTransformCustomFullAccess : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui fournit un accès complet à AWS Transform custom.	5 décembre 2025
AWSTransformCustomExecuteTransformations : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui permet d'exécuter des transformations dans AWS Transform custom.	5 décembre 2025
AWSTransformCustomManageTransformations : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui permet de créer, de mettre à jour, de lire et de supprimer des ressources de transformation dans AWS Transform custom, ainsi que d'exécuter des transformations.	5 décembre 2025

Modifier	Description	Date
AWSServiceRoleForAWSTransform— Politique mise à jour	Ajout d'autorisations pour accéder au secret lié au service AWS Transform utilisé pour stocker le secret client pour les fournisseurs d'identité externes. Ajout d'autorisations pour créer un dossier d'assistance premium à partir de l'application Web AWS Transform.	1er décembre 2025
AWSTransformApplicationECSDeploymentPolicy— Politique mise à jour	Ajout d'autorisations d'inspection des rôles IAM, de création de rôles liés aux services ECS et d'autorisations KMS pour la prise en charge du chiffrement ECR.	22 novembre 2025
AWSTransformApplicationDeploymentPolicy— Politique mise à jour	Ajout d'autorisations réseau EC2, d'autorisations d'inspection des rôles IAM, d'autorisations de liste de compartiments S3 et de la prise en charge du chiffrement KMS pour des capacités de déploiement améliorées.	22 novembre 2025
AWSServiceRoleForAWSTransform— Politique mise à jour	Ajout de la prise en charge des clés gérées par le client dans IAM Identity Center.	17 septembre 2025

Modifier	Description	Date
AWSTransformApplicationDeploymentPolicy : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui permet à AWS Transform de déployer des applications .NET transformées en créant et en gérant des instances Amazon EC2, des CloudFormation piles et des ressources associées.	28 août 2025
AWSServiceRoleForAWSTransform— Politique mise à jour	Ajout d'une nouvelle politique.	15 mai 2025

AWS stratégie gérée : AWSServiceRoleForAWSTransform

Cette politique est associée au rôle AWSServiceRoleForAWSTransform lié aux services (SLR).

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez AWSServiceRoleForAWSTransform le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSServiceRoleForAWSTransformCustom

Cette politique est associée au rôle AWSServiceRoleForAWSTransformCustom lié aux services (SLR). Ce rôle permet à AWS Transform custom de publier CloudWatch des statistiques et des journaux sur votre compte en votre nom.

Description

Cette politique inclut les autorisations suivantes :

- Amazon CloudWatch — Permet de publier des métriques CloudWatch dans l'espace de `AWS/TransformCustom` noms. Cela permet de surveiller le nombre de transformations, les latences et les codes d'état dans vos CloudWatch tableaux de bord.
- Amazon CloudWatch Logs : permet de créer des groupes de journaux, des flux de journaux, de définir des politiques de conservation et de publier des événements de `/aws/TransformCustom`

journal dans le groupe de journaux. Cela donne une visibilité sur les problèmes rencontrés lors des transformations.

AWS stratégie gérée : AWSTransformApplicationDeploymentPolicy

Cette politique permet à AWS Transform de déployer des applications .NET transformées en créant et en gérant des instances Amazon EC2, des CloudFormation piles et des ressources associées.

Description

Cette politique inclut les autorisations suivantes :

- CloudFormation— Permet de créer, de mettre à jour, de supprimer et de décrire des CloudFormation piles dont le nom commence par AWSTransform. Les opérations de stack sont limitées aux ressources étiquetées avec CreatedBy : AWSTransform et limitées au même compte. AWS
- Amazon EC2 — Permet de décrire les VPC, les sous-réseaux, les groupes de sécurité, les images, les instances, les tables de routage et les passerelles Internet. Permet d'exécuter, de démarrer, d'arrêter, de terminer et de modifier des instances EC2, mais uniquement lorsqu'elles sont appelées via. CloudFormation La création de balises est limitée à des clés de balise autorisées spécifiques et uniquement pendant CloudFormation les opérations.
- Gestion des identités et des accès AWS (IAM) : permet d'obtenir et de transmettre des rôles IAM spécifiques pour les instances de déploiement d'AWSTransform. Inclut des autorisations pour inspecter les politiques relatives aux rôles et les pièces jointes. L'accès est limité au même AWS compte.
- Amazon EC2 Systems Manager (SSM) : permet de récupérer les paramètres de l'AMI Amazon Linux à partir du magasin de paramètres AWS géré et d'envoyer des commandes aux instances. AWSTransform-tagged
- Amazon S3 : permet de gérer les objets dans les compartiments de déploiement d'AWSTransform, notamment en répertoriant les compartiments et en obtenant l'emplacement des compartiments sur le même compte. AWS
- AWS Key Management Service (KMS) : autorise les opérations de chiffrement et de déchiffrement à l'aide de clés KMS balisées pour AWSTransform, avec des restrictions quant à l'utilisation des services S3 et EC2.

La politique met en œuvre l'accès au moindre privilège via des autorisations au niveau des ressources, des conditions basées sur des balises, des restrictions de contrôle des services, des restrictions au niveau du compte et des instructions de refus explicites pour empêcher les modifications non autorisées des balises en dehors des opérations. `aws:CalledVia` CloudFormation

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez AWSTransformApplicationDeploymentPolicy le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSTransformApplicationECSDeploymentPolicy

Cette politique permet à AWS Transform de déployer des applications transformées sur Amazon ECS en créant et en gérant des clusters, des services, des tâches et des ressources associées ECS.

Description

Cette politique inclut les autorisations suivantes :

- CloudFormation— Permet de créer, de mettre à jour, de supprimer et de décrire des CloudFormation piles dont le nom commence par AWSTransform. Les opérations de stack sont limitées aux ressources étiquetées avec CreatedBy : AWSTransform et limitées au même compte. AWS
- Amazon ECS : permet de créer, de mettre à jour et de supprimer des clusters, des services et des définitions de tâches ECS. Permet d'exécuter des tâches, de répertorier les tâches et de décrire leur état. Toutes les opérations sont limitées aux ressources dont le nom commence par AWSTransform et est marqué par : AWSTransform. CreatedBy
- Gestion des identités et des accès AWS (IAM) — Permet d'obtenir et de transmettre des rôles IAM spécifiques pour les tâches ECS (AWSTransform-Deploy-ECS-Task-Role et AWSTransform-Deploy-ECS-Execution-Role). Inclut des autorisations pour inspecter les politiques relatives aux rôles et créer le rôle lié au service ECS si nécessaire.
- Amazon CloudWatch Logs : permet de créer, de supprimer et de gérer des groupes de journaux dont le nom commence par/aws/ecs/AWSTransform. Permet de récupérer les événements du journal pour dépanner les applications déployées.
- Amazon ECR — Permet de créer des référentiels de conteneurs dont les noms commencent par awstransform pour stocker les images des conteneurs d'applications.

- AWS Key Management Service (KMS) : permet de créer des autorisations et de générer des clés de données pour le chiffrement ECR lors de l'utilisation de clés KMS gérées par le client.

La politique met en œuvre l'accès au moindre privilège via des autorisations au niveau des ressources, des conditions basées sur des balises et des restrictions au niveau du compte afin de garantir que les opérations sont limitées aux ressources du même compte. AWSTransform-managed AWS

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez AWSTransformApplicationECSDeploymentPolicy le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSTransformCustomFullAccess

Cette politique fournit un accès complet à AWS Transform custom.

Description

Cette politique inclut les autorisations suivantes :

- AWS Transform Custom : autorise toutes les actions sur toutes les ressources personnalisées AWS Transform. Cela fournit un accès administratif complet au service.
- Gestion des identités et des accès AWS (IAM) : permet de créer le rôle personnalisé lié à un service AWS Transform (). `AWSServiceRoleForAWSTransformCustom` Ce rôle est requis pour que AWS Transform custom émette CloudWatch des statistiques et des journaux sur votre compte. L'autorisation est limitée pour autoriser uniquement la création de ce rôle spécifique lié à un service.

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez AWSTransformCustomFullAccess le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSTransformCustomExecuteTransformations

Cette politique permet d'exécuter des transformations dans AWS Transform custom.

Description

Cette politique inclut les autorisations suivantes :

- AWS Transform Custom : permet de diffuser des conversations, d'exécuter des transformations et de gérer des campagnes. Inclut des autorisations pour obtenir les détails des campagnes, mettre à jour l'état du référentiel des campagnes et mettre à jour les campagnes.
- Gestion des identités et des accès AWS (IAM) : permet de créer le rôle personnalisé lié à un service AWS Transform (). `AWSServiceRoleForAWSTransformCustom` Ce rôle est requis pour que AWS Transform custom émette CloudWatch des statistiques et des journaux sur votre compte. L'autorisation est limitée pour autoriser uniquement la création de ce rôle spécifique lié à un service.

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez AWSTransformCustomExecuteTransformations le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSTransformCustomManageTransformations

Cette politique permet de créer, de mettre à jour, de lire et de supprimer des ressources de transformation dans AWS Transform custom, ainsi que d'exécuter des transformations.

Description

Cette politique inclut les autorisations suivantes :

- AWS Transform Custom : permet une gestion complète des ressources de transformation, notamment le streaming des conversations, l'exécution de transformations et la gestion des packages de transformation. Permet de créer, d'obtenir et de supprimer les URL des packages de transformation et de terminer les téléchargements des packages.
- Gestion des connaissances : permet de répertorier, d'obtenir, de supprimer et de mettre à jour les éléments de connaissances, ainsi que leur configuration et leur statut.
- Gestion des campagnes : permet d'obtenir les détails des campagnes, de mettre à jour l'état du référentiel des campagnes et de mettre à jour les campagnes.
- Balisage des ressources : permet de répertorier, d'ajouter et de supprimer des balises pour les ressources personnalisées AWS Transform.
- Gestion des identités et des accès AWS (IAM) : permet de créer le rôle personnalisé lié à un service AWS Transform (). `AWSServiceRoleForAWSTransformCustom` Ce rôle est requis pour que AWS Transform custom émette CloudWatch des statistiques et des journaux sur votre compte. L'autorisation est limitée pour autoriser uniquement la création de ce rôle spécifique lié à un service.

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez AWSTransformCustomManageTransformations le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSTransformInfrastructureExecutorAccessBatch

Cette politique accorde les autorisations nécessaires pour exécuter les évaluations et les transformations de AWS Transform Continuous Modernization à l'aide de AWS Batch. Associez cette politique à un rôle IAM de votre compte. L'interface de ligne de commande et l'agent AWS Transform Continuous Modernization assument ce rôle pour télécharger le code source, récupérer les résultats, surveiller l'état des tâches par lots, lire les journaux et gérer les calendriers de transformation.

Description

Cette politique inclut les autorisations suivantes :

- AWS Lambda : permet d'invoquer et de récupérer la configuration de fonctions Lambda `atx` préfixées spécifiques qui orchestrent le flux de travail de transformation, y compris les fonctions de déclenchement des tâches, de récupération de statut et de liste des tâches.
- Amazon S3 : permet de charger le code source dans des `atx-source-code-*` compartiments, de télécharger les résultats de transformation depuis `atx-custom-output-*` et des compartiments, et d'écrire la `atx-ct-output-*` sortie du sidecar par lots dans des compartiments. `atx-custom-output-*`
- AWS Key Management Service (KMS) — Permet le chiffrement et le déchiffrement des données à l'aide de la clé de chiffrement AWS Transform (`alias/atx-encryption-key`).
- Amazon CloudWatch Logs : permet de lire les événements du journal des tâches par lots et des journaux d'exécution Lambda à des fins de surveillance et de débogage des transformations.
- Amazon CloudWatch — Permet d'obtenir et de répertorier le tableau de bord AWS Transform CLI pour une visibilité opérationnelle.
- AWS Batch : permet de décrire et de répertorier les environnements de calcul, les files d'attente des tâches, les définitions des tâches et l'état des tâches.
- CloudFormation— Permet de décrire et de répertorier les piles d'infrastructure AWS Transform, y compris la pile Security Agent, pour vérifier l'état du déploiement.
- API de balisage des groupes de ressources : permet de récupérer des ressources balisées pour découvrir l'infrastructure AWS Transform de votre compte.

- AWS Secrets Manager— Permet de récupérer et de décrire les secrets de AWS transformation stockés sous le `atx/` préfixe.
- Amazon EventBridge Scheduler : permet de gérer les tâches de transformation planifiées au sein du groupe `atx-ct` de planification.
- Amazon EC2 — Permet de décrire la configuration du VPC, du sous-réseau, du groupe de sécurité, de la table de routage et de la passerelle NAT pour la mise en réseau d'un environnement de calcul par lots.
- Gestion des identités et des accès AWS (IAM) — Permet de lire les configurations de rôles avec `ATX` préfixe et avec `Atx` préfixe pour valider la configuration de l'infrastructure, et de les transmettre à Amazon EventBridge Scheduler afin qu'il puisse invoquer des tâches planifiées. `AtxSchedulerInvocationRole`

La politique met en œuvre l'accès au moindre privilège via des autorisations au niveau des ressources, des conditions basées sur des balises, la `aws:ResourceAccount` condition et des `iam:PassedToService` conditions étendues au service afin de garantir que les opérations sont limitées aux ressources Transform au sein d'un même compte. AWS AWS

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez AWSTransformInfrastructureExecutorAccessBatch le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSTransformInfrastructureExecutorAccessEC2

Cette politique accorde les autorisations nécessaires pour exécuter les évaluations et les transformations de AWS Transform Continuous Modernization à l'aide d'Amazon EC2. Associez cette politique à un rôle IAM de votre compte. L'interface de ligne de commande et l'agent AWS Transform Continuous Modernization assument ce rôle pour télécharger le code source, récupérer les résultats, surveiller l'état des tâches et gérer les calendriers de transformation.

Description

Cette politique inclut les autorisations suivantes :

- CloudFormation— Permet de décrire les piles d'infrastructure AWS Transform (y compris la pile Security Agent), les événements des piles, les ressources des piles et l'état de détection des dérivations, de répertorier les piles et de valider les CloudFormation modèles avant le déploiement.

- Amazon EC2 — Permet de décrire des instances, des AMI, des VPC, des sous-réseaux, des groupes de sécurité, des paires de clés, des tables de routage, des passerelles NAT et des passerelles Internet. Permet de démarrer et d'arrêter les instances EC2 balisées avec`atx-remote-infra: true`.
- Amazon EC2 Systems Manager (SSM) : permet de surveiller l'état d'exécution des commandes et d'exécuter des commandes et des sessions sur des AWS Transform-tagged instances, y compris l'exécution du `AWS-RunShellScript` document.
- Amazon S3 — Permet de gérer le code source et les artefacts de sortie dans les compartiments AWS Transform, notamment en récupérant, en plaçant et en supprimant des objets et en répertoriant les compartiments.
- AWS Key Management Service (KMS) — Permet le chiffrement et le déchiffrement des données à l'aide de la clé de chiffrement AWS Transform (`alias/atx-encryption-key`).
- AWS Secrets Manager— Permet de récupérer et de décrire les secrets de transformation, tels que les informations d'identification du référentiel, stockés sous le `atx/` préfixe.
- Amazon EventBridge Scheduler : permet de gérer les tâches de transformation planifiées au sein du groupe `atx-ct` de planification.
- API de balisage des groupes de ressources : permet de récupérer des ressources balisées pour découvrir l'infrastructure AWS Transform de votre compte.
- Gestion des identités et des accès AWS (IAM) — Permet de transmettre le `atx-transform-role*` rôle à Amazon EC2 et `AtxSchedulerInvocationRole` à Amazon EventBridge Scheduler, et de lire la configuration du rôle et du profil d'instance pour les instances EC2.

La politique met en œuvre l'accès au moindre privilège via des autorisations au niveau des ressources, des conditions basées sur des balises, la `aws:ResourceAccount` condition et des `iam:PassedToService` conditions étendues au service afin de garantir que les opérations sont limitées aux ressources Transform au sein d'un même compte. AWS AWS

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez AWSTransformInfrastructureExecutorAccessEC2 le AWS Managed Policy Reference Guide.

AWS stratégie gérée : AWSTransformSecurityAgentExecutorAccess

Cette politique accorde à AWS Transform Continuous Modernization les autorisations nécessaires pour appeler le service AWS Security Agent afin d'automatiser les révisions de sécurité du code

et la correction. Associez cette politique à un rôle IAM dans votre compte que la CLI et l'agent de AWS Transform Continuous Modernization assument pour charger les artefacts de numérisation et récupérer les résultats.

Description

Cette politique inclut les autorisations suivantes :

- AWS Agent de sécurité : permet de répertorier les espaces réservés aux agents, de créer des révisions de code, de démarrer des tâches de révision de code, de répertorier et de récupérer les résultats, et de démarrer la correction du code. Ces actions sont limitées aux espaces d'agent de votre compte.
- Amazon S3 : permet de télécharger les résultats et les résultats de l'analyse depuis le `atx-security-agent-*` compartiment, et de télécharger le code source pour l'analyse de sécurité vers le `security-scans/*` préfixe de ce compartiment.
- Gestion des identités et des accès AWS (IAM) — Permet de transmettre le `security-agent-*` rôle au service AWS Security Agent afin qu'il puisse effectuer l'analyse.
- CloudFormation— Permet de `AtxSecurityAgentStack-*` répertorier les piles dans le compte et de les décrire pour découvrir et surveiller l'état du déploiement de l'infrastructure Security Agent.

La politique met en œuvre l'accès au moindre privilège via des autorisations au niveau des ressources, des préfixes de compartiment et de clé S3, les `s3:ResourceAccount` conditions `aws:ResourceAccount` et, ainsi qu'une `iam:PassedToService` condition étendue au service pour garantir que les opérations sont limitées aux ressources des agents de sécurité au AWS sein du même compte. AWS

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez AWSTransformSecurityAgentExecutorAccess le AWS Managed Policy Reference Guide.

AWS stratégie gérée : DBModDiscoveryAndAssessment

Cette politique fournit des fonctionnalités complètes de découverte et d'évaluation de la modernisation des bases de données pour AWS Transform.

Description

Cette politique inclut les autorisations suivantes :

- Amazon EC2 — Permet de décrire les composants de l'infrastructure, notamment les instances, les VPC, les sous-réseaux, les groupes de sécurité, les zones de disponibilité, les points de terminaison des VPC et les passerelles Internet.
- Amazon RDS : permet de décrire les instances de base de données, les clusters et les groupes de sous-réseaux. Permet de modifier des groupes de sous-réseaux de base de données au sein d'un même AWS compte pour préparer la migration.
- API de données Amazon RDS : permet d'activer et de désactiver les points de terminaison HTTP et d'exécuter des instructions SQL sur des clusters de bases de données balisés pour le projet de modernisation de la base de données.
- AWS DMS— Permet de décrire les points de terminaison, les instances de réplication, les tâches, les groupes de sous-réseaux et les instances commandables. Permet de répertorier les fournisseurs de données, les profils d'instance et les projets de migration. Permet de décrire les statistiques des tables, les cycles d'évaluation et les opérations des modèles de métadonnées. Les opérations de description détaillée et de métadonnées sont limitées aux ressources étiquetées pour le projet de modernisation de la base de données.
- — Permet de répertorier les secrets pour découvrir les informations d'identification de la base de données.
- Gestion des identités et des accès AWS (IAM) : permet d'inspecter des rôles de AWS DMS service spécifiques et les politiques qui y sont associées. Inclut l'accès aux AWS DMS politiques AWS gérées en lecture.
- AWS Key Management Service (KMS) — Permet de répertorier les alias de clé et de décrire les clés. Permet le déchiffrement de secrets par intégration, limité au même AWS compte.

La politique met en œuvre l'accès au moindre privilège via des autorisations au niveau des ressources, des conditions basées sur des balises et des restrictions au niveau du compte afin de garantir que les opérations sont limitées aux ressources du projet de modernisation de la base de données au sein du même compte. AWS

Détails de l'autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez DBModDiscoveryAndAssessment le AWS Managed Policy Reference Guide.

AWS stratégie gérée : DBModProvisioningAndMigration

Cette politique fournit des fonctionnalités de provisionnement et de migration de bases de données pour les projets de modernisation des bases de données AWS Transform. Elle inclut les autorisations

nécessaires pour créer et gérer l'infrastructure de migration, provisionner les bases de données cibles et stocker les données de migration.

Description

Cette politique inclut les autorisations suivantes :

- AWS DMS— Permet de créer et de gérer des groupes de sous-réseaux de réplication, des profils d'instance, des fournisseurs de données, des projets de migration, des points de terminaison, des instances de réplication et des tâches de réplication. Inclut les opérations de conversion de schéma telles que l'importation, la conversion, l'exportation et l'évaluation de modèles de métadonnées. Permet la gestion du cycle de vie des instances de réplication (création, suppression, modification, redémarrage) et des tâches de réplication (suppression, démarrage, arrêt, évaluation). Toutes les opérations d'écriture sont limitées aux ressources étiquetées pour le projet de modernisation de la base de données.
- Amazon RDS — Permet de créer des groupes de sous-réseaux de base de données, des clusters de bases de données et des instances de base de données. Toutes les ressources doivent être étiquetées pour le projet de modernisation de la base de données.
- — Permet de créer, de mettre à jour et de baliser des secrets à l'aide du préfixe de dénomination de modernisation de la base de données. Permet de récupérer les valeurs secrètes et de décrire les secrets des ressources balisées.
- Amazon S3 : permet de créer et de gérer des compartiments et des objets S3 pour le stockage des données de migration. Comprend le balisage des compartiments, la gestion des versions et les opérations relatives au cycle de vie des objets. Limité aux compartiments dotés du préfixe de dénomination de modernisation de la base de données.
- Gestion des identités et des accès AWS (IAM) : permet de transmettre des rôles de AWS DMS service spécifiques à des services de conversion de schémas AWS DMS et à des services de conversion de schémas. Permet de créer le rôle lié au service Amazon RDS requis pour les opérations de base de données.

La politique met en œuvre l'accès au moindre privilège via des autorisations au niveau des ressources, des conditions basées sur des balises et des restrictions au niveau du compte afin de garantir que les opérations sont limitées aux ressources du projet de modernisation de la base de données au sein du même compte. AWS

Détails de l’autorisation

Pour consulter les détails des autorisations relatives aux politiques, consultez DBModProvisioningAndMigration le AWS Managed Policy Reference Guide.

AWS Transformer la référence des autorisations

Cette section fournit des informations sur les API utilisées par AWS Transform et sur leur fonction.

Rubriques

- AWS Transformez les API

AWS Transformez les API

- transformer : BatchGetMessage
- transformer : BatchGetUserDetails
- transformer : CompleteArtifactUpload
- transformer : CreateArtifactDownloadUrl
- transformer : CreateArtifactUploadUrl
- transformer : CreateAssetDownloadUrl
- transformer : CreateConnector
- transformer : CreateFeedback
- transformer : CreateJob
- transformer : CreateSession
- transformer : CreateWorkspace
- transformer : DeleteConnector
- transformer : DeleteJob
- transformer : DeleteSelfRoleMappings
- transformer : DeleteUserRoleMappings
- transformer : DeleteWorkspace
- transformer : DetectIsAllowedForOperation
- transformer : GetConnector
- transformer : GetFeedbackQuestions
- transformer : GetHitlTask

- transformer : GetJob
- transformer : GetLoginRedirectUri
- transformer : GetUserDetails
- transformer : GetUserPreferences
- transformer : GetWebAppUrl
- transformer : GetWorkspace
- transformer : ListArtifacts
- transformer : ListConnectors
- transformer : ListHitlTasks
- transformer : ListJobPlanSteps
- transformer : ListJobs
- transformer : ListMessages
- transformer : ListPlanUpdates
- transformer : ListUserRoleMappings
- transformer : ListWorklogs
- transformer : ListWorkspaces
- transformer : PutUserPreferences
- transformer : PutUserRoleMappings
- transformer : RevokeSession
- transformer : SearchUsers
- transformer : SearchUsersTypeahead
- transformer : SendMessage
- transformer : StartJob
- transformer : StopJob
- transformer : SubmitCriticalHitlTask
- transformer : SubmitStandardHitlTask
- transformer : TestReleaseTraitPreProd
- transformer : TestReleaseTraitProd
- transformer : UpdateHitlTask

- transformer : UpdateJob
- transformer : UpdateWorkspace
- transformer : VerifySession

Validation de conformité pour AWS Transformation

Notre nouvelle expérience AWS d'inscription n'est pas conçue pour les charges de travail réglementées. Si vous utilisez notre nouvelle interface d' AWS inscription, mais que vous souhaitez l'utiliser AWS pour des charges de travail réglementées, vous pouvez vous inscrire à des fonctionnalités AWS (avancées) ou activer des fonctionnalités avancées pour votre AWS environnement.

Pour savoir si un s' Service AWS inscrit dans le cadre de programmes de conformité spécifiques, consultez Services AWS la section Étendue par programme de conformité et choisissez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

Résilience dans AWS Transformation

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS globale, AWS Transform propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

AWS Transform et points de terminaison d'interface (AWS PrivateLink)

Vous pouvez établir une connexion privée entre votre VPC et créer un point de AWS Transform terminaison VPC d'interface. Les points de terminaison de l'interface sont alimentés par AWS PrivateLinkune technologie qui vous permet d'accéder à la AWS Transform console en privé sans passerelle Internet, périphérique NAT, connexion VPN ou Direct Connect connexion. Le trafic entre votre VPC et celui qui AWS Transform ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux.

Pour de plus amples informations, consultez Points de terminaison VPC (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

> **Note**
>
> Pour une PrivateLink documentation AWS Transform personnalisée, voirAWS Transform points de terminaison personnalisés et d'interface (AWS PrivateLink).

Considérations relatives à AWS Transform Points de terminaison d'un VPC

Avant de configurer un point de terminaison VPC d'interface pour AWS Transform, assurez-vous de consulter les propriétés et les limites du point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

Conditions préalables

Avant de commencer toute procédure ci-dessous, vérifiez que vous disposez des éléments suivants :

- Un AWS compte doté des autorisations appropriées pour créer et configurer des ressources.
- Un VPC déjà créé dans votre AWS compte.
- Connaissance des AWS services, en particulier Amazon AWS Transform VPC et.

Création d'un point de terminaison VPC d'interface pour AWS Transform

Vous pouvez créer un point de terminaison VPC pour le AWS Transform service à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

AWS Transform prend en charge les services de point de terminaison VPC suivants :

Nom du service	Endpoint	Remarque
Plan de contrôle	`com.amazonaws.`*`region`*`.transform`	
API Agentic	`com.amazonaws.`*`region`*`.transform-agents`	
Application web	`com.amazonaws.`*`region`*`.api.transform`	Nécessaire pour l'application AWS Transform Web. Le DNS privé doit être activé sur ce point de terminaison (option Activer le nom DNS) afin qu'il soit `api.transform.`*`region`*`.on.aws` résolu en une adresse IP privée dans votre VPC.

*`region`*Remplacez-le par la AWS région dans laquelle votre AWS Transform profil est installé, par exemple com.amazonaws.us-east-1.transform.

> **Note**
>
> Si vous utilisez l'application AWS Transform Web, le `api.transform` point de terminaison est obligatoire. Pour le guide de configuration complet, voirAccès au AWS Transform application Web à partir d'un VPC.

Pour plus d'informations, consultez Régions prises en charge pour AWS Transform la section Accès à un service via un point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

Utilisation d'un ordinateur local pour se connecter à un AWS Transform point de terminaison

Cette section décrit le processus d'utilisation d'un ordinateur local pour se connecter AWS Transform via un AWS PrivateLink point de terminaison de votre AWS VPC.

1. Créez une connexion VPN entre votre appareil sur site et votre VPC.
2. Créez un point de terminaison VPC d'interface pour. AWS Transform
3. Configurez un point de terminaison Amazon Route 53 entrant. Cela vous permettra d'utiliser le nom DNS de votre AWS Transform point de terminaison depuis votre appareil local.

Accès au AWS Transform application Web à partir d'un VPC

Lorsque vous accédez AWS PrivateLink à l' AWS Transform API en privé depuis votre VPC, l'application Web nécessite une configuration réseau supplémentaire. Il diffuse du contenu statique (HTML JavaScript, CSS) via CloudFront, ce qui nécessite une connexion Internet. Les appels d'API provenant de l'application Web passent par le point de terminaison de votre VPC et restent totalement privés.

Ce guide explique comment configurer une sortie Internet contrôlée depuis votre VPC afin que l'application Web puisse se charger tout en maintenant votre VPC verrouillé uniquement aux domaines requis.

Comment ça marche

L'application AWS Transform Web utilise deux chemins réseau :

- Appels d'API : lorsque vous interagissez avec l'application Web (démarrage de tâches, affichage d'espaces de travail, etc.), le navigateur envoie des demandes d'API à`api.transform.region.on.aws`. Lorsque le point de terminaison `com.amazonaws.region.api.transform` VPC et le DNS privé sont activés, ces demandes sont résolues vers une adresse IP privée dans votre VPC et ne quittent jamais le réseau. AWS
- Contenu statique — Les fichiers HTML et CSS de l'application Web sont diffusés CloudFront via`tenant-id.transform.region.on.aws`. JavaScript Le chargement de ces fichiers

nécessite une connexion Internet, car la diffusion de CloudFront contenu n'est disponible que sur l'Internet public.

- Authentification : utilisation des flux de connexion AWS IAM Identity Center`region`.signin.aws, qui nécessitent également une connexion Internet.

Pour activer l'application Web tout en préservant la sécurité, vous devez créer un chemin de sortie contrôlé à l'aide de AWS Network Firewall avec filtrage basé sur le domaine. Cela permet à votre VPC d'accéder uniquement aux domaines spécifiques requis par l'application Web tout en bloquant tout autre trafic Internet.

Architecture

Le schéma suivant montre le chemin réseau pour le trafic des applications 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

Le Network Firewall doit détecter le trafic dans les deux sens (routage symétrique) pour effectuer une inspection TLS SNI. Vous devez configurer une route de retour dans le sous-réseau NAT Gateway qui renvoie le trafic destiné au sous-réseau privé via le pare-feu. Sans cela, les règles de filtrage basées sur le domaine ne fonctionneront pas.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un AWS compte autorisé à créer des ressources VPC, un Network Firewall et des passerelles NAT.
- Un VPC doté d'un sous-réseau privé sur lequel s'exécutent vos instances ou charges de travail.
- Une passerelle Internet attachée au VPC (ou des autorisations pour en créer une).
- Un point de terminaison AWS Transform VPC pour lequel le `com.amazonaws.region.api.transform` DNS privé est activé. Il s'agit du point de terminaison utilisé par le client du navigateur d'applications Web. Pour obtenir des instructions sur la création de points de terminaison, consultezAWS Transform et points de terminaison d'interface (AWS PrivateLink).

Configuration de la politique de point de terminaison du VPC

Si votre point de terminaison `com.amazonaws.region.api.transform` VPC dispose d'une politique de point de terminaison personnalisée, vous devez ajouter une instruction autorisant AWS Transform les opérations. Sans cela, l'application Web ne pourra pas effectuer d'appels d'API via le point de terminaison.

Ajoutez la déclaration suivante à votre politique de point de terminaison VPC. *AWS_TRANSFORM_PROFILE_ARN*Remplacez-le par l'ARN de votre profil de AWS Transform service, que vous pouvez trouver dans la AWS Transform console sur la page Paramètres.

```
{
    "Statement": [
        {
            "Sid": "AllowAWSTransform",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalArn": [
                        "AWS_TRANSFORM_PROFILE_ARN"
                    ]
```

```
                }
            }
        }
    ]
}
```

> **Note**
>
> Si votre point de terminaison VPC utilise la politique par défaut (accès complet), aucune modification n'est nécessaire et vous pouvez ignorer cette étape.

Configuration d'une sortie Internet contrôlée

Procédez comme suit pour configurer Network Firewall avec un filtrage basé sur le domaine pour l'application AWS Transform Web.

Étape 1 : créer le sous-réseau du pare-feu

Créez un petit sous-réseau /28 dédié au point de terminaison Network Firewall. Ce sous-réseau doit se trouver dans la même zone de disponibilité que votre sous-réseau privé.

```
aws ec2 create-subnet \
  --vpc-id your-vpc-id \
  --cidr-block firewall-subnet-cidr \
  --availability-zone your-az \
  --region region
```

Étape 2 : créer un sous-réseau public pour la passerelle NAT

```
aws ec2 create-subnet \
  --vpc-id your-vpc-id \
  --cidr-block public-subnet-cidr \
  --availability-zone your-az \
  --region region
```

Étape 3 : Configuration de la table de routage du sous-réseau public

Créez une table de routage pour le sous-réseau public qui achemine le trafic Internet vers la passerelle 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
```

Étape 4 : Création de la passerelle 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
```

Étape 5 : Création du groupe de règles Network Firewall

Créez un groupe de règles dynamiques qui autorise le trafic uniquement vers les domaines requis par l'application 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
```

Remplacez *region* par la AWS région dans laquelle votre AWS Transform profil est installé (par exemple,`us-east-1`). *directory-id*Remplacez-le par votre ID de répertoire IAM Identity Center (par exemple,`d-1234567890`). Vous pouvez trouver l'ID de votre répertoire dans la console IAM Identity Center.

Le tableau suivant décrit les domaines autorisés.

Domain	Objectif
`.cloudfront.net`	CloudFront CDN — fournit des actifs statiques d'applications Web (CSSJavaScript, images)
`.transform.` *`region`*`.on.aws`	URL du locataire de l'application Web : le navigateur charge la page initiale à partir de ce domaine via CloudFront
`region``.signin.aws`	Page de redirection de connexion SSO
`.s3.`*`region`*`.amazonaws.com`	URL présignées S3 : chargements et téléchargements d'artefacts
`oidc.`*`region`*`.amazonaws.com`	Échange de jetons OIDC pour l'authentification SSO
`portal.sso.` *`region`*`.amazonaws.com`	Page de connexion au portail SSO
`assets.sso-portal.` *`region`*`.amazonaws.com`	Ressources statiques du portail SSO (CSS, JavaScript)
`directory-id` `.awsapps.com`	Portail IAM Identity Center pour votre organisation

> **Note**
>
> Le `.cloudfront.net` caractère générique autorise le trafic vers n'importe quelle CloudFront distribution, et pas seulement vers celle de l'application AWS Transform Web. Un filtre de domaine plus étroit n'est pas possible car les adresses IP CloudFront périphériques sont partagées entre les distributions et l'inspection TLS SNI ne permet pas de distinguer les distributions individuelles derrière le même domaine.

> **Note**
>
> Les appels d'API `api.transform.`*`region`*`.on.aws` doivent être AWS PrivateLink traités et ne nécessitent pas de sortie Internet. Ils ne sont pas affectés par le pare-feu.

Étape 6 : Création de la politique de pare-feu

La politique doit utiliser l'évaluation des `STRICT_ORDER` règles `drop_established` comme action par défaut. Cela garantit que tout trafic ne correspondant pas à la liste d'autorisation est supprimé.

```
# 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
```

Étape 7 : Création du 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
```

Étape 8 : obtenir l'identifiant du point de terminaison du pare-feu

```
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"
```

Étape 9 : Configuration de la table de routage du sous-réseau du pare-feu

Acheminez le trafic Internet du sous-réseau du pare-feu vers la passerelle 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
```

Étape 10 : Mettre à jour la table de routage du sous-réseau privé

Acheminez tout le trafic Internet depuis le sous-réseau privé via le pare-feu.

```
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 un itinéraire par défaut existe déjà, utilisez-le à la `replace-route` place de`create-route`.

Étape 11 : Ajouter l'itinéraire de retour symétrique (obligatoire)

> **Important**
>
> Cette étape est essentielle. Network Firewall utilise l'inspection TLS SNI et doit détecter les deux directions d'une connexion TCP. Ajoutez une route dans la table de routage du sous-réseau NAT Gateway qui renvoie le trafic de retour destiné au sous-réseau privé via le pare-feu.

```
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*Remplacez-le par le bloc CIDR de votre sous-réseau privé (par exemple,`10.0.144.0/20`).

Sans routage symétrique, le pare-feu ne voit que le trafic dans une seule direction. Le moteur d'inspection TLS ne peut pas extraire l'indication du nom du serveur (SNI) du handshake TLS, et toutes les règles basées sur le domaine échoueront silencieusement.

Étape 12 : Supprimer la route IPv6 par défaut (le cas échéant)

Si la table de routage du sous-réseau privé possède une route IPv6 par défaut (`::/0`) pointant directement vers une passerelle Internet, elle contournera le pare-feu pour les IPv6-capable destinations. Retirez-le :

```
aws ec2 delete-route \
  --route-table-id private-subnet-route-table-id \
  --destination-ipv6-cidr-block ::/0 \
  --region region
```

Vérification

À partir d'une instance du sous-réseau privé, vérifiez la configuration :

```
# 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)
```

Résolution des problèmes

Les appels d'API à api.transform sont bloqués par votre pare-feu

Le domaine `api.transform.region.on.aws` doit être converti en une adresse IP privée via le point de terminaison VPC et ne doit pas atteindre votre pare-feu Internet.

- Vérifiez que vous avez créé le `com.amazonaws.region.api.transform` point de terminaison.
- Vérifiez que le DNS privé est activé sur le terminal :

```
aws ec2 describe-vpc-endpoints \
  --filters "Name=service-name,Values=com.amazonaws.region.api.transform" \
  --query 'VpcEndpoints[*].[State,PrivateDnsEnabled]' \
  --output table
```

Résultat attendu : `available | True`

L'application Web ne se charge pas (délai d'expiration de la connexion)

- Vérifiez que la table de routage du sous-réseau privé possède un `0.0.0.0/0` itinéraire pointant vers le point de terminaison du pare-feu.
- Vérifiez que la table de routage du sous-réseau du pare-feu possède une `0.0.0.0/0` route pointant vers la passerelle NAT.
- Vérifiez que la passerelle NAT est dans un `available` état.

Non-allowlisted les domaines ne sont pas bloqués

- Vérifiez s'il existe une `::/0` route IPv6 pointant vers la passerelle Internet. Cela permet de contourner le pare-feu. Retirez-le (étape 12).
- Vérifiez que le routage symétrique est configuré. La table de routage du sous-réseau de la passerelle NAT doit disposer d'une route de retour à travers le pare-feu pour le CIDR du sous-réseau privé (étape 11).
- Vérifiez la politique de pare-feu utilisée `STRICT_ORDER` avec `drop_established` et `alert_established` comme actions par défaut.

Considérations de coût

Ressource	Coût approximatif
Network Firewall	~0 $. 395/hr (~$288/month) par zone de disponibilité
Passerelle NAT	~0 $. 045/hr (~$33/month) + frais de traitement des données
IP élastique (IPv4 public)	~0 $. 005/hr (~3 $). 60/month)
Traitement des données par Network Firewall	0$. 065/GB
Traitement des données par passerelle NAT	0$. 045/GB

Le coût de base estimé est d'environ $ 325/month pour un déploiement dans une seule zone de disponibilité. Pour les déploiements de production, déployez le pare-feu, la passerelle NAT et les sous-réseaux associés dans chaque zone de disponibilité où existent des sous-réseaux privés.

Nettoyage

Pour supprimer toutes les ressources créées par ce guide, exécutez les commandes suivantes dans l'ordre inverse. Remplacez les espaces réservés par les identifiants de ressources de votre déploiement. Vous pouvez trouver ces valeurs dans la console AWS de gestion ou en utilisant les `describe` commandes indiquées dans les étapes de configuration.

```
# 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
```

Contrôle AWS Transformation

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de AWS Transform et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller AWS Transform, signaler un problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos fichiers journaux à partir d'instances Amazon EC2 et d'autres sources. CloudTrail CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.
- Amazon EventBridge peut être utilisé pour automatiser vos AWS services et répondre automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Logging AWS Transformez les appels d'API à l'aide AWS CloudTrail

AWS Transform est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Transform. CloudTrail capture tous les appels d'API pour AWS Transform sous forme d'événements. Les appels capturés incluent des appels provenant de la console AWS Transform et des appels de code vers les opérations de l'API AWS Transform. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour AWS Transform. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à AWS Transform, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AWS Transformez les informations en CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AWS Transform, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre entreprise Compte AWS, y compris ceux de AWS Transform, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge

- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou Gestion des identités et des accès AWS (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Compréhension AWS Transformer les entrées du fichier journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Notifications

AWS Transform fournit des notifications par e-mail pour vous tenir informé des modifications relatives à l'accès à l'espace de travail, des mises à jour du statut des tâches et des demandes de collaboration en attente.

Notifications par e-mail

Les notifications par e-mail sont activées par défaut et sont envoyées aux utilisateurs disposant d'autorisations en lecture seule ou supérieures sur une tâche. Les utilisateurs peuvent modifier leurs préférences de notification. Il existe trois catégories de notifications par e-mail :

- Mises à jour de l'accès

  Vous recevez une notification lorsque vous êtes ajouté à un nouvel espace de travail et lorsque votre rôle est modifié dans un espace de travail.

- E-mails de synthèse quotidiens

  Vous recevez un résumé quotidien par e-mail à 9 h 00, heure du Pacifique, résumant vos offres d'emploi en cours si vous avez des offres d'emploi pour lesquelles une ou plusieurs demandes de collaboration sont requises. L'e-mail inclut un tableau indiquant le nom de l'espace de travail, le nom du poste, le statut du poste, les détails de la demande du collaborateur et les actions requises (limité à 10 lignes)

  > **Note**
  >
  > Les e-mails de synthèse quotidiens ne sont envoyés que pour les tâches nécessitant des demandes de collaboration. Les demandes facultatives des collaborateurs ne déclenchent pas les e-mails de synthèse.

- Mises à jour du statut des emplois

  Vous recevez un e-mail lorsqu'une tâche à laquelle vous avez accès est terminée ou échoue.

- Mises à jour des demandes de collaboration

  Vous recevez un e-mail chaque fois qu'une tâche nécessite votre contribution, votre révision ou votre approbation.

Gestion des notifications par e-mail

Vous pouvez modifier vos préférences de notification par e-mail dans l'application Web en cliquant sur le bouton Paramètres dans le coin supérieur droit de l'application, puis en choisissant Paramètres de notification.

La page des paramètres de notification propose les commandes suivantes :

Type de notification	Description	Paramètre par défaut
Mises à jour de Workspace	Recevez des e-mails lorsque vous êtes ajouté à un espace de travail ou lorsque votre rôle est modifié dans un espace de travail	Activé
Résumé des demandes quotidiennes des collaborateurs	Recevez un résumé quotidien des demandes d'emploi ouvertes de collaborateurs dans des espaces de travail accessibles	Activé
Mises à jour sur l'achèvement des tâches	Recevoir des e-mails lorsqu'une tâche est terminée ou échoue	Activé
Mises à jour des demandes de collaboration	Recevez des e-mails lorsqu'une saisie ou une approbation est requise de votre part	Désactivé

Vous pouvez utiliser un paramètre général pour activer ou désactiver toutes les notifications, ou configurer les différents types de notifications séparément.

Quotas pour AWS Transformation

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est Region-specific. Vous pouvez demander des augmentations de certains quotas, tandis que d'autres quotas ne peuvent pas être augmentés.

Pour consulter les quotas de AWS Transform, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez les AWS services, puis sélectionnez AWS Transformer.

Pour demander une augmentation de quota, consultez Demander une augmentation de quota dans le Guide de l'utilisateur de Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le formulaire d'augmentation de limite.

Votre AWS compte possède les quotas suivants liés à AWS Transform.

Charge de travail	Dimension	Quota	Ajustable	Description
Plateforme	Espaces de travail Région AWS par compte AWS Transform activé	100 espaces de travail pris en charge pour chacun Région AWS	Oui	Le nombre maximum d'espaces de travail par compte AWS Transform activé par Région AWS
Migration vers VMware	Nombre de serveurs pour chaque vague	Chaque vague : 150 serveurs	Non	Le nombre maximum de serveurs par vague
ordinateur central	Tâches simultanées pour chaque compte IAM Identity Center	10 emplois pour chaque région prise en charge	Oui	Nombre maximal de tâches mainframe simultanées dans un compte IAM Identity Center

Charge de travail	Dimension	Quota	Ajustable	Description
	Des lignes de code pour chaque tâche	3 000 000 lignes de code pour chaque région prise en charge	Non	Le nombre maximum de lignes de code pour chaque tâche.
	Analyse des lignes de code mensuelles	100 000 000 lignes de code pour chaque région prise en charge	Oui	Le nombre maximum de lignes de code pour l'objectif de la tâche Analyser le code par mois civil
	Génération de documents commerciaux (lignes de code mensuelles)	50 000 000 lignes de code pour chaque région prise en charge	Oui	Le nombre maximum de lignes de code pour l'objecti f du poste de génération de documentation commerciale par mois civil
	Génération de documents techniques (lignes de code mensuelles)	50 000 000 lignes de code pour chaque région prise en charge	Oui	Le nombre maximum de lignes de code pour l'objecti f du poste de génération de documentation technique par mois civil

Charge de travail	Dimension	Quota	Ajustable	Description
	Transformation de lignes de code	10 000 000 lignes de code pour chaque région prise en charge	Oui	Le nombre maximum de lignes de code transformées au cours d'un mois civil
	Décomposition des lignes de code mensuelles	50 000 000 lignes de code pour chaque région prise en charge	Oui	Le nombre maximum de lignes de code pour l'objectif de la tâche de décomposition par mois civil
	Reforgez les lignes de code mensuelles	50 000 000 lignes de code pour chaque région prise en charge	Oui	Le nombre maximum de lignes de code pour l'objecti f du travail de Reforge par mois civil
	Lignes de code mensuelles de logique métier extraites	50 000 000 lignes de code pour chaque région prise en charge	Oui	Le nombre maximum de lignes de code pour l'objectif du job Extracted Business Logic par mois civil

Charge de travail	Dimension	Quota	Ajustable	Description
.NET	Lignes de code mensuelles .NET (Web et IDE)	1 000 000 de lignes de code pour chaque région prise en charge	Oui	Nombre maximal de lignes de code d'application .NET pouvant être transformées en un mois civil dans chaque compte IAM Identity Center pris en charge Région AWS
	Tâches .NET simultanées avec l'extension Microsoft Visual Studio pour chaque compte IAM Identity Center	10 emplois pour chaque région prise en charge	Oui	Nombre maximal de tâches de transformation .NET simultanées dans chaque compte IAM Identity Center pris en charge Région AWS lors de l'utilisation de l'extension Microsoft Visual Studio.

Charge de travail	Dimension	Quota	Ajustable	Description
	Tâches Web .NET simultanées pour chaque compte IAM Identity Center	5 emplois pour chaque région prise en charge	Oui	Nombre maximal de tâches de transform ation .NET simultanées dans chaque compte IAM Identity Center pris en charge lors Région AWS de l'utilisation de l'application Web AWS Transform.
Transformations personnalisées	Définitions de transformation personnalisées	1 000	Oui	Le nombre maximum de définitions de transformation personnalisées
	Taille de définitio n de transform ation personnal isée	10 Mo	Non	Taille totale maximale de tous les fichiers inclus dans la définition de transformation, y compris les références aux documents.

Charge de travail	Dimension	Quota	Ajustable	Description
	Demandes de conversation CLI mensuelles de transformation personnalisée	1 000 000	Oui	Le nombre maximum de demandes de conversation de transformation personnalisées effectuées dans la CLI autorisées au cours d'un mois civil
Évaluation	Limite du nombre de serveurs pour chaque évaluation	Chaque évaluation : 30 000 serveurs	Non	Nombre maximal de serveurs par tâche d'évaluation

Régions prises en charge pour AWS Transform

> **Note**
>
> Si vous faites une demande qui nécessite de AWS Transform récupérer des informations d'une région optionnelle non répertoriée sur cette page, AWS Transform vous pouvez passer des appels vers cette région. Pour gérer l'accès aux régions vers AWS Transform lesquelles vous pouvez passer des appels, voirSécurité dans AWS Transformation.

Cette rubrique décrit l' Régions AWS endroit où vous pouvez utiliser AWS Transform. Pour plus d'informations Régions AWS, voir Spécifier les comptes que Régions AWS votre compte peut utiliser dans le Guide de Gestion de compte AWS référence.

Vos données peuvent être traitées dans une région différente de celle dans laquelle vous les utilisez AWS Transform. Pour plus d'informations sur le traitement interrégional dans AWS Transform, voirCross-region traitement. Pour en savoir plus sur l'endroit où les données sont stockées pendant le traitement, consultez Protection des données.

Pris en charge Régions AWS (activé par défaut)

Vous pouvez créer des AWS Transform espaces de travail comme suit Régions AWS. Ces régions sont activées par défaut ; il n'est pas nécessaire de les activer avant de les utiliser. Pour plus d'informations, consultez Regions that are enabled by default.

- USA Est (Virginie du Nord)
- Europe (Francfort)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Sydney)
- Asia Pacific (Tokyo)
- Europe (Londres)
- Asie-Pacifique (Séoul)
- Canada (Centre)
- Amérique du Sud (São Paulo) - Agents de modernisation du mainframe uniquement

L'espace de travail dans lequel vous créez une tâche détermine la Région AWS nature de la tâche. Pour créer un emploi dans une autre région, vous devez utiliser un autre espace de travail situé dans la région de votre choix.

Pour les projets VMware, la région de l'espace de travail est utilisée pour la découverte. Vous pouvez toutefois spécifier une autre région comme cible de migration. Cette région cible est celle où vos charges de travail sont hébergées une fois la migration terminée. Pour plus d'informations sur les Région AWS considérations relatives aux migrations VMware, y compris la liste des régions cibles possibles, consultezthe section called “Régions cibles prises en charge”.

AWS support pour AWS Transform

AWS Transform vous permet de créer et de gérer des dossiers de AWS Support via le chat si vous rencontrez des problèmes lors de vos tâches de transformation. Vos dossiers sont automatiquement enrichis en fonction du contexte du poste et acheminés vers l'équipe d'assistance appropriée. Si vous êtes un client actif de Countdown Premium, votre ingénieur désigné vous contactera pour gérer la résolution des problèmes. Pour en savoir plus, consultez AWS Countdown Premium. Dans le cas contraire, votre cas sera examiné par l'équipe d' AWS Transform assistance dans sa file d'assistance.

Conditions préalables

Avant de pouvoir utiliser la gestion des dossiers d'assistance, vous devez :

- Un plan de AWS Support actif (Business On-Ramp, Enterprise ou Enterprise)
- Une AWS Transform application existante

Activation de la gestion des dossiers de support

1. Ouvrez la AWS Transform console.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sous Support, choisissez Activer la gestion des dossiers de support.
4. Sélectionnez Enregistrer les modifications.

AWS Transform utilise un rôle lié au service (SLR) pour créer et gérer les demandes d'assistance en votre nom. Aucune autorisation IAM supplémentaire n'est requise.

Création d'un dossier de support

Pour créer un dossier d'assistance, utilisez l'interface de chat :

1. Demandez à créer un dossier d'assistance. Par exemple :
   - « Créer un dossier de soutien pour mon projet de transformation qui a échoué »
   - « J'ai besoin d'aide pour corriger des erreurs de travail, créer un dossier »

2. Le chat vous invite à saisir les informations requises :
    - Brève description de votre problème
    - Une description détaillée
3. Confirmez la création du dossier lorsque vous y êtes invité.

Le dossier est automatiquement renseigné avec le contexte de votre tâche de transformation, notamment :

- Numéro et statut du job
- Métadonnées du job
- Journaux d'exécution des tâches (journaux de travail)
- Plan d'emploi

Le dossier est automatiquement attribué en fonction de votre type de poste et de la catégorie de problème.

Afficher les dossiers de support

Pour consulter vos demandes d'assistance, lancez le chat :

- « Répertorier mes demandes d'assistance »
- « Montrez-moi les dossiers d'assistance en cours »
- « Quel est l'état de mes dossiers ? »

Le chat affichera :

- ID du cas
- Sujet
- État, tel que ouvert, en attente, résolu ou fermé
- Date de dernière mise à jour
- ID de tâche associé

Pour consulter les détails d'un cas spécifique, procédez comme suit :

- « Afficher les détails du dossier [numéro de dossier] »
- « Quelle est la dernière mise à jour concernant le dossier [numéro de dossier] ? »

Ajouter des communications à un dossier

Pour ajouter un message à un dossier existant :

1. Demandez au chat : « Ajouter un message au dossier [case id] »
2. Entrez votre message lorsque vous y êtes invité.
3. Le chat confirmera que le message a été ajouté.

Vous recevrez des notifications lorsque le AWS Support répondra à votre demande.

Résolution d'un cas

Pour résoudre un dossier d'assistance, procédez comme suit :

1. Demandez au chat : « Résoudre le dossier [identifiant de cas] »
2. Confirmez la résolution lorsque vous y êtes invité.

> **Note**
>
> Vous ne pouvez résoudre que les cas qui ont été traités par le AWS Support.

Désactivation de la gestion des dossiers de support

1. Ouvrez la AWS Transform console.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sous Support, choisissez Désactiver la gestion des demandes d'assistance.
4. Sélectionnez Enregistrer les modifications.

> **Note**
>
> La désactivation de la gestion des dossiers de support supprime l'interface de gestion des dossiers basée sur le chat, mais ne ferme pas les dossiers existants. Vous pouvez toujours accéder à vos dossiers via le AWS Support Center.

Télémétrie d'utilisation

Le plugin AWS Transform IDE, AWS Transform Agent Skill et AWS Transform Kiro Power collectent la télémétrie d'utilisation par défaut lors de l'exécution de la transformation. La télémétrie comprend différents points de données, tels que le nom de l'IDE (par exemple, VS Code ou Kiro), le nom de l'agent AI (par exemple, Claude Code ou OpenAI Codex) et le mode d'exécution (local ou distant). Ces données sont utilisées par AWS Transform pour prioriser les tests de compatibilité, ainsi que la latence et la fiabilité.

Pour désactiver la télémétrie, indiquez à l'agent pendant votre session de chat que vous ne voulez pas que la télémétrie soit émise. Cette désinscription s'applique uniquement à la session de chat en cours et doit être répétée à chaque nouvelle session. Si vous exécutez directement la CLI AWS Transform, définissez la variable d'`ATX_DISABLE_TELEMETRY=true`environnement.

Données opérationnelles

Nous pouvons collecter des signaux opérationnels concernant votre utilisation de AWS Transform, tels que les fonctionnalités que vous utilisez, les journaux d'erreurs et les indicateurs basés sur vos commentaires en langage naturel (par exemple si vous avez approuvé la poursuite d'un plan de transformation ou avez fourni des instructions pour itérer un plan proposé) afin de fournir le service et d'évaluer les performances du service.

Journal des modifications

Le tableau suivant décrit les principales versions et mises à jour de AWS Transform.

Date	Titre	Description	Liens
16/08/2026	AWS Transform for migrations ajoute la suppression des règles de groupe de sécurité obsolètes	AWS Transform for migrations identifie désormais les règles de pare-feu entrantes non utilisées migrées depuis votre environnement sur site et suggère de les supprimer dans le cadre des recommandations réseau guidées. Cela vous permet d'éviter de reporter une exposition à la sécurité, telle que l'accès entrant ouvert, qui ne sert plus à rien. La suppression est limitée aux règles d'entrée non utilisées, où l'absence de trafic observé constitue un signal fiable indiquant qu'une règle n'est pas utilisée.	Documentation
29/07/2026	AWS Transform for Migrations s'étend au-delà de VMware	AWS Transform for migrations prend désormais en charge	Documentation

Date	Titre	Description	Liens
		la migration d'environnements de serveurs virtuels et bare metal depuis pratiquement toutes les sources, y compris VMware et d'autres plateformes. Hyper-V Les fonctionnalités de migration sont disponibles quelle que soit votre infrastructure source : découverte, planification de la migration, création de zones d'atterrissage, migration du réseau et réhébergement du serveur. Le flux de travail des applications Web a été renommé de « VMware Migrations » en « Migrations (y compris VMware) ».	

Date	Titre	Description	Liens
29/07/2026	AWS Transform for migrations ajoute la prise en charge des actions après le lancement	AWS Transform for migrations prend désormais en charge les actions post-lancement qui automatisent les tâches de modernisation et de validation sur chaque serveur après son lancement en tant qu'instance de test ou de basculement. L'agent recommande, configure et exécute des actions en votre nom à l'aide AWS Systems Manager de. Les actions peuvent être prédéfinies ou personnalisées, définies au niveau du compte ou personnalisées par serveur.	Documentation

Date	Titre	Description	Liens
03 juillet 2026/07	AWS L'outil Transform Discovery ajoute la prise en charge des bases de données Oracle	L'outil de découvert e AWS Transform collecte désormais des métadonnées Oracle détaillée s directement à partir de vos bases de données sur VMware et sur des serveurs bare metal. Hyper-V Vous pouvez découvrir des instances Oracle via des connexions SQL directes. L'outil collecte l'énuméra tion de la Database/ Pluggable base de données de conteneurs (CDB/ PDB), l'inventaire des composants et le dimensionnement des fichiers de données. Il capture également les indicateurs de topologie pour les Real Application Clusters (RAC), Data Guard et l'archite cture multitenant. Si vous n'avez pas configuré les informati ons d'identification de	Découverte de bases de données Oracle

Date	Titre	Description	Liens
		la base de données, l'outil revient à OS-level la détection. Toutes les versions d'Oracle sont prises en charge.	
22/06/2026	Soutien de la région Amérique du Sud (São Paulo) aux agents de modernisation des ordinateurs centraux	AWS Transform pour les agents de modernisation des ordinateurs centraux est désormais disponible dans la région Amérique du Sud (São Paulo) (sa-east-1). Ajout de sa-east-1 aux régions prises en charge et aux tables d'inférence interrégionales.	Régions prises en charge, Cross-region inférence
22/06/2026	AWS Transform for migrations prend en charge la localisation	AWS Transform for migrations prend désormais en charge la localisation. Vous pouvez modifier la langue d'affichage de l'application Web lorsque vous utilisez des flux de migration VMware en choisissant l'icône Paramètres et en sélectionnant la langue de votre choix.	Paramètres de localisation

Date	Titre	Description	Liens
18/06/2026/06	AWS Transform for migrations soutient toutes les régions AWS commerciales en tant que cibles de migration	AWS Transform for migrations prend en charge toutes les régions AWS commerciales en tant que cibles de migration, à l'exception du Moyen-Orient (Bahreïn) et du Moyen-Orient (Émirats arabes unis). Une région cible de migration est la AWS région dans laquelle les ressources migrées sont déployées, y compris les zones d'atterrissage, l'infrastructure réseau et le réhébergement des serveurs.	Régions cibles de migration prises en charge

Date	Titre	Description	Liens
18/06/2026/06	AWS Transform for migrations vous permet de joindre des ENI existants à votre modèle de lancement	AWS Transform vous permet d'associer des interfaces réseau élastiques (ENI) existantes à votre modèle de lancement pour votre migration . AWS Transform affiche tous les ENI existants trouvés dans votre compte cible, et vous pouvez les baliser afin qu'ils puissent être utilisés via la configuration de lancement lorsque les instances sont lancées.	Marquage des ressources ENI pour la migration
18/06/2026/06	AWS Transform for migrations vous permet de configure r les paramètres de réplication et de lancement	AWS Transform vous permet de configure r vos paramètre s de réplication et de lancement pour votre migration. Vous pouvez définir la configuration en fonction de votre compte cible ou en fonction de serveurs sources spécifiques.	Paramètres de réplication et de lancement

Date	Titre	Description	Liens
17/06/2020	Model-to-model évaluation de la migration pour les charges de travail génératives d'IA	AWS Transform propose désormais une transformation personnalisée de migration de modèle à modèle. La transform ation évalue vos charges de travail génératives en matière d'IA. Il produit un plan de migration pour passer de fournisseurs tiers à Amazon Bedrock. L' AI-powered agent analyse votre base de code pour identifie r chaque SDK et modèle d'IA utilisés. L'agent recueille les exigences en matière de migration au moyen de questions interactives. Il associe ensuite les modèles aux équivalents d'Amazon Bedrock grâce à des comparaisons de coûts transparentes et à des modificat ions de code prêtes à être mises en production. Prend en	Quoi de neuf ? Article, Transformations personnalisées

Date	Titre	Description	Liens
		charge les migration s depuis OpenAI, Google Gemini, l'utilisation directe du SDK Anthropic et les modèles open source via LiteLM ou Ollama. Gère les intégrations directes du SDK et les modèles encapsulé s dans un framework LangChain LlamaInde x, y compris CrewAI et les couches de routage multifour nisseurs. LangGraph Disponible sans frais supplémentaires au-delà de la tarificat ion standard de AWS Transform.	

Date	Titre	Description	Liens
16/06/2026	AWS Transform for mainframe permet de réinventer le flux de travail traçable	AWS Transform for mainframe propose désormais une expérienc e de réinvention connectée et traçable, de l'évaluation à la génération de code. Les entreprises utilisant z/OS COBOL et PL/I des charges de travail peuvent évaluer leur portefeui lle afin d'identifier des fonctions métier distinctes, d'extrair e des règles métier, de générer des exigences prêtes au développement et de produire du code natif cloud traçable dans un flux de travail connecté unique. Chaque exigence remonte au code source pour une auditabilité complète.	Quoi de neuf ? Article, Documentation

Date	Titre	Description	Liens
16/06/2026	AWS Transform prend désormais en charge Amazon FSx pour NetApp ONTAP en tant que stockage cible (version préliminaire publique)	Vous pouvez désormais migrer les charges de travail de stockage par blocs vers Amazon FSx pour NetApp ONTAP en plus d'Amazon EBS dans le cadre du réhébergement informatique. AWS Transform réplique les données de stockage par blocs directement sur les volumes FSx pour ONTAP au cours de la même vague de migration qui gère le calcul et le réseau.	Quoi de neuf ? Article, Documentation

Date	Titre	Description	Liens
05/06/2026	Assistance à l'évaluation du coût total de possession d'Amazon RDS pour SQL Server	Vous pouvez désormais estimer les coûts liés à la migration de bases de données SQL Server locales vers Amazon RDS pour SQL Server. Utilisez l'évaluation du AI-powered coût total de possession de AWS Transform pour analyser votre environnement et obtenir des recommandations d'instance de base de données optimales. L'évaluation prend en charge les options Bring Your Own Media (BYOM) et License Included (LI) avec des plans d'économie de base de données permettant d'économiser jusqu'à 20 %.	Quoi de neuf ? Article, Documentation

Date	Titre	Description	Liens
04/06/2026	AWS L'outil Transform Discovery est désormais pris en charge en tant que source d'entrée pour la migration réseau	Vous pouvez désormais utiliser l'outil de découvert e AWS Transform comme source de migration réseau aux côtés de ModelizeI T, permettant ainsi des migrations de réseaux hybrides pour les environne ments exécutant à la fois des charges de travail VMware et non VMware.	Guide de l'utilisateur
27/05/2026	AWS La documenta tion personnalisée de Transform ajoute des exemples de compétences et des meilleures pratiques côté client	La documentation sur les compétences côté client comprend désormais des exemples pratiques sur la conformité à Dockerfile, la sécurité de la migration des bases de données, l'application des politiques Terraform et les aides à la dépréciation des API, ainsi que les meilleures pratiques pour développe r et partager des compétences.	Documentation

Date	Titre	Description	Liens
22/05/2026	De nouvelles fonctionnalités d'évaluation de la migration des agences sont désormais disponibles avec Transform AWS	AWS Transform propose désormais des fonctionn alités avancées d'évaluation de la migration, notamment des scénarios hypothétiques, des hypothèses personnal isables, une prise en charge flexible des formats de fichiers et de nombreuses nouvelles fonctionn alités d'évaluation du coût total de possession (TCO).	Quoi de neuf ? Article, Documentation
20/05/2026	AWS Transform détecte les VPC existants lors de l'examen de la migration du réseau	AWS Transform détecte désormais les VPC existants dans votre compte cible lors de l'examen de la migration du réseau. Vous pouvez voir les VPC existants à côté de vos VPC mappés, identifier les conflits CIDR et les résoudre avant le déploiement.	Documentation

Date	Titre	Description	Liens
14/05/2026	AWS Les agents de transformation sont désormais disponibles dans Kiro, Claude, Cursor et Codex	AWS Les agents de transformation sont désormais accessibles via une alimentation Kiro, des plug-ins d'agent et le serveur AWS Transform MCP, ce qui permet aux développeurs d'utiliser les fonctionnalités de transformation directement depuis leur environnement de développement préféré.	Quoi de neuf ?
14/05/2026	AWS Transform présente la boîte à outils de création d'agents pour créer des agents de transformation personnalisés	Les partenaires et les clients peuvent désormais créer, partager et enregistrer des agents de transformation spécialisés à l'aide de la boîte à outils de création d'agents Kiro power, qui intègre des outils et des flux de travail personnalisés à AWS Transform.	Quoi de neuf ?

Date	Titre	Description	Liens
14/05/2026	AWS Transform ajoute un assistant d'IA agentic à la AWS boîte à outils pour Visual Studio	Les développeurs .NET peuvent désormais moderniser les applications grâce à une expérience conversationnelle guidée étape par étape directement dans Visual Studio, tout en préservant l'intégralité du contexte dans l'IDE et la console Web.	Quoi de neuf ?
14/05/2026	AWS Transform prend désormais en charge les boutiques d'artefacts appartenant à des clients	Vous pouvez configurer votre propre compartiment Amazon S3 et éventuellement chiffrer les artefacts avec votre propre clé AWS KMS, ce qui vous permet de contrôler totalement l'emplacement de stockage des artefacts de transformation.	Article des nouveautés, Guide de l'utilisateur

Date	Titre	Description	Liens
14/05/2026	AWS Transform ajoute des recommandations en matière de stratégie de migration (7R)	Avec AWS Transform , vous pouvez désormais analyser l'inventaire que vous avez découvert et obtenir une recommandation de stratégie de migration pour chaque serveur et chaque applicati on. Les recommand ations suivent les sept stratégies de migration (7R) standard du secteur. Chaque recommand ation comprend un service AWS cible suggéré, un score de confiance et le raisonnement qui le sous-tend. Vous pouvez générer un tableau de bord HTML interactif, un PDF ou une PowerPoint sortie Microsoft.	Recommandations des 7R

Date	Titre	Description	Liens
11/05/2026	AWS Transform ajoute une fonctionnalité de conteneurisation lors des migrations	AWS Transform prend désormais en charge le reformatage des applications vers des conteneurs pendant la migration, l'automatisation de la génération de Dockerfile, la création d'images de conteneurs à l'aide de la numérisation CVE et le déploiement sur Amazon ECS ou Amazon EKS.	Article des nouveautés, Guide de l'utilisateur
01/05/2026	AWS Transform propose désormais des agents de migration BI pour Power BI et Tableau vers Quick	Partner-built les agents de Wavicle Data Solutions convertissent les tableaux de bord Power BI et Tableau en actifs rapides dans le cadre du flux de travail AWS Transform.	Quoi de neuf ?
21/04/2026	AWS Transform custom est désormais disponible dans six AWS régions supplémentaires	AWS Transform custom s'étend à l'Asie-Pacifique, au Canada et à l'Europe (Londres), pour atteindre un total de huit AWS régions.	Quoi de neuf ?

Date	Titre	Description	Liens
15/04/2026	AWS Transform ajoute la création de zones d'atterrissage aux flux de migration	Ajout de la création de zones d'atterrissage directement dans les flux de migration . AWS Transform vérifie la présence d'une base existante , recommande des structures d'unités organisationnelles (OU) et des comptes cibles, et propose un déploiement entièrement automatisé ou une sortie d'infrastructure en tant que code (IaC) (CloudFormationformats AWS CDK ou Landing Zone Accelerator (LZA)).	Quoi de neuf ? Article, Documentation

Date	Titre	Description	Liens
15/04/2026	AWS Transform ajoute des diagrammes et des rapports de planification de la migration	Vous pouvez désormais générer des diagrammes interactifs et des rapports analytiques lors de la planification de la migration. Les types de diagrammes incluent les cartes de topologie du réseau, les graphiques de dépendance des applications, les diagrammes de Gantt ondulatoires et les diagrammes généraux. Les types de rapports incluent les évaluations des risques, les recommandations 7R et les rapports analytiques personnalisés. Les sorties sont disponibles sous forme de fichiers HTML, PDF ou Microsoft PowerPoint (.pptx) interactifs.	Création de diagrammes et rapports

Date	Titre	Description	Liens
14/04/2026	AWS Transform est désormais disponible dans Kiro et VS Code	AWS Les transform ations personnalisées de Transform sont désormais accessibl es depuis Kiro et VS Code, l'état des tâches étant partagé entre l'IDE, la CLI et les surfaces de console Web.	Quoi de neuf ?
10/04/2026	AWS Transform ajoute le protocole DHCP avec mappage des groupes de sécurité pour la migration du réseau	Ajout de la prise en charge du protocole DHCP avec mappage des groupes de sécurité lors de la migration du réseau. Si vous avez des charges de travail liées à la DHCP-enab led migration, vous pouvez désormais vous assurer que vos règles de sécurité restent valides après la migration. Cela s'applique à la fois au référencement des groupes de sécurité intégrés au VPC et aux règles sortantes entre VPC et entre comptes via Transit Gateway.	Documentation

Date	Titre	Description	Liens
31/03/2020	AWS Transform Custom annonce la disponibilité générale de l'analyse automatisée de la base de code	La transformation complète de l'analyse de la base de code atteint la disponibilité générale, générant des documents d'architecture, des rapports de dette technique et des recommandations de modernisation dans n'importe quelle langue.	Quoi de neuf ?
31/03/2020	AWS Transform Custom introduit de nouvelles transformations gérées pour moderniser le code à grande échelle	Sept nouvelles transformations gérées ont été ajoutées, notamment les Node.js mises à niveau (disponibilité générale), l'optimisation Java, la migration Log4j Angular-to-React, les mises à niveau Angular et les mises à niveau Vue (accès anticipé).	Quoi de neuf ?

Date	Titre	Description	Liens
20/03/2026	AWS Transform ajoute des API publiques pour la migration du réseau	Ajout d'API publiques pour la migration du réseau, permettant aux partenaires et aux programmeurs d'accéder aux fonctionnalités de migration du réseau.	API Reference
14/01/2026	AWS Transform Custom ajoute AWS PrivateLink du support et s'étend à l'Europe (Francfort)	AWS Transform Custom prend désormais en charge l'accès privé aux VPC via AWS PrivateLink et est disponible en Europe (Francfort) ainsi qu'aux États-Unis (Virginie du Nord).	Quoi de neuf ?
23/12/2025	AWS Transform permet la conversion réseau pour les migrations de centres de données hybrides	AWS Transform for VMware convertit automatiquement les configurations réseau des centres de données hybrides (VLAN, plages IP) en AWS VPC, sous-réseaux et groupes de sécurité sans mappage manuel.	Quoi de neuf ?

Date	Titre	Description	Liens
01/12/2025	AWS lance AWS Transform custom pour accélérer la modernisation à l'échelle de l'organisation	AWS Transform Custom atteint la disponibilité générale, permettant aux entreprises d'automatiser les transformations de code répétables à grande échelle via une seule commande CLI.	Quoi de neuf ?
01/12/2025	AWS Transform ajoute de nouvelles fonctionnalités d'IA agentique pour les migrations VMware d'entreprise	AWS L'agent VMware de Transform peut désormais découvrir les environnements sur site, cartographier les dépendances, générer des plans de vagues de migration et migrer vers des cibles HyperV, Nutanix, KVM et bare-metal.	Quoi de neuf ?

Date	Titre	Description	Liens
01/12/2025	AWS Transform lance un agent d'IA pour une modernisation complète de Windows	Un nouvel agent Windows complet automatise la transformation des applications .NET et des bases de données SQL Server vers Aurora PostgreSQL, en les déployant sur des conteneurs sur Amazon ECS ou EC2 Linux.	Quoi de neuf ?
01/12/2025	AWS Transform étend les capacités de transformation de .NET et améliore l'expérience des développeurs	AWS Transform ajoute la prise en charge de .NET 10, le portage de formulaires ASP.NET Web vers Blazor et une expérience IDE interactive améliorée via AWS Toolkit pour Visual Studio.	Quoi de neuf ?

Date	Titre	Description	Liens
01/12/2025	AWS Transform for mainframe offre de nouvelles fonctionn alités d'automatisation des tests	AWS Transform for mainframe introduit la génération automatiq ue de plans de test, des scripts de collecte de données de test et l'automatisation des scénarios de test afin d'accélérer les tests de modernisation du mainframe.	Quoi de neuf ?
01/12/2025	AWS Transform for mainframe permet désormais de réimaginer les applications	De nouvelles analyses de données et d'activités ainsi que des fonctionn alités d'extract ion de la logique métier permetten t de décompose r les applications mainframe existantes en architectures cloud natives.	Quoi de neuf ?

Date	Titre	Description	Liens
13/11/2025	AWS Transform automatise la configuration du réseau de Landing Zone Accelerator	AWS Transform for migrations génère automatiquement des fichiers LZA-compatible réseau YAML, rationalisant ainsi la configuration de l'infrastructure cloud multi-comptes à partir des environnements VMware.	Quoi de neuf ?
16/07/2025	AWS Transform for mainframe introduit des fonctionnalités améliorées de refactorisation du code et de logique métier	AWS Transform for mainframe ajoute la disponibilité générale de la reforge (restructuration du code) et une extraction étendue de la logique métier au niveau des applications afin d'améliorer la qualité du code.	Quoi de neuf ?
15/05/2025	AWS Transform pour VMware est désormais disponible pour tous	AWS Transform for VMware, un service d'IA agentique qui automatise l'intégralité du cycle de vie de modernisation de VMware, de la découverte au déploiement, est désormais disponible pour tous.	Quoi de neuf ?

Date	Titre	Description	Liens
15/05/2025	AWS Transform pour mainframe est désormais disponible pour tous	AWS Transform for mainframe, le premier service d'IA agentique destiné à moderniser les z/OS applications IBM à grande échelle, atteint la disponibi lité générale avec de nouvelles fonctionn alités d'analyse, de décomposition et de gestion des tâches.	Quoi de neuf ?

Téléchargez ces données.

Historique des documents pour AWS Guide de l'utilisateur de Transform

Le tableau suivant décrit l'historique des documents du guide de l'utilisateur de AWS Transform.

Modification	Description	Date
La migration réseau ajoute la suppression des règles de groupe de sécurité obsolètes	Les recommandations réseau guidées peuvent désormais identifier les règles de pare-feu entrantes non utilisées migrées depuis votre environnement sur site et suggérer de les supprimer. Consultez la section Recommandations relatives au réseau guidé.	16 août 2026
La rubrique Connecteurs a été déplacée vers Mise en route	La rubrique Connecteurs a été déplacée de la navigation de niveau supérieur à la section Getting started. Voir Connecteurs.	8 août 2026
La modernisation continue ajoute l'exécution AWS Transform-managed à distance	La modernisation continue permet désormais d'effectuer des analyses sur AWS Transform-managed l'infrastructure sans rien provisionner sur votre compte, en utilisant `atx ct remote analysis --mode aws-managed` . Vous pouvez également planifier des analyses récurrentes qui s'exécutent sur AWS Transform-managed	7 août 2026

	l'infrastructure sans Amazon EventBridge. Consultez la section Options de calcul.	
La modernisation continue ajoute l'exécution, la planification et le balisage à distance	La modernisation continue inclut désormais des `atx ct remote` commandes pour provisionner et exécuter des analyses et des corrections sur Amazon EC2 ou AWS Batch, des `atx ct schedule` commandes pour exécuter des analyses récurrentes avec Amazon EventBridge Scheduler et le balisage des ressources pour le contrôle d'accès basé sur les attributs (ABAC). Les nouvelles politiques AWS gérées prennent en charge l'exécution des agents de sécurité et à distance avec le moindre privilège. La `atx ct server` commande est obsolète. Consultez la section Travailler dans le cadre de la modernisation continue.	28 juillet 2026
Modernisation continue, analyse et remédiation du portefeuille	Ajout d'un nouveau chapitre documentant la fonctionnalité de modernisation continue de AWS Transform (`atx ct`sous-commandes) pour l'analyse et la correction automatisées du code. Voir Modernisation continue.	3 juin 2026

Réseau Brownfield : visibilité des VPC existants	Ajout de la détection VPC existante lors de l'examen de la migration du réseau. AWS Transform détecte automatiquement les VPC déjà déployés sur votre compte cible et signale les conflits d'adresse CIDR avec vos VPC mappés. Consultez les VPC existants dans votre compte cible.	18 mai 2026
Ajout d'un format de compétences, de compétences côté client et de journaux de sous-agents pour Transform custom AWS	Les définitions de transformation utilisent désormais le format skills (`SKILL.md`avec le frontmatter YAML et `references/` le dossier optionnel). Ajout de compétences côté client pour étendre l'agent avec des fonctionnalités supplémentaires, et de journaux de sous-agent pour améliorer le débogage. Nécessite la version 2.0 ou ultérieure de la CLI. Voir Définitions et Client-Side compétences en matière de transformation.	11 mai 2026

Ajout de la conteneurisation du code source	AWS Transform peut désormais conteneuriser vos applications grâce à l'IA générative. Fournissez votre code source à partir de référentiels Git ou de téléchargements zip, et AWS Transform l'analyse, génère des artefacts Docker, publie des images de conteneurs sur Amazon ECR, génère une infrastructure sous forme de code et déploie sur Amazon Elastic Container Service ou Amazon Elastic Kubernetes Service. Voir Conteneurisation du code source.	7 mai 2026
Ajout d'opérations d'optimisation du réseau et de recommandations guidées	Ajout de l'étape 5 : examiner et optimiser le réseau, avec les opérations relatives au VPC et aux sous-réseaux (supprimer, exclure, fusionner, scinder, redimensionner, renommer, modifier l'adresse IP) et des recommandations guidées pour la normalisation de la dénomination, la révision de la portée, le redimensionnement des capacités, l'examen de la sécurité et la consolidation des VPC. Consultez la section Révision et optimisation du réseau.	27 avril 2026

AWS Transform custom disponible dans 6 nouvelles régions	Ajout du support pour ca-central-1, eu-west-2, ap-northeast-1, ap-northeast-2, ap-southeast-2 et ap-south-1 dans Transform custom. AWS	21 avril 2026
Documentation sur les autorisations des connecteurs mise à jour	Ajout d'une ventilation détaillée des autorisations pour le Compte AWS connecteur cible, couvrant les autorisations S3, MGN, Migration Hub, la migration de la charge de travail et le provisionnement de l'infrastructure de la zone de destination. Voir Connecter Compte AWS les cibles s.	19 avril 2026
Types de tâches de migration VMware mis à jour	Ajout des types de tâches de planification de la découverte et de la migration, de zone d'atterrissage et de zone d'atterrissage, de réseau et de serveur. Migration réseau renommée uniquement en Migration réseau et planification de la migration en Build migration plan. Consultez les types de tâches de migration vers VMware.	19 avril 2026

Compte AWS Cibles Connect restructurées	Restructuration de la configuration du connecteur en trois étapes : sélection du type de migration, accord MAP et configuration du connecteur, y compris les régions cibles prises en charge, les rôles de compte, les conseils d'administrateur délégué et les rôles IAM. Voir Connecter Compte AWS les cibles s.	19 avril 2026
Ajout de régions cibles supplémentaires réservées à la migration de serveurs	14 régions commerciales supplémentaires documentées sont disponibles pour les tâches de migration de serveurs sans migration de réseau, avec une liste d'autorisation requise jusqu'au troisième trimestre 2026. Voir Régions cibles prises en charge.	19 avril 2026
Ajout du chapitre sur la migration des serveurs	Ajout d'un nouveau chapitre sur les serveurs Migrate couvrant l'ensemble du flux de travail de réhébergement, y compris la structure des comptes, les rôles IAM, la configuration des administrateurs délégués, le déploiement de l'agent de réplication, les tests et le basculement.	19 avril 2026

Ajout du chapitre « Construire une zone d'atterrissage »	Ajout d'un nouveau chapitre sur la création d'une zone d'atterrissage avec les détails des autorisations des connecteurs pour l'approvisionnement de la zone d'atterrissage.	19 avril 2026
Cartographie et référencement des groupes de sécurité	Ajout de stratégies de mappage des groupes de sécurité (MAP, MAP_DHCP, SKIP) et de la documentation de référencement des groupes de sécurité au réseau Migrate. https://docs.aws.amazon.com/transform/latest/userguide/transform-vmware-migrate-network.html	13 avril 2026
Auto-conversion pour les types de fichiers réseau non pris en charge	Ajout de la prise en charge de la conversion automatique des types de fichiers de configuration réseau non pris en charge dans Migrate network.	6 avril 2026
Ajout d'une politique clé KMS pour la migration de base de données	Ajout de la section Chiffrement pour la migration des bases de données.	26 mars 2026
Nouvelle politique AWS gérée documentée	DBModProvisioningAndMigrationSection ajoutée.	24 mars 2026
Nouvelle politique AWS gérée documentée	DBModDiscoveryAndAssessmentSection ajoutée.	24 mars 2026

Génération de diagrammes de réseau	Ajout de la génération optionnelle de diagrammes de réseau (formats Mermaid et PNG) au réseau https://docs.aws.amazon.com/transform/latest/userguide/transform-vmware-migrate-network.html Migrate.	18 mars 2026
Prise en charge du pare-feu et des fichiers de configuration SDN	Ajout de la prise en charge des fichiers de configuration Palo Alto Networks FortiGate , Fortinet et Cisco ACI pour la migration du réseau dans le réseau Migrate.	11 février 2026
Balisage personnalisé pour les ressources réseau	Ajout de la prise en charge du balisage VPC-level personnalisé et au niveau de la tâche pour la migration du réseau dans le réseau Migrate.	28 janvier 2026
Documentation d'assistance ajoutée	Ajout AWS du support pour la section.	23 décembre 2025
Nouvelles politiques AWS gérées documentées	Ajout AWSTransformCustomFullAccess AWSTransformCustomExecuteTransformations de AWSTransformCustomManageTransformations sections et.	7 décembre 2025
Migration vers VMware	Mise à jour de la section sur la migration vers VMware.	1er décembre 2025

Politique AWS gérée mise à jour	Mise à jour de la AWSServiceRoleForAWSTransform documentation pour refléter les autorisations supplémentaires.	1er décembre 2025
Régions prises en charge	Mise à jour de la rubrique Régions prises en charge.	1er décembre 2025
Modernisation du mainframe	Mise à jour de la section sur la modernisation de l'ordinateur central.	1er décembre 2025
Mise en route	Mise à jour de la rubrique Getting Started.	1er décembre 2025
Full-stack Modernisation de Windows	Ajout de la rubrique relative à la modernisation de Full-stack Windows, qui inclut la section .NET mise à jour et la nouvelle section relative à la modernisation de SQL Server.	1er décembre 2025
Outil de découverte	Ajout de la section Outil de découverte.	1er décembre 2025
Politique AWS gérée mise à jour	Mise à jour du AWSTransformApplicationECSDeploymentPolicy avec des autorisations étendues d'inspection des rôles IAM, la création de rôles liés aux services ECS et des autorisations KMS pour la prise en charge du chiffrement ECR.	22 novembre 2025

Politique AWS gérée mise à jour	Mise à jour du AWSTransformApplicationDeploymentPolicy avec une mise en réseau EC2 supplémentaire, une inspection des rôles IAM, une gestion des compartiments S3 et des autorisations de chiffrement KMS supplémentaires.	22 novembre 2025
Collectionneur Discovery	Ajout de l'outil de découverte AWS Transform > documentation.	31 octobre 2025
Schéma d'architecture de migration VMware ajouté	Ajout d'un schéma d'architecture de migration VMware dans le réseau Migrate.	23 octobre 2025
Mise à jour des résultats de migration vers VMware	Informations sur les résultats de migration mises à jour dans le réseau Migrate.	12 octobre 2025
Mise à jour des résultats de migration vers VMware	Informations sur les résultats de migration mises à jour dans le réseau Migrate.	12 octobre 2025
Documentation sur le connecteur S3	Ajout de la documentation du connecteur S3 pour l'application Web .NET.	8 octobre 2025
Nouveau sujet relatif aux connecteurs utilisateurs	Ajout d'une rubrique sur les connecteurs utilisateur.	21 septembre 2025
Politique AWS gérée mise à jour	Mise à jour de AWSServiceRoleForAWSTransform la documentation.	17 septembre 2025

Assistance à l'évaluation du stockage	Ajout de la prise en charge des fichiers NetApp Data Infrastructure Insights (DII) pour les évaluations du stockage.	2 septembre 2025
Mise à jour des régions cibles	Ajout de trois régions cibles prises en charge.	31 août 2025
Mise à jour de politique gérée	Ajout d'autorisations en lecture seule à IAM Identity Center à utiliser par. AWSServiceRoleForAWSTransform	29 août 2025
Nouvelle politique AWS gérée documentée	AWSTransformApplicationDeploymentPolicySection ajoutée.	28 août 2025
points de terminaison de l'interface	Ajout d'une rubrique sur les points de terminaison d'interface.	9 juillet 2025
Première version	Publication initiale du guide de l'utilisateur de AWS Transform.	15 mai 2025

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.