



Guida per l'utente

AWS Trasformazione



AWS Trasformazione: Guida per l'utente

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è AWS Trasformare?	1
Terminologia	1
Nozioni di base	4
Configurazione	4
Prima di iniziare	4
Iscriviti per un Account AWS	4
Iniziare con IAM-only l'accesso	4
Utilizzo delle credenziali IAM	5
Nozioni di base su AWS Organizations	6
Nozioni di base su Centro identità AWS IAM	7
Utilizzo di provider di identità di terze parti	8
Onboarding	11
Usando il tuo bucket S3	12
Attiva AWS Trasformazione	21
Avvio rapido: sto provando AWS Trasformazione	23
Gestione degli utenti	23
Aggiungere utenti in IAM Identity Center	23
Aggiungere utenti a AWS Trasformazione	24
Gestione degli utenti con accesso IAM-only	25
Comprensione delle autorizzazioni dei collaboratori	25
AWS Trasforma l'ambiente	28
Impostazioni della lingua	29
Inizia il tuo progetto	30
AWS Trasforma la chat	31
Strumenti per sviluppatori	33
Kiro Power	33
Plugin Agent	33
Plugin IDE	34
Server MCP	34
Autenticazione	35
Crea agenti personalizzati per AWS Trasformazione	35
Valutazioni della migrazione	37
Prerequisiti	37
Come funzionano le valutazioni della migrazione	37

Caricamento dei dati di inventario	38
Revisione dei risultati della scoperta	39
Gestione dell'ambito dell'inventario	39
Configurazione degli scenari di valutazione	39
Funzionalità di valutazione	40
Amazon EC2 dimensionamento corretto	40
Archiviazione Amazon EBS	40
Amazon FSx	40
Amazon RDS per SQL Server	41
Server SQL Amazon EC2	41
On-premises prezzi	42
Sostenibilità	42
Valutazione del valore aziendale	42
Costi di rete	42
Costi di supporto	43
Elaborazione degli utenti finali	43
Utilizzo di valutazioni basate su chat	43
Stima approssimativa con dati limitati	43
Aggiungere l'inventario tramite chat	43
Modifica dei costi e aggiunta di servizi	44
Scenari a confronto	44
Creazione di scenari	44
Esecuzione di confronti	44
What-if analisi	45
Generazione di risultati	45
Argomenti correlati	45
Personalizzato	47
Che cos'è AWS Trasformazione personalizzata?	47
Funzionalità chiave	47
Modelli di trasformazione	47
In che modo AWS Transform Custom Works	50
Comprensione dei concetti chiave di	50
Definizioni di trasformazione	50
Registro delle trasformazioni	51
Bozza e trasformazioni pubblicate	52
Riferimenti vs. lezioni	52

Comandi di creazione e convalida	53
Apprendimento continuo	53
Client-Side Competenze	54
Nozioni di base	54
Prerequisiti	55
Installazione di AWS Trasforma CLI	55
Configurazione dell'autenticazione	56
Configurazione AWS Region	58
Esecuzione della prima trasformazione	62
Comprensione dei risultati della trasformazione	62
Creazione di una trasformazione personalizzata	62
AWS Transform Web Application (opzionale)	63
Introduzione ai comandi di trasformazione personalizzati	64
Flussi di lavoro	65
Esecuzione di trasformazioni	65
Apprendimento continuo	70
Configurazione avanzata	71
Crea trasformazioni personalizzate	85
Riferimento ai comandi	89
Comandi interattivi	89
Comandi di definizione della trasformazione	89
Comandi della lezione	93
Comandi per tag	94
Comandi di aggiornamento	94
Comandi MCP	94
AWS-Trasformazioni gestite	95
Panoramica di	95
Disponibilità AWS-Trasformazioni gestite	95
Personalizzazione AWS-Trasformazioni gestite	112
Casi di utilizzo comune	112
Aggiornamenti Lambda Runtime	112
Endpoint VPC (AWS PrivateLink)	114
Considerazioni per AWS Transform endpoint VPC personalizzati	115
Prerequisiti	115
Creazione di un endpoint VPC di interfaccia per AWS Transform personalizzato	115
Creazione di una policy per gli endpoint VPC per AWS Transform personalizzato	116

Utilizzo di un computer locale per connettersi a un AWS Transform endpoint personalizzato	116
Risoluzione dei problemi	117
Posizioni dei log	117
Problemi comuni	118
Ottenere supporto	120
Problemi di accesso a S3	120
Cronologia delle versioni CLI	121
Modernizzazione continua	131
Che cos'è AWS Trasformare la modernizzazione continua?	131
Funzionalità chiave	131
Tipi di analisi	132
Comprensione dei concetti chiave	133
Origini	133
Repositories	133
Analisi	134
Esiti	134
Correzioni	134
Definizioni di trasformazione	134
In che modo AWS Trasforma i lavori di modernizzazione continua	134
Opzioni di calcolo	135
Configurazione del Security Agent	137
Nozioni di base	138
Prerequisiti	138
Avvio rapido	138
Lavorare con una modernizzazione continua	139
Gestione delle fonti	139
Individuazione e gestione dei repository	140
Analisi in corso	141
Gestione degli esiti	141
Creazione di soluzioni correttive	142
AWS Trasforma l'applicazione web (opzionale)	143
Strumenti per sviluppatori	144
Competenze dell'agente	144
Documentazione di riferimento della CLI	145
Risoluzione dei problemi	147

Strumento di scoperta	149
Flusso di lavoro	149
Configurare lo strumento di scoperta	150
Prerequisiti	150
Implementa su VMware	152
Implementa su Hyper-V	154
Implementa su Linux	154
Configura lo strumento di rilevamento	157
Autorizzazioni richieste	170
VMware vCenter	170
Hyper-V host (Windows)	171
Server Linux (SSH)	172
Server Windows (WinRM) — metriche del sistema operativo	173
Server Windows (WinRM): raccolta SQL Server	175
Database Oracle (SQL)	176
Raccolta di rete	176
Riferimento rapido: autorizzazioni minime per caso d'uso	177
Raccolta dei dati	178
Programma di raccolta	178
Inventario scoperto	179
OS-related dati	184
Considerazioni relative alla sicurezza	204
Protezione della VM dello strumento di rilevamento	204
Protezione delle credenziali	204
Archiviazione delle credenziali	206
Usare Auto-Connect la funzionalità con cautela	206
Sicurezza di importazione CSV	208
Considerazioni sulla revoca dell'accesso	208
Risolvi i problemi relativi allo strumento di rilevamento	208
Verifica della connettività degli strumenti di rilevamento a vCenter	208
Risoluzione dei problemi WinRM	210
Risoluzione dei problemi Kerberos	211
Risoluzione dei problemi del database Orac	215
Risoluzione dei problemi SNMP	216
Errori di raccolta in rete	217
Errori di raccolta delle metriche del sistema operativo	218

Problemi di accesso nell'inventario Discovered	218
Risoluzione dei problemi di autenticazione tramite chiave SSH	219
Risoluzione dei problemi del programma di installazione Linux	220
Messaggi di errore comuni	220
Note di rilascio	221
Connettori	226
Tracciabilità degli utenti per le operazioni agentiche	226
Gestione dei connettori	228
Migrazioni (incluso VMware)	230
Funzionalità e caratteristiche principali	230
Architecture	230
Lavori di migrazione	231
Ottenere uno spazio di lavoro	231
Tipi di Job	232
Creazione e avvio di un lavoro	233
Scaricare un rapporto di riepilogo sull'area di lavoro	233
Limitazioni	234
Scopri i dati di origine	234
Crea un piano di migrazione	235
Flusso di lavoro	237
Raccomandazioni 7Rs	239
Diagrammi e report	240
Connect target Account AWS s e regioni	241
Fase 1: Selezione del tipo di migrazione	242
Fase 2: accordo MAP	242
Fase 3: Configurazione del connettore	242
Costruisci una landing zone	249
Configurazione del connettore	249
Configurazione Foundation	250
Progettazione dell'account Workload	254
Formati IAc	256
Processo di approvazione dell'implementazione	257
Etichetta: risorse per le landing zone	257
Inversione delle modifiche	258
Risorse correlate	258
Migra la tua rete a AWS	258

Fase 1: Mappatura della rete di origine	259
Fase 2: File di configurazione aggiuntivi	260
Fase 3: Topologie di rete	261
Fase 4: Mappatura dei gruppi di sicurezza	264
Fase 5: Rivedi e ottimizza la tua rete	267
Fase 6: Diagramma reticolare	271
Fase 7: Configurare la codifica delle risorse	271
Fase 8: Implementa la rete	273
Elimina le risorse di rete distribuite	274
Estrazione del file di configurazione	275
Migrazione dei server	276
Prerequisiti e configurazione delle impostazioni predefinite di migrazione	277
Passaggio 1: configurare l'ondata di migrazione	279
Fase 2: Convalida e conferma dell'inventario	282
Fase 3: Implementazione degli agenti di replica	284
Fase 4: Replica dei dati	291
Fase 5: Test	292
Fase 5b: Contrassegna le applicazioni come pronte per il cutover	292
Fase 6: Cutover	292
Stati del ciclo di vita del server	293
Approvazioni di implementazione	294
Note di rilascio	294
giugno 2026	294
Maggio 2026	295
Aprile 2026	295
Marzo 2026	295
febbraio 2026	296
gennaio 2026	296
dicembre 2025	296
Ottobre 2025	296
settembre 2025	296
agosto 2025	297
Maggio 2025	297
Containerizzazione del codice sorgente	298
Funzionalità e caratteristiche principali	298
Come funziona la containerizzazione	299

Prerequisiti	299
Flusso di lavoro di containerizzazione	300
Avvio di un processo di containerizzazione	300
Permissions	301
Politica di base	301
Politica di rete	302
Politica di archiviazione	302
AWS KMS policy	302
Politica di Amazon ECS	302
Politica di Amazon EKS	303
Fase 1: Dichiarazione di non responsabilità in materia di sicurezza	303
Cosa copre il disclaimer	303
Cosa devi fare tu	304
Fase 2: clonare il codice sorgente	304
Opzione 1: repository Git	304
Opzione 2: caricamento di file zip	305
Facoltativo: configura le dipendenze private	306
Conferma delle preferenze di containerizzazione	306
Fase 3: Containerizzazione	307
Cosa succede durante la containerizzazione	307
Tipi di applicazioni supportati	307
Cosa devi fare tu	308
Fase 4: Esamina gli artefatti	308
Revisione delle modifiche dai repository Git	308
Revisione delle modifiche apportate ai carichi in formato zip	308
Richiesta di modifiche	309
Fase 5: Pubblicare immagini	309
Cosa succede durante la pubblicazione	309
Cosa devi fare tu	309
Fase 6: Generazione di IaC	310
Servizio Amazon Elastic Kubernetes (Kubernetes)	310
Amazon Elastic Container Service (Terraform)	311
Convalida e scansione di sicurezza automatizzate	311
Generazione di IaC senza immagini pubblicate	311
Cosa devi fare tu	312
Fase 7: Implementazione dell'infrastruttura di test	312

Cosa succede durante l'implementazione dei test	312
Cosa devi fare tu	313
Iterazione sull'infrastruttura	313
Ripristino della sessione	313
Fase 8: Pulizia dell'infrastruttura di test	314
Cosa devi fare tu	314
Fase 9: Implementazione dell'infrastruttura cutover	314
Cosa devi fare tu	314
Ripristino della sessione	315
Modernizzazione del mainframe	316
Funzionalità e caratteristiche principali	316
High-level guida dettagliata	317
Human in the loop (HITL)	317
Tipi di file supportati per la trasformazione delle applicazioni mainframe	318
Regioni e quote supportate per AWS Trasforma il mainframe	318
Percorso di modernizzazione	319
Fase 1: valutazione	319
Fase 2: Mobilitazione	320
Fase 3: migrazione e modernizzazione	321
Fase 4: gestione, ottimizzazione e innovazione	323
Trasformazione del flusso di lavoro delle applicazioni mainframe	323
Prerequisito: preparare gli input del progetto in S3	324
Raccolta di artefatti sorgenti per mainframe	325
Sign-in e crea un lavoro	334
Monitoraggio dei progressi della trasformazione	334
Configura un connettore	335
Valuta e reinventa il piano di lavoro	339
Reinventa il piano di lavoro	344
Piano di lavoro personalizzato	345
Crea e distribuisce un'applicazione modernizzata	375
Prerequisiti	376
Fase 1: Recuperare il codice modernizzato	377
Fase 2: Creazione dell'applicazione modernizzata	377
Fase 3: Configurazione dell'ambiente di test	378
Fase 4: Implementazione dell'applicazione modernizzata	379
Fase 5: Testare l'applicazione modernizzata	379

Esempio aggiuntivo	379
Full-stack Modernizzazione di Windows	380
.NET	380
Esperienze	380
Funzionalità e caratteristiche principali	381
Versioni e tipi di progetto supportati	381
Limitazioni	382
Intervento umano	383
Ulteriori informazioni	383
App web.NET	383
IDE.NET	400
Porting del codice di livello dell'interfaccia utente	408
Rapporti di trasformazione	411
Best practice	412
Modernizzazione di SQL Server	418
Regioni supportate	419
Funzionalità e caratteristiche principali	419
Versioni e tipi di progetto supportati	420
Requisiti di SQL Server	424
Requisiti dell'applicazione	425
Requisiti di infrastruttura	426
Requisiti del repository	426
Configurazione di SQL Server	426
AWS Configurazione della trasformazione	435
Crea un processo di modernizzazione di SQL Server	435
Flusso di lavoro di modernizzazione di SQL Server	442
Test e implementazione dopo la trasformazione	474
Best practice e risoluzione dei problemi	477
Sicurezza	482
Protezione dei dati	483
Cross-region elaborazione	484
Crittografia dei dati	493
Miglioramento del servizio	503
Gestione dell'identità e degli accessi	504
Destinatari	505
Autenticazione con identità	505

Gestione dell'accesso tramite policy	507
In che modo AWS Transform funziona con IAM	508
Identity-based esempi di politiche	514
Risoluzione dei problemi	524
Uso di ruoli collegati ai servizi	526
AWS politiche gestite	532
AWS Trasforma il riferimento alle autorizzazioni	548
Convalida della conformità	550
Resilienza	550
Endpoint VPC (AWS PrivateLink)	551
Considerazioni per AWS Transform Endpoint VPC	551
Prerequisiti	551
Creazione di un endpoint VPC di interfaccia per AWS Transform	551
Utilizzo di un computer locale per connettersi a un AWS Transform endpoint	553
Accesso tramite VPC alle applicazioni Web	553
Come funziona	553
Architecture	554
Prerequisiti	554
Configurazione della policy degli endpoint VPC	555
Configurazione dell'uscita controllata da Internet	556
Verifica	563
Risoluzione dei problemi	563
Considerazioni sui costi	564
Pulizia	565
Monitoraggio	567
CloudTrail registri	568
AWS Trasforma le informazioni in CloudTrail	568
Comprensione AWS Trasforma le voci dei file di registro	569
Notifications	569
Notifiche via e-mail	569
Quote	572
Regioni supportate	578
Supportata Regioni AWS (abilitato per impostazione predefinita)	578
Supporto	580
Prerequisiti	580
Abilitazione della gestione dei casi di supporto	580

Creazione di un Support Case	580
Visualizzazione dei casi di supporto	581
Aggiungere comunicazioni a un caso	582
Risolvere un caso	582
Disattivazione della gestione dei casi di Support	582
Telemetria di utilizzo	583
Dati operativi	584
Log delle modifiche	585
Cronologia dei documenti	609
.....	dcxviii

Che cos'è AWS Trasformare?

AWS Transform è un servizio che ti aiuta ad accelerare e semplificare la trasformazione dell'infrastruttura, delle applicazioni e del codice con un'esperienza di intelligenza artificiale agentica. Fornisce strumenti specializzati per semplificare le attività di modernizzazione e migrazione su vari carichi di lavoro.

Con AWS Transform puoi:

- Modernizza e migra IBM z/OS e Fujitsu GS21 su AWS
- Migrazione dei carichi di lavoro VMware su Amazon EC2
- Modernizza le applicazioni.NET in un formato multiplatforma Linux-ready
- Valuta i carichi di lavoro per renderli pronti alla migrazione

AWS Transform ti aiuta a delegare le attività di trasformazione complesse e laboriose nelle fasi di scoperta, pianificazione ed esecuzione ad agenti di intelligenza artificiale con esperienza in linguaggi, framework e infrastrutture. Questo approccio consente ai team di concentrarsi sull'innovazione mentre trasforma in modo efficiente progetti complessi e su larga scala attraverso un'esperienza web unificata.

Non sono previsti costi aggiuntivi per l'utilizzo di Transform. AWS

Terminology

All'interno di questa sezione, il corsivo indica un termine ufficiale all'interno della definizione di un termine diverso.

Connessione all'*account*

L'*account* in questo contesto è un riferimento generalizzato a un contenitore di proprietà del cliente o a un limite di sicurezza per le risorse AWS o il servizio remoto, ad esempio un *account* or. *Account AWS GitHub*

Artefatto

Un risultato finale prodotto da Transform. AWS

Amministratore

Gli amministratori possono leggere e modificare tutto ciò che si trova nell'area di lavoro. Possono iniziare le chat con AWS Transform, avviare e interrompere lavori e artefatti. upload/download Gli amministratori possono interagire con l'esecuzione di job for human-in-the-loop (HITL) e possono approvare azioni HITL critiche come l'unione a main, l'esecuzione della scomposizione dei grafici o la distribuzione del codice negli ambienti di produzione. [Gli amministratori possono modificare aree di lavoro, connettori e utenti.](#)

Agente

Un servizio specifico per un'attività che esegue un tipo di trasformazione specifico. Ad esempio, le migrazioni VMware.

Approvatore

Gli approvatori dispongono di autorizzazioni simili a quelle degli amministratori, tranne per il fatto che non dispongono delle autorizzazioni per modificare aree di lavoro, connettori o utenti. [Gli approvatori non possono modificare aree di lavoro, connettori o utenti.](#)

Risorsa

Input per un [lavoro di](#) trasformazione. Ad esempio, codice sorgente, server, database, rete del cliente. L'accesso alle risorse avviene tramite un [connettore](#).

Richiesta del collaboratore

Un'attività in cui AWS Transform chiede a un umano di fare qualcosa.

Connettore

I connettori sono fornitori di risorse che consentono l'accesso alle risorse di proprietà del cliente in un sistema esterno a AWS Transform.

Quando si configura un connettore, l'amministratore dell'account a cui ci si connette deve accettare la connessione. Per accettare la connessione, devono disporre delle autorizzazioni fornite nella politica di [accettazione del connettore](#).

I due account seguenti devono essere identici o appartenere alla stessa AWS Organizations organizzazione:

- L'account da cui l'amministratore di AWS Transform abilita il servizio.
- L'account che sarà il destinatario della trasformazione. A questo account deve essere assegnato un ruolo IAM che gli consenta di utilizzare un [connettore](#).

Collaboratore

I collaboratori possono leggere tutto ciò che si trova nell'area di lavoro. [Possono iniziare le chat con AWS Transform, avviare e interrompere i lavori, caricare o scaricare artefatti e interagire con i job in esecuzione per le azioni HITL](#). Tuttavia, non possono eseguire azioni HITL critiche come l'unione al file principale, la decomposizione dei grafici o l'implementazione del codice negli ambienti di produzione. [Inoltre, i contributori non possono modificare gli spazi di lavoro, i connettori o gli utenti](#).

Obiettivo

Uno stato finale definito dall'utente che AWS Transform lavora per raggiungere. Gli utenti lo scrivono, quindi AWS Transform converte l'obiettivo in una serie di attività che esegue insieme agli utenti quando necessario.

Job

Un processo di lunga durata (weeks/months+) su cui AWS Transform sta lavorando per raggiungere un [obiettivo](#) definito da un utente. Composto da più [attività](#) e richieste di [collaboratori](#).

Piano

[Un elenco di attività che AWS Transform intraprende \(con l'aiuto di utenti umani\) per perseguire un obiettivo](#).

Lettore

I lettori possono visualizzare lo stato e i risultati dei lavori AWS Transform, ma non possono apportare modifiche. Possono leggere tutto ciò che si trova nell'[area di lavoro](#), scaricare artefatti, visualizzare i [lavori](#) e visualizzare le azioni human-in-the-loop (HITL). Tuttavia, i lettori non possono eseguire azioni di mutazione in Transform. AWS

Attività

Una singola unità di lavoro che fa parte di un [lavoro](#).

Registro di lavoro

Un registro delle azioni eseguite da AWS Transform e dagli utenti nell'ambito di un [job](#).

Spazio di lavoro

Una risorsa AWS Transform che contiene altre risorse come [connettori](#) e [lavori](#). Uno [spazio di lavoro](#) funge da limite di autorizzazioni.

Nozioni di base su AWS Trasformazione

Argomenti

- [Configurazione AWS Trasformazione](#)
- [Attiva AWS Trasformazione](#)
- [Avvio rapido: sto provando AWS Trasformazione](#)
- [Gestione degli utenti](#)
- [AWS Trasforma l'ambiente](#)

Configurazione AWS Trasformazione

Prima di iniziare

Prima di configurare AWS Transform, assicurati di disporre di un AWS account con accesso da amministratore

Note

Se vuoi provare AWS Transform come prova di concetto o per ambienti di test, consulta [Quick start: Trying Transform. AWS](#)

Iscriviti per un Account AWS

Per iniziare AWS, hai bisogno di un Account AWS. Per informazioni sulla creazione di un Account AWS, vedi Guida [introduttiva a un Account AWS](#) nella Guida Gestione dell'account AWS di riferimento.

Iniziare con IAM-only l'accesso

Con IAM-only Access, gli utenti si autenticano con le AWS credenziali esistenti.

Per configurare IAM-only l'accesso:

1. Nella AWS console, accedi a AWS Transform e scegli Inizia.
2. Completa la configurazione delle impostazioni dell'account.

3. In Accesso utente, seleziona IAM-only accesso.
4. Scegli Abilita per creare il tuo profilo.

Gli utenti accedono all'applicazione web AWS Transform tramite [AWS Sign-In](#). Il loro identificatore utente nell'applicazione web si basa sul loro principio IAM.

Important

Non è possibile aggiungere un provider di identità una volta completata la configurazione. Per gestire gli utenti con IAM Identity Center o un provider di identità esistente, scegli una di queste opzioni durante la configurazione iniziale.

Con IAM-only l'accesso, qualsiasi responsabile IAM con l'`transform:AccessTransformProfile` autorizzazione sulla risorsa del profilo può accedere a AWS Transform. Gestisci l'accesso degli utenti tramite le policy IAM anziché tramite le assegnazioni degli utenti dei provider di identità.

L'`transform:AccessTransformProfile` azione concede solo l'accesso a Transform. AWS Una volta all'interno di AWS Transform, i ruoli dell'area di lavoro controllano le azioni che un utente può eseguire. Questi ruoli includono Amministratore, Collaboratore, Approvatore e Read-only. I ruoli di Workspace si applicano indipendentemente dal modo in cui l'utente si è autenticato.

Utilizzo delle credenziali IAM

Gestione delle informazioni degli utenti

Quando i responsabili IAM accedono a AWS Transform, il servizio gestisce l'identità degli utenti in modo diverso rispetto all'accesso basato su provider di identità.

Identità utente

[Gli utenti IAM sono identificati dal loro responsabile IAM.](#)

Doppia identità

Un utente che ha sia un'identità di provider di identità (come IAM Identity Center) sia una sessione IAM appare come due utenti separati in AWS Transform. Il loro lavoro non è collegato tra le due identità.

Notifiche via e-mail

Le notifiche e-mail sono abilitate solo per gli utenti SSO. I presidi IAM possono ancora essere aggiunti agli spazi di lavoro, ma non riceveranno notifiche e-mail.

Audit

Le chiamate API IAM vengono registrate AWS CloudTrail con l'identità IAM del chiamante. Le azioni eseguite dagli utenti IAM in un job sono tracciabili anche nei worklog di AWS Transform.

Abilitazione dell'accesso IAM insieme a un provider di identità

Se configuri AWS Transform con IAM Identity Center o un provider di identità di terze parti, puoi anche abilitare l'accesso IAM come metodo aggiuntivo di autenticazione. Ciò consente ai responsabili IAM di accedere a AWS Transform insieme agli utenti esistenti del provider di identità.

L'accesso IAM è abilitato per impostazione predefinita quando crei un profilo con IAM Identity Center o un provider di identità di terze parti. Per abilitare o disabilitare l'accesso IAM in qualsiasi momento:

1. Nella console AWS Transform, vai a Impostazioni.
2. In Access AWS Transform with IAM credenziali, attiva o disattiva Abilita l'accesso IAM.

Quando l'accesso IAM è abilitato, sia gli utenti dei provider di identità che i dirigenti IAM possono utilizzare Transform. AWS Gli utenti IAM e gli utenti dei provider di identità possono collaborare nello stesso spazio di lavoro.

Nozioni di base su AWS Organizations

Segui questi passaggi per configurare AWS Transform:

1. Accedi al tuo account di gestione AWS Organizations.
2. Vai al servizio AWS Transform.
3. Scegli Abilita il servizio per consentire alla tua organizzazione di utilizzare AWS Transform.
4. Configura le autorizzazioni necessarie per gli account dei membri dell'organizzazione.
5. Accedi all'esperienza web AWS Transform dai tuoi account membro.

 Note

Per utilizzare Landing Zone Accelerator (LZA) su AWS una soluzione per creare una landing zone insieme alle funzionalità di AWS Transform for migration, l'account AWS Transform e l'installazione di LZA devono trovarsi nella stessa organizzazione. AWS L'utilizzo di Organizations ID separati per le distribuzioni LZA e AWS Transform non è supportato perché ciò può causare incongruenze nella gestione organizzativa e nella distribuzione delle risorse. Per informazioni su come configurare l'installazione LZA utilizzando Organizations, consulta [Deploy a cloud foundation per supportare carichi di lavoro altamente regolamentati e requisiti di conformità complessi nella guida per l'utente della Landing Zone Accelerator on Implementation Guide](#). AWS

Nozioni di base su Centro identità AWS IAM

Segui questi passaggi per utilizzare IAM Identity Center for AWS Transform e aggiungere utenti e gruppi.

Per impostazione predefinita, nessun utente ha accesso a AWS Transform quando lo attivi per la prima volta.

 Note

IAM Identity Center non si limita alla regione in cui è configurato. Se hai già configurato IAM Identity Center in una regione non supportata da AWS Transform, puoi utilizzarlo per AWS Transform.

1. Configura IAM Identity Center seguendo le istruzioni riportate in [Per abilitare un'istanza di IAM Identity Center](#).

Configura IAM Identity Center per utilizzare un provider di identità aziendale esterno e replicane le informazioni su utenti e gruppi in IAM Identity Center.

2. Nella AWS console, seleziona AWS Trasforma e scegli Inizia.
3. Scegli Abilita il servizio per consentire alla tua organizzazione di utilizzare AWS Transform.
4. Seleziona una chiave di crittografia. La selezione predefinita è una chiave AWS gestita. Per utilizzare una chiave personalizzata:

- a. In Chiave di crittografia, scegli Personalizza le impostazioni di crittografia.
- b. Seleziona Usa una chiave AWS KMS.
- c. Scegli una chiave esistente o creane una nuova.
- d. Scegli Invia per applicare le modifiche, quindi scegli Abilita AWS trasformazione.

Scegli Visualizza profilo per visualizzare la configurazione. L'URL dell'applicazione Web viene utilizzato dagli utenti per accedere all'esperienza web unificata AWS Transform.

5. Seleziona Utenti nel riquadro di navigazione e seleziona Assegna utenti o gruppi.
6. Cerca il nome dell'utente o dei gruppi che desideri autorizzare a utilizzare AWS Transform. La ricerca fa riferimento a utenti e gruppi propagati dal tuo provider di identità.
7. Seleziona un gruppo o un utente, seleziona Fine e quindi Assegna. Questi utenti sono autorizzati a utilizzare l'interfaccia web unificata AWS Transform.

Utilizzo di provider di identità di terze parti

AWS Transform supporta l'integrazione con provider di identità di terze parti (IdPs) come Azure Active Directory (Entra ID) e Okta Workforce Identity. Ciò consente di utilizzare il sistema di gestione delle identità esistente per l'autenticazione degli utenti.

Prerequisiti

Prima di configurare l'integrazione con provider di identità di terze parti, assicurati che gli utenti del tuo provider di identità abbiano configurato gli attributi di nome, email e nome utente

Informazioni archiviate

Quando si utilizza AWS Transform with IdPs, AWS archivia un numero minimo di informazioni utente crittografate e protette:

Informazioni utente archiviate

AWS Transform memorizza le informazioni di base del profilo utente al primo accesso, tra cui nome visualizzato, indirizzo e-mail, nome utente (preferred_username) e un identificatore utente univoco. Queste informazioni vengono crittografate utilizzando una chiave KMS di proprietà del cliente o una chiave di proprietà del servizio, a seconda della configurazione del profilo Transform del cliente. AWS I dati vengono archiviati nel database di autenticazione di AWS Transform e

vengono raccolti solo durante la sessione di accesso iniziale. Questo compila i risultati della ricerca quando si invitano altri utenti in uno spazio di lavoro.

Ciclo di vita dei dati

Le informazioni utente vengono archiviate solo per gli utenti che hanno effettuato l'accesso all'app Web AWS Transform almeno una volta e possono diventare obsolete se gli utenti aggiornano le proprie informazioni nel proprio provider di identità senza accedere nuovamente a Transform. AWS Tutte le informazioni utente memorizzate vengono eliminate quando viene eliminato il profilo AWS Transform.

Archiviazione segreta del client

Il segreto del client fornito durante la configurazione viene memorizzato AWS Secrets Manager tramite un Service Linked Secret (SLS) nell'account.

Gestione degli identificatori utente

Entra

Utilizza l'attestazione «oid» (object identifier) come identificatore utente univoco, che è immutabile e identifica in modo univoco gli utenti in tutto il tenant Microsoft. Questo valore è visibile ai clienti nella console Entra e viene visualizzato nei registri. CloudTrail

Okta Workforce Identity

Utilizza diverse attestazioni per l'identificazione degli utenti a seconda del tipo di token: l'attestazione «sub» nei token ID e l'attestazione «uid» nei token di accesso. AWS Transform verifica che entrambe le attestazioni contengano lo stesso valore durante l'autenticazione. Questo valore è visibile ai clienti nella console Okta e viene visualizzato nei CloudTrail registri.

Configurazione di Azure Active Directory (Entra ID)

Per configurare l'integrazione di Azure Active Directory con AWS Transform:

1. Accedi al portale di Azure e seleziona Azure Active Directory.
2. Nel riquadro di navigazione a sinistra, scegli Gestisci > Registrazioni app.
3. Scegli + Nuova registrazione.
4. Inserisci il nome di un'applicazione, scegli il tipo di account supportato, lascia vuoto l'URI di reindirizzamento e scegli Registra.

5. Nella barra di navigazione a sinistra, scegli Gestisci > Manifesto.
6. Aggiorna `requestedAccessTokenVersion` da `null` a `2` e scegli Salva.
7. Scegli Gestisci > Esponi un'API e scegli Aggiungi un ambito.
8. Crea un URI dell'ID dell'applicazione utilizzando la struttura `api://<client-id>` predefinita.
9. Aggiungi l'ambito `transform:read_write`.
10. Scegli Aggiungi un certificato o un segreto e crea un nuovo segreto client. Salva questo valore in quanto è necessario per la creazione del profilo.
11. Trova l'URL dell'emittente scegliendo Endpoints e selezionando il documento di metadati OpenID Connect. Il campo «emittente» nei metadati è l'URL dell'emittente.
12. Crea un profilo nella console AWS Transform utilizzando l'ID client, il segreto del cliente e l'URL dell'emittente.
13. Dopo la creazione del profilo, aggiungi un URI di reindirizzamento scegliendo Aggiungi una piattaforma, selezionando Web e inserendo. `<web-application-url>/login/callback`

Configurazione di Okta Workforce Identity

Per configurare l'integrazione di Okta Workforce Identity con Transform: AWS

1. Vai alla tua console Okta Workforce Identity.
2. Scegli Applicazioni > Applicazioni e seleziona Crea integrazione tra app.
3. Seleziona OIDC - OpenID Connect and Web Application, quindi scegli Avanti.
4. Assegna un nome all'applicazione, lascia il tipo di concessione come codice di autorizzazione, lascia vuoti gli URI di reindirizzamento, configura le assegnazioni degli utenti e scegli Salva.
5. Vai alla scheda Accedi e imposta l'emittente su Okta URL anziché su Dynamic.
6. Copia l'ID client e configuralo come pubblico per il tuo server di autorizzazione andando su Sicurezza > API e aggiungendo un server di autorizzazione.
7. Nel server di autorizzazione, aggiungi l'`transform:read_write`ambito nella scheda Ambiti.
8. Aggiungi una politica di accesso che consenta all'applicazione OIDC di utilizzare questo server di autorizzazione e configura una regola per la politica.
9. Nella pagina Impostazioni del server di autorizzazione, annota l'URL dell'emittente per la creazione del profilo in Transform. AWS
10. Crea un profilo in AWS Transform utilizzando l'URL dell'emittente, l'ID client e il segreto del client dalle impostazioni dell'applicazione.

11. Dopo la creazione del profilo, aggiungilo `<web-application-url>/login/callback` come URL di reindirizzamento nella scheda Generale dell'applicazione.

Note

Se desideri essere reindirizzato all'applicazione web AWS Transform dopo il logout, dovrai configurare l'URL dell'applicazione web come origine attendibile in Sicurezza > API.

Onboarding degli utenti

Questa sezione descrive l'esperienza degli utenti a cui è stato concesso l'accesso a AWS Transform.

Accettazione dell'invito

Quando un utente viene aggiunto a AWS Transform, riceve un invito via e-mail contenente:

- Un saluto e informazioni sull'invito
- L'URL dell'applicazione web AWS Transform
- Il loro nome utente
- Un link per accettare l'invito e impostare la password

Per configurare il loro account:

1. L'utente fa clic sul link «Accetta invito» contenuto nell'e-mail.
2. Nella pagina «Registrazione nuovo utente», inserisce e conferma una password.
3. La password deve soddisfare i requisiti di sicurezza, tra cui:
 - Almeno 8 caratteri
 - Almeno una lettera maiuscola
 - Almeno una lettera minuscola
 - Almeno un numero
 - Almeno un carattere speciale
4. Dopo aver creato una password, vedono una conferma che il loro account è stato creato con successo.

Accedere a AWS Trasformazione

Per accedere a AWS Transform:

1. Vai all'URL dell'applicazione web AWS Transform fornito nell'e-mail di invito.
2. Inserisci il nome utente.
3. Scegli Next (Successivo).
4. Immetti la password.
5. Selezionare Sign in (Accedi).

Esperienza di benvenuto

Al primo accesso, gli utenti AWS visualizzano la pagina di benvenuto di Transform con:

- Un saluto personalizzato
- Funzionalità di trasformazione disponibili
- Opzione per creare uno spazio di lavoro

La pagina di benvenuto fornisce informazioni sulle funzionalità di trasformazione disponibili in AWS Transform, tra cui:

- Modernizza le migrazioni IBM verso z/OS AWS
- Migrazione dei carichi di lavoro VMware su Amazon EC2
- Modernizza le applicazioni .NET in un formato multiplatforma Linux-ready
- Valuta i carichi di lavoro per renderli pronti alla migrazione

Gli utenti possono iniziare creando uno spazio di lavoro o chiedendo al proprio team di aggiungerlo a uno spazio di lavoro esistente.

Utilizzo del proprio bucket Amazon S3

Per impostazione predefinita, AWS Transform utilizza un bucket Amazon S3 gestito dal servizio per archiviare gli artefatti della trasformazione. Puoi invece scegliere di utilizzare il tuo bucket Amazon S3 per un maggiore controllo sullo storage dei dati, sulla crittografia e sulle politiche di accesso.

 Note

Se disponi di un bucket Amazon S3 per le trasformazioni del mainframe, puoi continuare a utilizzare quel connettore S3 senza dover utilizzare questa funzionalità.

 Note

Il tuo bucket Amazon S3 memorizza solo i caricamenti e gli artefatti di trasformazione con cui interagisci. Gli artefatti generati dal sistema interno non vengono archiviati nel bucket. Inoltre, AWS Transform indicizza gli artefatti nel bucket. Memorizza i dati indicizzati in una knowledge base gestita dal servizio che viene utilizzata per offrirti un'esperienza di chat arricchita.

Prerequisiti

Prima di configurare il tuo bucket Amazon S3, assicurati che siano soddisfatti i seguenti requisiti:

- Il bucket deve trovarsi nella stessa AWS regione in cui è abilitato AWS Transform.
- La policy del bucket richiesta deve essere applicata al tuo bucket. Per ulteriori informazioni, consulta [the section called “Politica sui bucket richiesta”](#).
- Se si utilizza l'applicazione web AWS Transform, CORS deve essere configurato sul bucket. Per ulteriori informazioni, consulta [the section called “Configurazione CORS richiesta”](#).
- Se si utilizza una chiave AWS KMS personalizzata, è necessario applicare la politica di chiave richiesta. Per ulteriori informazioni, consulta [the section called “Politica chiave KMS \(opzionale\)”](#).

Configurazioni di crittografia supportate

Il bucket deve utilizzare una delle seguenti configurazioni di crittografia:

- SSE-S3 (AES256) — Lascia vuoto il campo della chiave KMS. AWS Transform scrive oggetti senza specificare un'intestazione di crittografia e Amazon S3 applica la crittografia predefinita del bucket con chiavi. S3-managed Per ulteriori informazioni, consulta [Usare la crittografia lato server con le chiavi gestite di Amazon S3 SSE-S3 \(\)](#) nella Amazon S3 User Guide.
- SSE-KMS con una chiave KMS gestita dal cliente: fornisci la chiave KMS ARN. AWS Transform scrive oggetti utilizzando la chiave `arn:aws:kms:aws:amz-server-side-encryption:aws:kms`. Seguire [the section called “Politica chiave KMS \(opzionale\)”](#).

I seguenti non sono supportati:

- SSE-KMS con una chiave KMS AWS gestita (ad esempio,) aws/s3
- SSE-C
- DSSE-KMS
- chiavi KMS asimmetriche o chiavi KMS con una specifica chiave diversa da SYMMETRIC_DEFAULT

 Warning

AWS-le chiavi KMS gestite non sono supportate. Se il bucket è crittografato con aws/s3, esegui la migrazione a una chiave gestita dal cliente o SSE-S3 prima di utilizzare il bucket con Transform. AWS

Configurazione del bucket Amazon S3

Puoi configurare AWS Transform per utilizzare il tuo bucket Amazon S3 dalla console Transform. AWS

Per usare il tuo bucket Amazon S3

1. Nella console AWS Transform, scegli Impostazioni.
2. In Artifact storage, scegli Usa il mio bucket S3. Puoi usare un bucket nel tuo account corrente Account AWS o in un altro account.
3. Per Bucket, inserisci l'URI di Amazon S3.
4. (Facoltativo) Per la chiave KMS, inserisci una chiave AWS KMS ARN per crittografare gli oggetti nel bucket. Se lasci vuoto questo campo, AWS Transform scrive oggetti senza un'intestazione di crittografia e Amazon S3 applica le impostazioni di crittografia predefinite del bucket. Per ulteriori informazioni, consulta [Impostazione del comportamento di crittografia lato server predefinito per i bucket Amazon S3 nella Amazon S3 User Guide](#).

Se la crittografia predefinita del tuo bucket è SSE-KMS, inserisci l'ARN della chiave KMS gestita dal cliente in questo campo e aggiorna la politica delle chiavi. Per ulteriori informazioni, consulta [the section called “Politica chiave KMS \(opzionale\)”](#).

5. Scegli Salva. AWS Transform convalida la configurazione e le autorizzazioni del bucket prima di applicare la configurazione.

Dopo aver salvato la configurazione, AWS Transform utilizza il bucket per memorizzare gli artefatti della trasformazione.

Note

AWS Transform convalida la configurazione solo quando si salva. Se successivamente modifichi la policy del bucket, la configurazione CORS o la politica delle chiavi KMS, salva nuovamente le impostazioni del profilo per convalidarle nuovamente.

Politica sui bucket richiesta

È necessario configurare la policy del bucket per concedere l'accesso a AWS Transform. Aggiungi la seguente policy sui bucket al tuo bucket Amazon S3 per consentire al responsabile AWS del servizio Transform di leggere, scrivere, eliminare ed elencare gli artefatti della trasformazione.

```
{
  "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"
        }
      }
    }
  ]
}

```

Sostituisci i valori seguenti:

- *bucket-name*— Il nome del tuo bucket Amazon S3.
- *profile-account-id*— L' Account AWS ID associato al tuo profilo AWS Transform.
- *profile-arn*— L'ARN del tuo profilo AWS Transform.

Configurazione CORS richiesta

Se utilizzi l'applicazione web AWS Transform, devi configurare Cross-Origin Resource Sharing (CORS) sul tuo bucket Amazon S3. Puoi trovare il dominio dell'applicazione web dopo aver abilitato Transform. AWS Per ulteriori informazioni, consulta [Nozioni di base](#).

```

[
  {
    "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
}
]
```

Sostituisci i valori seguenti:

- *webapp-domain*— L'URL di origine dell'applicazione Web (ad esempio, `https://1a2b3c4d5e6f7a8b9.transform.us-east-1.on.aws`), che può essere trovato nella pagina delle impostazioni di AWS Transform. Non includere la barra finale.

Politica chiave KMS (opzionale)

Questa sezione si applica solo quando il bucket è crittografato con una chiave KMS gestita dal cliente. Se il tuo bucket lo utilizza SSE-S3, salta questa sezione.

Se specifichi la tua chiave AWS KMS per la crittografia dei bucket, aggiungi la seguente dichiarazione alla tua politica delle chiavi. AWS Transform si affida a Forward Access Sessions (FAS) per creare sovvenzioni per il responsabile del servizio. Queste concessioni vengono utilizzate per convalidare la chiave e accedere agli artefatti nel bucket 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"
    }
  }
}
```

Sostituisci i valori seguenti:

- *key-owner-account-id*— L' Account AWS ID che possiede la chiave KMS.
- *region*— La AWS regione in cui è abilitata la AWS trasformazione (ad esempio,us-east-1).

Tornare al bucket predefinito

Puoi tornare al bucket gestito dal servizio in qualsiasi momento.

Per passare a AWS Trasforma lo storage gestito

1. Nella console AWS Transform, scegli Impostazioni.
2. In Archiviazione degli artifatti, scegli Modifica.
3. Scegli AWS Transform managed storage.
4. Scegli Save (Salva).

 Warning

Se cambi configurazione di storage mentre i processi di trasformazione sono in corso, tali processi falliscono. Inoltre, eventuali artefatti già generati da quei lavori in corso non sarebbero accessibili.

 Important

Quando torni al bucket gestito dal servizio:

- Gli artefatti presenti nel bucket non vengono migrati automaticamente. Per conservare eventuali artefatti, scaricali dal tuo bucket Amazon S3 e caricali nuovamente tramite l'applicazione web Transform AWS nell'archivio degli artefatti per l'area di lavoro e il lavoro corrispondenti.
- AWS Transform annulla la sua concessione sulla tua chiave KMS. Gli oggetti scritti nel tuo bucket rimangono nel tuo bucket; eliminali manualmente se non sono più necessari.

Caricamento di file direttamente nel tuo bucket

Puoi caricare i file direttamente nel tuo bucket Amazon S3 senza utilizzare l'applicazione web AWS Transform. Per rendere i file caricati disponibili agli agenti di trasformazione, caricali nella User Uploads cartella del lavoro. Il percorso della directory di questa cartella utilizza il seguente formato:

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

Sostituisci i valori seguenti:

- *workspace-id*— L'ID dell'area di lavoro AWS Transform.
- *job-id*— L'ID del processo di trasformazione.

Ogni lavoro in AWS Transform ha una propria User Uploads cartella. I file caricati su questo percorso vengono visualizzati nell'applicazione Web e sono disponibili per gli agenti di trasformazione mentre completano il lavoro.

I percorsi dei file non devono contenere . . spazi iniziali o finali: i file che violano questi vincoli non sono visibili agli agenti. //

⚠ Important

Se il tuo bucket lo utilizza SSE-KMS, includi le seguenti intestazioni in ogni caricamento diretto:

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

Gli oggetti devono essere crittografati con la chiave KMS registrata nel tuo AWS profilo Transform. Gli oggetti crittografati con qualsiasi altra chiave non sono accessibili a AWS Transform.

Matrice di compatibilità

La tabella seguente riassume la compatibilità di AWS Transform con le funzionalità comuni dei bucket Amazon S3.

Funzionalità	Compatibilità	Note
Controllo delle versioni di Bucket	Supportata	Gestisci le versioni non correnti con una regola del ciclo di vita.
Proprietà dell'oggetto	Obbligatorio: il proprietario del bucket è stato imposto	Bucket owner Preferred e Object writer non sono supportati.
ACL	Non supportata	Gli ACL devono essere disabilitati nel bucket.
Object Lock (modalità di governance)	Parzialmente supportato	Le eliminazioni potrebbero essere bloccate dalle impostazioni di conservazione.
Object Lock (modalità di conformità)	Non supportata	—
Blocco dell'accesso pubblico	Supportata	—

Funzionalità	Compatibilità	Note
pagamento a carico del richiedente	Non supportata	—
Punto di accesso S3	Non supportata	Usa il nome del bucket.
Punti di accesso Lambda per oggetti S3	Non supportata	Usa il nome del bucket.
S3 on Outposts	Non supportata	—
S3 Express One Zone (bucket di directory)	Non supportata	—
Cross-Region secchi	Non supportata	—
Cross-account secchi	Supportata	—
Cross-account chiavi KMS	Non supportata	—
Regole del ciclo di vita	Supportata	—
CloudTrail eventi relativi ai dati	Supportata	—

Attiva AWS Trasformazione

Per abilitare AWS Transform:

1. Accedi alla console AWS di gestione.
2. Nella barra di ricerca nella parte superiore della console, cerca AWS Transform.
3. Seleziona AWS Transform dai risultati della ricerca.
4. Scegli Inizia per abilitare il servizio nella tua regione attuale.

5. Facoltativo: configura IAM Identity Center. Potrai anche scegliere di utilizzare un [provider di identità \(IdP\) di terze parti](#) in un passaggio successivo.
6. Seleziona una chiave di crittografia: chiave AWS gestita predefinita o Personalizza le impostazioni di crittografia.
7. Facoltativo: usa il tuo bucket Amazon S3. Per impostazione predefinita, AWS Transform utilizza un bucket Amazon S3 gestito dal servizio per archiviare gli artefatti della trasformazione. Puoi invece scegliere di utilizzare il tuo bucket. Per ulteriori informazioni, consulta [Utilizzo del proprio bucket Amazon S3](#).
8. Scegli le funzionalità di AWS trasformazione che desideri abilitare:
 - Interfaccia a riga di comando (CLI), necessaria per creare ed eseguire trasformazioni [personalizzate](#). Per abilitare la CLI, visualizza e segui le istruzioni per il download.
 - Applicazione Web, l'interfaccia utente agentica per la modernizzazione. Scegli Abilita l'applicazione web per usarla.
9. Scegli Abilita AWS trasformazione.
10. Facoltativo: scegli Abilita il profilo di visualizzazione per accedere alle schede AWS Trasforma utenti, Impostazioni e Connettori o Gestisci utenti per gestire gli utenti.

Puoi accedere alle schede Utenti, Impostazioni e Connettori in qualsiasi momento scegliendo l'icona del menu nell'angolo in alto a sinistra della console.

11. Configura l'accesso utente scegliendo una delle seguenti opzioni:
 - Centro identità IAM
 - Un [provider di identità \(IdP\)](#) di terze parti
 - [IAM-only accesso](#)

 Note

Questa scelta è finalizzata e non può essere modificata quando si abilita AWS Transform.

12. Scegli Abilita applicazione web.
13. Il sistema visualizza «Enabling AWS Transform» mentre crea le risorse necessarie.

Dopo aver abilitato la AWS trasformazione, la scheda Impostazioni visualizza le seguenti informazioni:

- URL dell'applicazione Web: l'URL per accedere all'applicazione Web AWS Transform
- URL di avvio per IDE: l'URL per accedere a AWS Transform in ambienti di sviluppo integrati
- Regione: la AWS regione in cui è abilitato AWS Transform

Avvio rapido: sto provando AWS Trasformazione

Il modo più semplice per provare AWS Transform è con un AWS account indipendente. Potresti volerlo fare come prova di concetto o per ambienti di test. Utilizzate questa procedura:

1. Accedere alla console AWS di gestione.
2. Accedi al servizio AWS Transform.
3. Scegli Inizia per abilitare il servizio.
4. Seleziona e configura il tuo provider di identità.
5. Assegna gli utenti al servizio AWS Transform.
6. Dopo aver abilitato il servizio, vedrai l'URL dell'applicazione web AWS Transform.
7. Apri l'URL in una nuova finestra del browser per accedere all'esperienza web AWS Transform.

Ora sei pronto per configurare il tuo spazio di lavoro.

Gestione degli utenti

Il modo in cui gestisci l'accesso degli utenti a AWS Transform dipende dal modello di accesso scelto durante la configurazione. Se hai configurato IAM Identity Center, aggiungi utenti tramite IAM Identity Center. Se hai configurato un provider di identità di terze parti, gestisci gli utenti di quel provider. Se hai scelto IAM-only l'accesso, l'accesso degli utenti viene gestito tramite le politiche IAM.

Aggiungere utenti in IAM Identity Center

Per aggiungere utenti in IAM Identity Center:

1. Accedi alla console IAM Identity Center.

2. Nel riquadro di navigazione, seleziona Users (Utenti).
3. Scegliere Add user (Aggiungi utente).
4. Inserisci le informazioni richieste:
 - Nome utente: un identificatore univoco per l'utente (non può essere modificato in seguito)
 - Indirizzo e-mail: l'indirizzo e-mail dell'utente
 - Nome e cognome: il nome dell'utente
 - Nome visualizzato: il nome che appare nell'elenco degli utenti
5. Per Password, scegli come l'utente riceve la password:
 - Invia un'e-mail: invia le istruzioni di configurazione tramite e-mail
 - Genera una password monouso: crea una password da condividere manualmente
6. Scegli Avanti per rivedere le informazioni sull'utente.
7. Controlla i dettagli e scegli Aggiungi utente.

Dopo l'aggiunta, l'utente riceverà un invito via e-mail per configurare il proprio account IAM Identity Center. Il link di invito è valido per 7 giorni.

Puoi anche scoprire come lavorare con IAM Identity Center and AWS Transform in questo video:

[VideoTitle](#)

Aggiungere utenti a AWS Trasformazione

Dopo aver aggiunto gli utenti a IAM Identity Center, puoi concedere loro l'accesso a AWS Transform:

1. Torna alla console AWS Transform.
2. Nel riquadro di navigazione, scegli Utenti e gruppi.
3. Seleziona la scheda Utenti o la scheda Gruppi.
4. Cerca e seleziona gli utenti o i gruppi che desideri aggiungere da IAM Identity Center.
5. Scegli Assegna utenti e gruppi per concedere agli utenti o ai gruppi selezionati l'accesso a AWS Transform.

Dopo aver aggiunto gli utenti, questi vengono visualizzati nell'elenco Utenti con lo stato «In sospeso» finché non accettano l'invito e non accedono.

Gestione degli utenti con accesso IAM-only

Se hai configurato AWS Transform con IAM-only access, l'accesso degli utenti viene gestito tramite le policy IAM. Qualsiasi principale IAM con l'`transform:AccessTransformProfile` autorizzazione sulla risorsa del profilo può accedere a AWS Transform.

Per concedere a un utente o un ruolo l'accesso a AWS Transform:

1. Passare alla IAM console (Console IAM).
2. Allega una policy che includa l'`transform:AccessTransformProfile` autorizzazione all'utente o al ruolo IAM. Per un esempio di policy, consulta [Consentire agli utenti di accedere a AWS Transform con credenziali IAM](#).

Per revocare l'accesso, rimuovi la policy dall'utente o dal ruolo IAM.

Comprensione delle autorizzazioni dei collaboratori

AWS Transform utilizza un modello di autorizzazione basato sull'area di lavoro per controllare l'accesso a risorse e azioni. A ogni utente viene assegnato un ruolo specifico all'interno di un workspace, che determina le azioni che può eseguire. Un utente può avere ruoli diversi in aree di lavoro diverse.

Ruoli utente

AWS Transform supporta cinque ruoli utente all'interno di ogni area di lavoro. Questi ruoli si applicano nel contesto di un'area di lavoro e a un utente verranno assegnati ruoli in ogni area di lavoro di cui è membro. Le autorizzazioni di accesso definite per ogni ruolo sono indipendenti dall'area di lavoro, pertanto l'utente A con il ruolo di amministratore nell'area di lavoro A dispone delle stesse autorizzazioni dell'utente B con il ruolo di amministratore nell'area di lavoro B.

Autorizzazioni del ruolo

Autorizzazioni dettagliate per ogni ruolo:

Azione	ResourceType	Admin	Approvatore	Collaboratore	ReadOnly
Crea	Workspace	✓	✓	✓	✓

Azione	ResourceType	Admin	Approvatore	Collaboratore	ReadOnly
List	Workspace	✓	✓	✓	✓
Get	Workspace	✓	✓	✓	✓
Aggiorna	Workspace	✓	✗	✗	✗
Elimina	Workspace	✓	✗	✗	✗
Crea	ChatMessage	✓	✓	✓	✗
Lettura	ChatMessage	✓	✓	✓	✓
Crea	RoleAssociation	✓	✗	✗	✗
Lettura	RoleAssociation	✓	✓	✓	✓
Aggiorna	RoleAssociation	✓	✗	✗	✗
Elimina	RoleAssociation	✓	✗	✗	✗
Lettura	Attività HITL critica	✓	✓	✓	✓
Aggiorna	Attività HITL critica	✓	✓	✗	✗
Elimina	Attività HITL critica	✓	✓	✗	✗
Lettura	Attività Hitl	✓	✓	✓	✓
Aggiorna	Operazione Hitl	✓	✓	✓	✗
Elimina	Operazione Hitl	✓	✓	✓	✗
Crea	Processo	✓	✓	✓	✗
Lettura	Processo	✓	✓	✓	✓
Aggiorna	Processo	✓	✓	✓	✗
Elimina	Processo	✓	✓	✓	✗

Azione	ResourceType	Admin	Approvatore	Collaboratore	ReadOnly
Lettura	Worklog	✓	✓	✓	✓
Crea	Artifact	✓	✓	✓	x
Lettura	Artifact	✓	✓	✓	✓
Aggiorna	Artifact	✓	✓	✓	x
Elimina	Artifact	✓	✓	✓	x
Crea	Connector	✓	✓	✓	x
Lettura	Connector	✓	✓	✓	✓
Aggiorna	Connector	✓	✓	✓	x
Elimina	Connector	✓	✓	✓	x

Human-in-the-loop azioni (HITL)

AWS Transform offre due tipi di azioni HITL: standard e critiche:

Azioni HITL standard

Si tratta di azioni di routine che possono essere eseguite da utenti con ruoli di Collaboratore, Approvatore o Amministratore.

Azioni HITL critiche

Si tratta di azioni con un impatto significativo e richiedono quindi livelli di autorizzazione più elevati. Gli esempi includono:

- Unire il codice alle filiali principali
- Esecuzione della decomposizione del grafico
- Distribuzione del codice negli ambienti di produzione

Le azioni HITL critiche possono essere eseguite solo da utenti con ruoli di approvatore o amministratore.

Per garantire una differenziazione tra le azioni HITL standard e le azioni HITL critiche nelle politiche AuthZ, AWS Transform fornisce due API HITL separate, una per il completamento di un'azione HITL standard e l'altra per il completamento di un'azione HITL critica.

AWS Trasforma l'ambiente

AWS Transform è un servizio agentico che utilizza l'elaborazione del linguaggio naturale per aiutarti a pianificare ed eseguire le trasformazioni del carico di lavoro. Interagisci con AWS Transform principalmente attraverso un'interfaccia conversazionale, in cui il servizio si adatta e risponde in base al contesto della discussione. Ad esempio, puoi iniziare descrivendo l'architettura e gli obiettivi di trasformazione attuali utilizzando un linguaggio comune, ad esempio «Devo migrare le mie macchine virtuali locali su EC2».

Mentre conversi con AWS Transform, il servizio crea un piano di lavoro personalizzato in linea con i tuoi requisiti specifici. Il flusso di conversazione è dinamico e guidato da te, e ti consente di perfezionare il tuo piano di trasformazione in modo iterativo. Puoi modificare il piano di lavoro durante la conversazione formulando richieste come «aggiungere una fase di test prima del termine della produzione» o «rimuovere la fase di backup poiché abbiamo già una soluzione». Puoi anche tornare a un'attività precedente ed eseguirla di nuovo. AWS Transform aggiorna continuamente il piano in base ai tuoi input, assicurando che la strategia di trasformazione finale soddisfi le tue esigenze tecniche e aziendali.

Ecco cosa vedi quando apri AWS Transform.

- Visualizza il pannello di controllo: questo è il riquadro stretto a sinistra di AWS Transform. Puoi scegliere una delle icone per scegliere quale vista mostrare a destra del riquadro di controllo della vista. Passa il mouse su ciascuna icona per visualizzare una descrizione che spiega la vista. Le cinque viste standard, dall'alto verso il basso, sono:
 - Job Plan
 - Dashboard
 - Approvazioni
 - Artefatti
 - Registro di lavoro

Alcuni flussi di lavoro forniscono visualizzazioni aggiuntive.

Quando si lavora a un piano di lavoro, le visualizzazioni sono:

- Chat
- Approvazioni
- Negozio di artifact
- Registro di lavoro

Quando ti trovi in un'area di lavoro, le viste sono in alto:

- Jobs
- Artefatti
- Collaboratori (utenti)
- Connectors (Connettori)
- Settings (Impostazioni)
- Il riquadro Visualizza si trova accanto ai controlli di visualizzazione.
- Il riquadro Chat è al centro. Qui è dove conduci la conversazione con AWS Transform.

Note

Gli utenti con autorizzazioni di sola lettura non sono in grado di inviare messaggi nella chat.

- A destra c'è il riquadro Collaborazione. Viene visualizzato quando vengono eseguite attività umane in the loop (HITL), come:
 - Caricamento di file di dati
 - Revisione delle informazioni e dei piani forniti da Transform AWS

Impostazioni della lingua

AWS Transform supporta la localizzazione per flussi di lavoro selezionati. È possibile modificare la lingua di visualizzazione dell'applicazione Web scegliendo l'icona Impostazioni nell'angolo in alto a destra e selezionando la lingua preferita dal menu Lingua.

Sono supportate le seguenti lingue:

- Inglese (Stati Uniti)
- Inglese (Regno Unito)
- Deutsch (tedesco)
- Español (spagnolo)

- Français (francese)
- 12 (giapponese)
- Bahasa Indonesia (indonesiano)
- English (Italiano)
- Português (portoghese)
- (coreano)
- () (cinese semplificato)
- () (Cinese tradizionale)
- Türkçe (turco)

I seguenti flussi di lavoro supportano la localizzazione:

- [Migrazioni \(incluso VMware\)](#)

Note

Gli altri flussi di lavoro AWS Transform sono attualmente disponibili solo in inglese. Il supporto alla localizzazione per flussi di lavoro aggiuntivi potrebbe essere aggiunto nei futuri aggiornamenti.

Inizia il tuo progetto

AWS Transform ti guida attraverso i tuoi progetti di modernizzazione e migrazione. Per iniziare

1. Crea uno spazio di lavoro per ospitare il tuo progetto. Nella pagina Aree di lavoro, scegli Crea area di lavoro. Segui le istruzioni e poi apri l'area di lavoro.
2. Nel riquadro Chat, digita «crea un lavoro»
3. Scegli un lavoro e segui le istruzioni fornite da AWS Transform. Se l'input è richiesto, viene visualizzato il riquadro Collaborazione che spiega cosa è richiesto.

Flessibilità del workflow

L'ambiente di flusso di lavoro AWS Transform offre flessibilità nella progressione dei progetti di modernizzazione. Utilizzando il linguaggio naturale nel riquadro della chat puoi:

- Riprova un'attività che AWS Transform ha già completato, fornendo diversi input umani in the loop lungo il percorso.
- Esegui nuovamente un lavoro, ad esempio, se sono state apportate modifiche alle fonti di modernizzazione.

Chiacchierando con AWS Trasformazione

AWS La chat Transform è disponibile in ogni fase del progetto. Per aprire la chat, fai clic sull'icona esagonale viola nell'angolo in basso a destra della console web.

La chat è a tua disposizione per chiedere qualsiasi cosa. Ad esempio, puoi chiedere alla chat di spiegare concetti, guidarti attraverso un processo, spiegare una richiesta o una risposta AWS Transform o spiegare un rapporto AWS Transform.

Note

Gli utenti con autorizzazioni di sola lettura non sono in grado di inviare messaggi nella chat.

AWS Trasforma le integrazioni di chat

AWS Transform chat è integrato con:

Experience-Based Accelerazione

[Experience-Based Accelerazione \(EBA\)](#) è offerta tramite AWS la chat Transform. Consente di eseguire una valutazione EBA per i carichi di lavoro Windows e generare un piano. Puoi iniziare importando i risultati della valutazione da CAST. Vi aiuta a scoprire il vostro portafoglio di applicazioni, dopodiché potete utilizzare AWS Transform chat per selezionare le applicazioni che soddisfano le vostre esigenze aziendali (ad esempio, filtrando le applicazioni in base alla complessità o alle righe di codice). È quindi possibile eseguire una valutazione più approfondita dell'applicazione selezionata e generare un piano di modernizzazione.

AWS Countdown Premium

[AWS Countdown Premium](#) (CDP) integrato in AWS Transform fornisce una guida continua ed esperta con supporto tecnico designato. AWS L'ingegnere CDP designato approfondisce a fondo il vostro stack tecnologico, fornendo un supporto personalizzato e sensibile al contesto in caso di problemi. Gli utenti possono sfruttare AWS Transform per registrare un ticket di assistenza

direttamente dalla sua interfaccia di chat. Il ticket di supporto incorpora i dettagli del registro di lavoro e del piano di lavoro per aiutare l'assistenza a comprendere il contesto del cliente. Se un cliente o un partner fa parte del programma CDP, il ticket di assistenza viene automaticamente indirizzato al tecnico CDP designato che può aiutare a eseguire il debug dei problemi, interpretare gli output di trasformazione e promuovere i progressi per una rapida risoluzione dei problemi. Ad esempio:

- Per i carichi di lavoro.NET, CDP può fornire assistenza per i problemi relativi ai connettori dei repository, la risoluzione delle dipendenze e l'implementazione post-trasformazione.
- Negli scenari mainframe, CDP può aiutare a risolvere i problemi del codice Java refactorizzato, configurare strumenti di migrazione del database e creare pipeline. CI/CD
- Nelle migrazioni VMware, CDP può accelerare la configurazione della rete, la configurazione di MGN e l'installazione degli agenti.

AWS Skill Builder

[AWS Skill Builder](#) fornisce moduli di apprendimento pertinenti tramite la chat. Puoi chiedere a AWS Transform chat quali sono le tue esigenze di apprendimento e ti presenterà il catalogo dei corsi pertinente. Skill Builder offre esperienze di microapprendimento contestuali mentre affronti le fasi di trasformazione.

Strumenti per sviluppatori

È possibile accedere agli agenti AWS Transform dagli IDE agentici, dai plug-in degli agenti e dal server MCP. Scegliete la superficie più adatta al vostro flusso di lavoro.

Note

I plugin Kiro Power e Agent installano automaticamente il server MCP. È necessario installare il server MCP manualmente solo se si desidera utilizzarlo senza un plug-in Kiro Power o un agente.

Kiro Power

[AWS Transform Kiro Power](#) fornisce l'accesso completo agli agenti AWS Transform dall'IDE Kiro.

Per installare il AWS Trasforma Kiro Power

1. Apri Kiro IDE e vai al pannello Powers.
2. Trova AWS Transform nell'elenco e installalo.
3. Apri Kiro Chat, fai clic su Power e seleziona Try power.

In alternativa, nel pannello Powers scegli Aggiungi alimentazione personalizzata > Importa alimentazione da GitHub e incolla: <https://github.com/kirodotdev/powers/tree/main/aws-transform>

Plugin Agent

Il plugin AWS Transform agent è disponibile all'indirizzo [awslabs/agent-plugins](https://github.com/aws-labs/agent-plugins) on GitHub, nella `plugins/aws-transform` directory. Il plugin supporta Claude Code, Codex e Cursor.

Il plugin include e `.claude-plugin` `.codex-plugin` configurazioni. `.mcp.json` Fornisce l'accesso a tutti gli agenti AWS Transform, come .NET, mainframe, VMware, SQL Server e alle trasformazioni personalizzate.

Da installare in Claude Code

Esegui i comandi seguenti:

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

Da installare in Codex o Cursor

Segui le istruzioni nel repository [agent-plugins README](#).

Plugin IDE

Il plugin AWS Transform IDE è disponibile sugli editor compatibili con VS Code e Open VSX. Espone le funzionalità personalizzate di AWS Transform, inclusa la creazione e l'esecuzione di definizioni di trasformazione. Espone inoltre le funzionalità del mainframe, tra cui la tracciabilità tra requisiti di modernizzazione, regole aziendali e codice sorgente, nonché la capacità di generare documentazione tecnica su richiesta. Per iniziare, installa utilizzando uno dei seguenti metodi:

- VS Code: installa da [VS Code Marketplace](#).
- Apri VSX: installa dal registro [Open VSX](#).

Server MCP

Utilizzate il server MCP per integrare AWS Transform a livello di codice con qualsiasi client. MCP-compatible È possibile installare il server MCP da `awslabs.aws-transform-mcp-server` PyPI come. Fornisce 19 strumenti per la gestione dell'area di lavoro, la gestione dei lavori, le attività HITL (human-in-the-loop), la gestione degli artefatti, la gestione dei connettori, la chat e la navigazione delle risorse.

Prerequisiti

- Python 3.10 o successivo

Installazione

Codice Claude

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


Kiro

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

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

Per i dettagli di configurazione per il tuo client MCP specifico, consulta il README di [aws-transform-mcp-server](#) su GitHub

Autenticazione

AWS Transform supporta l'autenticazione basata sui ruoli SSO (Identity Center) e IAM. AWS Identity and Access Management

SSO (IAM Identity Center)

Chiedi al tuo assistente AI di «Configurare AWS Transform with SSO». L'assistente fornisce un URL iniziale e apre il browser per l'accesso.

Ruolo IAM

L'ambiente fornisce automaticamente AWS le credenziali. Imposta `AWS_PROFILE` nel env blocco di configurazione del client MCP per selezionare un profilo specifico.

Per informazioni sulla configurazione dell'autenticazione per AWS Transform, consulta [Nozioni di base su AWS Trasformazione](#).

Crea agenti personalizzati per AWS Trasformazione

Il [toolkit agent builder](#) consente a AWS partner e clienti di creare agenti su misura per le loro specifiche esigenze di modernizzazione che funzionano all'interno di Transform. AWS

Per installare il toolkit Agent Builder

1. Apri Kiro IDE e vai al pannello Powers.

2. Trova AWS Transform Agent Toolkit nell'elenco e installalo.

In alternativa, nel pannello Powers scegliete Aggiungi alimentazione personalizzata > Importa alimentazione da GitHub e incolla: <https://github.com/kirodotdev/powers/tree/main/aws-transform-agent-toolkit>

Il toolkit agent builder consente ai partner, agli ISV o ai clienti competenti in materia di migrazione e modernizzazione di creare soluzioni di trasformazione per casi d'uso specifici. Puoi integrare agenti, strumenti, knowledge base e flussi di lavoro specializzati con le funzionalità di Transform Agent AI. AWS

Ciclo di vita degli agenti

Creazione

Usa Kiro Power per combinare l'agente di base e l'SDK per scrivere il tuo agente personalizzato.

Condivisione

Distribuisci gli agenti con i team o tra le reti di partner.

Registrati

Registra gli agenti con AWS Transform per farli scoprire da altri utenti.

Valutazioni della migrazione

AWS Le valutazioni di Transform ti aiutano a valutare il costo, la fattibilità e il valore aziendale della migrazione dell'infrastruttura locale a. AWS Le valutazioni forniscono consigli automatici sul corretto dimensionamento, il confronto tra più scenari e il perfezionamento interattivo tramite chat.

Puoi utilizzare le valutazioni della migrazione per:

- Ottieni stime dei costi per Amazon RDS per SQL Server, Amazon EC2, Amazon EBS, Amazon S3 e Amazon FSx
- Ricevi consigli automatici sul corretto dimensionamento
- Valuta il valore aziendale e l'impatto sulla sostenibilità
- Confronta più scenari di migrazione fianco a fianco
- Perfeziona le valutazioni in modo interattivo tramite chat
- Genera presentazioni esecutive e report dettagliati

Prerequisiti

Prima di creare una valutazione della migrazione, verifica di disporre di quanto segue:

- Un'area di lavoro AWS Transform
- Dati di inventario in un formato supportato oppure puoi utilizzare una stima approssimativa tramite chat
- Autorizzazioni appropriate per creare ed eseguire valutazioni

Come funzionano le valutazioni della migrazione

Le valutazioni della migrazione seguono un flusso di lavoro strutturato che guida l'utente dal caricamento iniziale dei dati alla generazione finale dei risultati finali.

Per completare una valutazione della migrazione

1. Crea un lavoro di valutazione della migrazione nel tuo spazio di lavoro AWS Transform.
2. Carica i dati dell'inventario locale.
3. Esamina i risultati di scoperta generati da AWS Transform dai tuoi dati.

4. Gestisci l'ambito dell'inventario escludendo i server o modificando i raggruppamenti.
5. Configura il tuo scenario di valutazione con ipotesi relative a prezzi e infrastruttura.
6. Esegui la valutazione.
7. Rivedi e perfeziona i risultati tramite chat.

Dopo aver esaminato i risultati, puoi creare scenari aggiuntivi, confrontare scenari e generare risultati finali come presentazioni e report.

Caricamento dei dati di inventario

AWS Transform accetta dati di inventario da più fonti. La tabella seguente elenca i formati di dati supportati.

Origine dati	Description
AWS Esportazione Transform Discovery Tool	Inventario automatizzato dei server scoperto dallo strumento di rilevamento AWS Transform
RVTools	Esportazioni da ambienti VMware in ZIP/CSV formato Excel. Sono supportate sia le esportazioni complete che le Info-only esportazioni v.
Dati CMDB	Esportazioni del database di gestione della configurazione
Strumenti di individuazione dei partner	Dati provenienti dagli strumenti di individuazione dei AWS partner
Migration Evaluator	File Quick Insights dalla console Migration Evaluator
Formato MPA	File di importazione della valutazione del portafoglio di migrazione
AWS Trasforma il modello di dati	File Microsoft Excel creato dal modello AWS Transform Assessment Data

AWS Transform identifica automaticamente il formato del file durante l'ingestione. Il processo di inserimento convalida i dati, accetta dati parziali quando mancano alcuni campi e supporta

caricamenti incrementali. Puoi caricare file aggiuntivi in qualsiasi momento per integrare il tuo inventario.

Revisione dei risultati della scoperta

Dopo aver AWS elaborato i dati di inventario, Transform genera un riepilogo della scoperta. La tabella di riepilogo include le seguenti informazioni:

- Numero di server per sistema operativo
- Suddivisione fisica e virtuale del server
- Rilevamento di SQL Server
- Riepiloghi dello storage
- Avvertenze sulla qualità dei dati

Esamina i risultati del rilevamento per confermare che AWS Transform abbia identificato correttamente la tua infrastruttura prima di procedere con la valutazione.

Gestione dell'ambito dell'inventario

Dopo aver esaminato i risultati della scoperta, è possibile affinare l'ambito della valutazione. Utilizza le seguenti azioni per gestire l'ambito dell'inventario:

- Interroga l'inventario per server o carichi di lavoro specifici
- Escludere i server dall'ambito di valutazione
- Esamina i raggruppamenti di server e le dipendenze delle applicazioni
- Identifica i carichi di lavoro di SQL Server per una valutazione specializzata

Configurazione degli scenari di valutazione

Prima di eseguire una valutazione, configura i presupposti utilizzati da AWS Transform per generare consigli. È possibile modificare questi presupposti in qualsiasi momento ed eseguire nuovi scenari con configurazioni diverse.

La tabella seguente elenca le categorie di presupposti disponibili.

Presupposto	Description
Modello tariffario	Database Savings Plans (per Amazon RDS for SQL Server) o On-Demand istanze riservate
Obiettivo Regione AWS	Il Regione AWS luogo in cui intendi ospitare i carichi di lavoro migrati
Esclusioni relative ai tipi di istanza	Famiglie o tipi di istanze Amazon EC2 da escludere dai consigli
Configurazione Amazon EBS	Tipo di volume e impostazioni prestazionali per lo storage
Licenze SQL Server	Bring Your Own Media (BYOM) o licenza inclusa (LI) per Amazon RDS for SQL Server; licenza inclusa (LI) o Bring Your Own License (BYOL) per SQL Server su EC2

Funzionalità di valutazione

AWS Le valutazioni di Transform coprono diverse dimensioni della migrazione. Le sezioni seguenti descrivono ogni capacità di valutazione.

Amazon EC2 dimensionamento corretto

AWS Transform analizza le specifiche del server locale e consiglia istanze Amazon EC2 di dimensioni adeguate. I consigli tengono conto dei requisiti di CPU, memoria e prestazioni.

Archiviazione Amazon EBS

AWS Transform consiglia i tipi di volume e le configurazioni di Amazon EBS in base all'utilizzo corrente dello storage e ai requisiti prestazionali.

Amazon FSx

AWS Transform valuta i carichi di lavoro di storage dei file e fornisce consigli per la migrazione ad Amazon FSx, comprese le stime dei costi per i tipi di file system Amazon FSx supportati.

Amazon RDS per SQL Server

AWS Transform valuta il costo della migrazione dei database SQL Server locali su Amazon RDS for SQL Server. Utilizzando AI-powered gli agenti, AWS Transform analizza l'ambiente SQL Server locale e fornisce un business case completo di migrazione in pochi minuti, con consigli di calcolo e memoria adeguati ai requisiti del carico di lavoro, in modo da evitare l'over-provisioning e pagare solo per ciò di cui hai bisogno.

La valutazione di RDS per SQL Server include le seguenti funzionalità:

- Licenze Bring Your Own Media (BYOM), che consentono di utilizzare le licenze SQL Server esistenti
- Opzioni di licenza License Included (LI)
- Ottimizzazione dei costi con Database Savings Plans, che offrono fino al 20% di risparmio rispetto ai On-Demand prezzi
- Valutazione dell'idoneità per il AWS Migration Acceleration Program (MAP), che fornisce crediti e supporto per compensare i costi di migrazione

Puoi iniziare la valutazione di RDS for SQL Server con qualsiasi formato di dati supportato, incluse le esportazioni RVTools, i dati del database di gestione della configurazione (CMDDB), le esportazioni dallo strumento di rilevamento AWS Transform e altri strumenti di rilevamento di terze parti. Crea scenari ipotetici per confrontare più modelli di costo con ipotesi personalizzate, tra cui regione, utilizzo delle risorse e condizioni di prezzo.

Prompt di esempio:

- «Stima il costo della migrazione dei miei database SQL Server a RDS per SQL Server»
- «Confronta i prezzi BYOM con quelli con licenza inclusa per RDS per SQL Server»
- «Mostrami le opzioni di Database Savings Plans per i miei carichi di lavoro RDS»

Server SQL Amazon EC2

AWS Transform valuta i carichi di lavoro di SQL Server e fornisce consigli per l'esecuzione di SQL Server su Amazon EC2, tra cui analisi delle licenze e mappature degli host dedicati.

On-premises prezzi

AWS Transform stima i costi correnti locali per fornire una base di riferimento per il confronto con AWS i prezzi. Puoi apportare modifiche complessive ai costi tramite chat. On-premises gli adeguamenti dei costi si riflettono nel rapporto PDF e nelle risposte alla chat, ma non nell'esportazione PPTX.

Prompt di esempio:

- «Aggiorna il costo del server locale a 500 dollari per server al mese»
- «Aggiungete i costi annuali delle strutture del centro dati di 50.000 dollari»

Sostenibilità

AWS Transform stima la riduzione dell'impronta di carbonio derivante dalla migrazione a AWS. Puoi esplorare le metriche di sostenibilità tramite chat.

Prova a usare istruzioni come:

- «Mostrami la riduzione di carbonio stimata per questa migrazione»
- «In cosa consiste il miglioramento dell'efficienza energetica per i miei carichi di lavoro AWS?»

Valutazione del valore aziendale

AWS Transform valuta il valore aziendale più ampio della migrazione oltre al risparmio sui costi dell'infrastruttura. La valutazione riguarda la produttività, la resilienza e l'agilità aziendale del personale.

Ecco alcuni esempi di istruzioni:

- «Stima i guadagni di produttività del personale derivanti dalla migrazione a» AWS
- «Quali miglioramenti della resilienza posso aspettarmi dopo la migrazione?»
- «Mostratemi i vantaggi di questa migrazione in termini di agilità aziendale»

Costi di rete

AWS Transform stima i costi relativi alla rete per la migrazione, inclusi il trasferimento dei dati e i requisiti di connettività.

Costi di supporto

AWS Transform include i costi del piano di AWS supporto nella valutazione in base al livello di supporto selezionato.

Elaborazione degli utenti finali

AWS Transform valuta i carichi di lavoro informatici degli utenti finali e fornisce consigli per i servizi informatici per gli utenti AWS finali.

Utilizzo di valutazioni basate su chat

Puoi interagire con AWS Transform tramite chat per creare e perfezionare le valutazioni. La chat supporta tre modalità di interazione.

Puoi affinare la tua valutazione in modo iterativo continuando la conversazione. AWS Transform mantiene il contesto tra i messaggi e aggiorna i risultati della valutazione in base ai tuoi input.

Stima approssimativa con dati limitati

Puoi ottenere una stima approssimativa dei costi descrivendo il tuo ambiente in chat senza caricare file di inventario dettagliati. La stima approssimativa è una funzionalità autonoma e non può essere combinata con i dati di inventario caricati o l'arricchimento dei dati tramite chat.

Puoi usare istruzioni come queste:

- «Ho 200 server Windows e 150 server Linux, stimate i miei costi» AWS
- «Datemi una stima approssimativa per la migrazione di 500 macchine virtuali verso» AWS
- «Stima dei costi per 50 server con una media di 8 CPU e 32 GB di RAM»

Aggiungere l'inventario tramite chat

Puoi fornire i dettagli dell'inventario direttamente tramite chat per integrare o sostituire i file caricati.

Utilizza istruzioni come le seguenti:

- «Includi un server di database che esegue Oracle su 4 CPU con 128 GB di RAM»
- «Aggiungi 20 server web che eseguono Linux con 4 CPU e 16 GB di RAM»

Modifica dei costi e aggiunta di servizi

Puoi modificare i costi locali e aggiungere AWS servizi alla tua valutazione tramite chat.

Esempi di istruzioni per gli aggiustamenti locali:

- «Aumenta i costi locali del 15% per tenere conto del prossimo aggiornamento dell'hardware»
- «Aggiungi costi di manutenzione annuali di 100.000 dollari alla linea di base locale»

Puoi anche aggiungere stime approssimative dei costi per AWS i servizi che non sono completamente supportati dalle valutazioni di Transform. AWS Ciò fornisce un'analisi più completa, ma queste stime sono meno accurate delle raccomandazioni automatiche.

- «Aggiungi i costi AWS di Backup per tutti i server migrati»
- «Includi i costi di CloudWatch monitoraggio di Amazon nella stima»
- «Aggiungi i costi AWS Direct Connect per una connessione a 10 Gbps»

Scenari a confronto

È possibile creare più scenari di valutazione con ipotesi diverse e confrontarli per identificare la strategia di migrazione ottimale.

Creazione di scenari

Prova i prompt come:

- «Crea uno scenario BYOM per la migrazione dei database di SQL Server a RDS per SQL Server»
- «Crea uno scenario con Database Savings Plans for RDS per SQL Server»
- «Crea uno scenario LI per tutti i carichi di lavoro di SQL Server su EC2»
- «Crea uno scenario con tutti i carichi di lavoro in us-west-2»

Esecuzione di confronti

Ecco alcuni esempi di istruzioni:

- «Mostrami un confronto dei costi in tutti gli scenari»

- «Qual è lo scenario con il costo totale di proprietà più basso?»

What-if analisi

Modella l'impatto di modifiche specifiche senza creare uno scenario completamente nuovo.

Prompt di esempio:

- «Cosa succede se sposto i miei carichi di lavoro di SQL Server su RDS per SQL Server anziché su EC2?»
- «Qual è la differenza di costo tra BYOM e License Included for RDS for SQL Server?»
- «Cosa succede se escludo i 50 server più piccoli dalla migrazione?»
- «E se utilizzo solo istanze ottimizzate per lo storage?»
- «Qual è l'impatto del passaggio dai volumi gp3 a io2?»

Generazione di risultati

Dopo aver completato la valutazione, puoi generare risultati finali in più formati. La tabella seguente descrive i formati di output disponibili.

Formato	Description	Personalizzazione
PPTX () PowerPoint	Presentazione esecutiva con sintesi dei risultati e delle raccomandazioni	Struttura fissa
XLSX (Excel)	Esportazione dettagliata dei dati con consigli a livello di server e suddivisione dei costi	Struttura fissa
PDF	Documento di rapporto	Personalizzabile tramite chat

Argomenti correlati

- [Nozioni di base](#)
- [Lavori personalizzati](#)

- [Strumento di scoperta](#)

Personalizzato

Che cos'è AWS Trasformazione personalizzata?

AWS Transform custom utilizza l'intelligenza artificiale agentica per eseguire la modernizzazione su larga scala di software, codice, librerie e framework per ridurre il debito tecnico. Gestisce diversi scenari, tra cui aggiornamenti delle versioni linguistiche, migrazioni di API e servizi, aggiornamenti e migrazioni del framework, refactoring del codice e trasformazioni specifiche dell'organizzazione.

Grazie all'apprendimento continuo, l'agente migliora sulla base di ogni esecuzione e feedback degli sviluppatori, offrendo trasformazioni ripetibili e di alta qualità senza richiedere competenze specializzate in automazione.

Funzionalità chiave

AWS Transform custom offre le seguenti funzionalità:

- Definizione di trasformazione basata sul linguaggio naturale: crea trasformazioni personalizzate utilizzando linguaggio naturale, documentazione ed esempi di codice
- Esecuzione della trasformazione: applica le trasformazioni in modo coerente e affidabile su più basi di codice
- Apprendimento continuo: migliora automaticamente la qualità della trasformazione a partire da ogni esecuzione
- AWS-trasformazioni gestite - Utilizza trasformazioni pronte all'uso e controllate per scenari comuni AWS

Modelli di trasformazione

AWS Transform custom supporta diversi modelli di trasformazione per soddisfare le vostre esigenze di modernizzazione. Ogni modello presenta caratteristiche di complessità diverse in base all'ambito e alla natura delle modifiche richieste.

Pattern	Description	Complessità	Esempi
Migrazioni di API e servizi	Migrazione tra versioni API o	Media	AWS SDK v1 → v2 (Java, Python,), Boto2

Pattern	Description	Complessità	Esempi
	servizi equivalenti mantenendo la funzionalità		→ Boto3, JUnit 4 → 5, javax → JavaScript jakarta
Aggiornamenti della versione linguistica	Aggiornamento a versioni più recenti dello stesso linguaggio o di programmazione, adozione di nuove funzionalità e sostituzione di funzionalità obsolete	Low-Medium	Java 8→17, Python 3.9→3.13, 12→22, aggiornamenti di versione Node.js TypeScript
Aggiornamenti del framework	Aggiornamento a versioni più recenti dello stesso framework, risoluzione delle modifiche più importanti	Media	Spring Boot 2.x→3.x, React 17→18, aggiornamenti Angular, aggiornamenti Django
Migrazioni del framework	Migrazione verso framework completamente diversi che hanno scopi simili	Elevata	Angular→React, Redux→Zustand, →React Vue.js
Aggiornamenti della libreria e delle dipendenze	Aggiornamento delle librerie di terze parti a versioni più recenti mantenendo lo stesso linguaggio e lo stesso framework	Low-Medium	Pandas 1.x→2.x, aggiornamenti, aggiornamenti delle librerie, aggiornamenti Lodash NumPy Hadoop/HBase/Hive

Pattern	Description	Complessità	Esempi
Rifattorizzazione del codice e modernizzazione dei pattern	Modernizzazione dei modelli di codice e adozione delle migliori pratiche senza modificare le funzionalità esterne	Low-Medium	Stampa → Framework di registrazione, concatenazione di stringhe → stringhe f, adozione di suggerimenti di tipo, strumentazione di osservabilità
File-by-File Script e traduzioni	Traduzione di script o file di configurazione indipendenti in cui i file sono per lo più autonomi	Low-Medium	AWS CDK→Terraform, Terraform→, Excel→Quaderni PythonCloudFormation, Bash→ PowerShell
Migrazioni dell'architettura	Migrazione tra architetture hardware o ambienti di runtime con modifiche minime al codice	Medium-High	x86 →AWS Graviton (ARM), locale → Lambda, server tradizionale → contenitori
Language-to-Language Migrazioni	Traduzione di codebase da un linguaggio di programmazione a un altro	Molto alto	Java→Python, →, C→Rust, JavaScript Python→Vai TypeScript
Personalizzazione Organization-Specific e trasformazioni	Requisiti organizzativi unici ed esigenze di modernizzazione specializzate	Può variare	Migrazioni personalizzate di librerie interne, standard di codifica specifici dell'organizzazione, migrazioni di framework proprietari

 Note

Per le lingue, usa Transform for COBOL/mainframe Mainframe. AWS Per gli aggiornamenti di .NET Framework a .NET Core, prendi in considerazione AWS Transform for Windows. Per le migrazioni da VMware a AWS, prendi in considerazione AWS Transform for VMware.

In che modo AWS Transform Custom Works

AWS Transform custom viene solitamente utilizzato in progetti su larga scala in cui vengono trasformate più basi di codice o moduli. I team in genere seguono un flusso di lavoro in quattro fasi:

Definisci la trasformazione: fornisci all'agente istruzioni, documentazione ed esempi di codice in linguaggio naturale, che genera una definizione iniziale di trasformazione. Questa definizione può essere perfezionata in modo iterativo tramite chat o modifiche dirette. Questa fase può essere saltata quando si utilizzano AWS trasformazioni gestite.

Pilota o Proof-of-Concept: testa la trasformazione su basi di codice di esempio e perfezionala in base ai risultati. Questa fase di convalida aiuta a stimare i costi e gli sforzi della trasformazione completa. L'apprendimento continuo migliora la qualità durante questa fase.

Esecuzione scalata: configura l'esecuzione di massa automatizzata utilizzando la CLI, con gli sviluppatori che esaminano e convalidano i risultati. Monitora i progressi utilizzando l'applicazione web e monitora le trasformazioni su più repository.

Monitoraggio e revisione: l'apprendimento continuo migliora automaticamente la qualità della trasformazione. Rivedi le lezioni estratte dalle esecuzioni precedenti per assicurarti che soddisfino gli standard di qualità e archivia quelle che non sono utili.

Comprensione dei concetti chiave di

Questa sezione spiega i concetti chiave per lavorare con AWS Transform custom.

Definizioni di trasformazione

Una definizione di trasformazione contiene le istruzioni e le conoscenze necessarie per eseguire una trasformazione specifica del codice. È rappresentata come un'abilità e consiste in:

- **SKILL.md**(obbligatorio) - Istruzioni in Markdown con frontespizio (name e description campi) YAML che contiene la logica di trasformazione di base e le istruzioni di esecuzione

- `references/folder` (opzionale) - Documentazione caricata secondo necessità durante l'esecuzione della trasformazione
- `scripts/folder` (opzionale): script che la trasformazione scarica ed esegue durante l'esecuzione

AWS Transform CLI scarica automaticamente le definizioni di trasformazione nella directory corrente quando necessario per l'esecuzione, l'ispezione o la modifica.

Important

Quando si pubblica una trasformazione, la directory deve contenere solo `SKILL.md` e facoltativamente la `references/` cartella, la `scripts/` cartella o entrambe. Non sono consentiti altri file o sottodirectory.

Note

La versione CLI 2.0 e successive utilizza il formato `skills`. Le definizioni di trasformazione esistenti vengono gestite automaticamente dalla CLI.

Registro delle trasformazioni

Il registro delle trasformazioni è l'archivio centralizzato del tuo AWS account per l'archiviazione e la gestione delle definizioni di trasformazione. Le trasformazioni nel registro possono essere:

- Elencato utilizzando `atx custom def list`
- Eseguito su più basi di codice
- Condiviso con altri utenti del tuo account AWS
- Version-controlled

Important

Le definizioni di trasformazione sono specifiche dell'account. Se desideri utilizzare una trasformazione in un AWS account diverso, devi pubblicarla separatamente in quell'account.

Bozza e trasformazioni pubblicate

AWS Transform custom supporta due stati per le trasformazioni nel registro:

Le bozze di trasformazione sono definizioni di trasformazione in corso o non testate. Vengono salvate come versioni specifiche e possono essere recuperate, aggiornate ed eseguite dagli utenti che fanno riferimento a quella versione specifica. Le bozze sono utili per lo sviluppo, il test e il perfezionamento iterativi prima che la trasformazione sia pronta per essere condivisa con il team. Le bozze sono anche associate a conversazioni specifiche. Se riavvii la CLI, puoi utilizzarla `atx --conversation-id {id}` per ripristinarne una precedente.

Le trasformazioni pubblicate sono disponibili nel registro delle trasformazioni del tuo account per essere eseguite da altri utenti con le autorizzazioni IAM richieste. Le trasformazioni pubblicate possono essere scoperte utilizzando `atx custom def list`

Il flusso di lavoro tipico è:

1. Creare la trasformazione a livello locale
2. Salva come bozza per il test (`atx custom def save-draft`)
3. Perfeziona e convalida
4. Pubblica per dividerlo con il tuo team (`atx custom def publish`)

Puoi anche pubblicare una trasformazione direttamente senza salvarla come bozza.

Riferimenti vs. lezioni

AWS Transform custom utilizza due tipi di conoscenze per migliorare la qualità della trasformazione:

I riferimenti sono documentazione fornita dall'utente memorizzata nella `references/` cartella di una definizione di trasformazione. I riferimenti supportano solo file di testo (massimo 10 MB in totale per tutti i file) e di solito contengono documentazione, specifiche API, guide alla migrazione ed esempi di codice. I riferimenti vengono caricati secondo necessità durante l'esecuzione della trasformazione. I riferimenti vengono aggiunti durante la creazione o l'aggiornamento di una definizione di trasformazione in modalità interattiva.

Le lezioni vengono estratte automaticamente dalle esecuzioni precedenti di una trasformazione. Il sistema di apprendimento continuo le genera sulla base delle traiettorie di esecuzione, del feedback degli sviluppatori e delle correzioni di codice riscontrate durante le trasformazioni. Raggruppa

le lezioni correlate in categorie in modo da poterle rivedere insieme. A differenza dei riferimenti, che vengono forniti in anticipo, le lezioni si accumulano nel tempo man mano che si esegue la trasformazione su diverse basi di codice e il sistema le applica automaticamente per migliorare le esecuzioni future. Puoi rivedere e gestire le lezioni in modo interattivo con `atx custom def learnings`

Comandi di creazione e convalida

Il comando `build` o `validation` è un parametro opzionale che specifica come convalidare il codice durante il processo di trasformazione. Questo comando viene eseguito in vari punti durante la trasformazione per garantire l'integrità del codice.

Fornire un comando che convalidi i risultati e restituisca problemi se la convalida fallisce è molto importante per migliorare la qualità della trasformazione attraverso l'apprendimento continuo. Se non è necessaria alcuna compilazione o convalida, omettila dal tuo input.

Per esempi e linee guida dettagliate, consulta Comandi di compilazione e convalida nella sezione Flussi di lavoro.

Apprendimento continuo

L'apprendimento continuo è il sistema che acquisisce automaticamente il feedback da ogni esecuzione di trasformazione e migliora la qualità della trasformazione nel tempo. Il sistema raccoglie informazioni tramite:

- Feedback esplicito: commenti e correzioni di codice forniti in modalità interattiva
- Osservazioni implicite: problemi riscontrati dall'agente durante la trasformazione e il debug del codice

Il sistema di apprendimento continuo elabora queste informazioni per creare lezioni da aggiungere alla definizione di trasformazione per migliorare le trasformazioni future. Il sistema esegue automaticamente il processo di apprendimento dopo il completamento delle trasformazioni, senza richiedere alcun input aggiuntivo da parte dell'utente.

Important

Le lezioni sono specifiche della trasformazione e non vengono condivise tra diverse trasformazioni o diversi account cliente.

Gestione delle lezioni

Il sistema genera automaticamente le lezioni, ma sei tu a decidere quali applicare alle sessioni future. Il `atx custom def learnings` comando apre una sessione terminale interattiva per la revisione e la cura delle lezioni accumulate durante la trasformazione.

In questa sessione, puoi:

- Sfoglia le lezioni raggruppate in categorie e scopri quante lezioni attive contiene ciascuna categoria.
- Apri una lezione per leggerne tutti i dettagli, tra cui il corpo della lezione, il suo impatto e quante sessioni precedenti l'hai consultata.
- Archivia una lezione per impedire al sistema di applicarla a esecuzioni future e ripristinala in un secondo momento, se necessario.
- Elimina definitivamente una lezione archiviata che non è più utile.

Per istruzioni dettagliate, consulta [the section called “Apprendimento continuo”](#).

Client-Side Competenze

Client-side le competenze sono funzionalità aggiuntive che estendono l'agente durante le esecuzioni di trasformazione. A differenza delle definizioni di trasformazione che definiscono la trasformazione da eseguire, le competenze lato client forniscono strumenti, script e istruzioni supplementari che l'agente può utilizzare insieme alle funzionalità integrate durante qualsiasi trasformazione.

Client-side le competenze vengono rilevate nelle directory a livello di progetto e a livello di utente. Posiziona le competenze a livello di progetto quando applicano gli standard specifici di un repository e a livello di utente quando si applicano a tutti i tuoi progetti. Project-level le competenze sono disponibili solo quando viene fornito un percorso di archiviazione del codice. Per la configurazione e l'utilizzo dettagliati, vedere [the section called “Client-Side Competenze”](#).

Nozioni di base

Questa sezione descrive come configurare AWS Transform personalizzato ed eseguire la prima trasformazione.

Prerequisiti

Prima di installare AWS Transform custom, assicurati di disporre di quanto segue:

Piattaforme supportate

AWS Transform custom supporta i seguenti sistemi operativi:

- Linux: supporto completo per tutte le distribuzioni Linux
- macOS: supporto completo per i sistemi macOS
- Windows: supporto completo per Windows nativo che utilizza Windows Terminal e PowerShell (i `atx` `ct` comandi non sono ancora supportati su Windows)
- Windows Subsystem for Linux (WSL): supportato durante l'esecuzione in WSL

Software richiesto

- Node.js 22 o versione successiva - Scarica da <https://nodejs.org/en/download>
- Git: deve essere installato e la directory di lavoro deve essere un repository Git valido per eseguire una trasformazione. Esegui `git init`; `git add .`; `git commit -m "Initial commit"` per inizializzare un repository Git nella tua directory di lavoro.

Requisiti di rete

È necessaria una connessione Internet con accesso ai seguenti endpoint:

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

Se lavori in un ambiente con restrizioni Internet, aggiorna le regole del firewall per inserire questi URL nella lista consentita.

Installazione di AWS Trasforma CLI

Il metodo di installazione consigliato è l'utilizzo dello script di installazione. Scegli la scheda relativa al tuo sistema operativo.

Per installare la CLI AWS Transform

1. Esegui lo script di installazione:

Linux and macOS

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

Windows (PowerShell)

Su Windows nativo, esegui lo script di installazione da Windows Terminal utilizzando PowerShell.

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

2. Verifica l'installazione:

```
atx --version
```

Il comando dovrebbe visualizzare la versione installata della CLI AWS Transform.

Configurazione dell'autenticazione

AWS Transform custom richiede AWS credenziali per l'autenticazione con il servizio. Configura l'autenticazione utilizzando uno dei seguenti metodi.

Variabili di ambiente

Imposta le seguenti variabili di ambiente.

Linux and macOS

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

Windows (PowerShell)

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

```
$env:AWS_SESSION_TOKEN="your_session_token"
```

È inoltre possibile specificare un profilo utilizzando la variabile di AWS_PROFILE ambiente.

Linux and macOS

```
export AWS_PROFILE=your_profile_name
```

Windows (PowerShell)

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

Note

Le variabili di ambiente impostate con `$env :` in PowerShell si applicano solo alla sessione corrente. Per mantenerle tra le sessioni, impostale tramite Proprietà del sistema > Variabili d'ambiente oppure utilizza `[System.Environment]::SetEnvironmentVariable()`.

AWS File di credenziali

Configura le AWS credenziali nel file delle credenziali, disponibile `~/.aws/credentials` su Linux e macOS o su Windows: `%USERPROFILE%\aws\credentials`

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

Autorizzazioni IAM

AWS Le tue credenziali devono disporre delle autorizzazioni per chiamare il servizio personalizzato Transform. AWS Ti consigliamo di allegare la policy [AWSTransformCustomFullAccess](#) AWS gestita al tuo utente o ruolo IAM. Questa policy fornisce l'accesso completo a AWS Transform custom, inclusa l'autorizzazione a creare il [ruolo collegato al servizio](#) necessario per l'emissione delle CloudWatch metriche sul tuo account.

Per un controllo più granulare, AWS Transform custom fornisce anche le seguenti politiche gestite: AWS

- [AWSTransformCustomExecuteTransformations](#)— Fornisce l'accesso per eseguire trasformazioni.
- [AWSTransformCustomManageTransformations](#)— Fornisce l'accesso per creare, aggiornare, leggere ed eliminare risorse di trasformazione, nonché per eseguire trasformazioni.

Per ulteriori informazioni su queste politiche, consulta le [politiche AWS gestite per AWS Transform](#). Per le policy IAM personalizzate con autorizzazioni a livello di risorsa, consulta la [AWS Transform Custom IAM](#) Service Authorization Reference Guide.

Note

- Le definizioni di trasformazione sono AWS risorse con ARN (Amazon Resource Names). Puoi utilizzare le policy IAM per controllare l'accesso a trasformazioni o gruppi di trasformazioni specifici specificando l'ARN della trasformazione nelle istruzioni di risorse delle policy IAM. I tag possono essere utilizzati per il controllo degli accessi raggruppati.
- AWS IAM Identity Center è necessario per accedere a AWS Transform, ma non è necessario per utilizzare la CLI.

Configurazione AWS Region

AWS Transform custom è disponibile in AWS aree specifiche e rileva automaticamente la configurazione della regione utilizzando la precedenza AWS CLI standard.

Regioni supportate

AWS Transform custom è disponibile nelle seguenti regioni: AWS

- `us-east-1`(Stati Uniti orientali - Virginia settentrionale)
- `eu-central-1`(Europa - Francoforte)
- `eu-west-2`(Europa - Londra)
- `ca-central-1`(Canada - Centrale)
- `ap-northeast-1`(Asia Pacifico - Tokyo)
- `ap-northeast-2`(Asia Pacifico - Seoul)
- `ap-southeast-2`(Asia Pacifico - Sydney)

- ap-south-1(Asia Pacifico - Mumbai)

Come viene determinata la regione

La CLI controlla queste fonti in modo prioritario per determinare quale regione utilizzare:

1. AWS_REGION variabile di ambiente (priorità massima)
2. Variabile di ambiente AWS_DEFAULT_REGION
3. Profilo selezionato nel file di AWS configurazione (tramite variabile di AWS_PROFILE ambiente)
4. Profilo predefinito nel file di AWS configurazione
5. Fallback predefinito us-east-1 se non viene trovata alcuna configurazione

Note

Il file di AWS configurazione si trova ~/.aws/config in Linux e macOS %USERPROFILE%\ .aws\config o in Windows.

Note

Se ATX_CUSTOM_ENDPOINT è impostata, la regione viene estratta dall'URL dell'endpoint e sostituisce tutte le altre impostazioni.

Impostazione della regione

Scegli uno di questi metodi per configurare la tua regione:

Opzione 1: variabile di ambiente (consigliata per l'uso temporaneo):

Linux and macOS

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

Windows (PowerShell)

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

Opzione 2: configurazione AWS CLI (consigliata per la configurazione permanente):

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

Opzione 3: Profile-specific configurazione:

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"
```

Opzione 4: modifica diretta dei file:

Modifica direttamente il file di AWS configurazione (~/.aws/config su Linux e macOS
%USERPROFILE%\aws\config o su Windows):

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

Verifica della configurazione della regione

Per verificare quale regione verrà utilizzata da AWS Transform custom:

Controlla l'impostazione attuale della regione:

```
aws configure get region
```

Controlla le variabili di ambiente:

Linux and macOS

```
echo "AWS_REGION: $AWS_REGION"
```

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

Windows (PowerShell)

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

Visualizza la risoluzione dettagliata della regione nei log di debug:

Linux and macOS

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

Windows (PowerShell)

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

Esempio di output di registro che mostra l'origine della regione:

```
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"  
}
```

Il `regionSource` campo mostra da dove è stata derivata la regione (ad esempio, «aws-config (profile: default)», «AWS_REGION», «default»).

Important

Se la configurazione della tua regione punta a un'area non supportata, la CLI mostrerà un messaggio di errore chiaro con le istruzioni per aggiornare la configurazione a una regione supportata.

Esecuzione della prima trasformazione

Il modo più veloce per iniziare è utilizzare una trasformazione AWS gestita. AWS-le trasformazioni gestite sono trasformazioni predefinite e AWS controllate, pronte all'uso senza alcuna configurazione.

Per eseguire una trasformazione gestita in modo interattivo: AWS

```
atx
```

Quindi chiedi all'agente di eseguire una trasformazione:

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

Per eseguire una trasformazione in modo non interattivo:

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

Per informazioni dettagliate sulle modalità di esecuzione, le opzioni di configurazione e i flag di comando, vedere. [the section called “Riferimento ai comandi”](#)

Comprensione dei risultati della trasformazione

Al termine di una trasformazione, AWS Transform custom fornisce un rapporto che descrive i risultati. Se la trasformazione non è stata convalidata (ad esempio, creazione riuscita per un'applicazione Java), il rapporto fornisce consigli per ulteriori azioni.

La maggior parte delle trasformazioni viene eseguita in più passaggi, utilizzando Git per eseguire il commit di quelle intermedie. Puoi rivedere le modifiche apportate dalla trasformazione usando i comandi Git standard:

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

Creazione di una trasformazione personalizzata

Quando le trasformazioni AWS gestite non soddisfano le tue esigenze, puoi creare trasformazioni personalizzate su misura per i tuoi requisiti specifici.

Per creare una trasformazione personalizzata

1. Avvia la CLI AWS Transform in modalità interattiva:

```
atx
```

2. Spiega all'agente che desideri creare una nuova trasformazione e descrivi le tue esigenze.
3. Fornisci materiali di riferimento come documentazione ed esempi di codice per migliorare la qualità.
4. Testa e perfeziona la trasformazione in modo iterativo.
5. Pubblicala nel registro delle trasformazioni della tua organizzazione.

Per istruzioni dettagliate sulla creazione di trasformazioni personalizzate, consulta [the section called “Flussi di lavoro”](#).

AWS Transform Web Application (opzionale)

L'applicazione web AWS Transform è un'interfaccia opzionale per il monitoraggio di campagne di trasformazione su larga scala su più repository. Prima di utilizzare l'applicazione web AWS Transform, devi avere un'identità utente abilitata per accedere a AWS Transform nella tua organizzazione. Per informazioni sull'attivazione di AWS Transform, consulta [Configurazione di AWS Transform](#).

Per utilizzare l'applicazione web AWS Transform:

1. Visita <https://aws.amazon.com/transform/> e accedi utilizzando le credenziali AWS IAM Identity Center.
2. Seleziona il tipo di lavoro «Personalizzato/codice» nell'applicazione web AWS Transform.
3. Indica all'agente il nome della definizione di trasformazione che desideri utilizzare.
4. L'applicazione Web fornisce un comando AWS Transform CLI che può essere condiviso con il team. Questo comando richiama la definizione della trasformazione e registra i risultati dell'esecuzione nell'applicazione Web.
5. Dopo aver acquisito i risultati della trasformazione, visualizza le statistiche, le misurazioni del risparmio di tempo e poni domande sullo stato di avanzamento del lavoro nella Dashboard.

L'applicazione Web è progettata per operazioni su scala aziendale in cui è necessario il monitoraggio centralizzato delle trasformazioni su più basi di codice.

 Note

AWS IAM Identity Center è necessario per accedere all'applicazione web Transform. AWS La CLI non richiede IAM Identity Center: sono necessarie solo AWS credenziali standard.

Introduzione ai comandi di trasformazione personalizzati

Di seguito sono riportati alcuni comandi che è possibile utilizzare con le trasformazioni personalizzate. L'elenco completo dei comandi si trova nel riferimento ai [comandi AWS Transform custom transformations](#).

- `atx custom`
 - Esegue un'esperienza interattiva di trasformazione personalizzata, che consente la creazione, l'individuazione, l'esecuzione e il perfezionamento delle trasformazioni.
 - Questo è il comando predefinito per `atx`
 - `--trust-all-tools(-t)` è facoltativo e consente implicitamente tutte le richieste di strumenti richieste dall'agente. Usare con cautela soprattutto negli ambienti di produzione. È possibile configurare l'attendibilità degli strumenti per strumenti e comandi specifici utilizzando il [file delle impostazioni di attendibilità](#).
- `atx custom --help` | `atx custom -h`
 - Mostra il menu di aiuto.
 - Ogni comando include anche un menu di aiuto, ad esempio `atx custom def exec --help`.
- `atx --version` | `atx -v`
 - Mostra la versione.
 - Il numero di versione cambia con ogni versione.
- `atx custom def list`
 - Stampa l'elenco delle trasformazioni disponibili nel registro delle trasformazioni.
- `atx custom def exec`
 - Esegue una trasformazione
- `atx custom def learnings`
 - Apre una sessione interattiva per visualizzare e gestire le lezioni apprese da una trasformazione nelle esecuzioni precedenti
- `atx mcp`

- Utilizzato per gestire le configurazioni del server MCP

Flussi di lavoro

Esecuzione di trasformazioni

Questa sezione descrive i diversi modi di eseguire le trasformazioni e le opzioni per controllare il comportamento di esecuzione.

Modalità di esecuzione

AWS Transform custom supporta tre modalità di esecuzione per adattarsi a diversi flussi di lavoro.

Modalità conversazionale interattiva

Avvia la CLI con `atx` e chiedi all'agente di eseguire una trasformazione tramite linguaggio naturale. Questa modalità consente di avere una conversazione completa con l'agente, interrompere l'esecuzione in qualsiasi momento e fornire feedback durante il processo di trasformazione.

Utilizzate questa modalità quando desiderate il massimo controllo e la capacità di guidare l'agente attraverso scenari complessi.

Esecuzione interattiva diretta

`atx custom def exec -n <transformation-name> -p <path>` Da utilizzare per avviare una trasformazione specifica in modo interattivo. Questa modalità consente di rivedere e interagire con l'agente all'inizio, durante o alla fine dell'esecuzione. L'agente si fermerà nei momenti decisionali chiave e chiederà il tuo contributo.

È ideale per testare e perfezionare le trasformazioni prima di eseguirle autonomamente.

È possibile eseguire trasformazioni in modalità non interattiva o in modalità headless. Non-interactive mode sopprime i prompt durante una trasformazione denominata. La modalità headless consente di eseguire l'agente con un prompt in testo semplice, ignorando completamente l'interfaccia interattiva.

Non-interactive modalità

Utilizzare `atx custom def exec -n <transformation-name> -p <path> -x -t` per l'automazione completa. Aggiungi `-x` per funzionare in modalità non interattiva e affidati automaticamente `-t` a tutti gli strumenti senza richiedere conferma.

Questa modalità è progettata per l'integrazione della CI/CD pipeline e l'esecuzione in blocco laddove non è disponibile o richiesto alcun intervento umano.

modalità Headless

Per completare le attività senza interagire con l'agente, esegui `atx -x "<prompt>" -t` e fornisci le istruzioni in testo semplice.

Esecuzione della trasformazione senza intoppi

Utilizzate questa modalità per applicare una definizione di trasformazione esistente alla vostra codebase. La trasformazione esegue automaticamente ogni fase senza richiedere l'approvazione dell'utente.

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

Sviluppo di una trasformazione senza fronzoli

Crea o modifica le definizioni di trasformazione.

Per convertire una definizione di trasformazione precedente nel nuovo formato di abilità (SKILL.md + references/), esegui il comando seguente:

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

Per creare una nuova definizione di trasformazione, esegui il comando seguente:

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

Bandiere di comando comuni

Quando si eseguono trasformazioni con `atx custom def exec`, vengono comunemente utilizzati i seguenti flag:

- `-no--transformation-name`: specifica il nome della trasformazione da eseguire
- `-po--code-repository-path`: specifica il percorso della base di codice (usa «.» per la directory corrente)

- `-co--build-command`: specifica il comando di compilazione o convalida da eseguire
- `-xo --non-interactive` - Abilita la modalità non interattiva (nessuna richiesta dell'utente)
- `-toppure --trust-all-tools` - Si fida automaticamente di tutti gli strumenti senza chiedere conferma
- `-do --do-not-learn` - Impedisce l'estrazione della lezione da questa esecuzione
- `--tvo--transformation-version`: specifica una versione specifica della trasformazione
- `-go --configuration` - Fornisce un file di configurazione o una configurazione in linea

Important

Il `--trust-all-tools` flag `-t` or approva automaticamente tutte le esecuzioni degli strumenti senza chiedere conferma e aggira la maggior parte delle barriere di sicurezza (i comandi che corrispondono all'`alwaysPromptCommandselenco` richiedono comunque un'autorizzazione esplicita a meno che non vengano sovrascritti da). `trustedShellCommands` Il passaggio è necessario per un'`--non-interactive` esperienza completamente autonoma, ma `--trust-all-tools` non è necessario per eseguire la trasformazione. Usare con cautela negli ambienti di produzione.

Utilizzo dei file di configurazione

AWS Transform custom supporta file di configurazione opzionali in formato YAML o JSON. I file di configurazione consentono di specificare i parametri di esecuzione e fornire un contesto aggiuntivo all'agente.

Per utilizzare un file di configurazione:

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

Puoi anche fornire la configurazione come coppie chiave-valore in linea:

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

File di configurazione di esempio (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
```

Il `additionalPlanContext` parametro fornisce un contesto aggiuntivo per il piano di esecuzione dell'agente. Ciò è particolarmente utile con le AWS trasformazioni gestite per personalizzare il loro comportamento in base a esigenze specifiche.

Comandi di compilazione e convalida

Il comando `build` o `validation` è un parametro opzionale che specifica come convalidare il codice durante il processo di trasformazione. AWS Transform custom tenterà di dedurre il miglior comando di compilazione in base alla trasformazione se non specificato, sebbene si consiglia di specificarlo per quanto riguarda la qualità.

Esempi di comandi di compilazione e convalida:

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

Anche per i linguaggi o le trasformazioni che non richiedono la compilazione, è molto importante fornire un comando che convalidi i risultati e restituisca problemi se la convalida fallisce per migliorare la qualità della trasformazione.

Se non è necessaria alcuna compilazione o convalida, omettila dal tuo input.

Controllo del comportamento di apprendimento

Per impostazione predefinita, AWS Transform custom estrae le lezioni da ogni esecuzione di trasformazione. È possibile impedire l'apprendimento per esecuzioni specifiche.

Per impedire l'apprendimento da un'esecuzione:

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

Il `--do-not-learn` flag `-d` disattiva l'estrazione della lezione dall'esecuzione corrente.

Ripresa delle conversazioni

AWS Transform custom ti consente di riprendere le conversazioni precedenti entro 30 giorni dalla creazione.

Per riprendere la conversazione più recente:

```
atx --resume
```

Per riprendere una conversazione specifica:

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

Important

Le conversazioni possono essere riprese solo entro 30 giorni dalla creazione. Dopo 30 giorni, la conversazione non può più essere ripresa.

Tracking Agent Minutes

AWS Transform custom tiene traccia dei [minuti consumati dall'agente](#) durante una sessione di trasformazione. I minuti degli agenti si accumulano durante il ciclo di vita della conversazione e vengono visualizzati al termine della conversazione:

```
Agent minutes used: 12.50
```

I minuti degli agenti persistono anche dopo le interruzioni. Se si interrompe una sessione con `Ctrl +C` e la si riprende in un secondo momento, i minuti accumulati in precedenza vengono trasferiti e continuano ad accumularsi nella sessione ripresa.

Per controllare Agent Minutes durante una sessione interattiva:

Digitate `/usage` al prompt di input per visualizzare gli Agent Minutes attualmente accumulati senza terminare la conversazione.

Per impostare un limite di budget per Agent Minutes:

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

L'`--limit` opzione imposta un budget massimo di [Agent Minutes](#) per la sessione. Gli Agent Minutes riflettono l'orario di lavoro attivo dell'agente, non l'ora dell'orologio da parete. Quando viene raggiunto il limite, la CLI visualizza un messaggio ed esce con le istruzioni per riprendere:

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

Puoi riprendere la conversazione in un secondo momento con un limite maggiore:

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

Apprendimento continuo

Questa sezione descrive come rivedere e gestire le lezioni create dall'apprendimento continuo.

Lezioni di comprensione

Il sistema di apprendimento continuo estrae automaticamente le lezioni dalle esecuzioni precedenti di una trasformazione. Il sistema le crea in modo asincrono sulla base di:

- Feedback degli sviluppatori fornito in modalità interattiva
- Problemi relativi al codice riscontrati durante le trasformazioni

Le lezioni si accumulano nel tempo man mano che si esegue la trasformazione su diverse basi di codice. Il sistema li applica automaticamente per migliorare le esecuzioni future. Ogni lezione appartiene a una categoria contenente tutte le lezioni di un dominio simile, in modo da poter rivedere insieme le lezioni correlate. Per le lezioni che non desideri vengano utilizzate, puoi archiviare o eliminare completamente la lezione.

Visualizzazione e gestione delle lezioni

Utilizzate il `learnings` comando per aprire una sessione interattiva per sfogliare e gestire le lezioni di una definizione di trasformazione.

Per aprire il visualizzatore delle lezioni:

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

Il visualizzatore si apre su un elenco di categorie di lezioni, ognuna delle quali mostra quante lezioni attive contiene. Seleziona una categoria per visualizzarne le lezioni, quindi seleziona una lezione per visualizzarne tutti i dettagli, tra cui il corpo della lezione, il suo impatto e il numero di sessioni precedenti consultate.

Archiviazione e ripristino delle lezioni

Il sistema applica le lezioni automaticamente. Se non vuoi che il sistema applichi una lezione, puoi archivarla. Il sistema conserva le lezioni archiviate ma non le applica alle esecuzioni future. Tutte le lezioni archiviate sono raggruppate in modo da poterle rivedere e ripristinare l'uso attivo di tutte le lezioni.

Eliminazione delle lezioni

Rimuovi definitivamente una lezione che non è utile. L'eliminazione non può essere annullata e il sistema potrebbe apprendere nuovamente una lezione eliminata dalle esecuzioni future.

Una lezione deve essere archiviata prima di poter essere eliminata.

Configurazione avanzata

Questa sezione descrive le funzionalità avanzate e le opzioni di configurazione per AWS Transform custom.

Variabili di ambiente

È possibile personalizzare il comportamento della CLI utilizzando variabili di ambiente.

Note

Gli esempi seguenti mostrano la sintassi di Linux e macOS (`()`). `export` In Windows, imposta le variabili di ambiente in PowerShell uso. `$env:NAME="value"` Consultate le schede Windows (PowerShell) per i comandi equivalenti.

ATX_SHELL_TIMEOUT

Sostituisci il timeout predefinito per i comandi della shell (900 minuti). seconds/15

Linux and macOS

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

Windows (PowerShell)

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

Ciò è utile per basi di codice di grandi dimensioni o processi di compilazione a esecuzione prolungata.

ATX_DISABLE_UPDATE_CHECK

Disattiva i controlli automatici delle versioni e le notifiche di aggiornamento durante l'esecuzione dei comandi.

Linux and macOS

```
export ATX_DISABLE_UPDATE_CHECK=true
```

Windows (PowerShell)

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

ATX_GIT_COMMITTER_NAME e ATX_GIT_COMMITTER_EMAIL

Configura l'identità dell'autore utilizzata per i commit del checkpoint che Transform custom crea nel tuo repository man mano che applica le modifiche durante una trasformazione. AWS Quando queste variabili non sono impostate, i commit dei checkpoint vengono attribuiti a un'identità predefinita (). ATX Bot <checkpoint@atx.bot> Imposta entrambe le variabili per attribuire i checkpoint a un autore specifico.

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"
```

Impostazioni di fiducia

Le impostazioni di attendibilità consentono di approvare preventivamente strumenti e comandi specifici da eseguire senza richieste. È inoltre possibile richiedere l'autorizzazione esplicita per comandi shell specifici indipendentemente dal livello di attendibilità. Queste impostazioni sono configurate nel `~/.aws/atx/trust-settings.yaml` file.

Il file contiene tre elenchi:

- `trustedTools`- Strumenti che possono essere eseguiti senza richiedere conferma
- `trustedShellCommands`- Comandi di shell che possono essere eseguiti senza richiedere conferma
- `alwaysPromptCommands`- Schemi di comandi della shell che richiedono un'autorizzazione esplicita a meno che non vengano sovrascritti da `trustedShellCommands`, indipendentemente dal `-t` flag o dall'attendibilità della sessione. Questi modelli non vengono applicati in modalità non interattiva (`()`). `-x`

Strumenti affidabili predefiniti:

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

Modifica delle impostazioni di attendibilità:

Puoi modificare manualmente il file `trust-settings.yaml` per aggiungere o rimuovere strumenti e comandi affidabili. Entrambi supportano i pattern glob wildcard utilizzando `trustedShellCommands`. `alwaysPromptCommands *`

 Note

Se un comando corrisponde a entrambi gli elenchi, ha la `trustedShellCommands` priorità.

Di seguito viene descritto ogni elenco di comandi e vengono forniti esempi:

- `trustedShellCommands`- I comandi che corrispondono a questi schemi vengono eseguiti senza richiedere conferma, aggirando tutti gli altri guardrail. I pattern vengono confrontati con la stringa di comando completa.

Esempi:

- `cd *-` Corrisponde ai comandi composti che iniziano con `cd`
- `*&&*-` Affida a tutti i comandi gli operatori `&&`
- `alwaysPromptCommands`- I comandi che corrispondono a questi modelli richiedono un'autorizzazione esplicita a meno che non vengano sovrascritti da `trustedShellCommands`, indipendentemente dal flag o dalla fiducia della `-t` sessione. Questi modelli non vengono applicati in modalità non interattiva (`()`). `-x` I modelli vengono confrontati con ogni sottocomando nelle espressioni composte (`&&`, `|`, sostituzioni di comandi).

Esempi:

- `rm -rf *-` Richiede sempre comandi ricorsivi di eliminazione forzata
- `sudo *-` Richiede sempre i comandi eseguiti con `sudo`
- `find * -exec *-` Richiede sempre di trovare i comandi con `-exec`

Session-level fiducia:

Durante i prompt interattivi, puoi scegliere:

- `(y)es`- Esegui una volta
- `(n)o`- Negare
- `(t)rust`- Affidati solo alla sessione corrente

Session-level le impostazioni di trust sono temporanee e vengono ripristinate al riavvio della CLI, fornendo un'approvazione temporanea senza modificare permanentemente `trust-settings.yaml`.

 Note

L'attendibilità della sessione non è disponibile per i comandi corrispondenti all'elenco.
`alwaysPromptCommands`

Server Model Context Protocol (MCP)

La CLI AWS Transform supporta i server Model Context Protocol (MCP), che ne estendono le funzionalità con strumenti aggiuntivi.

Configurazione:

Configurare i server MCP nel `~/.aws/atx/mcp.json` file. La CLI AWS Transform supporta due tipi di server MCP: server locali basati su comandi e server HTTP remoti.

Server locali basati su comandi:

I server locali vengono eseguiti come processi secondari sul computer. Configurali con la `command` proprietà:

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

Server HTTP remoti:

I server remoti si connettono ai server MCP ospitati su un URL HTTP o HTTPS. Configurali con la `url` proprietà:

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

```
}  
}  
}  
}
```

La `headers` proprietà è facoltativa e supporta l'espansione delle variabili di ambiente tramite la `${VAR_NAME}` sintassi. Ciò consente di memorizzare valori sensibili come i token API nelle variabili di ambiente anziché nel file di configurazione.

Proprietà di configurazione:

I server locali basati su comandi supportano le seguenti proprietà:

- `command`(obbligatorio) - Il comando per eseguire il server
- `args`(opzionale) - Matrice di argomenti della riga di comando
- `env`(opzionale) - Variabili di ambiente da passare al processo del server

I server HTTP remoti supportano le seguenti proprietà:

- `url`(obbligatorio): l'URL HTTP o HTTPS del server MCP remoto
- `headers`(opzionale) - Intestazioni HTTP da includere nelle richieste, con supporto per `${VAR_NAME}` l'espansione delle variabili di ambiente

Gestione dei server MCP:

Visualizza l'elenco dei server MCP configurati:

```
atx mcp tools
```

Elenca gli strumenti disponibili offerti da uno specifico server MCP:

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

Monitoraggio dell'utilizzo:

La CLI monitora automaticamente l'utilizzo dello strumento MCP durante le esecuzioni di trasformazione. Le statistiche di utilizzo vengono mantenute come `mcp_usage.json` nella `directory delle conversazioni a fianco.metadata.json` Il file registra le metriche per strumento per ogni esecuzione, tra cui:

- Numero di invocazioni per strumento
- Numero di errori per utensile
- Tempo di esecuzione totale per utensile
- Dettagli dell'ultimo errore (se presente)

Client-Side Competenze

Client-side le competenze sono funzionalità aggiuntive che estendono l'agente durante le esecuzioni di trasformazione. Consentono di fornire strumenti, script e istruzioni personalizzati che l'agente può utilizzare oltre alle funzionalità integrate.

Directory per la scoperta delle abilità:

Le abilità vengono rilevate da quattro elenchi in ordine di precedenza. Se un'abilità con lo stesso nome esiste in più directory, la prima directory dell'elenco ha la priorità:

1. <project>/aws/atx/skills/- Project-level, Trasforma AWS CLI-specific
2. <project>/agents/skills/- Project-level, cross-client (disponibile per qualsiasi strumento agente compatibile)
3. ~/.aws/atx/skills/- User-level, Trasforma AWS CLI-specific
4. ~/.agents/skills/- User-level, cross-client (disponibile per qualsiasi strumento agente compatibile)

Le `aws/atx/skills/` directory sono specifiche della CLI AWS Transform. Le `agents/skills/` directory sono interclient, il che significa che le competenze ivi inserite sono disponibili per qualsiasi strumento agente compatibile oltre alla CLI Transform AWS .

Struttura della directory delle abilità:

Ogni abilità è una directory contenente un `SKILL.md` file con frontmatter YAML:

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

```
### validate.py
```

SKILL.md formato:

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

Instructions for the agent...
```

Il name campo deve corrispondere al nome della directory principale.

Disabilitazione di un'abilità:

Per evitare che un'abilità venga caricata senza rimuoverne i file, aggiungi `disable-model-invocation: true` alla prima pagina:

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

Quando questa proprietà è impostata, la CLI ignora l'abilità durante il rilevamento. L'agente non può vedere o utilizzare l'abilità a meno che una definizione di trasformazione non gli indichi esplicitamente di leggere il file di abilità. Utilizzatelo per disattivare temporaneamente un'abilità, contrassegnarla come in corso di lavorazione o conservare materiale di riferimento destinato esclusivamente ai lettori umani.

Note

I file di una skill disabilitata rimangono su disco. Se una definizione di trasformazione indica all'agente di leggere un percorso di file specifico, l'agente può comunque accedere al contenuto. La `disable-model-invocation` proprietà impedisce il rilevamento automatico e l'inserimento del contesto, non l'accesso al file system.

Disponibilità delle competenze in base alla modalità di esecuzione:

- Modalità Exec (`atx custom def execon--code-repository-path`): rileva le competenze sia dalle directory a livello di utente che a livello di progetto.
- Modalità interattiva (`atx`): inizialmente vengono scoperte solo le competenze a livello di utente. Quando si fornisce un percorso di archiviazione del codice durante la sessione, vengono caricate anche le competenze a livello di progetto.

Verifica della scoperta delle abilità:

Controlla il registro di debug della CLI dopo l'esecuzione per verificare quali competenze sono state scoperte:

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
```

Le abilità che non superano la convalida vengono ignorate con un avviso nei log di debug.

Note

Client-side le competenze richiedono la versione CLI 2.0 o successiva.

Scelta tra Project-Level e competenze User-Level

Il luogo in cui si colloca un'abilità determina chi ne trae beneficio e quando si attiva.

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

Affidale al controllo delle versioni in modo che ogni membro del team che esegue trasformazioni sul repository le scopra automaticamente. Usa le competenze a livello di progetto per:

- Repository-specific controlli di conformità (regole Dockerfile, politiche Terraform, validatori di sicurezza della migrazione)

- Standard di codifica organizzativa che si applicano a questa base di codice (modelli di osservabilità, gestione degli errori, convenzioni di denominazione)
- Crea o testa script esclusivi per il progetto (linter personalizzati, architettura, funzioni di fitness)
- Guide alla migrazione delle API per le librerie interne utilizzate in questo repository

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

Questi rimangono sulla macchina e si attivano durante tutte le trasformazioni indipendentemente dal repository scelto come destinazione. Utilizza le competenze a livello di utente per:

- Strumenti personali per il flusso di lavoro (generatori di log delle modifiche, formattatori di messaggi di commit)
- Cross-project preferenze (modelli di test preferiti, promemoria in stile documentazione)
- controlli di conformità delle licenze richiesti dall'organizzazione in tutti gli archivi
- Soglie di copertura o limiti di qualità da applicare a ogni codebase con cui lavori

Suggerimenti per competenze efficaci:

- Scrivi `description` campi chiari nel `SKILL.md` frontespizio. L'agente utilizza questo campo per decidere quando un'abilità è rilevante.
- Esci dagli script di convalida con codice 0 in caso di successo e diverso da zero in caso di errore. L'agente interpreta i codici di uscita per determinare la conformità.
- Stampa messaggi di errore chiari e utilizzabili negli script. L'agente legge l'output per capire cosa correggere.
- Inserisci le competenze nella directory cross-client (`.agents/skills/`) a entrambi i livelli per condividerle con altri strumenti di sviluppo AI oltre alla CLI AWS Transform.

Client-Side Esempi di abilità

Questi esempi mostrano due modelli comuni: un'abilità di convalida basata su script e un'abilità di solo riferimento.

Esempio: Dockerfile Compliance Checker () Script-Based

Questa competenza convalida Dockerfiles rispetto alle migliori pratiche operative e di sicurezza. Utilizza uno script di convalida che l'agente esegue prima e dopo aver apportato le modifiche.

Struttura delle cartelle:

```
.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.
```

Lo script di convalida verifica la presenza di tag di immagine di base non bloccati, eseguiti come root, segreti codificati nelle ENV direttive e definizioni mancanti. HEALTHCHECK L'agente esegue lo script, corregge le violazioni utilizzando i modelli del file di riferimento e riesegue lo script per confermare la conformità.

Esempio: API Deprecation Helper () Reference-Only

Questa abilità guida l'agente nella sostituzione delle chiamate API obsolete durante le trasformazioni di aggiornamento. Utilizza solo file di riferimento senza script.

Struttura delle cartelle:

```
.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
```

I file di riferimento contengono esempi di codice prima e dopo. Ad esempio, `aws-sdk-v2-to-v3.md` mappa modelli simili `s3.putObject(params).promise()` all'equivalente modulare v3 usando `and.S3Client PutObjectCommand`

Tag e organizzazione

Puoi organizzare le trasformazioni con tag per il controllo degli accessi e la categorizzazione.

 Note

Alcuni di questi comandi richiedono la specificazione dell'Amazon Resource Name (ARN) per una definizione di trasformazione. La struttura ARN è: `arn:aws:transform-custom:<region>:<account-id>:package/<td-name>`

Per elencare i tag per una trasformazione:

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

Per aggiungere tag a una trasformazione:

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

Per rimuovere i tag da una trasformazione:

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

I tag possono essere utilizzati per il controllo degli accessi raggruppati nelle politiche IAM. Puoi creare politiche che concedono autorizzazioni a tutte le trasformazioni con tag specifici (ad esempio, tutte le trasformazioni contrassegnate con `o). team:frontend environment:production`

Log

AWS Transform CLI mantiene tre tipi di log per la risoluzione dei problemi e il debug.

Registri delle conversazioni:

Linux and macOS

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

Windows

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

Questi registri contengono la cronologia completa delle conversazioni per una sessione specifica.

Registri di Subagent:

Linux and macOS

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

Windows

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

Questi registri contengono l'output dei subagenti generati dall'agente principale durante le trasformazioni. Non è necessario gestire direttamente i subagenti.

Registri di debug per sviluppatori:

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
```

Questi registri forniscono informazioni avanzate sulla risoluzione dei problemi per la CLI stessa.

Note

Potrebbero esserci più file di registro di debug nella directory logs (ad esempio debug1.log, debug2.log). Esamina e fornisci tutti i log pertinenti, ad esempio `~/.aws/atx/<conversation-id>/custom/ *` e `~/.aws/atx/logs/ *`, all'apertura dei ticket di assistenza per una risoluzione più rapida.

Aggiornamenti CLI

Mantieni aggiornata la CLI per accedere a nuove funzionalità e miglioramenti.

Per verificare la presenza di aggiornamenti:

```
atx update --check
```

Per eseguire l'aggiornamento alla versione più recente:

```
atx update
```

Per eseguire l'aggiornamento a una versione specifica:

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

Crea trasformazioni personalizzate

Questa sezione descrive come creare, modificare e gestire definizioni di trasformazione personalizzate.

Creazione di una nuova trasformazione

Utilizza la CLI interattiva per creare una nuova definizione di trasformazione.

Per creare una definizione di trasformazione

1. Avvia la CLI AWS Transform:

```
atx
```

2. Comunica all'agente che desideri creare una nuova trasformazione.
3. Fornisci una descrizione chiara e dettagliata dell'obiettivo di trasformazione. Includi:
 - Lo stato di origine e di destinazione (ad esempio, «aggiornamento dalla versione X alla versione Y»)
 - Sono richieste modifiche specifiche (ad esempio, «aggiornamento delle istruzioni di importazione, sostituzione dei metodi obsoleti»)
 - Eventuali considerazioni o vincoli speciali
4. Quando l'agente richiede chiarimenti o informazioni aggiuntive, fornisci esempi e materiali di riferimento specifici.

5. Esamina la definizione di trasformazione iniziale creata dall'agente.
6. Prova la trasformazione su una base di codice di esempio.
7. Iterate fornendo feedback, correzioni al codice o esempi aggiuntivi.
8. Salva la trasformazione localmente o pubblicala nel registro.

Le migliori pratiche per creare trasformazioni:

- Inizia con trasformazioni semplici e ben definite prima di tentare trasformazioni complesse
- Fornisci materiali di riferimento completi, tra cui guide alla migrazione ed esempi di codice
- Esegui test su più basi di codice di esempio prima della pubblicazione
- Utilizza comandi di compilazione o convalida deterministici per consentire l'apprendimento continuo
- Prendi in considerazione la possibilità di suddividere trasformazioni complesse in più fasi più piccole
- Contrassegna le informazioni cruciali con «CRITICAL:» o «IMPORTANT:» nelle definizioni di trasformazione per garantire che l'agente dia priorità a questi requisiti
- Quando è necessario che vengano rispettati requisiti esatti (ad esempio utilizzando un comando o un valore di stringa specifico), specificate esplicitamente la stringa completa nelle definizioni di trasformazione. Puoi racchiuderli tra virgolette di bash per indicare chiaramente che si tratta di comandi da terminale o stringhe letterali, il che riduce la variabilità e garantisce un'esecuzione coerente

Fornire materiali di riferimento

Puoi fornire file di riferimento a AWS Transform custom specificando i percorsi dei file durante la conversazione. Questi file vengono archiviati nella `references/` cartella della definizione di trasformazione.

Tipi di file di riferimento consigliati:

- Before/after codice di esempio
- Documentazione per le API, le librerie o le funzionalità coinvolte
- Human-readable guide alla migrazione

Per fornire un file di riferimento:

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

Puoi anche fornire una directory contenente più file di riferimento:

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

Note

Sono supportati solo file basati su testo (.md, .html, .txt, file di codice). I file binari, le immagini e i file RTF (ad es. .pdf, .png, .docx) non sono attualmente supportati. Spesso è possibile estrarre il contenuto del testo e utilizzarlo come riferimento. Se hai molti file di testo di piccole dimensioni, valuta la possibilità di concatenarli in pochi file con nomi descrittivi. C'è un limite totale di 10 MB per tutti i file.

Modifica di una trasformazione esistente

È possibile modificare le trasformazioni personalizzate sia prima che dopo averle salvate come bozze o dopo averle pubblicate. Non è possibile modificare le trasformazioni AWS gestite. Se è necessario personalizzarle, è possibile fornire un contesto aggiuntivo utilizzando il file di configurazione.

Per modificare una trasformazione esistente

1. Avvia la CLI AWS Transform:

```
atx
```

2. Indica all'agente che desideri modificare una trasformazione esistente.
3. Scegli se:
 - Fornite un percorso di file per una trasformazione memorizzata localmente (cioè non una bozza salvata o pubblicata)
 - Richiedi l'elenco delle trasformazioni dal registro
4. Se scegli dal registro, seleziona la trasformazione che desideri modificare.
5. Collabora con l'agente per descrivere le modifiche che desideri apportare.
6. Prova la trasformazione aggiornata su una base di codice di esempio.
7. Se lo desideri, pubblica gli aggiornamenti nel registro.

Pubblicazione e gestione delle trasformazioni

Puoi pubblicare e gestire le tue trasformazioni utilizzando l'esperienza interattiva o con i seguenti comandi.

Per salvare una trasformazione come bozza:

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

Per pubblicare una trasformazione:

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

Per elencare le trasformazioni disponibili:

```
atx custom def list
```

Per scaricare una definizione di trasformazione:

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

Questa operazione scarica la definizione di trasformazione nella directory di lavoro corrente. È possibile specificare una directory di destinazione con il `--td` flag e una versione con il `--tv` flag.

Per eliminare una definizione di trasformazione:

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

Important

Ciò elimina definitivamente la definizione di trasformazione specificata dal tuo account.

Gestione delle versioni di trasformazione

AWS Transform custom mantiene le versioni delle definizioni di trasformazione. È possibile specificare una versione durante l'esecuzione o il download di una trasformazione.

Per eseguire una versione specifica:

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

Per scaricare una versione specifica:

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

Se non viene specificata alcuna versione, viene utilizzata la versione più recente.

Riferimento ai comandi

Questa sezione fornisce un riferimento completo di tutti i comandi CLI personalizzati di AWS Transform.

Comandi interattivi

atx

Inizia una conversazione interattiva con la CLI 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
```

Comandi di sessione interattivi

I seguenti comandi possono essere digitati al prompt di input durante una sessione interattiva:

- `/usage`- Visualizza i [minuti accumulati dagli agenti per la sessione](#) corrente

Comandi di definizione della trasformazione

atx custom def exec

Esegui una definizione di trasformazione su un repository di codice.

Opzione	Forma lunga	Parametro	Description
-p	--code-repository-path	<path>	Percorso del repository e del codice da trasformare. Per la directory corrente, usa «.»
-c	--build-command	<command>	Comando da eseguire durante la creazione del repository
-n	--transformation-name	<name>	Nome della definizione di trasformazione nel registro
-x	--non-interactive	-	Esegue la trasformazione senza assistenza da parte dell'utente
-t	--trust-all-tools	-	Si fida di tutti gli strumenti (nessuna richiesta)
-d	--do-not-learn	-	Disattiva l'estrazione delle lezioni da questa esecuzione
-g	--configuration	<config>	Percorso del file di configurazione (JSON o YAML) o delle coppie chiave=valore
--tv	--transformation-version	<version>	Versione della definizione di trasformazione da utilizzare

Opzione	Forma lunga	Parametro	Description
--limit	--limit	<limit>	Imposta il limite di budget per Agent Minutes . La trasformazione termina quando viene raggiunto il limite e può essere ripresa con un limite maggiore
-h	--help	-	Visualizza la guida per il comando

elenco di def personalizzato atx

Elenca le definizioni di trasformazione disponibili.

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

atx custom def get

Ottieni i dettagli di una definizione di trasformazione specifica.

Opzione	Forma lunga	Parametro	Description
-n	--transformation-name	<name>	Il nome della definizione di trasformazione da recuperare
--tv	--transformation-version	<version>	La versione della definizione di trasformazione da recuperare
--td	--target-directory	<directory>	La directory di destinazione in cui

Opzione	Forma lunga	Parametro	Description
			salvare la definizione di trasformazione (impostazione predefinita: «.»)
--json	--json	-	Risposta in uscita in formato JSON
-h	--help	-	Visualizza l'aiuto per il comando

atx custom def delete

Elimina definitivamente una definizione di trasformazione.

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

atx custom def publish

Pubblica una definizione di trasformazione nel registro.

Opzione	Forma lunga	Parametro	Description
-n	--transformation-name	<name>	Il nome della definizione di trasformazione da pubblicare
--tv	--transformation-version	<version>	La versione della definizione di trasformazione da utilizzare (non applicabile con --description o --source-directory)
--sd	--source-directory	<directory>	La directory di origine da cui leggere i file

Opzione	Forma lunga	Parametro	Description
			di definizione della trasformazione locale (non applicabile con --transformation-version)
--description	--description	<description>	Una descrizione per la definizione di trasformazione (non applicabile con --transformation-version)
--json	--json	-	Risposta in uscita in formato JSON
-h	--help	-	Visualizza l'aiuto per il comando

atx custom def save-draft

Salva una definizione di trasformazione come bozza nel registro. Le bozze scadono dopo 30 giorni e non vengono visualizzate nel registro. Questo comando restituisce il numero di versione della bozza. È necessario eseguire e recuperare le bozze in modo esplicito utilizzando il nome e il numero di versione della trasformazione.

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

Comandi della lezione

apprendimenti atx custom def

Apri una sessione interattiva per visualizzare e gestire le lezioni apprese da una definizione di trasformazione nelle esecuzioni precedenti. Sfoglia le lezioni per categoria, visualizza i dettagli delle lezioni e archivia, ripristina o elimina le lezioni.

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

Comandi per tag

tag di lista di def personalizzati atx

Elenca i tag per una definizione di trasformazione.

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

tag def personalizzato atx

Aggiungi tag a una definizione di trasformazione.

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

atx custom def untag

Rimuove i tag da una definizione di trasformazione.

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

Comandi di aggiornamento

aggiornamento atx

Aggiorna 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
```

Comandi MCP

strumenti atx mcp

Consente ai clienti di accedere alle configurazioni view/confirm degli strumenti MCP. Gli aggiornamenti delle configurazioni devono essere gestiti direttamente tramite il file ~/.aws/atx/mcp.json

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

AWS-Trasformazioni gestite

AWS-le trasformazioni gestite sono trasformazioni predefinite e AWS controllate per casi d'uso comuni, pronte all'uso senza alcuna configurazione aggiuntiva.

Panoramica di

AWS-le trasformazioni gestite hanno le seguenti caratteristiche:

- Convalidato da AWS: queste trasformazioni vengono controllate per garantire la massima qualità AWS
- Pronto all'uso: non è richiesta alcuna configurazione aggiuntiva
- Crescita continua: vengono continuamente aggiunte ulteriori trasformazioni
- Personalizzabile: Pre-built le trasformazioni possono essere personalizzate fornendo ulteriori indicazioni o requisiti specifici per le esigenze dell'organizzazione utilizzando il parametro di configurazione `additionalPlanContext`
- Supporto per l'accesso anticipato: alcune trasformazioni possono essere contrassegnate come accesso anticipato in quanto sottoposte a ulteriori test e perfezionamenti

Disponibilità AWS-Trasformazioni gestite

Il seguente catalogo elenca le trasformazioni AWS gestite attualmente disponibili, raggruppate per caso d'uso. Ogni tabella mostra il nome della trasformazione, la lingua o lo stack a cui si applica e il relativo stato. Per trovare rapidamente una trasformazione, usa la casella di ricerca nella parte superiore di questa pagina per cercare per nome, lingua o caso d'uso.

Questo catalogo è l'elenco canonico delle AWS trasformazioni gestite. Kiro Power, il plug-in agent, il plug-in VS Code e la CLI eseguono tutti le stesse trasformazioni. Per elencare le trasformazioni disponibili nel registro, esegui `atx custom def list`

Note

Le trasformazioni contrassegnate con accesso anticipato sono funzionali ma potrebbero essere aggiornate frequentemente in base al feedback dei clienti.

Aggiornamenti di runtime

Aggiorna un linguaggio o un runtime a una versione più recente o modifica la distribuzione del runtime.

Trasformazione	Lingua/ stack	Stato	Description
AWS/java-version-upgrade	Java	Disponibilità generale	Aggiorna le applicazioni Java utilizzando qualsiasi sistema di compilazione da qualsiasi versione JDK di origine a qualsiasi versione JDK di destinazione, con la modernizzazione delle dipendenze, tra cui la migrazione a Jakarta EE, i driver di database, i framework ORM e gli aggiornamenti dell'ecosistema Spring. Specificate la versione JDK di destinazione in chat o con il parametro <code>.additionalPlanContext</code>
AWS/python-version-upgrade	Python	Disponibilità generale	Migra i progetti Python da Python 3.8 o 3.9 a Python 3.11, 3.12 o 3.13 mantenendo funzionalità e prestazioni. Specificate la

Trasformazione	Lingua/ stack	Stato	Description
			versione Python di destinazione in chat o con il additionalPlanContext parametro.
AWS/nodejs-version-upgrade	Node.js	Disponibilità generale	Aggiorna Node.js le applicazioni da qualsiasi Node.js versione di origine a qualsiasi Node.js versione di destinazione. Specifica la versione di destinazione in chat o con il additionalPlanContext parametro.
AWS/lambda-nodejs-runtime-upgrade	Node.js (Lambda)	Accesso anticipato	Aggiorna le funzioni AWS Lambda dai Node.js runtime precedenti (da nodejs4.3 a nodejs22.x) a nodejs24.x, risolvendo le modifiche più importanti nel Lambda Runtime Interface Client (RIC) e nel runtime a 24 lingue. Node.js

Trasformazione	Lingua/ stack	Stato	Description
AWS/oracle-java-to-correcto	Java (distribuzione JDK)	Accesso anticipato	Esegui la migrazione di progetti Java da Oracle JDK ad Amazon Corretto. Sostituisce le API Oracle-specific interne con equivalenti Java standard, aggiorna le configurazioni di build (Maven e Gradle) e le immagini di base dei contenitori, rimuove i flag JVM commerciali e genera un rapporto sulle licenze.

Trasformazione	Lingua/ stack	Stato	Description
AWS/ruby-upgrade	Ruby	Accesso anticipato	Aggiorna le applicazioni Ruby da Ruby 2.x a Ruby 4.0 e i relativi framework a Rails 8.0 o Sinatra 4.1. Puoi utilizzare questa trasformazione con Rails e app, app Sinatra e gemme autonome. ActiveRecord La trasformazione abbina ogni aggiornamento della versione di Ruby all'aggiornamento del framework corrispondente ed esegue la suite di test. Quindi isola gli errori prima di passare alla versione successiva.

Migrazioni SDK

Esegui la migrazione tra le versioni principali di un SDK. AWS

Trasformazione	Lingua/ stack	Stato	Description
AWS/java-aws-sdk-v1-to-v2	Java	Disponibilità generale	Aggiorna l' AWS SDK dalla v1 alla v2 per i progetti Java utilizzando Maven o Gradle.

Trasformazione	Lingua/ stack	Stato	Description
AWS/python-boto2-to-boto3	Python	Disponibilità generale	Migra le applicazioni Python da boto2 a boto3, in base alla documentazione ufficiale sulla migrazione. AWS
AWS/nodejs-aws-sdk-v2-to-v3	Node.js	Disponibilità generale	Aggiorna Node.js le applicazioni dall'AWS SDK per la JavaScript v2 alla v3 per ottenere un'architettura modulare, un TypeScript supporto di prima classe e prestazioni migliorate, senza modificare la versione. Node.js

Aggiornamenti e migrazioni del framework

Aggiorna un framework a una versione più recente o esegui la migrazione a un framework diverso.

Trasformazione	Lingua/ stack	Stato	Description
AWS/spring-boot-version-upgrade	Java/Spring Boot	Disponibilità generale	Aggiorna una vecchia applicazione Spring Boot a una versione di Spring Boot di destinazione, inclusi file di build e starter, proprietà, pacchetti Jackson 3, Spring Security 7 DSL, infrastruttura di test

Trasformazione	Lingua/ stack	Stato	Description
			e dipendenze di osservabilità.
AWS/JBoss-to-Spring-Boot	Java (JBoss o Spring Boot) WildFly	Accesso anticipato	Migra le applicazioni aziendali Java EE o Jakarta EE in esecuzione su JBoss EAP o WildFly su Spring Boot, eliminando le dipendenze del server delle applicazioni per un modello di distribuzione containerizzato e nativo del cloud.
AWS/early-access-angular-to-react-migration	Da Angular a React	Accesso anticipato	Trasforma un'applicazione Angular in React.
AWS/angular-version-upgrade	Angular (Angolare)	Accesso anticipato	Aggiorna una vecchia applicazione Angular a una versione di Angular di destinazione, inclusi componenti, servizi, modelli e routing.

Trasformazione	Lingua/ stack	Stato	Description
AWS/vue.js-version-upgrade	Vue.js	Accesso anticipato	Esegui un aggiornamento della versione principale da Vue.js 2 a Vue.js 3, modernizzando i componenti, la gestione dello stato, il routing e le API globali. Gli aggiornamenti minori e le patch non rientrano nell'ambito di applicazione.

GenAI e migrazioni di modelli

Migra i carichi di lavoro di intelligenza artificiale generativa su.

Trasformazione	Lingua/ stack	Stato	Description
AWS/GenAI-to-Bedrock-Migration-Assessment	Carichi di lavoro di intelligenza artificiale generativa	Accesso anticipato	Valuta i carichi di lavoro di intelligenza artificiale generativa per la migrazione da fornitori di terze parti (OpenAI, Google Gemini, Anthropic direct e modelli open source) a. Scopre l'utilizzo e i modelli dell'SDK, chiarisce i requisiti, progetta una mappatura dei modelli, stima costi e rischi e genera

Trasformazione	Lingua/ stack	Stato	Description
			artefatti di valutazione. Assessment-only; non modifica il codice sorgente. Copre anche framework agentici come CrewAI e Strands. LangGraph

Language-to-language migrazioni

Traduci una base di codice da un linguaggio di programmazione a un altro.

Trasformazione	Lingua/ stack	Stato	Description
AWS/vba-to-python-migration	Da VBA a Python	Accesso anticipato	Migra macro, moduli e logica incorporata di Excel VBA in script e moduli Python equivalenti UserForms, utilizzando openpyxl, pandas, tkinter o 6 e librerie standard. PyQt Il linguaggio di destinazione è Python 3.8 o successivo. Da utilizzare per convertire codice VBA incorporato in .bas, .cls, .frm o .xlsm.

Migrazioni di database

Al momento non sono disponibili trasformazioni AWS gestite specifiche del database. Per modernizzare i database Microsoft SQL Server e le applicazioni.NET associate su Amazon Aurora PostgreSQL, consulta. [the section called “Modernizzazione di SQL Server”](#)

Osservabilità

Modernizza la registrazione e il monitoraggio con servizi nativi. AWS

Trasformazione	Lingua/ stack	Stato	Description
AWS/early-access-log4j-to-slf4j-migration	Java (registrazione)	Accesso anticipato	Migra le applicazioni Java da Log4j (1.x o 2.x) a SLF4J con un backend Logback. Gestisce il codice sorgente, la gestione delle dipendenze (Maven e Gradle) e la registrazione dei file di configurazione e convalida mediante compilazione, test e scansione delle importazioni residue.
AWS/datadog-monitors-to-cloudwatch-alarms	Infrastruttura come codice/monitoraggio	Accesso anticipato	Migra i monitor DataDog metrici che tengono traccia delle metriche AWS di servizio e delle metriche personalizzate agli CloudWatch allarmi nativi come infrastruttura come codice. Genera CloudForm

Trasformazione	Lingua/ stack	Stato	Description
			ation YAML, CDK e Terraform HCL. TypeScript

Architecture

Re-architect, riorganizza o ottimizza le applicazioni per. AWS

Trasformazione	Lingua/ stack	Stato	Description
AWS/java-performance-optimization	Java (prestazioni)	Disponibilità generale	Ottimizza le prestazioni delle applicazioni Java analizzando i dati di profilazione JFR per rilevare gli hotspot e gli anti-pattern di CPU e memoria, quindi applicando correzioni mirate al codice. Per istruzioni sulla raccolta dei dati JFR, consulta la guida di runtime JFR.
AWS/early-access-java-x86-to-graviton	Java (Arm64/Graviton)	Accesso anticipato	Convalida la compatibilità delle applicazioni Java con l'architettura Arm64 per i processor AWS Graviton e risolvi le incompatibilità aggiornando le dipendenze, rilevando modelli di codice

Trasformazione	Lingua/ stack	Stato	Description
			specifici dell'architettura e ricompilando le librerie native quando il codice sorgente è disponibile. Molte applicazioni Java moderne lo sono già. Arm64-compatible
AWS/oracle-service-bus-to-aws	Integrazione con Java /serverless	Accesso anticipato	Migra le configurazioni dei processi Oracle Service Bus (OSB) e BPEL su un'architettura serverless AWS nativa, generando un progetto CDK implementabile con TypeScript Amazon API Gateway, Lambda e Step Functions. AWS AWS

Trasformazione	Lingua/ stack	Stato	Description
AWS/mulesoft-to-aws-native	Da Java/a serverless MuleSoft	Accesso anticipato	Trasforma MuleSoft le applicazioni Mule 3.x e 4.x in architetture AWS serverless (Amazon API Gateway, AWS Lambda e AWS Step Functions) destinate a Java 17 su Lambda con. AWS SnapStart La trasformazione mappa i trigger di flusso alle sorgenti di AWS eventi, converte DataWeave le espressioni MEL (MuleSoft Expression Language) in AWS equivalenti e sostituisce i connettori con chiamate SDK for AWS Java v2. Produce modelli SAM, gestori AWS Lambda e test JUnit 5.

Trasformazione	Lingua/ stack	Stato	Description
AWS/payshield-hsm-to-aws-payment-cryptography	Java (crittografia da HSM a pagamento) AWS	Disponibilità generale	Esegui la migrazione e delle applicazioni Java dal protocollo PayShield Hardware Security Module (HSM) di Thales al Payment Cryptography SDK v2. AWS La migrazione include la mappatura dei comandi, la migrazione e delle chiavi, la configurazione delle dipendenze e il test di parità.

Analisi della base di codice

Analizza codebase e portafogli per pianificare la modernizzazione. Queste trasformazioni producono report e non modificano il codice.

Trasformazione	Lingua/stack	Stato	Description
AWS/comprehensive-codebase-analysis	Più lingue	Disponibilità generale	Esegui un'analisi statica approfondita di una base di codice per generare documentazione gerarchica e con riferimenti incrociati che combini analisi comportamentale, documentazione architetturale e

Trasformazione	Lingua/stack	Stato	Description
			business intelligence, con particolare attenzione agli approfondimenti tecnici sul debito.
AWS/agentic-readiness-analysis	Più lingue	Accesso anticipato	Valuta se i sistemi sono pronti per essere chiamati in sicurezza dagli agenti di intelligenza artificiale, coprendo API, identità, gestione dello stato, human-in-the-loop e osservabilità.
AWS/modernization-readiness-analysis	Più lingue	Accesso anticipato	Scansiona i portafogli per individuare le lacune di maturità native del cloud e associa i risultati ai percorsi di modernizzazione. AWS
AWS/portfolio-agentic-readiness-analysis	Portfolio	Accesso anticipato	Aggrega i report di analisi della prontezza dei singoli agenti su un portafoglio di applicazioni per identificare ostacoli trasversali, modelli di riparazione condivisi e raccomandazioni prioritarie.

Trasformazione	Lingua/stack	Stato	Description
AWS/portfolio-modernization-readiness-analysis	Portfolio	Accesso anticipato	Aggrega i report di analisi della modernizzazione individuali di un portafoglio in una roadmap consolidata con ondate di migrazione prioritarie e percorsi di modernizzazione consigliati.

Trasformazione	Lingua/stack	Stato	Description
AWS/business-rules-extraction	Più lingue	Accesso anticipato	Questa trasformazione analizza staticamente una base di codice monolitica per produrre documentazione pronta per la riscrittura senza richiedere una compilazione, un'esecuzione o modifiche al codice sorgente. Scompone il sistema in domini limitati ed estrae regole aziendali, flussi di lavoro, problemi trasversali e struttura del database per dominio. L'output include un manifesto leggibile dalla macchina, un dashboard interattivo e specifiche di implementazione indipendenti dalla lingua per dominio per guidare la modernizzazione o le riscritture complete.

Personalizzazione AWS-Trasformazioni gestite

È possibile personalizzare le AWS trasformazioni gestite per soddisfare le esigenze specifiche dell'organizzazione fornendo un contesto aggiuntivo tramite il parametro di configurazione. `additionalPlanContext`

Esempio: personalizzazione dell'aggiornamento della versione di 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.
```

Esempio: personalizzazione AWS della migrazione 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.
```

Casi di utilizzo comune

Questa sezione fornisce indicazioni dettagliate per scenari di trasformazione comuni utilizzando la CLI Transform AWS .

Aggiornamenti Lambda Runtime

Lambda rende obsoleti periodicamente i runtime delle lingue precedenti, richiedendo ai team di aggiornare le proprie funzioni Lambda alle versioni supportate. AWS Transform custom può automatizzare questi aggiornamenti utilizzando le trasformazioni di aggiornamento della versione in linguaggio gestito. AWS Ad esempio, per aggiornare una funzione Lambda scritta in Python 3.9 a Python 3.13, dovresti usare la trasformazione. `AWS/python-version-upgrade` Trasformazioni

simili sono disponibili per Java (AWS/java-version-upgrade) e Node.js (AWS/nodejs-version-upgrade), che coprono i più comuni linguaggi di runtime Lambda.

Per aggiornare una singola funzione Lambda in modo interattivo, vai alla radice del repository dei sorgenti della funzione e avvia la CLI Transform AWS con. `atx` Nella sessione interattiva, descrivi l'aggiornamento necessario, ad esempio «Aggiorna questa funzione Lambda di Python 3.9 a Python 3.13». L'agente selezionerà la trasformazione AWS gestita appropriata, analizzerà il codice, aggiornerà la sintassi del linguaggio, regolerà le dipendenze e modernizzerà le chiamate API obsolete. È possibile fornire un comando di compilazione o convalida, ad esempio in python `-m py_compile *.py` modo che l'agente possa verificare la compilazione e il superamento dei test del codice trasformato. `pytest` Durante la sessione interattiva, è possibile esaminare le modifiche proposte dall'agente, fornire feedback e richiedere modifiche prima di accettare il risultato finale.

Quando devi aggiornare i runtime Lambda su molti repository, utilizza la modalità non interattiva per eseguire trasformazioni su larga scala. Per ogni repository, richiama la CLI con i flag appropriati per l'esecuzione senza l'input dell'utente. Ad esempio, per aggiornare una funzione Lambda Node.js 16 a Node.js 22:

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

Il `-x` flag esegue la trasformazione in modo non interattivo e considera `-t` attendibili tutte le esecuzioni degli strumenti, quindi non sono richieste richieste. È possibile eseguire lo script di questo comando su dozzine o centinaia di repository utilizzando un semplice loop di shell. Al termine di ogni trasformazione, esamina Git diff per verificare le modifiche ed esegui la suite di test per confermare che la funzione aggiornata funzioni correttamente. Puoi anche integrare AWS Transform custom nella tua CI/CD pipeline per identificare le funzioni Lambda obsolete su base continuativa. Questo approccio non solo risolve il problema immediato dei runtime obsoleti, ma stabilisce anche un processo continuo per rilevare e aggiornare le funzioni prima che raggiungano lo stato di fine del supporto.

I team della piattaforma centrale possono creare campagne tramite l'[applicazione web AWS Transform](#) per definire la trasformazione, specificare gli archivi Lambda di destinazione e monitorare i progressi in tutta l'organizzazione. Per una procedura dettagliata sulla creazione di una soluzione

di implementazione scalabile di livello di produzione utilizzando AWS Batch, vedi [Creazione di una soluzione di modernizzazione del codice scalabile](#) con Transform custom. AWS

AWS Transform endpoint personalizzati e di interfaccia (AWS PrivateLink)

Puoi stabilire una connessione privata tra il tuo VPC e quello AWS Transform personalizzato creando un endpoint VPC di interfaccia. Gli endpoint di interfaccia sono basati su una tecnologia che consente di accedere in modo privato a servizi AWS Transform personalizzati senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. [AWS PrivateLink](#) Direct Connect Il traffico tra il tuo VPC e quello AWS Transform personalizzato non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più [interfacce di rete elastiche](#) nelle sottoreti.

Per ulteriori informazioni, consultare [Endpoint VPC di interfaccia \(AWS PrivateLink\)](#) nella Guida per l'utente di Amazon VPC.

Note

- È necessario abilitare AWS PrivateLink l'integrazione per Amazon S3 poiché effettua chiamate API S3 AWS Transform personalizzate. Per istruzioni dettagliate, consulta la [AWS PrivateLink documentazione di Amazon S3](#). Se riscontri problemi di accesso a S3 durante l'utilizzo di AWS Transform Custom, consulta la nostra [guida alla risoluzione dei problemi](#).
- Se non utilizzi la funzionalità DNS AWS PrivateLink privato (vedi [DNS privato](#)), devi:
 - Configurare il routing verso gli endpoint dell'interfaccia VPC (consulta la documentazione del [routing verso gli endpoint dell'interfaccia VPC](#))
 - Imposta la variabile di ATX_CUSTOM_ENDPOINT ambiente per specificare il tuo dominio personalizzato, ad esempio:

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


Considerazioni per AWS Transform endpoint VPC personalizzati

Prima di configurare un endpoint VPC con interfaccia AWS Transform personalizzato, assicurati di esaminare le [proprietà e le limitazioni degli endpoint dell'interfaccia nella](#) Amazon VPC User Guide.

AWS Transform custom supporta l'esecuzione di chiamate a tutte le sue azioni API tramite l'endpoint dell'interfaccia.

Prerequisiti

Prima di iniziare una qualsiasi delle procedure sottostanti, assicurati di disporre di quanto riportato di seguito:

- Un AWS account con le autorizzazioni appropriate per creare e configurare risorse.
- Un VPC già creato nel tuo AWS account.
- Familiarità con AWS i servizi, in particolare Amazon VPC AWS Transform e custom.

Creazione di un endpoint VPC di interfaccia per AWS Transform personalizzato

Puoi creare un endpoint VPC per il servizio AWS Transform personalizzato utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consultare [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di Amazon VPC.

Crea i seguenti endpoint VPC per AWS Transform personalizzarli utilizzando questo nome di servizio:

- `com.amazonaws. region.transform-personalizzato`

Sostituisci *region* con la AWS regione in cui desideri utilizzare la CLI AWS Transform personalizzata, ad esempio `com.amazonaws.us-east-1.transform-custom`.

Per ulteriori informazioni, consultare [Accesso a un servizio tramite un endpoint di interfaccia](#) in Guida per l'utente di Amazon VPC.

Creazione di una policy per gli endpoint VPC per AWS Transform personalizzato

Puoi allegare una policy per gli endpoint al tuo endpoint VPC che controlla l'accesso ai dispositivi personalizzati. AWS Transform La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire operazioni.

Per ulteriori informazioni, consulta [Controllo degli accessi ai servizi con endpoint VPC](#) in Guida per l'utente di Amazon VPC.

Esempio: policy sugli endpoint VPC per AWS Transform operazioni personalizzate

Di seguito è riportato un esempio di policy per gli endpoint personalizzata. AWS Transform Se collegata a un endpoint, questa policy consente l'accesso alle azioni AWS Transform personalizzate elencate per tutti i principali su tutte le risorse.

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

Utilizzo di un computer locale per connettersi a un AWS Transform endpoint personalizzato

Questa sezione descrive il processo di utilizzo di un computer locale per la connessione a un dispositivo AWS Transform personalizzato tramite un AWS PrivateLink endpoint nel tuo AWS VPC.

1. [Crea una connessione VPN tra il dispositivo on-premises e il VPC.](#)

2. [Crea un endpoint VPC con interfaccia personalizzata. AWS Transform](#)
3. [Configura un endpoint Amazon Route 53 in entrata](#). Ciò ti consentirà di utilizzare il nome DNS del tuo endpoint AWS Transform personalizzato dal tuo dispositivo locale.

Risoluzione dei problemi

Questa sezione fornisce indicazioni per la risoluzione dei problemi comuni relativi a Transform custom. AWS

Posizioni dei log

AWS Transform CLI mantiene i log nelle seguenti posizioni:

Registri delle conversazioni:

Linux and macOS

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

Windows

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

Questi registri contengono la cronologia completa delle conversazioni per il debug di specifiche esecuzioni di trasformazione.

Registri di Subagent:

Linux and macOS

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

Windows

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

Questi registri contengono l'output dei subagenti generati dall'agente principale durante le trasformazioni. Non è necessario gestire direttamente i subagenti.

Registri di debug per sviluppatori:

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
```

Questi registri forniscono informazioni dettagliate sulle operazioni e sugli errori della CLI. Ogni file di registro ha un limite di 5 MB prima del rollover. In questa directory possono essere presenti più registri di debug, ad esempio debug1.log e debug2.log.

Problemi comuni

Problemi di installazione:

Se l'installazione fallisce, assicurati di avere installato Node.js 22 o versioni successive:

```
node --version
```

Node.js Scaricala da <https://nodejs.org/en/download> se necessario.

Problemi di autenticazione:

Verifica che AWS le tue credenziali siano configurate correttamente:

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

Assicurati che il tuo utente o ruolo IAM disponga delle `transform-custom:*` autorizzazioni richieste.

Problemi di connettività di rete:

Se riscontri errori di connessione, verifica l'accesso alla rete agli endpoint richiesti:

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

- *.s3.amazonaws.com

Se lavori in un ambiente con restrizioni Internet, aggiorna le regole del firewall per consentire questi URL.

Problemi di configurazione della regione:

Se riscontri errori relativi alla regione:

- Verifica che la tua regione sia supportata
- Controlla le variabili di ambiente che potrebbero sovrascrivere la tua configurazione: `echo $AWS_REGION $AWS_DEFAULT_REGION`
- Controlla la configurazione della tua regione: `aws configure get region`
- Aggiorna la tua regione se necessario: `aws configure set region <your-region>`
- Controlla i registri di debug per i dettagli sulla risoluzione della regione

Problemi con Git:

Assicurati che Git sia installato e che il tuo repository sia sotto il controllo del codice sorgente git:

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

AWS Transform custom richiede che i repository siano sotto il controllo del codice sorgente di git.

Problemi di esecuzione della trasformazione:

Se una trasformazione fallisce:

1. Consulta i registri delle conversazioni all'indirizzo `~/.aws/atx/custom/<conversation_id>/logs/`
2. Verifica la presenza di errori di compilazione o test nell'output della trasformazione
3. Verifica che il comando build sia corretto per il tuo progetto
4. Prova a eseguire la trasformazione in modalità interattiva per fornire feedback

Problemi di ripresa della conversazione:

Se non riesci a riprendere una conversazione:

- Verifica che la conversazione risalga a meno di 30 giorni
- Verifica che l'ID della conversazione sia corretto
- Assicurati di disporre di connettività di rete

Ottenere supporto

Per ulteriore assistenza, visita AWS Support tramite la [AWS console](#).

Quando apri un ticket di assistenza, includi:

- Registri delle conversazioni da `~/.aws/atx/custom/<conversation_id>/logs/`
- Registri di Subagent da `~/.aws/atx/custom/<conversation_id>/logs/subagents/`
- Registri di debug da `~/.aws/atx/logs/`
- Procedure per riprodurre il problema
- AWS Versione Transform CLI () `atx --version`

Problemi di accesso a S3

Il servizio personalizzato AWS Transform fornisce URL prefirmati S3 per facilitare il caricamento e il download dei computer client dei file di trasformazione potenzialmente grandi. to/from Ciò significa che non solo la CLI interagisce con gli endpoint del servizio AWS Transform, ma interagisce anche con gli endpoint del servizio S3. Queste interazioni utilizzano URL prefirmati, quindi le credenziali IAM del cliente non richiedono alcuna autorizzazione S3, ma a volte le configurazioni del server proxy del computer locale e le policy degli endpoint VPC S3 della rete possono limitare questo traffico.

Esamina i messaggi di errore più dettagliati [the section called “Posizioni dei log”](#) per aiutare a causare eventuali errori degli strumenti o negare l'accesso a S3 in relazione al download e al caricamento dei file di trasformazione.

Se utilizzi un VPN/Proxy server che sfrutta le variabili di `no_proxy` ambiente `https_proxy` e, ad esempio, prendi in considerazione l'aggiunta dei seguenti valori al valore della variabile di `no_proxy` ambiente per aggirare il proxy per gli endpoint dei servizi personalizzati S3 e AWS Transform:

Linux and macOS

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

Windows (PowerShell)

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

Se utilizzi un account [AWS PrivateLink per Amazon S3](#) nel tuo VPC, è possibile che sia stata definita una politica per limitare il traffico S3. Assicurati che la tua policy sugli endpoint VPC S3 GetObject consenta PutObject e operi per i bucket di proprietà AWS del servizio personalizzato Transform. Ciò può essere ottenuto aggiungendo la seguente dichiarazione alla policy degli endpoint VPC:

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

DenyLe dichiarazioni esplicite nelle policy hanno la precedenza sulle dichiarazioni. Allow Consulta le policy degli endpoint VPC di S3 Deny per le dichiarazioni che potrebbero limitare l'accesso.

AWS Cronologia delle versioni di Transform CLI

Consulta la tabella seguente per i dettagli sulle versioni correnti e precedenti della CLI AWS Transform. La tabella include la versione, la data di rilascio e le note di rilascio per ciascuna versione.

Versione	Data di rilascio	Note di rilascio
3.6.0 (più recente)	17 luglio 2026	- È stato aggiunto il <code>atx custom def learnings</code> sottocomando, che apre una sessione TUI interattiva per visualizzare e gestire gli apprendimenti generati automaticamente per una definizione di trasformazione basata su esecuzioni precedenti. - È stata aggiunta la raccolta di telemetria di utilizzo durante l'esecuzione della trasformazione. Per disabilitare la telemetria, imposta la variabile di ambiente. <code>ATX_DISABLE_TELEMETRY=true</code> Per ulteriori informazioni, consulta Utilizzo: telemetria.

Versione	Data di rilascio	Note di rilascio
		• È stato risolto un problema in Windows a causa del quale le operazioni sui file che ~ utilizzavano percorsi (home directory) venivano risolte in una directory inaspettata. Ciò ha causato read/write errori nei file durante una sessione. • È stato risolto un problema a causa del quale i nomi dei server e degli strumenti MCP contenenti caratteri speciali potevano causare errori di connessione. La CLI ora disinfecta automaticamente i nomi per utilizzare solo caratteri validi.
3.5.0	8 luglio 2026	• Aggiunto il supporto nativo per Windows. Ora puoi eseguire i comandi AWS Transform Custom direttamente su Windows. (I <code>atx ct</code> comandi non sono ancora supportati in Windows) • Sono stati aggiunti alcuni input di controllo per consentire e alle analisi di <code>atx ct analysis run</code> prontezza degli agenti e di prontezza alla modernizzazione di riflettere le preferenze dell'utente. Utilizzateli <code>--context</code> per l'inquadramento strategico, per impostare l'accesso degli agenti in <code>--agent-scope</code> modo da renderli pronti per gli agenti e /per indirizzare le raccomandazioni di modernizzazione verso o allontanarle da tecnologie specifiche. <code>--prefer --avoid</code> • Le definizioni di trasformazione nel formato skill possono ora includere una <code>scripts/</code> cartella, che consente di raggruppare gli script di supporto insieme ai riferimenti e ai riferimenti. <code>SKILL.md</code> • Aggiunto <code>--wait atx ct remediation create</code>, che attende il completamento della riparazione. • È stata aggiunta la modalità headless per l'esecuzione in un colpo solo. Esegui <code>atx -x "prompt" -t</code> per passare una richiesta, ottenere una risposta ed esci senza istruzioni interattive. La modalità Headless richiede la fiducia in tutti gli strumenti.

Versione	Data di rilascio	Note di rilascio
3.4.1	2 luglio 2026	È stato risolto un problema relativo alla sessione interattiva introdotto dalla versione 3.4.0. Dopo che l'agente ha finito di rispondere, la CLI potrebbe rimanere sul prompt «Thinking» (mostrato con i puntini di sospensione nell'interfaccia utente) invece di tornare al prompt di input. La CLI ora ti riporta al prompt di input dopo ogni risposta.

Versione	Data di rilascio	Note di rilascio
3.4.0 (non consigliato)	29 giugno 2026	 Problema noto Nelle sessioni interattive, la CLI potrebbe rimanere sul prompt «Thinking» (mostrato con i puntini di sospensione nell'interfaccia utente) dopo che l'agente ha finito di rispondere. Questo ti impedisce di inserire il tuo prossimo messaggio. Per risolvere questo problema, esegui l'aggiornamento alla versione 3.4.1 o successiva. <code>atx update</code> • È stato aggiunto <code>atx ct schema</code> un manifesto leggibile dalla macchina dell'intera superficie di <code>atx ct</code> comando per lo scripting e l'automazione. • È stata aggiunta la convalida dell'ambito del token quando si aggiunge o aggiorna una fonte, facendo emergere immediatamente problemi relativi a credenziali o autorizzazioni anziché fallire successivamente durante l'analisi. • Le pull request di riparazione automatica sono state migliorate per includere la ricerca del contesto e supportare la modalità bozza per PR più revisionabili. • Feedback migliorato sull'avanzamento della CLI con contesto in tempo reale sull'attività corrente, sui minuti stimati degli agenti e sull'attività dei subagenti. • È stata aggiunta l'identità configurabile dell'autore del commit del checkpoint tramite le <code>ATX_GIT_COMMITTER_NAME</code> variabili di ambiente e <code>ATX_GIT_COMMITTER_EMAIL</code> • Diverse correzioni e miglioramenti di piccole dimensioni.

Versione	Data di rilascio	Note di rilascio
3.3.0	18 giugno 2026	• Aggiunta coerenza <code>--json</code> e <code>--help</code> supporto per tutti <code>atx ct</code> i comandi. • È stata corretta la configurazione del Security Agent in modo che lo spazio dell'agente venisse creato durante la configurazione e rimosso durante lo smontaggio. • Diverse correzioni e miglioramenti di piccole dimensioni.
3.2.0	15 giugno 2026	• Aggiunti comandi di modernizzazione continua (<code>atx ct</code>) alla distribuzione CLI standard per tutti gli utenti. • È stata migliorata l'esecuzione dei subagenti per mostrare uno spinner «Thinking...» in attesa delle risposte del server, fornendo un chiaro feedback visivo sull'avanzamento del lavoro. • Spinner migliorato che si riavvia automaticamente con «Working on it...» dopo 3 secondi di silenzio dopo l'uscita dell'agente, in modo che il terminale non appaia mai bloccato tra le fasi di elaborazione. • Thinking spinner migliorato con una sottile animazione luccicante per un aspetto visivo più raffinato.

Versione	Data di rilascio	Note di rilascio
3.1.0	3 giugno 2026	• È stata aggiunta una variabile di <code>ATX_MAX_VALIDATION_LOOPS</code> ambiente per configurare il numero massimo di cicli di convalida. • Il controllo fisso degli aggiornamenti non mostra più falsi avvisi di «aggiornamento disponibile» quando la versione installata è già più recente della versione del registro. • Il problema fisso <code>delete --transformation-name ""</code> non mostra più una richiesta di conferma senza senso; i valori vuoti vengono ora rifiutati con un chiaro errore di convalida. • I sottocomandi fissi non riconosciuti ora mostrano «comando sconosciuto» invece di un messaggio di errore interno confuso. • Risolto il problema del confronto tra le versioni per utilizzare il confronto numerico anziché la disuguaglianza di stringhe per i controlli di aggiornamento.
3.0.0	21 maggio 2026	• È stata aggiunta la convalida dei nomi prima della conversione che suggerisce nomi simili dal registro quando non viene trovato un nome, aiutando a catturare gli errori di battitura senza bisogno di un comando <code>list</code> separato. • Sono state aggiunte spiegazioni opzionali per i comandi di shell, che mostrano a cosa servono e perché. • Banner sulle impostazioni di attendibilità migliorato per includere ulteriori informazioni sulle autorizzazioni degli strumenti. • È stato aggiunto il banner per i disabili dell'apprendimento quando si utilizza il flag <code>Do-not-Learn</code>, che dà visibilità alla funzionalità di apprendimento e spiega come attivarla. • Ora è richiesta la modifica definitiva: Node.js 22 o versioni successive. Effettua l'upgrade da https://nodejs.org/ se utilizzi una versione precedente.

Versione	Data di rilascio	Note di rilascio
2.0.0	14 maggio 2026	• È stato aggiunto il supporto remoto per i server MCP: connessi ai server MCP HTTP e HTTPS con fallback SSE automatico, autenticazione con token Bearer con espansione delle variabili di ambiente nelle intestazioni e supporto proxy (). HTTP_PROXY/HTTPS_PROXY • È stato aggiunto un sottocomando come alias per. <code>atx resume atx --resume</code> • È stato aggiunto <code>grep</code> uno strumento per la ricerca di testo su più file con controllo dell'output: supporta modelli regex, filtraggio dei file glob, ricerca senza distinzione tra maiuscole e minuscole, limiti configurabili e troncamento dell'output. <code>depth/result</code> • Implementazione MCP migliorata per utilizzare l'SDK MCP standard per un comportamento più coerente e un supporto più semplice per le future funzionalità MCP. • Migliore gestione dell'output della shell: l'output viene ora troncato senza problemi a 30.000 caratteri per stream anziché causare un errore grave, preservando l'inizio e la fine dell'output per uso contestuale. • È stato risolto un problema per cui <code>Ctrl+C</code> durante una sessione interattiva poteva uscire prematuramente dalla CLI anziché interrompere l' Linux/macOS operazione corrente e tornare al prompt. • È stato corretto il messaggio di rifiuto della fiducia che mostrava un motivo specifico per cui la fiducia non è disponibile, separato dal motivo per cui il comando richiedeva l'autorizzazione. • È stato corretto un avviso di comando pericoloso che non menzionava più la fiducia quando il comando è attivo. <code>alwaysPromptCommands</code>

Versione	Data di rilascio	Note di rilascio
1.10.0	29 aprile 2026	• Descrizioni degli strumenti migliorate con indicazioni su più strumenti, che aiutano l'agente a scegliere lo strumento migliore per ogni attività e riducono l'uso non necessario della shell. • Aggiunto <code>alwaysPromptCommands</code> in <code>trust-settings.yaml</code> : configura modelli di comandi della shell che richiedono sempre un'autorizzazione esplicita , indipendentemente dalle impostazioni di attendibilità. Supporta i caratteri jolly glob e le corrispondenze con ogni sottocomando nelle espressioni composte. <code>trustedShellCommands</code> può sovrascrivere questi schemi. Non applicato in modalità non interattiva per evitare di interrompere le pipeline automatizzate. • I percorsi relativi fissi non venivano risolti in percorsi assoluti.
1.9.0	23 aprile 2026	• Procedure di approvazione degli strumenti migliorate: ogni opzione ora mostra il suo effetto in linea, un messaggio «Perché» spiega perché è necessaria l'approvazione e la conferma dell'attendibilità include un suggerimento sull'attendibilità permanente. <code>trust-settings.yaml</code>
1.8.0	16 aprile 2026	• Il prefisso di output dell'agente è stato modificato da <code>></code> a <code>ATX:</code> per una distinzione visiva più chiara tra input utente e output dell'agente. • Visualizzazione fissa del comando <code>resume</code> quando i tentativi CLI sono esauriti. • Risolto il problema del curriculum da una directory di lavoro diversa. In modalità interattiva, richiede il percorso corretto; in modalità non interattiva, fallisce rapidamente con un errore descrittivo.

Versione	Data di rilascio	Note di rilascio
1.7.1	9 aprile 2026	• È stato risolto l'errore di accesso SSO («Token di sessione non trovato o non valido») quando la regione del fornitore di credenziali è diversa da quella del profilo. <code>sso_region</code> • È stato corretto il caching delle credenziali in modo che le sessioni di lunga durata non abbiano più esito negativo quando le credenziali vengono ruotate sul disco.
1.7.0	2 aprile 2026	• <code>execComando</code> fisso per uscire con il codice 1 sugli errori di convalida dell'input, rendendo la CLI affidabile negli script CI/CD e nelle pipeline. • Aggiunta la visualizzazione dei messaggi di avviso dal servizio. • È stato aggiunto il supporto MFA prompt per AWS i profili di credenziali. • Chiamate di credenziali STS fisse per rispettare le impostazioni del proxy HTTP (S).
1.6.0	18 marzo 2026	• È stata aggiunta <code>--limit <minutes></code> l'opzione per impostare il budget <code>exec</code> e <code>interactive</code> i comandi di Agent Minutes. Quando viene raggiunto il limite, la CLI mostra l'utilizzo ed esce con le istruzioni di ripristino. • Registrazione fissa del messaggio iniziale dell'utente nei registri delle conversazioni.
1.5.0	11 marzo 2026	• È stato aggiunto il supporto per l'esecuzione simultanea delle attività, che consente trasformazioni più rapide. • È stato aggiunto il display di utilizzo di Agent Minutes alla fine di ogni conversazione e <code>/usage</code> il comando in modalità interattiva per controllare l'utilizzo in qualsiasi momento.

Versione	Data di rilascio	Note di rilascio
1.4.0	2 marzo 2026	• Messaggi di errore migliorati durante il salvataggio delle definizioni di trasformazione con file non supportati. • È stato aggiunto un timeout alle chiamate di servizio per evitare che la CLI si blocchi quando la connessione viene interrotta. • Il processo CLI fisso si bloccava dopo il completamento con successo. • Convalida fissa della regione alla ripresa delle conversazioni.
1.3.0	19 febbraio 2026	• Restrizione rimossa per i percorsi del server MCP: gli utenti possono ora specificare qualsiasi percorso per la command proprietà nella configurazione MCP. • Migliore stabilità delle connessioni ai server MCP.
1.2.0	9 febbraio 2026	• È stato aggiunto il supporto per la configurazione del proxy tramite variabili di ambiente (<code>https_proxy</code> <code>no_proxy</code>, ecc.). • Miglioramenti generali della stabilità e correzioni di bug.
1.1.1	16 gennaio 2026	Correzioni di bug e miglioramenti dell'affidabilità.
1.1.0	13 gennaio 2026	Aggiunto il supporto per la configurazione della regione AWS CLI, i controlli precoci di convalida delle credenziali e la funzionalità fissa di ripresa della campagna.
1.0.1	18 dicembre 2025	Arresti agevoli, registri degli errori più puliti e miglioramenti generali.
1.0.0	1 dicembre 2025	Versione iniziale della CLI AWS Transform.

AWS Trasforma la modernizzazione continua

Che cos'è AWS Trasformare la modernizzazione continua?

AWS La modernizzazione continua di Transform fornisce analisi e correzione per i tuoi repository di codice sorgente. Puoi connettere GitHub organizzazioni, GitLab gruppi, aree di lavoro Bitbucket e repository locali, quindi eseguire analisi automatizzate per identificare il debito tecnico, le vulnerabilità di sicurezza, le opportunità di modernizzazione e la disponibilità degli agenti nell'intera codebase.

Tutte le Account AWS analisi e le correzioni vengono eseguite direttamente utilizzando le tue credenziali. Il codice sorgente rimane sotto il tuo controllo.

Note

Ti consigliamo di iniziare con Kiro Power o il plugin Agent. L'abilità dell'agente orchestra la configurazione, l'onboarding e l'uso continuo della modernizzazione continua, tra cui il provisioning dell'infrastruttura, la configurazione dei sorgenti, l'esecuzione dell'analisi, la valutazione dei risultati e la correzione. Per le istruzioni di installazione, consulta [Strumenti per sviluppatori](#).

Funzionalità chiave

AWS La modernizzazione continua di Transform offre le seguenti funzionalità:

- **Analisi del debito tecnologico:** scansiona gli archivi alla ricerca di dipendenze obsolete, vulnerabilità di sicurezza, problemi di qualità del codice e opportunità di modernizzazione. Esegui scansioni rapide dei metadati tra i manifesti dei pacchetti o analisi complete a livello di codice. Definisci criteri di analisi personalizzati utilizzando definizioni di trasformazione adattate al tuo ambiente.
- **Riparazione autonoma:** genera richieste pull convalidate su larga scala. Ogni risultato può essere riparato automaticamente utilizzando la definizione di trasformazione associata. Remediation crea filiali e si apre PRs/MRs automaticamente su GitHub GitLab, e Bitbucket.
- **Reporting:** genera report HTML che mostrano i risultati per gravità, archivio e tipo di analisi. Monitora l'avanzamento delle misure correttive e la ricerca di una soluzione nel tempo.

- Monitoraggio continuo: pianifica analisi ricorrenti utilizzando Amazon Scheduler. EventBridge Configura pianificazioni cron giornaliere, settimanali o personalizzate per monitorare continuamente il tuo portafoglio alla ricerca di nuove emissioni.

Tipi di analisi

AWS La modernizzazione continua di Transform supporta i seguenti tipi di analisi per soddisfare le vostre esigenze di modernizzazione.

Tipo	Description
rapid-techdebt-analysis	Scansione rapida dei manifesti dei pacchetti (pom.xml,,requirements.txt) basata solo sui metadati per identificare versioni package.json obsolete e dipendenze obsolete. Non analizza il codice sorgente.
tech-debt-comprehensive	Analisi tecnica approfondita del debito a livello di codice utilizzando l'agente AWS Transform . Esamina il codice sorgente per identificare i modelli di debito, i problemi di qualità del codice, i problemi di architettura e le opportunità di miglioramento.
security	Vulnerabilità di sicurezza e rilevamento CVE tramite Security Agent. AWS Esegue la scansione del codice sorgente e delle dipendenze alla ricerca di vulnerabilità note, modelli di codifica non sicuri e punti deboli sfruttabili. Richiede una configurazione dell'infrastruttura una tantum.
agentic-readiness	Valutazione della preparazione all'integrazione di AI e agenti. Assegna 56 criteri in cinque categorie: infrastruttura e piattaforma, architettura delle applicazioni, Data Foundations e

Tipo	Description
	Operations & Observability. Identity/Security/Governance
modernization-readiness	Valutazione delle opportunità di modernizzazione del cloud. Valuta la preparazione in tutte le dimensioni di infrastruttura, applicazione, dati, sicurezza e operazioni. Identifica i candidati per la containerizzazione, la migrazione senza server e gli aggiornamenti della piattaforma.
custom	Esegui qualsiasi definizione di trasformazione (TD) come analisi. Utilizzate questo tipo per definire criteri di analisi personalizzati o per eseguire trasformazioni AWS gestite non coperte dai tipi integrati.

Comprensione dei concetti chiave

Origini

Una fonte indica alla modernizzazione continua dove si trovano i tuoi repository. Tipi di fonti supportati:

- GitHub— Organizzazioni con token di accesso personali (classico)
- GitLab— Gruppi o utenti, incluse le istanze ospitate autonomamente
- Bitbucket: spazi di lavoro (cloud) o progetti (data center)
- Locale: directory principali contenenti repository git

Repositories

I repository vengono scoperti mediante la scansione delle fonti. Dopo l'individuazione, è possibile filtrare in base alla fonte, alle etichette o ad altri criteri, applicare etichette in base all'organizzazione (team, priorità, ondata di migrazione) e indirizzare repository specifici per l'analisi o la correzione.

Analisi

Un'analisi è una scansione di uno o più repository utilizzando un tipo di analisi specifico. Ogni analisi produce risultati che identificano i problemi nel codice. È possibile eseguire analisi su richiesta o pianificarne l'esecuzione automatica. I tipi di analisi includono l'analisi rapida del debito tecnologico, l'analisi completa del debito tecnico, la sicurezza, la preparazione agli agenti, la preparazione alla modernizzazione e la personalizzazione. Ogni analisi tiene traccia del proprio stato (in sospeso, in esecuzione, completa, annullata o non riuscita) e dei repository scansionati.

Esiti

I risultati sono i risultati dell'analisi. Ogni risultato include la gravità (alta, media o bassa), lo stato (aperto, ignorato o obsoleto) e la trasformazione della correzione che può porvi rimedio (se risolvibile automaticamente). Le nuove scoperte iniziano come aperte. Gli utenti possono respingere i risultati con un motivo. Re-analysis contrassegna automaticamente i risultati risolti come obsoleti.

Correzioni

Le riparazioni applicano le definizioni di trasformazione per correggere i risultati. Tre modalità: basata sui risultati (ogni risultato utilizza la propria trasformazione fissa), TD override (sovrascrive la definizione di trasformazione per risultati specifici) e TD diretta (esegue una trasformazione su un repository senza risultati). L'output dipende dal fornitore di origine (GitHub PR, GitLab MR, Bitbucket PR o filiale locale).

Definizioni di trasformazione

Una definizione di trasformazione contiene le istruzioni e le conoscenze necessarie per eseguire una trasformazione specifica del codice. La modernizzazione continua utilizza definizioni di trasformazione per analisi personalizzate (`--type custom --transformation-name name`) e correzione (`--transformation-name name`). Elenca le definizioni di trasformazione disponibili con `atx custom def list`

In che modo AWS Trasforma i lavori di modernizzazione continua

AWS La modernizzazione continua di Transform viene in genere utilizzata in progetti su larga scala in cui più codebase richiedono analisi e correzioni continue. I team in genere seguono questo flusso di lavoro:

1. **Connect Sources:** aggiungi GitHub organizzazioni, GitLab gruppi, aree di lavoro Bitbucket o directory locali come fonti. Fornisci token di autenticazione con ambiti appropriati.
2. **Scopri i repository:** esegui scansioni di rilevamento per enumerare tutti i repository nelle tue fonti. Usa le etichette per organizzare gli archivi per team, priorità o ondata di migrazione.
3. **Esegui analisi:** esegui analisi su tutto il tuo portafoglio. Scegli scansioni rapide per risultati rapidi o analisi complete per risultati dettagliati. L'analisi della sicurezza richiede una configurazione dell'infrastruttura a tantum.
4. **Esamina i risultati:** esamina i risultati per gravità, archivio o tipo di analisi. Elimina i falsi positivi con motivazioni documentate. Re-run analisi per contrassegnare i problemi risolti come obsoleti.
5. **Correzione:** crea correzioni per correggere i risultati. La modernizzazione continua crea automaticamente filiali e apre pull/merge le richieste con le correzioni. Tieni traccia dello stato delle riparazioni e riprova gli errori.
6. **Configura l'analisi continua:** pianifica analisi ricorrenti utilizzando Amazon Scheduler. EventBridge Configura la cadenza di analisi (giornaliera, settimanale o cron personalizzata) per monitorare continuamente il tuo portafoglio alla ricerca di nuove emissioni. Combinalo con la correzione automatica per mantenere l'integrità del codice nel tempo.

Opzioni di calcolo

La modernizzazione continua supporta tre opzioni di elaborazione per l'esecuzione di analisi e correzioni. Le competenze degli agenti nel plug-in Kiro Power and agent ti aiutano a configurare l'infrastruttura per ciascuna opzione.

Note

Indipendentemente dall'opzione di elaborazione, tutte le analisi e le correzioni avvengono Account AWS utilizzando le credenziali. Il codice sorgente rimane sotto il tuo controllo.

Locale (impostazione predefinita)

Per impostazione predefinita, le analisi vengono eseguite sul computer locale. Questa opzione non richiede alcuna infrastruttura aggiuntiva. Il server viene eseguito localmente ed esegue le analisi utilizzando risorse di calcolo locali. Ottimo per provare lo strumento, piccoli repository o per uso individuale.

Amazon Amazon EC2

Esegui analisi su un'istanza Amazon EC2 persistente nel tuo Account AWS. Questa opzione scarica l'elaborazione dal computer locale, supporta analisi più ampie e consente analisi pianificate ricorrenti. L'istanza rimane in esecuzione tra un invio e l'altro.

L'abilità dell'agente fornisce uno AWS CloudFormation stack che include:

- Un'istanza Amazon EC2 (Amazon Linux 2023) con Docker e il contenitore di modernizzazione continua
- Un ruolo IAM con autorizzazioni per AWS Transform, Amazon S3, KMS AWS , Secrets Manager e l'agente di sicurezza
- AmazonSSMManagedInstanceCore per l'accesso alla shell tramite SSM (non sono richieste coppie di chiavi SSH o porte in ingresso)
- Un gruppo di sicurezza senza regole in entrata

Il tuo utente o ruolo IAM necessita delle autorizzazioni per la gestione del ciclo di vita di Amazon EC2, le operazioni di stack AWS CloudFormation , la creazione di ruoli IAM, le operazioni sui bucket Amazon S3, la gestione segreta di Secrets Manager e i comandi SSM.

Per configurare l'esecuzione di EC2, installa Kiro Power o il plug-in dell'agente (vedi [Strumenti per sviluppatori](#)), quindi chiedi all'agente: «Configura un'istanza EC2 per l'analisi della modernizzazione continua». L'agente effettua il provisioning dell'infrastruttura, verifica che il contenitore sia integro e invia le analisi tramite SSM, senza bisogno di SSH.

AWS Batch (Fargate)

Esegui le analisi come lavori isolati su AWS Batch con Fargate per l'elaborazione senza server. Ogni analisi viene eseguita nel proprio contenitore senza gestire un'infrastruttura persistente. Ideale per l'analisi parallela di più fonti o tipi di analisi.

Questa opzione riutilizza lo stack di infrastruttura AWS Transform CDK. L'abilità dell'agente implementa l'infrastruttura richiesta, tra cui:

- AWS Ambiente di elaborazione e coda di lavoro in batch
- Definizione del lavoro con l'immagine del contenitore di modernizzazione continua
- Ruoli IAM per l'esecuzione di lavori in batch
- Una funzione Lambda per l'invio di lavori

Per configurare l'esecuzione in Batch, installa Kiro Power o il plug-in dell'agente (vedi [Strumenti per sviluppatori](#)), quindi chiedi all'agente: «Esegui la mia analisi su Fargate» o «Imposta l'esecuzione Batch per la modernizzazione continua». L'agente distribuisce lo stack CDK, memorizza le credenziali di origine in Secrets Manager e invia i lavori di analisi a Batch. AWS

Configurazione del Security Agent

Il tipo di security analisi utilizza il servizio AWS Security Agent per il rilevamento di vulnerabilità e CVE. A differenza di altri tipi di analisi, richiede la configurazione dell'infrastruttura una tantum presso l'azienda. Account AWS

Il comando setup fornisce uno AWS CloudFormation stack che include:

- Un bucket Amazon S3 per il caricamento del codice sorgente
- Un ruolo IAM assunto da `securityagent.amazonaws.com`
- Una politica gestita per il ruolo di agente di sicurezza

Il tuo utente o ruolo IAM deve disporre delle seguenti autorizzazioni aggiuntive per eseguire la configurazione:

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

Utilizza i seguenti comandi per gestire l'infrastruttura del Security Agent:

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

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

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

Una volta completata la configurazione, è possibile eseguire le analisi di sicurezza allo stesso modo degli altri tipi di analisi.

Nozioni di base

Prerequisiti

Per utilizzare in modo efficace la modernizzazione continua, è necessario avere una conoscenza di base del controllo della versione di Git, familiarità con la piattaforma del codice sorgente (o Bitbucket) GitHub GitLab, una conoscenza pratica delle autorizzazioni AWS IAM ed esperienza con gli strumenti da riga di comando.

Prima di utilizzare la modernizzazione continua, verifica di disporre di quanto segue:

- AWS Transform CLI installata:

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

- Node.js 22 o versione successiva
- AWS Credenziali valide (AWS_PROFILE o variabili di ambiente)
- La policy AWS gestita AWSTransformCustomFullAccess allegata al tuo utente o ruolo IAM

Avvio rapido

1. Avvia il server di modernizzazione continua:

```
atx ct server &
```

2. Aggiungi una fonte:

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

name Dov'è un identificatore descrittivo per la fonte, *provider* è la piattaforma (github, gitlab, olocal) bitbucket, *org-or-group* è il nome dell'organizzazione o del gruppo e *token* il token di autenticazione.

3. Scopri i repository:

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

4. Esegui un'analisi:


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

5. Esplora i risultati:

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

6. Correggere i risultati:

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

Lavorare con una modernizzazione continua

Gestione delle fonti

Usa `atx ct source` i comandi per connettere i repository. Provider supportati: GitHub GitLab, Bitbucket, local.

GitHub organizzazioni

Token: token di accesso personale (classico) con repo ambito. Read-only per l'analisi, repository completo per la correzione.

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

GitLab gruppi e utenti

Token: token di accesso personale con api ambito.

```
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
```

Spazi di lavoro e progetti Bitbucket

Bitbucket Cloud — ambiti:,,, read:repository:bitbucket write:repository:bitbucket
read:pullrequest:bitbucket write:pullrequest:bitbucket Inoltre ha bisogno di e. --
email --username

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

Centro dati Bitbucket:

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

Archivi locali

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

Important

--path deve puntare a una directory principale contenente i repository git come sottodirectory, non a un singolo repository.

Gestire le fonti

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

Individuazione e gestione dei repository

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

Dopo la scoperta:

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

Analisi in corso

Il `--type` flag specifica il tipo di analisi da eseguire:

- `rapid-techdebt-analysis`— Dipendenze obsolete e vittorie facili.
- `tech-debt-comprehensive`— AI-powered Analisi più approfondita sui risultati relativi a dipendenza, sicurezza, pattern, prestazioni, manutenibilità, architettura, qualità del codice e infrastruttura.
- `security`— Vulnerabilità ed esposizioni in materia di sicurezza.
- `agentic-readiness`— Disponibilità degli archivi per gli agenti di intelligenza artificiale (framework, API, documentazione).
- `modernization-readiness`— Opportunità di modernizzazione in tutte le dimensioni dell'infrastruttura, delle applicazioni, dei dati, della sicurezza e delle operazioni.

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

Analisi personalizzata

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

Configurazione con `-g` flag: key-value, JSON o percorso del file.

Elenca iTD: `atx custom def list`

Gestione degli esiti

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

Ricerca degli stati

- open— Attivo
- dismissed— Licenziato manualmente (richiede un motivo)
- obsolete— System-set quando la nuova analisi non produce più il risultato

```
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
```

Trovare l'obsolescenza

Re-analysis contrassegna i risultati risolti come obsoleti. Non può essere riaperto. Conservato per l'audit.

Creazione di soluzioni correttive

Tre modalità: basata sui risultati, TD override, TD diretto.

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

Output per provider: GitHub PR, GitLab MR, Bitbucket PR, filiale locale.

Note

Il token deve avere accesso in scrittura per la PR/MR creazione.

Esecuzione locale con `--local` flag.

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

```
atx ct remediation status --id id  
atx ct remediation retry --id id  
atx ct remediation delete --id id
```

AWS Trasforma l'applicazione web (opzionale)

L'applicazione web AWS Transform è un'interfaccia opzionale per il monitoraggio delle analisi, dei risultati e delle correzioni di modernizzazione continua in tutto il portafoglio di sorgenti di codice.

Prima di utilizzare l'applicazione web AWS Transform, è necessario disporre di un'identità utente abilitata per accedere a AWS Transform nella propria organizzazione. Per informazioni sull'attivazione di AWS Transform, consulta [Configurazione di AWS Transform](#).

Per utilizzare l'applicazione web AWS Transform:

1. Visita <https://aws.amazon.com/transform/> e accedi utilizzando le credenziali AWS IAM Identity Center.
2. Se la modernizzazione continua non viene visualizzata dopo l'accesso, accedi invece con le credenziali IAM. Per abilitare l'accesso alle credenziali IAM:
 - a. Nella console di AWS gestione, apri AWS Transform e scegli Impostazioni.
 - b. Nella sezione Access AWS Transform with IAM credentials, abilita l'accesso alle credenziali IAM.
 - c. Nella stessa pagina delle impostazioni, copia il link di accesso mostrato in URL dell'applicazione Web (con IAM).
 - d. Incolla l'URL di accesso nella stessa finestra del browser in cui è aperta la console di AWS gestione. Ciò garantisce che l'applicazione Web utilizzi le AWS credenziali di quell'account.
3. Apri il menu di navigazione a sinistra e scegli la modernizzazione continua. La dashboard mostra statistiche di riepilogo tra cui fonti, repository, risultati totali per gravità e tipi di analisi.
4. Utilizza le schede Analisi, Risultati e Correzioni per visualizzare i risultati dettagliati.
5. Chatta con AWS Transform direttamente dall'applicazione Web per porre domande sulle analisi, i risultati o le correzioni.

L'applicazione web è progettata per operazioni su scala aziendale in cui è necessaria una visibilità centralizzata sulle analisi e le correzioni di modernizzazione continua su più basi di codice.

Strumenti per sviluppatori

Puoi accedere alla modernizzazione continua dagli IDE agentici utilizzando il plug-in AWS Transform Power and agent. L'agente orchestra la configurazione, l'onboarding e l'uso continuo della modernizzazione continua attraverso l'interazione conversazionale.

- [Kiro IDE: installa Transform Kiro Power.AWS](#) Apri Kiro Chat e chiedi all'agente di aiutarti con i flussi di lavoro di modernizzazione continua.
- Claude Code, Codex, Cursor: [installa -plugins \(directory\). awslabs/agent](#) plugins/aws-transform Il plugin agent offre le stesse funzionalità di Kiro Power.

Competenze dell'agente

Il plug-in Kiro Power and agent include competenze che orchestrano flussi di lavoro di modernizzazione continua attraverso l'interazione conversazionale:

Abilità	Description
Guida	Onboarding interattivo che ti guida passo dopo passo attraverso l'intero flusso di lavoro
Origine	Aggiungi, elenca e rimuovi le connessioni di origine
Individuazione	Scansiona le fonti per scoprire i repository
Analisi	Esegui e gestisci analisi di tutti i tipi
Esiti	Interroga, filtra e gestisci i risultati delle analisi
Correzione	Crea e gestisci le correzioni per correggere i risultati
Esecuzione EC2	Esegui il provisioning e gestisci un'istanza Amazon EC2 per l'analisi remota
Esecuzione in batch	Invia lavori di analisi a AWS Batch with Fargate

Abilità	Description
Schedule	Imposta analisi ricorrenti su una pianificazione cron utilizzando Amazon Scheduler EventBridge
Creazione di report	Genera report HTML autonomi con grafici che mostrano i risultati, la distribuzione della gravità e lo stato di avanzamento della correzione

Documentazione di riferimento della CLI

La tabella seguente riassume tutti i sottocomandi. `atx ct`

Sottocomando	Description
<code>atx ct server</code>	Avviare il server di modernizzazione continua
<code>atx ct status</code>	Visualizza lo stato del sistema, incluse fonti, repository, analisi, risultati e correzioni
<code>atx ct source add</code>	Aggiungi una fonte (GitHub GitLab, Bitbucket o locale)
<code>atx ct source list</code>	Elenca le fonti configurate
<code>atx ct source remove</code>	Rimuovi una fonte
<code>atx ct discovery scan</code>	Scopri i repository da una fonte
<code>atx ct discovery status</code>	Controlla lo stato di Discovery Scan
<code>atx ct repository list</code>	Elenca i repository con filtri opzionali
<code>atx ct repository get</code>	Crea un unico repository
<code>atx ct repository update</code>	Aggiorna le etichette del repository
<code>atx ct repository delete</code>	Eliminare un repository

Sottocomando	Description
<code>atx ct analysis run</code>	Esegui un'analisi sui repository
<code>atx ct analysis get</code>	Ottieni i dettagli dell'analisi
<code>atx ct analysis list</code>	Elenca le analisi con filtri opzionali di stato e tipo
<code>atx ct analysis cancel</code>	Annula un'analisi in corso
<code>atx ct analysis delete</code>	Eliminare un'analisi
<code>atx ct findings list</code>	Elenca i risultati con filtri per repository, origine, gravità, tipo, stato e analisi
<code>atx ct findings get</code>	Ottieni una singola scoperta
<code>atx ct findings update</code>	Aggiorna lo stato della ricerca (aperta o ignorata)
<code>atx ct findings batch-update</code>	Aggiornamento in batch di più risultati
<code>atx ct findings delete</code>	Eliminare un risultato ignorato o obsoleto
<code>atx ct remediation create</code>	Crea una correzione in base ai risultati o a una definizione di trasformazione
<code>atx ct remediation list</code>	Elenca tutte le riparazioni
<code>atx ct remediation status</code>	Controlla lo stato della riparazione e visualizza i link PR/MR
<code>atx ct remediation retry</code>	Riprova una riparazione non riuscita
<code>atx ct remediation delete</code>	Eliminare una riparazione
<code>atx ct setup security-agent</code>	Fornisci o gestisci l'infrastruttura del Security Agent

Sottocomando	Description
<code>atx ct schema</code>	Stampa un manifesto JSON leggibile dalla macchina dell'intera superficie di comando (ogni <code>atx ct</code> comando, opzione e argomento) in modo che gli agenti e l'automazione possano scoprire la CLI senza analizzare il testo di aiuto

Risoluzione dei problemi

Connessione rifiutata o server non in esecuzione

La CLI di modernizzazione continua richiede un server in esecuzione. Inizia con `atx ct server` & e verifica con `atx ct status --health`

Discovery scan restituisce zero repository

Per le fonti locali, verifica che `--path` punti a una directory principale che contiene i repository come sottodirectory (ad esempio, `/home/user/repos`) e non direttamente a un repository (ad esempio, `/home/user/repos/my-app`). Lo scanner cerca le directory secondarie che contengono una cartella `.git`

Errore SETUP_REQUIRED

L'origine esiste nel tuo account ma le credenziali non sono configurate su questo computer. Esegui `atx ct source add --name name` per configurare le credenziali localmente.

Errore AUTH_REQUIRED

Nessun token valido trovato per l'origine. Verifica che il token sia corretto e abbia gli ambiti richiesti. Perché GitHub, assicurati che il token abbia un `repo` ambito. Perché GitLab, assicurati l'`api`ambito.

Errore INVALID_INPUT

Verificate di utilizzare il nome del tipo di analisi corretto. I valori validi sono: `rapid-techdebt-analysis`, `tech-debt-comprehensive`, `security`, `agentic-readiness`, `modernization-readiness`, `custom`.

Errori di autorizzazione durante la riparazione

La riparazione crea rami e pull/merge richieste, che richiedono l'accesso in scrittura al repository. Aggiorna il token con i permessi di scrittura. Perché GitHub, assicurati l'intero repo ambito. Perché GitLab, assicurati l'apiambito. Per Bitbucket, sure `write:repository:bitbucket` and `write:pullrequest:bitbucket` scopes.

La configurazione del Security Agent non riesce

Verifica che il tuo utente o ruolo IAM disponga delle autorizzazioni richieste AWS CloudFormation, IAM e Amazon S3 elencate nella sezione di configurazione del Security agent di. [In che modo AWS Trasforma i lavori di modernizzazione continua](#) Verifica lo stato con. `atx ct setup security-agent --status`

Modernizzazione continua non visibile nell'applicazione web

Se la modernizzazione continua non viene visualizzata dopo l'accesso all'applicazione web AWS Transform, accedi con le credenziali IAM del luogo in Account AWS cui AWS Transform è abilitato anziché AWS IAM Identity Center. Per le fasi, consulta [AWS Trasforma l'applicazione web \(opzionale\)](#).

Strumento di scoperta

Lo strumento di AWS Transform scoperta consente di individuare automaticamente l'inventario dei server dell'organizzazione per prepararsi alla migrazione. Lo strumento supporta VMware vCenter, Hyper-V Microsoft e server importati. Per utilizzare lo strumento di rilevamento, è necessario configurare una o più fonti di rilevamento, avviare lo strumento e quindi esaminare i risultati nel riquadro Inventario individuato.

Dopo aver configurato una fonte di rilevamento, lo strumento di rilevamento inizia a raccogliere informazioni. Il tempo necessario allo strumento di rilevamento per analizzare completamente la rete dipende dalle dimensioni dell'ambiente. Per un business case di migrazione direzionale, è possibile utilizzare i file Migration Portfolio Assessment (MPA) generati dallo strumento dopo il completamento della raccolta del server.

Workflow dello strumento Discovery

Il flusso di lavoro dello strumento di scoperta è costituito da due tipi di attività:

- Attività di configurazione
- Revisione e utilizzo dei dati

I passaggi seguenti descrivono come installare e utilizzare lo strumento di rilevamento e come utilizzare i dati raccolti:

1. Installa lo strumento di rilevamento.
2. Configura le fonti di rilevamento. È possibile configurare uno o più dei seguenti elementi: VMware vCenter, host Hyper-V Microsoft o server tramite un'importazione di file CSV. L'individuazione dei dati inizia dopo la configurazione di qualsiasi fonte.
3. Configura l'accesso al sistema operativo e quindi esamina lo stato della raccolta di server, database e connessioni di rete.
 - Modifica le credenziali del sistema operativo in base alle esigenze.
4. (Facoltativo) Configurare le credenziali Oracle per abilitare la raccolta diretta di SQL o utilizzare il rilevamento di OS-level fallback tramite SSH o WinRM.
5. Per generare un business case di migrazione, carica il file.zip in [Migration assessment](#) oppure decomprimilo e carica i file MPA dalla directory mpa_exports. L'esportazione include dati

provenienti da tutte le fonti configurate e contiene file MPA per VMware e server importati. Hyper-V

Lo strumento di rilevamento supporta i seguenti percorsi di rilevamento:

- Discovery automatico di VMware vCenter: individua automaticamente i server gestiti da VMware vCenter.
- Hyper-V individuazione automatica: individua automaticamente i server gestiti dagli Hyper-V host Microsoft.
- Importazione dal server: importa manualmente l'inventario del server tramite un file CSV.

Configurazione dello strumento di scoperta

Prerequisiti

Di seguito sono riportati i prerequisiti per l'utilizzo dello strumento di AWS Transform scoperta:

Prerequisiti generali

- Lo strumento richiede 4 vCPU, 16 GB di RAM e un disco rigido da 35 GB.
- Il DHCP deve essere disponibile nella rete per lo strumento di rilevamento VM.
- Lo strumento raccoglie i dati utilizzando un approccio centralizzato. I server inclusi nell'ambito devono consentire la connettività in entrata dalla macchina virtuale dello strumento di rilevamento (porte predefinite, è supportata la configurazione personalizzata delle porte):
 - Linux — SSH TCP/22
 - Windows: TCP/5985 per HTTP, TCP/5986 per HTTPS
 - SNMP — UDP/161 (utilizzato solo per la raccolta in rete, non per le metriche del sistema operativo)
- Per Linux, account utente che possono utilizzare SSH per connettersi al server. Lo strumento di rilevamento esegue comandi tramite SSH per la raccolta di rete e le metriche del sistema operativo. La maggior parte dei comandi viene eseguita come utente normale. Un numero limitato di comandi tenta di eseguire il comando `sudo` e lo ritira automaticamente se `sudo` non è disponibile: `dmidecode` (UUID e produttore del server), `lvs` (rilevamento LVM) e `ss` o `netstat` (connessioni di rete con informazioni sul processo). Senza `sudo`, lo strumento di scoperta raccoglie ancora la maggior parte dei dati, ma mancheranno i dettagli di UUID, LVM e della rete a livello

di processo. Consigliamo di configurare sudo senza password per l'utente SSH per garantire la raccolta completa dei dati. Per un'analisi completa, vedi. [the section called “Autorizzazioni richieste”](#)

Prerequisiti VMware

- VMware vCenter Server versione 6.5, 6.7, 7.0 o 8.0.
- Autorizzazioni per implementare un OVA nel tuo VMware vCenter.
- Per la configurazione di VMware vCenter Server, un utente vCenter con il Read-Only ruolo assegnato a livello di datacenter principale. Per informazioni dettagliate, vedi [the section called “Autorizzazioni richieste”](#).

Hyper-V prerequisiti

- Windows Server con il Hyper-V ruolo abilitato.
- WinRM abilitato sugli host. Hyper-V
- Un account utente che è membro dei gruppi Remote Management Users, Hyper-V Administrators e Performance Monitor Users su ogni Hyper-V host, con accesso in lettura WMI allo spazio dei nomi. root\cimv2 Per informazioni dettagliate, vedi [the section called “Autorizzazioni richieste”](#).
- Autenticazione supportata: NTLM (solo HTTPS) e Kerberos (HTTP o HTTPS).

Prerequisiti per l'importazione del server

- Un file CSV con i nomi host o gli indirizzi IP del server e i nomi delle credenziali (facoltativo) associati ai nomi descrittivi delle credenziali del sistema operativo configurate o da configurare nello strumento di rilevamento. Il file CSV deve utilizzare le seguenti intestazioni:

```
hostname_or_ip,os_credential_name,oracle_credential_name
```

- I server devono essere raggiungibili dalla macchina virtuale dello strumento di rilevamento. Porte predefinite: porta SSH 22 per Linux, porta 5985/5986 WinRM per Windows. Sono supportate porte personalizzate.

Prerequisiti del programma di installazione Linux

- Una distribuzione Linux supportata: Amazon Linux 2, Amazon Linux 2023, RHEL 8—9, Rocky Linux 8—9, 9, Ubuntu 20.04—24.04, Debian AlmaLinux 10—12 o SLES 15 SP5.
- Almeno 4 vCPU, 16 GB di RAM, 35 GB di spazio disponibile su disco.
- La porta 5000 deve essere disponibile (non utilizzata da un altro servizio).
- systemd è necessario per la gestione del servizio.
- Lo strumento di rilevamento VM deve avere accesso di rete all'infrastruttura di destinazione. Porte predefinite: vCenter sulla porta 443, Hyper-V host sulla porta 5985/5986, server sulla porta 22. Le porte personalizzate sono supportate per SSH, WinRM e SNMP.

Prerequisiti del database Oracle

- Accesso alla rete dallo strumento di rilevamento agli host Oracle sulla porta 1521 (o porta personalizzata).
- Versioni Oracle supportate: è possibile raccogliere Oracle Database 12c Release 1 (12.1) e versioni successive tramite connessioni SQL dirette. OS-level il rilevamento dei fallback funziona con tutte le versioni di Oracle.
- Un account di servizio Oracle di sola lettura con concessione SELECT_CATALOG_ROLE. Per informazioni dettagliate, vedi [the section called “Database Oracle \(SQL\)”](#).
- Per il rilevamento di OS-level fallback: accesso SSH o WinRM all'host Oracle (utilizza le credenziali del sistema operativo esistenti).

Implementa su VMware

Specifiche delle macchine virtuali VMware

- Sistema operativo — Amazon Linux 2023
- RAM: 16 GB
- CPU: 4 core
- Dischi: 35 GB
- Requisiti VMware: consulta i requisiti degli [host VMware per l'esecuzione](#) di AL2023 su VMware

Implementa VMware OVA

1. Scarica il file OVA da questo URL: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.ova>
2. Accedi a vCenter come amministratore VMware.
3. Utilizza uno di questi metodi per installare il file OVA:
 - a. Usa l'interfaccia utente: scegli File, scegli Deploy OVF Template, seleziona il file OVA dello strumento di rilevamento scaricato nel passaggio 1, quindi completa la procedura guidata. Assicurati che le impostazioni del proxy nella dashboard di gestione del server siano configurate correttamente.
 - b. Usa la riga di comando: per installare il file OVA dello strumento di rilevamento dalla riga di comando, scarica e utilizza VMware Open Virtualization Format Tool (ovftool). [Per scaricare ovftool, seleziona una versione dalla pagina della documentazione dello strumento OVF.](#) Questo è un esempio di utilizzo dello strumento da riga di comando ovftool per installare il file OVA dello strumento di scoperta.

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

Descrizioni dei valori sostituibili nell'esempio:

- Il nome è il nome che si desidera utilizzare per la VM dello strumento di rilevamento.
 - Il datastore è il nome del datastore nel tuo vCenter.
 - Il nome del file OVA è il nome del file OVA dello strumento di scoperta scaricato.
 - Queste username/password sono le tue credenziali vCenter.
 - Il vcenterurl è l'URL del tuo vCenter.
 - Il percorso vi è il percorso verso l'host VMware ESXi.
4. Individua lo strumento di rilevamento distribuito nel tuo vCenter. Right-click la VM, quindi scegli Power, Power On.
 5. Dopo alcuni minuti, l'indirizzo IP dello strumento di rilevamento viene visualizzato in vCenter. Questo indirizzo IP viene utilizzato per connettersi allo strumento di rilevamento.

Implementa su Hyper-V

Hyper-V specifiche della macchina virtuale

- Sistema operativo — Amazon Linux 2023
- RAM: consigliamo di allocare almeno 16 GB
- CPU: consigliamo di allocare almeno 4 core
- Dischi: 35 GB (inclusi nel disco rigido virtuale)
- Hyper-V requisiti: consulta i [requisiti Hyper-V dell'host per l'esecuzione di AL2023 su Hyper-V](#)

Implementa il disco rigido virtuale Hyper-V

1. Scarica il file VHD da questo URL: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.vhd>
2. Copia il file VHD sul computer Windows Server con il Hyper-V ruolo abilitato.
3. Apri Hyper-V Manager.
4. Scegli Nuovo, quindi scegli Macchina virtuale.
5. Completa la procedura guidata di configurazione. Nella pagina Specificare la generazione, selezionare Generazione 1. Le macchine virtuali di seconda generazione non supportano il formato VHD. Nella pagina Assegna memoria, allocare almeno 16384 MB. Nella pagina Connect Virtual Hard Disk, scegli Usa un disco rigido virtuale esistente e seleziona il file VHD che hai copiato.
6. Avvia la VM. Dopo alcuni minuti, controlla la scheda Networking della VM in Hyper-V Manager per trovare l'indirizzo IP, oppure connettiti alla console VM ed esegui `ip addr`. Utilizzi questo indirizzo IP per connetterti allo strumento di rilevamento.

Implementa su Linux

Lo strumento di rilevamento è disponibile come programma di installazione Linux autonomo per la distribuzione su distribuzioni Linux supportate. Utilizza questa opzione quando desideri installare lo strumento di rilevamento direttamente su un server Linux esistente anziché distribuire una macchina virtuale.

Specifiche del server Linux

- RAM: si consiglia di allocare almeno 16 GB
- CPU: consigliamo di allocare almeno 4 core
- Dischi: 35 GB

Distribuzioni supportate

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

Installa lo strumento di scoperta

Scarica lo script di installazione da questo URL: <https://s3.us-east-1.amazonaws.com/atx.discovery.collector.bundle/releases/latest/AWS-Transform-discovery-tool.sh>

Per installare lo strumento di scoperta su Linux

1. Scarica lo script di installazione sul tuo server 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. (Facoltativo) Eseguite il controllo di compatibilità per verificare che il sistema soddisfi i requisiti.

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

3. Installa lo strumento di scoperta. Scegli una delle seguenti opzioni:

Opzione 1: installazione con installazione automatica delle dipendenze (consigliata)

Questa opzione installa automaticamente tutte le dipendenze di sistema mancanti prima di installare il servizio.

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

Opzione 2: installazione senza installazione automatica delle dipendenze

Questa opzione verifica le dipendenze mancanti e visualizza gli errori con le istruzioni di installazione manuale se mancano dipendenze critiche. Utilizzate questa opzione se l'organizzazione limita l'installazione automatica dei pacchetti e preferite gestire i pacchetti di sistema manualmente.

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

4. Avvia il servizio Discovery Tool.

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

5. Accedi allo strumento di scoperta all'indirizzo `https://ip_address:5000`.

Per disinstallare lo strumento di rilevamento, esegui `sudo ./AWS-Transform-discovery-tool.sh uninstall`.

Puoi anche utilizzare i seguenti comandi per gestire il servizio:

- `sudo ./AWS-Transform-discovery-tool.sh status`— Verificare se il servizio è in esecuzione.
- `sudo ./AWS-Transform-discovery-tool.sh stop`— Interrompere il servizio.
- `sudo ./AWS-Transform-discovery-tool.sh logs`— Visualizza i registri di servizio.

Dipendenze del sistema

L'installatore verifica le seguenti dipendenze di sistema:

Dipendenza	Gravità	Scopo
OpenSSL	Critica	Genera la chiave di crittografia del database
libcrypt	Critica	Richiesto dal runtime Python

Dipendenza	Gravità	Scopo
Librerie Kerberos	Attenzione	Richiesto per l'autenticazione Kerberos sui server Windows. In caso contrario, NTLM e l'autenticazione di base continuano a funzionare.

Per l'avvio dello strumento di rilevamento sono necessarie dipendenze critiche. Se mancano e hai scelto l'opzione 2 (senza `--install-deps`), il programma di installazione visualizza un errore con le istruzioni per installarle manualmente. Warning-level le dipendenze sono opzionali: il programma di installazione avvisa l'utente ma procede con l'installazione.

Note

L'installatore verifica la compatibilità del sistema, inclusa la versione di glibc e la disponibilità di systemd. Su sistemi con systemd 250 o versioni successive (Amazon Linux 2023, RHEL 9, Rocky 9, 9, Ubuntu 24.04+, AlmaLinux Debian 12+), la chiave di crittografia del database viene crittografata a riposo utilizzando systemd-creds. Nei sistemi precedenti, la chiave di crittografia viene archiviata come file protetto da autorizzazioni.

Configura lo strumento di rilevamento

Accedi alla console dello strumento di rilevamento

1. In un browser Web, accedi a: `https://ip_address:5000`, *ip_address* dov'è l'indirizzo IP dello strumento di rilevamento di Deploy Discovery Tool. Lo strumento di rilevamento utilizza un certificato autofirmato per la connessione HTTPS che genera un avviso di sicurezza. Scegli Accetta il rischio e continua a passare alla console dello strumento di rilevamento.
2. Se accedi alla console del Discovery Tool per la prima volta, crea una password di accesso allo strumento di rilevamento. Crea una password, che utilizzerai per gli accessi futuri.

Important

Ricorda questa password: non esiste un meccanismo di recupero della password.

Accesso allo strumento di scoperta VM

- Lo strumento di rilevamento VM viene fornito di default con un nome utente e una password («discovery», «password»). Per una maggiore sicurezza, si consiglia di aggiornare la password utilizzando `sudo passwd discovery` dopo aver effettuato l'accesso alla macchina virtuale tramite la console dell'hypervisor (ad esempio, vSphere Client for VMware o Manager for). Hyper-V Hyper-V
- L'accesso SSH è disabilitato per impostazione predefinita. Gli utenti possono utilizzare alias preconfigurati `enablessh` e `disablessh` per l'accesso enable/disable SSH alla macchina virtuale dello strumento di rilevamento. Gli utenti possono accedere tramite SSH alla macchina virtuale dopo aver abilitato l'accesso SSH. `ssh discovery@<VM-IP>` Gli utenti sono incoraggiati a mantenere l'accesso SSH disabilitato la maggior parte delle volte e ad abilitarlo solo quando richiesto attivamente. La modifica della password viene applicata durante l'esecuzione. `enablessh`
- Per accedere alla directory dei dati dello strumento di rilevamento all'indirizzo `/home/ec2-user/.local/share/DiscoveryTool`, consigliamo di passare a `ec2-user` `sudo su ec2-user` eseguendo.

Configurazione dell'autenticazione Kerberos

L'autenticazione Kerberos è il metodo consigliato per la connessione ai server Windows dallo strumento di rilevamento. Lo strumento di rilevamento VM utilizza le librerie Kerberos native di Amazon Linux 2023 per l'autenticazione sul tuo dominio Active Directory.

Di seguito sono riportati i punti chiave dell'autenticazione Kerberos sulla VM dello strumento di rilevamento:

- Usa il `kinit` comando per ottenere un ticket Kerberos e `klist` per verificarlo.
- Il file di configurazione Kerberos si trova in `/etc/krb5.conf`
- Prima di configurare lo strumento di rilevamento, verifica che abbia `kinit` esito positivo dalla CLI sulla VM dello strumento di rilevamento.

Prerequisiti Kerberos

Prima di configurare l'autenticazione Kerberos, verificate di disporre delle seguenti informazioni e della connettività di rete.

1. Richiedete le seguenti informazioni all'amministratore di Active Directory:

- Il nome dell'area di autenticazione Kerberos (in genere il nome di dominio in lettere maiuscole, ad esempio). `EXAMPLE.COM`
- Il nome host o l'indirizzo IP del Key Distribution Center (KDC), che in genere è un controller di dominio (ad esempio,). `dc01.example.com`
- Un account di servizio con autorizzazioni per l'autenticazione sui server Windows di destinazione.

2. Verifica che lo strumento di rilevamento VM disponga di connettività di rete a quanto segue:

- Il KDC sulla porta 88 (TCP e UDP) per l'autenticazione Kerberos.
- I server Windows di destinazione sulle porte WinRM (5985 per HTTP, 5986 per HTTPS).

Configurazione di Kerberos

Completa i seguenti passaggi per configurare l'autenticazione Kerberos sulla macchina virtuale dello strumento di rilevamento.

1. SSH verso la macchina virtuale dello strumento di rilevamento.

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

2. Modifica il file di configurazione Kerberos in. `/etc/krb5.conf`

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

Aggiungete la seguente configurazione, sostituendo i valori segnaposto con i dettagli dell'ambiente.

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

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

[domain_realm]
```

```
.example.com = EXAMPLE.COM  
example.com = EXAMPLE.COM
```

Important

Kerberos fa distinzione tra maiuscole e minuscole. Il nome dell'area deve essere in maiuscolo (ad esempio, no). `EXAMPLE.COM` `example.com` Il nome di dominio nella `[domain_realm]` sezione deve essere in lettere minuscole.

Più domini Active Directory

Lo strumento di rilevamento supporta più credenziali Kerberos per diversi domini Active Directory. Ogni credenziale si autentica in modo indipendente, quindi è possibile configurare più credenziali normalmente e l'isolamento è automatico.

Se disponi di server in più domini, aggiungi voci per ogni area del file: `/etc/krb5.conf`

```
[libdefaults]  
    default_realm = DEV.COMPANY.COM  
    dns_lookup_realm = false  
    dns_lookup_kdc = true  
  
[realms]  
    DEV.COMPANY.COM = {  
        kdc = dc01.dev.company.com  
    }  
    PROD.COMPANY.COM = {  
        kdc = dc01.prod.company.com  
    }  
  
[domain_realm]  
    .dev.company.com = DEV.COMPANY.COM  
    dev.company.com = DEV.COMPANY.COM  
    .prod.company.com = PROD.COMPANY.COM  
    prod.company.com = PROD.COMPANY.COM
```

3. Verifica di poter ottenere un ticket Kerberos eseguendo il comando. `kinit`

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

Inserisci la password quando richiesto. Se il comando viene completato senza errori, l'autenticazione è riuscita.

4. Verifica il ticket eseguendo il `klist` comando.

```
klist
```

L'output previsto è simile al seguente.

```
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. Configura lo strumento di rilevamento con lo stesso principio con distinzione tra maiuscole e minuscole utilizzato con `kinit` (ad esempio, `username@REALM.COM`).

Una `krb5.conf` configurazione esplicita potrebbe non essere necessaria se l'ambiente ha record DNS SRV configurati per il rilevamento del servizio Kerberos. [Per ulteriori informazioni sulle opzioni di configurazione Kerberos, consultate la documentazione di MIT Kerberos `krb5.conf` e il file di esempio `krb5.conf`.](#)

Trova la configurazione Kerberos dai computer aggiunti al dominio

Se non disponi dei dettagli di configurazione Kerberos, puoi recuperarli da un computer Windows che fa parte del dominio. Esegui i seguenti comandi da un prompt dei comandi sul computer aggiunto al dominio.

Per trovare il nome di dominio, esegui il comando seguente.

```
echo %USERDNSDOMAIN%
```

Output di esempio:

```
EXAMPLE.COM
```

Per trovare il nome host del controller di dominio, esegui il comando seguente.

```
nlttest /dsgetdc:EXAMPLE.COM
```

Output di esempio:

```
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
```

Associa l'output alla tua `krb5.conf` configurazione come segue:

- Realm: utilizza il valore da `%USERDNSDOMAIN%` in maiuscolo (ad esempio,). `EXAMPLE.COM`
- KDC: utilizza il nome host DC dell'`nlttest` output (ad esempio,). `dc01.example.com`

Configurazione dell'accesso vCenter

1. Nella pagina dello strumento Discovery, al passaggio 1. Configura le fonti di rilevamento, scegli Configura sorgenti.
2. Nella pagina Configura sorgenti di rilevamento, fornire il nome descrittivo, vCenter FQDN/IP, il nome utente e la password.
3. Seleziona Save configuration (Salva configurazione).

Lo strumento di rilevamento inizia a raccogliere informazioni su vCenter, come descritto in [Discovered](#) Inventory.

Dopo la configurazione iniziale, scegli Modifica accesso vCenter nel riquadro di stato dello strumento Discovery per modificare le impostazioni di accesso a vCenter.

Lo strumento di rilevamento raccoglie dati da tutti i server vCenter configurati in parallelo. Se un server vCenter non è raggiungibile durante la raccolta, lo strumento segnala un successo parziale e continua la raccolta dai server vCenter rimanenti.

Se una VM viene visualizzata su più server vCenter (ad esempio, a causa di host ESXi condivisi o Cross-vCenter vMotion), lo strumento di rilevamento deduplica automaticamente le VM. Ogni VM unica appare solo una volta nell'inventario.

Configura l'accesso Hyper-V

1. Nella pagina dello strumento Discovery, al passaggio 1. Configura le fonti di rilevamento, scegli Configura sorgenti.
2. Nella pagina Configura fonti di rilevamento, fornire un nome descrittivo, l'FQDN o l'indirizzo IP dell'host, il tipo di autenticazione (NTLM o Kerberos), il nome utente WinRM e la password WinRM.
3. Seleziona Save configuration (Salva configurazione).

[Lo strumento di rilevamento inizia a raccogliere informazioni, come descritto in Inventario scoperto. Hyper-V](#)

La raccolta inizia automaticamente dopo il salvataggio delle credenziali.

Per i cluster Hyper-V di failover, è possibile aggiungere più host nello stesso cluster. Lo strumento deduplica automaticamente le macchine virtuali che appaiono su più di un host.

Server di importazione

1. Vai alla pagina Importa server dalla home page dello strumento Discovery.
2. Prepara un file CSV con le seguenti colonne: `hostname_or_ip` (obbligatorio), `os_credential_name` (opzionale) e `oracle_credential_name` (opzionale).
 - Il `hostname_or_ip` valore deve essere un indirizzo IPv4 valido o un nome di dominio completo (FQDN).
 - Il `os_credential_name` valore, se fornito, deve corrispondere al nome descrittivo di una credenziale del sistema operativo già configurata (SSH, WinRM o SNMP). Lascia vuoto per i server in cui non hai ancora configurato una credenziale del sistema operativo.
 - Il `oracle_credential_name` valore, se fornito, deve corrispondere al nome descrittivo di una credenziale Oracle già configurata.
3. Carica il file CSV. Lo strumento convalida tutte le righe e rifiuta il file se una riga non è valida.

Dopo una corretta importazione, lo strumento avvia automaticamente la raccolta delle metriche del database, della rete e del sistema operativo per i server importati, se le credenziali del sistema operativo sono configurate. Se carichi un altro file CSV, i record esistenti vengono aggiornati senza creare duplicati e i nuovi record vengono uniti all'inventario.

Importa un'autorità di certificazione autofirmata nello strumento di individuazione (opzionale)

Ciò è necessario quando si utilizza WinRM su HTTPS e i server di destinazione utilizzano certificati HTTPS WinRM firmati da un'autorità di certificazione (CA) autofirmata e si desidera abilitare «Convalida certificato SSL del server» sullo strumento di rilevamento.

Prerequisiti

1. Self-signed Certificato CA utilizzato per firmare i certificati HTTPS WinRM sui server di destinazione
2. Certificato in formato PEM (estensione.pem o.crt)

Per importare un'autorità di certificazione autofirmata sulla VM dello strumento di rilevamento:

1. Da Ssh a Discovery Tool VM
2. Inserisci i certificati CA che hanno firmato i certificati WinRM dei server di destinazione nella directory `/etc/pki/ca-trust/source/anchors/` del trust store sulla VM dello strumento di rilevamento. Ad esempio: `sudo cp winrm-ca.pem /etc/pki/ca-trust/source/anchors/winrm-ca.pem`. Nota: se i server di destinazione utilizzano certificati firmati da CA diverse, copia tutti i certificati CA pertinenti in questa directory.
3. Aggiorna il Certificate Trust Store: `sudo update-ca-trust`
4. Riavviare la macchina virtuale
5. (Facoltativo) Per verificare che i certificati siano stati importati correttamente, è possibile eseguire il seguente comando. `sudo trust list --filter=ca-anchors | grep -A 5 "<certificate_name>"`

Vedi [Installazione e configurazione per Gestione remota Windows](#)

Configura lo strumento di rilevamento per l'accesso al sistema operativo

Configura l'accesso al sistema operativo in modo che lo strumento di rilevamento possa:

- Scopri i database per eseguire la valutazione dei database e fornire assistenza nella migrazione delle macchine virtuali,
- Tieni traccia delle connessioni di rete tra i server del tuo inventario, incluso il processo associato a ciascuna connessione, per facilitare la mappatura delle dipendenze delle applicazioni e la pianificazione delle ondate. Sono incluse solo le connessioni in cui entrambi gli endpoint sono presenti nell'inventario dello strumento di rilevamento.

Abilita lo strumento di rilevamento OS Access

1. Vai alla pagina di configurazione dell'accesso al sistema operativo per fornire le credenziali Windows e Linux.
2. Scegliete un protocollo per il quale desiderate aggiungere le credenziali.
3. Fornisci le credenziali richieste per il protocollo selezionato.
4. Selezionare questa opzione Auto-connect per consentire allo strumento di rilevamento di provare tutte le credenziali fornite sui server rilevati fino a trovare le credenziali corrispondenti per ogni server.

Consulta [the section called “Usare Auto-Connect la funzionalità con cautela”](#) importanti consigli di sicurezza relativi alla funzionalità di connessione automatica.

5. Scegli Configura e connettiti.

Una volta completato il processo di abbinamento del sistema operativo, viene visualizzato un messaggio che indica che la raccolta dei dati è in corso e un errore relativo ai server per i quali non è stata trovata una corrispondenza tra le credenziali.

Configurazione dei protocolli supportati

È necessario configurare i protocolli WinRM, SSH e SNMP sui server di destinazione affinché lo strumento di rilevamento possa comunicare con essi.

Configurare WinRM e WMI

WinRM viene installato automaticamente con tutte le versioni attualmente supportate del sistema operativo Windows.

Per verificare o modificare la configurazione di WinRM, utilizzare `winrm` lo strumento da riga di comando:

- Verifica i listener WinRM installati: `winrm enumerate winrm/config/listener`
- Verifica le configurazioni WinRM: `winrm get winrm/config`
- Comando di esempio per configurare WinRM: `winrm quickconfig -transport:https`

Porte per listener

La porta HTTP predefinita è 5985; HTTPS è 5986. È possibile utilizzare altre porte in base alle esigenze. Le porte devono essere aperte tra lo strumento di rilevamento e i server di destinazione.

Encryption (Crittografia)

Lo strumento di rilevamento utilizza la comunicazione WinRM crittografata. Si consiglia che anche i listener WinRM sui server di destinazione utilizzino la crittografia: `winrm set winrm/config/service '@{AllowUnencrypted="false"}'`

NTLM e Kerberos

I protocolli di autenticazione WinRM Kerberos e NTLM sono supportati dallo strumento di rilevamento. NTLM può essere utilizzato solo con HTTPS e Kerberos può essere utilizzato sia con HTTP che HTTPS.

Requisiti WMI

Lo strumento di rilevamento interroga i seguenti namespace WMI. L'account WinRM richiede l'accesso in lettura a ogni spazio dei nomi relativo ai moduli di raccolta:

Spazio dei nomi WMI	Utilizzato da
<code>root\cimv2</code>	Metriche del sistema operativo, metadati dell' Hyper-V host, raccolta SQL Server
<code>root\virtualization\v2</code>	Hyper-V Inventario delle macchine virtuali
<code>root\StandardCIMV2</code>	Raccolta di rete
<code>root\Microsoft\SqlServer\ComputerManagement*</code>	Raccolta SQL Server
<code>root\Microsoft\SqlServer\ReportServer*</code>	Raccolta SQL Server (SSRS)

Per la raccolta in rete, assicurati che siano soddisfatte le seguenti condizioni:

- Consenti la connettività di rete tramite ICMP
- Consenti la connettività di rete tramite la porta TCP 135 + intervallo temporaneo di porte TCP (49152 - 65535)
- Disabilita UAC
- Le autorizzazioni DCOM remote sono configurate
- Crea un account di servizio dedicato con autorizzazioni minime richieste
- Le autorizzazioni per lo spazio dei nomi WMI sono configurate per gli account Windows con namespace:, class \\root\\standardcimv2 MSFT_NetTCPConnection

Per la raccolta di SQL Server, è necessario un account Windows (locale o di dominio) appartenente al gruppo di amministratori locali a causa dei complessi requisiti di autorizzazione degli oggetti WMI.

Configurazione di SSH

- La porta predefinita è 22. Sono supportate porte personalizzate. La porta configurata deve essere aperta tra lo strumento di rilevamento e i server di destinazione.
- Affinché la raccolta di reti SSH funzioni correttamente, fornisci un utente configurato per sudo senza password.
- Assicurati che i seguenti comandi siano disponibili sui server Linux di destinazione (installati per impostazione predefinita sulla maggior parte delle distribuzioni): ss o netstat per la raccolta in rete e,lsblk, iostat dmidecode smartctl top ps freeip, e df per la raccolta delle metriche del sistema operativo.

Lo strumento di scoperta supporta due metodi di autenticazione per SSH:

Opzione 1: nome utente e password

Fornisci il nome utente e la password SSH. Questo è il metodo di autenticazione predefinito.

Opzione 2: chiave privata SSH

Fornisci il nome utente SSH e una chiave privata in formato PEM. Per utilizzare questa opzione, scegli Chiave SSH dal menu a discesa Tipo di autenticazione durante la configurazione delle credenziali SSH. Se la chiave privata è crittografata con una passphrase, inserisci la passphrase nel campo opzionale Key Passphrase.

Sono supportati i seguenti formati chiave:

- RSA
- ECDSA
- Ed25519
- Formato OpenSSH
- Formato PKCS #8

Entrambi i metodi di autenticazione supportano la connessione automatica. Le credenziali vengono archiviate crittografate quando sono inutilizzate.

Configurare SNMP

- La porta predefinita è 161/UDP. Le porte personalizzate sono supportate. La porta configurata deve essere aperta tra lo strumento di rilevamento e i server di destinazione.
- Per SNMP v2: fornite una stringa di community di sola lettura in grado di accedere agli OID di connessione TCP.
- Per SNMP v3: fornisci auth/privacy dettagli con l'autorizzazione di sola lettura per accedere agli username/password OID di connessione TCP

Lo strumento di scoperta richiede l'accesso a:

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

Configurare l'accesso al database Oracle

Configura l'accesso al database Oracle per raccogliere i metadati dettagliati del database Oracle direttamente tramite connessioni SQL. I metadati raccolti includono la topologia CDB e PDB, l'utilizzo delle funzionalità e le opzioni installate. Questi dati consentono di pianificare le migrazioni dei database Oracle in modo più accurato. È possibile raccogliere Oracle Database 12c Release 1 (12.1) e versioni successive tramite connessioni SQL dirette. OS-level il rilevamento dei fallback funziona con tutte le versioni di Oracle.

Configura le credenziali Oracle nello strumento di rilevamento

1. Nella pagina dello strumento Discovery, nella barra laterale, scegli Accesso al database.
2. Scegli Aggiungi credenziali Oracle.
3. Inserisci le informazioni che seguono:
 - Nome descrittivo: un nome descrittivo per questa credenziale (ad esempio,). `Oracle Production`
 - Porta: la porta del listener Oracle (impostazione predefinita 1521).
 - Nome del servizio: il nome del servizio Oracle per il database di destinazione.
 - Nome utente: il nome utente dell'account del servizio Oracle.
 - Password: la password dell'account del servizio Oracle.
 - Auto-connect— Attiva questa opzione per provare la credenziale su tutti i server del tuo inventario. Disattiva questa opzione per assegnare manualmente le credenziali a server specifici.
4. Per aggiungere altre credenziali (ad esempio, per diversi ambienti Oracle), scegli nuovamente Aggiungi credenziali Oracle.
5. Scegli Save (Salva).

Modalità di credenziali

Quando configuri le credenziali Oracle, puoi scegliere tra due modalità:

- Manuale: aggiungi una credenziale a un server specifico. Lo strumento di scoperta utilizza tale credenziale esclusivamente per quel server. Se la connessione fallisce, non si verifica alcun fallback. Correggi la configurazione delle credenziali per risolvere il problema.
- Auto-connect— Lo strumento di rilevamento prova ogni credenziale di connessione automatica su ogni server dell'inventario. Quando una credenziale ha esito positivo per un server, lo strumento di rilevamento utilizza tale credenziale per tutti i cicli di raccolta successivi.

Flusso di rilevamento

Quando si configurano le credenziali Oracle, lo strumento di rilevamento tenta innanzitutto una connessione SQL diretta. Se tutte le credenziali del database falliscono, lo strumento torna al OS-level rilevamento tramite SSH o WinRM, così puoi comunque scoprire le installazioni Oracle senza accedere al database.

Aggiornamento dello strumento di rilevamento

Lo strumento di rilevamento non dispone di una funzionalità di aggiornamento automatico, tuttavia riceverai una notifica di promemoria dopo 30 giorni dall'installazione per l'aggiornamento. Si consiglia di mantenere l'applicazione aggiornata per ricevere le funzionalità e le patch di sicurezza più recenti.

Per aggiornare manualmente lo strumento

1. Scarica il file di immagine più recente dello strumento di rilevamento (OVA per VMware o VHD per Hyper-V) dal link fornito.
2. (Facoltativo) Si consiglia di eliminare il precedente file di immagine dello strumento di rilevamento prima di distribuire quello più recente.
3. Segui i passaggi indicati nella sezione Implementa lo strumento di rilevamento per distribuire la versione aggiornata.

Revoca dell'accesso

È possibile revocare l'accesso a ciascuna fonte di rilevamento in modo indipendente. Quando si revoca l'accesso a una fonte, i dati provenienti da altre fonti non ne risentono.

- Revoca dell'accesso a vCenter: elimina le credenziali e i dati vCenter. VMware-collected Non elimina Hyper-V dati, dati del server importati o credenziali del sistema operativo.
- Revoca dell' Hyper-V accesso: elimina solo le Hyper-V credenziali e i dati. Hyper-V-collected
- Eliminazione dei server importati: rimuove i server importati dall'inventario. I dati di raccolta a valle (rete, database) raccolti da tali server vengono conservati.

Autorizzazioni richieste per lo strumento di rilevamento

Lo strumento di rilevamento si connette all'infrastruttura utilizzando diversi protocolli. Ogni protocollo e modulo di raccolta richiede autorizzazioni specifiche per l'account. Questa sezione descrive le autorizzazioni minime necessarie per completare la raccolta dei dati e quali dati si perdono se determinate autorizzazioni non sono disponibili.

VMware vCenter

Lo strumento di rilevamento si connette a VMware vCenter Server sulla porta 443 (HTTPS) ed esegue operazioni di sola lettura. Non viene apportata alcuna modifica all'ambiente vCenter.

Ruolo minimo richiesto: Read-Only, assegnato a livello root di vCenter.

Il Read-Only ruolo fornisce tutto l'accesso necessario allo strumento di rilevamento per raccogliere l'inventario delle macchine virtuali (nome, UUID, CPU, memoria, disco, rete, stato di alimentazione, sistema operativo guest) e le metriche delle prestazioni (utilizzo della CPU, utilizzo della memoria, IOPS del disco e velocità effettiva).

Raccomandazione: creare un utente vCenter dedicato con il Read-Only ruolo integrato a livello di datacenter principale.

Hyper-V host (Windows)

Lo strumento di rilevamento si connette agli Hyper-V host tramite WinRM (porta 5985 per HTTP, porta 5986 per HTTPS) ed PowerShell esegue comandi per raccogliere l'inventario delle macchine virtuali, i metadati degli host e le prestazioni di archiviazione.

Appartenenze minime di gruppo richieste su ogni host: Hyper-V

Gruppo Windows	Perché è necessario
Utenti con gestione remota	Accesso remoto WinRM di base
Hyper-V Amministratori	Raccolta dell'inventario delle macchine virtuali (elenco delle macchine virtuali, disco, rete, memoria, sistema operativo ospite)
Utenti di Performance Monitor	Contatori I/O delle prestazioni di storage (read/write IOPS e throughput per VM)

L'account richiede inoltre l'accesso in lettura WMI allo `root\cimv2` spazio dei nomi per la versione del sistema operativo host e l'UUID hardware. Questo accesso è concesso per impostazione predefinita agli amministratori locali, ma deve essere configurato in modo esplicito per gli account non amministratori.

Raccomandazione: creare un account di servizio di dominio dedicato e aggiungerlo ai gruppi Remote Management Users, Hyper-V Administrators e Performance Monitor Users su ciascun host. Hyper-V Evitare di utilizzare account di amministratore di dominio.

Server Linux (SSH)

Lo strumento di rilevamento si connette ai server Linux tramite SSH (porta 22) per raccogliere metriche del sistema operativo, connessioni di rete e inventario dei server. La maggior parte della raccolta di dati viene eseguita come utente normale. Se sudo non è disponibile, un numero limitato di comandi tenta di eseguire un tentativo sudo e lo ritira automaticamente.

Accesso minimo richiesto: un account utente SSH in grado di accedere al server di destinazione.

Accesso consigliato: lo stesso utente SSH configurato con sudo senza password per la raccolta completa dei dati.

Cosa richiede sudo e cosa succede senza di esso:

Dati raccolti	Sudo era necessario?	Cosa perdi senza sudo
Nome del server, sistema operativo, CPU, memoria, IP, numero di dischi	No	Niente, raccolto come utente normale
Utilizzo della CPU, della memoria e della rete	No	Niente, raccolto come utente normale
IOPS, velocità effettiva e spazio su disco	No	Niente, raccolto come utente normale
Configurazione dell'interfaccia di rete	No	Niente, raccolto come utente normale
Processi in esecuzione (nome, PID, comando)	No	Niente: raccolti come utente normale
UUID del server e UUID SMBIOS	Sì	I campi UUID sono vuoti nell'esportazione
Produttore di hardware (rilevamento fisico o virtuale)	Sì	Il rilevamento del tipo di risorsa è meno accurato nelle distribuzioni precedenti

Dati raccolti	Sudo era necessario?	Cosa perdi senza sudo
Rilevamento logico del volume LVM	Sì	Volumi LVM non rilevati; il tipo di volume può essere visualizzato come «Sconosciuto»
Connessioni di rete con nome del processo e PID	Sì	Le connessioni vengono ancora raccolte, ma senza l'attribuzione del processo (le colonne PID e nome del processo sono vuote)
OS-level Rilevamento del database Oracle (fallback quando le credenziali Oracle non sono configurate)	Sì	Il rilevamento di presenza Oracle di base (oratab, process monitor) funziona senza sudo. La raccolta dettagliata (opatch, lsnrctl, ASM, Grid Infrastructure) richiede l'accesso senza password ai file binari di Oracle Home. <code>sudo -u oracle</code>

Note

Lo strumento di scoperta non fallisce mai completamente a causa della mancanza di sudo. Raccoglie ciò che può e riporta risultati parziali. Tuttavia, per i dati più completi, in particolare la mappatura delle dipendenze della rete con i nomi dei processi, consigliamo sudo senza password.

Utilità necessarie sui server di destinazione: dovrebbero essere disponibili i seguenti comandi (installati per impostazione predefinita sulla maggior parte delle distribuzioni Linux): `ss`, `netstat`, `lsof`, `lsblk`, `top`, `ps`, `free`, `ip` e `df`. `hostname`, `cat`, `nproc`, `grep`. Facoltativo per dati aggiuntivi: `iostat` (I/O dettaglio del disco), `dmidecode` (UUID hardware), (tipo di interfaccia disco), `smartctl` (rilevamento LVM), `lvs` (display).

Server Windows (WinRM) — metriche del sistema operativo

Lo strumento di rilevamento si connette ai server Windows tramite WinRM per raccogliere i parametri del sistema operativo (inventario dei server, prestazioni, archiviazione, interfacce di rete e processi in esecuzione).

Accesso minimo richiesto: un account WinRM-enabled utente con accesso remoto al server di destinazione.

Accesso consigliato: un utente del gruppo Administrators locale per la raccolta completa dei dati.

Livello di autorizzazione	Cosa consente	Cosa si perde senza di essa
Utenti con gestione remota (accesso WinRM)	Raccolta di tutti i dati di Windows	Nessun dato raccolto dal server
Accesso in lettura WMI a root\cimv2	Nome del server, versione del sistema operativo, memoria, UUID, seriale BIOS, spazio su disco	I campi dell'inventario del server sono vuoti
Utenti di Performance Monitor	Utilizzo della CPU, velocità effettiva di rete, IOPS e velocità effettiva del disco	Metriche delle prestazioni non raccolte
Amministratore locale	Nomi dei proprietari dei processi in esecuzione	Elenco dei processi raccolto ma la user/owner colonna è vuota

Note

L'iscrizione a Local Administrator concede implicitamente l'accesso agli utenti di Performance Monitor e l'accesso in lettura a WMI, quindi soddisfa tutti i requisiti di cui sopra.

Note

Il rilevamento dei OS-level fallback di Oracle Database su Windows utilizza le query e i Get-Process comandi del registro quando le credenziali Oracle non sono Get-Service configurate. Questi comandi richiedono solo l'accesso degli utenti di gestione remota standard. Non sono necessarie autorizzazioni aggiuntive oltre ai requisiti delle metriche del sistema operativo.

Server Windows (WinRM): raccolta SQL Server

La raccolta SQL Server rileva le istanze di SQL Server, Reporting Services (SSRS) e Integration Services (SSIS) sui server Windows.

Accesso consigliato: un utente del gruppo Administrators locale su ogni server Windows di destinazione.

L'amministratore locale è consigliato perché SQL Server Discovery esegue query su più namespace WMI e richiede un accesso elevato per alcune operazioni:

Cosa viene scoperto	Autorizzazione necessaria	Cosa si perde senza di essa
Istanze di SQL Server Database Engine (versione, edizione, stato)	Accesso in lettura WMI ai namespace <code>root\Microsoft\SqlServer\ComputerManagement*</code>	Istanze di SQL Server non rilevate
SQL Server Reporting Services (SSRS)	Accesso in lettura WMI ai namespace <code>root\Microsoft\SqlServer\ReportServer</code>	Componenti SSRS non rilevati
Configurazione dell'URL e della porta SSRS	Privilegi elevati (amministratore locale)	Mancano i dettagli della prenotazione dell'URL SSRS
SQL Server Integration Services (SSIS)	Accesso alla lettura del registro (HKLM)	Versione ed edizione SSIS mancanti
Port-to-service associazione	Accesso all'enumerazione dei listener TCP	Impossibile associare le porte di ascolto ai servizi SQL Server

Note

La raccolta SQL Server è Windows-only. Lo strumento di rilevamento ignora i server Linux per l'individuazione di SQL Server.

Database Oracle (SQL)

Oracle Database collection si connette direttamente alle istanze Oracle sulla porta 1521 (o su una porta personalizzata) per raccogliere i metadati del database. Lo strumento di rilevamento non richiede privilegi DBA o SYSDBA.

Accesso minimo richiesto: un account di servizio Oracle di sola lettura con la concessione `SELECT_CATALOG_ROLE`.

Lo strumento di rilevamento non accede alle visualizzazioni di Diagnostics Pack o Tuning Pack, quindi non è richiesta alcuna licenza Oracle aggiuntiva per la raccolta dei dati.

SQL per creare l'account:

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

OS-level fallback: se le credenziali del database non sono configurate o la connessione fallisce, lo strumento di rilevamento utilizza le credenziali del sistema operativo SSH o WinRM esistenti per rilevare le installazioni Oracle. Non sono necessarie autorizzazioni del Oracle-specific sistema operativo aggiuntive oltre a quelle richieste dal modulo di metrica del sistema operativo.

Raccolta di rete

La raccolta in rete utilizza protocolli diversi a seconda del sistema operativo del server:

Sistema operativo del server	Protocollo	Autorizzazioni necessarie
Linux	SSH	Utente normale per i dati di connessione. Sudo senza password consigliato per i dettagli a livello di processo (PID e nome del processo).
Linux	SNMPv2	Una stringa di community di sola lettura con accesso a TCP MIB (tcpConnState, tcp) e Host Resources MIB (hrConnectionProcess). SWRunName

Sistema operativo del server	Protocollo	Autorizzazioni necessarie
Linux	SNMPv3	Un utente USM con accesso in lettura agli stessi MIB di SNMPv2. Supporta i livelli di sicurezza noAuthNoPriv, auth e authPrivNoPriv.
Windows	WinRM	Accesso in lettura WMI allo <code>root\StandardCIMV2</code> spazio dei nomi (classe <code>MSFT_NetTCPConnection</code>).

Riferimento rapido: autorizzazioni minime per caso d'uso

Caso d'uso	Tipo di account	Autorizzazioni minime
Individuazione di VM VMware	Utente vCenter	Read-Only ruolo a livello di datacenter principale
Hyper-V individuazione di macchine virtuali	Dominio Windows o account locale	Utenti di gestione remota + Hyper-V amministratori + utenti di Performance Monitor su ogni host
Metriche del sistema operativo Linux: dati completi	Utente SSH	sudo senza password
Metriche del sistema operativo Linux: dati parziali	Utente SSH	Utente normale (no sudo). Mancano le informazioni su UUID, produttore, LVM e processo di rete.
Metriche del sistema operativo Windows: dati completi	Utente WinRM	Amministratore locale
Metriche del sistema operativo Windows: dati di base	Utente WinRM	Utenti di gestione remota + accesso in lettura WMI a <code>root\cimv2</code>

Caso d'uso	Tipo di account	Autorizzazioni minime
Individuazione del database SQL Server	Utente WinRM	Amministratore locale
Individuazione del database Oracle (SQL)	Account di servizio Oracle	SELECT_CATALOG_ROLE (sola lettura, senza DBA o SYSDBA)
Raccolta di rete: Linux (SSH)	Utente SSH	sudo senza password per dati a livello di processo; utente normale solo per i dati di connessione
Raccolta in rete: Linux (SNMP)	Stringa di comunità SNMP o utente USM	Accesso in lettura ai MIB TCP e Host Resources
Raccolta di rete — Windows	Utente WinRM	Accesso in lettura WMI a root\StandardCIMV2

Raccolta dei dati

Programma di raccolta degli strumenti Discovery

Dopo la raccolta di rilevamento iniziale, lo strumento di scoperta continua a funzionare secondo una pianificazione scaglionata per evitare un conflitto di risorse:

- VMware Discovery: ogni ora (alle :00 UTC)
- Hyper-V discovery: ogni ora (alle 20 UTC)

Lo strumento di scoperta raccoglie anche le metriche del sistema operativo attraverso i seguenti moduli indipendenti, ciascuno con una propria pianificazione scaglionata:

- Metriche di rete: ogni 15 secondi, potrebbero essere meno frequenti per ambienti di grandi dimensioni
- Metriche delle prestazioni del server: ogni 10 minuti (alle :03, :13, :23, :33, :43, :53 UTC)
- Metriche delle prestazioni di archiviazione: ogni 10 minuti (alle :07, :17, :27, :37, :47, :57 UTC)
- Processi in esecuzione: ogni ora (alle :40 UTC)

- Dati di provisioning del server: giornalieri (alle 00:05 UTC)
- Dati relativi al provisioning dello storage: tutti i giorni (alle 00:35 UTC)
- Interfacce di rete: tutti i giorni (alle 01:05 UTC)
- Rilevamento di SQL Server: tutti i giorni (alle 03:05 UTC)
- Individuazione del database Oracle: ogni giorno (alle 05:05 UTC)

Puoi avviare, arrestare o attivare in modo indipendente ogni modulo di metrica del sistema operativo utilizzando **Collect data now**.

Per eseguire manualmente una raccolta, dal menu **Azioni** scegli:

- **Start**: abilita il modulo di rilevamento.
- **Stop**: disattiva il modulo di rilevamento.
- **Raccogli subito i dati**: avvia immediatamente il rilevamento. Utilizzate questa opzione, ad esempio, dopo aver apportato una modifica alla rete.

Queste azioni si applicano a ogni modulo. È possibile controllare i moduli di metrica del sistema operativo singolarmente.

Tentativi di raccolta dati del sistema operativo

Quando viene scoperto un nuovo server, lo strumento di rilevamento tenta ogni credenziale configurata per ogni indirizzo IP e nome host. Dopo che lo strumento di rilevamento ha trovato una credenziale valida, continua a utilizzare tale credenziale a meno che non venga aggiunta una nuova credenziale.

Dopo un errore di raccolta, lo strumento di rilevamento tenta di raccogliere i dati di rete per un server dopo 3 minuti, 30 minuti, 2 ore e poi 6 ore. Dopo 4 tentativi falliti, lo strumento di rilevamento continua a provare tutte le credenziali configurate una volta ogni 6 ore.

Inventario scoperto

Dopo aver configurato una fonte di rilevamento, il valore del numero di server rilevati nel riquadro di stato dello strumento **Discovery** inizia ad aumentare. Lo stato di rilevamento per l'origine configurata cambia in **Enabled** nel frame del modulo **Collection**. La pagina di inventario mostra i server di tutte le fonti configurate: VM VMware, Hyper-V VM e server importati. Ogni server mostra l'origine e lo stato della raccolta per modulo.

Vai alla pagina **Inventario scoperto** per vedere i server trovati dallo strumento di rilevamento. Da questa pagina, scegli **Scarica inventario** per scaricare un file ZIP (`discovery_tool_export.zip`) che contiene fino a 30 giorni di dati raccolti, inclusi i file MPA per tutte le fonti configurate, i dati sull'utilizzo delle prestazioni, le informazioni sul database e le informazioni sulle comunicazioni da server a server.

Puoi scaricare il file ZIP mentre lo strumento di rilevamento continua a funzionare e ottenere risultati parziali. Carica questo file in [Migration assessment](#) per ottenere un business case per la migrazione.

Opzioni di esportazione

Quando si esportano dati, è possibile personalizzare l'esportazione con le seguenti opzioni:

Intervallo di date

Seleziona una data di inizio e una data di fine per esportare solo i dati raccolti in quel periodo di tempo. Entrambe le date sono incluse. L'intervallo di date massimo è 30 giorni.

Note

Lo strumento di rilevamento memorizza fino a 30 giorni di dati raccolti. Se hai bisogno di dati per più di 30 giorni, esegui esportazioni incrementali ogni 30 giorni per acquisire tutti i dati.

Selezione del modulo

Scegli quali moduli di dati includere nell'esportazione. Puoi esportare tutti i moduli o selezionarne di specifici:

Modulo	Description
Dati VMware	Inventario di macchine virtuali dai server vCenter
Hyper-V dati	inventario di macchine virtuali fornito dagli Hyper-V host
Dati di rete	Connessioni di rete tra server
Inventario dei server	Informazioni sull'hardware e sul sistema operativo del server
Metriche delle prestazioni del server	Utilizzo di CPU, memoria e rete

Modulo	Description
Prestazioni di storage del server	IOPS e velocità effettiva del disco
Configurazione dello storage	Configurazione del disco e del volume
Interfacce di rete	Dettagli dell'adattatore di rete
Parametri di elaborazione	Processi in esecuzione
Dati SQL Server	Inventario del database SQL Server
Dati del database Oracle	Inventario dei database Oracle: CDB, PDB, funzionalità, opzioni e componenti

Se non si seleziona alcun modulo, lo strumento di scoperta esporta tutti i dati disponibili.

Punti dati raccolti

Lo strumento di rilevamento raccoglie dati completi su VMware, metriche del sistema operativo Hyper-V, database e componenti di rete. Le sezioni seguenti descrivono in dettaglio i punti dati specifici raccolti per ciascun componente.

Raccolta dati VMware

Questa tabella descrive le informazioni sulle macchine virtuali VMware raccolte dallo strumento di rilevamento:

Nome	Tipo	Categoria	Valore di esempio
vm_name	Stringa	Informazioni sulla macchina virtuale	«w2k22-snmpd-v2-it-us-mssql-2022-testcase4-1»
vm_id	Stringa	Informazioni sulla VM	«vm-30920»

Nome	Tipo	Categoria	Valore di esempio
vm_uuid	Stringa	Informazioni sulla VM	«4201ecf8-cc44-ee7e-01da-34dfb2acf6c0»
stato di alimentazione	Stringa	Informazioni sulla VM	«Powered On»
host	Stringa	Informazioni sulla VM	«esxi-70-node1.testlab.local»
indirizzo_IP primario	Stringa	Informazioni sulla macchina virtuale	«192.168.052»
tazze	Numero intero	Informazioni sulla VM	2
memory	Numero intero	Informazioni sulla VM	4096
total_disk_capacity_mib	Numero intero	Informazioni sulla VM	32768
os_secondo il_file_di configurazione	Stringa	Informazioni sulla VM	«Microsoft Windows Server 2016 o versione successiva (64 bit)»
max_cpu_usage_pct_dec	Float	Prestazioni delle macchine virtuali	79.33
avg_cpu_usage_pct_dec	Float	Prestazioni delle macchine virtuali	45,06

Nome	Tipo	Categoria	Valore di esempio
max_ram_usage_pct_dec	Float	Prestazioni delle macchine virtuali	63,99
avg_ram_util_pct_dec	Float	Prestazioni delle macchine virtuali	29,27

Hyper-V raccolta dati

Questa tabella descrive le informazioni sulla macchina Hyper-V virtuale raccolte dallo strumento di rilevamento:

Nome	Tipo	Categoria	Valore di esempio
vm_name	Stringa	Informazioni sulla macchina virtuale	«win2022-hyperv-test-01»
vm_id	Stringa	Informazioni sulla VM	«a1b2c3d4-e5f6-7890-abcd-ef1234567890»
stato di alimentazione	Stringa	Informazioni sulla VM	«In esecuzione»
tazze	Numero intero	Informazioni sulla VM	4
memory_mb	Numero intero	Informazioni sulla macchina virtuale	8192

Nome	Tipo	Categoria	Valore di esempio
disk_paths	Stringa	Disk	«C:\ VM\ disk1.vhdx»
disk_size_gb	Float	Disk	127,0
adattatori di rete	Stringa	Rete	«00:15:5» D:01:02:03
indirizzi_ip	Stringa	Rete	«10.0.1.50"
host_name	Stringa	Host	«hyperv-host-01.example.com »
versione_host_os_	Stringa	Host	«Centro dati Windows Server 2022"
nome_cluster	Stringa	Host	«01" FailoverCluster
hypervisor	Stringa	Informazioni sulla VM	"Hyper-V"

Dati del server importati

I server importati non vengono rilevati automaticamente. Vengono importati tramite un file CSV. Lo strumento di rilevamento non raccoglie dati a livello di hypervisor per i server importati. Al contrario, raccoglie i dati relativi alle metriche del database, della rete e del sistema operativo utilizzando le credenziali del sistema operativo associate a ciascun server durante l'importazione.

I dati dello strumento Discovery OS-related

Lo strumento di rilevamento raccoglie l'inventario, le prestazioni, lo storage, l'interfaccia di rete e i dati di processo del server tramite SSH (Linux) e WinRM (Windows). Le tabelle seguenti descrivono i punti dati raccolti.

Inventario del server (server_inventory.csv)

Combina il provisioning del server (configurazione hardware e del sistema operativo) con prestazioni di storage aggregato. Raccolto ogni 24 ore.

Nome	Tipo	Categoria	Valore del campione
server_id	Stringa	Informazioni sul server	«vm-web-server-01»
nome_server	Stringa	Informazioni sul server	«server-web-01»
resource_type	Stringa	Informazioni sul server	«macchina virtuale»
stato_potere	Stringa	Informazioni sul server	«In esecuzione»
os_type	Stringa	Informazioni sul server	«Linux»
nome_sistema operativo	Stringa	Informazioni sul server	«Amazon Linux»
os_version	Stringa	Informazioni sul server	«2023»
nome_host primario	Stringa	Informazioni sul server	«web-server-01.example.com»
indirizzo_IP primario	Stringa	Informazioni sul server	«10.0.2.101»
maschera di rete	Stringa	Informazioni sul server	«255,255.255,0»
totale_num_cartelline_network_card	Numero intero	Informazioni sul server	2
numero_dischi_totale	Numero intero	Informazioni sul server	1

Nome	Tipo	Categoria	Valore del campione
cpu_count	Numero intero	Informazioni sul server	4
memoria_totale_gb	Float	Informazioni sul server	15,88
server_uuid	Stringa	Informazioni sul server	«4201ecf8-cc44-ee7e-01da-34dfb2acf6c0»
smbios_uuid	Stringa	Informazioni sul server	«4201ecf8-cc44-ee7e-01da-34dfb2acf6c0»
nome_cluster	Stringa	Informazioni sul server	«cluster-01»
hypervisor_object_id	Stringa	Informazioni sul server	«vm-30920»
tipo_hypervisor	Stringa	Informazioni sul server	«VMware»
versione_hypervisor	Stringa	Informazioni sul server	«8.0.0»
nome_host dell'hypervisor	Stringa	Informazioni sul server	«esxi-node1.example.com»
hypervisor_host_id	Stringa	Informazioni sul server	«host-1234»
hypervisor_id	Stringa	Informazioni sul server	«4201ecf8-cc44-ee7e-01da-34dfb2acf6c0»
disk_read_iops_avg	Float	Prestazioni di archiviazione	12,5
disk_read_iops_peak	Float	Prestazioni di archiviazione	245.0

Nome	Tipo	Categoria	Valore del campione
disk_write_iops_avg	Float	Prestazioni di archiviazione	8.3
disk_write_iops_peak	Float	Prestazioni di archiviazione	180.0
disk_total_iops_avg	Float	Prestazioni di archiviazione	20.8
disk_total_iops_peak	Float	Prestazioni di archiviazione	425,0
velocità di lettura del disco avg_mbps	Float	Prestazioni di archiviazione	1.2
disk_read_throughput_peak_m bps	Float	Prestazioni di archiviazione	24,5
throughput_disk_write_avg_m bps	Float	Prestazioni di archiviazione	0.8
disk_write_throughput_peak_ mbps	Float	Prestazioni di archiviazione	18.0
throughput_total_disk_avg_m bps	Float	Prestazioni di archiviazione	2.0
disk_total_throughput_peak_ mbps	Float	Prestazioni di archiviazione	42,5

Metriche delle prestazioni del server (server_performance_metrics.csv)

Utilizzo della CPU, della memoria e del throughput di rete. Campionato ogni 10 minuti, aggregato in 30 giorni.

Nome	Tipo	Categoria	Valore del campione
server_id	Stringa	Informazioni sul server	«vm-web-server-01»
data_source	Stringa	Informazioni sul server	«SISTEMA OPERATIVO»
cpu_utilization_avg_pct	Float	CPU	45,06
cpu_utilization_peak_pct	Float	CPU	79,33
cpu_count	Numero intero	CPU	4
memoria_total_gb	Float	Memoria	15,88
memory_utilization_avg_pct	Float	Memoria	29,27
memory_utilization_peak_pct	Float	Memoria	63,99
rete_in_avg_mbps	Float	Rete	0,52
rete_in_peak_mbps	Float	Rete	12.3
rete_out_avg_mbps	Float	Rete	0,31
network_out_peak_mbps	Float	Rete	8.7
network_total_avg_mbps	Float	Rete	0,83
network_total_peak_mbps	Float	Rete	21,0

Prestazioni di archiviazione (server_storage_performance.csv)

Per-volume utilizzo del disco I/O e dello spazio. Campionato ogni 10 minuti, aggregato in 30 giorni.

Nome	Tipo	Categoria	Valore del campione
server_id	Stringa	Informazioni sul server	«vm-web-server-01»
data_source	Stringa	Informazioni sul server	«SISTEMA OPERATIVO»
disk_volume_id	Stringa	Informazioni sul volume	"/dev/nvme0n1p1"
disk_mount_point	Stringa	Informazioni sul volume	"/"
file_system	Stringa	Informazioni sul volume	«xfs»
disk_total_gb	Float	Spazio su disco	30,0
disk_used_gb	Float	Spazio su disco	12,5
disk_free_gb	Float	Spazio su disco	17,5
disk_read_iops_avg	Float	Disco I/O	12,5
disk_read_iops_peak	Float	Disco I/O	245.0
disk_write_iops_avg	Float	Disco I/O	8.3
disk_write_iops_peak	Float	Disco I/O	180.0
disk_total_iops_avg	Float	Disco I/O	20.8
disk_total_iops_peak	Float	Disco I/O	425,0

Nome	Tipo	Categoria	Valore del campione
velocità di lettura del disco avg_mbps	Float	Velocità effettiva del disco	1.2
disk_read_throughput_peak_m bps	Float	Velocità effettiva del disco	24,5
throughput_disk_write_avg_m bps	Float	Velocità effettiva del disco	0.8
disk_write_throughput_peak_ mbps	Float	Velocità effettiva del disco	18.0
throughput_total_disk_avg_m bps	Float	Velocità effettiva del disco	2.0
throughput_total_peak_mbps del disco	Float	Velocità effettiva del disco	42,5

Configurazione dello storage (storage_config.csv)

Dettagli sull'hardware fisico del disco. Raccolto ogni 24 ore.

Nome	Tipo	Categoria	Valore del campione
server_id	Stringa	Informazioni sul server	«vm-web-server-01"
id_controllore del disco	Stringa	Informazioni sul disco	"/dev/sda"

Nome	Tipo	Categoria	Valore del campione
vmdk_vhd_file_name	Stringa	Informazioni sul disco	«web-server-01.vmdk»
tipo_volume del disco	Stringa	Informazioni sul disco	«Virtuale»
disk_provisioned_gb	Float	Informazioni sul disco	30,0
tipo_dispositivo del disco	Stringa	Informazioni sul disco	«DISCO RIGIDO SCSI»
tipo_interfaccia disco	Stringa	Informazioni sul disco	«SCSI»
protocollo_disco	Stringa	Informazioni sul disco	«LSI Logic SAS»

Interfacce di rete (network_interfaces.csv)

Configurazione dell'adattatore di rete. Raccolto ogni 24 ore.

Nome	Tipo	Categoria	Valore del campione
server_id	Stringa	Informazioni sul server	«vm-web-server-01»
nome_interfaccia	Stringa	Informazioni sull'interfaccia	«eth0»
indice_interfaccia	Numero intero	Informazioni sull'interfaccia	2

Nome	Tipo	Categoria	Valore del campione
mac_address	Stringa	Informazioni sull'interfaccia	«A:1B:2C:3D:4E:5F0"»
tipo_adattatore	Stringa	Informazioni sull'interfaccia	«vmxnet3"»
nome_rete_virtuale	Stringa	Informazioni sull'interfaccia	«Rete VM»
id_rete_virtuale	Stringa	Informazioni sull'interfaccia	«dvportgroup-1234"»
commutatore_virtuale	Stringa	Informazioni sull'interfaccia	«vSwitch0"»
indirizzo_ipv4	Stringa	Config IP	«10.0.2.101"»
ipv4_subnet_mask	Stringa	Config IP	«255,255.255,0"»
gateway_ipv4	Stringa	Config IP	«10.0.2.1»
indirizzo_ipv6	Stringa	Config IP	«fe80: :a1b:2cff:fe3d:4e5f»
lunghezza del prefisso ipv6	Numero intero	Config IP	64
gateway_ipv6	Stringa	Config IP	«fe80: :1"»
server_dns	Stringa	Config IP	«10.0.0.2»
dhcp_abilitato	Booleano	Config IP	false

Nome	Tipo	Categoria	Valore del campione
stato_interfaccia	Stringa	Informazioni sull'interfaccia	«Su»
vlan_id	Numero intero	Informazioni sull'interfaccia	100
is_primary	Booleano	Informazioni sull'interfaccia	true

Processi in esecuzione (process_metrics.csv)

Istantanea dei processi in esecuzione. Raccolto ogni ora, deduplicato nell'arco di 30 giorni.

Nome	Tipo	Categoria	Valore del campione
server_id	Stringa	Informazioni sul server	«vm-web-server-01»
nome_processo	Stringa	Informazioni sul processo	«sshd»
process_id	Numero intero	Informazioni sul processo	1234
riga di comando del processo	Stringa	Informazioni sul processo	«/usr/sbin/sshd -D»
utente_processo	Stringa	Informazioni sul processo	«radice»

Raccolta di rete

Il modulo Network collection ti aiuta a scoprire le dipendenze tra i server del tuo data center locale. Questi dati di rete accelerano la pianificazione della migrazione fornendo visibilità sul modo in cui le applicazioni comunicano tra i server.

Questo modulo raccoglie i dati di rete per i server da tutte le fonti configurate, tra cui VMware Hyper-V, e server importati. Utilizza WinRM per raccogliere dati dai server Windows e utilizza SSH, SNMPv2 e SNMPv3 per raccogliere dati dai server Linux.

Raccolta di dati di rete

Il modulo di raccolta Network acquisisce le connessioni TCP IPv4 nello stato ESTABLISHED o TIME_WAIT tra i server dell'inventario rilevato. Una connessione viene visualizzata nell'output solo quando sia l'indirizzo IP di origine che quello di destinazione appartengono a server che lo strumento di rilevamento ha rilevato o che sono stati importati dall'utente. Le connessioni da o verso indirizzi IP esterni all'inventario, come servizi esterni, endpoint cloud o server non ancora aggiunti allo strumento di rilevamento, non sono incluse.

Questo design concentra i dati di rete sulle dipendenze da server a server all'interno dell'ambiente, ovvero le informazioni necessarie per la mappatura delle dipendenze delle applicazioni e la pianificazione delle ondate di migrazione.

Questi punti dati vengono raccolti per ogni connessione:

Nome	Tipo	Categoria	Valore di esempio
IP di origine	Stringa	Connessione	«192.168.1.10»
Porta sorgente	Numero intero	Connessione	49152
ID del processo di origine	Numero intero	Processo	1234
Nome del processo di origine	Stringa	Processo	"java"
IP di destinazione	Stringa	Connessione	«192.168.1.20»

Nome	Tipo	Categoria	Valore di esempio
Porta di destinazione	Numero intero	Connessione	5432
ID del processo di destinazione	Numero intero	Processo	5678
Nome del processo di destinazione	Stringa	Processo	«postgres»
Stato	Stringa	Connessione	«STABILITO»
Protocollo di trasporto	Stringa	Connessione	«TCP»
Versione IP	Stringa	Connessione	«IPv4»
Conteggio	Numero intero	Connessione	42

 Tip

Per massimizzare la completezza della mappa delle dipendenze della rete, configura tutte le fonti di rilevamento (VMware e importazione CSV del server) e aggiungi le Hyper-V credenziali del sistema operativo prima di esaminare i dati di rete. Maggiore è il numero di server nell'inventario, maggiore è il numero di connessioni che il modulo di rete è in grado di acquisire.

Raccolta di indirizzi privati in rete

Per impostazione predefinita, il modulo di raccolta Network acquisisce solo le connessioni in cui entrambi gli endpoint sono server presenti nell'inventario rilevato. È possibile abilitare la raccolta di indirizzi privati per acquisire anche le connessioni da e verso gli indirizzi IP privati RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) che non sono presenti nel tuo inventario.

Per iniziare la raccolta privata degli indirizzi

1. Nella pagina di configurazione di Collector, individua la sezione Moduli Collection.

2. Trova il rilevamento delle connessioni di rete in Scoperta delle applicazioni.
3. Apri il menu a discesa Azioni.
4. Scegli Inizia la raccolta privata di indirizzi.
5. Se lo stato del modulo era Abilitato, puoi vederlo cambiare in Abilitato · Indirizzo privato su.

Per interrompere la raccolta di indirizzi privati, apri il menu a discesa Azioni e scegli Interrompi la raccolta di indirizzi privati. I dati degli indirizzi privati raccolti in precedenza vengono conservati anche dopo l'interruzione.

Le connessioni agli indirizzi privati vengono visualizzate solo nell'esportazione CSV completa (all'interno del file ZIP), non nei file CSV MPA. Se un indirizzo IP appartiene a un server già presente nell'inventario, viene sempre identificato dall'ID del server rilevato indipendentemente da questa impostazione.

Questa impostazione persiste anche dopo i riavvii. Puoi avviare o interrompere la raccolta di indirizzi privati in qualsiasi momento. I dati degli indirizzi privati raccolti in precedenza vengono esportati indipendentemente dall'impostazione corrente.

Raccolta SQL Server

Il modulo di raccolta SQL Server raccoglie le informazioni di SQL Server dai server Windows in tutte le fonti configurate, incluso VMware Hyper-V, e i server importati. Il modulo utilizza WinRM per connettersi in remoto a ciascun server Windows ed eseguire query. PowerShell Raccoglie informazioni su tutti i servizi (componenti) di SQL Server installati utilizzando gli spazi dei nomi, il registro e le proprietà dei file WMI.

Un componente di SQL Server è un'istanza specifica di servizio o funzionalità installata come parte di una distribuzione di SQL Server su un server Windows. Lo strumento di rilevamento raccoglie Database Engine, Analysis Services, Reporting Services e Integration Services.

Raccolta di dati in SQL Server

Il modulo di raccolta SQL Server raccoglie informazioni sui componenti di SQL Server. Questa tabella descrive i punti dati chiave raccolti:

Nome	Tipo	Categoria	Valore di esempio
Tipo di motore	Stringa	Componente	sql_server

Nome	Tipo	Categoria	Valore di esempio
È un componente del motore	Booleano	Componente	Y
Stato	Stringa	Servizio	In funzione, fermo, StartPending
Versione	Stringa	Servizio	2015.131,5026,0
Edizione	Stringa	Servizio	Edizione per sviluppatori (64 bit)
Nome del servizio SQL	Stringa	Servizio	MsDtsServer130, Mssql
Tipo di servizio SQL	Stringa	Servizio	Servizio SQL Server, servizio Integration Services
Nome dell'istanza	Stringa	Istanza	MSSQLSERVER
Nome visualizzazione	Stringa	Servizio	SQL Server (MSSQLSERVER2017)
Modalità di avvio	Stringa	Servizio	Automatico, manuale, disabilitato
Nome account del servizio	Stringa	Servizio	NT Service/MsDtsServer130
È raggruppato	Booleano	Configurazione	N

Note

Il formato completo include tutti i tipi di servizio. Il formato MPA include solo i componenti del motore di database. Non tutti i campi sono disponibili a seconda del tipo e della configurazione del servizio SQL.

Raccolta di database Oracle

Con Oracle Database Collection, puoi scoprire le istanze di database Oracle su tutte le fonti configurate, incluso VMware Hyper-V, e sui server importati. Il modulo raccoglie i seguenti dati:

- Enumerazione del database contenitore (CDB) e del database collegabile (PDB)
- Versione ed edizione
- Opzioni installate
- Statistiche sull'utilizzo delle funzionalità
- Inventario dei componenti (DBA_REGISTRY)
- Dimensionamento dei file di dati
- Flag topologici (RAC, Data Guard e architettura multitenant)

Database-connected (SQL)

Quando si configurano le credenziali Oracle, lo strumento di rilevamento si connette direttamente al database Oracle utilizzando l'account di servizio di sola lettura. Ciò fornisce una SQL-level raccolta completa che include i dettagli PDB, l'utilizzo delle funzionalità e le opzioni installate. Tutti i file CSV contengono dati completi.

OS-level riserva

Se non sono state configurate le credenziali del database o se la connessione non riesce, lo strumento di rilevamento utilizza SSH o WinRM per rilevare le installazioni Oracle. Rileva le home, i listener, le patch, la versione e l'edizione di Oracle senza accesso al database. Per OS-detected gli host, il CDB CSV esportato contiene il nome dell'istanza, il nome host, la versione e l'edizione. I file CSV PDB, delle funzionalità, delle opzioni e dei componenti non contengono righe.

La collezione Oracle produce i seguenti file CSV nel file ZIP di esportazione. Ogni tabella descrive i punti dati raccolti per file.

Dati CDB (oracle_data_cdb_full.csv)

Una riga per istanza CDB. Questa tabella descrive i punti dati CDB raccolti:

Nome	Tipo	Categoria	Valore di esempio	Origine
Nome dell'istanza	Stringa	Identità	«ORCL»	SQL, SISTEMA OPERATIVO
Host Name (Nome host)	Stringa	Identità	«oracledb01.examp le.com»	SQL, SISTEMA OPERATIVO
Nome DB	Stringa	Identità	«ORCL»	Solo SQL
Nome univoco DB	Stringa	Identità	«ORCL_PRIMARY»	Solo SQL
DBID	Numero intero	Identità	1234567890	Solo SQL
Versione	Stringa	Versione	«19.0.0.0"	SQL, SISTEMA OPERATIVO
Versione completa	Stringa	Versione	«19.21.0.0.0"	Solo SQL
Edizione	Stringa	Versione	«Edizione Enterprise»	SQL, SISTEMA OPERATIVO
Tipo di database	Stringa	Configura zione	«SINGOLO»	Solo SQL
Ruolo di database	Stringa	Configura zione	«PRIMARIO»	Solo SQL
Modalità aperta	Stringa	Configura zione	«LEGGI E SCRIVI»	solo SQL
Modalità log	Stringa	Configura zione	«REGISTRO DI ARCHIVIO»	Solo SQL

Nome	Tipo	Categoria	Valore di esempio	Origine
Platform (Piattaforma)	Stringa	Configurazione	«Linux x86 a 64 bit»	Solo SQL
Bandiera CDB	Stringa	Configurazione	«Sì»	Solo SQL
È RAC	Stringa	Topologia	«Sì» o «NO»	Solo SQL
Data Guard è in standby	Stringa	Topologia	«Sì» o «NO»	Solo SQL
Modalità di protezione	Stringa	Topologia	«PRESTAZIONI MASSIME»	solo SQL
Broker Data Guard	Stringa	Topologia	«ABILITATO»	Solo SQL
Set di caratteri NLS	Stringa	Configurazione	«AL32UTF8»	Solo SQL
Conteggio PDB	Numero intero	Dimensionamento	3	Solo SQL
Flashback attivo	Stringa	Configurazione	«Sì»	Solo SQL
Percorso di rilevamento	Stringa	Metadati	«phase2» o «phase1b»	SQL, SISTEMA OPERATIVO

dati PDB (oracle_data_pdb_full.csv)

Una riga per PDB (database collegabile). Questa tabella descrive i punti dati PDB raccolti:

Note

I dati PDB richiedono le credenziali del database Oracle (connessione SQL). OS-level il fallback non compila questo file CSV.

Nome	Tipo	Categoria	Valore di esempio	Origine
Nome dell'istanza CDB	Stringa	Identità	«ORCL»	Solo SQL
Nome PDB	Stringa	Identità	«APPPDB1»	Solo SQL
Modalità aperta	Stringa	Stato	«LEGGI E SCRIVI»	solo SQL
Stato del ciclo di vita	Stringa	Stato	«NORMALE»	Solo SQL
Numero di tablespaces	Numero intero	Dimensionamento	5	Solo SQL
Conteggio dei file di dati	Numero intero	Dimensionamento	12	Solo SQL
Dimensione totale (byte)	Numero intero	Dimensionamento	5368709120	Solo SQL
Conteggio dello schema utente	Numero intero	Dimensionamento	8	Solo SQL
Numero di link DB	Numero intero	Connettività	2	Solo SQL
Componenti installati	Stringa	Configurazione	«APEX; JVM; XML»	Solo SQL
Numero di tablespaces crittografati	Numero intero	Sicurezza	1	Solo SQL

Dati sull'utilizzo delle funzionalità (oracle_data_features_full.csv)

Una riga per voce sull'utilizzo delle funzionalità da DBA_FEATURE_USAGE_STATISTICS. Questa tabella descrive i punti dati sull'utilizzo delle funzionalità raccolti:

Note

I dati sull'utilizzo delle funzionalità richiedono le credenziali del database Oracle (connessione SQL). OS-level fallback non compila questo file CSV.

Nome	Tipo	Categoria	Valore di esempio	Origine
Nome dell'istanza CDB	Stringa	Identità	«ORCL»	Solo SQL
Nome	Stringa	Funzionalità	«Partizionamento (utente)»	Solo SQL
Usi rilevati	Numero intero	Utilizzo	42	Solo SQL
Attualmente in uso	Stringa	Utilizzo	«VERO»	Solo SQL
Data del primo utilizzo	DateTime	Utilizzo	«2024-01-15T00:00:00»	Solo SQL
Data ultimo utilizzo	DateTime	Utilizzo	«2026-06-01T00:00:00»	Solo SQL

Dati relativi alle opzioni (oracle_data_options_full.csv)

Una riga per voce V\$OPTION per CDB. Questa tabella descrive i punti dati delle opzioni installate raccolti:

Note

I dati delle opzioni richiedono le credenziali del database Oracle (connessione SQL). OS-level fallback non compila questo file CSV.

Nome	Tipo	Categoria	Valore di esempio	Origine
Nome dell'istanza CDB	Stringa	Identità	«ORCL»	Solo SQL
Nome opzione	Stringa	Opzione	«Analisi avanzate»	Solo SQL
È installato	Stringa	Opzione	«VERO»	Solo SQL
ID del contenitore	Numero intero	Opzione	0	Solo SQL

Dati dei componenti (oracle_data_components_full.csv)

Una riga per componente DBA_REGISTRY. Questa tabella descrive i punti dati raccolti dai componenti:

Note

I dati dei componenti richiedono le credenziali del database Oracle (connessione SQL). OS-level fallback non compila questo file CSV.

Nome	Tipo	Categoria	Valore di esempio	Origine
Nome dell'istanza CDB	Stringa	Identità	«ORCL»	Solo SQL
Nome PDB	Stringa	Identità	«APPPDB1»	Solo SQL
ID del componente	Stringa	Componente	«APICE»	Solo SQL
Nome del componente	Stringa	Componente	«Oracle Application Express»	Solo SQL
Versione	Stringa	Componente	«22.1.0.15.0»	Solo SQL
Stato	Stringa	Componente	«VALIDO»	Solo SQL

Nome	Tipo	Categoria	Valore di esempio	Origine
Schema	Stringa	Componente	«APEX_220100»	Solo SQL

Considerazioni relative alla sicurezza

Protezione della macchina virtuale dello strumento di rilevamento

La sicurezza delle VM di Discovery Tool è fondamentale perché lo strumento di rilevamento archivia tutte le credenziali, i log e i dati dei clienti sulla VM dello strumento di rilevamento.

Lo strumento di rilevamento VM ha l'accesso ssh disabilitato per impostazione predefinita ed è accessibile solo dal client. vCenter UI -> "Launch Web Console"

Lo strumento di rilevamento VM viene fornito con una password di accesso predefinita («password») per l'utente «discovery».

- Si consiglia di aggiornare questa password immediatamente dopo la distribuzione.
- È necessario aggiornare la password se si desidera abilitare ssh utilizzando il comando `enablessh` dopo l'accesso tramite vCenter. Launch Web Console Tieni presente che ogni volta che viene chiamato questo comando, devi resettarlo.

Protezione delle credenziali

Best practice generali per la gestione delle credenziali

- Archivia le credenziali in modo sicuro
- Ruota regolarmente tutte le credenziali
- Usa gestori di password o casseforti sicuri
- Monitora l'utilizzo delle credenziali
- Segui il principio del privilegio minimo e concedi solo le autorizzazioni minime necessarie

Credenziali SNMP v2

- Usa stringhe di community complesse e non predefinite

- Evita stringhe comuni come «public» o «private»
- Tratta le stringhe della community come password

Credenziali SNMP v3

- Abilita sia l'autenticazione che la privacy
- Utilizza protocolli di autenticazione avanzati (preferibilmente SHA rispetto a MD5)
- Utilizza protocolli di crittografia avanzati (AES preferito rispetto a DES)
- Utilizza password complesse sia per l'autenticazione che per la privacy
- Usa nomi utente univoci (evita nomi comuni)

Credenziali WinRM

- Evitare di disabilitare il controllo dei certificati WinRM.
- Si consiglia di creare un account di servizio dedicato con autorizzazioni minime richieste.
- Evita di utilizzare account di amministratore di dominio o amministratore locale a meno che non sia necessaria la raccolta di SQL Server. La raccolta SQL Server richiede l'accesso come amministratore locale perché esegue query su più namespace WMI e utilizza comandi con privilegi elevati. Per le metriche del sistema operativo senza SQL Server Discovery, è sufficiente un account non amministratore con Remote Management Users, Performance Monitor Users e accesso in lettura WMI. root\cimv2 Per i dettagli relativi ai singoli moduli, vedere [the section called “Autorizzazioni richieste”](#).

Hyper-V credenziali

- Utilizza account di servizio dedicati con autorizzazioni di Hyper-V gestione minime.
- Evita di utilizzare account di amministratore di dominio.
- Hyper-V le credenziali supportano l'autenticazione NTLM (solo HTTPS) e Kerberos.
- Lo strumento di rilevamento archivia le credenziali crittografate a riposo utilizzando SQLCipher.

Credenziali Oracle

- Utilizza un account di servizio dedicato in sola lettura con solo SELECT_CATALOG_ROLE. Non utilizzare i privilegi DBA, SYSDBA o SYSOPER.

- Lo strumento di rilevamento esegue solo operazioni di lettura e non scrive mai nel database Oracle.
- Lo strumento di rilevamento non accede alle visualizzazioni di Diagnostics Pack o Tuning Pack, quindi non è richiesta alcuna licenza Oracle aggiuntiva.
- Ruota regolarmente la password dell'account del servizio Oracle e aggiorna la credenziale nello strumento di scoperta.

Archiviazione delle credenziali

Lo strumento di rilevamento crittografa le credenziali archiviate a riposo utilizzando una chiave di crittografia del database. Su sistemi con systemd 250 o versioni successive, questa chiave viene crittografata utilizzando systemd-creds. Nei sistemi più vecchi, la chiave viene archiviata come file protetto da autorizzazioni. In entrambi i casi, un utente malintenzionato con accesso root all'host dello strumento di rilevamento potrebbe accedere alla chiave di crittografia e decrittografare le credenziali archiviate. Limita l'accesso all'host dello strumento di rilevamento e trattalo come un sistema privilegiato nel tuo ambiente.

Usare la Auto-Connect funzionalità con cautela

Lo strumento di rilevamento utilizza due meccanismi per assegnare le credenziali ai server durante la OS-level raccolta: connessione automatica e manuale. OS-level la raccolta include i moduli Network, SQL Server, Oracle Database e OS Metrics. Questi moduli si connettono a singoli server da tutte le fonti, incluse VM VMware, Hyper-V VM e server importati.

Manuale: un server può essere associato manualmente a una credenziale specifica. In questo caso, lo strumento di scoperta utilizza solo quella credenziale, indipendentemente dal successo o dal fallimento. È necessario monitorare manualmente lo stato della raccolta per quel server e apportare modifiche.

Auto-connect: se nessuna credenziale è associata manualmente al server, lo strumento di rilevamento utilizza il meccanismo di connessione automatica per quel server. Ciò significa:

- All'inizio di ogni round di raccolta, lo strumento di rilevamento ottiene un elenco di credenziali disponibili per quel server (in base ai tipi di sistema operativo) e configurate anche per essere «connettibili automaticamente».
- Lo strumento di rilevamento verifica quindi tutte le credenziali rispetto al server in un ciclo.

- Se viene trovata una credenziale funzionante, il ciclo di raccolta per il server ha esito positivo. Lo strumento di scoperta la ricorda e la prova per primo la prossima volta.
- Se non viene trovata alcuna credenziale funzionante, il ciclo di raccolta per il server non è riuscito.
 - Modulo di rete: il server utilizza una pianificazione di backoff, iniziando il prossimo round di raccolta tra 3 minuti, 30 minuti, 2 ore e 6 ore dopo ogni errore (simile al backoff esponenziale).
 - Raccolta SQL Server: lo strumento di rilevamento non riprova. Effettua un tentativo per server ogni giorno.

Impacts/Risks:

Usa la connessione automatica solo quando sei sicuro che i rischi siano mitigati nel tuo sistema:

Rischio 1: con la connessione automatica configurata su più credenziali errate, provarle automaticamente contro i server potrebbe innescare il blocco degli account per gli ambienti di produzione in cui sono configurate le politiche di blocco. Ad esempio, un data center può impostare il blocco delle proprie macchine virtuali dopo 3 tentativi di accesso SSH falliti. In questo caso, se la connessione automatica è configurata per 3 credenziali SSH errate, si verificherebbero blocchi legittimi degli account. Se si verificano blocchi su più sistemi, i processi aziendali critici potrebbero risentirne, causando potenzialmente guasti a cascata nei sistemi dipendenti. Inoltre, i Security Operations Center potrebbero subire tempeste di allarmi in caso di errori di autenticazione di massa, generando incidenti di sicurezza falsi positivi che esauriscono le risorse e possono mascherare attacchi reali.

Rischio 2: un utente con accesso allo strumento di rilevamento (conosce la password dello strumento di rilevamento) può utilizzare credenziali del sistema operativo con forza bruta su tutti i server, configurando un gran numero di credenziali di test e utilizzando la connessione automatica per trovare quelle di successo.

Mitigazioni:

Seguire queste linee guida:

- Assicurati che la password dello strumento di rilevamento sia adeguatamente protetta e nota solo agli attori autorizzati
- Assicurati che vengano inserite le credenziali corrette per l'ambiente se sono in atto politiche di blocco. Consigliamo di configurare solo credenziali funzionanti note anche se le policy di blocco degli account sono assenti per garantire un carico operativo minimo sulle singole macchine virtuali.

- "Auto-connect" è una funzionalità opzionale. Non selezionatela e utilizzate l'assegnazione manuale delle credenziali se il blocco degli account rappresenta un problema per l'ambiente.

Sicurezza dell'importazione in formato CSV

Quando importi server utilizzando un file CSV, considera le seguenti implicazioni di sicurezza:

- Il file CSV potrebbe contenere nomi host o indirizzi IP di server interni. Trattali come dati sensibili.
- Le `oracle_credential_name` colonne `os_credential_name` e fanno riferimento alle credenziali preconfigurate utilizzando un nome descrittivo. Il file CSV non contiene segreti.
- All-or-nothing convalida: se una riga del file CSV non è valida, l'intero caricamento viene rifiutato. In questo modo si evitano importazioni parziali che potrebbero creare confusione.
- I server importati sono immediatamente visibili nell'inventario e idonei alla raccolta. Assicuratevi che le credenziali del sistema operativo e Oracle abbiano un ambito corretto prima dell'importazione.

Considerazioni sulla revoca dell'accesso

Quando si revoca l'accesso, l'eliminazione è limitata alla fonte specifica:

- La revoca dell'accesso a vCenter elimina solo i dati vCenter. Non influisce sui Hyper-V dati del server né li importa.
- La revoca dell' Hyper-V accesso elimina solo i dati. Hyper-V Non influisce su VMware o sui dati del server importati.
- L'eliminazione dei server importati li rimuove dall'inventario, ma i dati di raccolta a valle (rete, database, metriche del sistema operativo) vengono conservati.
- Per rimuovere tutti i dati di inventario specifici dell'origine, è necessario revocare o eliminare ogni fonte in modo indipendente. I dati di raccolta a valle (rete, database, metriche del sistema operativo) vengono conservati anche dopo la revoca di tutte le fonti.

Risoluzione dei problemi

Verifica della connettività degli strumenti di rilevamento a vCenter

Se riscontrate errori di configurazione dei moduli VMware, segui questi passaggi per verificare la connettività:

Accedi allo strumento di rilevamento VM

- Log-in allo strumento di rilevamento VM, aprire Remote Console in vCenter
 - Nome utente: discovery
 - Password: password

Test della connettività vCenter

1. Test dell'accesso all'API vCenter:

```
curl -v --insecure -u <username>:<password> https://<vcenter-ip-or-hostname>:443/mob
```

2. Risultato di successo previsto:

```
[ec2-user@discoverytool ~]$ curl -v --insecure -u <user>:<password> https://vcsa/mob > tmp.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %         0         0              0             0 --:--:-- --:--:-- --:--:--    0*
Trying 192.168.2.125:443...
* Connected to vcsa (192.168.2.125) port 443 (#0)
...
</xml>
* Connection #0 to host vcsa left intact
```

Certificato SSL di prova

1. Eseguire il comando:

```
openssl s_client -showcerts -servername <hostname> -connect <hostname>:443
```

2. Risultato di successo previsto:

- Dovrebbe mostrare i dettagli del certificato vSphere
- Verifica la SSL/TLS connettività sulla porta 443

```
[ec2-user@discoverytool ~]$ openssl s_client -showcerts -servername vcsa -connect
vcsa:443
CONNECTED(00000003)
depth=0 CN = vcsa.onpremsim.env, C = US
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = vcsa.onpremsim.env, C = US
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/CN=vcsa.onpremsim.env/C=US
  i:/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
  Engineering
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
---
Server certificate
subject=/CN=vcsa.onpremsim.env/C=US
issuer=/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=vcsa.onpremsim.env/OU=VMware
  Engineering
---
```

Risoluzione dei problemi WinRM

Se riscontri problemi di connettività con WinRM, segui questi passaggi per testare la connessione. Questi passaggi si applicano anche ai problemi di Hyper-V connettività, poiché lo strumento di rilevamento utilizza WinRM per comunicare con gli host. Hyper-V

Verifica la connettività WinRM di base utilizzando le porte 5985 (HTTP) e 5986 (HTTPS). Dobbiamo assicurarci che la connettività funzioni sulla porta 5986 (HTTPS)

```
# Check WinRM listener configuration
winrm enumerate winrm/config/listener

# Note: Replace <HOST> with the target computer's hostname or IP address. Adjust the
  username and password as needed.
# Test WinRM connection on port 5985 (HTTP)
$cred = Get-Credential
```



```
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5985

# Test WinRM connection on port 5986 (HTTPS)
Test-WSMan -Computer <HOST> -Authentication Negotiate -Credential $cred -Port 5986
```

Se i test precedenti falliscono, prova a stabilire una PowerShell sessione con la convalida dei certificati disabilitata:

```
$cred = Get-Credential
$so = New-PsSessionOption -SkipCACHeck -SkipCNCheck -SkipRevocationCheck
Enter-PSSession -ComputerName <HOST> -Credential $cred -Port 5985 -SessionOption $so
```

Risoluzione dei problemi Kerberos

Se riscontri errori di autenticazione Kerberos durante la raccolta di dati dai server Windows, utilizza le seguenti sezioni per diagnosticare e risolvere i problemi più comuni.

Verifica i requisiti di rete

Prima di risolvere i problemi di autenticazione Kerberos, verifica che lo strumento di rilevamento possa raggiungere gli endpoint di rete richiesti.

Per verificare i requisiti di rete per Kerberos

1. Verifica la risoluzione DNS sul controller di dominio. Esegui il comando seguente dalla macchina virtuale dello strumento di rilevamento:

```
nslookup dc01.example.com
```

In alternativa, è possibile utilizzare dig:

```
dig dc01.example.com
```

Se la risoluzione DNS fallisce, verifica che lo strumento di rilevamento VM sia configurato per utilizzare un server DNS in grado di risolvere il dominio Active Directory. Verifica `/etc/resolv.conf` e conferma che le voci del nameserver puntino ai server DNS del tuo dominio.

2. Verifica la connettività al Key Distribution Center (KDC) sulla porta 88. Esegui il comando seguente:

```
nc -zv dc01.example.com 88
```

Output previsto:

```
Connection to dc01.example.com 88 port [tcp/kerberos] succeeded!
```

Se la connessione fallisce, verifica che nessuna regola del firewall blocchi il traffico dalla macchina virtuale dello strumento di rilevamento al controller di dominio sulla porta 88.

3. Verifica la connettività ai server Windows di destinazione sulle porte WinRM. Esegui i comandi seguenti:

```
nc -zv <windows-server> 5985  
nc -zv <windows-server> 5986
```

Se la connessione fallisce, verifica che WinRM sia abilitato sul server di destinazione e che le regole del firewall consentano il traffico in entrata sulle porte 5985 e 5986.

Problemi comuni relativi a Kerberos

Di seguito sono riportati i problemi comuni di Kerberos e le relative soluzioni.

Errori di distinzione tra mai

Sintomo: durante l'autenticazione viene visualizzato l'errore «Server non trovato nel database Kerberos».

Questo errore si verifica in genere quando il nome dell'area di autenticazione Kerberos non è in maiuscolo. I realm Kerberos devono essere specificati in lettere maiuscole nel file. `krb5.conf` Ad esempio, utilizza `EXAMPLE.COM` anziché `example.com`.

Prevenzione del blocco dell'account

Lo strumento di rilevamento utilizza un meccanismo di backoff per impedire il blocco degli account dovuto a ripetuti tentativi di autenticazione falliti. Se il tuo account di servizio viene bloccato, puoi reimpostare il processo di raccolta interrompendo e quindi avviando il modulo di raccolta tramite l'interfaccia utente web dello strumento di rilevamento all'indirizzo. `https://<discovery-tool-vm-ip>:5000`

kinit fallisce dalla CLI

La tabella seguente elenca gli kinit errori più comuni e le relative soluzioni.

Errore	Causa	Soluzione
Impossibile trovare KDC for realm	Il nome host o l'indirizzo IP del KDC non sono raggiungibili oppure il realm non è configurato in <code>krb5.conf</code>	Verifica che il <code>krb5.conf</code> file contenga il nome host e il realm KDC corretti. Conferma la risoluzione DNS e la connettività di rete al KDC sulla porta 88.
Preautenticazione non riuscita	La password per l'account di servizio non è corretta.	Verifica la password e riprova. Se l'account è bloccato, sbloccalo in Active Directory prima di riprovare.
Client non trovato nel database Kerberos	Il nome principale non corrisponde a nessun account in Active Directory.	Verifica che il nome principale corrisponda esattamente al nome dell'account, maiuscole e minuscole. Usa il formato <code>username@REALM</code> con il realm in maiuscolo.
Impossibile risolvere l'indirizzo di rete per KDC	Il DNS non è in grado di risolvere il nome host KDC.	Verifica la configurazione DNS in <code>/etc/resolv.conf</code> . Verifica che il server DNS sia in grado di risolvere il nome host KDC. Esegui il test con <code>o. nslookup dig</code>

La raccolta fallisce nonostante il successo di kinit

Se `kinit` riesce ma la raccolta dei dati continua a fallire, controlla quanto segue:

1. Verifica che il nome principale utilizzato per la raccolta corrisponda `kinit` esattamente al maiuscolo/minuscolo utilizzato durante.
2. Verificate che l'account di servizio disponga delle autorizzazioni richieste sui server di destinazione.
3. Verificare che WinRM sia abilitato sui server di destinazione.

4. Verifica che il nome host utilizzato per la raccolta corrisponda al nome host registrato in Active Directory.

Kerberos funziona per alcuni server ma non per altri

Se l'autenticazione Kerberos riesce per alcuni server ma fallisce per altri, esamina le seguenti aree:

Se i tuoi server si estendono su più domini Active Directory, configura una credenziale Kerberos separata per ogni dominio. Assicurati che il `/etc/krb5.conf` file includa voci per tutti i reami. Ogni dominio richiede la propria credenziale con il principale `correttousername@REALM`.

Confronta la configurazione WinRM su un server funzionante con un server guasto. Esegui il comando seguente su ogni server:

```
winrm get winrm/config
```

Verifica la connettività con Remote Desktop per isolare il problema. Lo strumento di rilevamento utilizza il `formatusername@DOMAIN`, mentre Remote Desktop utilizza il formato `DOMAIN\username`.

Verificate che l'account di servizio sia membro del gruppo Administrators locale sul server in cui si verifica l'errore. Esegui il comando seguente sul server di destinazione:

```
net localgroup Administrators
```

WMI richiede i privilegi di amministratore locale per accedere alle informazioni del sistema operativo. La raccolta SQL Server richiede inoltre che l'account di servizio disponga dell'accesso di amministratore locale sul server di destinazione.

Elenco di controllo per la configurazione Kerberos

Utilizza la seguente lista di controllo per verificare la configurazione di Kerberos prima di iniziare la raccolta dei dati.

- Il `krb5.conf` file esiste nella macchina virtuale dello strumento di rilevamento.
- Il nome del realm è in maiuscolo in `krb5.conf`
- L'esecuzione `kinit` con l'account del servizio riesce senza errori.
- Running `klist` mostra un ticket valido e non scaduto.

- Il nome principale corrisponde esattamente al nome dell'account di Active Directory.
- La risoluzione DNS funziona per il nome host KDC.
- La connettività di rete al KDC sulla porta 88 è confermata.
- La connettività di rete ai server Windows di destinazione sulle porte 5985 e 5986 è confermata.
- (Multi-domain) Ogni dominio Active Directory ha le proprie credenziali configurate nello strumento di rilevamento `[realms]` e `krb5.conf` contiene `[domain_realm]` voci per tutti i domini.

Risoluzione dei problemi del database Orac

Per diagnosticare problemi di raccolta del database Oracle, come dati mancanti o errori, controlla quanto segue.

Connessione rifiutata o timeout

Sintomo: lo stato della raccolta Oracle mostra un errore di connessione per un server.

Per risolvere questo problema, controlla quanto segue:

- Verifica che il listener Oracle sia in esecuzione sull'host di destinazione: `lsnrctl status`
- Verifica la connettività di rete dallo strumento di rilevamento all'host Oracle sulla porta 1521 (o sulla porta personalizzata): `nc -zv <oracle-host> 1521`
- Verifica che le regole del firewall consentano le connessioni in entrata sulla porta del listener Oracle.
- Verifica il nome del servizio eseguendolo `lsnrctl services` sull'host Oracle. Se il nome del servizio non è corretto, il listener Oracle rifiuta la connessione.

Errori di autenticazione () ORA-01017

Sintomo: la raccolta non riesce a causa di un errore di nome utente o password non validi.

Per risolvere questo problema, controlla quanto segue:

- Verifica che l'account del servizio Oracle esista e non sia bloccato: `SELECT account_status FROM dba_users WHERE username = 'DISCOVERY_USER';`
- Verifica che la password sia corretta collegandoti manualmente: `sqlplus discovery_user/<password>@<host>:1521/<service_name>`

- Se l'account è bloccato, sbloccalo: `ALTER USER discovery_user ACCOUNT UNLOCK;`

Privilegi insufficienti () ORA-01031

Sintomo: la connessione riesce ma la raccolta restituisce dati incompleti.

Per risolvere questo problema, controlla quanto segue:

- Verifica che `SELECT_CATALOG_ROLE` sia concesso: `SELECT * FROM dba_role_privs WHERE grantee = 'DISCOVERY_USER';`
- Concedi il ruolo richiesto se manca: `GRANT SELECT_CATALOG_ROLE TO discovery_user;`

Le credenziali manuali mostrano errori ma la connessione automatica funziona

Quando si aggiunge manualmente una credenziale a un server, lo strumento di rilevamento non ritorna se la connessione fallisce. Verifica che la porta e il nome del servizio configurati sulla credenziale corrispondano al listener Oracle su quel server specifico. Se il server ha una porta o un nome di servizio non standard, aggiorna di conseguenza la configurazione delle credenziali.

OS-level fallback che non rileva Oracle

Se non sono configurate credenziali del database e il OS-level fallback non rileva Oracle:

- Verificate che le credenziali del sistema operativo SSH o WinRM siano configurate e funzionanti per il server (controllate lo stato della raccolta delle metriche del sistema operativo).
- Per gli host Linux, verifica che `/etc/oratab` esistano o che i processi Oracle process monitor () `pmon` siano in esecuzione.
- Per gli host Windows, verifica che esistano voci del registro Oracle `HKLM\SOFTWARE\Oracle` o che `oracle.exe` i processi siano in esecuzione.

Risoluzione dei problemi SNMP

Accedi allo strumento di rilevamento VM

- Log-in allo strumento di rilevamento VM, aprire Remote Console in vCenter
 - Nome utente: `discovery`
 - Password: `password`

Installare gli strumenti SNMP (se necessario)

- `sudo yum install net-snmp-utils -y`

Verifica la connessione SNMP ai server Linux

1. `snmptable -v 2c -c <COMMUNITY_STRING>
<REMOTE_SERVER_IP> .1.3.6.1.2.1.6.13.1`
2. Esempio:

```
#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
```

Errori di raccolta in rete

è necessario un terminale per leggere la password

Errore:

```
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
```

Il comando `ss` richiede la password dell'utente. L'utente `ssh` configurato deve appartenere al gruppo `sudoers` ed essere configurato con `sudo` senza password per il comando. `ss/netstat` Per configurare `sudo` senza password:

1. Crea un nuovo file `sudoers`:

```
sudo vi -f /etc/sudoers.d/<username>
```

2. Aggiungi la riga:

```
<username> ALL=(ALL) NOPASSWD: /usr/sbin/ss, /usr/bin/netstat
```

3. Dopo questa modifica, l'esecuzione `sudo ss -tnap` e `sudo netstat -tnap` dovrebbe essere eseguita senza richiedere una password

La raccolta di rete è stata eseguita senza sudo

Se viene visualizzato il seguente avviso nella pagina Inventario scoperto:

```
Network collection ran without sudo. Process-level connection data may be missing.
```

Questo avviso indica che l'account utente SSH non dispone dell'accesso sudo sul server di destinazione. Senza sudo, lo strumento di rilevamento può comunque raccogliere i dati delle connessioni di rete, ma non può determinare a quale processo appartiene ciascuna connessione. Per raccogliere dati di connessione completi a livello di processo, assicurati che l'utente SSH disponga dell'accesso sudo sul server di destinazione.

Errori di raccolta delle metriche del sistema operativo

UUID del server mancante per i server Linux

Se lo strumento di rilevamento non è in grado di raccogliere l'UUID del server (visualizzato come vuoto o mancante) per i server Linux, verifica che le credenziali SSH configurate per tali server abbiano i privilegi sudo. Lo strumento utilizza `dmidecode` per leggere l'UUID del server. Se non `dmidecode` è installato, lo strumento torna alla lettura `/sys/class/dmi/id/product_uuid`, che richiede anche l'accesso sudo. Senza sudo, nessuno dei due metodi può recuperare l'UUID.

Risoluzione: assicurati che l'account utente SSH fornito allo strumento di rilevamento disponga dell'accesso sudo sui server Linux di destinazione.

Problemi di accesso nell'inventario Discovered

Se viene visualizzato un messaggio nello stato della raccolta sul server, ad esempio Credenziali mancanti o Accesso negato:

1. Seleziona il server nella tabella dei server rilevati.

2. Scegli Gestisci credenziali di accesso Puoi scegliere di:
 - a. Seleziona credenziali alternative dal menu a discesa Seleziona credenziali.
 - b. Seleziona Usa nuove credenziali e fornisci nuove credenziali.
3. Save (Salva).

Lo strumento di rilevamento riprova la connessione dopo aver salvato le modifiche.

Risoluzione dei problemi di autenticazione tramite chiave SSH

Test della connettività delle chiavi SSH dallo strumento di rilevamento

Se l'autenticazione con chiave SSH fallisce, verifica la connettività dallo strumento di rilevamento al server di destinazione:

1. Accedere allo strumento di rilevamento (tramite console vSphere o SSH sull'host Linux).
2. Verifica la connettività SSH utilizzando la tua chiave privata:

```
ssh -i /path/to/private_key -o StrictHostKeyChecking=no <username>@<target_ip>
```

3. Se la connessione riesce, il problema riguarda il modo in cui la chiave è stata caricata nello strumento di rilevamento. Re-upload inserisci la chiave e verifica che il nome utente corrisponda.
4. Se la connessione fallisce, controlla il messaggio di errore nella tabella seguente.

Messaggio di errore	Causa	Risoluzione
Permission denied (publickey)	La chiave pubblica non è nel <code>authorized_keys</code> file del server di destinazione o il nome utente è sbagliato.	Aggiungi la chiave pubblica <code>~/.ssh/authorized_keys</code> al server di destinazione per l'utente corretto. Verifica le autorizzazioni dei file: <code>chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys</code> .
Connection timed out after 20s	La porta 22 non è raggiungibile dallo strumento di rilevamento.	Verificate che la porta 22 sia aperta tra lo strumento di rilevamento e il server di destinazione. Controlla i firewall e i gruppi di sicurezza.

Messaggio di errore	Causa	Risoluzione
Connection refused	Il servizio SSH non è in esecuzione sul server di destinazione.	Avvia il servizio SSH: <code>sudo systemctl start sshd</code>
Invalid SSH key for credential ' <i>name</i> '	Il formato della chiave non è supportato, i dati chiave sono danneggiati o la passphrase è mancante o errata.	Verifica che il formato della chiave sia RSA, ECDSA o Ed25519 in formato PEM, OpenSSH o PKCS #8. Se la chiave è crittografata, assicurati che la passphrase sia corretta.

Risoluzione dei problemi del programma di installazione Linux

La porta 5000 è già in uso

Sintomo: il servizio Discovery Tool non si avvia dopo l'installazione.

Risoluzione: identifica e interrompi il processo utilizzando la porta 5000:

```
sudo ss -tlnp | grep :5000
```

Interrompi il processo in conflitto, quindi riavvia lo strumento di rilevamento:

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

Messaggi di errore comuni

Questa tabella descrive i messaggi di errore più comuni e le relative spiegazioni:

Messaggio	Location (Ubicazione)	Spiegazione
È già stata creata una password	Crea una pagina con password	Condizione di gara in cui due utenti creano password contemporaneamente ; aggiorna

Messaggio	Location (Ubicazione)	Spiegazione
Esportazione non riuscita	Pagina dell'inventario	Riprova o invia i registri
È già in corso una raccolta su richiesta	Pagina dell'inventario	Condizione di gara quando due utenti avviano le raccolte manuali contemporaneamente; riprova al termine della raccolta manuale corrente
Command timed out after 60s	Stato della raccolta sul server	Un comando sul server di destinazione non è stato completato entro 60 secondi. Ciò può verificarsi su server con carichi elevati. Riprova la raccolta o esamina il carico del server di destinazione.
Una o più credenziali contengono UUID sconosciuti	Pagina di accesso al sistema operativo	Condizione valida quando due utenti modificano le credenziali del sistema operativo contemporaneamente; riprova
Password non valida	Sign-in pagina	Password errata per l'accesso; contatta l'amministratore o contattaci
La tua sessione è scaduta. Effettua nuovamente il login.	Sign-in pagina	La sessione è scaduta, è necessario effettuare nuovamente il login
Si è verificato un errore interno	Diverse pagine	Riprova o invia i log

Note di rilascio

Questa sezione descrive le funzionalità, i miglioramenti e le correzioni di bug per lo strumento di AWS Transform scoperta, organizzate per data di rilascio.

Data	Versione	Note di rilascio
30 giugno 2026	1,0,1646	Nuove funzionalità • Aggiunto il rilevamento del database Oracle. Lo strumento raccoglie la topologia, la versione, l'edizione, le opzioni installate, l'utilizzo delle funzionalità e l'inventario dei componenti di CDB e PDB. Lo strumento di rilevamento supporta connessioni SQL dirette (utilizzando SELECT_CATALOG_ROLE) e il rilevamento di OS-level fallback tramite SSH o WinRM. • È stato aggiunto il supporto per più credenziali Kerberos su diversi domini Active Directory. Ogni credenziale si autentica in modo indipendente, abilitando la raccolta dai server Windows in più domini senza conflitti di autenticazione. Miglioramenti • Raccolta di metriche del sistema operativo migliorata per gli host legacy. È stata aggiunta la raccolta di dati di fallback per i sistemi operativi precedenti (RHEL 5, SLES 11, Windows Server 2008 R2) in cui i comandi moderni non sono disponibili. I dati di archiviazione, prestazioni e interfaccia di rete vengono ora raccolti utilizzando interfacce di sistema alternative. Correzioni di bug • Sono stati corretti gli errori di autenticazione Kerberos per i server rilevati tramite Hyper-V. Lo strumento di rilevamento ora risolve correttamente il nome host del server (FQDN) dai metadati Hyper-V degli ospiti, necessari per la corrispondenza tra Kerberos SPN.
14 maggio 2026	1,0,1363	Nuove funzionalità

Data	Versione	Note di rilascio
		• È stato aggiunto il programma di installazione Linux per la distribuzione dello strumento di rilevamento su distribuzioni Linux supportate (Amazon Linux 2, Amazon Linux 2023, RHEL 8—9, Rocky Linux 8—9, 9, Ubuntu 20.04—24.04, Debian 10—12, AlmaLinux SLES 15 SP5). • È stato aggiunto il supporto per la configurazione di più server VMware vCenter con deduplicazione automatica delle VM tra vCenter. • È stata aggiunta l'autenticazione con chiave privata SSH come alternativa al nome utente e alla password per l'accesso al sistema operativo Linux. I formati chiave supportati includono RSA, ECDSA, Ed25519, OpenSSH e PKCS #8. • È stata aggiunta la raccolta di indirizzi di rete privati per acquisire le connessioni da e verso gli indirizzi IP privati RFC 1918 non presenti nell'inventario rilevato. • Sono state aggiunte opzioni di esportazione per selezionare un intervallo di date personalizzato e scegliere quali moduli di dati includere nell'esportazione. Miglioramenti • Maggiore affidabilità della raccolta programmata grazie alla suddivisione delle tempistiche dei raccoglitori. • Prestazioni di raccolta delle metriche del sistema operativo migliorate tramite il batching dei comandi SSH. • Le modifiche alle credenziali ora riprovano immediatamente i server precedentemente guasti. • La raccolta di metriche del sistema operativo ora riporta lo stato parziale quando alcuni comandi restituiscono risultati vuoti. • Migliore visibilità degli errori per i problemi di connessione vCenter nella dashboard.

Data	Versione	Note di rilascio
7 aprile 2026	1,0,1074	Nuove funzionalità • È stato aggiunto il supporto per Microsoft Hyper-V Discovery, incluso il rilevamento automatico delle VM dagli Hyper-V host con deduplicazione dei cluster di failover. • È stato aggiunto il supporto per l'importazione di server tramite caricamento di file CSV. • È stata aggiunta la raccolta di parametri del sistema operativo con sei moduli indipendenti: prestazioni del server, prestazioni di archiviazione, provisioning dei server, provisioning dello storage, interfacce di rete e processi in esecuzione. • È stata aggiunta Hyper-V l'opzione di distribuzione utilizzando un file di immagine VHD. • Migliore rafforzamento della sicurezza locale rimuovendo EC2-specific i servizi e bloccando l'accesso all'endpoint dei metadati dell'istanza.
26 marzo 2026	1.0.1014	Correzioni di bug e miglioramenti • È stata spostata la convalida delle maiuscole dei domini Kerberos dal backend al frontend. • È passato da a e ha impostato la cache basata su file Python-kerberos come impostazione predefinita. Python-pykerberos • Risolto il problema di convalida dell'ID del server di modifica in blocco senza distinzione tra maiuscole e minuscole. • Nome file ZIP di esportazione fisso (ora). <code>discovery_tool_export.zip</code> • Servizio fisso che eseguiva il controllo e aggiunti registri di debug per le credenziali di sistema. • Aggiunto uno script di configurazione di rete per creare artefatti.

Data	Versione	Note di rilascio
16 dicembre 2025	1.0.718	Nuove funzionalità e miglioramenti • È stato aggiunto il supporto SMBIOS UUID per impedire la duplicazione delle VM nei servizi downstream. • Sono state introdotte le Min/Max/Avg metriche di tracciamento e di archiviazione ampliate per un migliore monitoraggio delle risorse. • Aggiunti miglioramenti alla convalida delle API. • Aggiunta la funzionalità del pannello di aiuto con guida contestuale. • Terminologia aggiornata da «raccoglitore» a «strumento» in tutta l'interfaccia.
31 ottobre 2025	1.0.0	Versione iniziale Lancio iniziale dello strumento di AWS Transform scoperta. Questa versione include: • Raccolta offline (nessuna dipendenza da un AWS account o da Application Discovery Service). • Individuazione e monitoraggio di VMware. • Individuazione del database SQL Server. • Server-to-server raccolta delle comunicazioni tramite SSH, WMI e SNMP.

AWS Connettori Transform

AWS I connettori Transform consentono di accedere in modo sicuro alle risorse oltre i confini degli account per i flussi di lavoro di migrazione e modernizzazione. Ciò consente di accedere e gestire le risorse oltre i confini dell'account, mantenendo al contempo i controlli e le autorizzazioni di sicurezza. Un connettore rappresenta una connessione tra l'account di AWS Transform-enabled origine e le risorse esterne negli account di AWS destinazione o nei sistemi di terze parti.

I connettori richiedono richieste di accesso dal connettore di origine e l'approvazione del proprietario dell'account di destinazione. Questa richiesta viene effettuata quando si configura un connettore di origine. Allo stesso modo, potresti ricevere richieste di approvazione dei connettori di destinazione per consentire ad altri account di accedere al tuo account.

- Creazione di connettori: crea connettori nel tuo account di AWS Transform-enabled origine, specificando l'account di destinazione e le autorizzazioni richieste
- Configurazione delle autorizzazioni: AWS Transform richiede ruoli e autorizzazioni IAM specifici nell'account di destinazione per eseguire azioni di migrazione, tra cui:
 - Gestione dei dati di migrazione con AWS KMS
 - Effettuare chiamate API interregionali
 - Installazione di agenti di replica su server VMware
 - Creazione di un'infrastruttura di rete (VPC, sottoreti, routing)
 - Avvio di istanze Amazon EC2 e distribuzione di stack CloudFormation
 - Esecuzione di flussi di lavoro di migrazione tramite Migration Hub
- Processo di approvazione: è necessario approvare le richieste del connettore di destinazione prima che AWS Transform possa accedere alle risorse.
- Connessione attiva: una volta approvato, un connettore consente a AWS Transform Jobs di accedere e gestire in modo sicuro le risorse nell'account di destinazione.

Tracciabilità degli utenti per le operazioni agentiche

Per impostazione predefinita, AWS CloudTrail registra le azioni dell'agente sulle AWS risorse nell'identità del AWS servizio Transform. La tracciabilità degli utenti attribuisce tali azioni all'utente specifico di AWS IAM Identity Center che ha avviato o interagito con il job, permettendo il controllo di sicurezza e l'indagine sugli incidenti a livello di singolo utente.

 Note

La tracciabilità degli utenti è supportata solo per gli utenti di IAM Identity Center (IDC).

Per abilitare la tracciabilità degli utenti, abilita la sessione in background nelle impostazioni del profilo Transform. AWS. Se abilitato, AWS Transform crea automaticamente una [sessione in background](#) di IAM Identity Center quando interagisci con un job e la utilizza per produrre sessioni di ruolo IAM con identità migliorata per le operazioni dei connettori. Queste sessioni incorporano l'identità dell'utente nelle chiamate di servizio e negli eventi a valle AWS. AWS CloudTrail. Quando le sessioni in background sono disabilitate, AWS Transform torna alle sessioni standard con ruolo assunto senza il contesto dell'identità dell'utente.

I nuovi connettori vengono configurati automaticamente per supportare la tracciabilità degli utenti. Per i connettori esistenti, è necessario aggiungere manualmente `sts:SetContext` alla politica di attendibilità del ruolo del connettore:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": ["transform.amazonaws.com"] },
      "Action": ["sts:AssumeRole", "sts:SetContext"],
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "your-account-id" }
      }
    }
  ]
}
```

È possibile visualizzare e revocare le sessioni in background attive dalla scheda Sessioni in background nella pagina del lavoro. La revoca di una sessione invalida immediatamente la sessione stessa e tutte le sessioni di connessione da essa derivate.

Per ulteriori informazioni, consulta la [panoramica sulla propagazione delle identità affidabili](#) nella Guida per l'utente di AWS IAM Identity Center.

Gestione dei connettori

Nella pagina Connettori puoi vedere:

- Scheda Connettori di origine: elenca tutti i connettori che hai creato per connetterti ad altri account, mostrando gli account di destinazione e lo stato dei connettori
- Scheda Destination Connectors: mostra le richieste di connettori in entrata da altri account che desiderano accedere alle tue risorse e che richiedono la tua approvazione o il tuo rifiuto

AWS Transform richiede la conferma di azioni critiche come l'approvazione, il rifiuto o l'eliminazione dei connettori, per evitare modifiche accidentali che potrebbero interrompere i flussi di lavoro di migrazione attiva.

Per creare un connettore

1. Vai alla scheda Source Connectors.
2. Specificare l'account e il tipo di risorsa di destinazione.
3. Configura le autorizzazioni e l'ambito di accesso richiesti.

Per configurare le autorizzazioni

1. Scegli di creare un nuovo ruolo IAM con le autorizzazioni richieste oppure
2. Seleziona un ruolo esistente che hai creato in precedenza per i connettori.
3. Assicurati che il ruolo disponga di tutte le autorizzazioni necessarie per le operazioni di AWS trasformazione.

Per gestire le richieste in arrivo

1. Rivedi le richieste dei connettori nella scheda Connettori di destinazione.
2. Approva le richieste legittime per abilitare l'accesso tra più account.
3. Rifiuta i tentativi di connessione non autorizzati o non necessari.

Per gestire i connettori

1. Monitora i connettori attivi per motivi di sicurezza e conformità.

2. Elimina i connettori quando non ti servono più. Tieni presente che ciò causerà l'interruzione dei lavori in esecuzione utilizzando il connettore.
3. Aggiorna le autorizzazioni man mano che i requisiti cambiano.

Migrazioni (incluso VMware)

AWS Transform può aiutarti a migrare i tuoi ambienti server virtuali e bare metal su Amazon EC2 utilizzando l'intelligenza artificiale generativa, incluso Hyper-V VMware, e altre fonti. Questo capitolo fornisce una panoramica delle funzionalità di migrazione di AWS Transform e del flusso di lavoro del processo di migrazione.

Funzionalità e caratteristiche principali

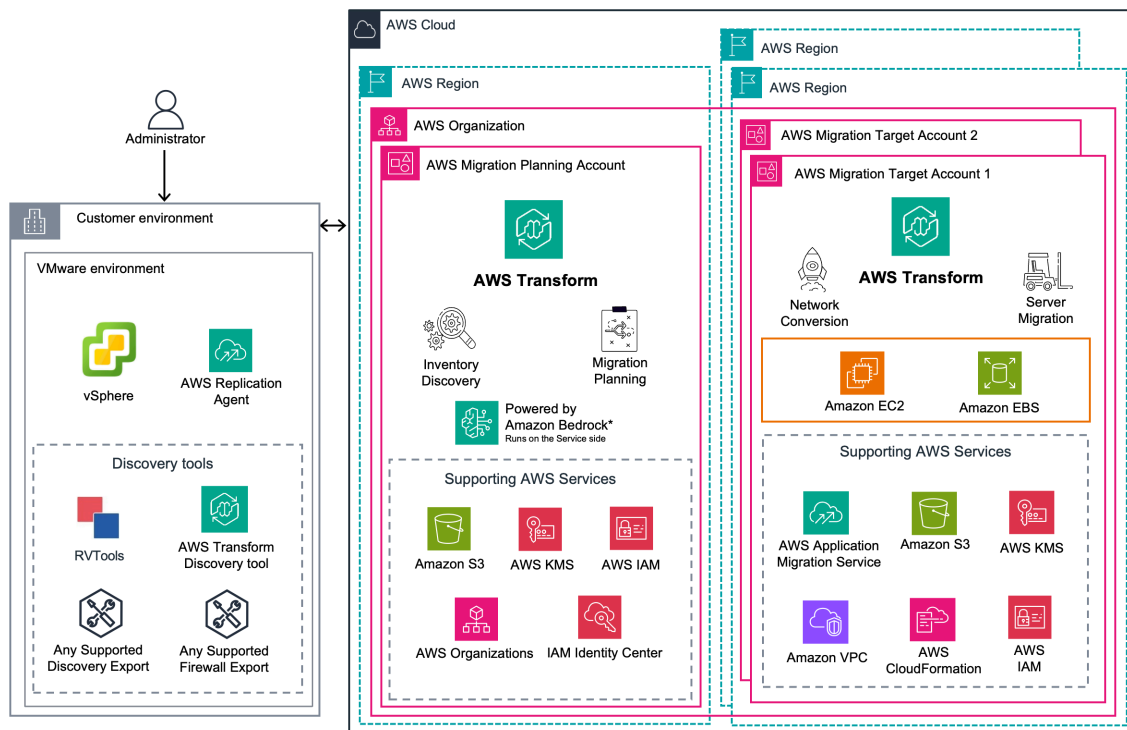
AWS Transform offre le seguenti funzionalità e caratteristiche chiave per la migrazione degli ambienti server verso AWS.

- Molteplici opzioni di rilevamento:
 - Individuazione assistita dell'ambiente VMware utilizzando i raccoglitori di AWS Application Discovery Service
 - Utilizza lo strumento open source [Export for vCenter](#) (ambienti VMware).
 - Importazione di dati di discovery raccolti in modo indipendente (qualsiasi ambiente di origine).
- AI-driven conversione della configurazione della rete di origine in un'architettura di rete Amazon VPC.
- AI-driven generazione di piani di migrazione, incluso il raggruppamento delle applicazioni e le ondate di migrazione suggerite.
- Rehosting dei server per l'esecuzione nativa su Amazon EC2.
- Interfaccia applicativa web localizzata, che consente di utilizzare AWS Transform per le migrazioni nella lingua preferita. Per ulteriori informazioni, consulta [Impostazioni della lingua](#).

AWS Transform supporta la migrazione dei server Windows e Linux dei sistemi operativi supportati. Per l'elenco completo dei sistemi operativi supportati, consulta [Sistemi operativi supportati](#) nella Guida per l'AWS Transform MGN utente.

AWS Trasforma l'architettura di migrazione

Questo diagramma mostra una panoramica dell'architettura di migrazione AWS Transform.



Lavori di migrazione

Per utilizzare AWS Transform for migrations, è innanzitutto necessario uno spazio di lavoro, che è un contenitore logico in cui è possibile creare uno o più processi di trasformazione. Le sezioni di questo argomento descrivono come ottenere uno spazio di lavoro e come creare e avviare un processo di migrazione al suo interno.

Ottenere uno spazio di lavoro

Per informazioni su come ottenere uno spazio di lavoro, vedi [Guida introduttiva](#).

L'area di lavoro che utilizzi determina il Regione AWS luogo in cui puoi creare lavori di trasformazione. È Regione AWS lì che risiederanno i tuoi lavori. In questo rientreranno anche i tuoi dati di scoperta e i consigli di AWS Transform. Regione AWS Per creare spazi di lavoro e lavori in un altro modo Regione AWS, chiedi all'amministratore di creare uno spazio di lavoro diverso per te. Per informazioni sull'assistenza Regioni AWS, consulta. [Regioni supportate](#)

Anche se il Regione AWS luogo in cui è possibile creare lavori e archiviare i dati e i consigli di discovery è determinato dall'amministratore di AWS Transform, è possibile specificare un obiettivo

diverso Regione AWS come destinazione per la migrazione. In altre parole, puoi eseguire il discovery e ricevere i consigli di AWS Transform in uno Regione AWS, ma poi creare l'ambiente di destinazione in un altro Regione AWS. Se lo fai, trasferirai i tuoi dati da un'altra parte Regioni AWS. Per ulteriori informazioni, consulta [the section called “Connect target Account AWS s e regioni”](#).

Tipi di Job

AWS Transform offre i seguenti tipi di lavori di migrazione tra cui è possibile scegliere in base alle proprie esigenze di migrazione. Oltre a queste opzioni preimpostate, puoi aggiungere o rimuovere dinamicamente qualsiasi fase del tuo lavoro in qualsiasi momento per personalizzare il flusso di lavoro di migrazione.

End-to-end migrazione

1. Esegui il rilevamento
2. Crea un piano di migrazione
3. Connect account target
4. Costruisci una landing zone
5. Migrazione della rete
6. Migrazione dei server

Pianificazione dell'individuazione e della migrazione

1. Esegui il rilevamento
2. Crea un piano di migrazione

Migrazione della rete

1. Connect account target
2. Migrazione della rete

Zona di atterraggio

1. Connect account target
2. Costruisci una landing zone

Migrazione di zone di atterraggio, rete e server

1. Connect account target
2. Costruisci una landing zone
3. Migrazione della rete
4. Migrazione dei server

Pianificazione della migrazione e migrazione dei server

Include discovery, wave plan e rehost.

1. Esegui la scoperta
2. Crea un piano di migrazione
3. Connect account target
4. Migrazione dei server

Creazione e avvio di un lavoro

Il primo passo di un progetto di migrazione consiste nel creare un lavoro AWS Transform. Per i progetti di migrazione, puoi scegliere diversi tipi di lavoro, a seconda dei tuoi obiettivi. La procedura seguente descrive come creare e avviare un nuovo processo di migrazione di qualsiasi tipo. Per informazioni sui diversi tipi di job, vedere [the section called “Tipi di Job”](#).

Per creare e avviare un nuovo processo di migrazione

1. Nella pagina di destinazione del tuo spazio di lavoro, scegli Crea un lavoro.
2. Scegli l'opzione di migrazione, quindi specifica il tipo di processo di migrazione che desideri creare. Per informazioni sui passaggi inclusi in ogni tipo di processo di migrazione, consulta [the section called “Tipi di Job”](#).
3. Dopo aver risposto a tutte le domande della chat, scegli Crea lavoro.

Scaricare un rapporto di riepilogo sull'area di lavoro

Puoi generare un rapporto di riepilogo sull'area di lavoro come PDF scaricabile in qualsiasi momento durante la migrazione. Il rapporto fornisce una visione consolidata di tutti i processi di migrazione

nell'area di lavoro, inclusi lo stato dei lavori e le fasi correnti del flusso di lavoro, le azioni e le approvazioni degli utenti, i dettagli della pianificazione delle ondate, la topologia della migrazione della rete, la configurazione delle landing zone, l'avanzamento del rehosting, le decisioni sulla containerizzazione e gli elementi chiave prodotti. Per generare un rapporto, chiedi all'agente nella chat un riepilogo dell'area di lavoro, ad esempio «Dammi un riepilogo dell'area di lavoro dei miei progressi di migrazione tra tutti i lavori». L'agente compila i dati di tutti i lavori e consegna il PDF direttamente nella chat come file scaricabile. Puoi utilizzare questo rapporto per tenere traccia dei progressi complessivi della migrazione o condividere lo stato con le parti interessate.

Limitazioni

AWS Transform presenta le seguenti limitazioni:

- Se interrompi un processo di migrazione in esecuzione e poi chiedi all'agente di riavviarlo, il processo riprenderà dall'inizio e perderai tutti i progressi compiuti nel processo. Tuttavia, gli artefatti creati nel processo prima del riavvio saranno ancora disponibili.
- È possibile specificare una destinazione Regione AWS per processo di migrazione. Per migrare le applicazioni in diverse regioni di destinazione, crea più processi di migrazione.
- Multi-account migrazione — Solo una regione — È possibile migrare verso più account all'interno di un'unica regione. Regione AWS Per le migrazioni multiregionali, è necessario creare progetti separati per ciascuna regione di destinazione.
- Multi-account migrazione: un account per ondata: ogni ondata di migrazione può essere indirizzata a un solo account. Le applicazioni che richiedono account target diversi devono essere inserite in ondate separate.
- Multi-account migrazione — AWS Organizzazioni richieste — Tutti gli account di destinazione devono far parte di un' AWS organizzazione.

Scopri i dati di origine

Per scoprire e raccogliere dati in locale, puoi utilizzare [lo strumento di rilevamento AWS Transform](#), il collettore AWS Migration Evaluator o caricare esportazioni da RVTools e ModelizeIT, nonché esportazioni in formato AWS Migration Portfolio Assessment (MPA) generate da strumenti come Cloudamize. AWS Transform può elaborare le esportazioni degli strumenti di rilevamento AWS Transform come file CSV e JSON in un formato di file ZIP, le esportazioni di RVTools come file Excel o file ZIP contenente file CSV e le esportazioni CSV di ModelizeIT in un file ZIP. Per ogni fonte di dati Transform accetta singolarmente il file del server principale. AWS Tuttavia, i file supplementari come

le connessioni verranno elaborati solo quando sono inclusi in un file ZIP con i file del server o in un file Excel con il foglio del server.

Ti consigliamo di caricare i dati più dettagliati disponibili e di rivedere i file di esportazione prima di caricarli per garantire la completezza e l'accuratezza dei dati. Verifica che tutti i file richiesti siano inclusi nel caricamento e verifica che i dati riflettano lo stato attuale dell'ambiente. Questa revisione preliminare aiuta a ridurre al minimo la necessità di ricaricamenti e garantisce che AWS Transform possa acquisire con maggiore precisione l'ambiente locale e supportare meglio la pianificazione della migrazione, compresi il raggruppamento delle applicazioni e la pianificazione a ondate. È inoltre possibile aggiungere dati in modo incrementale man mano che si ottengono dati migliori.

AWS Transform rileva automaticamente il formato e la struttura dei file, analizza ed estrae i record delle entità strutturate, rimuove i duplicati su più file, convalida la qualità dei dati e segnala i problemi, quindi prepara un riepilogo pronto per la pianificazione della migrazione a valle.

Dopo aver condiviso e confermato i dati locali, puoi rivedere i dati di discovery espandendo Discover on-premises data nel Job Plan e selezionando Inventory readiness summary. Puoi anche porre domande sui dati che hai caricato per verificare che AWS Transform abbia ingerito tutto correttamente o per identificare e correggere eventuali errori nell'elaborazione dei dati. Ad esempio, puoi chiedere informazioni sul sistema operativo e sulle versioni. Se devi correggere gli errori, puoi caricare nuovamente i dati di inventario dallo strumento di rilevamento che hai utilizzato e AWS Transform elaborerà, deduplicherà e unirà automaticamente i record aggiornati. Puoi anche rimuovere un file caricato in precedenza se non desideri più utilizzare quei dati di inventario.

Crea un piano di migrazione

La fase di pianificazione della migrazione all'interno di AWS Transform for VMware è un'esperienza collaborativa basata su chat per la pianificazione di migrazioni di grandi dimensioni. AWS Gli agenti di Transform applicano AWS Prescriptive Guidance per guidare i clienti dall'analisi dei dati locali ai piani di migrazione finalizzati.

Una volta completato con successo il processo Discover on-premises Data, AWS Transform utilizza i dati di discovery per raggruppare le applicazioni in ondate di migrazione. AWS Transform ti guida attraverso i passaggi per analizzare e definire l'ambito dei server, raggrupparli in applicazioni, generare gruppi di spostamenti e creare ondate di migrazione. Quando si analizza l'ambiente locale, è possibile porre domande per comprendere meglio in che modo AWS Transform ha analizzato il software installato, ad esempio le dipendenze dei server e l'architettura di rete.

AWS Transform supporta la regolazione dell'ambito all'interno di gruppi di applicazioni e ondate. Puoi ricaricare i dati di discovery in qualsiasi momento e AWS Transform elaborerà, deduplicherà e unirà automaticamente i nuovi record con i dati esistenti. Quando vengono rilevate modifiche, ad esempio dipendenze scoperte di recente o aggiunte all'infrastruttura, AWS Transform contrassegnerà i gruppi di dipendenze interessati e fornirà consigli per gli aggiustamenti del piano d'ondata. La pianificazione della migrazione può anche utilizzare dati di testo non strutturati per arricchire il processo di pianificazione.

Esistono quattro fasi di pianificazione della migrazione:

- In **Scope and analyze**, è possibile esaminare i dati di discovery, porre domande sul software e sull'ambiente di rete e determinare le risorse da migrare.
- Nelle **app di gruppo**, puoi fornire una combinazione di regole aziendali e tecniche riguardanti, ad esempio, l'analisi dei nomi host, le dipendenze di rete e le regole aziendali, in modo che la pianificazione della migrazione possa raggruppare l'infrastruttura in applicazioni. Se disponi già di un inventario delle tue applicazioni, la pianificazione della migrazione può invece utilizzarlo.
- In **Generate move groups**, puoi indicare alla pianificazione della migrazione i requisiti tecnici e aziendali in modo che possa determinare quali applicazioni devono essere spostate insieme. Le dipendenze tecniche includono database, code di messaggi o altre risorse condivise tra più app. Le dipendenze aziendali e operative includono la criticità aziendale, l'RPO e l'RTO, la posizione del data center e i proprietari delle applicazioni.
- Infine, in **Build waves**, puoi fornire un contesto alla pianificazione della migrazione in merito alle tempistiche e alle priorità in modo che possa creare un piano ondato da migrare. È possibile selezionare i gruppi di spostamento da includere in un'ondata in base a fattori quali il punteggio di priorità, la dimensione del gruppo di spostamento, il numero di utenti e la complessità dell'applicazione.

Terminologia della pianificazione della migrazione:

- Le ondate di migrazione sono gruppi logici che vengono migrati insieme. Le ondate migratorie sono costituite da uno o più gruppi di movimenti.
- Un **move group** è un insieme di applicazioni co-dipendenti che devono essere spostate insieme. Possono avere dipendenze tecniche, come un database condiviso, o dipendenze aziendali, come il supporto di una funzione aziendale condivisa.
- Una **dipendenza** è una relazione tra sistemi. Esistono diversi tipi di dipendenze, tra cui:

- Dipendenze critiche o rigide, in cui i sistemi non possono funzionare senza la dipendenza. Esempi comuni di ciò sono le applicazioni che dipendono da database, altre applicazioni o servizi.
- Dipendenze morbide, che non sono fondamentali per il funzionamento del sistema. Tra gli esempi più comuni vi sono le dipendenze insensibili alla latenza che possono essere migrate indipendentemente.
- Non-technical le dipendenze includono le dipendenze aziendali, organizzative, operative e di conformità. Si tratta di dipendenze legate all'organizzazione e alle sue priorità. Esempi di ciò includono la funzione aziendale condivisa e la proprietà organizzativa.

Flusso di lavoro

La pianificazione della migrazione è un flusso di lavoro interattivo e iterativo. Puoi tornare indietro e apportare modifiche ai passaggi precedenti in qualsiasi momento. Un tipico flusso di lavoro di pianificazione della migrazione è:

1. La pianificazione della migrazione inizia con il riepilogo dei dati di scoperta disponibili. Esamina i dati disponibili e torna alla fase di scoperta in qualsiasi momento per fornire dati aggiuntivi.
2. Nella fase di definizione e analisi, puoi porre domande sull'ambiente locale per convalidare i dati raccolti. Le domande di esempio includono:
 - a. Elenca i miei server per sistema operativo
 - b. Riassumi la mia topologia di rete locale
 - c. Elenca le tecnologie più comuni in esecuzione nel mio ambiente.
3. Durante l'analisi dell'ambiente, se identifichi server che non dovrebbero rientrare nell'ambito della migrazione, puoi dire a AWS Transform di escludere tali risorse. Esempi di questo tipo includono:
 - a. Rimuovi tutti i server che hanno un nome host legacy
 - b. Rimuovi tutti i server nella versione 10.0.2. 0/24 sottorete
 - c. Rimuovi tutti i server che eseguono versioni di Windows precedenti al 2022
4. Dopo aver esplorato a fondo l'ambiente e determinato l'ambito della migrazione, puoi dire a AWS Transform di passare alla fase successiva di pianificazione della migrazione.
5. Il passaggio successivo è il raggruppamento delle applicazioni. Se i server sono già mappati alle applicazioni, puoi dire a AWS Transform di utilizzare quella mappatura e saltare questo passaggio. Se le applicazioni non sono predefinite, è possibile fornire la logica tecnica e aziendale che definisce le applicazioni. AWS Transform vi guiderà attraverso il processo di raggruppamento delle

- applicazioni e vi suggerirà i punti dati che potete fornire per raggruppare efficacemente i server in applicazioni. Più informazioni puoi fornire sulle tue applicazioni locali, più efficacemente AWS Transform può raggruppare i tuoi server in app. Dopo aver fornito informazioni sufficienti, puoi indicare a AWS Transform di eseguire il raggruppamento delle applicazioni.
6. Una volta eseguito il raggruppamento delle applicazioni, esaminate i gruppi di applicazioni. È possibile indicare a AWS Transform di apportare le modifiche necessarie, ad esempio:
 - a. Sposta server example-server su application-5
 - b. Rinomina l'applicazione-5 «HR App Test Environment»
 - c. Rimuovi tutti i server Linux da IIS Dev Farm
 7. Una volta raggruppate le app, chiedi a AWS Transform di passare alla fase successiva
 8. Il passaggio successivo è spostare il raggruppamento. Nella fase di spostamento del raggruppamento si identificano le applicazioni che devono essere spostate insieme. Fornisci un contesto relativo alle tue dipendenze tecniche e non tecniche. AWS Transform ti guiderà attraverso il processo e ti suggerirà punti dati da fornire per raggruppare le tue app. Ci sono diverse considerazioni da fare in questa fase, tra cui:
 - a. Quale dovrebbe essere la dimensione target del gruppo di traslochi?
 - b. Vuoi combinare ambienti, ad esempio dev, test e prod, per ogni app o dividerli?
 - c. Come vuoi considerare le dipendenze di rete? Tutte le dipendenze sono fondamentali o alcune dipendenze possono essere considerate dipendenze morbide ed essere suddivise tra gruppi di movimento?
 9. Dopo aver fornito le regole per il raggruppamento dei movimenti, chiedi a AWS Transform di eseguire la tua strategia di raggruppamento dei movimenti. È quindi possibile rivedere e modificare i gruppi di spostamenti. Dopo aver esaminato i gruppi di traslochi, potete indicare a AWS Transform di passare alla fase finale di pianificazione della migrazione.
 10. La pianificazione ondata è la fase finale della pianificazione della migrazione. In questa fase, raggruppate i vostri gruppi di traslochi in ondate di migrazione e date priorità a tali ondate. Nella fase di pianificazione delle ondate, AWS Transform vi guiderà nella definizione delle priorità aziendali necessarie per raggruppare i vostri gruppi di traslochi in ondate e poi dare priorità a tali ondate. Le considerazioni relative alla pianificazione delle ondate includono:
 - a. La criticità aziendale di ogni vostro gruppo di traslochi
 - b. Le tempistiche di migrazione e le tempistiche per ogni gruppo di trasloco
 - c. I rischi associati a ciascun gruppo di traslochi
 - d. Il numero di server da migrare per ondata

11. Dopo aver fornito indicazioni sufficienti su come raggruppare le ondate, chiedete a AWS Transform di eseguire la pianificazione delle ondate. È quindi possibile rivedere le onde e modificarle.
12. Una volta finalizzato il piano wave, puoi completare la pianificazione della migrazione e passare all'esecuzione. Puoi tornare alla pianificazione della migrazione in qualsiasi momento per perfezionare e perfezionare il tuo piano.
13. Per ogni ondata, puoi assegnare una strategia di migrazione: rehosting (migrazione dei server su Amazon EC2) e containerizzazione (containerizzazione del codice sorgente e distribuzione su Amazon Elastic Container Service o Amazon Elastic Kubernetes Service). Quando assegni a un'ondata la strategia containerizza, Transform esegue il flusso di lavoro di containerizzazione del codice sorgente per quell'ondata durante l'esecuzione della migrazione. AWS Per ulteriori informazioni, consulta [Containerizzazione del codice sorgente](#). Per conoscere le strategie AWS consigliate nel framework 7Rs prima di assegnarle, consulta [the section called “Raccomandazioni 7Rs”](#)

Raccomandazioni sulla strategia di migrazione (7R)

Durante la pianificazione della migrazione, AWS Transform può analizzare l'inventario rilevato e consigliare una strategia di migrazione, una delle 7R standard del settore, per ogni server e applicazione. Ogni raccomandazione include un servizio di AWS destinazione consigliato, un punteggio di affidabilità e il motivo alla base. Questo vi offre un punto di partenza sostenibile per il vostro piano d'ondata e offre opportunità di modernizzazione che altrimenti rischiereste di perdere.

Le sette strategie sono rehost, replatform, refactoring, repurchase, retire, retention e relocate. AWS Trasforma i segnali di lettura nei tuoi dati, come il sistema operativo, l'utilizzo e il tipo di carico di lavoro, per formulare consigli spiegabili. Ad esempio, può consigliare di ritirare i server inattivi o fuori uso, spostare SQL Server o database open source su Amazon RDS, spostare i carichi di lavoro di posta elettronica e collaborazione su Microsoft 365, conservare sistemi legacy specializzati e riospitare i carichi di lavoro rimanenti su Amazon EC2. I consigli vengono raggruppati dai singoli server alle applicazioni e all'intero portafoglio, con una visione delle criticità per strategia e riepiloghi a livello di ondata.

Per generare un rapporto sulla strategia di migrazione (7R):

1. Completa il passaggio Scopri i dati locali e raggruppa i server in applicazioni. Entrambi sono necessari affinché AWS Transform possa fornire consigli per server e per applicazione.
2. Nella chat sulla pianificazione della migrazione, chiedi a AWS Transform un rapporto sulla strategia di migrazione (7R), ad esempio Genera un rapporto. R-strategy Una volta completato

il raggruppamento delle applicazioni, AWS Transform offre anche la possibilità di generare il rapporto per te.

3. AWS Transform analizza il vostro inventario, applica il framework 7Rs e genera il report. Puoi fornire dettagli come il nome dell'organizzazione ed eventuali filtri per l'ambito dell'analisi.
4. Esamina i consigli. Per modificare un consiglio, comunica a AWS Transform nella chat: modifica un singolo server o applicazione o applica una modifica in blocco (ad esempio, in base al sistema operativo, all'ambiente, all'ondata o alla priorità). AWS Transform aggiorna il rapporto con le modifiche apportate.

Per impostazione predefinita, AWS Transform produce una dashboard HTML interattiva che puoi filtrare ed esplorare. Su richiesta, puoi anche generare un documento PDF da condividere con le parti interessate o una presentazione Microsoft PowerPoint (PPTX) da presentare; il PDF e PowerPoint gli output sono istantanee point-in-time della stessa analisi. Il rapporto include una strategia e un servizio AWS mirato consigliati per ogni server e applicazione, punteggi di affidabilità e ragionamenti, opportunità di modernizzazione evidenziate, una panoramica delle criticità per strategia, riepiloghi a livello di ondata e indicatori di rischio.

La strategia consigliata in questo rapporto integra la strategia per ondata assegnata durante la pianificazione a ondata. Per la containerizzazione del codice sorgente, consulta [Containerizzazione del codice sorgente](#)

Creazione di diagrammi e creazione di report

Durante la pianificazione della migrazione, AWS Transform trasforma l'inventario e i risultati della pianificazione rilevati in diagrammi visivi e report analitici. Li generi in modo colloquiale nella chat di pianificazione, ad esempio «Mostrami un diagramma della topologia di rete» o «Genera un rapporto sui rischi». AWS Transform li crea a partire dai dati che hai già fornito, senza alcuna configurazione richiesta.

I diagrammi sono interattivi e consentono di esplorare visivamente l'ambiente. I diagrammi disponibili includono:

- Topologia di rete: una mappa interattiva dei server e delle relative relazioni di rete, progettata per adattarsi a grandi ambienti con migliaia di nodi.
- Dipendenza dalle applicazioni: relazioni dirette tra applicazioni derivate dalle connessioni di rete osservate.

- Diagramma di Wave Gantt: una visualizzazione temporale delle ondate di migrazione che mostra pianificazioni, dipendenze, tappe fondamentali e progressi (disponibile dopo la pianificazione ondata).
- Grafici generali: grafici a torta, grafici a barre, istogrammi, mappe ad albero e tabelle di riepilogo con le dimensioni dei dati che scegli.

I report forniscono analisi narrative e consigli sui dati di migrazione. I report disponibili includono:

- Valutazione del rischio: assegna un punteggio a ciascuna applicazione in base alla complessità tecnica, al rischio di dipendenza, alla preparazione alla migrazione e al rischio operativo, con riepiloghi per applicazione, per ondata e a livello di portafoglio.
- Strategia di migrazione (7R) e raccomandazioni sulla strategia per applicazione. Per-server Per ulteriori informazioni, consulta [the section called “Raccomandazioni 7Rs”](#).
- Report generali e personalizzati: report analitici per richieste quali riepiloghi sulla preparazione dei dirigenti, compromessi tra costi e rischi e valutazioni dei candidati alla containerizzazione.

Alcuni risultati dipendono dalla fase di pianificazione. Ad esempio, i diagrammi delle dipendenze delle applicazioni utilizzano i dati della connessione di rete. Il diagramma di Gantt delle onde e i riepiloghi dei report a livello d'onda diventano disponibili dopo il completamento della pianificazione delle ondate. Se manca un prerequisito, AWS Transform indica cosa è necessario e può eseguire prima il passaggio richiesto.

AWS Transform fornisce diagrammi in formato HTML interattivo che puoi filtrare ed esplorare. Per impostazione predefinita, AWS Transform fornisce i report come file HTML autonomo. Su richiesta, AWS Transform può anche generare un documento PDF da condividere con le parti interessate o una presentazione Microsoft PowerPoint (PPTX) da presentare. Il PDF e PowerPoint gli output sono istantanee temporali della stessa analisi.

Connect target Account AWS s e regioni

Configura il Account AWS connettore di destinazione per la migrazione di rete, la creazione di landing zone e la migrazione dei server. Ciò prevede tre passaggi: selezionare il tipo di migrazione, fornire i dettagli del contratto MAP (se applicabile) e configurare il connettore. Queste impostazioni si applicano a tutte le fasi della migrazione: migrazione di rete, landing zone e rehosting del server.

Fase 1: Selezione del tipo di migrazione

Scegli se stai eseguendo una migrazione con account singolo o multiplo:

- **Single-account migrazione:** tutti i carichi di lavoro migrano verso un unico obiettivo. Account AWS L'account di destinazione del connettore e l'account di destinazione sono gli stessi.
- **Multi-account migrazione:** i carichi di lavoro migrano verso diversi account di destinazione. Il connettore deve essere collegato all'account di gestione dell'organizzazione o a un account di amministratore delegato (DA) registrato per entrambi e. AWS Transform MGN CloudFormation StackSets

Fase 2: accordo MAP

Se la migrazione fa parte del AWS Migration Acceleration Program (MAP 2.0), fornisci il tuo ID Migration Portfolio Experience (MPE), un codice di 10 caratteri che utilizza lettere e cifre maiuscole (ad esempio, ABCDE12345). Quando fornisci il tuo ID MPE, il tag MAP viene applicato a tutte le risorse create durante le fasi di migrazione di rete, landing zone e rehosting del server. Il formato del tag è:

- Chiave: map-migrated Valore: migMPE_ID

È necessario applicare i tag MAP per ricevere il credito MAP. Per ulteriori informazioni su MAP, vedere [AWS Migration Acceleration Program](#).

Fase 3: Configurazione del connettore

Utilizzi il connettore dell'account di destinazione per connettere il processo di migrazione all' AWS ambiente in cui risiederanno i carichi di lavoro dopo la migrazione. Prima di iniziare, verifica che la destinazione Account AWS disponga delle autorizzazioni, delle quote e delle configurazioni necessarie per supportare l'infrastruttura migrata.

Quando approvi la richiesta del connettore, concedi le autorizzazioni Transform a: AWS

- Gestisci le operazioni con i bucket di Amazon S3 (read/write) per la migrazione a VMware, oltre all'accesso a Migration Hub e AWS Application AWS Migration Service (MGN). Ciò include le autorizzazioni per i seguenti elementi, tutte limitate alle risorse dell'account di destinazione contrassegnate con o: CreatedBy:AWSTransform CreatedFor:AWSTransform

- Gestisci le ondate di migrazione.
- Gestisci le configurazioni di rete (Amazon EC2, VPC, Transit Gateway, Direct Connect, Load Balancers, Network Firewall).
- CloudFormation Gestisci le implementazioni degli stack.
- Esegui installazioni automatiche degli agenti tramite Systems Manager.
- Esegui la migrazione dei carichi di lavoro locali verso la destinazione Account AWS e la regione utilizzando le informazioni archiviate nella regione di scoperta.
- Fornitura e gestione dell'infrastruttura delle landing zone nell'obiettivo Account AWS e nella regione. Ciò include le autorizzazioni per i seguenti elementi, limitate alle risorse contrassegnate con, `CreatedBy:AWSTransform` ove applicabile:
 - Esegui operazioni sui bucket Amazon S3 (creazione, lettura, scrittura, eliminazione) per i bucket che iniziano con `transform-vmware-landing-zone-`
 - Gestisci le distribuzioni degli CloudFormation stack e modifica i set per gli stack delle landing zone.
 - Esegui le operazioni AWS del Control Tower. È possibile gestire le zone di atterraggio, abilitare le linee di base e abilitare i controlli.
 - Gestisci AWS le organizzazioni. È possibile creare e gestire unità organizzative, creare account e spostare account.
 - Gestisci le policy di controllo dei servizi (SCP) tramite AWS Control Tower.
 - Gestisci gli artefatti di provisioning del AWS Service Catalog.

Note

I tipi di connettori potrebbero essere aggiornati quando le nuove funzionalità richiedono modifiche alle autorizzazioni. La versione attuale per il tipo di connettore dell'account di destinazione è 2.0. Quando si crea un nuovo connettore, viene utilizzata la versione più recente.

Prima di configurare il connettore, scopri i ruoli degli account coinvolti nella migrazione:

Account	Description
AWS Trasforma l'account	Qualsiasi account membro AWS dell'organizzazione in cui hai configurato AWS Transform. È qui che si trova l'area di lavoro AWS Transform. Non è necessario che sia l'account di gestione.
Account di destinazione del connettore	L'account su cui è configurato il connettore AWS Transform. Dipende dal tipo di migrazione: • Single-account migrazione: Connettiti all'account verso cui stai migrando i carichi di lavoro. L'account di destinazione del connettore e l'account di destinazione coincidono. • Multi-account migrazione: Connettiti all'account di gestione dell'organizzazione o a un account Delegated Administrator (DA). L'account DA deve essere registrato come amministratore delegato sia per MGN che per l'organizzazione CloudFormation StackSets. AWS Transform verifica se l'account collegato è l'account di gestione o un account DA e ne regola il comportamento di conseguenza.
Account Target	Il Account AWS luogo in cui vengono migrati i tuoi carichi di lavoro. In una migrazione con un solo account, è lo stesso dell'account di destinazione del connettore. In una migrazione con più account, questi sono gli account dei singoli membri che ricevono i carichi di lavoro migrati.

Utilizzo di un account amministratore delegato

Per le migrazioni con più account, si AWS consiglia di utilizzare un account Delegated Administrator (DA) anziché direttamente l'account di gestione dell'organizzazione. Un account DA segue il principio del privilegio minimo limitando l'ambito delle autorizzazioni richieste per le operazioni di migrazione. L'account DA deve essere registrato come amministratore delegato sia per MGN che per l'organizzazione. CloudFormation StackSets AWS

La differenza fondamentale tra le due opzioni è:

- Account di gestione: può consentire l'accesso affidabile per MGN e per CloudFormation StackSets tutta l'organizzazione. AWS Trasforma le CloudFormation StackSets API delle chiamate con. `CallAs: SELF`

- Account amministratore delegato: non è possibile abilitare direttamente l'accesso affidabile (operazione che deve essere eseguita dall'account di gestione), ma può gestire i server di origine MGN, avviare istanze e distribuire CloudFormation StackSets tra gli account dei membri. AWS Trasforma le API delle chiamate con CloudFormation StackSets CallAs: DELEGATED_ADMIN

Per ulteriori informazioni, vedere [Amministratore delegato per MGN nella Guida per l'utente di MGN](#).

Ruoli IAM creati durante la configurazione del connettore

Durante la configurazione del connettore, AWS Transform crea il seguente ruolo IAM nell'account di destinazione:

- `AWSTransform-Connector-role`— Creato quando configuri il connettore dell'account di destinazione, nell'account di gestione o nell'account amministratore delegato della tua AWS organizzazione. Questo ruolo consente a AWS Transform di connettersi all'account di destinazione e di agire per conto dell'utente per eseguire operazioni di migrazione.

Configurazione del connettore dell'account Target

Important

Durante la configurazione del connettore, viene creato un bucket Amazon S3 nella destinazione. Account AWS Per impostazione predefinita, questo bucket non imporrà HTTPS-only access (SecureTransport). Se desideri che la policy del bucket includa il trasporto sicuro, devi aggiornare tu stesso la policy. Per ulteriori informazioni, consulta [Best practice di sicurezza per Amazon S3](#).

Per utilizzare un connettore per account di destinazione esistente

1. Nel riquadro Job Plan, espandi Scegli account di destinazione, quindi scegli Crea o seleziona connettori.
2. Nella scheda Collaborazione, seleziona un connettore esistente, quindi scegli Usa connettore. Se un connettore non è disponibile, la sua versione non è compatibile con il tipo di lavoro selezionato.

 Important

Se specifichi un connettore con una destinazione Regione AWS diversa dalla regione di AWS trasformazione, AWS Transform trasferirà i tuoi dati Regioni AWS.

3. Scegli Continua.

Per creare un nuovo connettore

1. Nel riquadro Job Plan, espandi Connect target account, quindi scegli Crea o seleziona connettori.
2. Specificate la Account AWS e Regione AWS per il target, quindi scegliete Avanti.

 Important

Se la destinazione è Regione AWS diversa dalla scoperta Regione AWS, AWS Transform trasferirà i dati tra Regioni AWS di loro.

3. Scegli se utilizzare le chiavi gestite di Amazon S3 per la crittografia. Se specifichi la tua chiave KMS, puoi utilizzare la politica delle chiavi predefinita o una meno permissiva. Per informazioni sulla creazione di una chiave KMS, consulta [Creare una chiave KMS](#) nella Guida per gli sviluppatori. AWS Key Management Service

AWS Transform utilizza l'`kms:DescribeKey` autorizzazione per verificare l'esistenza della chiave e `kms:Decrypt` per crittografare `kms:GenerateDataKey` e decrittografare i dati di lavoro nel bucket Amazon S3. Per ulteriori informazioni, consulta [Ridurre il costo di SSE-KMS con Amazon S3 Bucket Keys](#).

4. Scegli Continua.
5. Copia il link di verifica, condividilo con un amministratore della destinazione Account AWS e chiedigli di approvare la richiesta di connessione.
6. Dopo che l'amministratore ha approvato la richiesta, seleziona il connettore appena creato dall'elenco e scegli Usa connettore.
7. Scegli Invia per AWS trasformare.

Se intendi modificare il AWS Transform MGN modello per abilitare le azioni post-lancio, aggiungi la seguente autorizzazione al ruolo del connettore di destinazione. Questa dichiarazione sulla politica JSON concede l'`iam:PassRole` autorizzazione per il ruolo delle azioni post-lancio. Puoi trovare il nome del ruolo nella scheda Collaborazione dopo la creazione del connettore. Per informazioni sull'aggiunta di autorizzazioni a un ruolo, consulta [Update permissions for a role](#) nella IAM User Guide.

```
{
  "Sid": "MGNPostLaunchActions",
  "Effect": "Allow",
  "Action": [
    "iam:PassRole"
  ],
  "Resource": "arn:aws:iam::target-account-ID:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
}
```

Regioni target supportate

Una regione di destinazione per la migrazione è quella Regione AWS in cui vengono distribuite le risorse migrate, comprese le zone di destinazione, l'infrastruttura di rete e il rehosting dei server. Quando crei il connettore, specifica una destinazione. Regione AWS È possibile utilizzare uno dei seguenti elementi Regioni AWS:

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Africa (Città del Capo)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Taipei)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Hyderabad)
- Asia Pacifico (Tokyo)
- Asia Pacifico (Seoul)
- Asia Pacifico (Osaka)

- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Melbourne)
- Asia Pacifico (Malesia)
- Asia Pacifico (Nuova Zelanda)
- Asia Pacifico (Thailandia)
- Canada (Centrale)
- Canada occidentale (Calgary)
- Europa (Francoforte)
- Europa (Zurigo)
- Europa (Irlanda)
- Europa (Londra)
- Europe (Paris)
- Europe (Stockholm)
- Europa (Milano)
- Europa (Spagna)
- Israele (Tel Aviv)
- Messico (centrale)
- Sud America (San Paolo)

 Important

Se specifichi una destinazione Regione AWS diversa dalla AWS Transform Regione AWS, alcuni dei tuoi dati vengono trasferiti. Regioni AWS

Tieni presente che i dati di replica del server passano direttamente dall'ambiente di origine all'account e alla regione di destinazione.

Costruisci una landing zone

AWS Transform ti guida nella progettazione e implementazione di una AWS landing zone come parte del tuo progetto di migrazione. Una landing zone è un AWS ambiente multi-account che funge da base per i carichi di lavoro con confini organizzativi, controlli di governance e struttura degli account in atto prima dell'arrivo dei carichi di lavoro. AWS Transform analizza l'inventario delle migrazioni e i requisiti aziendali per consigliare un'unità organizzativa (OU) e una struttura degli account, applicare le Service Control Policies (SCP) consigliate e generare la and/or distribuzione dell'infrastruttura come codice (IaC).

L'agente della landing zone ti guida attraverso due fasi:

- Configurazione della base: stabilisci la struttura principale della landing zone: AWS Control Tower, unità organizzative di base e account principali.
- Progettazione degli account per i carichi di lavoro: progetta e crea unità organizzative e account per i carichi di lavoro in base alle ondate di migrazione, alle unità aziendali e ai requisiti di separazione degli ambienti.

AWS Transform supporta sia ambienti greenfield (nessuna landing zone esistente) che ambienti brownfield (unità organizzative esistenti e account già distribuiti). Negli scenari dismessi, AWS Transform rileva la struttura organizzativa esistente e consiglia solo le modifiche necessarie per colmare le lacune rispetto alle best practice. AWS

Configurazione del connettore

L'agente di landing zone richiede un Account AWS connettore di destinazione per fornire risorse nell'account di gestione dell'organizzazione. Il connettore dispone delle autorizzazioni per:

- Configura [AWS Control Tower](#)
- Crea [unità organizzative e account](#)
- Configura [le politiche di controllo dei servizi \(SCP\)](#)

Quando approvi la richiesta del connettore, concedi le autorizzazioni AWS Transform a:

- Fornitura e gestione dell'infrastruttura delle landing zone nell'obiettivo Account AWS e nella regione. Ciò include le autorizzazioni per i seguenti elementi, limitate alle risorse contrassegnate con `CreatedBy:AWSTransform` e da `ATWorkspace:{workspace-id}` dove applicabile:

- Operazioni sui bucket S3 (creazione, lettura, scrittura, eliminazione) per i bucket che iniziano con `transform-vmware-landing-zone-`
- CloudFormation implementazioni degli stack e gestione dei set di modifiche per gli stack delle landing zone
- AWS Operazioni Control Tower (gestione delle zone di atterraggio, abilitazione delle linee di base e dei controlli)
- AWS Gestione delle [organizzazioni](#) (creazione e gestione di unità organizzative, creazione di account e trasferimento di account)
- Gestione della policy di controllo dei servizi (SCP) tramite AWS Control Tower
- [AWS Service Catalog](#): provisioning, gestione degli artefatti

Quando si crea il connettore, si specifica una destinazione. Regione AWS Questa regione deve essere la stessa della regione Control Tower della tua casa. Per ulteriori informazioni sulle regioni Control Tower, vedi [Come Regioni AWS lavorare con AWS Control Tower](#).

All'inizio della configurazione della landing zone, AWS Transform recupera la configurazione del connettore e presenta l'ID dell'account di gestione dell' AWS organizzazione e la regione di destinazione per la conferma. Per ulteriori informazioni, consulta [Connettori](#).

Important

Dipendenza dalla regione IAM Identity Center: AWS Transform richiede AWS IAM Identity Center (IAM Identity Center), il che significa che la regione del connettore deve corrispondere sia alla regione principale del AWS Control Tower che alla regione del centro di identità IAM. Se IAM Identity Center è già configurato nell'organizzazione, l'inizializzazione di AWS Control Tower avrà esito negativo se il connettore si rivolge a una regione diversa. Per ulteriori informazioni, consulta [Considerazioni per i clienti di IAM Identity Center](#) nella AWS Control Tower User Guide.

Configurazione Foundation

La fase di configurazione delle fondamenta stabilisce l'infrastruttura principale delle landing zone utilizzando [AWS Control Tower](#). Quando AWS Control Tower configura una landing zone, fornisce automaticamente una serie di risorse gestite nel tuo account di gestione che costituiscono la base di governance per l'intera AWS organizzazione:

- **Root:** l'elemento principale di primo livello che contiene tutte le unità organizzative presenti nella landing zone.
- **Security OU:** creata automaticamente da Control Tower. Contiene due account condivisi: l'account Log Archive (registrazione centralizzata e immutabile per tutte le attività delle AWS API e le modifiche delle risorse all'interno dell'organizzazione) e l'account Audit (accesso in sola lettura a tutti gli account per la verifica della sicurezza e della conformità). Questi account non possono essere rinominati o sostituiti dopo la configurazione iniziale.
- **Controlli obbligatori (guardrail):** Control Tower applica automaticamente controlli preventivi e investigativi in tutta l'organizzazione per applicare le politiche di governance di base. Questi non possono essere disabilitati.
- **Directory IAM Identity Center** — Control Tower crea una directory nativa per il cloud con gruppi preconfigurati e accesso Single Sign-On per gli utenti delle landing zone. [Per ulteriori informazioni, consulta IAM Identity Center.AWS](#)

Control Tower utilizza [CloudFormation StackSets](#) per distribuire e gestire queste risorse in modo coerente in tutti gli account e le regioni dell'organizzazione. Non devi modificare o eliminare le risorse gestite da Control Tower al di fuori dei metodi supportati, poiché così facendo la landing zone potrebbe entrare in uno stato sconosciuto.

Convenzione relativa alla posta elettronica dell'account

AWS richiede un indirizzo e-mail univoco per ogni account. Queste e-mail ricevono notifiche importanti per l'account. AWS Transform utilizza l'indirizzamento plus per generare email di account uniche da un'unica casella di posta.

Formato: `prefix+account-name@domain`

Fornisci un prefisso (ad esempio, `aws-admin`) e un dominio (ad esempio, `acme.com`) e AWS Transform ricava automaticamente tutte le email dell'account. Ad esempio:

- Account di controllo: `aws-admin+audit@acme.com`
- Account di archiviazione dei log: `aws-admin+log-archive@acme.com`
- Account Sandbox: `aws-admin+sandbox@acme.com`

Negli scenari dismessi, AWS Transform ispeziona le e-mail degli account esistenti per dedurre la convenzione plus-address già in uso e offre la possibilità di continuare con lo stesso schema.

Struttura di base consigliata

In base alle AWS best practice, AWS Transform consiglia la seguente struttura di unità organizzative di base. È possibile personalizzarlo prima della creazione.

OU	Scopo	Account
Sicurezza	Registrazione e monitoraggio centralizzati degli audit. L'isolamento di questi servizi in account dedicati è progettato per aiutare a mantenere l'audit trail separato dai team addetti al carico di lavoro.	Controllo, archiviazione dei registri
Infrastruttura	Rete condivisa (Transit Gateway, VPN), DNS e servizi comuni. Si consiglia di centralizzarli per ridurre la duplicazione e offrire al team di rete un unico posto per gestire la connettività.	Nessuno (creato vuoto)
Sandbox	Sperimentazione degli sviluppatori con limiti di spesa e accesso limitato. Consigliato per dare agli sviluppatori uno spazio per sperimentare senza rischiare le risorse di produzione.	Sandbox
Carichi di lavoro	Contiene unità organizzative secondarie di produzione e Non-Production, facoltativamente, regolamentate. Gli account per i carichi di lavoro vengono progettati nella fase successiva in base ai requisiti di migrazione.	Nessuno (creato vuoto)

Note

L'unità organizzativa di sicurezza con [account Audit e Log Archive](#) viene creata come parte della configurazione di base Control Tower. Le unità organizzative Infrastructure, Sandbox e Workloads vengono create separatamente dopo la conferma della struttura.

Negli scenari dismessi, AWS Transform confronta la base esistente con questa struttura consigliata e riporta solo le lacune. Ad esempio: «La tua fondazione dispone di unità organizzative per la sicurezza e l'infrastruttura ma nessuna unità organizzativa Sandbox».

Policy di controllo dei servizi (SCP)

Gli SCP sono [barriere di autorizzazione a livello di organizzazione che impostano le autorizzazioni](#) massime per tutti gli account dell'organizzazione. AWS Non concedono l'accesso, ma definiscono limiti che nessun membro dell'account può superare, nemmeno gli amministratori dell'account.

Come parte dell'implementazione del Control Tower, i guardrail di base vengono applicati automaticamente. AWS Transform consiglia inoltre SCP aggiuntivi progettati per contribuire a rafforzare la posizione dell'organizzazione. Questi si basano sulle AWS migliori pratiche per una landing zone minima praticabile.

Gli SCP possono essere applicati alle unità organizzative Infrastructure, Sandbox e Workloads. L'unità organizzativa di sicurezza è gestita da Control Tower e non può essere presa di mira dagli SCP tramite questo strumento.

Important

La Security OU è un'unità organizzativa di base gestita da Control Tower. Non puoi aggiungere account, SCP o risorse tramite l'agente della landing zone.

Negli scenari dismessi, AWS Transform verifica quali SCP sono già applicati e consiglia solo quelli in grado di colmare le lacune.

Distribuzione della Fondazione

Una volta completata la progettazione delle fondamenta, scegli come implementare:

- Implementa per me: AWS Transform implementa le unità organizzative, gli account e gli SCP di base nella tua organizzazione. AWS
- Lo implementerò da solo: AWS Transform genera artefatti Infrastructure as Code (IaC) da scaricare nel formato preferito (vedi). [the section called “Formati IaC”](#)
- Progetta innanzitutto gli account per i carichi di lavoro: salta la distribuzione e continua con la fase di progettazione degli account per il carico di lavoro. Potrai distribuire tutto insieme in un secondo momento.

Inizializzazione Control Tower

Se AWS Transform rileva che AWS Control Tower non è ancora inizializzato nell'organizzazione, fornisce all'utente un collegamento alla pagina della console AWS Transform. La generazione dell'operazione nel link creerà uno CloudFormation stack per avviare Control Tower. Il processo creerà questo stack nella CloudFormation console per la regione di destinazione. Una volta completata la creazione dello stack, AWS Transform continua con la distribuzione.

Progettazione dell'account Workload

Nella fase di progettazione dell'account per il carico di lavoro, AWS Transform progetta l'unità organizzativa e la struttura degli account per i carichi di lavoro delle applicazioni in base all'inventario di migrazione, ai requisiti aziendali e alle preferenze di separazione dell'ambiente.

Contesto di pianificazione della migrazione

AWS Transform recupera i dati dalla fase di pianificazione della migrazione, inclusi piani d'ondata, mappature tra server e applicazioni e contesto condiviso. Se i dati di pianificazione della migrazione sono disponibili, AWS Transform visualizza un riepilogo e chiede di confermarli o modificarli. Se non sono disponibili dati sulla pianificazione della migrazione, AWS Transform pone direttamente domande di scoperta.

Individuazione

AWS Transform pone domande per comprendere i requisiti del carico di lavoro. Puoi saltare qualsiasi domanda. Gli argomenti includono:

- Numero di unità aziendali o team che utilizzano AWS
- Settore e qualsiasi framework applicabile (HIPAA, SOC2 PCI-DSS, FedRAMP)
- Se i carichi di lavoro gestiscono dati sensibili (PII, PHI, finanziari)
- Preferenze di separazione degli ambienti (dev/test/staging/prod come account separati o condivisi)
- Requisiti di isolamento del carico di lavoro
- Applicazioni aziendali e relative finalità
- Raggruppamento dei server in applicazioni
- Esigenze di tracciamento e allocazione dei costi (per unità aziendale, progetto, ambiente)
- Crescita prevista nei prossimi 12-24 mesi

- Preferenza relativa alla strategia dell'account (app singola per account, raggruppata o basata sull'ambiente)

Struttura del carico di lavoro proposta

Sulla base delle risposte fornite e dei dati di pianificazione della migrazione, AWS Transform propone un'unità organizzativa e una struttura di account nell'ambito dell'unità organizzativa Workloads. La proposta include il ragionamento alla base di ogni decisione di progettazione.

AWS Transform segue questi principi di progettazione:

- Tutti i server coinvolti in un'ondata di migrazione accedono allo stesso account: le ondate non possono essere suddivise tra account. Si tratta di una limitazione del rehost durante l'esecuzione dell'ondata.
- Se richiedi ambienti isolati, AWS Transform crea un sistema operativo Workloads/Production Workloads/Non-Production secondario.
- Se vengono identificati i framework applicabili, AWS Transform crea Workloads/Regulated e Sub-OUTS. Workloads/Standard
- Se più unità aziendali richiedono una governance diversa, AWS Transform crea unità organizzative specifiche per unità aziendali nell'ambito dei carichi di lavoro.
- Alle applicazioni con dati critici o sensibili viene fornita un'unica app per account. In questo caso, ti potrebbe essere chiesto di modificare il tuo piano d'onda.
- Le applicazioni strettamente accoppiate con dipendenze condivise sono raggruppate in un unico account.

Ogni account proposto include: nome, scopo, unità organizzativa di destinazione e unità aziendale. AWS Transform mostra la convenzione di denominazione utilizzata (ad esempio, <business-unit>-<environment>-<workload>).

È possibile esaminare e modificare la struttura proposta prima che AWS Transform applichi le modifiche. Dopo l'applicazione, puoi iterare, apportando ulteriori modifiche finché non sei soddisfatto.

Configurazione SCP del carico di lavoro

Dopo aver creato la struttura del carico di lavoro, AWS Transform presenta gli SCP disponibili e chiede se desideri applicarli alle unità organizzative del carico di lavoro. L'utente seleziona quali

SCP applicare e a quali unità organizzative. AWS Transform applica gli SCP e mostra l'albero organizzativo aggiornato con una tabella riassuntiva SCP.

Distribuzione del carico di lavoro

Una volta completata la progettazione del carico di lavoro, scegli come implementare:

- Implementa per me: AWS Transform distribuisce le unità organizzative, gli account e gli SCP del carico di lavoro nella tua organizzazione. AWS
- Lo implementerò da solo: AWS Transform genera artefatti IaC da scaricare nel formato preferito (vedi). [the section called “Formati IaC”](#)

Formati IaC

Quando si sceglie l'implementazione automatica, AWS Transform genera artefatti Infrastructure as Code nei seguenti formati:

- [AWS Cloud Development Kit \(AWS CDK\)](#) — TypeScript progetto per l'implementazione programmatica dell'infrastruttura.
- HashiCorp Terraform: genera modelli HCL (HashiCorp Configuration Language) per la gestione delle risorse delle landing zone.
- Landing Zone Accelerator (LZA) — File di configurazione YAML basati sulla versione 1.1.0 di LZA Universal Configuration. Questi modelli pronti per l'uso aziendale funzionano con Landing Zone Accelerator per creare ambienti con più account. AWS AWS I file generati includono impostazioni preconfigurate per la governance, la struttura organizzativa e il networking in linea con le migliori pratiche. AWS Per ulteriori informazioni, consulta [LZA](#) Universal Configuration.

Note

Quando si esegue la distribuzione tramite la pipeline Landing Zone Accelerator (LZA), l'account AWS Transform e l'installazione di LZA devono trovarsi nella stessa organizzazione. AWS La distribuzione avrà esito negativo in caso di mancata corrispondenza tra gli Organizations ID utilizzati in AWS Transform e LZA. Per informazioni su come configurare l'installazione LZA utilizzando Organizations, consulta [AWS Organizations based installation](#).

Dopo aver selezionato un formato, AWS Transform genera gli artefatti e li rende disponibili per il download.

Per verificare che il file scaricato non sia stato danneggiato o manomesso, genera e scarica un checksum, quindi confrontalo con un hash generato localmente utilizzando:

```
openssl dgst -sha256 -binary <file.zip> | base64
```

Processo di approvazione dell'implementazione

Le richieste di implementazione delle zone di atterraggio richiedono un'approvazione esplicita prima dell'esecuzione. Quando invii una richiesta di distribuzione, questa viene indirizzata automaticamente agli approvatori autorizzati tramite la scheda AWS Transform Approvals.

Gli approvatori esaminano i CloudFormation modelli e le configurazioni delle landing zone. Solo gli utenti con il ruolo di amministratore in AWS Transform possono approvare le richieste di distribuzione. Ogni invio attiva un nuovo ciclo di revisione e le distribuzioni procedono solo dopo aver ricevuto la conferma.

Se un approvatore rifiuta la tua richiesta, contattalo direttamente per discutere delle modifiche necessarie. Il sistema tiene traccia di tutte le decisioni di approvazione a fini di controllo e conserva la cronologia delle implementazioni.

Etichetta: risorse per le landing zone

AWS Transform etichetta automaticamente tutte le risorse generate "CreatedBy": "AWSTransform" insieme agli ID di definizione e di esecuzione per scopi di tracciamento.

Tag automatici

Tutte le risorse delle landing zone ricevono i seguenti tag:

- CreatedBy— AWS Transform
- ATWorkspace— Identificatore dell'area di lavoro

Note

Se la migrazione fa parte del AWS Migration Acceleration Program (MAP 2.0), puoi includere il tag MAP richiesto: Key: Value map-migratedmigMPE_ID: (dove MPE_ID è l'identificatore

di valutazione del portafoglio di migrazione). Il tag MAP viene richiesto durante la fase di configurazione del connettore. AWS Transform applica questi tag durante l'implementazione delle landing zone.

Inversione delle modifiche

È possibile rimuovere solo gli elementi non distribuiti. Una volta che un'unità organizzativa o un account sono stati implementati, non possono essere rimossi tramite l'agente di landing zone.

Quando si rimuovono elementi, l'ordine è importante: è necessario rimuovere i bambini prima dei genitori:

1. Rimuovi prima gli account (tramite e-mail).
2. Rimuovi gli SCP dalle unità organizzative.
3. Rimuovi unità organizzative secondarie: un'unità organizzativa non può essere rimossa se dispone ancora di account o unità organizzative annidate.

Risorse correlate

- [the section called “Connect target Account AWS s e regioni”](#)
- [the section called “Migra la tua rete a AWS”](#)
- [AWS Guida per l'utente di Control Tower](#)
- [AWS Guida per l'utente di Organizations](#)
- [AWS Guida per l'utente di IAM Identity Center](#)
- [CloudFormation Guida per l'utente](#)
- [Landing Zone Accelerator attivo AWS](#)
- [AWS Well-Architected Framework](#)
- [AWS Guida prescrittiva: costruzione di zone di atterraggio](#)

Migra la tua rete a AWS

Con AWS Transform, puoi migrare la tua rete verso. AWS AWS Transform traduce la configurazione dell'ambiente di origine in risorse di rete AWS equivalenti: VPC, sottoreti, gruppi di sicurezza,

gateway NAT, gateway di transito, IP elastici, percorsi e tabelle di routing in base alle esigenze. È possibile rivedere e modificare la configurazione di rete generata prima della distribuzione. È possibile implementare la configurazione con AWS Transform e analizzare la connettività di rete. In alternativa, puoi scegliere l'implementazione automatica e ricevere Infrastructure as Code (IaC) nel formato che preferisci: AWS Cloud Development Kit (AWS CDK) Landing Zone Accelerator (LZA) o Terraform. HashiCorp

Per migrare la rete, procedi nel seguente modo:

1. Carica il file di rete di origine.
2. Carica file di configurazione aggiuntivi (opzionale, per ambienti RVTools).
3. Seleziona una topologia di rete.
4. Seleziona una strategia di mappatura dei gruppi di sicurezza.
5. Rivedi e ottimizza la tua rete.
6. Genera un diagramma di rete (opzionale).
7. Configura l'etichettatura delle risorse.
8. Implementa la tua rete.

Note

Per le implementazioni con più account, è necessario configurare i ruoli IAM su più account e l'accesso affidabile per AWS Organizations prima di iniziare la migrazione di rete. Per ulteriori informazioni sui tipi di migrazione, consulta [the section called “Fase 1: Selezione del tipo di migrazione”](#)

Fase 1: Mappatura della rete di origine

Il processo di mappatura della rete richiede il caricamento di un file di configurazione dall'ambiente di origine. Lo strumento scelto dipende dal tipo di rete di origine:

- Software Defined Networks (SDN): Import/Export per la virtualizzazione della rete VMware NSX o Cisco ACI config per Cisco Application Centric Infrastructure.
- Reti VMware vSphere: RVTools. Quando utilizzi file RVTools, AWS Transform genera solo configurazioni Amazon VPC. Le configurazioni dei gruppi di sicurezza richiedono input aggiuntivi

da firewall o file di rete definiti dal software. [Per ulteriori informazioni sulla generazione di gruppi di sicurezza da file aggiuntivi, vedere File di configurazione aggiuntivi.](#)

- Reti basate sui dati di configurazione del firewall: esportazione di file da Palo Alto Networks Firewall, Fortinet FortiGate Firewall o Cisco ACI. [Per ulteriori informazioni sulle versioni supportate e sulle istruzioni di estrazione, consulta Estrazione dei file di configurazione.](#)
- Reti ibride che eseguono carichi di lavoro VMware e non VMware:AWS [Transform discovery tool o ModelizeIt.](#)
- Altri tipi di file: se il file di configurazione non è uno dei formati supportati sopra elencati, il file viene convertito automaticamente in un formato supportato. Questa conversione può richiedere fino a due ore in base alla dimensione e alla complessità del file.

Note

La dimensione massima supportata del file di rete di origine è 70 MB.

Warning

Scarica RVTools solo dal sito ufficiale Dell all'indirizzo. <https://www.dell.com/en-us/shop/vmware/sl/rvtools> Non scaricate RVTools da fonti non ufficiali.

Ogni segmento della rete di origine è mappato sul proprio VPC distinto. La segmentazione della rete varia in base al tipo di sorgente:

- vNetwork: AWS Transform raggruppa le macchine virtuali tramite vSwitch e LAN virtuale (VLAN). Le VLAN possono apparire su più vSwitch (eccetto VLAN 0).
- Reti NSX: AWS trasformano i segmenti della rete in base ai router, raggruppando Tier-1 i router e raccogliendo i relativi segmenti.

Fase 2: File di configurazione aggiuntivi

Per gli ambienti di origine RVTools, è possibile caricare facoltativamente file di configurazione aggiuntivi per abilitare la generazione di gruppi di sicurezza. Se non caricate file di configurazione aggiuntivi, non viene generato alcun gruppo di sicurezza per la migrazione. RVTools-based

AWS Transform supporta i seguenti tipi di file di configurazione aggiuntivi. È possibile caricare un solo file di configurazione da una piattaforma.

- Cisco Application Centric Infrastructure (ACI) fornisce configurazioni delle policy di rete.
- Palo Alto Networks fornisce politiche di sicurezza firewall.
- Fortinet FortiGate fornisce politiche di sicurezza firewall.

Quando carichi un firewall o un file Cisco ACI, AWS Transform genera infrastrutture di rete e gruppi di sicurezza. Quando si carica un file RVTools da solo, AWS Transform genera solo l'infrastruttura di rete.

Per ulteriori informazioni sulle versioni supportate e sulle istruzioni di estrazione, consulta Estrazione dei [file di configurazione](#).

Fase 3: Topologie di rete

Durante la fase di definizione della rete, si seleziona una topologia di rete. È possibile scegliere la topologia dei VPC isolati o la topologia Hub and Spoke.

VPC isolati

Cosa viene distribuito

I VPC isolati sono ambienti di rete indipendenti che operano all'interno come unità separate. AWS I tuoi VPC sono completamente isolati, senza percorsi di comunicazione integrati tra di loro. Questa separazione offre il massimo livello di protezione dei confini della rete.

AWS Transform crea le seguenti risorse:

- Un VPC dedicato per ogni segmento di rete sorgente rilevato.
- Sottoreti private basate sulla configurazione della rete di origine.
- Gruppi di sicurezza (se hai fornito file di configurazione del firewall o SDN).

Completa la configurazione

AWS Transform implementa l'infrastruttura di rete ma lascia a te l'accesso a Internet e la connettività tra VPC, così puoi scegliere la configurazione che soddisfa i requisiti della tua organizzazione.

Per abilitare l'accesso a Internet per un VPC isolato, completa i seguenti passaggi:

1. Crea un [gateway Internet](#) e collegalo al VPC.
2. Crea sottoreti pubbliche in ogni zona di disponibilità in cui è necessario l'accesso a Internet. Aggiungi un percorso per 0.0.0.0/0 puntare al gateway Internet. Per ulteriori informazioni sulla configurazione delle [sottoreti](#), consulta [Subnet for your VPC](#).
3. Crea [gateway NAT](#) nelle sottoreti pubbliche (uno per AZ per un'elevata disponibilità). Assegna un IP elastico per ogni gateway NAT.
4. Aggiorna le [tabelle](#) di routing delle sottoreti private: aggiungi una route per 0.0.0.0/0 puntare al gateway NAT nella stessa AZ.
5. Rivedi [le regole del tuo gruppo di sicurezza](#): assicurati che le regole in uscita consentano il traffico necessario ai tuoi carichi di lavoro (HTTPS, DNS, ecc.).

Per la VPC-to-VPC comunicazione, configura il [peering VPC](#) o un [Transit Gateway](#) e aggiorna le tabelle di routing in ogni VPC per instradare il traffico verso la connessione peering o l'allegato TGW.

Hub and Spoke

In questo modello, un [AWS Transit Gateway](#) funge da hub centrale che collega più VPC per carichi di lavoro (gli spoke).

Cosa viene distribuito

AWS Transform crea le seguenti risorse:

- VPC Spoke: un VPC per segmento di rete di origine rilevato, con sottoreti private e un allegato Transit Gateway.
- Inspection VPC: ospita il dispositivo firewall per l'ispezione del traffico. Tutto il traffico tra VPC viene instradato attraverso questo VPC. L'allegato Transit Gateway utilizza la [modalità appliance](#), un'impostazione che assicura che il traffico scorra simmetricamente attraverso lo stesso dispositivo per entrambe le direzioni di una connessione.
- VPC in entrata: gestisce il traffico che entra nella rete dalla rete Internet pubblica (in entrata nord-sud). Include un [gateway Internet](#) e sottoreti pubbliche su più zone di disponibilità.
- VPC in uscita: gestisce il traffico che esce dalla rete verso la rete Internet pubblica (direzione nord-sud in uscita). Include un gateway Internet, gateway [NAT](#) con [indirizzi IP elastici](#) in ogni zona di disponibilità per l'alta disponibilità e sottoreti private per l'allegato Transit Gateway.
- Tabelle di routing Transit Gateway: due tabelle di routing indirizzano il traffico attraverso il VPC di Inspection. La tabella Uninspected è associata a Spoke VPC, VPC in entrata e VPC in uscita:

indirizza tutto il traffico (0.0.0. 0/0) all'allegato Inspection VPC ed è la tabella dei percorsi di associazione predefinita. La tabella Inspected è associata al VPC di ispezione: contiene le route propagate da tutti i VPC spoke ed è la tabella delle rotte di propagazione predefinita.

Per le implementazioni con più account, il Transit Gateway è condiviso tra gli account tramite [AWS Resource Access Manager \(RAM\)](#).

Flusso di traffico

Tutto il traffico cross-VPC segue questo percorso:

1. Il traffico proveniente da un VPC spoke viene inviato al Transit Gateway (route predefinita 0.0.0. 0/0).
2. La tabella delle rotte non ispezionate indirizza il traffico verso il VPC di ispezione.
3. Il firewall nel VPC di Inspection ispeziona il traffico e lo inoltra al Transit Gateway.
4. La tabella delle rotte ispezionate indirizza il traffico verso il VPC spoke di destinazione utilizzando rotte propagate.

Per il traffico Internet in uscita, la tabella delle rotte ispezionate indirizza il traffico verso il VPC in uscita. I gateway NAT traducono gli indirizzi IP privati prima che il traffico venga inoltrato al gateway Internet. La tabella delle route pubbliche VPC in uscita include percorsi specifici per ogni intervallo di routing VPC Inter-Domain Classless Routing (CIDR) a pozzetti verso il Transit Gateway. Questi percorsi consentono al traffico di ritorno di raggiungere il VPC con razze corrette.

Il traffico Internet in entrata entra attraverso il gateway Internet di Inbound VPC e segue lo stesso percorso di ispezione per raggiungere i VPC spoke.

Completa la configurazione

AWS Transform implementa l'infrastruttura di rete ma lascia a te la configurazione del firewall e dei servizi in entrata, così puoi scegliere le appliance e le politiche di sicurezza che soddisfano i requisiti della tua organizzazione.

Note

Per impostazione predefinita, il traffico cross-VPC passa attraverso il VPC di ispezione senza ispezione. È necessario implementare un firewall per abilitare l'ispezione del traffico.

Implementa un firewall: crea sottoreti aggiuntive nel VPC di ispezione per gli endpoint del firewall. AWS Transform crea sottoreti solo per l'allegato Transit Gateway. Indirizza il traffico dalle sottoreti degli allegati TGW agli endpoint del firewall e dalle sottoreti del firewall al Transit Gateway. È possibile distribuire [AWS Network Firewall](#) o un'appliance di terze parti. Per ulteriori informazioni sull'implementazione di un firewall con un Transit Gateway, vedere [Creazione di un firewall con un Transit Gateway](#).

Verifica la connettività: dopo aver implementato il firewall, verifica l'accesso a Internet in uscita da un'istanza VPC spoke (ad esempio,). `curl https://aws.amazon.com` È possibile utilizzare [Reachability Analyzer](#) per risolvere i problemi di connettività.

Configura i servizi in entrata: per ospitare servizi rivolti al pubblico, implementa un [Application Load Balancer o un Network Load Balancer](#) nelle sottoreti pubbliche VPC in entrata. Configura i gruppi target che puntano alle istanze nei tuoi VPC spoke tramite Transit Gateway e verifica che la tabella delle rotte ispezionate contenga percorsi di ritorno verso il VPC in entrata.

Se desideri un controllo granulare sulla comunicazione tra i VPC, scegli l'opzione VPC isolati e modifica la rete generata per creare i percorsi di comunicazione specifici di cui hai bisogno.

Fase 4: Mappatura dei gruppi di sicurezza

Scegli in che modo le tue politiche di sicurezza di origine si traducono in gruppi AWS di sicurezza. AWS Transform crea gruppi di sicurezza in base alle configurazioni dell'ambiente di origine. Le politiche di sicurezza, le regole della politica di sicurezza, le politiche del gateway e le regole delle politiche del gateway vengono convertite in gruppi di sicurezza.

Important

AWS Transform crea gruppi di sicurezza nel miglior modo possibile, in base all'ambiente di origine. Rivedi e modifica i gruppi di sicurezza generati per assicurarti che soddisfino le esigenze e le politiche di sicurezza della tua azienda.

Riferimenti dei gruppi di sicurezza

Quando vengono generati i gruppi di sicurezza, AWS Transform utilizza i riferimenti ai gruppi di sicurezza, ove supportato. Il riferimento ai gruppi di sicurezza imposta le regole di sicurezza basate su un altro ID di gruppo di sicurezza anziché su intervalli di indirizzi IP specifici (blocchi CIDR). Questo approccio offre configurazioni di sicurezza più flessibili e gestibili.

Le regole del gruppo di sicurezza possono fare riferimento solo ad altri gruppi di sicurezza all'interno dello stesso VPC o in un VPC connesso all'interno della stessa regione. Cross-account sono supportati anche i riferimenti. Non è possibile fare riferimento a un gruppo di sicurezza in un VPC non connesso o in più regioni. Per i VPC connessi, solo le regole in entrata supportano i riferimenti ai gruppi di sicurezza tra VPC: le regole in uscita devono utilizzare regole CIDR-based. Il modo AWS in cui Transform crea le regole dei gruppi di sicurezza dipende dalla topologia di rete scelta:

- **Hub and Spoke:** Transit Gateway fornisce connettività di rete tra VPC. AWS Transform utilizza il riferimento sia per le regole all'interno di VPC che per quelle di ingresso incrociato. VPC/cross-account Cross-VPC/cross-account Le regole di uscita (in uscita) utilizzano le regole CIDR-based.
- **VPC isolati:** i tuoi VPC non hanno alcuna connettività di rete tra di loro. AWS Transform utilizza il riferimento solo per le regole all'interno del VPC. Tutte le regole tra VPC e tra account utilizzano regole CIDR-based.

CIDR-based le regole vengono utilizzate anche quando le configurazioni di origine non sono simmetriche.

Scegliete una delle seguenti strategie di mappatura dei gruppi di sicurezza:

- **MAP:** traduce le regole di sicurezza dall'ambiente di origine in gruppi e regole AWS di sicurezza. Utilizzate questa opzione per le migrazioni che utilizzano l'indirizzamento IP statico.
- **MAP_DHCP (Translate with DHCP support):** traduce le regole di sicurezza dall'ambiente di origine con compatibilità DHCP. DHCP assegna gli indirizzi IP in modo dinamico dall'intervallo CIDR della sottorete. Di conseguenza, le regole di uscita tra VPC vengono ampliate per corrispondere all'intera sottorete di destinazione CIDR. Un CIDR più ristretto bloccherebbe gli DHCP-assigned IP che non rientrano in tale intervallo: rivedi queste regole dopo la migrazione.

Utilizza questa opzione per il supporto DHCP con la comunicazione Transit Gateway tra VPC. Funziona anche con IP statici, ma potrebbe generare regole più ampie rispetto a MAP.

- **SKIP:** non traduce le regole di sicurezza. Configura manualmente i gruppi AWS di sicurezza dopo la migrazione. Funziona con ambienti IP statici e DHCP. Per gli ambienti di origine RVTools senza file di configurazione aggiuntivi, AWS Transform utilizza automaticamente SKIP.

 Note

La strategia di mappatura determina le opzioni di assegnazione degli IP. MAP supporta solo l'IP statico. MAP_DHCP e SKIP supportano sia DHCP statico che DHCP.

Approcci alla migrazione IP

Sono disponibili due opzioni di configurazione di rete per la migrazione:

Selezione dell'intervallo di rete

- Mantieni gli intervalli esistenti (conservazione degli intervalli di indirizzi IP): conserva gli intervalli di indirizzi IP originali durante la migrazione. Ideale per le migrazioni in cui si spostano le applicazioni AWS senza modifiche (lift-and-shift), in particolare con applicazioni legacy che hanno dipendenze IP codificate o regole firewall esistenti.
- Aggiornamento a nuovi intervalli IP (aggiornamento CIDR): puoi modificare ogni intervallo CIDR VPC durante la migrazione AWS e Transform propaga automaticamente le modifiche a sottoreti, tabelle di routing e gruppi di sicurezza.

Assegnazione dell'indirizzo IP

- Indirizzi IP fissi (statici): AWS Transform assegna IP statici in base al CIDR. È la soluzione ideale per le applicazioni che richiedono un comportamento di rete prevedibile, la gestione DNS o il controllo degli accessi. IP-based Gli IP persistono anche dopo il riavvio delle istanze tramite Elastic Network Interfaces (ENI), che sono schede di rete virtuali collegate alle istanze.
- Assegnazione IP dinamica (AWS DHCP): assegna automaticamente gli IP dai pool di sottoreti all'avvio dell'istanza. Ottimale per applicazioni progettate per l'esecuzione nel cloud e carichi di lavoro con scalabilità automatica. Riduce il sovraccarico operativo ma richiede alle applicazioni di utilizzare DNS o service discovery.

È possibile combinare la selezione di entrambi gli intervalli con entrambi i metodi di assegnazione IP.

 Note

La strategia di assegnazione degli indirizzi IP è impostata a livello di onda. È possibile assegnare strategie diverse a server specifici personalizzando il file wave. Ad esempio, se si

è scelto un approccio basato su un indirizzo IP statico per il wave ma si desidera assegnare un approccio dinamico a un server specifico, è possibile utilizzare [RESET_VALUE] quanto descritto in [Modifica della configurazione nella guida per l'utente](#) di MGN.

Fase 5: Rivedi e ottimizza la tua rete

Dopo che AWS Transform ha generato la configurazione di rete di destinazione, è possibile esaminare i segmenti di rete locali convergenti verso l'infrastruttura. AWS Utilizza l'interfaccia visiva per esaminare la rete e l'interfaccia di chat per apportare modifiche e ricevere consigli guidati. AWS Transform esegue analisi di impatto a cascata e implementa le modifiche necessarie per mantenere la coerenza della rete e la conformità alle migliori pratiche. [Puoi anche chiedere a AWS Transform di analizzare la tua rete e suggerire ottimizzazioni: vedi Consigli guidati.](#)

VPC esistenti nel tuo account di destinazione

Se il tuo account di destinazione contiene già VPC, provenienti da precedenti fasi di migrazione o progetti di infrastruttura parallela, AWS Transform li rileva automaticamente e li visualizza insieme ai tuoi VPC mappati durante il processo di revisione. Per le migrazioni con più account, AWS Transform rileva i VPC esistenti su tutti gli account dell'organizzazione. AWS

Questa visibilità ti aiuta a capire in che modo la rete pianificata si relaziona all'infrastruttura esistente, a identificare potenziali conflitti CIDR e a prendere decisioni informate prima dell'implementazione.

Note

AWS Transform rileva solo i VPC esistenti (non le sottoreti o altre risorse). Il rilevamento è di sola lettura: AWS Transform non modifica i VPC esistenti.

Ottimizza la tua rete

Note

Queste operazioni si applicano solo ai VPC per carichi di lavoro. Per i VPC delle appliance con topologia Hub and Spoke (Inspection, Inbound, Outbound), è supportata solo la modifica dell'indirizzo IP.

Non è possibile annullare le operazioni di eliminazione, unione e divisione. Esamina attentamente la configurazione prima di applicare queste modifiche.

Le seguenti operazioni sono disponibili per i VPC:

- **Elimina:** rimuove definitivamente un VPC dalla configurazione. Usalo per segmenti di rete obsoleti verso i quali non è necessario migrare. AWS
- **Escludi:** rimuovi temporaneamente un VPC dalla migrazione per strategie di migrazione graduale. I VPC esclusi non vengono distribuiti ma possono essere reinclusi in un secondo momento.
- **Includi:** aggiungi un VPC precedentemente escluso nella migrazione.
- **Unisci:** combina due VPC in uno solo. Il primo VPC mantiene la sua identità e assorbe tutte le sottoreti dal secondo VPC. I gruppi di sicurezza vengono spostati nel VPC unito e le relative associazioni vengono ricostruite di conseguenza. Il CIDR del primo VPC si espande fino all'intervallo CIDR più piccolo che contiene entrambi i CIDR originali e il routing viene aggiornato automaticamente. Il secondo VPC viene rimosso dalla configurazione.

Unisci i requisiti:

- I CIDR di sottorete non devono sovrapporsi tra i due VPC.
- Il CIDR unito non deve superare /16.
- Per le distribuzioni con più account, entrambi i VPC devono essere assegnati allo stesso account.
- **Modifica indirizzo IP:** modifica l'indirizzo IP di base di un CIDR VPC mantenendo la stessa lunghezza del prefisso. AWS Transform traduce automaticamente tutti i CIDR di sottorete con lo stesso offset. Ad esempio, cambiando un VPC da 10.0.0.0/16 a 10.20.0.0/16 si sposta una sottorete da a. 10.0.1.0/24 10.20.1.0/24

Le regole del gruppo di sicurezza che corrispondono esattamente al vecchio CIDR VPC vengono aggiornate automaticamente. Le regole che si sovrappongono parzialmente o non corrispondono al vecchio CIDR non vengono modificate: rivedi queste regole dopo la modifica.

- **Rinomina:** modifica il nome di un VPC per allinearli alle convenzioni di denominazione dell'organizzazione per l'allocazione dei costi, il monitoraggio della conformità e gli standard operativi.
- **Ridimensiona:** modifica la lunghezza del prefisso di un CIDR VPC per espandere o ridurre l'intervallo di indirizzi IP.

- Riduzione della lunghezza del prefisso (più IP, ad esempio da /20 a /16): le sottoreti rientrano ancora nell'intervallo più ampio. Non sono necessarie modifiche alla sottorete.
- Aumento della lunghezza del prefisso (meno IP, ad esempio da /16 a /20): le sottoreti che non rientrano nel nuovo intervallo devono essere prima ridimensionate utilizzando l'operazione di ridimensionamento della sottorete.

Le regole del gruppo di sicurezza che corrispondono esattamente al vecchio CIDR VPC vengono aggiornate automaticamente. Le regole che si sovrappongono parzialmente o non corrispondono al vecchio CIDR non vengono modificate: rivedi queste regole dopo il ridimensionamento.

Requisiti di ridimensionamento:

- Il nuovo CIDR deve essere compreso tra /16 e /28.
- Il nuovo CIDR non deve sovrapporsi ad altri VPC della rete (topologia Hub and Spoke).
- Quando si riduce il CIDR, tutte le sottoreti esistenti devono rientrare nel nuovo CIDR. Se necessario, ridimensiona prima le sottoreti.
- Dividi: dividi un VPC in due VPC in base ai limiti CIDR che fornisci. Le sottoreti vengono assegnate al nuovo VPC il cui CIDR le contiene. I gruppi di sicurezza vengono clonati su entrambi i nuovi VPC, ma i CIDR delle regole dei gruppi di sicurezza non vengono aggiornati automaticamente: rivedi le regole dopo la suddivisione per assicurarti che la comunicazione tra VPC funzioni come previsto. Il VPC originale viene sostituito dai due nuovi VPC.

Requisiti suddivisi:

- È necessario fornire esattamente due intervalli CIDR.
- I due CIDR non devono sovrapporsi.
- Ogni CIDR deve essere compreso tra /16 e /28.
- Ogni sottorete deve rientrare esattamente in uno dei due CIDR. Se una sottorete non si adatta, l'operazione viene rifiutata.

Le seguenti operazioni sono disponibili per le sottoreti:

- Modifica indirizzo IP: modifica l'indirizzo IP di base di una sottorete CIDR mantenendo la stessa lunghezza del prefisso.
- Elimina: rimuove definitivamente una sottorete dalla configurazione senza influire sul VPC principale.

- **Ridimensiona:** modifica la lunghezza del prefisso di una sottorete CIDR per espandere o ridurre l'intervallo di indirizzi IP.

Requisiti di ridimensionamento della sottorete:

- Il nuovo CIDR deve essere compreso tra /16 e /28.
- Il nuovo CIDR non deve sovrapporsi ad altre sottoreti nello stesso VPC.
- Il nuovo CIDR deve trovarsi all'interno del VPC CIDR principale.

Dopo ogni operazione, AWS Transform rivaluta i riferimenti ai gruppi di sicurezza, il che potrebbe convertire CIDR-based le regole in riferimenti ai gruppi di sicurezza o viceversa. Rivedi le regole del gruppo di sicurezza dopo aver apportato le modifiche per verificare che soddisfino i tuoi requisiti.

Consigli guidati sulla rete

AWS Transform analizza la rete mappata e fornisce consigli prioritari tramite l'interfaccia di chat. I consigli si basano sui dati di rete e richiedono la conferma dell'utente prima di applicare qualsiasi modifica.

AWS Transform potrebbe consigliare le seguenti ottimizzazioni:

- **Risoluzione dei conflitti CIDR:** contrassegna gli intervalli CIDR che si sovrappongono tra i VPC mappati e i VPC esistenti in tutti gli account dell'organizzazione. AWS I VPC in conflitto vengono mostrati per primi. È possibile risolvere i conflitti reindirizzando il VPC mappato, escludendolo o eliminandolo oppure riconoscendo il conflitto e risolvendolo autonomamente dopo la distribuzione.
- **Standardizzazione dei nomi:** contrassegna i nomi VPC che non seguono uno schema coerente (ad esempio, nomi contenenti riferimenti hardware). AWS Transform richiede la convenzione di denominazione nel cloud prima di proporre sostituzioni.
- **Revisione dell'ambito:** identifica i segmenti di rete verso i quali potrebbe non essere necessario migrare AWS, come i sistemi o i costrutti legacy in attesa di smantellamento. AWS Transform richiede la conferma dell'utente prima di escludere qualsiasi costrutto.
- **Dimensionamento corretto della capacità VPC:** espone i VPC in cui il CIDR appare sovradimensionato o sottodimensionato per le sottoreti che contiene. AWS Transform presenta i dati sulla capacità corrente e consente di decidere se ridimensionarli.
- **Revisione della sicurezza:** contrassegna le regole del gruppo di sicurezza che consentono il traffico in entrata senza restrizioni (0.0.0. 0/0) per la tua recensione.

- Consolidamento VPC: identifica i VPC frammentati che sembrano separati dai limiti dell'infrastruttura fisica anziché dai requisiti di isolamento logico e suggerisce di unirli.

Note

Tutti i consigli richiedono una conferma esplicita dell'utente prima che Transform applichi qualsiasi modifica. AWS AWS Transform presenta dei compromessi quando una raccomandazione influisce su più aspetti della rete.

Fase 6: Diagramma reticolare

Dopo aver esaminato le configurazioni VPC generate, puoi facoltativamente generare un diagramma di rete per visualizzare la topologia della tua rete. AWS Transform supporta i seguenti formati di diagrammi:

- Mermaid code (.mmd): questo formato produce un file di definizione del diagramma basato su testo che è possibile renderizzare con strumenti Mermaid-compatible
- Immagine (.png): questo formato produce un'immagine renderizzata della topologia di rete.

Fase 7: Configurare la codifica delle risorse

Le risorse di rete sono contrassegnate per l'avvio e la replica. Puoi anche aggiungere tag personalizzati e tag AWS Migration Acceleration Program (MAP).

Tag automatici per l'avvio e la replica

AWS Transform etichetta automaticamente le risorse di rete migrate (VPC, sottoreti, gruppi di sicurezza e tabelle di routing) con i seguenti tag:

- Chiave: CreatedBy Valore: AWSApplicationMigrationService
- Chiave: ATWorkspace Valore: *workspace-id*

Questi tag consentono di utilizzare il VPC e la sottorete per avviare istanze di test e cutover. AWS

 Note

I VPC e le sottoreti migrati non includono la connettività Internet per impostazione predefinita, quindi non sono adatti come aree di memorizzazione per la replica.

Per utilizzare il VPC e la sottorete anche come area di gestione temporanea (replica), aggiungi manualmente i seguenti tag:

- Chiave: CreatedFor Valore: AWSTransform
- Chiave: ATWorkspace Valore: *workspace-id*

È inoltre possibile applicare questi tag a qualsiasi risorsa di AWS rete esistente per renderla disponibile per la replica.

Trova l'ID del tuo spazio di lavoro nell'URL dell'app web AWS Transform: [https://... *workspace-id* / workspace//id job/job](https://... workspace-id / workspace//id job/job)

Tag personalizzati

Oltre ai tag applicati automaticamente da AWS Transform, puoi aggiungere opzionalmente tag personalizzati per organizzare, tenere traccia dei costi e gestire la conformità per le tue risorse di rete migrate. È possibile applicare tag personalizzati a due livelli:

- Job-level tag: si applicano a tutte le risorse create da questo lavoro, inclusi tutti i VPC, le sottoreti, i gruppi di sicurezza e le tabelle di routing.
- VPC-level tag: si applica a un VPC specifico e passa automaticamente a cascata a tutte le risorse associate (sottoreti, gruppi di sicurezza, tabelle di routing).

 Note

Massimo 40 tag per richiesta. Ogni tag richiede una chiave e un valore. AWS si applicano le convenzioni di etichettatura.

AWS Transform applica questi tag quando genera i modelli Infrastructure as Code.

AWS Programma di accelerazione della migrazione

Se la migrazione fa parte del AWS Migration Acceleration Program (MAP 2.0) AWS , Transform applica un tag MAP alle risorse. Se hai fornito il tuo ID MPE in precedenza nel processo di migrazione, il tag viene applicato automaticamente. Altrimenti, dopo aver esaminato le configurazioni VPC generate, AWS Transform chiede se disponi di un accordo MAP e ti chiede di fornire il tuo ID MPE, un codice di 10 caratteri che utilizza lettere e cifre maiuscole (ad esempio, ABCDE12345). Il tag applicato utilizza il formato:

- Chiave: map-migrated Valore: migMPE_ID

Fase 8: Implementa la rete

Dopo aver aggiunto i tag, seleziona la tua strategia di implementazione:

- AWS Transform-managed implementazione: AWS Transform utilizza CloudFormation modelli per implementare la rete ed esegue Reachability Analyzer per verificare la connettività tra sottoreti su più VPC e all'interno dello stesso VPC.

Note

È necessario ottenere l'approvazione esplicita prima che venga eseguita la richiesta di distribuzione della rete. Vedi [Procedura di approvazione della distribuzione](#).

- Self-deployment: AWS Transform genera modelli Infrastructure as Code (IaC). CloudFormation i modelli vengono generati per impostazione predefinita. Puoi anche selezionare formati di output aggiuntivi:
 - AWS CDK genera un TypeScript progetto per l'implementazione dell'infrastruttura programmatica.
 - HashiCorp Terraform genera modelli di HashiCorp Configuration Language (HCL) per la gestione delle risorse di rete.
 - Landing Zone Accelerator (LZA) genera un file network-config.yaml per la configurazione di rete LZA.

Note

Quando si esegue la distribuzione tramite la pipeline Landing Zone Accelerator (LZA), l'account Transform e l'installazione di LZA devono trovarsi nella stessa organizzazione. AWS AWS La distribuzione avrà esito negativo in caso di mancata corrispondenza tra gli ID dell'organizzazione.

Per la distribuzione automatica, utilizza il link fornito per scaricare un file zip contenente i modelli generati. La cartella zip include un README.md file che spiega come utilizzare i modelli generati.

Per verificare che il file scaricato non sia stato danneggiato o manomesso, genera e scarica un checksum, quindi confrontalo con un hash generato localmente utilizzando il comando. `openssl dgst -sha256 -binary <file.zip> | base64`

Processo di approvazione della distribuzione

Per garantire che le modifiche alla rete siano conformi agli standard di sicurezza e ai requisiti architetturali dell'organizzazione, tutte le richieste di implementazione vengono sottoposte a un flusso di lavoro di approvazione. È necessario ottenere l'approvazione esplicita prima che venga eseguita la richiesta di distribuzione della rete. Quando invii una richiesta di distribuzione, questa viene indirizzata automaticamente agli approvatori autorizzati tramite la scheda AWS Transform Approvals. Gli approvatori convalidano sia i CloudFormation modelli che le configurazioni di rete per garantire la conformità agli standard di sicurezza e ai requisiti architettonici. Ogni invio attiva un nuovo ciclo di revisione e le implementazioni procedono solo dopo aver ricevuto la conferma. Se un approvatore rifiuta la tua richiesta, contattalo direttamente per discutere delle modifiche necessarie. AWS Transform tiene traccia di tutte le decisioni di approvazione a fini di controllo e conserva la cronologia delle implementazioni.

Elimina le risorse di rete distribuite

Se è necessario ripristinare una distribuzione, è possibile eliminare le risorse di rete distribuite da AWS Transform. È possibile eliminare le risorse immediatamente dopo il completamento della distribuzione. Se si modificano le risorse di rete distribuite dopo la distribuzione, le risorse non possono essere eliminate automaticamente.

- **AWS Transform-managed distribuzioni:** AWS Transform rimuove tutti gli CloudFormation stack creati durante la distribuzione. Questa azione richiede l'approvazione tramite la scheda AWS Transform Approvals.

- Self-deployments: è necessario eliminare manualmente le risorse distribuite tramite la console di AWS gestione o la AWS CLI.

Estrazione del file di configurazione

Se l'ambiente di origine utilizza Cisco ACI, Palo Alto Networks o Fortinet FortiGate, devi estrarre un file di configurazione da fornire a Transform. AWS È possibile utilizzare questi file come file sorgente autonomi per generare infrastrutture di rete e gruppi di sicurezza o come file complementari insieme a un caricamento di RVTools per aggiungere la generazione di gruppi di sicurezza. Il processo di estrazione è lo stesso in entrambi i casi.

Per estrarre i file di configurazione dal firewall e dagli ambienti di rete, segui queste procedure. Consulta la documentazione del fornitore per le informazioni più recenti.

Fortinet FortiGate

- La versione del firmware deve essere v7.0 o successiva.
- Hai bisogno dei super_admin nostri super_admin_readonly privilegi a livello globale.
- Fasi:
 1. Connect al firewall tramite SSH o client CLI integrato
 2. Esegui: `show | grep "" (| grep ""disabilita l'impaginazione)`
 3. Salva tutto l'output in un file a partire dal comando show

Palo Alto Networks

- La versione del firmware deve essere 10.1 o successiva.
- È necessario il ruolo di superadmin.
- Connect al firewall tramite SSH, esegui i seguenti comandi per disabilitare l'impaginazione, impostare il formato di output, accedere alla modalità di configurazione ed esportare la configurazione e gli oggetti predefiniti. Salva gli output:

```
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 versione del firmware deve essere 6.0 o successiva.
- È necessario il ruolo di amministratore con tutti i privilegi e una destinazione configurata Secure Copy Protocol (SCP), SSH File Transfer Protocol (SFTP) o File Transfer Protocol (FTP).
- Fasi:
 1. Connect all'Application Policy Infrastructure Controller (APIC) tramite il browser
 2. Apri il menu Admin e scegli Config Rollbacks
 3. Nella finestra di dialogo Scatta un'istantanea, seleziona l'opzione di posizione remota e scegli Crea un'istantanea adesso.
 4. Dopo aver ricevuto il messaggio «Trasferimento riuscito», connettiti al server di localizzazione remota e recupera il file di istantanea più recente (file.gz)

Migrazione dei server

AWS Transform utilizza AWS Transform MGN (MGN) per riospitare i server su Amazon EC2. Il flusso di lavoro di migrazione dei server ti guida nella configurazione di ogni fase di migrazione, nella convalida dell'inventario dei server, nella distribuzione degli agenti di replica, nel monitoraggio della replica dei dati, nel test delle istanze migrate e nell'esecuzione del cutover finale. [Per saperne di più, consulta *What is? AWS Transform MGN*](#) nella Guida per l'utente di MGN.

La migrazione dei server è organizzata a ondate. Ogni ondata rappresenta un gruppo di server che vengono migrati insieme. Per ogni ondata, completate le seguenti fasi:

Per le ondate con una strategia di migrazione containerizzata, AWS Transform esegue il flusso di lavoro di containerizzazione del codice sorgente anziché i passaggi di rehosting descritti di seguito. Il flusso di lavoro di containerizzazione ti guida attraverso la clonazione del codice sorgente, la generazione di artefatti Docker, la pubblicazione di immagini dei container e la distribuzione su Amazon Elastic Container Service o Amazon Elastic Kubernetes Service. Per il flusso [Containerizzazione del codice sorgente](#) di lavoro completo di containerizzazione, consulta.

1. Prerequisiti e configurazione delle impostazioni predefinite di migrazione
2. Fase 1: configurare l'ondata di migrazione
3. Fase 2: convalida e conferma dell'inventario
4. Fase 3: Implementazione degli agenti di replica

5. Fase 4: Replica dei dati
6. Fase 5: Test
7. Fase 6: Cutover

Prerequisiti e configurazione delle impostazioni predefinite di migrazione

Prerequisiti

Prima di iniziare la migrazione del rehost, assicurati di aver predisposto quanto segue:

Note

Se hai completato tutti i passaggi di un processo di migrazione end-to-end in AWS Transform, gli account di destinazione e il file di inventario sono già pronti: il file di inventario sarà stato generato automaticamente durante la fase di pianificazione della migrazione. Anche l'infrastruttura di rete configurata tramite la migrazione di rete AWS Transform è pronta. Se non hai creato la tua infrastruttura di rete tramite AWS Transform, assicurati che sia configurata in anticipo prima di iniziare la migrazione con rehost. Prima di iniziare la migrazione di rehosting, verifica di disporre delle risorse e dell'infrastruttura di rete necessarie per ospitare i server. Puoi utilizzare le funzionalità di migrazione delle landing zone e della rete di AWS Transform o qualsiasi altro strumento a tale scopo.

- Sistemi operativi supportati: i server di origine devono eseguire un sistema operativo supportato. Per l'elenco completo, vedere [Sistemi operativi supportati](#) nella Guida per l'utente di MGN.
- Account Target per la migrazione: Account AWS gli ID su cui è necessaria la migrazione dei server. Puoi utilizzare AWS Transform landing zone o qualsiasi altro strumento per configurare la tua infrastruttura.
- Infrastruttura di rete esistente: VPC, sottoreti e gruppi di sicurezza distribuiti e configurati. È possibile utilizzare AWS Transform Network Migration o qualsiasi altro strumento per configurare l'infrastruttura di rete.
- File di inventario: preparato con dettagli sul server, assegnazioni delle ondate, informazioni sull'account di destinazione e preferenze relative al tipo di istanza Amazon EC2. Puoi utilizzare la pianificazione della migrazione di AWS Transform per generare questo file.

Configurare i valori predefiniti di migrazione

Prima di iniziare l'esecuzione della migrazione di più account, è necessario configurare le impostazioni predefinite che si applicano a tutti gli account di destinazione. Queste impostazioni predefinite definiscono come vengono lanciate le istanze Amazon EC2 e come viene configurata la migrazione generale. Puoi ignorare queste impostazioni predefinite a livello di onda durante la configurazione dell'ondata.

Preferenze di raccomandazione di Amazon EC2

AWS Transform fornisce consigli sui tipi di istanze Amazon EC2 in base alle specifiche di utilizzo delle macchine virtuali di origine. Puoi configurare le preferenze di raccomandazione di Amazon EC2 per controllare come vengono selezionati i tipi di istanza per i server migrati.

Per ulteriori informazioni sulla generazione di consigli Amazon EC2, consulta [Generazione di consigli Amazon EC2](#) in AWS Migration Hub

Note

Puoi modificare i tipi di istanza Amazon EC2 suggeriti per includere raccomandazioni provenienti da [Migration Evaluator](#), [AWS Optimization and Licensing Assessment \(OLA\)](#) o da [un AWS job di valutazione](#) Transform.

Inizializzazione della migrazione

Per avviare la migrazione, AWS Transform inizializza MGN per tutti gli account Regione AWS in cui intendi migrare, nonché per tutti gli account di destinazione in cui verrà utilizzato il servizio. Durante il processo di inizializzazione:

- Vengono creati i ruoli e le policy IAM richiesti.
- I modelli predefiniti richiesti sono configurati.

Per informazioni sul processo di inizializzazione, vedere [Inizializzazione AWS Transform MGN con la console nella Guida per l'utente](#) di MGN.

Modello di avvio di Amazon EC2

Le impostazioni di avvio comprendono due parti: le impostazioni generali di avvio e il modello di lancio di Amazon EC2, che determina il modo in cui viene avviata un'istanza di test o cutover per ciascun server di origine. AWS

Le impostazioni di avvio, incluso il modello di avvio di Amazon EC2, possono essere definite a livello di account e vengono quindi applicate automaticamente a ciascun server di origine ogni volta che aggiungi un server di origine a AWS Transform MGN. Le impostazioni di avvio predefinite in questa sezione possono essere applicate automaticamente a tutti gli account di destinazione.

AWS Transform presenta l'elenco delle impostazioni disponibili del modello di avvio. Puoi scegliere di continuare con le impostazioni predefinite o configurare il modello di lancio. Se scegli di eseguire la configurazione, AWS Transform fornisce un collegamento a una recensione HITL (human-in-the-loop) che contiene tutti i parametri delle impostazioni del modello di lancio. Puoi anche apportare modifiche direttamente tramite l'interfaccia di chat per tutti i parametri che desideri.

[I server di origine](#) vengono creati con le impostazioni del modello di avvio dell'account. Una volta creati i server di origine con queste impostazioni predefinite, è possibile modificarle a livello delle impostazioni di avvio del server di origine. È possibile modificare le impostazioni del server di origine su qualsiasi parametro utilizzando l'interfaccia di chat o, per operazioni di massa, utilizzando il file di inventario Excel durante [Fase 2: Convalida e conferma dell'inventario](#).

Per rivedere l'elenco completo delle impostazioni e dei dettagli del modello di lancio, consulta le [impostazioni generali di Launch nella Guida](#) per l'utente di MGN.

Modifiche aggiuntive al modello di lancio di Amazon EC2

Per ulteriori modifiche al modello di lancio di Amazon EC2, è necessario eseguirle sull'ID del modello per ciascun account di destinazione. Questa opzione è disponibile all'interno della configurazione wave. AWS Transform ti guida nella procedura e fornisce il link appropriato.

Passaggio 1: configurare l'ondata di migrazione

In questa fase, AWS Transform prepara l'ondata di migrazione configurando l'account di destinazione, verificando le autorizzazioni di servizio, impostando i tag delle risorse, aggiungendo dati di rete all'inventario e configurando le impostazioni di replica e avvio.

Modalità di migrazione e configurazione dell'account

AWS Transform supporta due modalità di migrazione:

- Single-account migrazione: tutti i server del wave migrano verso lo stesso account di destinazione configurato nel connettore.
- Multi-account migrazione: i server migrano verso diversi account di destinazione specificati nel file di inventario. Per le migrazioni con più account, il modello di inventario deve includere una `mgn:account-id` colonna con l'ID dell'account di destinazione per ogni server.

AWS Transform conferma la configurazione dell'account di destinazione e verifica che MGN sia inizializzato in ogni account di destinazione. Se MGN non è ancora inizializzato, AWS Transform fornisce le istruzioni per completare l'inizializzazione. Durante l'inizializzazione, MGN crea i seguenti ruoli di servizio IAM per le operazioni di replica e avvio:

- `AWSApplicationMigrationReplicationServerRole`
- `AWSApplicationMigrationConversionServerRole`
- `AWSApplicationMigrationMGHRole`
- `AWSApplicationMigrationLaunchInstanceWithDrsRole`
- `AWSApplicationMigrationLaunchInstanceWithSsmRole`
- `AWSApplicationMigrationAgentRole`

Per ulteriori informazioni su questi ruoli, consulta [Inizializzazione di MGN con la console o Inizializzazione di MGN con l'API nella Guida per l'utente di MGN](#).

Per le migrazioni multi-account, AWS Transform crea anche il seguente ruolo durante la fase di inizializzazione: `AWSTransformRehostSharingRole_<management-or-delegated-admin-account-id>`. Questo ruolo viene distribuito su tutti gli account di destinazione della migrazione.

Verifica dell'etichettatura delle risorse

Dopo la conferma delle autorizzazioni di servizio, AWS Transform verifica che tutte le risorse richieste siano etichettate correttamente per consentire la corretta esecuzione della migrazione da parte dell'agente. Se in alcune risorse mancano i tag richiesti, AWS Transform fornisce un collegamento alla pagina di tagging in cui è possibile applicare i tag mancanti prima di continuare. Sono obbligatori i seguenti tag:

- I server di origine esistenti devono avere tag `CreatedBy: AWSTransform` e `ATWorkspace: <workspace_id>`. Se hai già avviato la replica sui server di origine e li hai creati nel servizio AWS Transform MGN, devi etichettare questi server in modo che AWS Transform possa metterli

in correlazione con i server di origine rilevati nell'ambiente locale ed evitare la creazione non necessaria di server di origine duplicati. AWS Transform si correla automaticamente tra di essi utilizzando le chiavi ID, FQDN o hostname fornite dall'utente.

- Le risorse di rete devono essere etichettate correttamente sia per le istanze di replica (area di staging) che per quelle di avvio. AWS Transform visualizza l'elenco completo delle risorse di rete nell'account di destinazione, con un'indicazione se ogni risorsa è già etichettata o meno. Puoi rivedere l'elenco e selezionare le risorse senza tag che desideri aggiungere. Per ogni risorsa selezionata, AWS Transform applica il tag pertinente:
 - `CreatedBy: AWSTransform` oppure `CreatedFor: AWSTransform`, a seconda del tipo di risorsa.
 - `ATWorkspace: <workspace_id>` viene applicato a tutte le risorse selezionate.

I VPC e le sottoreti creati dall'agente di migrazione di rete AWS Transform vengono etichettati automaticamente.

- Oltre ai VPC e alle sottoreti, AWS Transform mostra anche tutte le interfacce di rete elastiche (ENI) esistenti presenti nell'account di destinazione. Se desideri che AWS Transform le utilizzi come parte del lancio dell'istanza, devono essere contrassegnate con `e.CreatedFor: AWSTransform` e `ATWorkspace: <workspace_id>`. Per ulteriori informazioni su come allegare o aggiungere ENI al modello di lancio di Amazon EC2, [consulta Considerazioni dettagliate](#) nella MGN User Guide.

Aggiungi dati di rete all'inventario

AWS Transform aggiunge le informazioni di rete dalla migrazione di rete al file di inventario. Questo passaggio associa i server alle sottoreti e ai gruppi di sicurezza di destinazione appropriati in base alla configurazione di rete generata durante la fase di migrazione della rete.

Impostazioni di replica e avvio

Configurazione delle impostazioni di replica

Le impostazioni di replica determinano il modo in cui i dati vengono replicati dai server di origine verso AWS. Configurare le impostazioni di replica nel modello di replica prima di aggiungere i server di origine a Transform MGN. AWS Transform mostra tutti i parametri delle impostazioni di replica: puoi configurarli tramite un HITL dedicato o tramite l'interfaccia di chat.

Per maggiori dettagli sui parametri delle impostazioni di replica, consultate il [modello delle impostazioni di replica nella Guida per l'utente](#) di MGN.

Avvia le impostazioni del modello

Il modello di avvio consente di controllare il modo in cui AWS Transform MGN avvia le istanze in AWS. La configurazione predefinita definita nel modello viene applicata automaticamente a ogni server appena aggiunto. È possibile configurare le impostazioni del modello di avvio tramite un HITL dedicato o tramite l'interfaccia di chat.

Per maggiori dettagli sui parametri delle impostazioni del modello di lancio, consulta [Launch template](#) nella MGN User Guide.

AWS Transform fornisce anche un collegamento all'ID del modello di lancio di Amazon EC2 associato al modello di lancio, che consente di modificare gli attributi aggiuntivi del modello di lancio di Amazon EC2. Per modificare il modello di lancio di Amazon EC2, segui le istruzioni nel modello di [lancio](#) nella MGN User Guide.

Strategia di assegnazione degli IP

Sei tu a scegliere come assegnare gli indirizzi IP ai server migrati:

- **IP statico:** viene mantenuto l'indirizzo IP del server di origine. Se è richiesta la trasformazione CIDR, AWS Transform converte automaticamente l'indirizzo IP in modo che corrisponda al nuovo CIDR.
- **IP dinamico (DHCP):** a ciascun server viene assegnato un nuovo indirizzo IP dal pool IP della sottorete.

Note

Se è stata selezionata la strategia di mappatura dei gruppi di sicurezza MAP durante la migrazione di rete, è disponibile solo l'assegnazione IP statica. Per maggiori dettagli, consulta Mappatura dei [gruppi di sicurezza](#).

Fase 2: Convalida e conferma dell'inventario

Prima di caricare i dati del server in MGN, AWS Transform prepara il file di inventario per la revisione. È possibile scaricare il file in formato CSV o XLSX, rivedere le configurazioni del server e apportare modifiche se necessario.

Il file di inventario include dettagli come nomi di server, sistemi operativi, consigli sui tipi di istanze Amazon EC2, sottoreti di destinazione, gruppi di sicurezza, assegnazioni IP e opzioni di licenza. I campi obbligatori includono:

- Informazioni sul server: nome del server, VMID e specifiche di origine.
- Assegnazione delle ondate: raggruppamento delle ondate di migrazione.
- Raggruppamento di applicazioni: associazioni logiche di applicazioni.
- Configurazione di Target: account Target, regione e tipo di istanza Amazon EC2.
- Configurazione di rete: sottorete e gruppi di sicurezza di Target.

Puoi modificare il file per adattare le configurazioni di Amazon EC2, cambiare le opzioni di licenza del sistema operativo (BYOL o License Included) e aggiornare le impostazioni di locazione.

Dopo aver esaminato l'inventario, puoi accettarlo come mostrato o caricare una versione modificata. AWS Transform carica quindi i dati in MGN, che crea i record del server di origine per ogni server dell'ondata.

Note

Non rimuovete colonne o modificate le intestazioni delle colonne nel file di inventario. AWS Transform richiede la struttura originale del file per elaborare correttamente i dati.

Note

AWS Transform consente un'importazione verso una determinata destinazione Account AWS e una destinazione Regione AWS alla volta. Se si lavora su più di un'ondata contemporaneamente o se è in esecuzione più di un processo di migrazione con lo stesso account di destinazione, è necessario attendere il completamento dell'importazione prima di poter eseguire un'altra importazione in un'ondata o un processo diverso.

È possibile controllare le opzioni di licenza del sistema operativo (BYOL o License Included) e la locazione specificando la configurazione nelle colonne del file di inventario e. `mgn:launch:placement:operating-system-licensing`
`mgn:launch:placement:tenancy` Per ulteriori informazioni, consultate [Import parameters](#) nella MGN User Guide.

Fase 3: Implementazione degli agenti di replica

Per iniziare a replicare i dati dai server di origine a AWS, è necessario installare l'agente di AWS replica su ciascun server di origine. AWS Transform offre tre metodi di installazione:

- **Strumenti organizzativi:** utilizza gli strumenti di distribuzione esistenti della tua organizzazione (come SCCM, Ansible o Chef) per installare gli agenti sui tuoi server. AWS Transform fornisce ai comandi di installazione parametri aggiuntivi per l'installazione invisibile all'utente, tra cui `--no-prompt` `--aws-access-key-id` `--aws-secret-access-key`, e. `--aws-session-token`
- **Connettore MGN:** utilizzate un connettore MGN per automatizzare l'installazione dell'agente. Il connettore si connette ai computer di origine tramite SSH (Linux) o WinRM (Windows) e installa automaticamente l'agente di replica. Una volta configurato, un connettore può essere riutilizzato su più onde e destinazioni diverse. Account AWS Per ulteriori informazioni sul connettore MGN, vedere [Configurare il connettore MGN nella Guida per l'utente di MGN](#).

Note

Prima di utilizzare il connettore MGN con AWS Transform, è necessario etichettare l'istanza gestita del connettore in AWS Systems Manager Fleet Manager con i seguenti tag:

- Chiave: `CreatedFor` Valore: `AWSTransform`
- Chiave: `ATWorkspace` Valore: *workspace-id*

Per etichettare l'istanza gestita, apri la AWS Systems Manager console, vai a Fleet Manager in Node Tools, scegli l'istanza gestita del tuo connettore MGN e applica i tag sopra riportati. Trova l'ID del tuo spazio di lavoro nell'URL dell'app web AWS Transform: `https://.../workspace/workspace-id/job/job-id`

- **Installazione manuale:** installa l'agente direttamente su ciascun server di origine. Questo metodo richiede l'accesso diretto a ciascun server ma offre il pieno controllo sul processo di installazione.

AWS Configurazione del connettore Transform MGN

Il connettore AWS Transform MGN automatizza la distribuzione degli agenti di replica sui server di origine. Il connettore è un client leggero distribuito su un computer Linux dedicato nell'ambiente locale. Si connette ai server di origine tramite SSH (Linux) o WinRM (Windows) per installare e configurare agenti di replica, eliminando la necessità di coordinarsi manualmente tra più servizi. AWS

Come funziona il connettore

Il connettore funziona tramite i seguenti componenti:

- Client Connector: distribuito su una macchina Linux dedicata nell'ambiente dell'utente.
- Agente SSM: installato sulla stessa macchina per consentire una comunicazione sicura con AWS.
- Attivazione ibrida SSM: collega la macchina del connettore a AWS Systems Manager per l'esecuzione sicura dei comandi.
- Gestione delle credenziali: recupera le credenziali del server di origine da Secrets Manager AWS.

Quando si distribuiscono gli agenti, AWS Transform invia un documento SSM alla macchina del connettore. Il connettore recupera quindi le credenziali del server di origine da AWS Secrets Manager, stabilisce una connessione a ciascun server di origine, verifica che il server di origine soddisfi i prerequisiti, installa e configura l'agente di replica e verifica la corretta installazione.

Requisiti del computer Connect

Requisito	Informazioni
Sistema operativo	Sistema operativo Linux supportato. Per l'elenco completo, consultate i prerequisiti del connettore MGN nella Guida per l'utente di MGN.
Accesso alla rete	Deve raggiungere tutti i server di origine (Linux su SSH, Windows su WinRM)
Connettività Internet	HTTPS (443) in uscita verso gli AWS endpoint (Systems Manager, Secrets Manager, MGN)
Spazio su disco	Minimo 200 MB gratuiti
Permissions	Accesso root o sudo

Note

Il connettore deve essere installato su un computer Linux, ma può distribuire agenti su server di origine Linux e Windows.

Processo di configurazione

AWS Transform guida l'utente attraverso i seguenti passaggi per configurare il connettore:

Fase 1: Configurazione del connettore

Fornisci un nome per il connettore o usa il nome predefinito generato automaticamente. Il connettore può essere installato sull'account di gestione o su un account amministratore delegato in MGN. Per le migrazioni con più account, il connettore può distribuire agenti sui server tra gli account dei membri.

Fase 2: configurazione delle risorse AWS

AWS Transform apre una pagina di configurazione che viene eseguita nel browser utilizzando AWS le credenziali dell'utente. È necessario accedere alla Console di AWS gestione con il proprio account di gestione o l'account amministratore delegato. Deve essere lo stesso account a cui è collegato il connettore di destinazione AWS Transform.

La pagina di configurazione crea automaticamente le seguenti risorse:

- Ruoli IAM (creati in modo idempotente, ignorati se già esistono):
 - `AWSApplicationMigrationConnectorManagementRole`— Utilizzato durante l'installazione dell'agente per accedere alle credenziali.
 - `AWSApplicationMigrationConnectorSharingRole_<ACCOUNT-ID>`— Contiene le autorizzazioni per l'installazione dell'agente.
- Attivazione ibrida SSM: periodo di scadenza di 30 giorni. Collega la macchina del connettore a AWS Systems Manager e genera credenziali di attivazione sicure.

In alternativa, puoi scaricare un CloudFormation modello dalla pagina di configurazione per distribuire tu stesso i ruoli IAM.

La pagina di configurazione genera un comando di installazione su una riga con tutte le credenziali e la configurazione necessarie.

Important

Tieni aperta la pagina di configurazione fino al completamento dell'installazione. Per chiuderla sarà necessario riavviare il processo. Tutte le credenziali esistono solo nel browser e non vengono archiviate da Transform. AWS

Fase 3: Installazione del connettore

Installa il connettore su una macchina Linux nel tuo ambiente:

1. Copia il link di installazione dalla pagina di configurazione.
2. SSH nella macchina Linux prescelta.
3. Incolla ed esegui il comando di installazione.
4. Attendi il completamento dell'installazione (in genere 2-3 minuti).

Fase 4: Collegare i server di origine

Dopo l'installazione, AWS Transform identifica tutti i server di origine che appartengono all'ondata corrente e li collega automaticamente al connettore MGN.

Fase 5: Configurare le credenziali

Fornisci gli ARN di AWS Secrets Manager per le credenziali del server di origine. AWS Transform offre tre opzioni di configurazione delle credenziali:

- Segreto singolo per server Linux: un segreto condiviso contenente chiavi SSH o username/password per tutti i server di origine Linux.
- Segreto singolo per server Windows: un segreto condiviso contenente nome utente e password per tutti i server di origine Windows.
- Più segreti per server: segreti diversi per server o gruppo di server. Usalo quando i server hanno credenziali diverse. AWS Transform genera un file CSV precompilato con l'elenco dei server. Compilate la `secret_arn` colonna per ogni server e caricate il file completo.

Note

Puoi combinare le opzioni a segreto singolo Linux e Windows se disponi di entrambi i tipi di server con un segreto condiviso ciascuno. L'opzione dei segreti per server si esclude a vicenda con le opzioni a segreto singolo.

Formato segreto delle credenziali. Per saperne di più, consulta le [credenziali del connettore MGN](#) nella Guida per l'utente di MGN:

```
{
  "WinConnectionProtocol": "HTTPS",
  "WinUserName": "windows_username",
  "WinPassword": "windows_password",
  "LinuxUserName": "linux_username",
  "LinuxPrivateKey": "linux_private_key",
  "LinuxHostKeyValidation": false
}
```

Distribuzione degli agenti

Una volta configurate e verificate le credenziali, AWS Transform distribuisce gli agenti di replica sui server di origine. È possibile eseguire la distribuzione su tutti i server nell'ondata corrente o selezionare server specifici.

Il processo di distribuzione per ogni server:

1. AWS Transform invia i comandi di distribuzione al connettore tramite SSM.
2. Il connettore recupera le credenziali da AWS Secrets Manager.
3. Il connettore si connette al server di origine utilizzando le credenziali configurate.
4. Il connettore verifica che il server di origine soddisfi tutti i prerequisiti richiesti per eseguire l'agente di replica.
5. Il connettore installa e configura l'agente di replica.
6. Il connettore verifica la corretta installazione e connettività.

È possibile monitorare l'avanzamento dell'implementazione in tempo reale con il monitoraggio dello stato per server, inclusa la fase di installazione corrente, il tempo trascorso e il tempo residuo stimato. In caso di guasto di un server, AWS Transform visualizza il motivo dell'errore e offre opzioni di riprova per server. I server distribuiti correttamente possono procedere in modo indipendente mentre i server guasti vengono riprovati.

Riutilizzo e ciclo di vita dei connettori

Quando si distribuiscono agenti per le ondate successive, è possibile riutilizzare un connettore esistente o crearne uno nuovo. AWS Transform elenca tutti i connettori configurati nell'account, mostrando il nome del connettore, lo stato (Attivo o scaduto), il numero di server collegati e la data di scadenza dell'attivazione ibrida.

- Connettore attivo: l'attivazione ibrida è ancora valida. AWS Transform verifica i ruoli IAM per la nuova ondata e procede alla configurazione delle credenziali. Non è necessaria alcuna nuova attivazione ibrida.
- Connettore scaduto: l'attivazione ibrida SSM è scaduta. Le attivazioni scadute non possono essere rinnovate. È necessario selezionare un connettore diverso o crearne uno nuovo.

Le attivazioni ibride SSM scadono dopo 30 giorni. L'attivazione è richiesta solo per l'installazione del connettore sulla macchina Linux. Una volta installato il connettore, è possibile continuare a utilizzarlo per installare gli agenti di replica sui server di origine anche dopo la scadenza dell'attivazione. Se è necessario installare il connettore su un nuovo computer dopo la scadenza dell'attivazione, è necessario creare un nuovo connettore tramite la procedura di configurazione.

Installazione manuale dell'agente

Per l'installazione manuale, è necessario innanzitutto generare AWS le credenziali (temporanee o permanenti) e quindi installare l'agente su ciascun server di origine.

Opzioni relative alle credenziali:

- Credenziali temporanee (consigliate): crea un ruolo IAM con la policy `AWSApplicationMigrationAgentInstallationPolicy` gestita, quindi utilizzalo `aws sts assume-role` per generare credenziali temporanee. Per saperne di più, consulta le [autorizzazioni di installazione dell'agente](#) nella Guida per l'utente di MGN.
- Credenziali permanenti: crea un utente IAM con la policy `AWSApplicationMigrationAgentInstallationPolicy` gestita e genera una chiave di accesso.

Fasi di installazione:

Per i server Linux, scarica ed esegui il programma di installazione:

```
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
```

Per i server Windows, scarica ed esegui il programma di installazione appropriato utilizzando PowerShell come amministratore:

```
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

Il parametro `--user-provided-id` è obbligatorio. Sostituiscilo *server-identifier* con il valore esatto riportato nella `mgn:server:user-provided-id` colonna del file di inventario. Questo identificatore collega il server fisico al relativo record del server di origine MGN.

Per ulteriori informazioni sull'installazione dell'agente, consultate l'[agente Linux](#) e l'[agente Windows](#) nella Guida per l'utente di MGN.

Dopo l'installazione, AWS Transform verifica che tutti gli agenti siano collegati correttamente controllando che i server mostrino uno stato di replica pari o. INITIATING INITIAL_SYNC

Note

AWS Transform non supporta la replica MGN senza agenti. Per informazioni sulla replica senza agenti, vedere [Panoramica sulla replica senza agenti](#) nella Guida per l'utente di [MGN](#).

Note

È necessario installare l'agente di replica su tutti i server in un'unica ondata. Disconnetti e archivia i server su cui non è installato l'agente di replica. È possibile utilizzare il `disconnect-from-service` comando per disconnettere i server e il `mark-as-archived` comando per archiviare i server disconnessi. Il comando di archiviazione funziona solo per i server di origine il cui stato del ciclo di vita è. DISCONNECTED

Per le quote relative alla replica, vedere i [limiti delle quote di servizio MGN nella Guida](#) per l'utente di MGN.

Fase 4: Replica dei dati

Dopo l'installazione degli agenti di replica, la replica dei dati inizia automaticamente. AWS Transform utilizza la replica continua a livello di blocco per sincronizzare i dati dai server di origine a. AWS

Il processo di replica si compone di due fasi:

- Sincronizzazione iniziale: una copia completa dei dati del server di origine su. AWS I dati vengono archiviati come snapshot di Amazon Elastic Block Store (Amazon EBS) o su volumi Amazon FSx NetApp for ONTAP (FSx for ONTAP) nell'account di destinazione, a seconda del tipo di storage di destinazione configurato. Per ulteriori informazioni, consulta il [tipo di storage Target](#) nella MGN User Guide. La durata dipende dal volume dei dati e dalla larghezza di banda della rete.
- Replica continua: sincronizzazione continua dei blocchi modificati con un impatto minimo sulle prestazioni del server di origine. Mantiene una copia aggiornata in. AWS

I server di replica sono istanze Amazon EC2 temporanee distribuite nella sottorete dell'area di staging. Ricevono dati replicati dai server di origine e vengono gestiti automaticamente da MGN. Per saperne di più, consultate le [impostazioni del server di replica](#) nella Guida per l'utente di MGN.

AWS Transform monitora l'avanzamento della replica e fornisce aggiornamenti sullo stato, tra cui lo stato della replica, il ritardo di replica (la differenza di tempo tra i dati di origine e quelli replicati) e l'utilizzo della larghezza di banda.

Durante la replica, ogni server passa attraverso i seguenti stati:

- Non pronto: il server è in fase di sincronizzazione iniziale e non è ancora pronto per il test.
- Pronto per il test: il server è stato aggiunto correttamente e la replica dei dati è iniziata. È ora possibile avviare istanze di test o cutover.

Una volta che tutti i server inclusi nella nuova ondata hanno superato NOT_READY lo stato, la fase di replica dei dati è completa ed è possibile procedere al test.

È possibile controllare la replica per singoli server o per l'intera ondata in qualsiasi momento:

- Sospendi la replica: sospendi temporaneamente la replica per server specifici o per l'intera ondata.

- **Riprendi la replica:** riprende la replica precedentemente sospesa.
- **Interrompi la replica:** interrompi definitivamente la replica. La replica interrotta può essere riavviata, ma inizia dalla sincronizzazione iniziale.

Fase 5: Test

Una volta completata la replica dei dati, è possibile avviare istanze di test per convalidare i server migrati prima di eseguire il cutover finale. Per saperne di più, consulta [Launch test instances](#) nella MGN User Guide. AWS Transform supporta due opzioni di test:

- **Test a ondata completa:** avvia istanze di test per tutti i server inclusi nell'ondata.
- **Test selettivi:** avvia istanze di test per server specifici selezionati fornendo gli ID forniti dall'utente dal file di inventario.

AWS Transform avvia le istanze Amazon EC2 dai dati replicati e fornisce gli ID delle istanze in modo da poterti connettere e convalidare le istanze di test. Dopo il test, puoi:

- Procedere al cutover se il test ha esito positivo.
- Avvia nuove istanze di test per ripetere il test.
- Termina le istanze di test e risolvi eventuali problemi prima di ripetere il test.

Fase 5b: Contrassegna le applicazioni come pronte per il cutover

Una volta completato il test e dopo che sarete soddisfatti dei risultati, contrassegna le applicazioni come pronte per il cutover. AWS Transform esamina lo stato di replica di ogni applicazione e risolve eventuali avvisi di replica prima di consentire all'utente di procedere. Solo le applicazioni con uno stato di replica pulito possono essere contrassegnate come cutover.

Fase 6: Cutover

Cutover è l'ultima fase di migrazione in cui vengono trasferiti i carichi di lavoro di produzione. AWS Per saperne di più, consulta [Launch cutover instances](#) nella MGN User Guide. Analogamente ai test, AWS Transform supporta il cutover a onda intera o il cutover selettivo per server specifici.

Durante il cutover, AWS Transform avvia le istanze Amazon EC2 dai dati replicati più recenti e fornisce gli ID di istanza per ogni server. Dopo aver verificato le istanze di cutover, si completa il cutover, che interrompe la replica continua della macchina di origine.

Il processo di cutover include i seguenti passaggi:

1. Avvia istanze cutover: AWS Transform avvia le istanze Amazon EC2 per i server selezionati. Puoi scegliere il cutover a onda intera o il cutover selettivo.
2. Verifica le istanze cutover: connettiti alle istanze avviate e verifica che funzionino correttamente.
3. Finalizza il cutover: conferma il cutover per interrompere la replica del computer di origine. È possibile finalizzare tutti i server dell'ondata o selezionare server specifici. La finalizzazione impedisce agli agenti di replica di inviare dati, rimuove gli agenti di replica dai server di origine e blocca lo stato del ciclo di vita del server. Questa azione non può essere annullata facilmente. Per saperne di più, consulta [Finalize cutover](#) nella MGN User Guide.
4. Server di origine di archiviazione (opzionale): dopo la finalizzazione, puoi contrassegnare i server di origine come archiviati per liberare la quota del server di origine nel tuo account.

Important

La finalizzazione del cutover interrompe la replica continua del computer di origine. Assicurati di aver verificato le istanze cutover prima di finalizzarle.

Note

I tempi di inattività si verificano tra lo spegnimento dell'origine e la disponibilità dell'istanza cutover. Pianifica di conseguenza la tua finestra di taglio.

Stati del ciclo di vita del server

Durante la migrazione, ogni server passa attraverso i seguenti stati del ciclo di vita. Per saperne di più, consulta il [ciclo di vita del server di origine](#) nella Guida per l'utente di MGN.

- Non pronto: il server è in fase di sincronizzazione iniziale e non è ancora pronto per il test.
- Pronto per il test: la replica dei dati è iniziata ed è possibile avviare istanze di test o cutover.
- Test in corso: è attualmente in fase di avvio un'istanza di test.
- Pronto per il cutover: il server è stato testato ed è pronto per il cutover.
- Cutover in corso: è attualmente in corso il lancio di un'istanza cutover.

- Cutover completato: il server è stato interrotto. Tutti i dati sono stati migrati all'istanza cutover. AWS
- Disconnesso: il server è stato disconnesso da MGN.

Puoi chiedere a AWS Transform lo stato dei tuoi server in qualsiasi momento durante la migrazione. AWS Transform fornisce una tabella interattiva sullo stato dell'onda che mostra tutte le informazioni pertinenti sul server, tra cui il ciclo di vita della migrazione, lo stato della replica e i passaggi successivi consigliati. Puoi anche chiedere in linguaggio naturale, ad esempio:

- Qual è lo stato dei miei server?
- Qual è lo stato della mia onda?
- Qual è lo stato della fase in cui mi trovo attualmente?

Durante la migrazione via ondata, puoi chiedere a AWS Transform di aggiornare o modificare lo stato dei singoli server. Ad esempio, se 9 server su 10 del tuo wave hanno superato la fase di test ma uno ha fallito, puoi consentire a AWS Transform di continuare a spostare i 9 server nella fase successiva eseguendo nuovamente il test sul server fallito.

Approvazioni di implementazione

Alcune operazioni di migrazione richiedono l'approvazione esplicita prima dell'esecuzione. Quando un'operazione richiede l'approvazione, AWS Transform indirizza la richiesta agli approvatori autorizzati tramite la scheda Approvazioni. Solo gli utenti con il ruolo di amministratore in AWS Transform possono approvare le richieste di distribuzione. Le distribuzioni procedono solo dopo aver ricevuto la conferma.

Note di rilascio

Le seguenti note di rilascio riguardano le ultime modifiche apportate a [Migrazioni \(incluso VMware\)](#). Per le regioni AWS Transform supportate, consulta [Regioni supportate](#). Per le aree di destinazione supportate, consulta la [pagina di configurazione del connettore dell'account](#).

giugno 2026

- AWS Transform for migrations ora supporta la localizzazione. È possibile modificare la lingua di visualizzazione dell'applicazione Web quando si lavora con flussi di lavoro di migrazione. [Scopri di più sulle impostazioni della lingua](#).

- AWS Transform ora ti consente di configurare le impostazioni di replica e le impostazioni di avvio per la migrazione. Puoi impostare la configurazione per il tuo account di destinazione o su server di origine specifici. [Scopri di più sulle impostazioni di replica e avvio.](#)
- AWS Transform ora consente di collegare interfacce di rete elastiche (ENI) esistenti al modello di lancio. Puoi taggare gli ENI nel tuo account di destinazione in modo che siano disponibili per l'uso all'avvio delle istanze. [Scopri di più sulla codifica delle risorse di rete.](#)
- AWS Transform for migrations ora supporta tutte le regioni AWS commerciali come obiettivi di migrazione, esclusi il Medio Oriente (Bahrein) e il Medio Oriente (Emirati Arabi Uniti). [Scopri di più sulle regioni target supportate.](#)

Maggio 2026

- AWS Transform ora rileva i VPC esistenti nell'account di destinazione durante la revisione della migrazione di rete. Puoi vedere i VPC esistenti insieme ai tuoi VPC mappati, identificare i conflitti CIDR e risolverli prima della distribuzione. [Scopri di più sul rilevamento VPC esistente.](#)
- AWS Transform supporta la ripiattaforma degli archivi di codice sorgente in container durante la migrazione verso. AWS [Scopri di più sulla containerizzazione.](#)

Aprile 2026

- Aggiunta la creazione di landing zone direttamente all'interno dei flussi di lavoro di migrazione. AWS Transform verifica la presenza di una base esistente, consiglia le strutture delle unità organizzative (OU) e gli account di destinazione e offre la distribuzione automatizzata o i formati di output Infrastructure as Code (IaC) (CloudFormation o Landing Zone Accelerator (LZA)). AWS CDK [Scopri di più sulla creazione di landing zone.](#)
- È stato aggiunto il supporto per DHCP con mappatura dei gruppi di sicurezza durante la migrazione di rete. [Scopri di più sulla creazione di gruppi di sicurezza.](#)

Marzo 2026

- Sono state aggiunte API pubbliche per la migrazione di rete, che consentono ai partner e all'accesso programmatico alle funzionalità di migrazione della rete. Consulta il riferimento all'[API per la migrazione di rete.](#)

febbraio 2026

- [La migrazione di rete ora supporta l'acquisizione di file di configurazione firewall o Software-Defined di rete \(SDN\) senza richiedere i dati di rilevamento di RVTools.](#) È possibile utilizzare i file di configurazione firewall o SDN in modo indipendente o combinarli con le esportazioni RVTools.

gennaio 2026

- È stato aggiunto il supporto per il tagging del [Migration Acceleration Program \(MAP\)](#) e il tagging [definito dall'utente](#) sugli elementi di migrazione della rete, che consente di tenere traccia delle risorse di migrazione per scopi creditizi e organizzativi MAP.

dicembre 2025

- È stata aggiunta una nuova [esperienza di migrazione](#) con un flusso di lavoro riprogettato e una migliore usabilità. Per ulteriori informazioni, consulta [Accelerare la migrazione a VMware: AWS](#) la nuova esperienza di Transform.
- Aggiunta la configurazione di [rete Landing Zone Accelerator \(LZA\)](#) per la configurazione automatica delle zone di atterraggio.
- È stato aggiunto il supporto per [più AWS account di destinazione](#) nell'esecuzione della migrazione, che consente di migrare i carichi di lavoro tra account.
- È stato aggiunto il supporto per la migrazione di rete per i formati sorgente [Cisco ACI, Palo Alto e FortiGate ModelizeIT](#).

Ottobre 2025

- Esecuzione della migrazione estesa a [16 regioni target](#) con l'aggiunta dell'Asia Pacifico (Osaka).

settembre 2025

- È stato aggiunto il supporto per la configurazione delle licenze nelle [ondate di rehosting](#), che consente di specificare le opzioni Bring Your Own License (BYOL) o incluse nella licenza per ogni ondata.

- È stato aggiunto il supporto per [Terraform nella migrazione di rete, che consente di implementare l'infrastruttura di rete](#) utilizzando i modelli Terraform.
- È stato aggiunto il supporto per l'aggiornamento della configurazione della sottorete di replica, eliminando la necessità di un VPC predefinito nell'account di destinazione.

agosto 2025

- Esecuzione estesa della migrazione (migrazione e rehosting della rete) a [15 regioni target](#) con l'aggiunta di Stati Uniti orientali (Ohio), Europa (Stoccolma) ed Europa (Irlanda).
- Sono state aggiunte [funzionalità flessibili della gamma CIDR](#) per la migrazione di rete, che consentono di personalizzare gli intervalli di indirizzi IP durante l'implementazione della rete.

Maggio 2025

- Lancio iniziale del servizio [Migrazioni \(incluso VMware\)](#), che fornisce funzionalità di migrazione end-to-end tra cui [individuazione](#), valutazione, [pianificazione della migrazione](#), [migrazione](#) della rete e rehosting del server.
- Esecuzione della migrazione supportata in 12 [regioni target](#): Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Canada (Centrale), Sud America (San Paolo), Europa (Francoforte), Europa (Londra), Europa (Parigi), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Tokyo), Asia Pacifico (Singapore) e Asia Pacifico (Sydney).

Containerizzazione del codice sorgente

AWS Transform supporta la ripiattaforma delle applicazioni in container durante la migrazione verso. AWS Questo capitolo descrive le funzionalità di intelligenza artificiale agentica di AWS Transform per automatizzare la containerizzazione del codice sorgente. Puoi migrare e modernizzare in parallelo, riducendo i tempi e la complessità del passaggio dalle architetture on-premise a quelle native per il cloud. Puoi containerizzare il codice sorgente da GitHub file Bitbucket o.zip, generare immagini Docker GitLab, pubblicare su Amazon Elastic Container Registry (Amazon ECR) e distribuirlo su Amazon Elastic Container Service (Amazon ECS) o Amazon Elastic Kubernetes Service (Amazon EKS). Ciò introduce la containerizzazione nello stesso flusso di lavoro utilizzato per pianificare ed eseguire le migrazioni di rehosting.

Note

La containerizzazione del codice sorgente è progettata per applicazioni non ancora containerizzate. Richiede l'accesso al codice sorgente dell'applicazione e non supporta la migrazione dei carichi di lavoro containerizzati esistenti. Per migrare i contenitori esistenti AWS, utilizza metodi di distribuzione standard per Amazon Elastic Container Service o Amazon Elastic Kubernetes Service.

Funzionalità e caratteristiche principali

AWS Transform offre le seguenti funzionalità per la containerizzazione delle applicazioni.

- **AI-driven analisi del codice sorgente:** analizza il codice sorgente dell'applicazione e genera automaticamente artefatti Docker, inclusi i Dockerfile e i relativi file di configurazione.
- **Creazione e pubblicazione di immagini di container:** crea e testa immagini di container utilizzando le build AI-driven Docker e le pubblica su Amazon Elastic Container Registry con scansione automatica delle vulnerabilità.
- **Infrastruttura come generazione di codice:** genera un'infrastruttura di distribuzione per Amazon Elastic Kubernetes Service (Helm charts) o Amazon Elastic Container Service (moduli Terraform), con convalida e scansione di sicurezza automatizzate.
- **Supporto per dipendenze private:** puoi facoltativamente configurare AWS CodeArtifact repository (Maven, PyPI, npm) e immagini di base private di Amazon ECR come fonti di dipendenza per le tue build.

- Test iterativi e implementazione cutover: implementa l'infrastruttura di test per la convalida, quindi implementa l'infrastruttura definitiva per il cutover della produzione.

Come funziona la containerizzazione

AWS Transform utilizza un AI-powered agente per guidarti attraverso il processo di containerizzazione in un flusso di lavoro basato su chat. AWS Transform coordina attività specializzate come l'analisi del codice sorgente, la generazione di immagini Docker e la creazione dell'infrastruttura. Nei punti chiave del flusso di lavoro, rivedi e approvi l'output prima di procedere.

È possibile accedere alla containerizzazione del codice sorgente creando un processo di migrazione VMware. All'interno del job, puoi eseguire la containerizzazione come flusso di lavoro autonomo o come parte di una migrazione end-to-end quando la strategia di migrazione di a wave è impostata per la containerizzazione. Per ulteriori informazioni sulla migrazione a VMware, consulta. [Migrazioni \(incluso VMware\)](#)

Prerequisiti

Prima di iniziare, assicurati di disporre di quanto riportato di seguito:

- Un'area di lavoro AWS Transform. Per informazioni su come ottenere uno spazio di lavoro, consulta [Guida introduttiva](#).
- Il codice sorgente dell'applicazione in un repository Git accessibile tramite AWS CodeConnections o impacchettato come file zip per il caricamento. I singoli file non devono superare 1 GB e la dimensione totale di tutto il codice sorgente non deve superare gli 8 GB.
- (Facoltativo) Un repository Amazon ECR per la pubblicazione di immagini di container. Puoi configurare l'accesso ad Amazon ECR più avanti nel flusso di lavoro quando sei pronto per la pubblicazione.
- Per le implementazioni Amazon EKS: un cluster Amazon EKS esistente o autorizzazioni per creare l'infrastruttura richiesta.
- Per le distribuzioni Amazon ECS: autorizzazioni per creare cluster Amazon ECS, servizi e risorse correlate utilizzando Terraform, o. AWS CloudFormation AWS Cloud Development Kit (AWS CDK)

Flusso di lavoro di containerizzazione

Il flusso di lavoro di containerizzazione prevede i seguenti passaggi. L'agente AWS Transform ti guida in ogni fase dell'interfaccia di chat.

1. [the section called “Fase 1: Dichiarazione di non responsabilità in materia di sicurezza”](#)— Rivedi e accetta il disclaimer di sicurezza.
2. [the section called “Fase 2: clonare il codice sorgente”](#)— Fornisci il codice sorgente dell'applicazione.
3. [the section called “Fase 3: Containerizzazione”](#)— L'agente AI analizza il codice e genera artefatti Docker.
4. [the section called “Fase 4: Esamina gli artefatti”](#)— Rivedi gli artefatti generati e approva le modifiche al codice.
5. [the section called “Fase 5: Pubblicare immagini”](#)— Pubblica immagini di container su Amazon ECR.
6. [the section called “Fase 6: Generazione di IaC”](#)— Generazione di modelli di distribuzione Amazon EKS o Amazon ECS.
7. [the section called “Fase 7: Implementazione dell'infrastruttura di test”](#)— Implementazione e convalida dell'infrastruttura di test.
8. [the section called “Fase 8: Pulizia dell'infrastruttura di test”](#)— Eliminare le risorse di test.
9. [the section called “Fase 9: Implementazione dell'infrastruttura cutover”](#)— Implementazione dell'infrastruttura di produzione.

Avvio di un processo di containerizzazione

Per containerizzare le applicazioni, è innanzitutto necessario creare un processo di migrazione VMware nell'area di lavoro Transform. AWS Dall'interno del processo, puoi scegliere di eseguire un flusso di lavoro di containerizzazione autonomo o un flusso di migrazione end-to-end che include la containerizzazione.

- Containerizzazione autonoma: containerizza il codice sorgente senza eseguire una migrazione VMware completa. Scegli questa opzione quando desideri containerizzare le applicazioni indipendentemente da qualsiasi migrazione dell'infrastruttura.
- End-to-end migrazione con containerizzazione: esegui l'intero flusso di lavoro di migrazione di VMware con una strategia di migrazione containerizzata assegnata a una o più ondate. Il flusso

di lavoro di containerizzazione viene eseguito come parte della migrazione per tali ondate. Per ulteriori informazioni sulla migrazione a VMware, consulta. [Migrazioni \(incluso VMware\)](#)

Per avviare un processo di containerizzazione

1. Nella pagina iniziale del tuo spazio di lavoro, scegli Crea un lavoro.
2. Scegli la migrazione a VMware.
3. Scegli se eseguire un flusso di lavoro di containerizzazione autonomo o un flusso di migrazione end-to-end che includa la containerizzazione.
4. AWS Transform ti guida attraverso le fasi del flusso di lavoro, a partire da. [the section called “Fase 1: Dichiarazione di non responsabilità in materia di sicurezza”](#)

Autorizzazioni di containerizzazione

Durante il flusso di lavoro di containerizzazione, AWS Transform assegna al cliente un ruolo IAM da utilizzare per creare immagini Account AWS di container e implementare l'infrastruttura. Ti viene chiesto di esaminare e approvare la creazione di questo ruolo prima che il flusso di lavoro continui.

Il ruolo ha un nome `AWSTransformCodeBuildExecutionRole` e viene distribuito tramite uno AWS CloudFormation stack. Include le seguenti politiche gestite.

Politica di base

Fornisce le autorizzazioni di base per il flusso di lavoro di containerizzazione:

- Amazon S3: lettura e scrittura di oggetti in bucket `aws-transform-*`
- Amazon ECR: autentica, estrai immagini (contrassegnate con `Project: atx-migration`) e invia immagini a repository contrassegnati con `CreatedBy: AWSTransform`
- AWS CodeArtifact — Leggi dai repository contrassegnati con `Project: atx-migration`, elenca i repository, ottieni token di autorizzazione e leggi gli endpoint dei repository. Queste autorizzazioni supportano sia la risoluzione delle dipendenze pubbliche che le fonti di dipendenza private configurate durante il flusso di lavoro
- Amazon CloudWatch Logs: crea gruppi di log e stream e scrivi eventi di log per gruppi di log Amazon ECS
- AWS KMS — Descrivi e decrittografa le chiavi (limitate ad Amazon S3 tramite condizioni di servizio)

- Amazon EC2: creazione e gestione di interfacce di rete per progetti VPC-enabled
- AWS CodeConnections — Utilizza le connessioni per accedere ai repository del codice sorgente tramite l'ARN configurato CodeConnections

Politica di rete

Gestisce le risorse di rete per le applicazioni distribuite:

- Elastic Load Balancing: crea, descrivi e gestisci sistemi di bilanciamento del carico, gruppi target, ascoltatori e regole (contrassegnati con) `CreatedBy: AWSTransform`
- Route 53: creazione e gestione di zone ospitate e record DNS
- AWS Cloud Map: crea e gestisci namespace e servizi per l'individuazione dei servizi (contrassegnati con) `CreatedBy: AWSTransform`

Politica di archiviazione

Gestisce le risorse di storage per le applicazioni distribuite:

- Amazon S3: crea e gestisci bucket, tra cui crittografia, controllo delle versioni, ciclo di vita e policy di accesso
- Amazon EFS: creazione e gestione di file system, destinazioni di montaggio e punti di accesso (contrassegnati con `CreatedBy: AWSTransform`)
- Amazon EBS: creazione e gestione di volumi e snapshot (con tag) `CreatedBy: AWSTransform`

AWS KMS policy

Gestisce le operazioni con le chiavi di crittografia:

- Descrivi le chiavi, elenca gli alias e leggi le politiche chiave
- Crittografa, decrittografa e genera chiavi di dati (limitate ad Amazon CloudWatch Logs, Amazon EFS, Amazon EC2 e Amazon S3 tramite condizioni di servizio)

Politica di Amazon ECS

Gestisce le risorse di Amazon Elastic Container Service per le distribuzioni di container:

- Crea e gestisci cluster, servizi e definizioni di attività (contrassegnate con) CreatedBy: AWSTransform
- Registra e annulla le definizioni delle attività, esegui le attività
- Trasferisci i ruoli IAM alle attività e ai servizi di Amazon ECS
- Leggi le informazioni sui ruoli IAM e i certificati ACM
- Descrivi i VPC, le sottoreti, i gruppi di sicurezza e le interfacce di rete di Amazon EC2

Politica di Amazon EKS

Gestisce le risorse di Amazon Elastic Kubernetes Service per le implementazioni Kubernetes:

- Accedi all'API Kubernetes, descrivi i cluster ed elenca i componenti aggiuntivi
- Trasferisci i ruoli IAM ad Amazon EKS

Note

Tutte le autorizzazioni sono limitate al tuo Account AWS indirizzo e. Regione AWS Le risorse create da AWS Transform sono contrassegnate con CreatedBy: AWSTransform e le operazioni di scrittura sono limitate alle risorse con questo tag, ove applicabile.

Fase 1: Rivedi la dichiarazione di non responsabilità sulla sicurezza

Prima dell'inizio del flusso di lavoro di containerizzazione, AWS Transform presenta una dichiarazione di non responsabilità sulla sicurezza che è necessario esaminare e accettare.

Cosa copre il disclaimer

Il processo di containerizzazione richiede l'accesso a Internet per scaricare le dipendenze delle applicazioni (come pacchetti da registri pubblici come npm, PyPI o Maven Central). Il disclaimer sulla sicurezza ti informa che:

- Gli ambienti di compilazione avranno accesso a Internet in uscita per risolvere e scaricare le dipendenze specificate nella configurazione di build dell'applicazione.
- L'utente è responsabile della revisione delle dipendenze richieste dall'applicazione e della garanzia che soddisfino le politiche di sicurezza dell'organizzazione.

- Facoltativamente, puoi configurare fonti di dipendenza private (come AWS CodeArtifact repository o immagini di base private di Amazon ECR) in una fase successiva per evitare il download da registri pubblici.

Cosa devi fare tu

Per esaminare e accettare il disclaimer sulla sicurezza

1. Leggi l'informativa sulla sicurezza presentata da Transform. AWS
2. Accetta il disclaimer per procedere con il flusso di lavoro di containerizzazione.

Dopo aver accettato il disclaimer, AWS Transform passa alla fase successiva in cui fornisci il codice sorgente.

Note

La configurazione del connettore per AWS CodeConnections Amazon ECR non è più richiesta in anticipo. AWS Transform richiede di configurare l'accesso a questi servizi più avanti nel flusso di lavoro, solo quando necessario. Ad esempio, configuri CodeConnections quando scegli di clonare dai repository Git e configuri l'accesso ad Amazon ECR quando sei pronto per pubblicare le immagini dei container.

Fase 2: clonare il codice sorgente

In questo passaggio, fornisci il codice sorgente dell'applicazione a AWS Transform. Puoi fornire il codice sorgente dai repository Git o caricando file zip.

Opzione 1: repository Git

Puoi fornire il tuo codice sorgente dai repository Git. Se non l'hai ancora configurato AWS CodeConnections, AWS Transform ti chiederà di fornire il tuo CodeConnections ARN a questo punto. Hai due modi per specificare i tuoi repository:

- Carica un file CSV: prepara un file CSV con colonne `repo_name` `branch` `repo_nameDeve` essere in `owner/repo-name` formato. La `branch` colonna è facoltativa; lasciala vuota per utilizzare il ramo predefinito del repository. Esempio:

```
repo_name,branch  
owner/my-app,main  
owner/api-service,develop  
owner/another-repo,
```

- Fornisci i dettagli del repository nella chat: comunica a AWS Transform i nomi e i rami del repository direttamente nella chat invece di caricare un file CSV.

AWS Transform verifica che ogni repository esista e sia accessibile tramite la tua CodeConnections configurazione, quindi clona i repository.

Note

I singoli file non devono superare 1 GB e la dimensione totale di tutti gli archivi non deve superare gli 8 GB. AWS Transform clona più repository contemporaneamente per un'elaborazione più rapida.

Important

Le applicazioni che si estendono su più repository non sono supportate tramite l'opzione Git clone. Se la tua applicazione richiede il codice sorgente proveniente da più repository, impacchettali insieme come file zip e usa invece l'opzione di caricamento zip.

Opzione 2: caricamento di file zip

Se non l'hai CodeConnections configurato o preferisci caricare direttamente il codice sorgente, puoi caricare file zip.

Per caricare il codice sorgente come file zip

1. Quando richiesto, carica un file zip per applicazione. Puoi trascinare i file nella chat o utilizzare il pulsante degli allegati.
2. Ogni file zip deve contenere il codice sorgente di un'applicazione.
3. I singoli file non devono superare 1 GB e la dimensione totale di tutti i file caricati non deve superare gli 8 GB.

Facoltativo: configura le dipendenze private

Se la tua applicazione dipende da pacchetti provenienti da registri privati, puoi configurare le fonti di dipendenza private durante questo passaggio. AWS Transform supporta i seguenti tipi di dipendenze private:

- **AWS CodeArtifact repository:** configura i repository Maven, PyPI o npm ospitati in AWS CodeArtifact. AWS Transform presenta un elenco di repository disponibili nel tuo account tra cui scegliere.
- **Immagini di base private di Amazon ECR:** se i tuoi Dockerfile utilizzano immagini di base da un repository Amazon ECR privato, fornisci i dettagli del repository in modo che l'ambiente di compilazione possa estrarre queste immagini.

Quando configuri dipendenze private, AWS Transform ti chiede di connetterti al luogo in cui sono ospitate queste risorse. Account AWS Questa configurazione del connettore è richiesta solo se si utilizzano dipendenze private.

Conferma delle preferenze di containerizzazione

Dopo che il codice sorgente è disponibile, AWS Transform chiede se avete istruzioni specifiche su come eseguire la containerizzazione. Facoltativamente, puoi specificare:

- Se generare un nuovo Dockerfile o riutilizzarne uno esistente.
- Se elaborare un servizio specifico in un monorepo o tutti i servizi.
- Qualsiasi altra preferenza per il processo di containerizzazione.

Le impostazioni predefinite sono:

1. Usa l'immagine base di Amazon Linux 2023 (`public.ecr.aws/amazonlinux/amazonlinux:latest`).
2. Elabora tutte le applicazioni nel repository.
3. Riutilizza un Dockerfile esistente se presente, apportando modifiche minori se necessario.

Puoi confermare di procedere con le impostazioni predefinite o fornire istruzioni specifiche.

Fase 3: Containerizzazione

In questa fase, l'agente AWS Transform AI analizza il codice sorgente dell'applicazione e genera artefatti Docker. AWS Transform esamina la struttura, le dipendenze e i requisiti di runtime dell'applicazione per produrre i Dockerfile appropriati e i relativi file di configurazione.

Cosa succede durante la containerizzazione

L'agente di containerizzazione svolge le seguenti attività:

1. **Analisi del codice sorgente:** AWS Transform esamina i file di progetto, le dipendenze, la configurazione di build e i requisiti di runtime dell'applicazione. AWS Transform sostituisce anche i valori codificati (come gli indirizzi IP del database o i nomi DNS), identifica le variabili di ambiente, rileva i volumi e tenta di reindirizzare i log verso lo standard output.
2. **Generazione di Dockerfile:** in base all'analisi, Transform genera un Dockerfile personalizzato per l'applicazione. AWS
3. **Creazione e test dell'immagine del contenitore:** AWS Transform crea l'immagine del contenitore ed esegue un test per verificare che il Dockerfile produca un'immagine funzionante. Se la compilazione fallisce, AWS Transform esegue automaticamente un'iterazione sul Dockerfile.
4. **Analisi della sicurezza:** AWS Transform analizza gli artefatti generati alla ricerca di valori codificati come credenziali, chiavi API o altri dati sensibili e segnala eventuali risultati per la revisione.

Se hai fornito più repository o un monorepo con più servizi, elabora ogni servizio in parallelo.

Tipi di applicazioni supportati

AWS Transform supporta la containerizzazione dei seguenti tipi di applicazioni:

- **.NET 7 e versioni successive:** containerizzazione ottimizzata per le applicazioni .NET in esecuzione sulla versione 7 o successiva.
- **Applicazioni generali:** containerizzazione per applicazioni create con qualsiasi linguaggio o framework, inclusi Java, Python Node.js, Go e altri.
- **Applicazioni non supportate:** Windows, Xcode o qualsiasi ambiente di compilazione proprietario non sono supportati.

Cosa devi fare tu

Questo passaggio viene eseguito automaticamente. AWS Transform mostra gli aggiornamenti sullo stato di avanzamento man mano che analizza e containerizza ogni applicazione. Se AWS Transform riscontra dei problemi, potrebbe chiederti chiarimenti o informazioni aggiuntive.

Una volta completata la containerizzazione, AWS Transform passa alla fase successiva in cui si esaminano gli artefatti generati. Gli output vengono salvati nell'Artifact Store.

Passaggio 4: rivedi gli artefatti e le modifiche al codice di Docker

In questo passaggio, esaminerai gli artefatti Docker e le modifiche al codice che AWS Transform ha generato durante la containerizzazione.

Revisione delle modifiche dai repository Git

Se hai fornito codice sorgente dai repository Git, AWS Transform esegue il commit delle modifiche alla containerizzazione in un nuovo ramo in ogni repository. Se disponi di più repository, AWS Transform presenta tutte le modifiche come batch per la revisione consolidata.

Per rivedere e approvare le modifiche

1. Esamina i link differenziali di codice forniti da AWS Transform. Ogni diff mostra tutti i file che sono stati aggiunti o modificati, inclusi Dockerfile, file di configurazione ed eventuali modifiche al codice sorgente.
2. Quando AWS Transform presenta la finestra di dialogo di approvazione, approva o rifiuta le modifiche. Per più repository, si approvano tutte le modifiche in un'unica operazione batch.
3. Se approvi, AWS Transform invia le modifiche ai nuovi rami dei tuoi repository.
4. Conferma di essere pronto per procedere al passaggio successivo.

Revisione delle modifiche apportate ai caricamenti in formato zip

Se hai caricato il codice sorgente come file zip, AWS Transform fornisce i link per il download degli artefatti containerizzati. Scarica e rivedi gli artefatti, che includono i Dockerfile generati ed eventuali modifiche al codice sorgente.

Richiesta di modifiche

Se gli artefatti generati necessitano di modifiche, puoi fornire un feedback a AWS Transform, riavvia la fase di containerizzazione con le istruzioni aggiornate e genera nuovi artefatti da esaminare.

Fase 5: Pubblicare immagini

In questa fase, AWS Transform pubblica le immagini dei container su Amazon Elastic Container Registry. Se non hai ancora configurato l'accesso ad Amazon ECR, AWS Transform ti chiederà di fornire i dettagli del tuo repository Amazon ECR a questo punto.

Cosa succede durante la pubblicazione

AWS Transform esegue le seguenti attività per ogni immagine del contenitore:

1. Configurazione del connettore: se non hai già configurato l'accesso ad Amazon ECR, AWS Transform presenta un modulo di connettore in cui fornisci l'ARN del tuo repository Amazon ECR e ti connetti al tuo Account AWS
2. Richiesta di approvazione: AWS Transform presenta l'elenco delle immagini da pubblicare e richiede la tua approvazione. È possibile approvare o rifiutare l'operazione di pubblicazione.
3. Image push: dopo l'approvazione, AWS Transform pubblica le immagini del contenitore nel tuo repository Amazon ECR utilizzando. Se disponi di più servizi, AWS Transform pubblica tutte le immagini in un'unica operazione in batch.
4. Scansione delle vulnerabilità: Amazon ECR analizza automaticamente le immagini pubblicate alla ricerca di vulnerabilità note. AWS Transform riporta i risultati della scansione. Per un'analisi più completa, abilita la scansione avanzata AWS ECR e il monitoraggio del AWS GuardDuty runtime.

Note

La pubblicazione delle immagini viene eseguita in modo asincrono utilizzando. Se la sessione viene interrotta durante la pubblicazione, AWS Transform ripristina automaticamente l'operazione quando ci si riconnette.

Cosa devi fare tu

- Controlla l'elenco delle immagini da pubblicare.

- Approva o rifiuta l'operazione di pubblicazione. Se rifiuti, AWS Transform salta la pubblicazione delle immagini e puoi procedere al passaggio successivo senza immagini pubblicate.
- Controlla i risultati della scansione delle vulnerabilità al termine della pubblicazione.

Dopo la pubblicazione, AWS Transform fornisce gli URI delle immagini utilizzati nelle fasi di distribuzione dell'infrastruttura.

Fase 6: Generazione dell'infrastruttura come codice

In questa fase, AWS Transform genera modelli di AWS infrastruttura per la distribuzione dell'applicazione containerizzata. Puoi scegliere tra Amazon Elastic Kubernetes Service e Amazon Elastic Container Service come piattaforma di destinazione.

Servizio Amazon Elastic Kubernetes (Kubernetes)

Se scegli Amazon EKS, AWS Transform genera grafici Helm con manifesti Kubernetes per la tua applicazione. I modelli generati includono:

- Implementazioni e servizi
- Regole di ingresso
- ConfigMaps e risorse SecretProviderClass
- Account di servizio
- Dichiarazioni di volume persistenti (EBS ed EFS)
- Record DNS Route 53
- Configurazioni Health check

Opzionale: registrazione CloudWatch

AWS Transform chiede se desideri includere la CloudWatch registrazione per la tua distribuzione Amazon EKS. Se attivi, AWS Transform genera una DaemonSet configurazione Fluent Bit che raccoglie i log dei pod e li invia a Logs. CloudWatch

Se scegli la CloudWatch registrazione, l'amministratore del cluster deve completare i seguenti prerequisiti prima della distribuzione:

1. Crea lo spazio dei nomi `amazon-cloudwatch` nel cluster.

2. Crea un ruolo IAM per l'account del servizio Fluent Bit con i permessi di scrittura CloudWatch Logs. Durante la distribuzione viene richiesto il ruolo ARN.

Amazon Elastic Container Service (Terraform)

Se scegli Amazon ECS, AWS Transform genera moduli Terraform per la distribuzione della tua applicazione. I modelli generati includono:

- Cluster ECS
- Servizio ECS con definizioni delle attività
- Application Load Balancer con registrazione degli accessi
- Amazon EFS per lo storage persistente
- Zone private ospitate per l'individuazione dei servizi
- Configurazioni Health check

Convalida e scansione di sicurezza automatizzate

AWS Transform convalida automaticamente i modelli di infrastruttura generati prima di presentarli all'utente. La convalida include:

- Per Terraform: `terraform fmt` e per `terraform validate` verificare la correttezza della sintassi e della configurazione.
- Per Helm: convalida dei grafici per verificare che i manifesti generati siano ben formati.
- Scansione di sicurezza con Checkov per identificare potenziali errori di configurazione di sicurezza nel codice di infrastruttura generato.

AWS Transform segnala eventuali problemi di convalida e li risolve prima di procedere.

Generazione di IAc senza immagini pubblicate

Puoi generare modelli di infrastruttura anche se non hai pubblicato immagini di container nel passaggio precedente. I modelli generati utilizzano URI di immagini segnaposto che è possibile aggiornare in seguito con le posizioni effettive delle immagini.

Cosa devi fare tu

Per generare modelli di infrastruttura

1. Quando richiesto, scegli la piattaforma di destinazione: Amazon EKS o Amazon ECS.
2. Se hai scelto Amazon EKS, AWS Transform ti chiede se includere CloudWatch la registrazione. Rispondi sì o no.
3. Se richiesto, fornisci i dettagli dell'endpoint per il controllo dello stato dell'applicazione (ad esempio un `/health` percorso).
4. AWS Transform genera e convalida i modelli di infrastruttura. Questo passaggio viene eseguito automaticamente e AWS Transform mostra gli aggiornamenti sullo stato di avanzamento, inclusi eventuali risultati di convalida o scansione di sicurezza.
5. Rivedi i modelli generati quando AWS Transform li presenta.

Fase 7: Implementazione dell'infrastruttura di test

In questa fase, AWS Transform implementa l'infrastruttura di test in modo da poter convalidare l'applicazione containerizzata prima del termine della produzione.

Cosa succede durante l'implementazione dei test

AWS Transform implementa i modelli di infrastruttura generati nel passaggio precedente sul tuo Account AWS. Per le implementazioni Amazon EKS, questo utilizza Helm. Per le implementazioni di Amazon ECS, questo utilizza Terraform.

Prima della distribuzione, AWS Transform presenta un modulo di valori dell'infrastruttura in cui è possibile configurare i parametri di distribuzione come i nomi delle risorse, il numero di repliche e le impostazioni specifiche dell'ambiente. AWS Transform genera anche un'anteprima della distribuzione che mostra quali risorse verranno create, in modo da poter rivedere le modifiche prima dell'approvazione.

Cosa devi fare tu

Per implementare e convalidare l'infrastruttura di test

1. Completa il modulo sui valori dell'infrastruttura con la configurazione di implementazione. Il modulo include parametri come i nomi dei cluster, i namespace, il numero di repliche e altre impostazioni specifiche dell'ambiente.
2. Controlla l'anteprima della distribuzione che mostra le risorse che verranno create o modificate.
3. Approva la distribuzione dell'infrastruttura quando AWS Transform la richiede.
4. Attendi il completamento della distribuzione. AWS Transform mostra i risultati della distribuzione.
5. Testa l'applicazione distribuita per verificare che funzioni correttamente in un container e che l'infrastruttura soddisfi i tuoi requisiti.
6. Indica a AWS Transform se sei soddisfatto dell'implementazione o se desideri modificare l'infrastruttura e ridistribuirla.

Iterazione sull'infrastruttura

Se è necessario modificare i modelli di infrastruttura, è possibile caricare modelli aggiornati e ridistribuire:

1. Indica a AWS Transform che desideri modificare l'IAC.
2. Carica un file zip contenente i modelli di infrastruttura modificati.
3. AWS Transform sostituisce i modelli ed esegue un aggiornamento incrementale (Terraform apply o Helm upgrade).
4. Rivedi i risultati di distribuzione aggiornati.

È possibile ripetere questo ciclo finché non si è soddisfatti della distribuzione.

Ripristino della sessione

Le implementazioni dell'infrastruttura vengono eseguite in modo asincrono utilizzando. Se la sessione viene interrotta durante una distribuzione, AWS Transform ripristina automaticamente l'operazione quando ci si riconnette e visualizza i risultati della distribuzione.

Fase 8: Pulizia dell'infrastruttura di test

Dopo aver completato la convalida, AWS Transform demolisce l'infrastruttura di test per evitare costi inutili.

Cosa devi fare tu

Per ripulire l'infrastruttura di test

1. AWS Transform ti informa che l'infrastruttura di test verrà demolita.
2. Approva l'operazione di distruzione quando AWS Transform la richiede.
3. Attendi il completamento della pulizia. AWS Transform visualizza i risultati quando tutte le risorse di test sono state rimosse.

Per le distribuzioni di Amazon ECS, questo passaggio rimuove tutte le risorse create durante la distribuzione di test, incluse risorse di calcolo, bilanciatori del carico, storage e componenti di rete.

Per le implementazioni di Amazon EKS, la pulizia è limitata per etichetta al progetto specifico. Vengono rimosse solo le risorse etichettate per questo flusso di lavoro di containerizzazione. Gli altri carichi di lavoro in esecuzione sullo stesso cluster Amazon EKS non sono interessati.

Fase 9: Implementazione dell'infrastruttura Cutover

In questa fase finale, AWS Transform implementa l'infrastruttura finalizzata per l'uso in produzione. L'implementazione cutover utilizza gli stessi modelli di infrastruttura convalidati durante la fase di test di implementazione.

Cosa devi fare tu

Per implementare un'infrastruttura cutover

1. Completa il modulo sui valori dell'infrastruttura con la configurazione dell'implementazione di produzione. È possibile modificare i parametri della distribuzione di test o utilizzare gli stessi valori.
2. Esamina l'anteprima della distribuzione che mostra le risorse di produzione che verranno create.
3. Approva la distribuzione di produzione quando AWS Transform la richiede.

4. Attendi il completamento della distribuzione. AWS Transform mostra i risultati finali della distribuzione.
5. Verifica che l'applicazione funzioni correttamente nell'ambiente di produzione.

 Important

Rivedi le configurazioni dell'infrastruttura generate con il tuo team per assicurarti che soddisfino i requisiti aziendali, di sicurezza e di conformità dell'organizzazione. Sebbene AWS Transform fornisca consigli di configurazione automatizzati, sei responsabile della convalida e della regolazione delle impostazioni in base alle tue esigenze prima di procedere con l'implementazione definitiva.

Ripristino della sessione

Le implementazioni di produzione vengono eseguite in modo asincrono utilizzando. Se la sessione viene interrotta durante la distribuzione, AWS Transform ripristina automaticamente l'operazione quando ci si riconnette e visualizza i risultati della distribuzione.

Modernizzazione delle applicazioni mainframe

AWS Transform è progettato per accelerare la modernizzazione delle applicazioni mainframe legacy. Orchestra l'analisi delle basi di codice mainframe, genera documentazione, estrae la logica di business, scompone strutture monolitiche, trasforma il codice legacy e gestisce l'intero percorso con input umani (HITL) quando necessario. Le funzionalità di AWS trasformazione di Transform per la modernizzazione e la migrazione delle applicazioni mainframe consentono di modernizzare più rapidamente le applicazioni mainframe critiche, preservando al contempo la logica aziendale critica durante tutto il processo di trasformazione.

Argomenti

- [Funzionalità e caratteristiche principali](#)
- [High-level guida dettagliata](#)
- [Human in the loop \(HITL\)](#)
- [Tipi di file supportati per la trasformazione delle applicazioni mainframe](#)
- [Regioni e quote supportate per AWS Trasforma il mainframe](#)
- [High-level panoramica del percorso di modernizzazione del mainframe](#)
- [Trasformazione delle applicazioni mainframe](#)
- [Crea e distribuisce la tua applicazione modernizzata dopo il refactoring](#)

Funzionalità e caratteristiche principali

AWS Transform offre le seguenti funzionalità per la modernizzazione del mainframe:

- Supporta la modernizzazione delle applicazioni z/OS mainframe scritte in COBOL (Common Business-Oriented Language) e PL/I (Programming Language One) con transazioni JCL (Job Control Language), CICS (Customer Information Control System), schermate BMS (Basic Mapping Support), database Db2 e file di dati VSAM (Virtual Storage Access Method).
- Supporta il refactoring delle applicazioni mainframe Fujitsu GS21 con PSAM (Presentation Service Access Method), set di caratteri giapponesi e file di dati NDB (Network Data Base).
- Esegue ragionamenti, analisi, scomposizione, pianificazione, generazione di documentazione e rifattorizzazione del codice basati su obiettivi.
- Refattorizza automaticamente i carichi di lavoro COBOL-based mainframe in applicazioni Java moderne e ottimizzate per il cloud.

- Orchestra e si integra perfettamente con gli strumenti sottostanti che eseguono analisi, documentazione, scomposizione, pianificazione e rifattorizzazione del codice.
- Ti aiuta a configurare ambienti cloud per applicazioni mainframe modernizzate fornendo modelli Infrastructure as Code (IaC) pronti all'uso.

High-level guida dettagliata

Ecco una guida dettagliata di AWS Transform per la modernizzazione e la migrazione delle applicazioni mainframe.

1. Avvia una chat con AWS Transform e inserisci un obiettivo.
2. In base al tuo obiettivo, AWS Transform propone un piano di modernizzazione, suddividendo l'obiettivo di alto livello in fasi intermedie.
3. A seconda dell'obiettivo che hai fornito, Transform può: AWS
 - Valuta e reinventa la base di codice
 - Crea un lavoro personalizzato in base all'obiettivo

Lungo il percorso, AWS Transform potrebbe chiederti informazioni per eseguire le attività.

Note

Per ulteriori informazioni sulle funzionalità di refactor di AWS Transform for mainframe, consulta [Creare un progetto nella documentazione](#) di AWS Transform for mainframe refactor.

Human in the loop (HITL)

Durante la trasformazione delle applicazioni mainframe, è possibile monitorare l'avanzamento e lo stato delle attività di trasformazione tramite l'esperienza web AWS Transform.

AWS Transform raccoglierà informazioni aggiuntive dall'utente nei seguenti scenari:

- Quando sono necessarie informazioni aggiuntive per eseguire attività.
- Quando è richiesta l'approvazione per artefatti intermedi (ad esempio, la scomposizione dei domini o la pianificazione delle ondate).

- Quando sorgono problemi che AWS Transform non può risolvere automaticamente.

Tipi di file supportati per la trasformazione delle applicazioni mainframe

I tipi di file supportati per z/OS includono:

- Artefatti COBOL e relativi CPY (Copybook)
- PL/I file di origine
- JCL (Job Control Language) e Procedura JCL (PROC)
- Definizione del sistema CICS (CSD)
- BMS (Basic Mapping Support)
- Database Db2
- VSAM (metodo di accesso allo storage virtuale)
- IMS TM (Gestore delle transazioni)

I tipi di file supportati per Fujitsu GS21 includono:

- PSAM (metodo di accesso al servizio di presentazione)
- ADL (linguaggio di definizione AIM)
- NDB (banca dati di rete)

Per ulteriori informazioni su Fujitsu GS21, consultate questi argomenti nella guida alla migrazione AWS Transform for mainframe:

- [GS21](#)
- [Capture & Replay - Terminali GS21](#)
- [Mainframe, AS400, Open VMS e GS21](#)

Regioni e quote supportate per AWS Trasforma il mainframe

Per un elenco delle regioni supportate, consulta [Regioni supportate per AWS Transform](#).

 Note

I tuoi dati potrebbero essere elaborati in una regione diversa da quella in cui utilizzi AWS Transform. Per informazioni sull'elaborazione tra regioni, vedere [the section called “Cross-region elaborazione”](#).

Per i limiti di quota, vedere [Quote](#).

High-level panoramica del percorso di modernizzazione del mainframe

AWS La modernizzazione delle applicazioni mainframe avviene in genere in quattro fasi: (a) valutazione, (b) mobilitazione, (c) migrazione e modernizzazione e (d) gestione, ottimizzazione e innovazione. Ciascuna di queste fasi è ulteriormente descritta in dettaglio con obiettivi e attività associate per supportare il percorso di modernizzazione.

Fasi

- [Fase 1: valutazione](#)
- [Fase 2: Mobilitazione](#)
- [Fase 3: migrazione e modernizzazione](#)
- [Fase 4: gestione, ottimizzazione e innovazione](#)

Fase 1: valutazione

Obiettivo: comprendere la vostra preparazione alla modernizzazione e sviluppare piani di modernizzazione iniziali.

Con AWS Transform puoi valutare le applicazioni, l'infrastruttura e le operazioni del mainframe per determinare il giusto approccio di modernizzazione per le tue esigenze aziendali.

 Note

Ogni fase contiene un elenco di tutte le possibili attività che è possibile svolgere durante la modernizzazione dell'applicazione mainframe. Puoi saltare alcune delle attività che non sono in linea con il tuo caso d'uso o i tuoi obiettivi.

Attività

- Inizia con una conversazione informale sulla modernizzazione e lavora sulla qualificazione delle opportunità coinvolgendo le persone giuste
- Determinate la qualificazione delle opportunità
- Fai una presentazione alla prima chiamata con il piano di mappatura delle dipendenze delle applicazioni e l'architettura dell'applicazione
- Determina il ROM (ordine di grandezza approssimativo) che include i costi dell'infrastruttura durante la migrazione, la manodopera per la migrazione, i costi di post-produzione e la durata del progetto
- Rilevamento rapido del portafoglio:
 - Esegui una valutazione dei modelli e delle linee guida sugli strumenti
 - Esegui un'analisi del codice sorgente
 - Identifica i candidati Proof of Concept (POC)
- Crea una formazione tecnica abilitante:
 - Giornate di immersione
 - Workshop con argomenti generali
- Crea un rapporto MRA (Migration Readiness Assessment) per progetti di modernizzazione dei mainframe di grandi dimensioni o per nuovi clienti AWS
- Crea una dichiarazione di lavoro per la fase Mobilize

Fase 2: Mobilitazione

Obiettivo: costruire le fondamenta e convalidare l'approccio attraverso una serie di prototipi o modernizzazioni pilota di successo.

Con la fase di mobilitazione, è possibile stabilire i framework, gli strumenti e i processi necessari per supportare la modernizzazione del mainframe su larga scala.

Attività

- Dai il via al piano di modernizzazione con un progetto pilota e il POC identificato:
 - Analizza il progetto pilota e configura il codice per la modernizzazione
 - Crea e testa i dati pilota modernizzati

- Fornisci risultati e rivedi il progetto pilota per creare una soluzione dettagliata per una modernizzazione dei dati su larga scala
- Per la piattaforma:
 - Crea un piano di sicurezza, conformità e monitoraggio
 - Configura ambienti di landing zone con landing zone AWS mainframe e struttura degli account
 - Determina l'architettura, l'infrastruttura, l'applicazione, l'integrazione e altro
- Pensa alle persone e ai processi:
 - Cloud Center of Excellence è una buona risorsa
 - Modello operativo
- Crea un'analisi completa del portafoglio per diversi scenari applicativi:
 - Scoperta completa che include documentazione di alto livello
 - Piano di decomposizione (per tutte le applicazioni)
 - Guida ai modelli e agli strumenti per tutte le applicazioni
 - Elaborate un piano iniziale di modernizzazione e migrazione
- Crea una soluzione dettagliata considerando il progetto pilota, la piattaforma, le persone e i processi e un'analisi completa del portafoglio
- Determina il business case
- Completa il progetto pilota di successo con una soluzione per la dichiarazione di lavoro per la fase successiva

Fase 3: migrazione e modernizzazione

Obiettivo: completare la modernizzazione e la migrazione entro i tempi e il budget pianificati.

Durante questa fase, puoi migrare e modernizzare le applicazioni e i dati del mainframe verso AWS

Attività

- Alloca le risorse al codice applicativo pronto per la produzione
- Rivedi e analizza il progetto utilizzando la documentazione esistente o intervistando esperti in materia (PMI)
- Definisci gli scenari di test
- Configura ambienti di modernizzazione con runtime, database e software di terze parti appropriati

- Migra e modernizza il codice sorgente e i dati:
 - È possibile modernizzare l'applicazione in modo iterativo in base ai domini aziendali presenti nel codebase dell'applicazione
 - Scala gli ambienti di modernizzazione in base alle esigenze per supportare i carichi di lavoro di modernizzazione
- Stabilisci una CI/CD pipeline (integrazione continua, distribuzione continua)
- Migra carichi di lavoro selezionati per avviare la modernizzazione.
- Trasferisci i programmi applicativi e regola la scalabilità dell'ambiente in base alle esigenze:
 - È possibile scalare gli ambienti verso l'alto o verso il basso a seconda delle esigenze
 - Modernizza i pacchetti di lavoro eseguendo test di integrità del codice
 - Risincronizza con il codice sorgente, se necessario
- Esegui test completi e verifica la migrazione:
 - Raccogli i dati sullo stato iniziale
 - Registra gli scenari di test sul mainframe
 - Ambiente scenico, applicazione e dati
 - Esegui scenari di test sul cloud
 - Confronta i risultati dei test di origine e di destinazione
 - Crea pipeline automatizzate per l'esecuzione di scenari di test
 - Genera KPI e report
- Convalida i tuoi dati per la configurazione della produzione
- Convalida i tuoi progressi tramite:
 - Esecuzione di test di integrazione e sistema
 - Esecuzione di test delle prestazioni
 - Esecuzione dei test di accettazione degli utenti
 - Esecuzione HA/DR di test
- Definisci un piano di implementazione con il proprietario dell'applicazione e crea un piano per la formazione e il trasferimento delle conoscenze
- Prendi in considerazione il taglio ed esegui i tagli di produzione
- Stabilisci un supporto duraturo per le attività di post-produzione come operazioni, monitoraggio, pianificazione delle capacità e garanzia per le funzioni delle applicazioni

Fase 4: gestione, ottimizzazione e innovazione

Obiettivo: supportare l'eccellenza operativa e il miglioramento continuo delle applicazioni modernizzate.

Dopo la modernizzazione, è possibile ottimizzare le prestazioni, la sicurezza e i costi delle applicazioni AWS sfruttando al contempo i servizi per l'innovazione.

Attività

- Monitora l'applicazione per:
 - Metriche delle prestazioni
 - Pratiche di sicurezza
 - Linee guida sulla conformità
 - Costi
- Dettagli di registrazione
- Gestisci le operazioni delle applicazioni:
 - Gestione dell'infrastruttura
 - Transazioni e gestione del lavoro
 - Supporto per l'ambiente di runtime
- Ottimizzazione e modernizzazione delle applicazioni
- Sviluppo e manutenzione delle applicazioni:
 - IDE di codifica
 - Creazione
 - Integrazione
 - Test in corso
 - Implementazione

Trasformazione delle applicazioni mainframe

AWS Transform accelera la trasformazione delle applicazioni di modernizzazione del mainframe. Questo argomento descrive le funzionalità disponibili.

Argomenti

- [Prerequisito: preparare gli input del progetto in S3](#)
- [Raccolta di artefatti sorgenti per mainframe](#)
- [Sign-in e crea un lavoro](#)
- [Monitoraggio dei progressi della trasformazione](#)
- [Configura un connettore](#)
- [Valuta e reinventa il piano di lavoro](#)
- [Reinventa il piano di lavoro](#)
- [Piano di lavoro personalizzato](#)

Prerequisito: preparare gli input del progetto in S3

AWS Transform è in grado di gestire codebase mainframe complessi. Per utilizzare codebase, assicurati di avere tutte le risorse nella tua posizione S3.

Principali input del progetto:

- Codice sorgente: è necessario caricare i file del codice sorgente del mainframe su S3. Ciò include programmi COBOL, script JCL, quaderni e qualsiasi altro file sorgente pertinente.
- File di dati: se disponi di file VSAM o altri file di dati utilizzati dalle applicazioni mainframe, questi devono essere caricati su S3.
- File di configurazione: includi file di configurazione specifici per il tuo ambiente mainframe.

Altri input del progetto

- Record SMF (System Management Facility): se applicabile, carica i record SMF in una nuova cartella nel bucket S3 in cui è memorizzato il codice sorgente; questi record devono essere in un formato di file.zip.
- Formattazione: per la generazione di documentazione tecnica, è possibile utilizzare un file di configurazione opzionale per generare documenti PDF in linea con i formati e gli standard richiesti, tra cui intestazioni, piè di pagina, loghi e informazioni personalizzate.
- Glossario: AWS Transform AWS Transform sfrutta l'automazione con l'intelligenza artificiale generativa per la generazione di documentazione e l'estrazione di regole aziendali. L'inclusione di un file CSV di glossario con informazioni su abbreviazioni e terminologie importanti nella directory principale del file zip contribuirà a migliorare la qualità della documentazione generata.

- **Dati di test:** se disponibili, carica set di dati di test che possono essere utilizzati per convalidare l'applicazione modernizzata. Questi dati devono essere archiviati in una nuova cartella nel bucket S3 in cui è memorizzato il codice sorgente.

[I dettagli sugli input del progetto sono disponibili qui.](#)

Raccolta di artefatti sorgenti per mainframe

Questo argomento descrive il processo di raccolta del codice sorgente del mainframe e degli artefatti correlati per supportare le iniziative di modernizzazione del mainframe utilizzando Transform. AWS La raccolta e la preparazione adeguate degli artefatti di origine sono fondamentali per il successo dell'analisi, della pianificazione della migrazione e dell'implementazione.

Inventario del codice sorgente

Tipi di codice sorgente dell'applicazione

Sono supportati i seguenti tipi di codice sorgente dell'applicazione:

- Programmi COBOL
- script JCL
- Programmi Assembler
- PL/I programmi
- transazioni CICS
- Programmi naturali
- Script REXX
- Programmi Easytrieve
- Quaderni e articoli inclusi
- Librerie Proc

Risorse del database

Sono supportate le seguenti risorse di database:

- Script DB2 DCLGEN e DDL
- Definizioni del database IMS (PSB e DBD)
- Definizioni dei file VSAM

- Schemi di database fisici e logici
- Procedure e trigger del database

Estensioni dei file del codice sorgente

Se non sei sicuro dell'estensione, lasciala vuota o in formato.txt e AWS Transform la classificherà automaticamente.

La tabella seguente elenca le estensioni di file più comuni per gli artefatti di origine del mainframe.

Estensioni dei file del codice sorgente del mainframe

Language/Type	Estensioni comuni	Description
COBOL	.cbl, .cob, .cobol	Programmi sorgente COBOL
JCL	.jcl	Script Job Control Language
Assemblatore	.asm	programmi in linguaggio Assembler
PL/I	.pl1	PL/I programmi linguistici
Definizione CICS	.csd	definizione del sistema CICS (CSD)
Naturale	.nat	Programmi naturali
REXX	.rex, .rexx	script REXX
Facile trieve	.ezt	Programmi di report Easytrieve
Quaderni	.copy	quaderni COBOL
BMS	.bms	Basic Mapping Support (BMS)
PL/I quaderni	.pl1_copy	PL/I quaderni
Db2 DCLGEN	.dcl	generatore di dichiarazioni Db2
Definizione Db2	.sql, .ddl	Definizioni del database Db2
Definizione IMS	.ims	Set di dati di definizione delle risorse IMS (IMS Stage 1)

Language/Type	Estensioni comuni	Description
MFS	.mfs	IMS MFS (servizio di formattazione dei messaggi)
PSB	.psb	IMS PSB (blocco delle specifiche del programma)
DBD	.dbd	Definizioni del database IMS
JCL Proc	.prc, .proc	Librerie di procedure JCL
JCL include	.inc	JCL Include file
Macro	.mac	Macro Assembler
Schede di controllo	.ctl	Schede di controllo JCL Utility

Metodi di raccolta

Estrazione del codice sorgente

Utilizzate client FTP sicuri (WinSCP/FileZilla) per l'estrazione interattiva del codice sorgente dalle librerie PDS mainframe.

Estrazione dello schema DB2

Il software client DB2 LUW (Linux, UNIX e Windows) include l'`db2look` utilità come parte del pacchetto di installazione. L'`db2look` utilità estrae le istruzioni DDL (Data Definition Language) da un database DB2.

Esegui il comando seguente:

```
db2look -d DATABASE_NAME -i userid -w password -a -e -m -l -x -f -createdb -printdbcfg
-o DATABASE_NAME.sql
```

L'elenco seguente descrive i parametri:

- `-d DATABASE_NAME`: specifica il nome del database da cui estrarre lo schema
- `-i userid`: ID utente per l'autenticazione del database

- -w *password*: password per l'autenticazione del database
- -a: estrae le informazioni di autorizzazione (concessioni)
- -e: estrae tutti gli oggetti del database (tabelle, viste, indici e così via)
- -m: estrae statistiche e caratteristiche fisiche
- -l: estrae i commenti di tabelle e colonne
- -x: gli estratti spiegano le tabelle
- -f: formatta l'output per una migliore leggibilità
- -createdb: include istruzioni per la creazione di database
- -printdbcfg: include i parametri di configurazione del database
- -o *DATABASE_NAME*.sql: specifica il nome del file di output

Estrazione delle informazioni del catalogo dal mainframe

Il comando LISTCAT di IDCAMS è un'utilità per recuperare le informazioni del catalogo sui set di dati sul mainframe. Ciò è utile durante i progetti di modernizzazione del mainframe per inventariare i set di dati e comprenderne le caratteristiche.

```
//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
/*
```

Estrazione delle definizioni CICS

L'utilità IBM-provided DFHCSDUP può estrarre le definizioni delle risorse CICS dal file CICS System Definition (CSD).

Utilizzate il seguente JCL per scaricare le definizioni esistenti dal 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
/*
```

Estrazione delle definizioni IMS

Per estrarre le definizioni IMS, è possibile generare il file di transazione IMS utilizzando l'utilità DFSURDD0. Questa utilità crea istruzioni macro di fase 1 che è possibile utilizzare per scopi di migrazione. Attualmente è supportato solo IMS Stage 1.

Utilizza il seguente JCL per estrarre le definizioni 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
/*
```

Estrazione CA-7 delle informazioni sullo scheduler

CA-7 le informazioni sulla pianificazione delle mansioni sono incluse nei report LJOB. Utilizzate l'utilità LJOB con il LIST=NODD parametro per generare i report sul mainframe. I report devono avere un'.ca7estensione. Ogni rapporto deve contenere caratteri ANSI Carriage Control nella colonna 1. È possibile creare un report con caratteri di controllo del carrello nella colonna 1 specificando DCB=RECFM=FBA (o FA) nel codice JCL utilizzato per eseguire l'utilità LJOB.

Ad esempio: LJOB, JOB=ZBN*, LIST=ALL

[Per ulteriori informazioni, consulta la documentazione di Broadcom.](#)

Estrazione di dati SMF

I record di System Management Facility (SMF) forniscono metriche di attività utilizzate da AWS Transform per analizzare i processi in batch e l'utilizzo delle transazioni CICS. Sono supportati i seguenti tipi di record SMF: 14, 15, 30 (sottotipo 5), 64, 102, 110 (sottotipo 1 con classe di dati 1, 3 e 4).

Requisiti di formato per i record SMF:

- Deve includere i tipi di record 30 e 110 (come minimo)
- Deve essere in formato EBCDIC binario non elaborato con byte RDW (Record Descriptor Word) inclusi
- Deve essere fornito in uno dei seguenti formati:
 - Un file fino a 600 MB compresso in formato.zip
 - Un file di dimensioni fino a 5 GB compresso in formato.tar.gz o .gz
- Deve essere archiviato in una cartella separata dal codice sorgente in Amazon S3

Fornisci almeno 13 mesi di record SMF per acquisire cicli di batch annuali e modelli stagionali che potrebbero non essere rilevati in intervalli di tempo più brevi.

Opzione 1: Estrarre e ordinare i record SMF

Utilizzate il seguente esempio di JCL per estrarre e ordinare i record 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
/*
```

Personalizza i seguenti valori nel JCL precedente:

1. Job card: aggiorna account, classe e msgclass
2. DUMPIN: indica i tuoi set di dati SMF
3. DUMPOUT: specifica il nome del set di dati di output e l'HLQ
4. TIPO: Seleziona i tipi di record (14, 15, 30, 110 o altri)
5. DATA: formato yyyy/ddd (ad esempio 2026/055,2026/056)
6. SPAZIO: regola in base al volume di dati previsto
7. Rimuovi il passaggio SORT se non necessario

Opzione 2: Estrarre i dati SMF con DFSORT

È possibile utilizzare DFSORT per consolidare e riportare i dati SMF storici. Ciò è utile se si archiviano i record SMF in un GDG per giorno o settimana. Il seguente processo utilizza DFSORT per consolidare i record SMF dal file SORTIN e filtrare in base ai record specificati nel parametro 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')
```

Per scaricare i dati conservando i dati RDW, è possibile utilizzare un server FTP per ricevere il file estratto. Assicurati che i dati vengano trasferiti in formato binario e che venga utilizzata l'opzione RDW in modo che l'RDW sia incluso nel trasferimento dei dati. Il seguente job mostra un esempio di job FTP per trasferire questo file.

```
//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
```

Caricamento del rapporto SCRT

Puoi anche caricare un Sub-Capacity rapporto SCRT (Reporting Tool) in Transform. AWS

Caricamento dell'inventario delle applicazioni

Dopo aver raccolto tutti gli artefatti, completa i seguenti passaggi:

1. Organizza i file in sottocartelle per tipo di elemento (ad esempio, /cobol, /jcl, /copybooks, /db2, /ims, /cics, /ca7).
2. Comprimi la cartella di primo livello in un unico file.zip.
3. Carica il file.zip nel bucket Amazon S3 collegato al tuo spazio di lavoro Transform. AWS

 Note

I record SMF devono essere collocati in una cartella separata dal codice sorgente all'interno del bucket Amazon S3 e devono essere in formato.tar.gz o.gz.

Per istruzioni dettagliate su come collegare il bucket Amazon S3 a AWS Transform, consulta. [the section called “Configura un connettore”](#)

Sign-in e crea un lavoro

Per accedere all'esperienza web AWS Transform, segui tutte le istruzioni nella [Nozioni di base su AWS Trasformazione](#) sezione della documentazione.

Per creare e avviare un lavoro: segui la procedura descritta in [Avvia il tuo progetto](#).

Crea area di lavoro: assegna un nome e descrivi l'area di lavoro in cui verranno archiviati i lavori, i collaboratori e gli artefatti associati.

Crea un lavoro: crea un lavoro selezionando tra i piani di lavoro preconfigurati oppure personalizza il piano di lavoro in base al tuo obiettivo selezionandolo dall'elenco delle funzionalità supportate.

 Important

AWS Transform rifiuterà le tue operazioni se non disponi delle autorizzazioni appropriate. Ad esempio, un collaboratore non può annullare un processo di trasformazione delle applicazioni mainframe o eliminare un lavoro. Solo un amministratore può eseguire queste funzioni.

Quando crei il tuo lavoro, puoi scegliere tra le funzionalità seguenti, ma la fase di avvio è sempre obbligatoria in quanto è dove si trova la posizione del codice sorgente del progetto. Nella prima configurazione di un processo in un'area di lavoro è necessario configurare un connettore per il bucket Amazon S3.

Monitoraggio dei progressi della trasformazione

È possibile monitorare l'avanzamento della trasformazione durante l'intero processo in due modi:

- Worklog: fornisce un registro dettagliato delle azioni intraprese da AWS Transform, insieme alle richieste di input umani e alle risposte a tali richieste.

- **Dashboard:** fornisce un riepilogo di alto livello della trasformazione delle applicazioni mainframe. Mostra le metriche relative al numero di lavori trasformati, alla trasformazione applicata e al tempo stimato per completare la trasformazione delle applicazioni mainframe. È inoltre possibile visualizzare i dettagli di ogni passaggio, tra cui righe di codice per tipo di file, documentazione generata per ogni tipo di file, codice scomposto e piano di migrazione.

Configura un connettore

AWS Transform utilizza un connettore per accedere alle risorse del tuo account necessarie per le funzioni di modernizzazione del mainframe. Il connettore viene configurato automaticamente con il primo processo eseguito nell'area di lavoro. A seconda del piano di lavoro scelto, AWS Transform ti guida nella creazione del connettore.

Il mainframe reinventa il connettore

Il connettore di reimmaginazione del mainframe è destinato ai lavori che eseguono i flussi di lavoro di valutazione e reimmaginazione. Utilizza un bucket S3 per accedere e archiviare le risorse di trasformazione, nonché un cluster Amazon Neptune per archiviare gli artefatti estratti. Il cluster Neptune funge da knowledge graph unificato che memorizza tutti gli artefatti estratti sul tuo lavoro e il knowledge graph risponde a tutte le domande nell'interfaccia di chat Transform. AWS

Implementa il cluster Amazon Neptune in un AWS VPC in cui Transform può creare interfacce di rete elastiche (ENI). Queste sono le connessioni di rete che consentono a AWS Transform di comunicare in modo sicuro con Neptune nel tuo VPC per caricare dati e interrogare il tuo Knowledge Graph.

AWS CloudFormation

Si consiglia di utilizzare il seguente CloudFormation modello per creare le risorse necessarie per il connettore mainframe reimagined. Utilizzate lo stesso bucket S3 che intendete utilizzare per il connettore durante l'esecuzione del modello. CloudFormation Per ulteriori informazioni sull'utilizzo dei CloudFormation modelli, consulta [Lavorare con](#) i modelli.

Per scaricare il CloudFormation modello, scegli [neptune-kg-setup.yaml](#).

Il modello accetta i seguenti parametri:

- **BucketName:** obbligatorio Nome del bucket S3 per l'accesso al bulk loader Neptune. È necessario utilizzare lo stesso bucket S3 che si prevede di utilizzare nel connettore Transform. AWS
- **KmsKeyId :** Opzionale. Chiave KMS per la crittografia Neptune. Accetta ID chiave, ARN, nome alias o alias ARN. Il valore predefinito è la chiave gestita se omessa. AWS

Fornisci i seguenti dettagli quando configuri il connettore:

- ARN di bucket S3
- ARN del cluster Neptune
- ID della risorsa del cluster Neptune
- ID di sottorete dell'applicazione
- ID del gruppo di sicurezza dell'applicazione
- Ruolo ARN del caricatore di massa Neptune S3

 Important

La scheda Output del CloudFormation modello include i dettagli da fornire a Transform durante la configurazione del connettore. AWS

Configurazione personalizzata

Se si preferisce utilizzare un VPC esistente o altri strumenti per creare l'infrastruttura richiesta, l'ambiente deve soddisfare i seguenti requisiti:

Ammasso di Nettuno

- Amazon Neptune Serverless con motore versione 1.4.5.1 o successiva
 - Autenticazione IAM abilitata
 - Crittografia dello storage abilitata (chiave AWS gestita o chiave KMS gestita dal cliente)
- Configurazione di scalabilità senza server (consigliata: 1—128 NCU)
- (Consigliato) Leggi la replica in una seconda zona di disponibilità per un'elevata disponibilità e prestazioni di lettura migliorate

Rete

- Un VPC con supporto DNS e nomi host DNS abilitati
- Almeno due sottoreti in zone di disponibilità separate. AWS Transform crea ENI in queste sottoreti per accedere al cluster Neptune, che può risiedere nelle stesse sottoreti o in sottoreti dedicate. Dimensiona le sottoreti a /20 per ospitare gli endpoint VPC e gli ENI delle applicazioni.

- Connettività di rete dalle sottoreti ai seguenti AWS servizi tramite endpoint dell'interfaccia VPC ():AWS PrivateLink
 - AWS API Transform Agents: coordina i lavori di modernizzazione del mainframe
 - Amazon Bedrock Runtime: richiama modelli di base per l'analisi e il ragionamento
 - Amazon Relational Database Service (Amazon RDS) — Gestione dei cluster Neptune
 - Amazon Elastic Compute Cloud (Amazon EC2) — Gestione degli ENI
 - Amazon CloudWatch — Metriche per l'osservabilità delle AWS trasformazioni
- Un endpoint gateway S3 collegato alle tabelle di routing associate alle sottoreti. AWS Transform utilizza questo endpoint per caricare i dati dal bucket S3 al cluster Neptune.

Gruppi di sicurezza

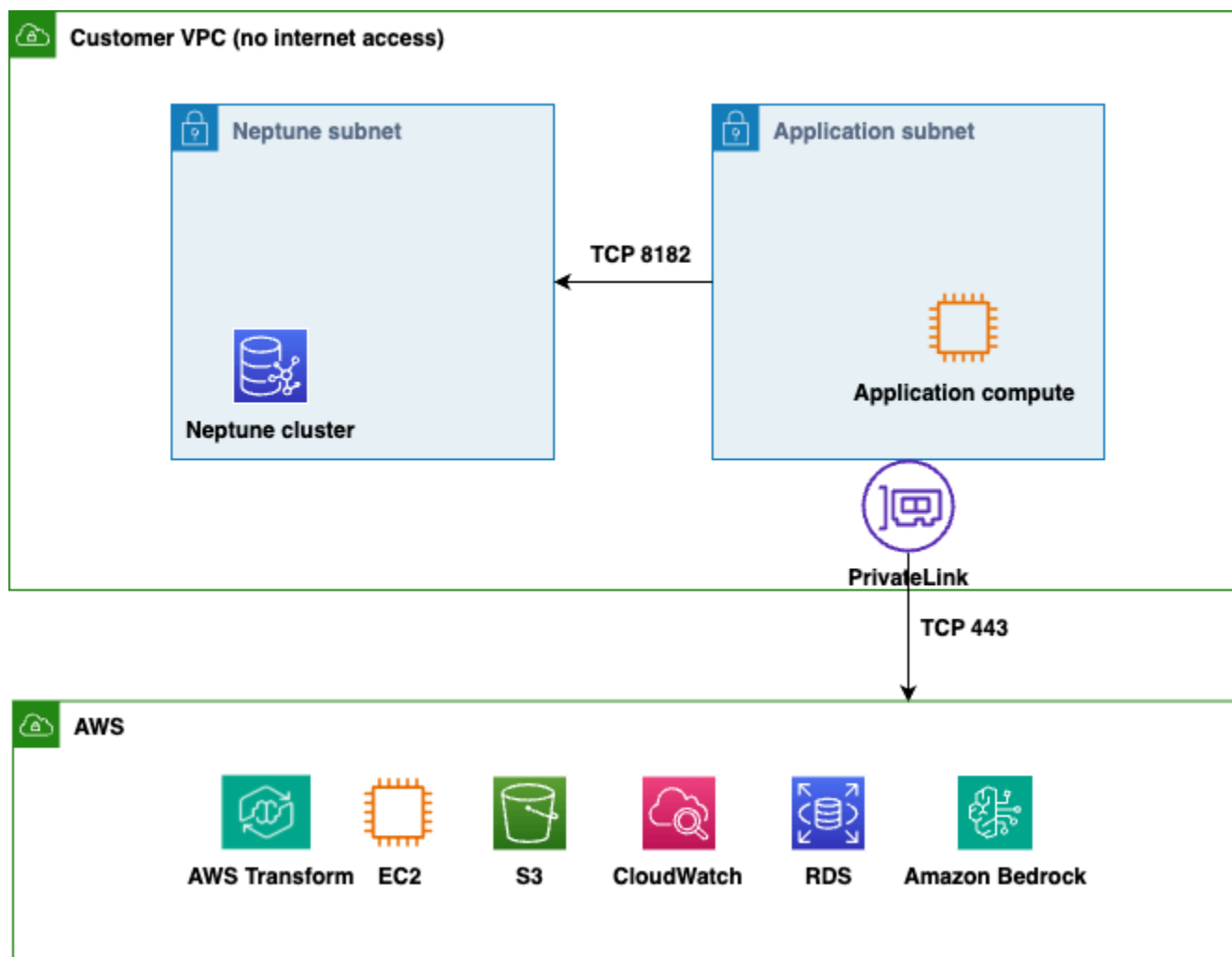
I gruppi di sicurezza sono collegati agli ENI, non alle sottoreti. Anche quando AWS Transform ENI e Neptune risiedono nella stessa sottorete, gruppi di sicurezza separati controllano l'accesso tra di loro.

- Un gruppo di sicurezza (collegato agli ENI creati da Transform) che consente: AWS
 - TCP 8182 in uscita verso il gruppo di sicurezza Neptune
 - TCP 443 in uscita per raggiungere gli endpoint VPC
- Un gruppo di sicurezza (collegato al cluster Neptune) che consente:
 - TCP 8182 in entrata dal gruppo di sicurezza dell'applicazione
- Un gruppo di sicurezza degli endpoint VPC (collegato all'endpoint di interfaccia eNIS) che consente:
 - TCP 443 in entrata dal gruppo di sicurezza dell'applicazione

IAM

- Un ruolo IAM con una policy di fiducia `rds.amazonaws.com` che garantisce `s3:GetObjects3:ListBucket`, e `s3:GetBucketLocation` sul tuo bucket S3
- Questo ruolo deve essere associato al cluster Neptune per il caricamento in blocco dei dati del knowledge graph

Il diagramma seguente mostra l'architettura consigliata.



Connettore S3

Per i lavori con un piano personalizzato, AWS Transform può utilizzare un connettore S3. Il connettore S3 utilizza un bucket S3 per accedere e archiviare le risorse di trasformazione e un bucket vettoriale S3 per l'output indicizzato.

Important

I dati vengono archiviati e resi persistenti nell'archivio di artefatti AWS Transform nell'area di lavoro e vengono utilizzati solo per l'esecuzione del processo.

Configurazione opzionale del bucket vettoriale S3.

Nelle regioni in cui sono disponibili i bucket vettoriali S3, AWS Transform memorizzerà le codifiche vettoriali ricercabili dell'output del lavoro in questo bucket vettoriale S3 del tuo account per fornire un'esperienza di ricerca e chat basata sull'intelligenza artificiale. I dati non vengono utilizzati al di fuori di questo lavoro e non vengono utilizzati per addestrare modelli. Per abilitare ciò, è necessario creare e fornire un bucket vettoriale S3. AWS Transform crea e assegna automaticamente un ruolo con le autorizzazioni necessarie per scrivere in questo bucket.

Autorizzazioni CORS del bucket S3

Dopo aver configurato il connettore, aggiungi la seguente politica CORS al tuo bucket S3 in modo da poter visualizzare e confrontare gli artefatti direttamente nella console Transform. AWS Se questa policy non è configurata correttamente, potresti non essere in grado di utilizzare le funzionalità di visualizzazione in linea o di confronto dei file di Transform. AWS

```
[
  {
    "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
  }
]
```

Valuta e reinventa il piano di lavoro

Il Job Plan di valutazione e reimmaginazione è un flusso di lavoro predefinito per la modernizzazione delle applicazioni mainframe. Ti guida attraverso due fasi: valutazione della tua base di codice

per identificare le funzioni aziendali e reinventare le funzioni selezionate. Per scegliere invece le funzionalità individuali, utilizza il piano di lavoro personalizzato.

Valutazione

I percorsi di modernizzazione del mainframe in genere iniziano con la valutazione della codebase per identificare i contenuti e comprendere le relazioni e le dipendenze. Dopo questa valutazione, è possibile iniziare a scomporre e selezionare parti del codice sorgente da modernizzare. I limiti della decomposizione sono determinati in base alle funzioni aziendali.

Il catalogo delle funzioni aziendali scompone la base di codice in funzioni aziendali discrete, basate su percorsi di dati deterministici che mappano ogni funzione aziendale dall'inizio alla fine. Un percorso dati è il percorso seguito dai dati, a partire da un trigger aziendale fino alla scrittura finale all'interno del codice mainframe. Anziché limitare l'analisi a un unico punto di ingresso, il sistema comprende processi in batch, transazioni CICS e relativi archivi di dati condivisi per identificare unità di lavoro aziendali coerenti.

Una funzione aziendale è un insieme di attività che parte da un fattore scatenante e termina con un risultato aziendale misurabile. AWS Transform offre un catalogo di funzioni aziendali su cui una linea di business può agire, permettendo di prendere decisioni informate su cosa modernizzare per primo.

Vantaggi della valutazione della base di codice per modernizzarla utilizzando le funzioni aziendali:

- Full-estate visibilità: scopri in che modo i processi in batch, le transazioni online e gli archivi di dati si collegano a funzioni significative per la tua azienda.
- Limiti attuabili: ogni funzione aziendale identificata è un'unità autonoma che gli stakeholder del settore possono esaminare e a cui assegnare priorità per la modernizzazione.
- Coerenza dal codice alle specifiche: gli stessi blocchi di codice che definiscono una funzione aziendale vengono utilizzati per generarne le specifiche, senza alcun livello di traduzione e senza la necessità di riconciliazione.
- Tempi di scoperta ridotti: il rilevamento automatico sostituisce mesi di interviste manuali basate su conoscenze tribali con analisi sistematiche e ripetibili.

Risultati della valutazione forniti tramite chat

I risultati della valutazione forniti tramite la chat includono un elenco di funzioni aziendali, incluso il numero di percorsi di dati, il contenuto di ciascuna funzione in termini di transazioni batch e CICS

e una descrizione dell'attività. Ti viene fornito un link agli artefatti generati nel bucket Amazon S3 e puoi accedervi anche tramite la chat. Vengono forniti due elementi: dettagli sulle funzioni aziendali e riepilogo delle funzioni aziendali.

- Riepilogo delle funzioni aziendali: fornisce un elenco delle funzioni aziendali e una descrizione in linguaggio naturale delle funzioni svolte dagli elementi all'interno del codice.
- Dettagli sulle funzioni aziendali: fornisce un grafico interattivo che illustra le relazioni tra il codice sorgente.

Per interagire con il grafico, selezionate un elemento per mostrarne ulteriori dettagli oppure aprite un elemento per interrogarne i dettagli. All'interno di ogni pagina è presente un riepilogo di tutti gli elementi presenti a quel livello e un'interfaccia grafica con cui interagire e ottenere ulteriori informazioni su ciascun componente, tra cui:

- Funzione aziendale: descrive quali funzioni aziendali sono collegate tra loro e fornisce una panoramica di ciascuna funzione aziendale. Quando si seleziona una funzione aziendale, vengono fornite le seguenti informazioni:
 - Numero di percorsi dati
 - Numero di righe di codice
 - Descrizione dell'attività: una panoramica della funzione aziendale che descrive, in linguaggio naturale, quali funzioni svolgono gli elementi all'interno del codice.
 - Interfacce: descrive in dettaglio come si relazionano gli elementi di dati all'interno della funzione aziendale (ad esempio, scambio o scrittura).
- Dettagli delle funzioni aziendali: illustrano le connessioni tra i percorsi di dati all'interno di una singola funzione aziendale, consentendo di approfondire la composizione della funzione aziendale. Quando si seleziona un elemento, viene visualizzato il modo in cui tale elemento si collega tra le diverse funzioni aziendali, oltre ai seguenti dettagli:
 - Datastore: autori e lettori per il datastore.
 - Altri elementi: una panoramica del relativo percorso di dati che descrive, in linguaggio naturale, le azioni e i risultati gestiti all'interno del percorso dati, un elenco di programmi e lettori e scrittori.
- Percorsi dati: illustra i dettagli di un percorso dati e il modo in cui gli elementi all'interno del percorso dati si relazionano tra loro.
 - Descrizione: una panoramica del percorso dei dati che descrive, in linguaggio naturale, le azioni e i risultati gestiti all'interno del percorso dati.
 - Contenuto del percorso dati:

- Punto di ingresso
- Letture
- Scritture
- Programmi

Tramite la chat, è possibile interrogare i risultati per comprendere gli elementi contenuti in ciascuna funzione aziendale ed esplorarne i limiti attraverso il grafico delle funzioni aziendali.

Dopo aver identificato i limiti della modernizzazione, la chat richiede di selezionare le funzioni aziendali che si desidera reimmaginare. È possibile selezionare una singola funzione aziendale o più funzioni aziendali. AWS Transform invia i limiti selezionati e i risultati di valutazione richiesti al flusso di reimmaginazione per continuare il percorso di modernizzazione.

Dopo aver completato la prima modernizzazione, puoi utilizzare la chat per selezionare un set aggiuntivo di funzioni aziendali da modernizzare.

Reimmagina

Nella fase di reimmaginazione, è possibile selezionare una o tutte le funzioni aziendali identificate dalla valutazione e prepararle per la modernizzazione. Ciò attiva l'estrazione della logica aziendale seguita dalla generazione dei requisiti per le funzioni aziendali selezionate. I requisiti generati sono l'input principale per la progettazione avanzata, che traduce la comprensione dei sistemi esistenti in una specifica precisa di ciò che l'applicazione modernizzata deve fornire.

Estrai la logica aziendale

Dopo aver selezionato una o più funzioni aziendali, AWS Transform inizia a generare la logica aziendale per le funzioni aziendali selezionate. Una volta completata l'estrazione, AWS Transform archivia i risultati in un bucket Amazon S3 in formato JSON per l'uso a valle. Puoi monitorare lo stato di avanzamento dell'estrazione ed esaminare eventuali problemi direttamente nella console Transform. AWS

Per esaminare i risultati dell'estrazione secondo la logica aziendale

1. Nel riquadro di navigazione a sinistra, scegli il passaggio Estrai la logica aziendale per espanderlo.
2. Visualizza quanto segue nei dettagli del passaggio:

- **Bucket Link S3:** la posizione in cui i risultati della business logic estratti vengono archiviati in formato JSON.
- **Problemi:** un elenco di tutti i problemi riscontrati durante il processo di estrazione della logica aziendale.

Se alcuni file hanno riscontrato problemi durante l'estrazione, vengono visualizzati i seguenti dettagli per ogni file interessato:

- **Nome file:** il nome del file che ha riscontrato un problema.
- **Tipo di file:** il tipo di file (ad esempio, COBOL o JCL).
- **Percorso del file:** la posizione del file all'interno dell'applicazione.
- **Stato:** lo stato attuale dell'estrazione del file.
- **Dettagli:** una descrizione del problema riscontrato.

Note

Una volta completata la fase di estrazione, AWS Transform inizia automaticamente a generare i requisiti. Non viene richiesto alcun input aggiuntivo prima dell'inizio di questo processo.

Genera requisiti

Una volta completata l'estrazione della logica aziendale, l'agente Generate Requirements consuma gli artefatti estratti (analisi del codice, analisi dei dati, regole aziendali) e produce requisiti di modernizzazione. Questi requisiti sono specifiche funzionali formali indipendenti dalla tecnologia e includono criteri di accettazione verificabili. AWS Transform produce un `requirements.md` file per ogni funzione aziendale selezionata e archivia l'output in un bucket Amazon S3. Per visualizzare la posizione dell'output in Amazon S3, scegli il passaggio Genera requisiti.

Ogni `requirements.md` file è organizzato nelle seguenti parti:

- **Titolo:** nomina la funzione aziendale e il flusso di lavoro che rappresenta.
- **Prerequisiti globali:** condizioni che devono valere per l'intero flusso di lavoro prima e durante l'elaborazione. I valori configurabili vengono visualizzati come segnaposto dei parametri.

- Sezioni numerate del flusso di lavoro: ogni sezione rappresenta una fase distinta della funzione aziendale. Ogni sezione contiene quanto segue:
 - Una storia utente che indica l'obiettivo come ruolo, l'azione che il ruolo vuole intraprendere e il risultato risultante.
 - Un elenco di requisiti in formato EARS (Easy Approach to Requirements Syntax), ciascuno con un identificatore univoco.

Note

La selezione di un secondo set di funzioni aziendali riavvia la fase di reimmaginazione per le nuove funzioni selezionate. La console mostra quindi i risultati solo per la nuova selezione, quindi eventuali problemi con le regole aziendali delle funzioni aziendali precedenti e i link Amazon S3 che memorizzano gli output per la logica e i requisiti aziendali non vengono più visualizzati. I tuoi output precedenti non vengono persi. Puoi comunque accedervi dalla scheda Artifacts o nel tuo bucket Amazon S3.

Tracciabilità tra gli artefatti di trasformazione

AWS Transform mantiene la tracciabilità tra gli artefatti che genera durante tutto il flusso di lavoro di valutazione e reimmaginazione. La tracciabilità consente di ricondurre ogni requisito alle regole aziendali estratte o direttamente al codice sorgente originale che ha prodotto il requisito.

È possibile visualizzare tutti i dettagli di tracciabilità per ogni funzione aziendale utilizzando il file `traceability.yaml`. Descrive in che modo ogni regola aziendale corrisponde a un requisito.

Per la tracciabilità interattiva, puoi utilizzare il plug-in IDE negli editor compatibili con VS Code e Open VSX. [Per ulteriori informazioni, consulta Strumenti per sviluppatori.](#)

Reinventa il piano di lavoro

Per le applicazioni che hai previsto la modernizzazione e che sei pronto a reimmaginare, puoi eseguire un processo di reimmaginazione autonomo. Il processo analizza il codice e i dati, estrae la logica aziendale, identifica i domini aziendali e genera requisiti di modernizzazione per ogni dominio aziendale.

Piano di lavoro personalizzato

Un piano di lavoro personalizzato consente di creare il proprio flusso di lavoro di modernizzazione selezionando le funzionalità che si desidera eseguire. Ti dà il pieno controllo sulle funzionalità incluse. Scegliete tra le seguenti funzionalità in base al vostro obiettivo di modernizzazione. Alcune funzionalità dipendono dal fatto che altre vengano eseguite per prime. Ad esempio, l'analisi del codice è necessaria per la maggior parte delle altre funzionalità.

Analizza il codice

Dopo aver condiviso il percorso del bucket Amazon S3 con AWS Transform, quest'ultimo analizzerà il codice di ogni file con dettagli come nome del file, tipo di file, righe di codice e relativi percorsi.

Note

Puoi scaricare i risultati del codice Analyze tramite la scheda Artifacts a livello di job o workspace. A livello di lavoro, vai all'opzione «Artefatti» nel menu di navigazione a sinistra e apri la cartella «risultati», oppure a livello di area di lavoro trova il nome del lavoro e apri la cartella «risultati». Verrà scaricato un file zip che contiene il file di classificazione per il flusso di lavoro di classificazione manuale, l'elenco delle risorse, il file JSON delle dipendenze e l'elenco dei file mancanti.

Nel piano di lavoro, seleziona Analizza il codice nel riquadro di navigazione a sinistra per visualizzare i risultati. Puoi visualizzare i risultati dell'analisi del codice in diversi modi:

- Visualizzazione a elenco: tutti i file nel bucket Amazon S3 che desideri trasformare per il mainframe
- Visualizzazione del tipo di file: tutti i file nel bucket Amazon S3 vengono visualizzati per tipo di file. Per un elenco dei tipi di file supportati, consulta File [supportati](#).
- Visualizzazione delle cartelle: tutti i file nel bucket Amazon S3 vengono visualizzati nella struttura delle cartelle.

Tra i risultati del file, AWS Transform fornisce le seguenti informazioni a seconda della visualizzazione del file scelta:

- Nome
- Tipo di file

- Righe di codice totali
- Percorso del file
- Righe di commento
- Righe vuote
- Righe di codice efficaci
- Numero di file
- Complessità ciclomatica - La complessità ciclomatica rappresenta il numero di percorsi linearmente indipendenti attraverso il codice sorgente di un programma. AWS Transform mostrerà una complessità ciclomatica per ciascuno dei file.

File mancanti: file mancanti dall'analisi del codice di modernizzazione del mainframe. Idealmente, questi file dovrebbero essere aggiunti come parte dell'input sorgente nel bucket Amazon S3 e la fase di analisi dovrebbe essere rieseguita per ottenere risultati migliori e coerenti.

Nome identico: AWS Transform fornisce un elenco di file che condividono lo stesso nome e possibilmente le stesse caratteristiche (ad esempio, il numero di righe di codice). Non sarà in grado di confrontare la differenza tra i contenuti di due file contemporaneamente.

ID duplicati — Con il programma Cobol, il campo Program ID funge da identificatore univoco del file. Questo ID deve essere unico perché viene utilizzato per chiamare il programma durante tutto il progetto. Tuttavia, alcuni progetti potrebbero avere file COBOL con nomi diversi ma con lo stesso ID di programma. Ottenere l'elenco di questi file durante la valutazione può aiutare a comprendere le dipendenze tra tutti i programmi.

 Note

Questo è specifico per il codice e i file COBOL.

In caso di programmi con ID duplicati, si consiglia di modificare gli ID di programma di questi file in modo da avere un identificatore univoco per ognuno di essi nel codice COBOL. È quindi possibile eseguire nuovamente il processo per ottenere risultati di analisi del codice più accurati e completi.

Risolvendo gli ID di programma duplicati, puoi:

- Migliorare la chiarezza e la manutenibilità del codice

- Riduci i potenziali conflitti nelle chiamate ai programmi
- Migliora l'accuratezza della mappatura delle dipendenze
- Semplifica le attività di modernizzazione future

Problemi relativi al codebase: potenziali problemi rilevati all'interno della codebase che è necessario risolvere prima di continuare con il progetto di modernizzazione. Questi problemi potrebbero includere riferimenti mancanti con istruzioni associate o collegamenti non supportati nel codice.

Aggiorna la classificazione: con la riclassificazione manuale, puoi riclassificare i file utilizzando la funzionalità di aggiornamento in blocco caricando il file JSON con la nuova classificazione.

 Important

Questa opzione è disponibile solo per i file e. UNKNOWN TXT

Dopo la riclassificazione, AWS Transform:

1. Aggiorna i risultati della classificazione
2. Re-runs analisi delle dipendenze con i nuovi tipi di file
3. Aggiorna tutti i risultati delle analisi interessate

 Note

È possibile riclassificare i file solo dopo il completamento del ciclo di analisi iniziale.

Visualizzatore in linea e confronto di file

Il visualizzatore in linea è una funzionalità delle funzionalità di AWS Transform for mainframe che offre due funzionalità di visualizzazione chiave:

- Visualizzazione dei file: visualizza il contenuto di file legacy selezionati dai lavori
- Confronto tra file: confronta il contenuto di due file precedenti fianco a fianco

Visualizzazione dei file di input

Per visualizzare i file in Analizza il codice fase

- In Visualizza i risultati dell'analisi del codice, seleziona un file utilizzando la casella di controllo nell'elenco.

Scegliete il pulsante di azione Visualizza (abilitato quando è selezionato 1 elemento).

Il contenuto del file verrà visualizzato sullo schermo nel componente File View.

Confronto tra file

Per confrontare i file in Analizza il codice fase

1. In Visualizza i risultati dell'analisi del codice, seleziona due file utilizzando le caselle di controllo nell'elenco.
2. Scegliete il pulsante di azione Confronta (abilitato solo quando sono selezionati 2 elementi).
3. I file verranno visualizzati fianco a fianco nel componente di confronto dei file.

Note

Non puoi selezionare più di due file per confrontarli.

Important

Se riscontri problemi con il visualizzatore in linea o il confronto di file, assicurati che il bucket S3 sia configurato correttamente. Per ulteriori informazioni sulla politica CORS del bucket S3, consulta. [the section called “Autorizzazioni CORS del bucket S3”](#)

Analisi dei dati

AWS Transform fornisce l'analisi dei dati per aiutare a comprendere l'impatto delle relazioni e degli elementi dei dati sul progetto di modernizzazione del mainframe. I due output forniti sono:

- Data lineage: traccia il ciclo di vita dei dati mappando le relazioni tra fonti di dati, processi e programmi

- Dizionario dei dati: funge da archivio che documenta i metadati strutturali degli elementi di dati legacy

Al termine dell'analisi, saranno presenti due schede per ogni output, quindi saranno disponibili più visualizzazioni descritte di seguito sia per la derivazione dei dati che per il dizionario.

Note

Quando richiedi l'analisi dei dati, AWS Transform esegue l'analisi del codice, necessaria per eseguire l'analisi dei dati.

Data lineage

AWS Transform offre viste multiple basate sulle relazioni tra i dati che devono essere comprese all'interno della base di codice da modernizzare. Le quattro visualizzazioni tabellari disponibili in Data Lineage includono:

- Set di dati: questa visualizzazione fornisce un'analisi completa dell'impatto, incluso il monitoraggio delle operazioni per aiutare a distinguere tra lettura, scrittura, aggiornamento ed eliminazione
- Tabelle Db2: forniscono l'analisi dell'impatto relativa alle tabelle Db2 e alle operazioni
- Program-to-data: Identifica quali programmi COBOL fanno riferimento a ciascun set di dati
- JCL-to-data relazioni: identifica quali script JCL fanno riferimento a ciascun set di dati

Il riepilogo fornisce una panoramica delle fonti di dati e delle loro relazioni con programmi e JCL, oltre a informazioni di riepilogo su come vengono sfruttate le fonti di dati e sulle operazioni totali presenti nel codebase.

Dizionario dati

Comprendere gli elementi di dati all'interno delle fonti di dati presenti nel codebase è il passo successivo per rendersi conto di come le varie fonti di dati siano dipendenti. Il dizionario dei dati è un catalogo di dati che fornisce metadati a livello di campo con descrizioni in linguaggio aziendale per una mappatura accurata delle trasformazioni.

- Struttura dei dati COBOL: fornisce informazioni sui campi nei quaderni COBOL e nei riferimenti INLINE presenti nel codebase, comprese le proprietà dei campi e la definizione aziendale

- Tabelle Db2: fornisce proprietà di colonne e tabelle tra le tabelle Db2 presenti nella codebase, incluse chiavi primarie ed esterne, informazioni su schemi e indici e tipi di dati

La relazione tra la derivazione dei dati e il dizionario è disponibile selezionando l'origine dati e quindi utilizzando il pulsante Data Lineage o Data Dictionary per approfondire la relazione tra l'origine dati e gli elementi di dati. La navigazione tra la derivazione dei dati e il dizionario offre una visibilità integrata dei dati, mentre la derivazione dei dati fornisce il «cosa», la struttura e il significato, oltre al «dove», l'utilizzo e la relazione.

Analisi delle metriche delle attività

L'analisi delle metriche delle attività consente di analizzare i record SMF (System Management Facility) di tipo 14, 15, 30, 64, 102 e 110. L'analisi fornisce informazioni su come gli elementi vengono utilizzati all'interno dell'applicazione mainframe. Può aiutare a eliminare il codice inutilizzato o a prendere decisioni sull'architettura di destinazione per l'applicazione modernizzata. Se includi l'analisi delle metriche delle attività nel tuo lavoro, il completamento della fase di analisi del codice fornisce innanzitutto risultati SMF più completi, sebbene non sia necessario.

Note

Quando si negozia il piano di lavoro per la modernizzazione del mainframe, il completamento delle fasi di analisi e scomposizione del codice fornisce innanzitutto risultati più ricchi.

Record SMF integrati per l'analisi

È necessario fornire la posizione del record SMF all'interno del bucket Amazon S3 come fase iniziale per l'analisi SMF. Fornisci un minimo di 13 mesi di record per registrare gli eventi annuali che potrebbero non essere rilevati in intervalli di tempo più brevi. Sebbene siano consigliati 13 mesi, qualsiasi periodo di tempo con record SMF rilevabili produce risultati di analisi.

L'estratto SMF deve soddisfare i seguenti requisiti di formato:

- Includi i tipi 14, 15, 30 (sottotipo 5), 64, 102 e 110.
- Utilizza un file binario non elaborato in formato EBCDIC.
- Includi byte RDW.

Fornisci un link ai record SMF all'interno del tuo bucket Amazon S3, assicurandoti che i record si trovino in una cartella separata dal codice sorgente. Le opzioni di formato includono .zip (fino a 600 MB) o .tar.gz (fino a 5 GB) compressi. Se si fornisce un collegamento a una cartella in cui i record SMF non vengono rilevati, viene visualizzato un messaggio di errore e l'analisi non viene completata.

Risultato dell'analisi

L'output dell'analisi contiene due componenti, a seconda del tipo di record: una vista tabulare e un output.csv (disponibile nel bucket Amazon S3). All'interno di AWS Transform, vengono visualizzati gli output per i tipi 30 e 110. Attraverso gli artefatti presenti nel tuo bucket Amazon S3, puoi esplorare l'analisi su altri tipi di record. Nell'interfaccia utente, l'istogramma mostra l'intervallo di tempo dei record forniti in modo da poter identificare eventuali date chiave mancanti. Ad esempio, se i tuoi record vanno dal 1° maggio al 31 ottobre ma escludono il giorno impegnativo dopo il Ringraziamento, puoi vedere che mancano i record chiave. I timestamp nell'applicazione Web riflettono il fuso orario del sistema e i record SMF.

Gli artefatti disponibili in Amazon S3 forniscono analisi per qualsiasi tipo di record presente nei record forniti.

Vista tabellare

La vista tabulare, disponibile solo per SMF 30 e 110, contiene fino a tre componenti principali per i lavori in batch e le transazioni CICS:

- Riepilogo: fornisce i lavori e le transazioni chiave.
- Analisi job/CICS delle transazioni in batch: fornisce analisi aggregate di lavori e transazioni.
- Confronto dell'analisi del codice (solo batch): fornisce dati di confronto quando la fase di analisi del codice viene eseguita prima dell'analisi SMF.

Il riepilogo di scoperta fornisce tre gruppi di lavori e transazioni che consentono di identificare rapidamente gli elementi per un'analisi più approfondita.

L'analisi dei processi Batch e delle transazioni CICS fornisce un'analisi aggregata di lavori e transazioni. Alcune colonne dei risultati dell'analisi sono nascoste per impostazione predefinita. Scegli l'icona a forma di ingranaggio per visualizzare campi aggiuntivi.

La chiave di transazione genera un'aggregazione di dati unica per le transazioni CICS, combinando quattro campi in un unico valore chiave:

- ID della transazione

- Nome del programma
- SysPlex ID
- SysID

È possibile eseguire la ricerca in base alla chiave completa o a qualsiasi componente della chiave nell'output dell'analisi.

Il confronto dell'analisi del codice evidenzia i lavori presenti nei record SMF o nella fase di analisi del codice, ma non presenti in entrambi. Questo mostra i lavori che non sono stati eseguiti durante l'intervallo di tempo di registrazione SMF o che non erano presenti nella fase di analisi del codice. Questo output è disponibile solo quando si esegue la fase di analisi del codice prima dell'analisi SMF nel lavoro.

Best practice

Per ottenere risultati completi per i lavori batch (tipo 30), assicuratevi che il nome del file JCL corrisponda al nome del lavoro per ottenere risultati significativi nel confronto dell'analisi del codice.

Genera documentazione tecnica

È possibile generare documentazione tecnica per le applicazioni mainframe in fase di modernizzazione. Analizzando il codice, AWS Transform può creare automaticamente una documentazione dettagliata dei programmi applicativi, comprese le descrizioni della logica del programma, dei flussi, delle integrazioni e delle dipendenze presenti nei sistemi legacy. Questa funzionalità di documentazione aiuta a colmare il divario di conoscenze, consentendoti di prendere decisioni informate durante la transizione delle applicazioni alle moderne architetture cloud.

Note

Quando richiedi la generazione di documentazione tecnica, AWS Transform esegue l'analisi del codice, inclusa l'analisi delle dipendenze del codice, necessarie per generare la documentazione.

Per generare documentazione tecnica

1. Nel riquadro di navigazione a sinistra, in Genera documentazione tecnica, scegli **Seleziona file e configura le impostazioni**.

2. Seleziona i file nel bucket Amazon S3 per cui desideri generare la documentazione e configura le impostazioni nella scheda Collaborazione.

 Note

I file selezionati devono avere lo stesso tipo di codifica (ovvero, tutti nello stesso CCSID: UTF8 o ASCII). In caso contrario, la documentazione tecnica generata potrebbe avere campi o sezioni vuoti.

3. Scegli il livello di dettaglio della documentazione:

- Riepilogo: fornisce una panoramica di alto livello di ogni file compreso nell'ambito. Inoltre, fornisce un riepilogo di ogni file in una riga.
- Specifiche funzionali dettagliate: fornisce dettagli completi per ogni file nell'ambito della trasformazione delle applicazioni mainframe. Alcuni dettagli includono logica e flusso, dipendenze, elaborazione di input e output e vari dettagli sulle transazioni.

 Note

La documentazione può essere generata solo per i file COBOL e JCL.

4. Scegli Continua.
5. Una volta che AWS Transform genera la documentazione, rivedi i risultati della documentazione seguendo il percorso del bucket Amazon S3 nella console, dove i risultati vengono generati e archiviati.
6. Una volta generata la documentazione, puoi anche utilizzare la chat AWS Transform per porre domande sulla documentazione generata e decidere i passaggi successivi.

Aggiungi le informazioni sull'utente nella documentazione

```
ARTIFACT_ID.zip
### app/
  ### File1.CBL
  ### File2.JCL
  ### subFolder/
    # # File3.CBL
### glossary.csv
### pdf_config.json
```

```
### header-logo.png
### footer-logo.png
# ...
```

È possibile aggiungere file opzionali nel file zip per migliorare la qualità della documentazione generata e fornire una copertina PDF personalizzata. Alcuni di questi possono essere:

- `file glossary.csv`: puoi scegliere di fornire e caricare un glossario opzionale nel file zip del bucket S3. Il glossario è in formato CSV. Questo glossario aiuta a creare documentazione con descrizioni pertinenti in linea con il vocabolario del cliente. Un file di esempio `glossary.csv` ha il seguente aspetto:

```
LOL, Laugh out loud
ASAP, As soon as possible
WIP, Work in progress
SWOT, "Strengths, Weaknesses, Opportunities and Threats"
```

- `pdf_config.json`: puoi sfruttare questo file di configurazione opzionale per generare documenti PDF in linea con i formati e gli standard aziendali, tra cui intestazioni, piè di pagina, loghi e informazioni personalizzate. Un esempio ha il seguente aspetto: `pdf_config.json`

```
{
  "header": {
    "text": "Acme Corporation Documentation",
    "logo": "header-logo.png"
  },
  "customSection": {
    "variables": [
      {
        "key": "business Unit",
        "value": "XYZ"
      },
      {
        "key": "application Name",
        "value": "ABC"
      },
      {
        "key": "xxxxxxxxxxx",
        "value": "yyyyyyyyyyyyyy"
      },
      {
        "key": "urls",
```



```
    "value": [
      {
        "text": "Product Intranet Site",
        "url": "https://example.com/intranet"
      },
      {
        "text": "Compliance Policies",
        "url": "https://example.com/policies"
      }
    ]
  },
  "footer": {
    "text": "This document is intended for internal use only. Do not distribute without permission.",
    "logo": "footer-logo.png",
    "pageNumber": true
  }
}
```

- Intestazione:
 - Per il file PDF della copertina, il testo predefinito sarà il nome del progetto.
 - Per ogni file PDF del programma, il testo predefinito sarà il nome del programma.
 - Non esiste un logo predefinito. Se un logo di intestazione non è configurato, non verrà visualizzato alcun logo.
 - La dimensione del carattere e la dimensione del logo devono essere modificate dinamicamente in base al numero di parole o alla dimensione del file del logo.
- Sezione personalizzata:
 - Se la sezione personalizzata non è configurata, verrà omessa dal PDF.
 - Il link deve poter essere cliccato.
- Piè di pagina:
 - Non esiste un testo o un logo predefinito per il piè di pagina.
 - Per impostazione predefinita, il numero di pagina verrà visualizzato nel piè di pagina, a meno che non venga configurato diversamente in modo esplicito.
 - La dimensione del carattere e la dimensione del logo devono essere modificate dinamicamente in base al numero di parole o alla dimensione del file del logo.

Genera un visualizzatore in linea di documentazione

È possibile visualizzare i file PDF nella fase di generazione della documentazione tecnica.

Per visualizzare i file PDF

1. Vai alla scheda Esamina i risultati della documentazione.
2. Individua il PDF nella tabella che elenca i PDF generati.
3. Seleziona il file e quindi seleziona Visualizza oppure seleziona l'elemento di collegamento sovrapposto al nome del file.

Il PDF si apre in AWS Transform, con la possibilità di espandere lo schermo in alto a destra.

Note

AWS Transform offre anche la possibilità di scaricare una versione XML o PDF della documentazione tecnica generata.

Important

Se riscontri problemi con il visualizzatore in linea della documentazione, assicurati che il bucket S3 sia configurato correttamente. Per ulteriori informazioni sulla politica CORS del bucket S3, consulta [the section called “Autorizzazioni CORS del bucket S3”](#)

Estrai la logica aziendale

È possibile estrarre la logica aziendale essenziale dalle applicazioni mainframe in fase di modernizzazione. AWS Transform analizza automaticamente il codice per identificare e documentare gli elementi aziendali critici, inclusi i flussi di processo dettagliati e la logica aziendale incorporata nelle applicazioni. Questa funzionalità è utile a più parti interessate nel percorso di modernizzazione. Gli analisti aziendali possono sfruttare la logica estratta per creare requisiti aziendali precisi e identificare lacune o incongruenze nelle implementazioni correnti. Gli sviluppatori acquisiscono la capacità di comprendere rapidamente le complesse funzionalità dei sistemi legacy senza una vasta esperienza nel mainframe.

 Note

Quando si richiede l'estrazione della logica aziendale, AWS Transform esegue l'analisi del codice, inclusa l'analisi della dipendenza dal codice e del punto di ingresso, necessarie per eseguire l'estrazione della logica aziendale.

Per estrarre la logica aziendale

1. Nel riquadro di navigazione a sinistra, in Estrai logica di business, scegli Configura impostazioni.
2. Nella scheda Collaborazione, seleziona il modo in cui desideri estrarre la logica aziendale:
 - Livello di applicazione: genera documenti aziendali per tutte le funzioni aziendali, le transazioni, i lavori in batch e i file. In questo modo vengono selezionati tutti i file dell'applicazione.
 - Livello di file: genera documenti aziendali solo per i file selezionati dalla tabella dei file.

 Note

- Per entrambe le opzioni è possibile selezionare Includi specifiche funzionali dettagliate in modo che AWS Transform includa il flusso di controllo e regole aziendali complete per i file selezionati.
- I file selezionati devono avere lo stesso tipo di codifica (ovvero, tutti nello stesso CCSID: UTF8 o ASCII). In caso contrario, la documentazione generata potrebbe avere campi o sezioni vuoti.
- La documentazione può essere generata solo per i file COBOL e JCL.
- A livello di applicazione, i programmi utilizzati dalle transazioni CICS e dai processi batch sono raggruppati insieme, mentre tutti gli altri programmi sono classificati come Non assegnati.

3. Scegli Continua.
4. Una volta estratta la logica aziendale, AWS Transform archivia i risultati in un bucket Amazon S3 in formato JSON in modo da poterli visualizzare online.

 Note

Il numero di file di regole aziendali generati potrebbe essere superiore alla selezione iniziale. Alcuni file selezionati possono attivare l'estrazione delle regole aziendali per includere file dipendenti aggiuntivi, che verranno visualizzati anche nella tabella dei risultati.

Visualizza la documentazione aziendale estratta in linea

È possibile visualizzare la logica aziendale nella fase Estrai la regola aziendale. Per farlo:

1. Vai a Rivedi i risultati dell'estrazione della logica aziendale.
2. Seleziona il documento che desideri visualizzare dalla tabella, quindi fai clic sul pulsante Visualizza risultato.

La pagina della documentazione aziendale si apre in una nuova scheda del browser.

Decomposizione

È possibile scomporre il codice in domini che tengono conto delle dipendenze tra programmi e componenti. Ciò consente di raggruppare in modo appropriato i file e i programmi correlati all'interno dello stesso dominio. Inoltre, aiuta a mantenere l'integrità della logica dell'applicazione durante il processo di decomposizione.

 Note

Quando si richiede la scomposizione, AWS Transform esegue l'analisi del codice, inclusa l'analisi delle dipendenze del codice, necessarie per eseguire la decomposizione. Si consiglia inoltre di eseguire l'estrazione della logica aziendale prima della decomposizione per ottenere risultati migliori.

Per iniziare a scomporre l'applicazione:

1. Seleziona Decomponi codice dal riquadro di navigazione a sinistra.

 Note

Un dominio, Non assegnato, viene creato automaticamente per tutti i file non associati a un dominio. Nella navigazione iniziale, tutti i file devono essere associati a Non assegnato, a meno che i domini non siano stati proposti dall'estrazione della logica aziendale a livello di applicazione.

2. Crea un nuovo dominio tramite il menu Azioni, quindi scegli Crea dominio.
3. In Crea dominio, fornisci il nome di dominio, una descrizione opzionale e contrassegna alcuni file come seed.
 - I file configurati CICS (CSD) e i file configurati dallo scheduler (SCL) possono essere utilizzati per il rilevamento automatico dei semi.
 - È inoltre possibile impostare un solo dominio come componente comune. I file in questo dominio sono comuni a più domini.
4. Scegli Create (Crea).

 Note

Puoi creare più domini con file diversi come seed.

5. Dopo aver confermato tutti i domini e i seed, scegli Decompose.
6. AWS Transform controllerà i file del codice sorgente e quindi si scomporrà in domini con programmi e set di dati con casi d'uso simili e dipendenze di programmazione elevate.

AWS Transform offre una visualizzazione tabulare e grafica dei domini scomposti come dipendenze. La visualizzazione del grafico ha tre opzioni:

- Visualizzazione del dominio: consente di visualizzare in che modo i diversi domini sono correlati tra loro in formato visivo.
- Visualizzazione delle dipendenze: può visualizzare tutti i file di ogni dominio come un grafico delle dipendenze complesso. Se un nodo aggiunto a un dominio non ha ricevuto informazioni da un seed nello stesso dominio, allora questo nodo verrà previsto come non assegnato (il nodo non ha ricevuto alcuna informazione), disconnesso (in un sottografo che non ha ricevuto informazioni sui seed) o inserito in un altro dominio (il nodo ha ricevuto informazioni almeno da quel dominio).

- Visualizzazione sottografo: l'utente può creare sottografi per visualizzare un sottoinsieme di nodi per comprendere più chiaramente l'impatto relazionale e i confini di quella raccolta di nodi.
- Per creare un sottografo, seleziona un gruppo di nodi e seleziona l'opzione Estrai sottografo dalla barra degli strumenti
- È disponibile l'unione dei sottografi, quando si fonde viene creato un nuovo terzo sottografo oltre ai due sottografi che si stanno unendo.

Note

Ripeti questi passaggi per aggiungere altri domini o per riconfigurare i domini già creati con un set di seed diverso se non ti piace la struttura attuale del dominio.

7. Al termine, scegli Continua.

Semi

I semi sono gli input fondamentali per la fase di decomposizione del codice. Ogni componente o file (ad esempio, JCL, COBOL, tabelle Db2, CSD e file di pianificazione) può essere assegnato come base a un solo dominio, garantendo confini e allineamento chiari durante il processo di scomposizione.

L'identificazione dei semi dipende dalla struttura dell'applicazione o del portafoglio. Nel caso di una tipica applicazione mainframe legacy, i seed possono spesso essere determinati aderendo a convenzioni di denominazione stabilite, al raggruppamento a livello di batch nello scheduler e al raggruppamento a livello di transazione definito nel sistema CICS. Inoltre, le tabelle del database possono fungere anche da base, fornendo un altro livello di struttura per la scomposizione.

Importa e and/or aggiorna i file delle dipendenze.

Durante la decomposizione, puoi caricare un file JSON per le dipendenze che sostituisce i file esistenti generati dall'analisi delle dipendenze eseguita da Transform. AWS

La funzione di esportazione delle dipendenze consente di scaricare il file json delle dipendenze generato nella fase di scomposizione. Dopo il download, puoi modificare il file in base alle tue esigenze. Quindi, puoi importare le dipendenze utilizzando la funzionalità di caricamento di AWS Transform che ti consente di caricare il nuovo file JSON delle dipendenze che sostituisce il file generato dall'analisi delle dipendenze. Successivamente, il grafico nella fase di scomposizione verrà aggiornato.

Per esportare, modificare e importare le dipendenze

1. Nella pagina Visualizza i risultati della scomposizione, scegli Azioni.
2. Nell'elenco a discesa, scegli l'opzione Aggiorna il file delle dipendenze in Altre azioni.
3. Nella modalità Aggiorna il file delle dipendenze,
 - a. Scarica il file di dipendenze AWS Transform creato dai risultati dell'analisi esistenti.
 - b. Nel file scaricato, modifica le dipendenze in base a ciò che desideri ottenere.
 - c. Dopo la modifica, salva e carica questo file utilizzando il pulsante Carica file di dipendenza.

Note

L'unico formato di file accettato è il file JSON.

4. Quindi, scegli Importa.

AWS Transform importerà il file delle dipendenze e creerà un nuovo grafico delle dipendenze basato sul tuo input.

Importa and/or e aggiorna domini

Per i clienti che dispongono di domini, seed e relazioni tra and/or file mappati prima della fase di scomposizione, è possibile caricare questa definizione di dominio tramite la funzione Importa file di domini disponibile nel menu Azioni. Alcuni esempi di quando questa funzione può essere utilizzata:

- Anticipa la decomposizione da un altro lavoro
- Esperti in materia che forniscono questa mappatura

Una volta importato il file dei domini, l'utente può eseguire la scomposizione rispetto alla definizione del dominio oppure, se soddisfatto, può salvare e quindi inviare la definizione del dominio.

Parent/child/neighbor file

In un grafico delle dipendenze, i programmi si relazionano tra loro tramite diversi tipi di connessioni. La comprensione di queste relazioni consente di analizzare le dipendenze dei programmi durante la trasformazione delle applicazioni mainframe. Inoltre aiuta a comprendere i confini di un dominio. Ad esempio, se si seleziona un dominio e quindi si seleziona il primo livello principale, verranno visualizzati i nodi connessi.

Relazioni principali: un file principale richiama o controlla altri programmi. I genitori si collocano al di sopra dei programmi dipendenti nella gerarchia. È possibile selezionare il genitore a un livello o a tutti i livelli.

Relazioni tra figli: un file secondario viene richiamato o controllato dal programma principale. I bambini si trovano al di sotto del genitore nella gerarchia dei file.

Relazioni tra vicini: i vicini sono file allo stesso livello gerarchico. Condividono lo stesso programma principale e potrebbero interagire direttamente tra loro.

Reforge il codice

Reforge utilizza Large Language Models (LLM) per migliorare la qualità del codice rifattorizzato. La COBOL-to-Java trasformazione iniziale preserva l'equivalenza funzionale pur mantenendo le strutture di COBOL-influenced dati e i nomi delle variabili del sistema precedente. Reforge ristrutturava questo codice per seguire le pratiche e gli idiomi Java moderni, sostituendo i COBOL-style costrutti con raccolte e convenzioni di denominazione Java native. Ciò rende il codice più leggibile e gestibile per gli sviluppatori Java.

Note

Le quote per il reforge sono:

- 3.000.000 di righe di codice per processo
- 50.000.000 di righe di codice per utente al mese

Reforge il codice dopo il refactoring seguendo questi passaggi:

1. Scegli Reforge java code nel riquadro di navigazione a sinistra, quindi seleziona Configure code reforge.
2. Fornisci la posizione S3 al tuo progetto sorgente compilabile compresso e scegli Continua. Usa questa struttura zip:

```
input.zip
  ### PROJECT-pom
  ### PROJECT-entities
  ### PROJECT-service
  ### PROJECT-tools
  ### PROJECT-web (optional)
```



```
### pom.xml
```

AWS Transform analizza il pacchetto zip per individuare i file all'interno della PROJECT-service directory in modo da fornire un elenco selezionabile di classi che è possibile riforgiare. Queste classi hanno il suffisso. `ProcessImpl.java`

3. Completa la pagina Seleziona le classi da riforgiare e scegli Continua. Tieni traccia dello stato della riforgiatura nella scheda Worklog.
4. Visualizza i risultati del reforge completato nella pagina Visualizza i risultati, che mostra lo stato del reforge per classe. Inoltre, specifica dove trovare il risultato Reforge nel bucket S3.

Una volta che AWS Transform riceve questo input da te, ti fornisce un file scaricabile con i risultati di Reforge.

Questa è la struttura zip risultante da un reforge riuscito:

```
reforge.zip
### maven_project
### reforge.log
###tokenizer_map.json
```

- `maven_project` contiene il codice sorgente riforgiato.
- I file che sono stati rifattorizzati ma la cui compilazione non è stata completata correttamente si trovano in e sono denominati. `/src/main/resources/reforge/originalClassName.java.incomplete` Confrontali con le versioni originali dei file per scegliere le funzioni riforgiate che desideri salvare.
- I file sorgente forniti a AWS Transform che sono stati rifattorizzati correttamente vengono sottoposti a `src/main/resources/reforge/originalClassName.java.original` backup e denominati. `originalClassName.java.original` Le versioni rifattorizzate dei file sostituiscono i file sorgente forniti a Transform. AWS

Note

I `originalClassName.java` file vengono sostituiti con i file riforgiati solo se il processo di riforgiatura ha esito positivo. In caso contrario, conservano il contenuto originale.

- `reforge.log` contiene log che è possibile utilizzare per diagnosticare gli errori dei processi o fornire AWS assistenza in caso di problemi.

- `tokenizer_map.json` contiene una mappatura degli ID dei token rispetto ai dati, come i percorsi e `class/method` i nomi dei file, che vengono tokenizzati nei log per la protezione della privacy. Puoi fornire questo file all'assistenza in caso di problemi. AWS

Pianificate i test delle vostre applicazioni modernizzate

Puoi creare e gestire piani di test per le tue applicazioni mainframe modernizzate in base agli attributi del codice estratti, alla complessità del lavoro e ai percorsi di pianificazione. AWS Transform aiuta a dare priorità ai lavori da testare e identifica gli artefatti specifici necessari per ogni test case. Il processo di pianificazione dei test è suddiviso in tre fasi principali: configurazione, ambito e revisione.

Per creare un piano di test

1. Configurare le impostazioni del piano di test
 - a. Nel riquadro di navigazione a sinistra, sotto Pianifica i tuoi test, scegli Configura impostazioni.
 - b. (Facoltativo) Fornisci percorsi S3 per Business Logic Extraction (BLE). Questi artefatti migliorano la qualità del piano di test. Senza artefatti BLE, alcuni campi del piano di test potrebbero rimanere incompleti.
2. Definisci l'ambito del piano di test
 - a. Seleziona i punti di ingresso, come i lavori in batch, da includere nel tuo piano di test.
 - b. Filtra e ordina i lavori in base a più attributi:
 - Funzioni aziendali (estratte da BRE BLE)
 - Domini (dalla fase di decomposizione)
 - Percorsi e posizioni dei file
 - Criteri di ricerca personalizzati
 - c. Seleziona singoli lavori o interi gruppi per i test.
 - d. Rivedi i rapporti di lavoro e le dipendenze.
3. Rivedi e modifica il piano di test

Il piano di test generato fornisce informazioni complete, tra cui:

- Ordine di esecuzione preferito basato sulle dipendenze
- Assegnazioni di gruppi di lavoro da scheduler

- Punteggi di complessità, che sono punteggi aggregati per i casi di test
- Associazioni di domini aziendali
- Metriche di complessità ciclomatica
- Dipendenze tra set di dati e tabelle
- Righe di codice, metriche
- Mappature delle funzioni aziendali

Opzioni di personalizzazione del piano di test

Il piano di test può essere personalizzato per soddisfare esigenze specifiche. Ad esempio, puoi:

- Crea nuovi casi di test selezionando più punti di ingresso
- Unisci i casi di test esistenti per combinare le funzionalità correlate
- Suddividi i casi di test per test più granulari
- Rimuovi i casi di test non necessari
- Aggiungi o rimuovi punti di ingresso per i casi di test esistenti
- Modifica le descrizioni e gli attributi dei test case
- Modifica l'ordine di esecuzione

Informazioni dettagliate sul test case

Ogni test case fornisce dettagli che ne descrivono il contenuto e il relativo set di dati o file di dati:

- Descrizione completa dell'ambito del test
- Elenco completo dei punti di ingresso incluso
- Metriche aggregate che mostrano complessità e dimensioni
- Regole aziendali e linee guida automatizzate ai test case
- Dipendenze tra set di dati e tabelle con direction () input/output
- Visualizzazione interattiva del grafico delle dipendenze
- Prerequisiti e requisiti di esecuzione

Funzionalità di gestione dei dati

Questi dettagli consentono di comprendere i dati relativi al test case. Puoi:

- Filtra i set di dati per input/output direzione
- Identifica gli artefatti necessari per l'esecuzione del test
- Tieni traccia delle dipendenze dei dati tra i casi di test
- Monitora l'utilizzo dei set di dati tra i piani di test

Note

AWS Transform analizza automaticamente le dipendenze dello scheduler e assegna punteggi di complessità per aiutare a dare priorità alle attività di test. I punteggi di complessità più elevati indicano lavori che potrebbero richiedere test o isolamento più approfonditi durante il processo di test.

Regole aziendali e linee guida ai test case

Il piano di test AWS Transform fornisce consigli per il piano di test case basato su Business Rule Extraction:

- Elaborazione automatica delle regole aziendali tramite LLM
- Generazione di casi di test sintetici
- Linee guida ai test per scenari aziendali specifici
- Tracciabilità tra regole e casi di test

Il piano di test finale viene archiviato nella posizione S3 specificata e include tutte le informazioni necessarie per eseguire la strategia di test in modo efficace. Puoi esportare il piano di test per l'integrazione con altri strumenti di test o sistemi di documentazione.

Note

Sebbene vengano fornite indicazioni sintetiche sui test case, gli artefatti dei test effettivi devono essere creati separatamente sulla base delle linee guida. Il piano di test funge da modello completo per la strategia di test, ma non genera i dati di test o gli script di esecuzione.

Regole per la creazione dei test case - Riepilogo

Regole generali

- Un test case contiene da 1 a più JCL nell'ordine di esecuzione programmato
- I test case vengono creati da pianificatori supportati validi (CA7 e) Control-M
- Il test esegue JCL, non lo scheduler stesso o le attività pianificate
- Un'attività pianificata è unica ed esegue solo un JCL
- Un JCL può essere eseguito da più attività pianificate
- Un JCL può esistere senza essere inserito in una pianificazione

Regole predefinite per la creazione dei test case

- Se un singolo JCL è in un test case:
 - JCL non è coinvolto in un programma
 - JCL viene eseguito da un'attività pianificata che diverge in più rami
 - Un ramo nella pianificazione contiene solo questo JCL
- Se più JCL in un test case: rappresenta una sequenza di percorso di esecuzione lineare all'interno di un ramo di pianificazione
- Se JCL svolge un'attività pianificata divergente: JCL diventa un test case separato
- Se JCL svolge un'attività pianificata convergente: JCL può avviare un nuovo test case ma non sarà incluso nei rami precedenti
- I JCL mancanti vengono ignorati e l'esecuzione continua (con future miglirie pianificate per ridurre il test case al punto JCL mancante)

Regole operative per gli utenti

- Create Test Case: l'utente seleziona tra i JCL disponibili
 - Ha successo se esistono JCL nella sequenza del ramo di esecuzione della pianificazione
 - Segue l'ordine di esecuzione della pianificazione
- Aggiungi un JCL al Test Case: l'utente seleziona tra i JCL disponibili
 - Ha successo se JCL può esistere nell'esecuzione della pianificazione del test case branch/path
- Rimuovi JCL dal test case: l'utente può rimuovere qualsiasi JCL da un test case
 - Consentito anche se causa lacune nel percorso di esecuzione

- Unisci casi di test: l'utente seleziona due casi di test da combinare
 - Ha successo se i JCL possono esistere insieme nello stesso ramo di esecuzione della pianificazione
 - Mantiene l'ordine di esecuzione della pianificazione
- Split Test Case: l'utente seleziona un JCL in un test case per split
 - Crea un nuovo test case da split point in avanti
 - Test case originale modificato per escludere JCL dopo il punto di divisione
- Elimina test case: l'utente può eliminare qualsiasi test case creato

Note

Non è possibile creare, aggiungere o unire casi di test da diversi scheduler branches/path. Sono previste future migliorie per consentire operazioni che vanno oltre le divergent/convergent attività dello scheduler.

Genera script di raccolta dei dati di test

È possibile generare script JCL per raccogliere dati di test dai sistemi mainframe in base al piano di test creato nel passaggio precedente. AWS Transform crea automaticamente script di raccolta dati per set di dati, tabelle di database e file sequenziali necessari per test completi. Il processo di raccolta dei dati è suddiviso in quattro fasi principali: configurazione degli input, selezione dei test case, configurazione degli script e generazione degli script.

Per generare script di raccolta dei dati di test

1. Fornisci un input per il piano di test
 - a. Nel riquadro di navigazione a sinistra, in Raccolta dei dati di test, scegli Fornisci l'input del piano di test.
 - b. Specificate il percorso S3 del file JSON del piano di test da [Pianifica il test delle vostre applicazioni modernizzate](#).
 - c. Il campo di input è precompilato se il piano di test è stato generato in una fase di lavoro precedente.
 - d. Puoi anche selezionare il piano di test tra altri lavori specificando la posizione S3 appropriata.

2. Seleziona i casi di test per la raccolta dei dati

- a. Consulta l'elenco completo dei casi di test inclusi nel tuo piano di test.
- b. Filtra e ordina i casi di test in base a più attributi:
 - Funzioni e domini aziendali
 - Dipendenze delle tabelle del database
 - Requisiti del set di dati
 - Metriche di complessità
 - Criteri di ricerca personalizzati
- c. Seleziona singoli casi di test o utilizza opzioni di selezione collettiva.
- d. Rivedi i dettagli del test case, inclusi punti di ingresso, metriche e regole aziendali, facendo clic su un test case per visualizzare i dettagli.

3. Configura gli script di raccolta dati

- a. Scarica modelli di esempio e file di configurazione come riferimento.
 - AWS Transform fornisce modelli di esempio per lo scaricamento del database Db2, il file VSAM REPRO e l'elaborazione sequenziale di set di dati da utilizzare come guida sui tipi di modello previsti dal processo.
 - Gli standard possono variare da sito a sito, pertanto ci si aspetta che i clienti modifichino o sostituiscano questi modelli conformi ai propri standard.
 - Questi modelli modificati devono essere caricati in un bucket S3 dove la raccolta dei dati di test possa elaborarli.
- b. Fornisci un file di configurazione variabile (formato JSON) contenente:
 - Prefissi utente e costanti specifiche dell'ambiente
 - Parametri di configurazione del database
 - Impostazioni dell'endpoint di destinazione e parametri di trasferimento dei dati
 - Altri parametri richiesti definiti dall'utente e da utilizzare nei modelli JCL
- c. Carica modelli JCL per diversi metodi di raccolta dati:
 - Modello Db2: per lo scaricamento delle tabelle del database (personalizzabile per BMC, IBM DSN o altre utilità di scaricamento)
 - Modello VSAM: per l'elaborazione di file VSAM (in genere utilizza l'utilità REPRO)

- Modello di set di dati sequenziali: per l'elaborazione di set di dati sequenziali, set di dati partizionati, GDG ecc.

4. Rivedi e gestisci gli script generati

Gli script generati forniscono funzionalità complete di raccolta dati, tra cui:

- Script separati per la raccolta dei dati «prima» e «dopo» l'esecuzione del test
- Struttura degli script organizzata per test case e tipo di dati
- Gli script vengono archiviati automaticamente nel bucket S3 per un facile accesso e trasferimento
- Gli script JCL generati sono pronti per l'esecuzione su mainframe
- La sostituzione delle variabili si basa sulla configurazione utente definita nei modelli

Funzionalità di generazione di script

Gli script generati vengono personalizzati automaticamente in base ai modelli e alla configurazione:

- Template-based generazione: utilizza i modelli JCL forniti con sostituzione di variabili
- Ambiente: incorpora la configurazione specifica del mainframe
- Gestione dei tipi di dati: crea script appropriati per set di dati sequenziali, file VSAM e tabelle di database
- Raccolta per casi di test: genera script di raccolta dati «prima» e «dopo»
- Elaborazione sequenziale di set di dati: l'esempio AWS fornito fornisce una funzione di trasferimento di file, ma questa può essere personalizzata con le utilità di compressione disponibili sul sito o utilità come Connect Direct o il trasferimento gestito di file ecc.

Strategia di raccolta dei dati

Gli script generati supportano strategie complete di raccolta dati:

- Raccolta sequenziale di set di dati: REPRO e utilità di copia per VSAM e file flat
- Scaricamento delle tabelle del database: processi di scaricamento Db2 personalizzabili
- Elaborazione sequenziale di set di dati: post-elaborazione personalizzabile di set di dati sequenziali come compressione, servizi di trasferimento di file gestiti ecc.
- Gestione delle dipendenze: raccolta coordinata basata sulla definizione del test case

 Note

AWS Transform genera script basati sui modelli e sulla configurazione. Esaminare tutti i file JCL generati prima di eseguirli sull'ambiente mainframe per garantire la compatibilità con la configurazione di sistema e i requisiti di sicurezza specifici.

Personalizzazione dei modelli e best practice

ATX Test Data Collection offre funzionalità flessibili di personalizzazione dei modelli:

- Multi-utility supporto: Adatta i modelli per diverse utilità mainframe (BMC, IBM, DSN)
- Variable-driven configurazione: utilizza le costanti per i parametri specifici dell'ambiente
- Modelli riutilizzabili: crea modelli standardizzati per una generazione coerente di script
- Gestione dei dati: incorpora i requisiti di gestione dei dati specifici dell'organizzazione
- Integrazione della sicurezza: includi controlli di sicurezza e accesso appropriati
- Ottimizzazione delle prestazioni: configurazione per una raccolta e un trasferimento efficienti dei dati

Struttura di output generata

Gli script generati sono organizzati nel tuo bucket S3 con la seguente struttura:

- Organizzazione dei test case: script raggruppati per casi di test associati
- Tempi di raccolta: cartelle separate per la raccolta dei dati «prima» e «dopo»
- Classificazione dei tipi di dati: script organizzati per set di dati sequenziali, tabelle di database e trasferimenti
- File di metadati: informazioni di riepilogo e linee guida all'esecuzione
- Ready-to-transfer formato: JCL formattato per l'implementazione diretta su mainframe

La raccolta finale degli script viene archiviata nella posizione S3 specificata e include tutto il JCL necessario per eseguire efficacemente la strategia di raccolta dei dati. È possibile scaricare gli script per trasferirli nell'ambiente mainframe o integrarli con processi di distribuzione automatizzati.

 Note

Sebbene vengano generati script JCL completi, l'esecuzione effettiva deve essere eseguita sull'ambiente mainframe. Gli script fungono da strumenti di raccolta dati pronti all'uso, ma richiedono l'accesso al mainframe e le autorizzazioni di esecuzione appropriate.

Generazione di script di automazione dei test

È possibile generare script di automazione dei test per eseguire casi di test sulla propria applicazione modernizzata in base al piano di test creato nel passaggio precedente. AWS Transform crea automaticamente script di test completi che utilizzano i dati raccolti dal processo di raccolta dei dati di test. Il processo di generazione degli script di automazione dei test consiste in tre fasi principali: configurazione degli input, selezione dei test case e risultati della generazione degli script.

Per generare script di test

1. Fornisci un input per il piano di test
 - a. Nel riquadro di navigazione a sinistra, in Generazione di script di automazione dei test, scegli Fornisci l'input del piano di test.
 - b. Specificate il percorso S3 del file JSON del piano di test in [Pianifica il test delle vostre applicazioni modernizzate](#).
 - c. Il campo di input è precompilato se il piano di test è stato generato in una fase di lavoro precedente.
 - d. Puoi anche selezionare il piano di test tra altri lavori specificando la posizione S3 appropriata.
 - e. Il sistema utilizza questo piano di test come base per la generazione di script di automazione.
2. Seleziona i casi di test per la generazione di script
 - a. Consulta l'elenco completo dei casi di test inclusi nel tuo piano di test.
 - b. Filtra e ordina i casi di test in base a più attributi:
 - Funzioni e domini aziendali
 - Dipendenze delle tabelle del database
 - Requisiti del set di dati

- Metriche di complessità
- Criteri di ricerca personalizzati
- c. Seleziona singoli casi di test o utilizza le opzioni di selezione collettiva con i pulsanti Seleziona tutto e Deseleziona tutto.
- d. Rivedi i dettagli dei test case, inclusi i punti di ingresso, le metriche e le regole aziendali, facendo clic sui singoli casi di test.

I casi di test selezionati avranno script di automazione generati per l'esecuzione sull'applicazione modernizzata.

3. Rivedi e gestisci gli script di automazione dei test generati:

- Il sistema visualizza un messaggio di conferma del completamento della generazione dello script.
- Gli script di test generati vengono archiviati automaticamente nella posizione specificata del bucket S3.
- Accedi all'elenco completo degli script di test generati con le rispettive posizioni S3.
- Ogni test case ha lo script di automazione corrispondente memorizzato in singole posizioni S3.
- Gli script sono pronti per la distribuzione e l'esecuzione nel tuo ambiente applicativo modernizzato.

Testate le funzionalità degli script di automazione

Gli script di automazione generati forniscono funzionalità di test complete:

- Test delle applicazioni modernizzati: gli script sono progettati specificamente per eseguire casi di test sull'applicazione trasformata
- Integrazione dei dati: utilizza i dati di test raccolti nella precedente fase di raccolta dei dati di test, questi dati devono essere copiati nelle cartelle per ogni caso di test
- Esecuzione automatizzata: gli script possono essere utilizzati per configurare data sink, eseguire casi di test e confrontare i risultati, alcuni parametri dovranno essere impostati in base all'ambiente di distribuzione
- Struttura organizzata: gli script sono organizzati sistematicamente per test case nel bucket S3
- Ready-to-deploy formato: gli script sono formattati per la distribuzione diretta nell'ambiente di test

Struttura di output generata

Gli script di automazione dei test generati sono organizzati nel bucket S3 con la seguente struttura:

- Organizzazione del test case: ogni test case ha il suo script dedicato memorizzato nella singola cartella S3
- Execution-ready formato: gli script sono formattati per la distribuzione e l'esecuzione immediate dopo aver impostato alcune variabili a seconda dell'ambiente
- Accesso centralizzato: tutti gli script sono accessibili da un unico bucket S3 per una gestione semplificata

Strategia di esecuzione dei test

Gli script generati supportano flussi di lavoro completi per l'esecuzione dei test:

- Configurazione dell'ambiente: gli script includono funzionalità per l'impostazione dei dati iniziali per l'esecuzione del test
- Preparazione dei dati: integrazione con i dati di test raccolti dalla fase di raccolta dei dati del test case
- Esecuzione del test case: esecuzione automatizzata di singoli casi di test sull'applicazione modernizzata
- Confronto dei risultati: Built-in funzionalità per confrontare i risultati dei test e convalidare il comportamento delle applicazioni

Note

AWS Transform genera script di automazione dei test basati sul piano di test e su casi di test selezionati. Gli script sono progettati per l'esecuzione in un ambiente applicativo modernizzato e utilizzano i dati di test raccolti nel passaggio precedente. Esamina tutti gli script generati prima della distribuzione per garantire la compatibilità con la configurazione e i requisiti di test specifici dell'applicazione.

Le migliori pratiche per l'automazione dei test

- Convalida dell'ambiente: assicuratevi che l'ambiente applicativo modernizzato sia configurato correttamente prima dell'esecuzione dello script

- **Verifica dei dati:** verifica che i dati di test richiesti dalla fase di raccolta siano disponibili e accessibili
- **Personalizzazione degli script:** rivedi e personalizza gli script generati secondo necessità per i tuoi requisiti di test specifici
- **Monitoraggio dell'esecuzione:** implementa il monitoraggio e la registrazione appropriati durante l'esecuzione dello script di test
- **Analisi dei risultati:** stabilisci processi per analizzare i risultati dei test e identificare i problemi delle applicazioni

La raccolta finale di script di automazione dei test fornisce un framework di test completo per la convalida delle funzionalità delle applicazioni modernizzate. Gli script possono essere integrati nei processi di test continui o eseguiti come parte del flusso di lavoro di convalida delle applicazioni.

Funzionalità di implementazione in AWS Trasformazione

AWS Transform ti aiuta a configurare ambienti cloud per applicazioni mainframe modernizzate fornendo modelli Infrastructure as Code (IaC) pronti all'uso. Tramite l'interfaccia di chat AWS Transform, puoi accedere a modelli predefiniti che creano componenti essenziali come risorse di calcolo, database, archiviazione e controlli di sicurezza. I modelli sono disponibili nei formati più diffusi tra cui CloudFormation (CFN) e Terraform AWS Cloud Development Kit (AWS CDK), offrendoti la flessibilità necessaria per implementare la tua infrastruttura.

Questi modelli fungono da elementi costitutivi che riducono il tempo e l'esperienza necessari per configurare gli ambienti per le applicazioni mainframe modernizzate. Puoi personalizzare questi modelli in base alle tue esigenze, offrendoti una base per creare il tuo ambiente di distribuzione.

Per recuperare i modelli IaC, chiedi nella chat AWS Transform i Infrastructure-as-Code modelli che chiariscono il tuo modello di modernizzazione preferito (come AWS Transform for mainframe refactor), la tua topologia preferita (standalone o alta disponibilità) e il tuo formato preferito (rispetto a Cloud Development CloudFormation Kit vs Terraform).

Crea e distribuisce la tua applicazione modernizzata dopo il refactoring

Dopo aver completato il processo di refactoring con AWS Transform, puoi creare e distribuire la tua applicazione Java modernizzata. Questa guida illustra come recuperare il codice modernizzato, configurare l'ambiente e distribuire e testare l'applicazione.

Note

Oltre alle indicazioni fornite qui, il pacchetto di codice generato da AWS Transform includerà un documento Configurazione dell'ambiente di sviluppo AWS automatizzato di Refactor che fornisce istruzioni per configurare un IDE (Integrated Development Environment) con Developer Runtime.

Argomenti

- [Prerequisiti](#)
- [Fase 1: Recuperare il codice modernizzato](#)
- [Fase 2: Creazione dell'applicazione modernizzata](#)
- [Fase 3: Configurazione dell'ambiente di test](#)
- [Fase 4: Implementazione dell'applicazione modernizzata](#)
- [Fase 5: Testare l'applicazione modernizzata](#)
- [Esempio aggiuntivo](#)

Prerequisiti

Prima di iniziare, assicurati di avere:

- Hai completato con successo un processo di refactoring con AWS Transform.
- Accesso al tuo codice modernizzato.
- [Stack di strumenti software di compilazione installato e configurato sulla tua macchina di sviluppo, come Apache Maven o Apache Tomcat. Per ulteriori informazioni sul controllo delle versioni di Runtime, AWS consulta le note di rilascio di Transform for mainframe Runtime.](#)
- Amazon Corretto o una versione di Java runtime installato e configurato. Per ulteriori informazioni sull'installazione di Amazon Corretto, consulta [Amazon Corretto 24](#).
- Accesso per creare e configurare database Amazon Aurora PostgreSQL per componenti Runtime, se necessario. [Per ulteriori informazioni sulla creazione del database Aurora PostgreSQL, consulta Working with Amazon Aurora PostgreSQL.](#)
- Accesso amministrativo per distribuire applicazioni nel tuo ambiente di runtime.
- Ho esaminato i concetti di [AWS Transform for mainframe Runtime per i concetti](#) fondamentali sulle applicazioni modernizzate con una soluzione di refactoring AWS automatizzato.

Fase 1: Recuperare il codice modernizzato

Per recuperare il codice modernizzato

1. Scarica ed estrai il pacchetto di codice generato.
2. Apri `codebase/app-pom/pom.xml` e annota la versione del motore di runtime richiesta. Ad esempio, `<gapwalk.version>4.6.0</gapwalk.version>`.
3. Individuate come riferimento il documento Configura l'ambiente di sviluppo AWS automatizzato di Refactor dal pacchetto di codice scaricato.

Fase 2: Creazione dell'applicazione modernizzata

Per creare la tua applicazione modernizzata

1. Accedi al Runtime dal Toolbox AWS Transform for mainframe.
2. Scaricate e installate la versione di runtime appropriata (identificata in [the section called “Fase 1: Recuperare il codice modernizzato”](#)) sul computer di sviluppo locale.

Note

Ulteriori informazioni per l'installazione delle dipendenze di runtime sul computer locale sono disponibili nella sezione 3.1 del documento Configurazione dell'ambiente di sviluppo AWS automatizzato di Refactor.

3. Apri il prompt dei comandi e accedi alla directory principale dell'applicazione.
4. Per creare pacchetti distribuibili per l'applicazione modernizzata, esegui il comando Maven build:

```
mvn package
```

Consulta la pagina [Organizzazione dell'applicazione](#) per i dettagli sull'organizzazione di base del codice modernizzato. Ad esempio, per un'applicazione modernizzata contenente un'applicazione Web front-end, è possibile aspettarsi almeno i seguenti `.war` aggregati distribuibili oltre ai componenti di runtime:

- Progetto di servizio: contiene elementi di modernizzazione della logica aziendale legacy

```
<business-app>-service.*.war
```

- Progetto Web: contiene la modernizzazione degli elementi relativi all'interfaccia utente

```
<business-app>-web.*.war
```

Fase 3: Configurazione dell'ambiente di test

Per configurare l'ambiente di test

1. Configura il runtime modernizzato dell'applicazione. Per ulteriori informazioni, consulta la sezione [Configurazione della configurazione per il runtime](#) nella guida per l'Modernizzazione del mainframe AWS utente.

Note

Fare riferimento alla sezione 5 della guida AWS Configurazione dell'ambiente di sviluppo automatizzato Refactor per esempi di configurazione specifici dei componenti di runtime.

2. Prepara i set di dati di input e output (I/O) per applicazioni modernizzate. Le applicazioni modernizzate possono elaborare set di I/O dati sequenziali, set di dati VSAM o altro.

Note

Per alcuni esempi, fare riferimento alla sezione 6 del Configura l'ambiente di sviluppo AWS automatizzato di Refactor.

3. Un ambiente di runtime: è possibile utilizzare l'ambiente di runtime esistente o creare un nuovo ambiente di runtime.
 - Per configurare un ambiente di runtime non gestito, consulta [Configurare un'applicazione non gestita](#).
 - Per configurare un ambiente di runtime gestito, vedi [Configurare un'applicazione gestita](#).

Dopo aver configurato l'ambiente di test, si passa alla fase successiva di implementazione dell'applicazione modernizzata.

Fase 4: Implementazione dell'applicazione modernizzata

Distribuisci gli artefatti dell'applicazione nel runtime che hai creato, and/or configurato nelle sezioni and. [the section called “Fase 2: Creazione dell'applicazione modernizzata”](#) [the section called “Fase 3: Configurazione dell'ambiente di test”](#)

Ulteriori indicazioni per l'implementazione dell'applicazione modernizzata sono disponibili utilizzando questi collegamenti:

- [Implementa su Amazon EC2](#)
- [Implementa su container su Amazon ECS e Amazon EKS](#)
- [Crea un'applicazione Modernizzazione del mainframe AWS](#)

Fase 5: Testare l'applicazione modernizzata

Dopo la distribuzione,

1. Consulta le [API Runtime](#) disponibili per scoprire come interagire con le applicazioni modernizzate.
2. Testa la tua applicazione per allinearne l'equivalenza funzionale con l'applicazione precedente.
Ad esempio, consulta [Test di un'applicazione di esempio nella guida](#) per l'Modernizzazione del mainframe AWS utente.

Esempio aggiuntivo

Per un esempio specifico di modernizzazione di un'applicazione mainframe con AWS Transform, consulta [Modernizzare l' CardDemo](#) applicazione mainframe.

Full-stack Modernizzazione di Windows

AWS Transform offre la modernizzazione completa di Windows, tra cui la modernizzazione di .NET e la modernizzazione di SQL Server.

L'agente AWS Transform for .NET può aiutarti a modernizzare le tue applicazioni .NET per renderle compatibili con .NET multiplatforma. [È possibile modernizzare .NET utilizzando l'app web .NET o l'IDE .NET.](#)

AWS Transform for [SQL Server modernization](#) è un AI-powered servizio che automatizza la modernizzazione completa dei database Microsoft SQL Server e delle applicazioni .NET associate su Amazon Aurora PostgreSQL. Il servizio orchestra l'intero percorso di migrazione dalla conversione dello schema, alla migrazione dei dati e alla modifica del codice dell'applicazione per adattarlo al nuovo obiettivo PostgreSQL, rendendo i team più produttivi automatizzando attività complesse e laboriose.

Argomenti

- [Modernizzare .NET con AWS Trasformazione](#)
- [Modernizzazione di SQL Server](#)

Modernizzare .NET con AWS Trasformazione

L'agente AWS Transform for .NET può aiutarti a modernizzare le tue applicazioni .NET per renderle compatibili con .NET multiplatforma. Questa funzionalità è denominata modernizzazione .NET.

Dopo [AWS Trasforma l'ambiente](#) AWS Transform, è possibile creare un processo di trasformazione di modernizzazione .NET.

Esperienze

AWS Transform è disponibile in diverse esperienze:

- Console Web: per la trasformazione su larga scala di un massimo di 500 repository alla volta.
- Visual Studio IDE: trasformazione guidata dallo sviluppatore di una soluzione o di un progetto che collabora con un agente in modo interattivo e iterativo. Consigliato per progetti di medie e grandi dimensioni.

Puoi passare liberamente dalla console web all'IDE per lavorare su un lavoro di trasformazione.

Puoi anche richiamare AWS Transform da altri IDE e compagni di codice AI:

- Kiro: trasforma da Kiro usando AWS Transform for Kiro power.
- Altri compagni di codice AI: passa dai tuoi assistenti di codifica AI preferiti utilizzando gli agenti Transform MCP. AWS

Funzionalità e caratteristiche principali

- Analizza le basi di code.NET Framework dai tuoi sistemi di controllo del codice sorgente, che include il NuGet supporto privato, l'identificazione delle dipendenze tra repository e la fornitura di un rapporto di analisi.
- Trasformazione automatizzata di applicazioni.NET Framework legacy in .NET multiplatforma, notifiche e-mail e un rapporto di riepilogo della trasformazione.
- Facile integrazione con le piattaforme di controllo del codice sorgente (BitBucket, GitHub, and GitLab) per importare il codice esistente e trasferire il codice trasformato in una nuova filiale.
- Convalida del codice trasformato tramite test unitari.

Versioni e tipi di progetto supportati

AWS Transform supporta la trasformazione per le seguenti versioni di.NET:

- .NET Framework 3.5+
- .NET Core 3.1
- .NET 5.x e versioni successive
- .NET 8

AWS Transform può trasformarsi nelle seguenti versioni di.NET di destinazione:

- .NET 8
- .NET 10

AWS Transform supporta la trasformazione di questi tipi di progetti (solo C#):

- Librerie di classi
- Applicazioni per console

- ASP.NET:
 - Model View Controller (MVC), incluso Razor Views front-end
 - Back-end per applicazioni a pagina singola (SPA) (livelli di logica aziendale)
 - API Web
 - Moduli Web
- Progetti di unit test (NUnit, xUnit e MSTest)
- Servizi Windows Communication Foundation (WCF)
- Progetti con versioni multiplatforma fornite per pacchetti privati NuGet o di terze parti. Se manca o non è disponibile un equivalente multiplatforma, AWS Transform for .NET tenterà una conversione nel miglior modo possibile.

AWS Transform può anche trasformare i seguenti tipi di progetto in una versione moderna di .NET. Questa è una funzionalità di anteprima e potrebbe non trasformarsi completamente come i tipi di progetto supportati.

- WinForms progetti desktop.
- progetti desktop WPF.
- Progetti mobili Xamarin.
- Progetti scritti in. VB.NET

Limitazioni

Per ulteriori informazioni su quote e limitazioni per AWS Transform, vedere [Quote per AWS Trasformazione](#).

AWS Transform non trasforma quanto segue:

- Componenti dell'interfaccia utente di Blazor
- DLL Win32 che non dispongono di librerie compatibili di base
- Repository che non contengono soluzioni.

AWS Transform non modificherà i rami dei repository originali e può scrivere solo su un ramo di destinazione separato specificato nel piano di trasformazione.

Intervento umano

Durante il trasferimento delle applicazioni .NET Framework su una piattaforma multiplatforma, è possibile che venga richiesto di fornire input o approvazioni nei seguenti scenari:

- Configura un connettore per il codice sorgente e le autorizzazioni
- Convalida il piano di modernizzazione proposto
- Carica le dipendenze dei pacchetti mancanti come NuGets
- Rivedi e accetta il codice trasformato

Ulteriori informazioni

È possibile modernizzare il codice .NET utilizzando l'applicazione web AWS Transform o AWS Toolkit for Visual Studio

- [Modernizzazione del codice .NET utilizzando AWS Transform l'applicazione web](#)
- [Modernizzare .NET nell'IDE](#)
- [Procedure consigliate per le trasformazioni .NET](#)

Modernizzazione del codice .NET utilizzando AWS Transform l'applicazione web

AWS Transform for .NET è un nuovo AI-powered agente generativo progettato per modernizzare le applicazioni .NET legacy. È possibile modernizzare il codice .NET esistente utilizzando l'applicazione web AWS Transform o l'Visual Studio AWS estensione Toolkit.

Per modernizzare il codice .NET utilizzando l'applicazione web AWS Transform, accedi all'applicazione web e segui questi passaggi dettagliati:

1. [Creando il AWS Transform il piano di lavoro .NET](#)
2. [Creazione di un connettore per l'archivio del codice sorgente](#)
3. [Conferma dei repository per prepararsi alla trasformazione](#)
4. [Risoluzione delle dipendenze dei pacchetti per prepararsi alla trasformazione](#)
5. [Revisione del piano per prepararsi alla trasformazione](#)
6. [Trasformazione del codice .NET](#)

Creando il AWS Trasforma il piano di lavoro.NET

Dopo aver creato l'area di lavoro, nella scheda Lavori, seleziona Crea lavoro. Quindi segui le istruzioni di AWS Transform nel riquadro della chat usando il linguaggio naturale. Questi sono i passaggi tipici per la creazione di un processo di modernizzazione.NET.

1. AWS Transform ti chiederà quale tipo di processo di trasformazione desideri creare. Nella chat, inserisci la modernizzazione di.NET.
2. AWS Transform suggerirà un nome di lavoro e ti chiederà se desideri cambiarlo. Se desideri cambiare il nome del lavoro, dì a AWS Transform in linguaggio naturale, ad esempio, cambia il nome del lavoro in ExampleCorpDotNet1. Altrimenti, nella chat, puoi accettare il nome del lavoro suggerito. Dopo aver accettato il nome del lavoro, AWS Transform ti avvisa nella finestra di chat che sta creando il lavoro.
3. AWS Transform crea il processo di trasformazione.

Componenti di AWS Trasforma il piano di lavoro.NET

La visualizzazione dei lavori AWS Transform .NET presenta 5 schede che puoi selezionare dalle icone verticali all'estrema sinistra: Tasks, Dashboard, Approvazioni, Artifacts e Worklog. Ogni scheda ha un riquadro a sinistra e un riquadro chat centrale. A volte può apparire un riquadro di collaborazione destro per mostrare dettagli aggiuntivi e richiedere l'input umano.

Attività (Job Plan)

Questa scheda mostra il tuo piano di lavoro nel riquadro a sinistra. Un lavoro.NET prevede 5 passaggi:

1. Ottieni risorse da trasformare: in questa fase, crei un connettore per il tuo repository di codice utilizzando AWS CodeConnections. A seconda delle autorizzazioni del repository, un amministratore del repository di codice potrebbe dover approvare il connettore e concedere a AWS Transform l'accesso al repository.
2. Scopri le risorse per la trasformazione: in questa fase, AWS Transform individua gli archivi controllati dal codice sorgente e tu li selezioni alcuni o tutti per la valutazione.
3. Valuta il codice per la trasformazione: i repository selezionati vengono valutati e puoi visualizzare i report di valutazione.
4. Preparati alla trasformazione: in questa fase, AWS Transform ti avvisa se mancano delle dipendenze nei tuoi repository. Puoi caricare le dipendenze mancanti o ignorarle. Se non sei

l'amministratore del repository, potrebbe essere necessario che un amministratore approvi il piano di trasformazione finale.

5. Trasforma: in questa fase, AWS Transform trasforma il tuo repository e ti fornisce lo stato continuo durante la trasformazione fino al suo completamento. Puoi consultare i report sulla trasformazione per capire cosa è cambiato e perché.

Puoi vedere lo stato di ogni passaggio:

- Non avviato
- Attendi l'input dell'utente
- In Progress (In corso)
- Completato

Pannello di controllo

La scheda Dashboard fornisce un riepilogo di alto livello della trasformazione. Visualizza le metriche relative al numero di lavori trasformati, alla trasformazione applicata e al tempo stimato per completare la trasformazione. Sotto la dashboard c'è una tabella degli archivi con il relativo stato: In-progress, Non riuscito o Operato correttamente.

Approvazioni

Le richieste di approvazione per il lavoro vengono visualizzate e completate in questa scheda.

Artifacts

Jjob-related gli artefatti vengono caricati o scaricati da questa scheda.

Worklog

AWS Transform registra le sue azioni nella scheda Worklog. Il Worklog fornisce un registro dettagliato delle azioni intraprese da AWS Transform, insieme alle richieste di input umani e alle risposte a tali richieste.

Creazione di un connettore per l'archivio del codice sorgente

Successivamente [Creando il AWS Trasforma il piano di lavoro.NET](#), nella scheda Attività, il riquadro sinistro della finestra AWS Transform elenca le fasi del processo di trasformazione. La prima fase è

Ottieni risorse da trasformare. In questa fase, puoi Invita collaboratori e Connect a un repository di codice sorgente. Il riquadro destro della finestra AWS Transform è dove si specificano i dettagli.

Ogni processo di trasformazione deve avere un solo connettore per il repository del codice sorgente. L'agente AWS Transform utilizza questo connettore per scaricare la tua codebase .NET da GitHub, GitLab, o Bitbucket utilizzando [AWS CodeConnections](#). È necessario eseguire la configurazione AWS CodeConnections nella stessa regione del job Transform. AWS In alternativa, puoi [Connect al codice sorgente in Amazon S3](#) anziché a un repository di codice sorgente.

Note

Se disponi di un connettore di repository di codice sorgente esistente, AWS Transform ti avviserà. Seleziona Usa connettore esistente per usare questo connettore. Se non desideri utilizzare il connettore esistente, vedi [Eliminazione di un connettore esistente](#) prima [Aggiungere un nuovo connettore](#). È possibile avere un solo connettore del repository di origine per job.

Aggiungere un nuovo connettore

Per creare un nuovo connettore per l'archivio del codice sorgente:

1. Inserisci il numero di AWS account che desideri utilizzare per il AWS CodeConnections connettore.
2. Se non hai configurato AWS CodeConnections lo stesso AWS account, [configura AWS CodeConnections](#).
3. Usa la [AWS Developer Tools Console](#) per creare una connessione a [Bitbucket](#), [GitHub](#), [GitHub Enterprise Server](#) o [GitLabAzureDevOps](#) repository.
4. Copia l'Amazon Resource Name (ARN) della connessione che hai creato.
5. Torna a AWS Transform e incolla l'ARN della connessione che hai creato.
6. Immettete un nome per il connettore.

Note

Non inserire informazioni personali come parte del nome del connettore.

7. Seleziona Avvia la creazione del connettore.

8. AWS Transform richiede la creazione di un connettore per l' AWS account inserito, nella stessa regione del processo di trasformazione corrente, e notifica che una richiesta di approvazione è pronta per essere approvata dall' AWS amministratore nella Console di AWS gestione. Seleziona Copia il link di verifica.
9. Se sei l' AWS amministratore, accedi all' AWS account e vai al link di verifica per approvare la richiesta di connessione. Se non sei l' AWS amministratore, fornisci il link di verifica all' AWS amministratore.
10. Dopo che l' AWS amministratore ha approvato la richiesta del connettore, seleziona Finalizza connettore per completare il processo di creazione del connettore. Se desideri utilizzare un connettore diverso, seleziona Riavvia per riavviare il processo di creazione del connettore.

La scheda Collaborazione include anche dettagli sul connettore, che includono:

- Stato: Approvato o in attesa di approvazione
- AWS ID dell'account
- AWS Regione
- Connessione ARN

Eliminazione di un connettore esistente

Note

Se disponi di un connettore per l'archivio del codice sorgente esistente, AWS Transform ti avviserà. Seleziona Usa connettore esistente o Elimina e crea un nuovo connettore.

Se scegli di eliminare un repository di codice sorgente esistente connect, AWS Transform ti avviserà prima di eliminare effettivamente il connettore.

1. Puoi eliminare un connettore esistente in due modi:
 - a. Se AWS Transform ti richiede di farlo, puoi selezionare Elimina e creare un nuovo connettore.
 - b. È inoltre possibile selezionare il riavvio nel prompt. Per modificare questo connettore, è necessario riavviare.
2. AWS Transform avvisa che il riavvio eliminerà il connettore. Per eliminare il connettore, seleziona nuovamente Riavvia.

3. AWS Transform ti avvisa nuovamente che l'eliminazione del connettore rimuoverà la connessione al tuo repository di terze parti, come Bitbucket, e. GitHub GitLab Inoltre, tutti i processi di AWS trasformazione che utilizzano questo connettore avranno esito negativo se il connettore viene eliminato. Per confermare l'eliminazione, digita delete e seleziona Elimina.
4. Per aggiungere un nuovo connettore per il repository del codice sorgente, consulta [Aggiungere un nuovo connettore](#).

Connect al codice sorgente in Amazon S3

Puoi connettere AWS Transform al codice sorgente in Amazon S3 in alternativa alla [connessione di un repository di codice sorgente](#).

Organizzazione dei bucket S3

Il codice sorgente originale e il codice trasformato vengono archiviati in un bucket S3 comune, organizzato come illustrato di seguito. È necessario configurare il bucket S3 nella stessa regione del job Transform. AWS Carica il codice sorgente nel bucket come file zip a livello di root. Il file zip deve contenere una cartella di primo livello per ogni repository.

Durante la trasformazione, AWS Transform crea una cartella di output di trasformazione e memorizza i risultati della trasformazione in quella cartella. Transformation crea un file zip denominato transformed-code.zip contenente il codice trasformato. Ciò include un report sulle differenze di codice denominato diff.txt che evidenzia le modifiche ai file a livello di progetto.

```
<customer-bucket>/  
### source-code.zip  
    ### repo 1  
    ### repo 2  
    ### .....  
    ### repo n  
### transform-output/  
    ### transformed-code.zip
```

Aggiungere un nuovo connettore S3

Per creare un nuovo connettore per l'archivio del codice sorgente S3:

1. Nella AWS console, crea un bucket S3.

2. Carica il codice sorgente come file zip nel bucket S3.
3. Nell'app web AWS Transform, avvia un processo di trasformazione.NET. Nel passaggio Connetti un repository di codice sorgente, seleziona Connetti il codice sorgente nel bucket S3 e scegli Salva.
4. Nella pagina successiva, inserisci i dettagli del tuo bucket S3 e scegli Invia.
 - a. Nome del connettore
 - b. AWS ID dell'account
 - c. S3 Bucket Arn
 - d. Chiave di crittografia S3 Bucket (opzionale)
5. Approva il connettore:
 - a. Nella pagina successiva, copia il link di verifica.
 - b. Chiedi a un approvatore di accedere al link per accedere alla pagina di richiesta di creazione del connettore AWS Transform.
 - c. Scegliete di creare un nuovo ruolo o utilizzare un ruolo esistente.
 - d. Dopo aver esaminato la richiesta, scegli Salva e approva per approvarla.
6. Specificate la posizione del file zip S3:
 - a. Nell'app web AWS Transform, attendi che lo stato mostri Approvato.
 - b. Nella pagina Specificare la posizione della risorsa, inserisci un URL S3 per il file zip del codice nel formato `s3://bucket-name/zip-file-name` e scegli Invia a AWS Transform.
 - c. Il lavoro procede alla fase Discovery per continuare la trasformazione.

Eliminazione di un connettore S3

Per eliminare un connettore S3 esistente:

1. Nell'app web AWS Transform, seleziona Gestisci connettori in alto a destra.
2. Nella finestra Gestisci connettori, seleziona il connettore.
3. Scegli Elimina.

Conferma dei repository per prepararsi alla trasformazione

Successivamente [Creazione di un connettore per l'archivio del codice sorgente](#), conferma i tuoi repository come primo passo per prepararti alla trasformazione. Puoi:

- Rivedi e modifica [Impostazioni predefinite](#) che influiscono sui contenuti del piano.
- Esamina i repository scoperti e seleziona quelli da valutare per la trasformazione.
- Esamina il [rapporto di valutazione del repository](#) e parla con AWS Transform dei suoi contenuti.
- [Utilizza il piano generato da AWS Trasformazione](#).
- [Personalizza il piano di trasformazione](#) utilizzando l'app Web o scaricando un file JSON, modificandolo e caricandolo su Transform. AWS

Impostazioni predefinite

Nella sezione Dettagli del lavoro della scheda Collaborazione, puoi impostare quanto segue:

Nella scheda Attività, nel passaggio Preparazione alla trasformazione - Conferma gli archivi da trasformare, puoi impostare quanto segue:

- Imposta il nome del ramo di destinazione in cui il codice trasformato viene scritto nel tuo repository.
- Imposta la versione.NET di destinazione:
 - .NET 8: trasforma tutti i progetti in.NET 8
 - .NET 10: trasforma tutti i progetti in.NET 10
- È possibile aggiornare le Job Settings predefinite o lasciarle così come sono. Ciò include:
 - Escludi i progetti.NET Standard dal piano di trasformazione Questa impostazione è selezionata per impostazione predefinita. Se selezionata, AWS Transform esclude tutti i progetti.NET Standard dal piano di trasformazione. Se deselezioni questa impostazione, i progetti.NET Standard verranno trasformati, il che li renderà non più compatibili con .NET Framework.
 - Controlla i NuGet sorgenti e scarica le versioni dei pacchetti compatibili.NET Consenti a AWS Transform di cercare e ottenere versioni di pacchetti compatibili.NET per il codice che desideri trasformare.

Consulta il rapporto di valutazione del repository

Il rapporto di valutazione del repository fornisce una visualizzazione tabulare delle informazioni su ciascun repository rilevato da Transform. AWS Questo include:

- Proprietario del repository
- Filiale valutata
- Numero di soluzioni

- N. di progetti
- Righe di codice totali
- Versioni.NET rilevate
- Tipi di progetto rilevati
- Numero di dipendenze private da Nuget
- Numero di dipendenze pubbliche di Nuget
- Complessità della trasformazione

Per scaricare il file:

1. Nel tuo spazio di lavoro, seleziona la scheda Collaborazione.
2. Nel riquadro Scegli i repository, seleziona Scarica e scegli Scarica come HTML o Scarica come JSON

Parla del rapporto di riepilogo del repository

Il riepilogo del tuo repository potrebbe essere molto lungo. Usa la chat per comprenderne meglio i contenuti. Il tuo rapporto è disponibile per la chat quando vedi questo messaggio nella scheda Worklog: Il rapporto di valutazione è ora disponibile in chat per le domande. Per aprire la chat, fai clic sull'icona esagonale viola nell'angolo in basso a destra della console web. Ecco alcuni esempi di istruzioni:

- Elenca tutti i repository scoperti o valutati.
- Quanti progetti.NET 6 sono stati scoperti durante la valutazione?
- Quali sono i progetti con la maggiore complessità?

Utilizza il piano generato da AWS Trasformazione

È possibile scegliere di utilizzare il piano AWS Transform creato dalla scoperta di repository con una maggiore probabilità di successo della trasformazione, che include gli archivi root, quelli di ultima modifica e quelli interdipendenti.

AWS Transform elenca alcuni dettagli di alto livello sul piano di trasformazione, che includono:

- Numero totale di repository scoperti Questo numero di repository .NET legacy rilevati da AWS Transform utilizzando il connettore del repository del codice sorgente. AWS Transform è in grado di

eseguire la scansione di un massimo di 1.000 repository per processo. Se disponi di più repository da scansionare o trasformare, puoi creare più processi di trasformazione.

- Repository selezionati Il numero di repository .NET legacy che AWS Transform sono stati selezionati per la trasformazione.
- Dipendenze selezionate Il numero di dipendenze richieste dai repository selezionati, che AWS Transform ha rilevato automaticamente e aggiunto al piano di trasformazione.

La tabella Repository selezionati elenca i repository selezionati. È possibile cercare i repository per nome, accedere a pagine aggiuntive di repository e scaricare un file in formato JSON che elenca i repository selezionati e le relative dipendenze. È possibile apportare qualsiasi modifica in questa visualizzazione.

La tabella Archivi selezionati elenca i seguenti dettagli sui repository che AWS Transform ha selezionato per la trasformazione:

- Nome del repository
- Ramo di origine
- Data e ora dell'ultima modifica
- Righe di codice Questo ti permette di vedere se ti stai avvicinando ai limiti di quota. Per ulteriori informazioni, consulta [Quote per AWS Trasformazione](#).
- Archivi dipendenti È possibile fare clic sul numero di archivi dipendenti per visualizzare maggiori dettagli su queste dipendenze.

Se sei soddisfatto del piano di trasformazione generato da AWS Transform, seleziona Confirm repository.

Se desideri apportare modifiche al piano di AWS trasformazione generato da Transform, seleziona [Personalizza il piano di trasformazione](#).

Personalizza il piano di trasformazione

Se scegli di non farlo [Utilizza il piano generato da AWS Trasformazione](#), puoi personalizzare l'elenco dei repository da trasformare utilizzando una delle seguenti opzioni:

1. Seleziona i repository nella tabella Archivi selezionati.
 - a. Quando aggiungi un repository al piano, AWS Transform selezionerà automaticamente le dipendenze del repository e le aggiungerà automaticamente al piano di trasformazione.

- b. Puoi anche deselezionare i repository nella tabella.
2. Scarica l'elenco JSON generato da AWS Transform di repository e rami.
 - a. Seleziona Scarica, quindi seleziona Scarica come JSON.
 - b. Rivedi e modifica il file JSON. Puoi rimuovere i repository, o le soluzioni all'interno dei repository, che non desideri trasformare.
 - c. Carica il JSON rivisto selezionando Carica piano personalizzato.
 - d. Se il file JSON viene caricato correttamente, la tabella Archivi selezionati mostra le selezioni effettuate.
3. Puoi selezionare Mostra repository dipendenti per visualizzare l'elenco dei repository che AWS Transform ha rilevato come dipendenze per i repository selezionati.
4. Puoi ripetere questi passaggi se necessario. Quando sei soddisfatto del tuo piano personalizzato, seleziona Conferma gli archivi.

Risoluzione delle dipendenze dei pacchetti per prepararsi alla trasformazione

Successivamente [Conferma dei repository per prepararsi alla trasformazione](#), se AWS Transform rileva le dipendenze del pacchetto mancanti, è necessario completare questo passaggio. È possibile eseguire uno PowerShell script di Windows per recuperare le dipendenze dei pacchetti mancanti dallo stesso dispositivo dell'ambiente di Visual Studio sviluppo oppure recuperare i pacchetti mancanti manualmente. Quindi, carica i pacchetti mancanti.

Le Missing Package Dependencies possono essere aggiornate in due modi:

- Risolvi utilizzando Artifact Connector: risolvi configurando un Artifact Repository (connettore ADO) tramite un flusso di lavoro HITL dedicato a Connect Artifact Repository, che viene visualizzato quando un Artifact NuGet Connector non è configurato e mancano i pacchetti.
- Aggiorna il pacchetto mancante: AWS Transform elenca i pacchetti mancanti nella tabella delle dipendenze dei pacchetti mancanti. È possibile cercare un pacchetto mancante per nome nella casella di ricerca. Questa tabella include i seguenti dettagli sui pacchetti mancanti:
 - Nome
 - Repository associati
 - Stato della versione del framework
 - Stato della versione principale

Per risolvere le dipendenze dei pacchetti mancanti, [Carica i pacchetti mancanti](#).

Carica i pacchetti mancanti

1. Se lo desideri, puoi scaricare uno script di PowerShell supporto di Windows per recuperare le dipendenze dei pacchetti mancanti dall'interno del tuo Visual Studio ambiente di sviluppo. Oppure puoi trovare i pacchetti mancanti manualmente.

Per usare lo PowerShell script di Windows:

- a. Seleziona Scarica PowerShell lo script di Windows.
 - b. Esegui lo script localmente con una connessione attiva ai repository che contengono i file di dipendenza dei pacchetti mancanti.
 - c. Questo script consente di scaricare le dipendenze dei pacchetti mancanti nell'ambiente locale.
2. Lo script creerà un singolo file zip da caricare che include tutte le dipendenze in un unico archivio. Puoi anche caricare file singoli .nupkg o zip per ogni dipendenza.
 3. Seleziona Carica i file del pacchetto.
 4. Nella modalità Carica i file di dipendenza, seleziona Scegli i file e cerca la posizione dei file del pacchetto compressi mancanti sul tuo dispositivo.
 5. Seleziona Carica.
 6. AWS Transform convalida i file che hai caricato. Durante la convalida, non è possibile effettuare aggiornamenti. AWS Transform riporta lo stato di convalida sopra la tabella delle dipendenze dei pacchetti mancanti.
 7. AWS Transform aggiorna anche le colonne di stato nella tabella delle dipendenze dei pacchetti mancanti da Missing a Resolved. Se un pacchetto non viene convalidato, il suo stato diventa Non valido. Per i file non validi, procedi come segue:
 - a. Nella tabella Dipendenze dei pacchetti mancanti, selezionate il pacchetto non valido utilizzando la casella di controllo.
 - b. Seleziona Rimuovi il file caricato.
 - c. Questo riporta lo stato a Mancante.
 8. Dopo aver caricato i pacchetti mancanti e risolto le dipendenze dei pacchetti, seleziona Procedi alla revisione.

Se si seleziona Procedi alla revisione senza risolvere le dipendenze dei pacchetti mancanti, AWS Transform chiede se si desidera avviare il processo di trasformazione senza i pacchetti mancanti. Se si seleziona Ignora le dipendenze del pacchetto mancante, AWS Transform utilizzerà

i riferimenti di assemblaggio per trasformare il codice. Procedere con questa azione può influire sulle risorse correlate.

Requisiti della struttura delle cartelle

Per i NuGet caricamenti AWS Transform richiede:

- Il .nuspec file da collocare al livello principale per i pacchetti caricati manualmente, oppure
- Utilizzo dello PowerShell script fornito per generare la struttura corretta

Requisiti di corrispondenza della versione

- Stato del framework: AWS Transform tenta di abbinare la versione della dipendenza specificata nel .csproj file (codice sorgente) alla versione della dipendenza caricata. Una corrispondenza esatta dà come risultato lo stato di successo.
- Stato principale: AWS Transform prevede una specifica della versione principale nella sezione delle dipendenze del file caricato .nuspec. Se ne viene trovato uno, lo stato principale è Successo.

Formato di esempio:

```
<dependencies>
  <group targetFramework="net8.0" />
</dependencies>
```

Le versioni più comuni includono:

- .NET 5.0 (net5.0)
- .NET 6.0 (net6.0)
- .NET 7.0 (net7.0)
- .NET 8.0 (net8.0)

Revisione del piano per prepararsi alla trasformazione

Successivamente [Conferma dei repository per prepararsi alla trasformazione](#)[Risoluzione delle dipendenze dei pacchetti per prepararsi alla trasformazione](#), l'amministratore dell' AWS account deve esaminare il piano di trasformazione e approvarlo in AWS Transform.

AWS Transform visualizza l'elenco dei repository, degli archivi dipendenti e dei pacchetti dipendenti del processo che sono stati selezionati per la trasformazione.

Revisione del piano di trasformazione

AWS Transform visualizza l'elenco dei repository, dei repository dipendenti e dei pacchetti dipendenti del job che sono stati selezionati per la trasformazione.

Note

AWS Transform può trasformare un massimo di 100 dipendenze e repository per piano di trasformazione.

1. Se non sei l'amministratore dell' AWS account, esamina il piano di lavoro e, se lo accetti, seleziona **Invia per approvazione**.
2. Se sei l'amministratore dell' AWS account, devi rivedere il piano e, quando sei pronto, approvare il piano per avviare la trasformazione. Dopo aver esaminato il piano di lavoro, seleziona una delle seguenti opzioni:
 - a. **Rifiuta** Se il lavoro è stato creato da un utente che non è l'amministratore dell' AWS account, ti consigliamo di avvisare l'autore del lavoro di riavviare il lavoro.
 - b. **Approva e avvia la trasformazione**.

La revisione del lavoro include i seguenti dettagli:

1. **Riepilogo del lavoro** Ciò include:
 - a. Il ramo di destinazione in cui AWS Transform inserirà il codice trasformato.
 - b. La versione.NET di destinazione, .NET 8.0 o .NET 10.
 - c. Le impostazioni del lavoro:
 - i. Escludi i progetti standard.NET
 - d. Numero di repository selezionati per la trasformazione
 - e. Numero di repository dipendenti
 - f. Numero di pacchetti privati NuGet
 - g. Righe di codice totali per il lavoro

2. Archivi selezionati Questi sono gli archivi selezionati per la trasformazione. Devono essere MVC, Web, Windows Communication Foundation (WCF), Console, class library, UI framework - Razor pages o pacchetti di unit test. Questa tabella include le seguenti informazioni:
 - a. Nome
 - b. Ramo di origine
 - c. Progetti supportati
 - d. Righe di codice
 - e. Progetti rilevati
 - f. Progetti ignorati
 - g. Dipendenze rilevate
3. Archivi dipendenti aggiunti Questi sono gli archivi dipendenti aggiunti per la trasformazione. Devono essere MVC, Web, Windows Communication Foundation (WCF), Console, libreria di classi, framework UI - Razor pages o pacchetti di unit test. Questa tabella include le seguenti informazioni:
 - a. Nome
 - b. Necessario da
 - c. Ramo di origine
 - d. Progetti supportati
 - e. Righe di codice
 - f. Progetti rilevati
 - g. Progetti ignorati
4. Pacchetti dipendenti Questi sono i pacchetti dipendenti aggiunti per la trasformazione. Devono essere MVC, Web, Windows Communication Foundation (WCF), Console, class library, UI framework - Razor pages o pacchetti di unit test. Questa tabella include le seguenti informazioni:
 - a. Nome
 - b. Repository associati
 - c. Stato della versione del framework
 - d. Stato della versione principale

Trasformazione del codice.NET

Dopo che l'amministratore dell' AWS account ha terminato [Revisione del piano per prepararsi alla trasformazione](#), puoi visualizzare l'avanzamento della trasformazione nella scheda Dashboard del processo di trasformazione.

Note

Oltre a trasformare gli archivi e le dipendenze, AWS Transform può eseguire progetti di unit test completamente trasformati (zero errori di costruzione). AWS Transform non ha accesso ai risultati dei test unitari precedenti alla trasformazione e può condividere solo i risultati successivi alla trasformazione. È quindi possibile confrontare i dati di base, prima della trasformazione, con i risultati post-trasformazione per comprendere eventuali lacune.

Nell'angolo in alto a destra, puoi vedere lo stato del lavoro, che ha uno dei seguenti valori:

- In attesa dell'input dell'utente
- Tempo trascorso
- In esecuzione

Puoi anche vedere le seguenti icone:

- Un'icona di interruzione della trasformazione
- Un'icona di aggiornamento
- Un'icona delle impostazioni

La Dashboard fornisce un riepilogo di alto livello della trasformazione. Mostra le metriche relative al numero di lavori trasformati e alla trasformazione applicata e il tempo stimato per completare la trasformazione.

La dashboard include:

1. La sezione Dettagli del job di trasformazione, che elenca le impostazioni e i dettagli predefiniti del processo di trasformazione, tra cui:
 - a. Destinazione del ramo di destinazione Per AWS trasformare il codice, Transform crea un nuovo ramo per il codice trasformato nel repository di codice.

- b. Versione.NET di Target, .NET 8.0 o .NET 10
 - c. L'ID del processo di AWS trasformazione.
 - d. Le impostazioni del lavoro:
 - i. Escludi i progetti standard.NET
2. La sezione di riepilogo della trasformazione contiene:
- a. Il numero di repository selezionati per la trasformazione
 - b. Il numero di progetti da trasformare
 - c. Il totale delle righe di codice in questi archivi e progetti

Dopo l'inizio della trasformazione, nelle sezioni Repository status, Package status e Unit test status vengono visualizzati grafici a torta che mostrano l'avanzamento in tempo reale. Lo stato dello Unit test mostra lo stato degli unit test presenti nei repository che AWS Transforms esegue dopo la trasformazione per testare il codice trasformato. AWS Transform condivide i risultati dei test eseguiti, insieme al nome del singolo test, per consentire ai clienti di esaminare l'elenco degli unit test superati e non riusciti.

Note

La sezione Repository elenca i repository consigliati da AWS Transform o selezionati per la trasformazione. Seleziona Scarica JSON per scaricare un elenco di repository, dipendenze e pacchetti inclusi nel tuo piano di trasformazione.

Consulta i report sulla trasformazione

Una volta completato un processo di trasformazione, puoi scaricare i [report di trasformazione](#):

- [Rapporto di riepilogo sulla trasformazione](#): questo rapporto fornisce una panoramica della trasformazione in formato HTML o JSON. Scarica il rapporto di riepilogo sulla trasformazione dalla scheda Dashboard. Seleziona Scarica e scegli Scarica come HTML o Scarica come JSON.
- [Rapporto dettagliato sulla trasformazione](#): questo rapporto fornisce informazioni approfondite su una trasformazione in formato HTML. Scarica i report dettagliati sulla trasformazione dalla scheda Dashboard. Seleziona il link Scarica un rapporto dettagliato nell'elenco del repository per scaricare un rapporto dettagliato.

Chatta con AWS Transform about the Transformation report

Puoi chattare con AWS Transform in merito al rapporto di trasformazione dopo che un repository è stato completamente elaborato o dopo il completamento del processo di trasformazione. La scheda Worklog mostra questo messaggio per ogni repository disponibile per la chat: i dettagli sulla *repository_name* trasformazione del repository sono ora disponibili nella chat per le domande. Visualizza questo messaggio quando il processo di trasformazione è completato: Il lavoro di AWS trasformazione è completato.

Per aprire la chat, fai clic sull'icona esagonale viola nell'angolo in basso a destra della console web.

Ecco alcuni esempi di istruzioni:

- Quali progetti sono stati trasformati con successo?
- Quali progetti sono stati parzialmente trasferiti?
- Quali modifiche sono state apportate al `repo_name` repository?
- Quali pacchetti sono stati aggiornati nel progetto? `project_name`

Modernizzare.NET nell'IDE

AWS Transform include un assistente AI interattivo e agentico nel AWS Toolkit for Visual Studio. Ti consente di modernizzare le applicazioni attraverso un'esperienza conversazionale guidata passo dopo passo direttamente nel tuo IDE. Per trasformare una soluzione o un progetto .NET, l'agente AWS Transform analizza la base di codice, determina gli aggiornamenti necessari per il porting dell'applicazione e genera un rapporto di valutazione e un piano di trasformazione prima dell'inizio della trasformazione.

L'esperienza Visual Studio IDE supporta solo l'autenticazione tramite IAM Identity Center. Per ulteriori informazioni, consulta [Aggiungere utenti in IAM Identity Center](#).

L'esperienza IDE offre modalità autonome e interattive. Utilizza la modalità autonoma per la trasformazione automatica, adatta per lavori notturni o di lunga durata. Utilizza la modalità interattiva per collaborare con l'agente in chat, con un'elevata visibilità sulla trasformazione, un piano di trasformazione personalizzabile e una revisione dettagliata di ogni progetto. Puoi iterare per affinare i risultati o cambiare direzione finché non sei soddisfatto.

Quando un processo di trasformazione è attivo, puoi interagire con tre finestre:

- La finestra di chat è il punto di interazione principale con l'agente di trasformazione. Usa la chat per porre domande, discutere le opzioni, guidare la trasformazione e iterare.
- La finestra AWS Transform Job Plan mostra le fasi di avanzamento ed è dove è possibile scaricare o caricare artefatti o visualizzare le differenze di modifica del codice.
- La finestra Worklog mostra un registro delle attività di trasformazione in linguaggio naturale.

AWS Transform esegue quattro attività chiave per portare le applicazioni.NET su Linux:

- Aggiorna le versioni di .NET e linguistiche: aggiorna il codice .NET C# precedente alle versioni correnti di .NET e linguistiche.
- Migra da .NET Framework a .NET multiplatforma: migra progetti e pacchetti da .NET Framework dipendenti da Windows a .NET multiplatforma compatibili con Linux.
- Riscrive il codice per la compatibilità con Linux: rifattorizza e riscrive componenti di codice obsoleti e inefficienti.
- Genera un rapporto sulla compatibilità con Linux: per le attività a tempo indeterminato in cui è necessario l'intervento dell'utente per creare ed eseguire il codice su Linux, AWS Transform fornisce un rapporto dettagliato sulle azioni necessarie per configurare l'applicazione dopo la trasformazione.

Per ulteriori informazioni su come AWS Transform esegue le trasformazioni.NET, vedere. [In che modo AWS Transform modernizza le applicazioni.NET](#)

Per modernizzare il codice.NET utilizzando AWS Transform from Visual Studio IDE, fai riferimento a quanto segue:

- [Modernizzazione di .NET utilizzando AWS Trasforma in Visual Studio](#)
- [In che modo AWS Transform modernizza le applicazioni.NET](#)
- [Risoluzione dei problemi relativi alle trasformazioni .NET nell'IDE](#)

Quote

Per le quote di trasformazione AWS Transform .NET nell'IDE, vedi. [Quote per AWS Trasformazione](#)

Modernizzazione di .NET utilizzando AWS Trasforma in Visual Studio

Completa questi passaggi per trasferire un' Windows-based applicazione.NET su un'applicazione.NET Linux-compatible multiplatforma con AWS Transform nel Visual Studio 2026 o nel 2022.

Fase 1: prerequisiti

Prima di continuare, assicurati di aver scaricato e installato l'[estensione AWS Toolkit con Amazon Q](#) da Visual Studio Marketplace. Esamina [le funzionalità e le limitazioni](#) di AWS Transform per la modernizzazione.NET per confermare che il codice può essere trasformato.

Passaggio 2: Autenticazione in Visual Studio

Per connetterti ai tuoi AWS account dal Toolkit for Visual Studio, apri la Guida introduttiva all'interfaccia utente Toolkit (interfaccia utente di connessione): AWS

1. Dal menu principale di Visual Studio, vai a Estensioni > AWS Toolkit > Guida introduttiva per aprire la pagina Getting Started: AWS Toolkit.
2. Seleziona AWS Transform authentication.
3. Scegli un profilo esistente o creane uno nuovo. Quando crei un nuovo profilo, inserisci un nome per il profilo e l'URL di avvio di AWS Transform, che ti è stato inviato via email dopo essere stato aggiunto a IAM Identity Center dal tuo amministratore.
4. Scegli Connetti. Segui le istruzioni per accedere e concedere le autorizzazioni di accesso tramite il tuo browser web. In Visual Studio, dovresti vedere Connected with IAM Identity Center.
5. Dopo l'accesso, verrai indirizzato alla AWS Transform Dashboard. Da questa pagina di destinazione, puoi effettuare le seguenti operazioni:
 - Seleziona un profilo di AWS trasformazione (regione)
 - Seleziona o crea uno spazio di lavoro
 - Visualizza lo stato dei lavori di trasformazione

Fase 3: Trasforma la tua applicazione

Per trasformare una soluzione o un progetto .NET, completa la procedura seguente:

Inizia la trasformazione

1. Apri qualsiasi soluzione o progetto VB.NET basato su C# o basato su C# Visual Studio che desideri trasformare.
2. Da Solution Explorer, fai clic con il pulsante destro del mouse sulla soluzione o sul progetto che desideri trasformare e scegli Port with AWS Transform.
3. Viene visualizzata la finestra di dialogo Port with AWS Transform.
 - a. Nel menu a discesa Scegli uno spazio di lavoro, crea uno spazio di lavoro o seleziona uno esistente. Le aree di lavoro rendono visibile la tua attività nell'applicazione web AWS Transform, dove puoi invitare i collaboratori a visualizzare e parlare dei lavori di trasformazione e parlarne in chat.
 - b. Nel menu a discesa Scegli una destinazione .NET, scegli la versione .NET a cui desideri eseguire l'aggiornamento.
 - c. Per la modalità di trasformazione, seleziona Autonomo per la trasformazione automatica o Interattivo per la trasformazione interattiva.
 - d. Scegli Avvia per iniziare la trasformazione.
4. Una volta avviato il processo di trasformazione, vengono visualizzate le finestre AWS Transform Job Plan, Chat e Worklog.

Piano di valutazione e trasformazione

1. Dopo che AWS Transform ha analizzato il codice, nella chat vengono visualizzati un rapporto di valutazione e un piano di trasformazione. In modalità interattiva, la chat verrà messa in pausa per consentirti di rivederla. Se preferisci non recensire in chat, puoi utilizzare queste alternative:
 - Per visualizzare la valutazione o il piano nell'editor di codice, scegli Mostra valutazione o Mostra piano di trasformazione nella finestra AWS Transform Job Plan.
 - Per scaricare la valutazione o il piano, utilizza l'icona di download nella finestra Job Plan.
2. Facoltativamente, modifica il piano di trasformazione. Puoi discutere del piano tramite chat, ad esempio esplorando altre opzioni. Puoi apportare modifiche al piano fornendo istruzioni in chat o caricando un piano di trasformazione rivisto utilizzando l'icona di download nella finestra Job Plan. Puoi aggiungere, rimuovere o modificare liberamente i passaggi. La chat confermerà di aver compreso le tue istruzioni con un piano rivisto.
3. Carica facoltativamente i documenti direttivi. Nella finestra della chat, usa l'icona di caricamento per caricare documenti direttivi come le specifiche dell'applicazione, le preferenze e le

convenzioni relative allo stack tecnico organizzativo o gli esempi di programmazione. Dopo aver caricato un documento direttivo, descrivilo nella finestra di chat per fornire un contesto all'agente.

4. Quando sarai soddisfatto del piano, dai l'approvazione in chat e la trasformazione avrà inizio.
5. In modalità interattiva, puoi impostare i checkpoint in modo che si interrompano dopo che un progetto è stato trasformato per la revisione. I passaggi in Transforming code nella finestra Job Plan avranno icone di checkpoint rotonde. Tutti i progetti hanno i checkpoint abilitati per impostazione predefinita. Utilizza le caselle di controllo per cancellare o impostare un checkpoint.

Revisioni della trasformazione e dei checkpoint

1. AWS Transform inizia a trasformare il tuo codice. È possibile monitorare l'avanzamento delle fasi di trasformazione nella finestra AWS Transform Job Plan. La finestra Job Plan mostra il tempo massimo residuo stimato e il tuo Job ID.
2. Man mano che i progetti vengono trasformati, i riepiloghi vengono visualizzati nella chat e vengono applicate le modifiche al codice.
3. In modalità interattiva, quando viene raggiunto un checkpoint, l'agente si ferma per consentirti di esaminare i risultati. Nella finestra Job Plan, vedrai il pulsante Visualizza risultati per la fase in cui è in pausa, in cui puoi esaminare le differenze di codice. Dopo aver esaminato le modifiche, puoi chiedere ulteriori modifiche in chat o apportare tu stesso modifiche al Visual Studio codice.
4. Puoi iterare al checkpoint quanto vuoi. Quando sei soddisfatto, chiedi alla chat di continuare e passerà al progetto successivo.

Fine della trasformazione

1. Dopo aver trasformato i progetti, l'agente.NET attiverà una compilazione locale per confermare che il codice viene compilato correttamente sul computer locale. Visual Studio Se ci sono errori, funzionerà per risolverli.
2. Una volta completata la trasformazione, potrebbero essere necessari passaggi aggiuntivi, ad esempio attività di trasformazione che AWS Transform non è riuscito a eseguire o modifiche necessarie per la compatibilità con Linux. È disponibile per il download un file markdown per i passaggi successivi (NextSteps.md) che puoi utilizzare come prompt per un complemento di codice AI. Utilizza l'icona di download nella finestra Job Plan per scaricare NextSteps.md.
3. Puoi continuare a interagire in chat per porre domande o richiedere ulteriori modifiche.
4. Comunica alla chat quando sei pronto per terminare il tuo lavoro di trasformazione.

In che modo AWS Transform modernizza le applicazioni.NET

Consulta le seguenti sezioni per informazioni dettagliate su come funziona la trasformazione.NET con AWS Transform.

Analisi dell'applicazione e generazione di un piano di trasformazione

Prima che inizi una AWS trasformazione, Transform crea il codice localmente per verificare che sia compilabile e configurato correttamente per la trasformazione. Se il codice non viene compilato, AWS Transform chiederà se continuare con la trasformazione. AWS Transform carica quindi il codice in un ambiente di compilazione sicuro e crittografato AWS, analizza la codebase e determina gli aggiornamenti necessari per il porting dell'applicazione

Durante questa analisi, AWS Transform divide la soluzione o il progetto .NET in gruppi di codice. Un gruppo di codice è un progetto con tutte le sue dipendenze che insieme generano un'unità di codice compilabile come una DLL (Dynamic Link Library) o un eseguibile. Anche se non hai selezionato tutte le dipendenze del progetto da AWS trasformare, Transform determina le dipendenze necessarie per creare i progetti selezionati e li trasforma anche, in modo che l'applicazione trasformata sia compilabile e pronta per l'uso.

Dopo aver analizzato il codice, AWS Transform genera un piano di trasformazione che delinea le modifiche proposte da apportare, incluso un elenco di gruppi di codici e delle relative dipendenze che verranno trasformate.

Trasformazioni nell'applicazione

Per avviare la trasformazione, AWS Transform crea nuovamente il codice nell'ambiente di compilazione sicuro per verificare se è compilabile in remoto. AWS Transform inizia quindi a trasferire l'applicazione. Funziona dal basso verso l'alto, a partire dal livello di dipendenza più basso. Se AWS Transform riscontra un problema con il porting di una dipendenza, interrompe la trasformazione e fornisce informazioni sulla causa dell'errore.

La trasformazione include i seguenti aggiornamenti dell'applicazione:

- Sostituzione di versioni di codice C# obsolete con versioni C# Linux-compatible
- Aggiornamento di .NET Framework a .NET multiplatforma, tra cui:
 - Identificazione e sostituzione iterativa di pacchetti, librerie e API
 - Aggiornamento e sostituzione di pacchetti e API NuGet
 - Transizione al runtime multiplatforma

- Configurazione del middleware e aggiornamento delle configurazioni di runtime
- Sostituzione di pacchetti privati o di terze parti
- Gestione dei componenti IIS e WCF
- Debugging errori di compilazione
- Riscrittura del codice per la compatibilità con Linux, inclusa la rifattorizzazione e la riscrittura di codice obsoleto e inefficiente per trasferire il codice esistente

Revisione del rapporto di trasformazione e accettazione delle modifiche

Una volta completata la AWS trasformazione, Transform fornisce un rapporto sulla trasformazione con informazioni sugli aggiornamenti proposti all'applicazione, incluso il numero di file modificati, i pacchetti aggiornati e le API modificate. Segnala tutte le trasformazioni non riuscite, inclusi i file o le porzioni di file interessati e gli errori riscontrati durante un tentativo di compilazione. Puoi anche visualizzare un riepilogo della compilazione con relativi log per saperne di più sulle modifiche apportate.

Il rapporto sulla trasformazione fornisce anche uno stato del porting di Linux, che indica se è necessario o meno un input aggiuntivo da parte dell'utente per rendere l'applicazione compatibile con Linux. Se uno qualsiasi degli elementi di un gruppo di codici richiede un input da parte vostra, scaricate un report sullo stato di preparazione di Linux che contiene Windows-specific considerazioni che AWS Transform non era in grado di risolvere in fase di compilazione. Se è necessario un input per qualsiasi gruppo di codice o file, consulta il report per i dettagli sul tipo di modifica ancora da apportare e, se applicabile, per i suggerimenti su come aggiornare il codice. Queste modifiche devono essere apportate manualmente prima che l'applicazione possa essere eseguita su Linux.

È possibile esaminare le modifiche proposte da AWS Transform apportate in una visualizzazione differenziale prima di accettarle come aggiornamenti immediati dei file. Dopo aver aggiornato i file e aver risolto tutti gli elementi del report di fattibilità di Linux, l'applicazione è pronta per l'esecuzione su .NET multiplatforma.

Puoi scaricare un file markdown Next Steps con istruzioni per continuare la trasformazione con AWS Transform o un codice AI complementare. Per scaricare il file, scegli il pulsante Scarica i passaggi successivi in alto a destra del rapporto.

Risoluzione dei problemi relativi alle trasformazioni .NET nell'IDE

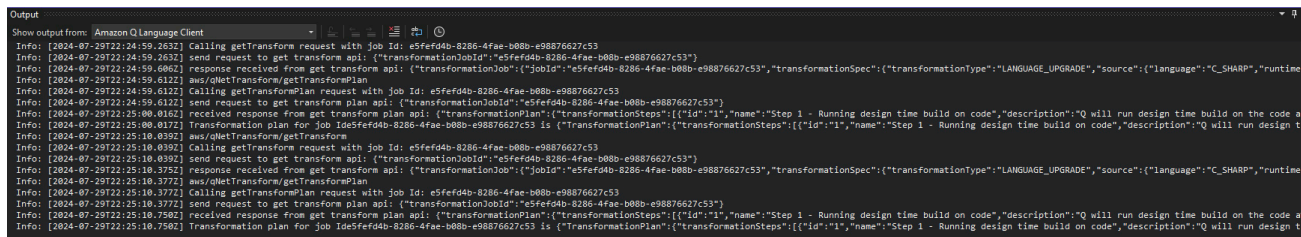
Utilizza le seguenti sezioni per risolvere i problemi più comuni relativi alle trasformazioni.NET nell'IDE con Transform. AWS

Come faccio a sapere se un lavoro sta procedendo?

Dovresti vedere un'attività regolare nella finestra Worklog. Se AWS Transform sembra dedicare molto tempo a una fase nella finestra AWS Transform Job Plan, è possibile verificare se il lavoro è ancora attivo nei log di output. Se vengono generati messaggi di diagnostica, il processo è ancora attivo.

Per controllare gli output, scegli la scheda Output in. Visual Studio Nel menu Mostra output da:, scegli Amazon Q Language Client.

La schermata seguente mostra un esempio degli output che AWS Transform genera durante una trasformazione.



```
Output
Show output from: Amazon Q Language Client
Info: [2024-07-29T22:24:59.263Z] Calling getTransform request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:24:59.263Z] send request to get transform api: {"transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53"}
Info: [2024-07-29T22:24:59.686Z] response received from get transform api: {"transformationJob":{"jobId":"e5fef04b-8286-4fae-b08b-e98876627c53"},"transformationSpec":{"transformationType":"LANGUAGE_UPGRADE","source":{"language":"C_SHARP","runtime
Info: [2024-07-29T22:24:59.612Z] aws/dllTransform/getTransformPlan
Info: [2024-07-29T22:24:59.612Z] Calling getTransformPlan request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:24:59.612Z] send request to get transform plan api: {"transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53"}
Info: [2024-07-29T22:25:00.016Z] received response from get transform plan api: {"transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design time build on the code a
Info: [2024-07-29T22:25:00.017Z] Transformation plan for job Id e5fef04b-8286-4fae-b08b-e98876627c53 is {"transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
Info: [2024-07-29T22:25:10.039Z] aws/dllTransform/getTransform
Info: [2024-07-29T22:25:10.039Z] Calling getTransform request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:25:10.039Z] send request to get transform api: {"transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53"}
Info: [2024-07-29T22:25:10.375Z] response received from get transform api: {"transformationJob":{"jobId":"e5fef04b-8286-4fae-b08b-e98876627c53"},"transformationSpec":{"transformationType":"LANGUAGE_UPGRADE","source":{"language":"C_SHARP","runtime
Info: [2024-07-29T22:25:10.377Z] aws/dllTransform/getTransformPlan
Info: [2024-07-29T22:25:10.377Z] Calling getTransformPlan request with job Id: e5fef04b-8286-4fae-b08b-e98876627c53
Info: [2024-07-29T22:25:10.377Z] send request to get transform plan api: {"transformationJobId":"e5fef04b-8286-4fae-b08b-e98876627c53"}
Info: [2024-07-29T22:25:10.750Z] received response from get transform plan api: {"transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
Info: [2024-07-29T22:25:10.750Z] Transformation plan for job Id e5fef04b-8286-4fae-b08b-e98876627c53 is {"transformationPlan":{"transformationSteps":[{"id":"1","name":"Step 1 - Running design time build on code","description":"Q will run design t
```

Perché alcuni progetti non vengono selezionati per la trasformazione?

AWS Transform può trasformare solo i tipi di progetto.NET supportati. Per un elenco dei tipi di progetto supportati e altri prerequisiti per la trasformazione dei tuoi progetti .NET, consulta [Fase 1: prerequisiti](#).

Come posso ottenere assistenza se il mio progetto o la mia soluzione non si sta trasformando?

Se non sei in grado di risolvere i problemi da solo, puoi contattare il tuo team Supporto o contattare il tuo Account AWS team per inviare una richiesta di supporto.

Per ricevere assistenza, fornisci l'ID del processo di trasformazione in modo da AWS poter indagare su un lavoro non riuscito. Per trovare un ID del processo di trasformazione, scegli la scheda Output inVisual Studio. Nel menu Mostra output da:, scegli Amazon Q Language Client.

Come posso evitare che il mio firewall interferisca con i processi di trasformazione?

Se la tua organizzazione utilizza un firewall, potrebbe interferire con le trasformazioni inVisual Studio. È possibile disattivare temporaneamente i controlli di sicurezza Node.js per risolvere i problemi o verificare cosa impedisce l'esecuzione della trasformazione.

La variabile di ambiente `NODE_TLS_REJECT_UNAUTHORIZED` verifica importanti controlli di sicurezza. L'impostazione `NODE_TLS_REJECT_UNAUTHORIZED` su «0» disabilita il rifiuto dei certificati non Node.js autorizzati. TLS/SSL Ciò significa che:

- Self-signed i certificati saranno accettati
- Saranno consentiti i certificati scaduti
- Saranno consentiti certificati con nomi host non corrispondenti
- Eventuali altri errori di convalida dei certificati verranno ignorati

Se il proxy utilizza un autocertificato, è possibile impostare le seguenti variabili di ambiente anziché disabilitarle `NODE_TLS_REJECT_UNAUTHORIZED`:

```
NODE_OPTIONS = -use-openssl-ca  
NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs
```

Altrimenti, è necessario specificare i certificati CA utilizzati dal proxy per disabilitare `NODE_TLS_REJECT_UNAUTHORIZED`.

Per disabilitare `NODE_TLS_REJECT_UNAUTHORIZED` su Windows:

1. Apri il menu Start e cerca le Variabili di ambiente.
2. Scegli Modifica le variabili d'ambiente di sistema.
3. Nella finestra Proprietà del sistema, scegli Variabili d'ambiente.
4. In Variabili di sistema, scegli Nuovo.
5. Imposta il Nome della variabile su `NODE_TLS_REJECT_UNAUTHORIZED` e il Valore della variabile su 0.
6. Scegli OK per salvare le modifiche.
7. Riavviare Visual Studio.

Porting del codice del livello dell'interfaccia utente

AWS Transform può trasferire il livello di interfaccia utente dei ASP.NET siti Web su framework di interfaccia utente compatibili con ASP.NET Core, che possono essere eseguiti su Linux. Sono disponibili le seguenti trasformazioni:

- Porting dell'interfaccia utente MVC Razor
- Trasferimento da Web Forms a Blazor UI

Portabilità dell'interfaccia utente MVC Razor

ASP.NET I progetti MVC con interfaccia utente Razor Views possono essere trasferiti su MVC Razor Views on ASP.NET Core, rimanendo sullo stesso framework dell'interfaccia utente. Sebbene le visualizzazioni di Razor siano simili tra ASP.NET e ASP.NET Core, ci sono differenze che richiedono modifiche al codice di portabilità:

- ASP.NET Le visualizzazioni MVC Razor utilizzano lo spazio dei System.Web.Mvc nomi e sono strettamente legate a .NET Framework.
- ASP.NET Le Core Razor Views sono modulari, integrate e con una migliore iniezione di Microsoft.AspNetCore.Mvc dipendenza.
- ASP.NET Core ha nuove funzionalità tra cui Tag Helpers e View Components.

AWS Transform rileva e trasferisce componenti e costrutti incompatibili comuni in Razor Views.

Trasferimento da Web Forms a Blazor UI

ASP.NET L'interfaccia utente di Web Forms non ha una controparte su Core. ASP.NET AWS Transform può trasferire il codice di livello dell'interfaccia utente di Web Forms su Blazor Server on Core. ASP.NET Il codice del livello dell'interfaccia utente viene riscritto per il framework dell'interfaccia utente di destinazione.

Per abilitare o disabilitare il porting dell'interfaccia utente da Web Forms a Blazor, seleziona o deselecta l'impostazione del processo Transform UI ASP.NET Web Forms to Blazor.

Dettagli sulla trasformazione

Il tuo progetto Web Forms viene convertito in un progetto Blazor con hosting lato server. Durante la trasformazione vengono apportate le seguenti modifiche al progetto e al file:

Mappatura della trasformazione dei file

Da	Per	Description
*.aspx, *.ascx	*.razor	Le pagine.aspx e i controlli personalizzati.ascx diventano file.razor
Web.config	appsettings.json	Web.config le impostazioni diventano impostazioni appsettings.json

Da	Per	Description
Global.asax	Program.cs	Global.asax Program.cs il codice diventa codice
*.master	*layout.razor	I file master diventano file layout.razor

Post-transformation struttura del progetto

Dopo la trasformazione, i file trasformati si trovano nelle seguenti posizioni del progetto:

- Cartella Components: tutti i componenti razor (*.razor) vengono inseriti in una cartella Components creata allo stesso livello del file.csproj del progetto.
- Mappatura delle pagine: le pagine Web Forms (*.aspx) vengono convertite in una struttura di cartelle. Components/Pages
- Mappatura dei controlli: i controlli Web Forms (*.ascx) vengono posizionati direttamente nella cartella Componenti.

Limitazioni e funzionalità non supportate

Le seguenti funzionalità non sono attualmente supportate. Se i carichi di lavoro utilizzano queste funzionalità, il codice dovrà essere trasferito manualmente o con un codice AI complementare dopo la trasformazione.

- file.svc (file di servizio)
- .ashx (file di gestione generici)
- Riferimenti ai servizi e riferimenti Web (file reference.map, reference.cs, .wsdl)
- Combinazioni di file.aspx (Web Forms) e file.cshtml (Razor) nello stesso progetto
- Dipendenze da tipi di progetto non ancora supportati da Transform for .NET AWS
- Third-party interfaccia utente del fornitore libraries/controls
- progetti di siti Web

Sono supportati solo i progetti di applicazioni Web (contenenti un file.csproj). Per convertire un progetto di sito Web in un progetto di applicazione Web, vedere la guida Microsoft sulla [conversione di un progetto di sito Web in un progetto di applicazione Web](#).

Rapporti sulla trasformazione

Una volta completato il processo di trasformazione.NET, sono disponibili i seguenti report di trasformazione:

- [Rapporto di riepilogo sulla trasformazione](#)
- [Rapporto dettagliato sulla trasformazione](#)

Rapporto di riepilogo sulla trasformazione

Una volta completato un processo di trasformazione, nella console web è disponibile un rapporto di riepilogo della trasformazione. Scarica il rapporto di riepilogo della trasformazione dalla scheda Dashboard. Seleziona Scarica il rapporto di riepilogo sulla trasformazione e scegli Scarica come HTML o Scarica come JSON.

Il rapporto di riepilogo sulla trasformazione offre una panoramica della trasformazione e delle informazioni specifiche di ciascun repository che è stato trasformato, tra cui:

- Dettagli del processo
 - Panoramica del lavoro di trasformazione
 - Panoramica dei risultati della trasformazione
 - Panoramica dei file
- Elenco dei repository e per ogni repository:
 - Panoramica dei nomi dei repository
 - Riepilogo della trasformazione della soluzione
 - Dettagli del progetto, tra cui stato, tipo, versione.NET, righe di codice totali, righe di codice trasformate e file modificati

Rapporto dettagliato sulla trasformazione

Al termine di un processo di trasformazione, i report dettagliati sulla trasformazione sono disponibili sia per gli utenti della console Web che per quelli IDE.

- Utenti della console Web: è disponibile un rapporto dettagliato per ogni repository trasformato. Nella scheda Dashboard, utilizza i collegamenti Scarica report dettagliati nell'elenco del repository per scaricare un report dettagliato.

- Utenti IDE: scaricate il report di trasformazione dalla finestra AWS Transform Job Plan utilizzando l'icona di download.

Il rapporto dettagliato sulla trasformazione è un rapporto HTML interattivo. Contiene informazioni approfondite sulla trasformazione, inclusi i motivi delle modifiche ai file e dettagli sugli errori risolvibili. Le informazioni sono disposte nella seguente gerarchia:

- Informazioni sul lavoro
- Per ogni soluzione:
 - Riepilogo della trasformazione della soluzione
 - Panoramica della trasformazione
 - Progetti
 - Per ogni progetto:
 - Riepilogo del progetto
 - Riepilogo degli errori di costruzione
 - NuGet modifiche al pacchetto
 - Modifiche ai file
 - Errori di compilazione
 - Risultati del test unitario
 - Rapporto sulla disponibilità di Linux

Per una panoramica dettagliata delle sezioni del report sui dettagli della trasformazione con esempi, consulta il post di blog [Announcing AWS Transform for .NET](#): report dettagliati sulle trasformazioni.

Procedure consigliate per le trasformazioni.NET

Segui queste linee guida per ottenere migliori risultati di modernizzazione.NET con Transform. AWS Queste best practice si applicano all'assistente di intelligenza artificiale conversazionale.NET, attualmente disponibile per IDE. Visual Studio

Argomenti

- [Prima della trasformazione](#)
- [Valutazione e pianificazione](#)
- [Trasforma in modo interattivo o autonomo](#)

- [Convalida e finalizzazione](#)

Prima della trasformazione

Leggi i seguenti consigli prima di iniziare un processo di trasformazione.NET.

Usa l'assistente di intelligenza artificiale conversazionale.NET

Usa il nuovo agente .NET per ottenere i migliori risultati di trasformazione. L'assistente di intelligenza artificiale conversazionale è disponibile Visual Studio tramite [AWS Toolkit](#) for Visual Studio. È disponibile anche per [Kiro](#) altri IDE tramite Kiro Power for AWS Transform and Transform MCP agent AWS . Il nuovo agente .NET non è ancora disponibile nella console Web.

Usa altri strumenti se l'obiettivo non è la trasformazione da .NET a.NET

AWS Transform for .NET è appropriato per la modernizzazione del codice da .NET Framework a.NET a .NET e per gli aggiornamenti di.NET alle versioni successive. Non è adatto per trasformazioni che includono linguaggi non .NET, come Java, o framework non .NET, come React. Inoltre, non fornisce il refactoring dell'architettura delle applicazioni. Usa [AWS Transform custom](#) o Kiro per questo tipo di modernizzazione.

Usa un'edizione stabile di Visual Studio, preferibilmente VS2026

Utilizza un'edizione GA Visual Studio anziché un'edizione di anteprima o un'edizione Insiders per evitare complicazioni dovute al software di anteprima. Il AWS Toolkit può essere utilizzato con il Visual Studio 2026 o il 2022. VS2026 è consigliato perché offre prestazioni migliori con un consumo di memoria ridotto.

Usa la versione più recente AWS Toolkit per Visual Studio

Rimani aggiornato sull'ultima versione di AWS Toolkit for Visual Studio per la correzione di bug e gli aggiornamenti delle funzionalità. Puoi controllare la versione del tuo toolkit ed eseguire l'aggiornamento in Estensioni > Gestione delle estensioni > Installate.

Lavora in Visual Studio IDE per progetti di complessità media o superiore

L'esperienza IDE offre una visione più approfondita della trasformazione, grazie alla quale è possibile collaborare con l'agente .NET nella trasformazione dei progetti. Per progetti di complessità media, alta o critica, utilizza l'IDE anziché la console web.

Predisponi di un piano di convalida

Decidete come convalidare la correttezza della vostra applicazione dopo la sua trasformazione. Post-transformation, dovrai confermare che si comporti e appaia correttamente quando viene eseguita e che i controlli di sicurezza, la logica aziendale e l'archiviazione dei dati siano intatti. La convalida verrà condotta manualmente and/or utilizzando l'automazione dei test? Se la soluzione contiene test unitari, AWS Transform li trasferirà automaticamente ed eseguirà, e i risultati verranno visualizzati nel rapporto di trasformazione.

Fornire NuGet dipendenze private dei pacchetti

Se la tua soluzione dipende da pacchetti privati, assicurati che siano disponibili sul tuo computer locale in modo che IDE e AWS Transform possano trovarli.

Specificate i pacchetti sostitutivi o chiedete consigli agli agenti

Per i pacchetti che non dispongono di versioni di .NET moderne, è possibile personalizzare il piano di trasformazione per specificare le sostituzioni di pacchetto previste oppure chiedere consigli all'agente.

Non terminate il vostro lavoro finché non siete sicuri di non volere altre modifiche

Una volta completata la trasformazione, non terminate subito il lavoro nel caso in cui desideriate apportare ulteriori modifiche. La trasformazione non è completa finché non lo affermate voi. Puoi richiedere modifiche fino a quando non contrassegni il lavoro come completato.

Dopo la trasformazione, passa a un complemento di codice AI per finalizzare la tua app

Aspettati di combinare AWS Transform con un compagno di codice AI come. Kiro Uno schema comune prevede prima la trasformazione con AWS Transform for .NET, quindi la passa a un complemento di codice AI per finalizzare l'applicazione. Tale lavoro di finalizzazione potrebbe includere l'identificazione e la correzione di errori di runtime, problemi comportamentali e stile UX.

Nel percorso di modernizzazione, pensate a AWS Transform come a un mezzo di trasporto rapido che vi aiuta a raggiungere il vostro obiettivo, e a un programma basato sull'intelligenza artificiale come al viaggio locale che vi condurrà alla destinazione finale.

Per facilitare il passaggio da AWS Transform ai compagni di codice AI, AWS Transform fornisce un rapporto sulla trasformazione HTML e un documento markdown Next Steps al termine della trasformazione.

Valutazione e pianificazione

Dopo aver avviato un processo di trasformazione, AWS Transform analizza il codice e produce un rapporto di valutazione e un piano di trasformazione. Utilizza le seguenti best practice per ottenere il massimo da questa fase.

Rivedi la valutazione e fai domande per definire le tue aspettative

Esamina attentamente i risultati della valutazione per capire quali progetti saranno difficili da trasformare e perché. L'agente presenta i progetti con un livello di complessità (basso, medio, alto, critico) e spiega perché hanno tale classificazione.

Fai domande per capire meglio le aree difficili. Ad esempio:

- Chiedi all'agente qual è il suo livello di fiducia in una trasformazione di progetto o in un caso d'uso.
- Chiedi all'agente quali attività post-trasformazione saranno probabilmente necessarie con un codice di intelligenza artificiale complementare.

Esamina il piano e discuti le opzioni con l'agente

L'agente fornisce un piano di trasformazione da esaminare. Puoi discutere e modificare questo piano. Inizia comprendendo le tue opzioni. Chiedi all'agente quali sono le alternative a qualsiasi parte del piano.

Ad esempio, il piano di trasformazione potrebbe proporre la trasformazione dei servizi WCF in API ASP.NET Web. Tuttavia, la tua organizzazione preferisce rimanere con WCF. Chiedi all'agente delle opzioni e scopri che un'alternativa è trasformarle in CoreWCF.

Carica i documenti direttivi per personalizzare un piano per la tua organizzazione

Il piano di trasformazione originale viene creato senza una comprensione dei requisiti e delle preferenze dell'organizzazione. È possibile informare l'agente sulle convenzioni organizzative, sulle specifiche delle applicazioni, sullo stack tecnologico preferito e sugli esempi di modelli di codifica preferiti.

Dopo aver caricato un documento direttivo, spiegallo per fornire un contesto all'agente. Con le informazioni aggiuntive contenute nei documenti direttivi, l'agente può preparare un piano personalizzato in base al modo in cui la tua organizzazione preferisce lavorare.

Personalizza liberamente il piano

L'agente.NET è flessibile e puoi personalizzare liberamente il piano di trasformazione, all'interno del dominio della trasformazione di.NET a.NET. Puoi chiedere modifiche al piano in chat o, se preferisci, puoi lavorare con i file markdown. Rivedi e perfeziona il piano fino a quando non sei soddisfatto.

Se un piano deve essere esaminato da più parti interessate, puoi scaricare il piano come file di markdown, dividerlo e successivamente caricare un piano personalizzato.

Ad esempio, si esamina il piano di trasformazione e si decide di voler trasformare i progetti della libreria di classi in.NET Standard anziché in .NET 10. In chat dici «Rivedi il piano per trasformare tutte le librerie di classi in.NET Standard 2.0» e l'agente ti presenta un piano rivisto.

Trasforma in modo interattivo o autonomo

L'esperienza Visual Studio IDE offre modalità autonome e interattive per controllare il grado di interattività durante la trasformazione.

Utilizza modalità interattive e autonome per controllare il grado di interattività

Seleziona la modalità quando inizi una trasformazione e puoi cambiarla in qualsiasi momento tramite un menu a discesa nella parte superiore della finestra della chat.

- Utilizza la modalità autonoma per la trasformazione non presidiata, adatta per lavori notturni o di lunga durata. Hai ancora la possibilità di rivedere i risultati e chiedere modifiche alla fine del lavoro.
- Utilizza la modalità interattiva per collaborare con l'agente in chat durante tutto il processo di trasformazione con un piano di trasformazione personalizzabile, un'elevata visibilità dei dettagli della trasformazione e una revisione dettagliata di ogni progetto. Puoi iterare per affinare i risultati o cambiare direzione finché non sei soddisfatto.

È possibile combinare le modalità. Ad esempio, inizia in modalità interattiva per rivedere e modificare il piano di trasformazione, quindi passa alla modalità autonoma per trasformare automaticamente i progetti.

Chiedi all'agente di spiegare le modifiche al codice

Se vedi modifiche al codice che non comprendi, chiedi all'agente di spiegarle.

Usa i checkpoint per fermarti ai progetti per rivederli o modificarli

In modalità interattiva, dopo aver approvato il piano, puoi impostare o cancellare i checkpoint per ogni progetto. Quando un progetto con un checkpoint è stato trasformato, il codice trasformato viene applicato al progetto in IDE e l'agente si ferma per la revisione. Puoi rivedere i risultati e, se non ti piacciono, puoi chiedere ulteriori modifiche.

Mentre sei fermato a un checkpoint, puoi:

- Rivedi i risultati così come sono presentati in chat e fai domande in chat. Ad esempio: «Perché hai modificato l'API di crittografia nel file X?»
- Visualizza le modifiche al codice, scegliendo il pulsante Visualizza risultati per il progetto nella finestra AWS Transform Job Plan.
- Perfeziona la trasformazione chiedendo ulteriori modifiche. Ad esempio: «Modifica questo per utilizzare il logger X» o «Modifica questo per utilizzare il pacchetto X anziché il pacchetto Y».
- Riprova la trasformazione, rifacendola con istruzioni diverse. Ad esempio: «Cambia questa libreria di classi impostando .NET Standard anziché .NET 10" o «Riprova questa trasformazione e cambia la destinazione da MVC Razor Blazor Pages».
- Apporta le tue modifiche al codice nell'IDE.
- Dite all'agente di passare al checkpoint successivo del progetto.

Iterate finché non siete soddisfatti

La modernizzazione è intrinsecamente iterativa e puoi aspettarti di iterare con l'agente. È possibile apportare modifiche ai punti di controllo del progetto e anche al termine della trasformazione. Esegui l'iterazione secondo necessità finché non sei soddisfatto. La trasformazione non è completa finché non lo dici.

Codifica insieme all'agente quando viene fermato a un checkpoint

Puoi apportare le tue modifiche al codice mentre lavori con l'agente. Quando ti fermi a un checkpoint, puoi modificare i file di codice in Visual Studio. Le modifiche verranno sincronizzate quando indicherai all'agente di continuare.

Convalida e finalizzazione

Al termine della trasformazione, convalida l'applicazione trasformata e finalizzala per l'uso in produzione.

Consulta il report sulla trasformazione e i passaggi successivi per capire cosa è stato fatto e cosa resta

Consulta il report sulla trasformazione HTML per capire cosa è stato fatto. Esamina il file di markdown Next Steps per capire quali attività rimangono ancora da svolgere. Chiedi all'agente di chiarire tutto ciò che non è chiaro.

Usa un codice AI complementare per convalidare, eseguire il debug e finalizzare l'applicazione

Verifica la correttezza della tua applicazione trasformata. Utilizza un codice di intelligenza artificiale complementare, ad esempio [Kiro](#) per risolvere i problemi.

Convalida i test unitari

Se la tua soluzione contiene progetti di unit test (NUnit, xUnit, oMSTest), AWS Transform li trasferirà sulla versione moderna di .NET ed eseguirà i test per te. Consulta il rapporto di trasformazione HTML per i risultati dei test unitari. Correggi i test non riusciti con un complemento di codice AI.

Convalida la funzionalità dell'applicazione

Esegui l'applicazione e verifica che la sua funzionalità corrisponda all'originale. Nota i problemi funzionali e gli errori di runtime. Correggi con un codice AI complementare.

Convalida l'interfaccia utente dell'applicazione

Esegui l'applicazione e verifica che appaia e si comporti come l'originale, inclusi navigazione e routing. Se l'applicazione non ha uno stile, è possibile che i file.css non si trovino nella posizione corretta. Correggi con un codice AI complementare.

Modernizzazione di SQL Server

AWS Transform for SQL Server Modernization è un AI-powered servizio che automatizza la modernizzazione completa dei database Microsoft SQL Server e delle applicazioni .NET associate su Amazon Aurora PostgreSQL. Il servizio orchestra l'intero percorso di migrazione dalla conversione dello schema, alla migrazione dei dati e alla modifica del codice dell'applicazione per adattarlo al nuovo obiettivo PostgreSQL, rendendo i team più produttivi automatizzando attività complesse e laboriose.

Regioni supportate

AWS Transform for SQL Server è disponibile negli Stati Uniti orientali (Virginia settentrionale) - us-east-1

Cross-Region Utilizzo: per i database in aree non supportate, è possibile clonare il database in un'area supportata per la trasformazione, quindi distribuire nuovamente i risultati nell'area di destinazione.

Funzionalità e caratteristiche principali

Trasformazione del database

- Conversione dello schema: converte automaticamente gli schemi di SQL Server in Aurora PostgreSQL, incluse tabelle, viste, indici, vincoli e relazioni
- Trasformazione delle procedure memorizzate: converte le procedure memorizzate in modo accurato T-SQL PL/pgSQL AI-enhanced
- Migrazione dei dati: migra i dati con convalida dell'integrità utilizzando AWS Database Migration Service (DMS)
- Oggetti del database: supporta trigger, funzioni, viste, colonne calcolate e colonne di identità
- Convalida: verifica automatizzata dell'integrità dei dati e controlli di integrità referenziale

Trasformazione delle applicazioni

- Trasformazione di Entity Framework: aggiorna le configurazioni di Entity Framework 6.3-6.5 ed EF Core 1.0-8.0 per PostgreSQL
- ADO.NET trasformazione: converte il codice di accesso ai ADO.NET dati da SQL Server ai provider PostgreSQL.
- Aggiornamenti delle stringhe di connessione: aggiorna automaticamente tutte le stringhe di connessione al database PostgreSQL di destinazione
- Modifiche al provider di database: sostituisce i provider di SQL Server con Npgsql (provider PostgreSQL)
- Aggiornamenti della configurazione ORM: modifica le mappature dei tipi di dati, le colonne di identità e le configurazioni specifiche del database

&Convalida dell'orchestrazione

- Wave-based modernizzazione: organizza grandi proprietà in fasi logiche di migrazione
- Mappatura delle dipendenze: identifica le relazioni tra applicazioni e database
- Human-in-the-loop Checkpoint (HITL): forniscono porte di revisione e approvazione nelle fasi critiche
- Convalida automatizzata: verifica la compatibilità dello schema, l'integrità dei dati e la funzionalità dell'applicazione
- CI/CD integrazione: si integra con le pipeline di sviluppo esistenti

Implementazione

- Implementazione di Amazon ECS e Amazon EC2: distribuzione containerizzata automatizzata con supporto per l'auto-scaling
- Infrastructure-as-code generazione: crea modelli o CDK CloudFormation AWS
- Convalida automatizzata dell'implementazione: verifica la corretta implementazione con controlli di integrità
- Funzionalità di rollback: supporta le procedure di rollback in caso di problemi

Versioni e tipi di progetto supportati

Versioni di SQL Server

AWS Transform supporta le seguenti versioni di SQL Server:

Versione SQL Server:	Stato del supporto
SQL Server 2022	Supportata
SQL Server 2019	Supportata
SQL Server 2017	Supportata
SQL Server 2016	Supportata
SQL Server 2014	Supportata

Versione SQL Server:	Stato del supporto
SQL Server 2012	Supportata
SQL Server 2008 R2	Supportata

Note

Sono supportate tutte le edizioni di SQL Server (Express, Standard, Enterprise). SQL Server può essere ospitato su AWS (Amazon RDS for SQL Server o SQL Server su Amazon EC2) o ospitato all'esterno di AWS.

Versioni .NET

Versione .NET	Stato del supporto
.NET 10	Supportata
.NET 8	Supportata
.NET 7	Supportata
.NET 6 (Nucleo)	Supportata
.NET Framework 4.x e versioni precedenti	Non supportato

Important

.NET Framework 4.x e versioni precedenti non sono supportate. Se l'applicazione utilizza .NET Framework, è necessario eseguire l'aggiornamento a .NET Core 6+ utilizzando AWS Transform for .NET modernization prima di utilizzare le funzionalità di trasformazione di SQL Server.

versioni Entity Framework

Framework	Versioni supportate
Entity Framework 6	6.3, 6.4, 6.5
Entity Framework Core	Da 1.0 a 8.0
ADO.NET	Tutte le versioni (GA)

Archivi di codice sorgente

AWS Transform supporta le seguenti piattaforme di codice sorgente:

- GitHub e GitHub Enterprise Server
- GitLab.com e GitLab Self-Managed
- Bitbucket Cloud e Bitbucket Data Center
- Azure e Azure Server DevOps DevOps
- Simple Storage Service (Amazon S3)

Database di destinazione

AWS Transform si rivolge ad Amazon Aurora PostgreSQL (compatibile con PostgreSQL 15+) con supporto per le più recenti funzionalità e ottimizzazioni di Aurora.

Requisiti tecnici

Requisiti del database

- Microsoft SQL Server versione 2008 R2 fino al 2022
- SQL Server ospitato su AWS (Amazon RDS for SQL Server o SQL Server su Amazon EC2) o ospitato all'esterno di AWS
- Per i database AWS ospitati, il database e AWS Transform devono trovarsi nella stessa regione. AWS
- Per i database ospitati all'esterno AWS, è richiesta la connettività di rete al servizio AWS Transform.

- Utente del database con autorizzazioni VIEW DEFINITION e VIEW DATABASE STATE
- Password del database che utilizzano solo caratteri ASCII stampabili (esclusi '/', '@', '' e spazi)
- Il VPC contenente il SQL Server di origine deve avere sottoreti in almeno 2 zone di disponibilità diverse (richiesta per i sottoreti di replica DMS)

Requisiti dell'applicazione

- Applicazioni.NET Core 6, 7 o 8
- Entity Framework 6.3-6.5 o Entity Framework Core 1.0-8.0, oppure ADO.NET
- Connessioni al database individuabili nel codice sorgente
- Le applicazioni vengono create ed eseguite correttamente
- Codice sorgente nelle piattaforme di repository supportate

AWS requisiti dell'account

- AWS account con accesso da amministratore
- IAM Identity Center abilitato
- Ruoli di servizio richiesti creati (vedi le istruzioni di configurazione riportate di seguito)
- VPC con configurazione di rete appropriata

Elaborazione e archiviazione dei dati

Luogo del trattamento

- L'elaborazione dello schema avviene in un'istanza DMS all'interno del tuo VPC
- La migrazione dei dati è facoltativa e può essere esclusa se necessario
- Gli artefatti di trasformazione vengono archiviati nell'area del servizio AWS Transform

Artefatti memorizzati

I seguenti elementi sono memorizzati nell'area di servizio:

- Log dell'agente
- Risultati della valutazione

- file di schema SQL
- Artefatti di output DMS

Important

Importante per la residenza dei dati: anche quando la migrazione dei dati viene disattivata, i metadati e gli elementi di elaborazione vengono archiviati nell'area di servizio. Questo è importante per le organizzazioni con requisiti rigorosi di residenza dei dati.

Gestione degli Artifact

- Opzione per il cliente per la crittografia utilizzando le proprie chiavi KMS
- Periodo TTL (time-to-live) definito per tutti gli artefatti
- Gli artefatti possono essere scaricati per l'archiviazione offline

Requisiti di SQL Server

Requisiti del database

Database ospitati esternamente

Sono supportati i database ospitati all'esterno AWS di. Per utilizzare un database ospitato esternamente, è necessario garantire la connettività di rete tra il database e il servizio AWS Transform.

Carichi di lavoro SSIS

- Limitazione: la trasformazione di SQL Server Integration Services (SSIS) non è supportata.
- Soluzione alternativa: utilizza AWS Glue o altri servizi ETL per la migrazione SSIS.

Server collegati

- Limitazione: le connessioni a database esterni tramite server collegati richiedono una configurazione umana.
- Soluzione alternativa: riconfigurare i server collegati dopo la migrazione o utilizzare approcci alternativi come collegamenti al database o integrazione a livello di applicazione.

Schemi complessi T-SQL

- Limitazione: alcuni T-SQL modelli avanzati potrebbero richiedere l'intervento umano.
- Soluzione alternativa: usa la CLI di Amazon Kiro per conversioni SQL complesse. AWS Transform li contrassegna per la revisione durante il processo di trasformazione.

Requisiti dell'applicazione

.NET Framework legacy

- Limitazione: .NET Framework 4.x e le versioni precedenti non sono supportate.
- Soluzione alternativa: utilizzare prima AWS Transform for .NET per eseguire l'aggiornamento a .NET Core 6+, quindi utilizzare la trasformazione di SQL Server.

versioni Entity Framework

- Limitazione: sono supportati solo Entity Framework 6.3-6.5 ed EF Core 1.0-8.0.
- Soluzione alternativa: eseguire l'aggiornamento a una versione di Entity Framework supportata prima della trasformazione.

VB.NET applicazioni

- Limitazione: non VB.NET è supportata.
- Soluzione alternativa: convertire in C# o utilizzare AWS Transform custom per VB.NET convertire da C#.

Cross-database dipendenze

- Limitazione: sfide quando gli schemi di database interagiscono tra più database.
- Soluzione alternativa: rivedi e rifattorizza le query tra database prima della migrazione. Prendi in considerazione il consolidamento dei database o l'utilizzo di schemi PostgreSQL.
- Impatto: può richiedere l'intervento umano per scenari complessi tra database.

Repository-database accoppiamento

- Limitazione: sfide quando un singolo repository serve più database.
- Soluzione alternativa: prendi in considerazione la ristrutturazione dei repository o un approccio di migrazione graduale.
- Impatto: potrebbe richiedere una pianificazione aggiuntiva per le migrazioni basate su ondate.

Requisiti di infrastruttura

Singola per lavoro account/region

- Limitazione: ogni processo di trasformazione riguarda un AWS account e una regione.
- Soluzione alternativa: crea più processi di trasformazione per implementazioni con più account o più regioni.

Destinazioni di implementazione

- Limitazione: sono supportate le distribuzioni di Amazon ECS e Amazon EC2.

Requisiti del repository

Pacchetti privati NuGet

- Limitazione: NuGet i pacchetti privati richiedono una configurazione aggiuntiva.
- Soluzione alternativa: configura NuGet i feed privati nelle impostazioni di trasformazione prima di iniziare il lavoro.

Configurazione di SQL Server

Esegui questi passaggi nel tuo ambiente SQL Server per abilitare la modernizzazione di AWS Transform.

Configurazione e configurazione del database

Passaggio 1: creare un utente del database con le autorizzazioni richieste

Crea un utente di database dedicato per AWS Transform con le autorizzazioni necessarie. Se hai già un utente DMS Schema Conversion, puoi riutilizzarlo.

Connect all'istanza di SQL Server ed esegui i seguenti comandi:

```
-- 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

Ripeti i comandi specifici del database (USE, CREATE USER, GRANT) per ogni database che desideri modernizzare.

Il ruolo db_datareader è necessario solo per la migrazione dei dati, non solo per la conversione dello schema.

- Il ruolo db_datareader garantisce l'accesso in lettura a tutte le tabelle del database
- Questo ruolo è richiesto SOLO quando si esegue la migrazione dei dati.
- Solo per la conversione dello schema (senza migrazione dei dati), il ruolo db_datareader NON è richiesto

- Le altre autorizzazioni (VIEW DEFINITION, VIEW DATABASE STATE, ecc.) sono sufficienti per la conversione dello schema

Passaggio 2: Archivia le credenziali in AWS Secrets Manager

Archivia le credenziali del database in modo sicuro in AWS Secrets Manager. Salta questo passaggio se hai già creato un segreto per DMS.

1. Vai a AWS Secrets Manager nella console
2. Scegli Memorizza un nuovo segreto
3. Configura il segreto:
 - Tipo segreto: credenziali per un altro database
 - Banca dati: Microsoft SQL Server
 - Nome utente: atx_user (o nome utente scelto)
 - Password: la password che hai creato
 - Nome del server: l'endpoint SQL Server
 - Nome del database: il nome del tuo database
 - Porta: 1433 (o porta personalizzata)
4. Seleziona Next (Successivo).
5. Inserisci il nome segreto: atx-db-modernization-sqlserver
6. Aggiungi i tag richiesti (questi tag sono obbligatori):
 - Chiave: progetto, valore: atx-db-modernization
 - Chiave: proprietario, valore: database-connector
7. Scegli Avanti nelle schermate rimanenti
8. Scegli Store
9. Nota l'ARN segreto da utilizzare nel passaggio successivo

Important

Le password del database devono utilizzare solo caratteri ASCII stampabili, esclusi '/', '@', '"' e gli spazi. I segreti programmati per l'eliminazione possono causare errori di trasformazione.

Fase 3: Creare i ruoli DMS richiesti

AWS Transform richiede ruoli IAM specifici per le operazioni DMS. Implementa questi ruoli utilizzando il CloudFormation modello seguente.

Note

Se il tuo AWS account ha già DMS-related ruoli esistenti, modifica questo modello per riutilizzare tali risorse anziché creare duplicati.

Crea un file denominato `dms-roles.yaml` con il seguente contenuto:

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'DMS Service Roles for AWS Transform SQL Server Modernization'

Resources:
  DMSCloudWatchLogsRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-cloudwatch-logs-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - dms.amazonaws.com
                - schema-conversion.dms.amazonaws.com
            Action: sts:AssumeRole
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

  DMSS3AccessRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: dms-s3-access-role
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
```

- dms.amazonaws.com
- schema-conversion.dms.amazonaws.com

Action: sts:AssumeRole

Policies:

- PolicyName: S3TaggedAccess

PolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Action:

- s3:GetBucketLocation
- s3:GetBucketVersioning
- s3:PutObject
- s3:PutBucketVersioning
- s3:GetObject
- s3:GetObjectVersion
- s3:ListBucket
- s3:DeleteObject

Resource: arn:aws:s3:::atx-db-modernization-*

Condition:

StringEquals:

aws:ResourceAccount: !Ref AWS::AccountId

DMSecretsManagerRole:

Type: AWS::IAM::Role

Properties:

RoleName: dms-secrets-manager-role

AssumeRolePolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Principal:

Service:

- dms.amazonaws.com
- schema-conversion.dms.amazonaws.com

Action: sts:AssumeRole

Policies:

- PolicyName: SecretsManagerTaggedAccess

PolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Action:

- secretsmanager:GetSecretValue

```
    - secretsmanager:DescribeSecret
  Resource: '*'
  Condition:
    StringEquals:
      secretsmanager:ResourceTag/Project: atx-db-modernization
      secretsmanager:ResourceTag/Owner: database-connector
```

DMSVPCRole:

```
Type: AWS::IAM::Role
Properties:
  RoleName: dms-vpc-role
  AssumeRolePolicyDocument:
    Version: '2012-10-17'
    Statement:
      - Effect: Allow
        Principal:
          Service:
            - dms.amazonaws.com
            - schema-conversion.dms.amazonaws.com
        Action: sts:AssumeRole
  ManagedPolicyArns:
    - arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole
```

DMSServerlessRole:

```
Type: AWS::IAM::ServiceLinkedRole
Properties:
  AWSServiceName: dms.amazonaws.com
  Description: 'Service Linked Role for AWS DMS Serverless'
```

Outputs:

```
DMSCloudWatchLogsRoleArn:
  Description: ARN of the DMS CloudWatch Logs Role
  Value: !GetAtt DMSCloudWatchLogsRole.Arn
DMSS3AccessRoleArn:
  Description: ARN of the DMS S3 Access Role
  Value: !GetAtt DMSS3AccessRole.Arn
DMSSecretsManagerRoleArn:
  Description: ARN of the DMS Secrets Manager Role
  Value: !GetAtt DMSSecretsManagerRole.Arn
DMSVPCRoleArn:
  Description: ARN of the DMS VPC Role
  Value: !GetAtt DMSVPCRole.Arn
Export:
  Name: !Sub ${AWS::StackName}-VPCRole
```

```
DMSServerlessRoleArn:
  Description: ARN of the DMS Serverless Role
  Value: !Sub 'arn:aws:iam::${AWS::AccountId}:role/aws-service-role/
dms.amazonaws.com/AWSServiceRoleForDMSServerless'
  Export:
    Name: !Sub ${AWS::StackName}-ServerlessRole
```

Implementa lo CloudFormation stack utilizzando la CLI: AWS

```
aws cloudformation create-stack \
  --stack-name dms-roles \
  --template-body file://dms-roles.yaml \
  --capabilities CAPABILITY_NAMED_IAM \
  --region us-east-1
```

Oppure esegui la distribuzione utilizzando la console: AWS

1. Passa a CloudFormation nella console AWS
2. Scegli Crea pila
3. Seleziona Carica un file modello
4. Carica il file dms-roles.yaml
5. Inserisci il nome dello stack: dms-roles
6. Riconosci le funzionalità IAM
7. Scegli Create stack

Fase 4: Configurazione della sicurezza di rete

Garantisci la corretta connettività di rete tra AWS Transform, il database SQL Server e altri AWS servizi.

Configurazione del gruppo di sicurezza (approccio consigliato)

Approccio consigliato: utilizza il controllo degli accessi basato sui gruppi di sicurezza anziché sulle IP-based regole. Ciò offre una maggiore sicurezza, una gestione più semplice e si integra perfettamente con l'architettura di AWS Transform.

Perché Security Group-Based Access Control?

- La conversione dello schema DMS crea interfacce di rete elastiche (ENI) all'interno del tuo VPC

- Non è necessario che i database siano accessibili al pubblico
- AWS Transform non espone indirizzi IP privati, il che rende IP-based le regole complesse
- I riferimenti ai gruppi di sicurezza forniscono aggiornamenti dinamici e automatici man mano che le risorse scalano

Configura il tuo gruppo di sicurezza di SQL Server

Quando si configura il profilo dell'istanza di conversione dello schema DMS in AWS Transform, si specifica un gruppo di sicurezza per l'istanza DMS SC. Il gruppo di sicurezza del database deve consentire il traffico in entrata da questo gruppo di sicurezza DMS SC.

Step-by-step configurazione:

1. Identifica il gruppo di sicurezza DMS Schema Conversion:
 - Questo viene specificato durante la creazione del profilo di istanza in Transform AWS
 - Nota l'ID del gruppo di sicurezza (ad esempio, sg-0123456789abcdef0)
2. Aggiorna le regole in entrata del tuo SQL Server Security Group:
 - Tipo: TCP personalizzato
 - Porta: 1433 (o la porta SQL Server personalizzata)
 - Fonte: ID del gruppo di sicurezza di DMS Schema Conversion
 - Descrizione: «Consenti l'accesso alla conversione dello schema DMS»
3. Per il target Aurora PostgreSQL (dopo la creazione):
 - Tipo: PostgreSQL
 - Porta: 5432 (o la tua porta PostgreSQL personalizzata)
 - Fonte: ID del gruppo di sicurezza di DMS Schema Conversion
 - Descrizione: «Consenti l'accesso alla conversione dello schema DMS»

Important

Importante per i modelli di sicurezza con privilegi minimi: se l'organizzazione utilizza un modello di sicurezza «meno privilegiato» che blocca tutto il traffico per impostazione predefinita, è necessario consentire esplicitamente il traffico in entrata dal DMS Schema Conversion Security Group alla porta del database. Non aprire la porta 1433 a tutte le sorgenti o intervalli IP.

Richiesto AWS connettività servizio

Assicurati che il tuo VPC possa comunicare con:

- AWS Trasforma gli endpoint del servizio
- AWS DMS endpoint
- Endpoint Aurora PostgreSQL
- Endpoint S3 per lo storage di artefatti
- AWS Secrets Manager endpoint
- AWS CodeConnections punti finali

Endpoint VPC: per le reti private, configura gli endpoint VPC per i AWS servizi richiesti per evitare le dipendenze dei gateway Internet.

Requisiti per i database ospitati esternamente

Se il database SQL Server è ospitato all'esterno AWS, assicurati che siano soddisfatti i seguenti prerequisiti, quindi completa i passaggi di configurazione prima di iniziare la modernizzazione.

Prerequisiti

- Un AWS account con un VPC
- Connettività di rete tra il VPC e il database esterno. Per informazioni sulla configurazione della connettività di rete, vedere [Configurazione della connettività di rete](#) nella Guida per l' AWS DMS utente.

Fasi di configurazione

1. Crea un accesso segreto AWS Secrets Manager con i dettagli di connessione per il database esterno. Per ulteriori informazioni, consulta [the section called “Passaggio 2: Archivia le credenziali in AWS Secrets Manager”](#).
2. Quando richiesto, fornisci l'ID VPC e l'ID del gruppo di sicurezza per la connessione al database esterno. AWS Transform richiede queste informazioni perché il nome host del database nel segreto non può essere risolto all'interno dell'account. AWS

AWS Configurazione della trasformazione

Inizia il tuo percorso di modernizzazione accedendo alla console AWS Transform e avviando un nuovo progetto di modernizzazione. Questo passaggio definisce lo spazio di lavoro e imposta la configurazione di base per la trasformazione completa.

Azioni da completare:

- Accedere al servizio AWS Transform nella console AWS di gestione
- Seleziona Microsoft Modernization dalle opzioni di servizio
- Scegli Crea un nuovo progetto di modernizzazione
- Fornisci il nome e la descrizione del progetto
- Seleziona la AWS regione di destinazione (deve corrispondere alla tua posizione di SQL Server)
- Rivedi e conferma le impostazioni del progetto

Note

Procedura ottimale: utilizzate nomi di progetto descrittivi che includano il nome dell'applicazione e l'ambiente di destinazione (ad esempio, 'CustomerPortal-Production-Modernization') per identificare facilmente i progetti in scenari a più ondate.

Crea un processo di modernizzazione di SQL Server

Connect database e repository del codice sorgente

Configura il connettore del database

Stabilisci una connettività sicura ai tuoi database SQL Server configurando i connettori di database. Il connettore esegue l'analisi dell'ambiente, l'individuazione delle dipendenze e consente a AWS Transform di accedere agli schemi e ai metadati del database per la valutazione e la conversione.

Azioni da completare:

- Seleziona Configure Database Connector dalla procedura guidata di configurazione
- Scegli il metodo di connessione: Nuova connessione o Connessione esistente

- Fornisci i dettagli della connessione a SQL Server (endpoint, porta, nomi di database)
- Configura l'autenticazione e verifica la connettività
- Rivedi i database scoperti e conferma la selezione

Note

Connettività di rete: assicurati che i gruppi di sicurezza e i NAC di SQL Server consentano le connessioni in entrata dagli endpoint del servizio AWS Transform.

Connect al repository del codice sorgente

Abilita AWS Transform per accedere al codice sorgente dell'applicazione.NET. AWS Transform supporta tre metodi per fornire il codice sorgente: un connettore PAT (Personal Access Token) (consigliato) o Amazon S3. AWS CodeConnections Questa integrazione consente al servizio di analizzare il codice dell'applicazione, identificare le dipendenze del database ed eseguire trasformazioni automatiche del codice per la compatibilità con PostgreSQL.

Azioni da completare:

- Vai alla sezione Connect Source Code Repository
- Scegli il metodo di autenticazione: connettore PAT (consigliato) o Amazon S3 AWS CodeConnections
- Seleziona i repository contenenti applicazioni.NET
- Specificate il ramo per l'analisi (in genere main/master o per lo sviluppo)
- Convalida l'accesso al repository e la struttura del codice

Note

Repository Discovery: AWS Transform analizza automaticamente i repository per identificare progetti.NET, configurazioni di Entity Framework, stringhe di connessione al database e dipendenze SQL.

 Note

Nota sulla sicurezza: AWS Transform richiede solo l'accesso in lettura ai repository e crea nuovi rami di funzionalità per il codice trasformato. La tua filiale principale rimane intatta.

Un essere umano al centro

AWS Transform utilizza meccanismi human-in-the-loop (HITL) per garantire la qualità e consentire di rivedere e approvare le decisioni critiche relative alla trasformazione. I seguenti punti di controllo richiedono la tua attenzione:

Revisione e approvazione del piano Wave

Cosa recensite: le ondate di migrazione proposte, compresi i database e le applicazioni raggruppati e la sequenza delle ondate.

Puoi:

- Approva il piano delle ondate
- Personalizza le onde spostando i database tra le onde
- Modifica la sequenza d'onda
- Dividi o unisci le onde

Dopo l'approvazione, AWS Transform procede con la conversione dello schema.

Revisione della conversione dello schema

Cosa esaminate: oggetti di database convertiti tra cui tabelle, stored procedure, funzioni e trigger. Le azioni evidenziano gli oggetti che richiedono attenzione.

Puoi:

- Accetta il codice convertito
- Modifica il codice convertito
- Contrassegno per la revisione umana dopo la trasformazione
- Visualizza il confronto fianco a fianco tra il codice originale e quello convertito

Cosa succede dopo l'approvazione: AWS Transform applica lo schema ad Aurora PostgreSQL e procede con la migrazione dei dati (se configurata).

Revisione del codice dell'applicazione

Cosa esaminate: tutte le modifiche al codice dell'applicazione, incluse le configurazioni di Entity Framework, le stringhe di connessione, il codice di accesso ai dati e le chiamate di stored procedure.

Puoi:

- Accetta le modifiche per ogni file
- Modifica il codice trasformato
- Rifiuta le modifiche (scelta non consigliata)
- Aggiungi commenti per il tuo team
- Scarica il codice trasformato per la revisione locale

Cosa succede dopo l'approvazione: AWS Transform trasferisce le modifiche in una nuova filiale del repository e procede con la convalida.

Revisione dei risultati della convalida

Cosa esaminate: risultati di convalida automatizzati, tra cui compatibilità dello schema, controlli di integrità dei dati e stato di creazione dell'applicazione.

Puoi:

- Rivedi i test superati
- Esamina i test falliti
- Indirizza gli avvisi
- Procedi alla distribuzione o torna per risolvere i problemi

Cosa succede dopo l'approvazione: AWS Transform si prepara per l'implementazione nell'ambiente di destinazione.

Approvazione della distribuzione

Cosa esamini: configurazione della distribuzione, inclusi modelli infrastructure-as-code, configurazione del servizio ECS e impostazioni di distribuzione.

Puoi:

- Rivedi e personalizza le impostazioni di distribuzione
- Approva la distribuzione per procedere
- Ritarda la distribuzione per ulteriori test
- Scarica il codice dell'infrastruttura per la revisione

Dopo l'approvazione, AWS Transform distribuisce l'applicazione e il database modernizzati nell'ambiente di destinazione.

Valutazione e pianificazione delle ondate

Configura la landing zone

Configura l'ambiente dell'infrastruttura di destinazione in cui verranno distribuite le applicazioni modernizzate. La configurazione della landing zone include il provisioning di Aurora PostgreSQL, la configurazione di rete e le configurazioni di distribuzione di riferimento.

Azioni da completare:

- Seleziona Configura la zona di atterraggio dal menu di configurazione
- Configurare il target Aurora PostgreSQL (versione, classe di istanza,) Multi-AZ
- Configurazione delle impostazioni di rete e sicurezza (VPC, sottoreti, gruppi di sicurezza)

Note

Considerazione dei costi: le istanze Aurora PostgreSQL comportano costi continui. Prendi in considerazione l'utilizzo di Aurora Serverless v2 per gli ambienti. development/testing

Valutazione

Conduci un'analisi completa degli schemi del database, del codice dell'applicazione e delle dipendenze. La fase di valutazione fornisce valutazioni della complessità della trasformazione, identifica le potenziali sfide e genera report dettagliati.

Azioni da completare:

- Seleziona Repository Branch per l'analisi del codice
- Seleziona Repository e database per la trasformazione
- Rivedi i risultati della valutazione e le valutazioni di complessità
- Genera un rapporto di valutazione con proiezioni degli sforzi
- Esporta il rapporto per la revisione e l'approvazione degli stakeholder

Note

Approfondimenti sulla valutazione: la valutazione fornisce un'analisi dettagliata degli oggetti dello schema, delle stored procedure, delle dipendenze delle applicazioni e stima il livello di intervento umano richiesto.

Pianificazione delle ondate

Organizza la modernizzazione in fasi gestibili basate sulla complessità della trasformazione, sulle priorità aziendali e sulle dipendenze delle applicazioni. AWS Transform genera raccomandazioni intelligenti che puoi personalizzare.

Azioni da completare:

- Rivedi il piano AI-Generated Wave e i consigli
- Personalizza la configurazione di Wave in base alle priorità aziendali
- Convalida le dipendenze tra applicazioni e database
- Finalizza Wave Plan utilizzando l'interfaccia conversazionale
- Stabilisci le priorità di esecuzione delle ondate e assegna le responsabilità

Note

AI-Powered Consigli: puoi interagire con l'intelligenza artificiale tramite il linguaggio naturale per adattare i consigli: «Sposta CustomerDB alla Wave 1" o «Combina queste due applicazioni nella stessa ondata».

 Note

Best practice: inizia con un'ondata pilota contenente 1-2 database a bassa complessità per stabilire processi e aumentare la fiducia del team.

Migrazione dei dati per ogni ondata

Conversione dello schema per ogni ondata

Trasforma gli schemi di database di SQL Server in PostgreSQL-compatible equivalenti utilizzando le funzionalità di AI-enhanced conversione. Questo processo converte tabelle, stored procedure, funzioni, trigger e altri oggetti di database.

Azioni da completare:

- Fornire obiettivi di conversione dello schema e configurare le preferenze
- Esegui la conversione automatizzata utilizzando il servizio DMS Schema Conversion
- Rivedi i risultati della conversione e identifica gli elementi di intervento umano
- Gestisci gli interventi manuali tramite istruzioni HITL
- Convalida le correzioni umane ed esegui nuovamente la conversione se necessario

 Note

Interventi manuali comuni: i server collegati, i tipi definiti dall'utente, i T-SQL modelli avanzati e le funzionalità SQL specifiche del fornitore richiedono in genere la revisione e la correzione da parte di un operatore.

Migrazione dei dati per ogni ondata

Trasferisci dati da SQL Server ad Aurora PostgreSQL utilizzando l'integrazione (). AWS Database Migration Service AWS DMS Scegli tra la migrazione dei dati di produzione o la generazione di dati sintetici a scopo di test.

Azioni da completare:

- Scegli la migrazione dei dati di produzione o la generazione di dati sintetici

- Configura l'istanza di replica DMS per il trasferimento dei dati
- Monitora l'avanzamento della migrazione e gestisci le incoerenze dei dati
- Convalida l'integrità dei dati e i vincoli referenziali
- Conferma il completamento con successo prima di procedere

Note

Integrazione DMS automatizzata: AWS Transform astrae la complessità della configurazione DMS, gestendo automaticamente la creazione degli endpoint, la configurazione delle attività e le mappature dei tipi di dati.

Note

Convalida dei dati: il servizio esegue test empirici eseguendo query identiche sui database di origine e di destinazione per garantire la coerenza dei dati.

Migrazione del codice per ogni ondata

Trasforma il codice dell'applicazione.NET per utilizzarlo con Aurora PostgreSQL, inclusi gli aggiornamenti della configurazione di Entity Framework, le modifiche delle stringhe di connessione, gli adattamenti delle query SQL e le regolazioni specifiche del framework.

Azioni da completare:

- Esegui l'analisi automatizzata del codice per le dipendenze di SQL Server
- Esegui la trasformazione del framework (aggiornamenti del provider Entity Framework)
- Adatta la sintassi di SQL Query a PostgreSQL-compatible SQL
- Configura Target Branch Management per il codice trasformato
- Gestisci gli interventi manuali per modelli complessi

Flusso di lavoro di modernizzazione di SQL Server

Questa sezione fornisce una guida dettagliata dell'intero processo di modernizzazione di SQL Server utilizzando Transform. AWS

Fase 1: Creare un processo di modernizzazione di SQL Server

Inizia il tuo percorso di modernizzazione creando un nuovo processo di trasformazione nella console AWS Transform.

1. Accedi alla console AWS Transform
2. Scegli Create modernization job
3. Seleziona il processo di modernizzazione di Windows, quindi seleziona Modernizzazione di SQL Server
4. Inserisci i dettagli del lavoro:
 - Job name: nome descrittivo per il tuo progetto
 - Descrizione: descrizione opzionale
 - Regione di destinazione: AWS regione per la distribuzione
5. Selezionare Create job (Crea attività).

Important

Non includere informazioni di identificazione personale (PII) nel nome del lavoro.

Passaggio 2: Connect al database SQL Server

Connect AWS Transform al database SQL Server per abilitare l'analisi e la conversione dello schema.

Crea un connettore per il database

1. Nel processo di modernizzazione di SQL Server, accedi a Connect to resources
2. Scegli Connetti al database SQL Server
3. Scegli Crea nuovo connettore
4. Inserisci le informazioni sul connettore:
 - Nome del connettore C: nome descrittivo
 - AWS ID account: account in cui è ospitato SQL Server
5. Una volta confermato, riceverai un link per l'approvazione. Copia il link di approvazione per ottenere l'approvazione dell'account dall' AWS amministratore. Una volta approvati, puoi procedere al passaggio successivo.

6. Dopo che l'amministratore ha approvato la richiesta del connettore, fate clic su **Invia** per procedere alla configurazione della connessione con il codice sorgente.

Passaggio 3: Connect il repository del codice sorgente

AWS Transform richiede l'accesso al codice sorgente dell'applicazione.NET per analizzare e trasformare il codice che interagisce con il database SQL Server. AWS Transform supporta tre metodi per fornire il codice sorgente.

Scegli il tuo metodo di autenticazione

Connettore PAT (Personal Access Token) (consigliato)

Ideale per i team che necessitano di ambiti di autorizzazione personalizzati, supporto da parte di provider ospitati autonomamente o accesso a API specifiche del provider come Secrets. GitHub Crei un PAT nel tuo provider di codice sorgente con autorizzazioni personalizzate, lo memorizzi e Transform lo recupera AWS Secrets Manager quando necessario. AWS Sei responsabile della gestione della rotazione e della scadenza dei token.

AWS CodeConnections

Ideale per i team che desiderano una gestione automatizzata delle credenziali. AWS CodeConnections utilizza un'integrazione con provider gestiti che gestisce l'autenticazione tramite un flusso di autorizzazione OAuth 2.0. AWS gestisce l'intero ciclo di vita delle credenziali, incluso l'aggiornamento e la rotazione automatici dei token. Non è richiesta la gestione manuale delle credenziali.

Simple Storage Service (Amazon S3)

Carica il codice sorgente direttamente in un bucket Amazon S3. AWS Transform accede al codice dal bucket durante il processo di trasformazione.

Funzionalità	Connettore PAT (consigliato)	AWS CodeConnections
Gestione delle credenziali	Manuale (gestito dal cliente)	Automatico (gestito)AWS
Ciclo di vita dei token	È richiesta una rotazione manuale	Aggiornamento automatico

Funzionalità	Connettore PAT (consigliato)	AWS CodeConnections
Flessibilità di autorizzazione	Ambiti completamente personalizzabili	Autorizzazioni fisse
Self-hosted supporto per i fornitori	Supportata	Non disponibile
Complessità di configurazione	Moderato (creazione e archiviazione manuali dei token)	Bassa (autorizzazione una tantum)
Archiviazione di token	Del cliente AWS Secrets Manager	Gestito da AWS

Configurare un connettore PAT (consigliato)

Con un connettore PAT, crei un token di accesso personale nel tuo provider di codice sorgente con autorizzazioni personalizzate, lo memorizzi in AWS Secrets Manager modo sicuro e AWS Transform lo recupera quando necessario. Sei responsabile della gestione del ciclo di vita del token, comprese la rotazione e la scadenza. AWS Transform crea automaticamente il ruolo IAM necessario con le autorizzazioni per accedere al tuo segreto.

Il connettore PAT supporta i seguenti provider, comprese le versioni self-hosted e personalizzate: DNS/URL

- GitHub e GitHub Enterprise Server
- GitLab.com e GitLab Self-Managed
- Bitbucket Cloud e Bitbucket Data Center
- Azure e Azure Server DevOps DevOps

Crea un token di accesso personale

Crea un PAT nel tuo provider di codice sorgente. Le autorizzazioni richieste variano in base al provider. Scegli la scheda relativa al tuo provider.

⚠ Important

Copia il token subito dopo la creazione. Non è possibile visualizzarlo di nuovo. Imposta la scadenza per la durata del processo di trasformazione. Non impostate la scadenza in modo che non scada mai.

⚠ Warning

Non archiviate mai i token PAT in archivi di codice né condivideteli attraverso canali non sicuri. Conservali sempre in AWS Secrets Manager

GitHub

Vai a Impostazioni, Impostazioni sviluppatore, Token di accesso personali, Fine-grained token. Seleziona i repository da trasformare e concedi le seguenti autorizzazioni.

Autorizzazioni per il repository

Autorizzazione	Accesso	Scopo
Indice	Leggi e scrivi	Legge il codice sorgente e riscrive il codice trasformato nel repository
Metadati	Read-only	Accede alle informazioni di base del repository

Autorizzazioni organizzative (richieste per gli archivi dell'organizzazione)

Autorizzazione	Accesso	Scopo
Membri	Read-only	Elenca le organizzazioni accessibili al token per l'individuazione dei repository

GitLab

Vai a Modifica profilo, Accedi ai token. Seleziona i seguenti ambiti.

Scope	Scopo
<code>read_api</code>	Legge i metadati del repository, le informazioni sul progetto, i dettagli degli utenti ed elenca gruppi e rami
<code>read_repository</code>	Legge i file del codice sorgente e la struttura del repository per l'analisi
<code>write_repository</code>	Scriva il codice trasformato nel repository

Bitbucket

Vai a Impostazioni account, Sicurezza, Crea e gestisci token API. Gli ambiti richiesti dipendono dal tipo di token.

Workspace/Repository Token (ATCT — Bearer auth, nessun nome utente richiesto)

Autorizzazione	Accesso	Scopo
Repositories	Leggi e scrivi	Elenca i repository, legge i rami e scrive codice trasformato tramite git push

Account API Token (ATAT — Autenticazione di base con e-mail) o password dell'app (ATBB — Autenticazione di base con nome utente)

Scope	Scopo
<code>read:account</code>	Identifica l'utente autenticato per risolvere l'appartenenza al repository
<code>read:workspace:bitbucket</code>	Elenca le aree di lavoro a cui il token può accedere in modo che AWS Transform possa enumerare i relativi repository. Non richiesto se si specifica un elenco di aree di lavoro nel segreto.
<code>read:repository:bitbucket</code>	Elenca gli archivi e legge i metadati e le informazioni sulle filiali

Scope	Scopo
<code>write:repository:bitbucket</code>	Scrivi il codice trasformato nel repository tramite git push

Azure DevOps

Vai a Impostazioni utente, Token di accesso personali. Seleziona Ambiti definiti su misura. Per l'ambito dell'organizzazione, scegli Tutte le organizzazioni accessibili (consigliato) o specifica una singola organizzazione.

Scope	Accesso	Scopo
Codice	Leggi e scrivi	Legge il codice sorgente, elenca repository e branch e riscrive il codice trasformato
Profilo utente	Lettura	Convalida l'accesso ai token e scopre l'identità dell'utente per la ricerca nell'organizzazione
Gestione dei diritti dei membri	Lettura	Elenca le organizzazioni accessibili al token per l'individuazione del repository

Memorizza il PAT in AWS Secrets Manager

1. Apri la AWS Secrets Manager console.
2. Scegli Archivia un nuovo segreto.
3. Per Secret type (Tipo di segreto), scegli Other type of secret (Altro tipo di segreto).
4. Aggiungi coppie chiave-valore in base al provider e al tipo di hosting:
 - Cloud-hosted provider: aggiungi una chiave denominata token con il tuo PAT come valore.
 - Per Azure DevOps con un'organizzazione specifica, aggiungi anche una chiave denominata organization con il nome della tua organizzazione.
 - Per le password delle app Bitbucket (ATBB), aggiungi anche una chiave denominata con il tuo nome username utente Bitbucket. Per i token API dell'account Bitbucket (ATAT), aggiungi una chiave denominata con il tuo indirizzo email Bitbucket. email

- Self-hosted e DNS/URL provider personalizzati: aggiungi le seguenti chiavi: `host` (l'URL del tuo server, ad esempio `https://github.mycompany.com`), `provider_type` (`github`, `gitlab`, `bitbucket`, o) e (il tuo PAT o) `token`.
- Per Azure DevOps con un'organizzazione specifica, aggiungi anche una chiave denominata `organization` con il nome della tua organizzazione.
- Per le password delle app Bitbucket (ATBB), aggiungi anche una chiave denominata con il tuo nome `username` utente Bitbucket. Per i token API dell'account Bitbucket (ATAT), aggiungi una chiave denominata con il tuo indirizzo email Bitbucket. `email`.

L'esempio seguente mostra come viene visualizzato un segreto per un provider ospitato nel cloud: AWS Secrets Manager GitHub

```
{
  "token": "your-github-personal-access-token"
}
```

L'esempio seguente mostra una password per l'app Bitbucket (ATBB):

```
{
  "token": "your-bitbucket-app-password",
  "username": "my-bitbucket-username"
}
```

L'esempio seguente mostra un'istanza ospitata autonomamente: GitLab

```
{
  "host": "https://gitlab.mycompany.com",
  "provider_type": "gitlab",
  "token": "your-gitlab-personal-access-token"
}
```

5. Scegli Next (Successivo).
6. Inserisci un nome segreto, ad esempio `github-pat-myproject`.
7. (Facoltativo) Seleziona una chiave KMS gestita dal cliente per la crittografia.
8. Completa la procedura guidata e scegli Store.
9. Copia l'ARN segreto. È necessario questo valore quando si configura il processo di AWS trasformazione.

Se utilizzi una chiave KMS gestita dal cliente per crittografare il tuo segreto (anziché la chiave AWS gestita predefinita), devi aggiornare la politica della chiave KMS per consentire AWS a Transform di decrittografare il segreto. Aggiungi la seguente dichiarazione alla politica delle chiavi KMS gestita dal cliente:

```
{
  "Sid": "Allow AWS Transform to decrypt secrets",
  "Effect": "Allow",
  "Principal": {
    "Service": "transform.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "secretsmanager.REGION.amazonaws.com",
      "kms:EncryptionContext:SecretARN": "YOUR-SECRET-ARN"
    }
  }
}
```

Sostituisci *REGION* con la tua AWS regione (ad esempio *us-east-1*) e *YOUR-SECRET-ARN* con l'ARN del tuo segreto. La `kms:ViaService` condizione garantisce che la chiave KMS possa essere utilizzata solo tramite il AWS Secrets Manager servizio. La `kms:EncryptionContext:SecretARN` condizione limita la decrittografia al tuo segreto specifico.

Per aggiornare la tua politica sulle chiavi KMS:

1. Apri la console AWS KMS all'indirizzo. <https://console.aws.amazon.com/kms>
2. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
3. Seleziona la tua chiave KMS.
4. Nella scheda Policy della chiave, seleziona Modifica.
5. Aggiungi la dichiarazione sulla politica alla politica esistente.
6. Scegli Save changes (Salva modifiche).

 Note

Se si utilizza la chiave predefinita AWS-managed (aws/secretsmanager), non è necessario modificare alcuna politica delle chiavi KMS.

Configura il AWS Trasforma il lavoro

1. Nel processo AWS Transform, accedi a Connect to resources.
2. Scegli Connect source code repository.
3. Seleziona PAT Connector come metodo di autenticazione.
4. Inserisci l'ARN segreto dal passaggio 2.
5. (Facoltativo) Inserisci l'ARN della chiave KMS se hai utilizzato una chiave KMS gestita dal cliente.
6. Seleziona il tuo repository e la filiale.
7. Scegli Continua.

AWS Transform crea automaticamente un ruolo IAM con le autorizzazioni necessarie per accedere al tuo segreto.

Rotazione e manutenzione dei token

Sei responsabile della rotazione dei token PAT prima che scadano. Per ruotare un token:

1. Genera un nuovo PAT nel tuo provider di codice sorgente con le stesse autorizzazioni.
2. Aggiorna il valore segreto in. AWS Secrets Manager
3. Verifica che il tuo job AWS Transform possa accedere al repository con il nuovo token.
4. Revoca il vecchio PAT nel tuo provider di codice sorgente.

Risolvi i problemi relativi al connettore PAT

Accesso negato: PAT non valido

Verifica che il PAT non sia scaduto. Verifica che il PAT abbia gli ambiti richiesti per il tuo provider. Verificate che il PAT sia memorizzato correttamente in. AWS Secrets Manager

Impossibile recuperare il segreto

Verifica che l'ARN segreto sia corretto. Controlla i log dei lavori per confermare che AWS Transform ha creato il ruolo IAM. Se utilizzi una chiave KMS gestita dal cliente, verifica la policy chiave.

Autorizzazioni insufficienti

Il PAT potrebbe non avere gli ambiti richiesti per l'operazione. Rigenera il PAT con gli ambiti richiesti e aggiorna il valore segreto in AWS Secrets Manager.

Configurazione AWS CodeConnections

AWS CodeConnections utilizza un'integrazione con provider gestiti che recupera automaticamente le credenziali OAuth temporanee tramite un flusso di autorizzazione OAuth 2.0. Le autorizzazioni sono configurate nell'app del provider e gestite interamente da AWS. Autorizzi l'app una sola volta e AWS gestisce tutta la gestione delle credenziali.

1. Nel processo di modernizzazione di SQL Server, accedi a Connect to resources.
2. Scegli Connect source code repository.
3. Se non disponi di una connessione esistente, scegli Crea connessione.
4. Seleziona il fornitore del tuo repository:
 - GitHub /Impresa GitHub
 - GitLab.com
 - Bitbucket Cloud
 - Repository di Azure
5. Segui il flusso di autorizzazione per il tuo provider.
6. Dopo l'autorizzazione, scegli Connect.

Seleziona il tuo repository e la tua filiale

1. Seleziona il tuo repository dall'elenco.
2. Scegli il ramo che vuoi trasformare (in genere principale, master o development).
3. (Facoltativo) Specificate una sottodirectory se l'applicazione.NET non si trova nella radice del repository.
4. Scegli Continua.

 Note

AWS Transform crea un nuovo ramo per il codice trasformato. È possibile rivedere e unire le modifiche tramite il normale processo di revisione del codice.

Approvazione dell'accesso al repository

Per GitHub alcune altre piattaforme, l'amministratore del repository deve approvare la richiesta di connessione:

1. AWS Transform visualizza un link di verifica.
2. Condividi questo link con l'amministratore del tuo repository.
3. L'amministratore esamina e approva la richiesta nelle impostazioni del repository.
4. Dopo l'approvazione della richiesta da parte dell'amministratore, lo stato della connessione diventa Approvato.

 Important

Il processo di approvazione può richiedere del tempo a seconda delle politiche dell'organizzazione. Pianifica le attività di conseguenza.

Fase 4: Creare un connettore di distribuzione (opzionale)

Se desideri distribuire le applicazioni trasformate nel tuo AWS account, hai la possibilità di selezionare un connettore di distribuzione.

Configura il connettore di distribuzione

1. Seleziona Sì se desideri distribuire le tue applicazioni. Selezionando No si salterà questo passaggio.
2. Aggiungi il tuo AWS account dove desideri distribuire le applicazioni trasformate.
3. Aggiungi un nome che ti aiuti a ricordare facilmente il connettore
4. Invia la richiesta di approvazione del connettore.

Approvazione del connettore di distribuzione

L'amministratore AWS dell'account deve approvare la richiesta di connessione per il connettore di distribuzione.

1. AWS Transform visualizza un link di verifica
2. Condividi questo link con l'amministratore AWS del tuo account
3. L'amministratore esamina e approva la richiesta nelle impostazioni del repository
4. Una volta approvata, lo stato della connessione diventa Approvato

Important

Il processo di approvazione può richiedere del tempo a seconda delle politiche dell'organizzazione. Pianifica le attività di conseguenza.

Fase 5: Conferma le tue risorse

Dopo la connessione al database e al repository, AWS Transform verifica che tutte le risorse richieste siano accessibili e pronte per la trasformazione.

What AWS Transform verifica

- Connettività al database: la connessione è attiva, l'utente ha le autorizzazioni richieste, i database sono accessibili, la versione è supportata
- Accesso al repository: il repository è accessibile, la filiale esiste, i file di progetto.NET sono stati rilevati, le connessioni al database sono individuabili
- Predisposizione dell'ambiente: la configurazione VPC supporta DMS, esistono ruoli di servizio AWS richiesti, connettività di rete stabilita, compatibilità regionale confermata

Consulta la lista di controllo prima del volo

1. Vai a Conferma le tue risorse nel piano di lavoro
2. Controlla gli elementi della lista di controllo:
 - # Connessione al database verificata
 - # Accesso al repository confermato

- # Versione .NET supportata
 - # Entity Framework o ADO.NET rilevato
 - # Configurazione di rete valida
 - # Autorizzazioni richieste concesse
3. Se tutti gli elementi vengono visualizzati come completi, scegli Continua
 4. Se alcuni articoli mostrano avvisi o errori, risolvi prima di procedere

Fase 6: Scoperta e valutazione

AWS Transform analizza il database SQL Server e l'applicazione.NET per comprendere l'ambito e la complessità della modernizzazione.

Cosa viene scoperto

- Oggetti del database: tabelle, viste, indici, stored procedure, funzioni, trigger, vincoli, tipi di dati, colonne calcolate, colonne di identità, relazioni con chiavi esterne
- Codice dell'applicazione: struttura del progetto.NET, modelli e configurazioni di Entity Framework, codice di accesso ai ADO.NET dati, stringhe di connessione al database, chiamate di stored procedure, query SQL nel codice
- Dipendenze: quali applicazioni utilizzano determinati database, dipendenze tra database, procedure archiviate condivise, modelli comuni di accesso ai dati

Processo di scoperta

- AWS Transform avvia automaticamente l'individuazione dopo la conferma delle risorse
- L'individuazione richiede in genere 5-15 minuti a seconda delle dimensioni del database e della complessità dell'applicazione
- Monitora i progressi nel registro di lavoro
- AWS Transform mostra gli aggiornamenti in tempo reale man mano che gli oggetti vengono scoperti

Rivedi i risultati della scoperta

Una volta completata la scoperta, accedi a Discovery and assessment per esaminare:

Analisi del database:

- Numero di oggetti: numero di tabelle, viste, procedure memorizzate, funzioni, trigger
- Punteggio di complessità: valutazione della complessità della trasformazione (bassa, media, alta)
- Oggetti d'azione: oggetti che possono richiedere l'attenzione umana
- Funzionalità supportate: funzionalità del database che verranno convertite automaticamente
- Funzionalità non supportate: funzionalità che richiedono soluzioni alternative

Analisi delle applicazioni:

- Tipo di progetto: ASP.NET Core, Console App, Class Library, ecc.
- Versione.NET: versione .NET Core rilevata
- Framework di accesso ai dati: versione Entity Framework o ADO.NET
- Connessioni al database: numero di stringhe di connessione trovate
- Complessità del codice: valutazione della complessità della trasformazione

Mappa delle dipendenze:

- Rappresentazione visiva delle relazioni tra applicazioni e database
- Cross-database dipendenze
- componenti condivisi

Comprendere la valutazione della complessità

AWS Transform classifica la modernizzazione in tre categorie:

Complessità	Caratteristiche	Risultato previsto
Basso (classe A)	Modelli SQL standard (ANSI SQL), procedure memorizzate semplici, tipi di dati di base, Entity Framework con configurazioni standard	Intervento umano minimo previsto, elevata percentuale di successo nell'automazione
Medio (classe B)	T-SQL Modelli avanzati, procedure memorizzate complesse con logica	È richiesto un intervento umano, si consiglia la revisione di un esperto

Complessità	Caratteristiche	Risultato previsto
	aziendale, funzioni definite dall'utente, colonne calcolate	
Alta (classe C)	Assemblaggi CLR, server collegati, Service Broker, ricerca complessa in tutto il testo	È necessario un significativo refactoring umano, si consideri un approccio graduale

Report di valutazione

AWS Transform genera un rapporto di valutazione dettagliato che include:

- Riepilogo esecutivo con panoramica di alto livello
- Inventario completo del database
- Inventario delle applicazioni
- Percentuale di preparazione alla trasformazione
- Stima dello sforzo
- Strategie di valutazione e mitigazione del rischio
- Approccio consigliato

Puoi scaricare il rapporto di valutazione per la revisione offline e la condivisione con le parti interessate.

Fase 7: Generazione e revisione del piano ondulatorio

Per aree di grandi dimensioni con più database e applicazioni, AWS Transform genera un piano d'ondata che sequenzia la modernizzazione in gruppi logici.

Cos'è un piano d'onda?

Un piano ondulatorio organizza la modernizzazione in fasi (ondate) basate su:

- Dipendenze tra database e applicazioni
- Priorità aziendali
- Tolleranza al rischio

- Disponibilità delle risorse
- Complessità tecnica

Ogni ondata contiene un gruppo di database e applicazioni che possono essere modernizzati insieme senza interrompere le dipendenze.

Rivedi il piano d'ondata

1. Vai alla pianificazione Wave nel piano di lavoro
2. Esamina le ondate proposte
3. Per ogni ondata, rivedi:
 - Database inclusi
 - Applicazioni incluse
 - Dipendenze da altre onde
 - Tempo di trasformazione stimato
 - Livello di complessità
 - Applicazioni implementabili

Personalizza il piano d'ondata

Puoi personalizzare il piano tariffario per adattarlo alle tue esigenze aziendali in 2 modi:

Utilizzando JSON:

1. Scegli Scarica tutte le onde per ottenere un file JSON con tutte le onde
2. Modifica le onde in JSON tramite:
 - Spostamento dei database tra le ondate
 - Suddivisione delle onde in gruppi più piccoli
 - Unire le onde
 - Modifica della sequenza d'onda
 - Aggiungere o rimuovere database dall'ambito
3. Carica nuovamente il file JSON sulla console scegliendo Upload wave plan
4. AWS Transform convalida le modifiche e avvisa se le dipendenze vengono violate
5. Scegli Confirm waves per aggiornare il piano d'ondata

Usare la chat:

Puoi modificare i piani d'onda chattando con l'agente e chiedendogli di spostare i repository e i database su ondate specifiche. Questo approccio funziona bene se è necessario apportare modifiche minori alle onde.

Important

Assicurati che le dipendenze siano rispettate durante la personalizzazione delle onde. La trasformazione di un'applicazione dipendente prima del relativo database può causare problemi.

Modernizzazione di un singolo database

Se stai modernizzando un singolo database e un'unica applicazione, AWS Transform crea un piano semplice in un'unica fase. Puoi procedere direttamente alla trasformazione senza una pianificazione ondata.

Approva il piano ondulatorio

1. Dopo aver esaminato e personalizzato (se necessario), scegli Approva il piano ondulatorio
2. AWS Transform blocca il piano d'onda e procede alla trasformazione
3. Puoi comunque modificare il piano in un secondo momento scegliendo Modifica piano ondulatorio

Fase 8: Conversione dello schema

AWS Transform converte lo schema del database SQL Server in Aurora PostgreSQL, incluse tabelle, viste, stored procedure, funzioni e trigger.

Come funziona la conversione dello schema

AWS Transform utilizza la conversione dello schema AWS DMS migliorata con l'intelligenza artificiale generativa per:

- Analizza gli schemi e le relazioni di SQL Server
- Mappa i tipi di dati da SQL Server agli equivalenti di PostgreSQL
- Trasforma in T-SQL PL/pgSQL

- Gestisci colonne di identità, colonne calcolate e vincoli
- Convalida la conversione e l'integrità referenziale
- Genera azioni per oggetti che richiedono la revisione umana

Conversioni supportate

Convertito automaticamente:

- Tabelle, viste e indici
- Chiavi primarie e chiavi esterne
- Controlla i vincoli e i valori predefiniti
- I tipi di dati più comuni
- Procedure memorizzate semplici
- Funzioni e trigger di base
- Colonne di identità (convertite in SERIAL o GENERATED)
- Colonne più calcolate

Potrebbe richiedere una revisione umana:

- Procedure memorizzate complesse con funzionalità avanzate T-SQL
- Server-specific Funzioni SQL (GETUTCDATE, SUSER_SNAME, ecc.)
- Colonne calcolate con espressioni complesse
- Full-text indici di ricerca
- operazioni sui tipi di dati XML
- Tipo di dati HIERARCHYID (richiede l'estensione Itree)

Non convertito automaticamente:

- assiemi CLR
- Server collegati
- Service Broker
- Lavori di SQL Server Agent

Avvia la conversione dello schema

1. Vai alla conversione dello schema nel piano di lavoro
2. Rivedi le impostazioni di conversione:
 - Versione Target PostgreSQL
 - Opzioni di estensione (ltree, PostGIS, ecc.)
 - Convenzioni di denominazione
3. Scegli Avvia conversione
4. Monitora i progressi nel registro di lavoro
5. La conversione richiede in genere 10-30 minuti a seconda del numero di oggetti del database

Rivedi i risultati della conversione

Al termine della conversione, vai a Rivedi la conversione dello schema:

Riepilogo della conversione:

- Oggetti convertiti: numero di oggetti convertiti con successo
- Oggetti d'azione: oggetti che richiedono l'attenzione umana
- Avvertenze: potenziali problemi da esaminare
- Errori: oggetti che non possono essere convertiti

Revisione per tipo di oggetto:

- Tabelle: mappature dei tipi di dati, vincoli, indici
- T-SQL PL/pgSQL Procedure memorizzate: alla conversione
- Funzioni: firma delle funzioni e modifiche logiche
- Trigger: attiva modifiche alla sintassi e alla tempistica

Rivedi gli elementi di azione

1. Scegli Visualizza azioni
2. Per ogni azione, esamina:
 - Nome dell'oggetto: l'oggetto del database

- Tipo di problema: cosa richiede attenzione
- Gravità: Critico, Avviso o Informazioni
- Raccomandazione: risoluzione consigliata
- Codice originale: versione SQL Server
- Codice convertito: versione PostgreSQL

3. Per ogni azione, puoi:

- Accetta: utilizza il codice convertito
- Modifica: modifica il codice convertito
- Contrassegna per dopo: Contrassegna per la revisione umana dopo la trasformazione

Esempio: conversione della procedura memorizzata

SQL Server T-SQL:

```
CREATE PROCEDURE GetProductsByCategory
    @CategoryId INT,
    @PageSize INT = 10
AS
BEGIN
    SET NOCOUNT ON;

    SELECT TOP (@PageSize)
        ProductId,
        Name,
        Price,
        DATEDIFF(DAY, CreatedDate, GETUTCDATE()) AS DaysOld
    FROM Products
    WHERE CategoryId = @CategoryId
    ORDER BY Name
END
```

PostgreSQL PL/pgSQL convertito:

```
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;
```

Modifiche apportate:

- Procedura convertita in funzione che restituisce TABLE
- Nomi dei parametri preceduti da p_
- TOP convertito in LIMIT
- DATEDIFF convertito in EXTRACT
- GETUTCDATE () convertito in NOW ()
- Nomi di colonna convertiti in lettere minuscole (convenzione PostgreSQL)

Approva la conversione dello schema

1. Dopo aver esaminato tutte le azioni e aver apportato le modifiche necessarie
2. Scegli Approva la conversione dello schema
3. AWS Transform prepara lo schema convertito per la distribuzione in Aurora PostgreSQL

Note

È possibile scaricare lo schema convertito come script SQL per la revisione offline o il controllo della versione.

Fase 9: Migrazione dei dati (opzionale)

AWS Transform offre opzioni per la migrazione dei dati da SQL Server ad Aurora PostgreSQL. La migrazione dei dati è facoltativa e può essere ignorata se è necessaria solo la trasformazione dello schema e del codice.

Opzioni di migrazione dei dati

Opzione 1: migrazione dei dati di produzione

Migra i dati di produzione effettivi utilizzando AWS DMS:

- Caricamento iniziale completo di tutti i dati
- Replica continua durante i test (CDC)
- Riduzione minima dei tempi di inattività
- Convalida dei dati e controlli di integrità

Opzione 2: ignora la migrazione dei dati

Trasforma solo schema e codice:

- Utile per development/testing gli ambienti
- Quando i dati verranno migrati separatamente
- Per progetti di prototipazione

Configura la migrazione dei dati

1. Passa alla migrazione dei dati nel piano di lavoro
2. Scegli la tua opzione di migrazione:
 - Migra i dati di produzione
 - Salta la migrazione dei dati
3. Se stai migrando i dati di produzione, configura:
 - Tipo di migrazione: Full load o Full load + CDC
 - Convalida: abilita la convalida dei dati
 - Prestazioni: dimensione dell'istanza DMS

- Scegli >Avvia migrazione

Processo di migrazione dei dati di produzione

Se scegli di migrare i dati di produzione:

1. Sincronizzazione iniziale: AWS DMS esegue il caricamento completo di tutte le tabelle
2. Replica continua: (se CDC abilitato) Mantiene i dati sincronizzati
3. Convalida: verifica il numero di righe e l'integrità dei dati
4. Preparazione del cutover: si prepara per la sincronizzazione finale

Cronologia della migrazione:

- Database di piccole dimensioni (< 10 GB): 30 minuti - 2 ore
- Database di medie dimensioni (10-100 GB): 2-8 ore
- Database di grandi dimensioni (> 100 GB): più di 8 ore

Convalida dei dati

AWS Transform convalida i dati migrati con i seguenti controlli:

- Confronto del numero di righe (origine e destinazione)
- Integrità della chiave primaria
- Relazioni con chiave esterna
- Compatibilità dei tipi di dati
- Risultati calcolati delle colonne
- Gestione dei valori nulli

Fase 10: trasformazione del codice dell'applicazione

AWS Transform trasforma il codice dell'applicazione.NET per utilizzarlo con Aurora PostgreSQL anziché con SQL Server. Richiede il nome del ramo di destinazione nei repository per eseguire il commit del codice sorgente trasformato. Dopo aver inserito il nome del ramo, AWS Transform creerà un nuovo ramo e avvierà la trasformazione in modo che corrisponda al database PostgreSQL.

Cosa viene trasformato

Modifiche al framework delle entità:

- Fornitore di database: UseSqlServer () → UseNpgsql ()
- Stringhe di connessione: formato SQL Server → formato PostgreSQL
- Mappature dei tipi di dati: tipi di SQL Server → tipi PostgreSQL
- DbContext configurazioni Server-specific : SQL → PostgreSQL-specific
- File di migrazione: aggiornati per la compatibilità con PostgreSQL

ADO.NET Modifiche:

- Classi di connessione: SqlConnection → NpgsqlConnection
- Classi di comando: SqlCommand → NpgsqlCommand
- Lettore di dati: SqlDataReader → NpgsqlDataReader
- Parametri: SqlParameter → NpgsqlParameter
- Sintassi SQL: T-SQL → PostgreSQL SQL

Modifiche alla configurazione:

- Stringhe di connessione in appsettings.json
- Pacchetti NuGet per fornitori di database
- Configurazioni di iniezione delle dipendenze
- Startup/Program.cs configurazioni

Inizia la trasformazione del codice

1. Passa alla trasformazione delle applicazioni nel piano di lavoro

2. Rivedi le impostazioni di trasformazione:

- Versione.NET di destinazione (in caso di aggiornamento)
- Versione del provider PostgreSQL
- Preferenze di stile del codice

3. Scegli Avvia trasformazione

4. Monitora i progressi nel registro di lavoro
5. La trasformazione richiede in genere 15-45 minuti a seconda della dimensione della codebase

Fase 11: Rivedere i risultati della trasformazione

Prima di procedere all'implementazione, esamina i risultati completi della trasformazione per assicurarti che tutto sia pronto per il test.

Puoi scaricare il codice trasformato dal ramo del repository per:

- Test e convalida locali
- Revisione del codice nel tuo IDE
- Integrazione con la tua CI/CD pipeline
- Impegno al controllo della versione

Puoi anche scaricare il riepilogo della trasformazione per esaminare le modifiche al linguaggio naturale apportate da AWS Transform come parte della trasformazione.

Riepilogo della trasformazione

1. Vai al riepilogo della trasformazione nel piano di lavoro
2. Esamina i risultati complessivi:
 - Conversione dello schema: oggetti convertiti, azioni, avvisi
 - Migrazione dei dati: tabelle migrate, righe trasferite, stato di convalida
 - Trasformazione del codice: file modificati, righe modificate, problemi risolti
 - Punteggio di preparazione: preparazione complessiva per l'implementazione

Genera un rapporto sulla trasformazione

AWS Transform genera un rapporto di trasformazione completo:

1. Scegli Genera rapporto
2. Seleziona il tipo di rapporto:
 - Sintesi: High-level panoramica per le parti interessate
 - Dettagli tecnici: documentazione completa sulla trasformazione

- Elementi d'azione: elenco delle attività umane richieste

3. Scegli Scarica rapporto

Il rapporto include:

- Ambito e obiettivi della trasformazione
- Oggetti e codice trasformati
- Problemi riscontrati e soluzioni
- Risultati della convalida
- Valutazione della preparazione all'implementazione
- Raccomandazioni per i test

Fase 12: Validazione e test

Prima di passare alla produzione, verifica che l'applicazione trasformata funzioni correttamente con Aurora PostgreSQL.

Tipi di convalida

Convalida automatizzata: AWS Transform esegue controlli automatici:

- Convalida dello schema rispetto al database di origine
- Verifica dell'integrità dei dati
- Test di equivalenza delle query
- Convalida della stringa di connessione
- Convalida della configurazione

Validazione umana: è necessario eseguire test aggiuntivi:

- Test funzionali delle funzionalità dell'applicazione
- Test di integrazione con altri sistemi
- Test e benchmarking delle prestazioni
- Test di accettazione da parte degli utenti
- Test di sicurezza

Esegui la convalida automatica

1. Vai alla convalida nel piano di lavoro
2. Scegli Esegui convalida
3. AWS Transform esegue i test di convalida:
 - Connettività al database
 - Compatibilità dello schema
 - Integrità dei dati
 - Creazione di applicazioni
 - Funzionalità di base
4. Rivedi i risultati della convalida:
 - Superati: test che hanno avuto esito positivo
 - Non riuscito: test che richiedono attenzione
 - Avvertenze: potenziali problemi da esaminare

Lista di controllo per i test

Funzionalità del database:

- Tutte le tabelle accessibili
- Le procedure memorizzate vengono eseguite correttamente
- Le funzioni restituiscono i risultati attesi
- I trigger si attivano in modo appropriato
- Vincoli applicati correttamente
- Gli indici migliorano le prestazioni delle query

Funzionalità dell'applicazione:

- L'applicazione viene avviata correttamente
- Connessioni al database stabilite
- Le operazioni CRUD funzionano correttamente
- Le chiamate di procedura memorizzata hanno esito positivo
- Transazioni commit/rollback corrette

- La gestione degli errori funziona come previsto

Integrità dei dati:

- Il conteggio delle righe corrisponde alla fonte
- Chiavi primarie uniche
- Chiavi esterne valide
- Le colonne calcolate sono corrette
- Gestione nulla appropriata
- Tipi di dati compatibili

Prestazioni:

- Tempi di risposta alle interrogazioni accettabili
- Pool di connessioni configurato
- Indici ottimizzati
- Nessun problema di interrogazione N+1
- Operazioni in batch efficienti
- Utilizzo delle risorse ragionevole

Fase 13: Implementazione

Dopo una convalida riuscita, distribuisce l'applicazione e il database modernizzati in produzione.

Opzioni di implementazione

- Amazon ECS e Amazon EC2 Linux

Pre-deployment lista di controllo

Prima della distribuzione in produzione:

- Tutti i test di convalida sono stati superati
- Test delle prestazioni completati
- Revisione della sicurezza completata

- Piano di backup e rollback documentato
- Monitoraggio e avvisi configurati
- Team formato sul nuovo ambiente
- Le parti interessate sono state informate dell'implementazione
- Finestra di manutenzione pianificata

Esegui la distribuzione su Amazon ECS

1. Passa a Deployment nel piano di lavoro
2. Scegli Deploy to ECS
3. Configura le impostazioni di distribuzione:
 - Cluster: seleziona o crea un cluster ECS
 - Servizio: configura il servizio ECS
 - Definizione dell'attività: rivedi la definizione dell'attività generata
 - Load balancer: configura ALB/NLB
 - Auto-scaling: Imposta le politiche di scalabilità
4. Rivedi l'infrastruttura come codice (modello o codice CDK) CloudFormation AWS
5. Scegli Deploy

Monitora l'implementazione

AWS Transform implementa la tua applicazione:

1. Crea un cluster Aurora PostgreSQL
2. Applica lo schema del database
3. Carica i dati (se applicabile)
4. Implementa contenitori di applicazioni
5. Configura il bilanciamento del carico
6. Imposta l'auto-scaling

Monitora l'avanzamento dell'implementazione e verifica:

- Fornitura dell'infrastruttura

- Inizializzazione del database
- Distribuzione delle applicazioni
- Superamento dei controlli sanitari
- Applicazione accessibile
- Connessioni al database funzionanti
- Registri che mostrano il normale funzionamento

Post-deployment convalida

Dopo la distribuzione:

Analisi del fumo:

- Verifica delle funzionalità critiche
- Testa i flussi di lavoro chiave degli utenti
- Verifica i punti di integrazione
- Monitora i tassi di errore

Monitoraggio delle prestazioni:

- Tieni traccia dei tempi di risposta
- Monitora le interrogazioni del database
- Controlla l'utilizzo delle risorse
- Rivedi i registri delle applicazioni

Convalida utente:

- Condurre test di accettazione da parte degli utenti
- Raccogli feedback
- Risolvi eventuali problemi
- Documenta le lezioni apprese

Procedure di rollback

Se sorgono problemi dopo la distribuzione:

Rollback immediato:

- Torna alla versione precedente dell'applicazione
- Torna a SQL Server (se ancora disponibile)
- Eseguire il ripristino dal backup, se necessario

Rollback parziale:

- Ripristina componenti specifici
- Mantieni le modifiche al database
- Ripristina solo il codice dell'applicazione

Correzione avanzata:

- Applica l'hotfix alla versione Aurora PostgreSQL
- Implementa codice applicativo aggiornato
- Monitora la risoluzione

Important

Mantieni disponibile il database SQL Server per un periodo dopo il cutover per abilitare il rollback, se necessario.

Post-deployment ottimizzazione

Dopo una corretta implementazione:

Ottimizzazione delle prestazioni:

- Ottimizza le query lente
- Modifica le impostazioni del pool di connessioni
- Fine-tune Parametri Aurora PostgreSQL
- Rivedi e ottimizza gli indici

Ottimizzazione dei costi:

- Right-size Istanza Aurora
- Configurare l'auto-scaling in modo appropriato
- Rivedi le impostazioni di archiviazione
- Ottimizza la conservazione dei backup

Configurazione del monitoraggio:

- Configurare i CloudWatch dashboard
- Configura gli avvisi
- Enable Enhanced Monitoring (Abilita il monitoraggio avanzato)
- Configurare Performance Insights

Documentazione:

- Aggiorna i runbook
- Modifiche all'architettura del documento
- Squadra operativa dei treni
- Crea guide per la risoluzione dei problemi

Test e implementazione dopo la trasformazione

Implementa le tue applicazioni trasformate nella landing zone e convalida la connettività tra le tue applicazioni e il database trasformato e, facoltativamente, configura le pipeline. CI/CD Le configurazioni di CI/CD pipeline di esempio vengono generate come riferimento per aiutarti a implementare l'automazione della distribuzione. Questa fase finale convalida la modernizzazione completa.

Configura le risorse

Devi configurare le risorse utilizzate nella distribuzione, come i ruoli IAM, i profili di istanza e il bucket S3. AWS Transform non dispone delle autorizzazioni per creare bucket S3 o apportare modifiche al tuo IAM. Questa azione deve essere eseguita da un utente che dispone delle autorizzazioni per creare nuovi ruoli. Di solito è l'amministratore dell'account.

Per semplificare il processo, forniamo uno script di configurazione che automaticamente:

- Esegue i modelli necessari CloudFormation
- Crea il ruolo ECS Service-Linked
- Imposta tutte le risorse IAM richieste

Important

Esegui lo script di configurazione fornito così com'è: non modificare i nomi delle risorse nei modelli o negli script poiché ciò potrebbe influire sul processo di distribuzione.

Per Linux:

```
./setup.sh --region <YOUR-Region>
```

Per Windows:

```
./setup.ps1 -Region <YOUR-Region>
```

Controlla i gruppi di sicurezza nel tuo VPC

AWS Transform distribuisce le applicazioni nella stessa sottorete e nello stesso gruppo di sicurezza dell'istanza Aurora PostgreSQL.

Per consentire all'applicazione di connettersi all'istanza Aurora, assicurati che questo gruppo di sicurezza abbia regole in uscita che consentano la connessione allo stesso gruppo di sicurezza e regole in entrata che consentano la connessione dallo stesso gruppo di sicurezza.

Seleziona e configura le applicazioni

L'interfaccia utente AWS Transform mostra un elenco di applicazioni che possono essere distribuite. Seleziona l'applicazione e fai clic su Configura e conferma per aprire una finestra di configurazione in cui puoi specificare:

- Infrastruttura di destinazione per le applicazioni: seleziona ECS o una delle istanze EC2
- Parametri dell'applicazione o dell'istanza

Dopo aver completato e chiuso la finestra di configurazione, AWS Transform:

- Genera artefatti di distribuzione in base alla tua configurazione
- Salva questi elementi nel tuo repository, tra cui:
 - Script di distribuzione
 - CloudFormation modelli
 - Configurazioni di CI/CD pipeline di esempio (che è possibile utilizzare come riferimento per configurare l'automazione della distribuzione)

Una volta completato il commit, lo stato dell'applicazione cambia in Configurato e confermato. È quindi possibile selezionare le applicazioni e utilizzare il pulsante Deploy in alto a destra per avviare la distribuzione.

Implementazione ECS

Tutte le applicazioni con ECS di destinazione vengono distribuite in un nuovo cluster ECS creato nell'account. Ogni applicazione viene distribuita nel proprio contenitore dedicato: non sono supportate più applicazioni per contenitore. I parametri del contenitore vengono configurati singolarmente per ogni applicazione, ad esempio la CPU e la memoria richieste.

Implementazione EC2

Puoi selezionare una delle istanze EC2 proposte e configurarne i parametri, come il tipo di istanza. È possibile distribuire più applicazioni sulla stessa istanza EC2:

- Per distribuire più applicazioni su una singola istanza, seleziona la stessa istanza EC2 di destinazione per ciascuna di queste applicazioni durante la configurazione.
- Tutte le applicazioni con la stessa istanza selezionata come destinazione vengono distribuite su quell'istanza e assegnate porte casuali diverse.
- Tieni presente che se modifichi i parametri dell'istanza per un'applicazione e quindi modifichi un'altra applicazione destinata alla stessa istanza, le modifiche influiscono su tutte le applicazioni distribuite su quell'istanza.

Implementazione riuscita

Dopo una corretta implementazione, le applicazioni vengono eseguite su Aurora PostgreSQL con costi di licenza ridotti, prestazioni migliorate e scalabilità nativa per il cloud. Il lavoro rimane aperto a meno che non venga interrotto esplicitamente. Ciò consente l'opzione per una possibile ridistribuzione con parametri di distribuzione aggiornati.

Best practice e risoluzione dei problemi

Procedure ottimali, problemi comuni e relative soluzioni durante il processo di modernizzazione.

Registri delle applicazioni ECS

CloudWatch registri

- Tutti i log dei contenitori ECS vengono inviati automaticamente a Logs CloudWatch
- Accedi ai log nella console sotto Log Groups CloudWatch
- Formato di denominazione dei gruppi di log: `/aws/ecs/{application-name}`
- Ogni istanza del contenitore crea un nuovo flusso di log all'interno del gruppo

Visualizzazione dei log di

Tramite AWS Console:

- Passa a CloudWatch > Gruppi di registro
- Seleziona il gruppo di log della tua applicazione
- Scegli il flusso di log pertinente per visualizzare i log del contenitore

Utilizzo della AWS CLI:

```
aws logs get-log-events --log-group-name /aws/ecs/your-app-name --log-stream-name your-stream-name
```

Posizioni di registro comuni

- Registri delle applicazioni: CloudWatch registri
- Eventi del servizio ECS: Console ECS > Cluster > Servizio > scheda Eventi
- Contenitore health/status: Console ECS > Cluster > Servizio > scheda Attività

Gestione delle connessioni al database

Le applicazioni utilizzano variabili di ambiente per le impostazioni di connessione al database

Se riscontri problemi di connettività:

- Verifica le impostazioni di connessione correnti nelle variabili di ambiente
- Aggiorna le variabili di ambiente per modificare le stringhe di connessione al database secondo necessità
- Le modifiche alla stringa di connessione possono essere apportate tramite aggiornamenti delle variabili di ambiente senza redistribuzione dell'applicazione

Problemi di connessione al database

Problema: impossibile connettere AWS Transform a SQL Server

Soluzioni:

- Verifica la connettività di rete tra AWS Transform e SQL Server
- Controlla le regole del gruppo di sicurezza per il corretto accesso alle porte (1433)
- Conferma le credenziali del database in Secrets Manager
- Verifica le autorizzazioni del database con l'utente creato
- Assicurati che SQL Server sia configurato per l'autenticazione in modalità mista
- Verify secret ha i tag richiesti (Progetto: atx-db-modernization, proprietario: database-connector)

Problemi relativi al firewall e ai gruppi di sicurezza

Problema: timeout della connessione o errore «impossibile raggiungere il database»

Causa principale: gruppi di sicurezza o ACL di rete che bloccano il traffico

Soluzioni:

1. Verifica la configurazione del gruppo di sicurezza:

- Verifica che il gruppo di sicurezza di SQL Server disponga di una regola in entrata che consente la porta 1433 del gruppo di sicurezza DMS Schema Conversion
- Verifica che l'origine sia l'ID del gruppo di sicurezza (ad esempio, sg-0123456789abcdef0), non un indirizzo IP
- Verifica che il gruppo di sicurezza DMS Schema Conversion sia specificato correttamente nel profilo dell'istanza
- Assicurati che non vi siano regole di negazione in conflitto

2. Controlla gli ACL di rete:

- Verifica che gli ACL di rete a livello di sottorete consentano il traffico in entrata sulla porta 1433
- Assicurati che gli ACL di rete consentano le porte effimere in uscita per il traffico di ritorno
- Controlla sia la sottorete del database che gli ACL di rete della sottorete DMS

3. Verifica la configurazione del VPC:

- Verifica che l'istanza di conversione dello schema DMS e SQL Server si trovino nello stesso VPC o che dispongano del peering VPC corretto
- Verifica che le tabelle dei percorsi consentano il traffico tra le sottoreti
- Verifica che nessun dispositivo firewall stia bloccando il traffico

4. Test di connettività:

- Avvia un'istanza EC2 di prova nella stessa sottorete di DMS Schema Conversion
- Collega lo stesso gruppo di sicurezza di DMS Schema Conversion
- Verifica la connessione a SQL Server utilizzando telnet o SQL Server Management Studio
- Se il test ha esito positivo, il problema riguarda la configurazione di AWS Transform; se fallisce, il problema è network/firewall

Errore comune: apertura della porta 1433 su 0.0.0.0/0 (tutte le fonti) rappresenta un rischio per la sicurezza. Utilizza sempre il controllo degli accessi basato sul gruppo di sicurezza per limitare l'accesso solo al gruppo di sicurezza DMS Schema Conversion.

Problemi di conversione dello schema

Problema: la conversione dello schema mostra molte azioni

Soluzioni:

- Esamina le azioni da intraprendere nel rapporto di conversione
- Assegna le priorità in base all'impatto
- Usa Amazon Q Developer per conversioni SQL complesse
- Consulta AWS Support per ricevere assistenza
- Prendi in considerazione un approccio graduale per database complessi

Problemi di trasformazione delle applicazioni

Problema: la trasformazione delle applicazioni non riesce a essere completata

Soluzioni:

- Esamina gli errori di compilazione nel rapporto di trasformazione
- Se necessario, configura NuGet i feed privati
- Se necessario, aggiorna i riferimenti ai pacchetti
- Verifica le Windows-specific dipendenze
- Esamina i log di trasformazione per eventuali errori dettagliati

Problemi di migrazione dei dati

Problema: la convalida della migrazione dei dati non riesce

Soluzioni:

- Esamina il rapporto di convalida per errori specifici
- Controlla le mappature dei tipi di dati
- Verifica la configurazione della colonna di identità (GENERATED BY DEFAULT vs GENERATED ALWAYS)
- Rivedi le espressioni delle colonne calcolate
- Contatta l' AWS assistenza per problemi complessi relativi ai dati

Problemi di pulizia delle risorse

Problema: il processo di trasformazione fallisce a causa di errori nelle risorse

Soluzioni:

- Verifica le risorse DMS esistenti (progetti di migrazione, fornitori di dati, profili di istanza)
- Pulisci le risorse fallite o incomplete dei tentativi precedenti
- Verifica che i segreti non siano pianificati per l'eliminazione
- Controlla le quote di servizio per DMS e Aurora PostgreSQL
- Contatta l' AWS assistenza se la pulizia non risolve il problema

Problemi relativi alla distribuzione

Problema: l'applicazione trasformata non può connettersi ad Aurora PostgreSQL

Soluzioni:

- Verifica il formato della stringa di connessione per PostgreSQL
- Controlla le regole del gruppo di sicurezza
- Verifica le credenziali del database in Secrets Manager
- Assicurati che SSL/TLS sia configurato correttamente
- Verifica la connessione usando psql o pgAdmin

Ottenere ulteriore assistenza

Quando contatti AWS l'assistenza, fornisci:

- ID del lavoro di trasformazione
- AWS ID dell'account
- Region
- Messaggi di errore e schermate
- Registri di trasformazione (disponibili nella console AWS Transform)

Sicurezza in AWS Trasformazione

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- **Sicurezza del cloud:** AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. Third-party i revisori testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per ulteriori informazioni sui programmi di conformità che si applicano a AWS Transform, consulta [AWS Services in Scope by Compliance Program AWS](#) .
- **Sicurezza nel cloud:** la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza AWS Transform. I seguenti argomenti mostrano come configurare AWS Transform per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse AWS Transform.

Argomenti

- [Protezione dei dati in AWS Transform](#)
- [Gestione delle identità e degli accessi per AWS Trasformazione](#)
- [Convalida della conformità per AWS Trasformazione](#)
- [Resilienza in AWS Trasformazione](#)
- [AWS Transform e endpoint di interfaccia \(AWS PrivateLink\)](#)
- [Accesso al AWS Transform applicazione web da un VPC](#)

Protezione dei dati in AWS Transform

Il [modello di responsabilità AWS condivisa](#) si applica alla protezione dei dati in AWS Transform.

Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza relative a Servizi AWS ciò che utilizza. Per ulteriori informazioni sulla privacy dei dati, consulta [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post [AWS Modello di responsabilità condivisa](#) e GDPRAWS nel blog sulla sicurezza di .

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il proprio lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Utilizzatelo per comunicare con AWS le risorse. È consigliabile TLS 1.2 o versioni successive.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza servizi di sicurezza gestiti avanzati come Amazon Macie, che aiutano a scoprire e proteggere i dati sensibili archiviati in Amazon S3
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei [tag](#) o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori o Servizi AWS utilizzi in altro modo l'API AWS Management Console, AWS Command Line Interface () AWS Transform o gli SDK.AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Per ulteriori informazioni su come AWS Transform utilizza i contenuti, consulta [AWS Transform miglioramento del servizio](#).

AWS Transform archivia le domande, le relative risposte e il contesto aggiuntivo, ad esempio i metadati della console e il codice nell'IDE, per generare risposte alle domande. Per ulteriori informazioni su come i dati vengono crittografati, consulta [Crittografia dei dati in AWS Transform](#). Per informazioni su come AWS possiamo utilizzare alcune domande poste dall'utente AWS Transform e le relative risposte per migliorare i nostri servizi, consulta [AWS Transform miglioramento del servizio](#).

Nel AWS Transform, i tuoi dati vengono archiviati nella AWS regione in cui è stato creato il tuo AWS Transform profilo.

Con l'inferenza incrociata, le tue richieste AWS Transform possono essere elaborate in una regione diversa all'interno della geografia in cui sono archiviati i tuoi dati. [Per ulteriori informazioni, vedere inferenza. Cross-Region](#)

Argomenti

- [Cross-region elaborazione in AWS Transform](#)
- [Crittografia dei dati in AWS Transform](#)
- [AWS Transform miglioramento del servizio](#)

Cross-region elaborazione in AWS Transform

Le sezioni seguenti descrivono come vengono utilizzate l'inferenza interregionale e le chiamate interregionali per fornire il servizio. AWS Transform

Cross-region inferenza

AWS Transform è basato su Amazon Bedrock e utilizza l'inferenza interregionale per distribuire il traffico tra diverse Regioni AWS regioni al fine di migliorare le prestazioni e l'affidabilità dell'inferenza del modello di linguaggio di grandi dimensioni (LLM). Con l'inferenza tra regioni, ottieni:

- Maggiore throughput e resilienza durante i periodi di forte domanda
- Prestazioni migliorate
- Accesso a AWS Transform funzionalità e caratteristiche appena lanciate che si basano sui più potenti LLM ospitati su Amazon Bedrock

Cross-region le richieste di inferenza vengono mantenute all' Regioni AWS interno della parte geografica in cui risiedono originariamente i dati. Ad esempio, una richiesta effettuata da una AWS

Transform configurazione negli Stati Uniti viene conservata all'interno degli Regioni AWS Stati Uniti. Sebbene l'inferenza tra regioni non modifichi il luogo in cui sono archiviati i dati, le richieste e i risultati dell'output potrebbero spostarsi al di fuori della regione in cui risiedono originariamente i dati. Tutti i dati vengono crittografati durante la trasmissione sulla rete sicura di Amazon. L'utilizzo dell'inferenza tra regioni non prevede costi aggiuntivi.

L'inferenza tra regioni non influisce su dove vengono archiviati i tuoi dati. Per informazioni su dove vengono archiviati i dati durante l'utilizzo AWS Transform, consulta [Protezione dei dati in AWS Transform](#).

Regioni supportate per AWS Transform inferenza tra Regioni

Alcune richieste che effettui AWS Transform potrebbero richiedere chiamate tra regioni diverse. La tabella seguente descrive le regioni verso cui le richieste possono essere indirizzate a seconda della geografia in cui ha avuto origine la richiesta.

Regione di origine	Regioni di destinazione
Stati Uniti orientali (Virginia settentrionale) (us-east-1)	Stati Uniti orientali (Virginia settentrionale) (us-east-1)
	Stati Uniti orientali (Ohio) (us-east-2)
	Stati Uniti occidentali (Oregon) (us-west-2)
Europa (Francoforte) (eu-central-1)	Europa (Francoforte) (eu-central-1)
	Europa (Stoccolma) (eu-north-1)
	Europa (Milano) (eu-south-1)
	Europa (Spagna) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (Parigi) (eu-west-3)
Asia Pacifico (Mumbai) (ap-south-1)	Asia Pacifico (Tokyo) (ap-northeast-1)
	Asia Pacifico (Seoul) (ap-northeast-2)
	Asia Pacifico (Osaka-Locale) (ap-northeast-3)

Regione di origine	Regioni di destinazione
	Asia Pacifico (Mumbai) (ap-south-1)
	Asia Pacifico (Hyderabad) (ap-south-2)
	Asia Pacifico (Singapore) (ap-southeast-1)
	Asia Pacifico (Sydney) (ap-southeast-2)
	Asia Pacifico (Melbourne) (ap-southeast-4)
Asia Pacifico (Tokyo) (ap-northeast-1)	Asia Pacifico (Tokyo) (ap-northeast-1)
	Asia Pacifico (Osaka-Locale) (ap-northeast-3)
Asia Pacifico (Seoul) (ap-northeast-2)	Asia Pacifico (Tokyo) (ap-northeast-1)
	Asia Pacifico (Seoul) (ap-northeast-2)
	Asia Pacifico (Osaka-Locale) (ap-northeast-3)
	Asia Pacifico (Mumbai) (ap-south-1)
	Asia Pacifico (Hyderabad) (ap-south-2)
	Asia Pacifico (Singapore) (ap-southeast-1)
	Asia Pacifico (Sydney) (ap-southeast-2)
	Asia Pacifico (Melbourne) (ap-southeast-4)
Asia Pacifico (Sydney) (ap-southeast-2)	Asia Pacifico (Sydney) (ap-southeast-2)
	Asia Pacifico (Melbourne) (ap-southeast-4)

Regione di origine	Regioni di destinazione
Europa (Londra) (eu-west-2)	Europa (Francoforte) (eu-central-1)
	Europa (Stoccolma) (eu-north-1)
	Europa (Milano) (eu-south-1)
	Europa (Spagna) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (Londra) (eu-west-2)
	Europa (Parigi) (eu-west-3)
Canada (Centrale) (ca-central-1)	Commerciale Regioni AWS + Canada (Central) (ca-central-1)
Sud America (San Paolo) (sa-east-1)	Commercial Regioni AWS + Sud America (San Paolo) (sa-east-1)

Per un elenco completo delle regioni in cui è possibile utilizzare AWS Transform, consulta. [Regioni supportate per AWS Transform](#)

Cross-Region conoscenza

Quando fai una domanda generale su AWS Transform servizi, flussi di lavoro di trasformazione o AWS documentazione correlata, AWS Transform potresti inviare richieste interregionali agli Stati Uniti orientali (Virginia) (us-east-1) per le regioni degli Stati Uniti o all'Europa (Francoforte) (eu-central-1) per tutte le altre regioni per recuperare la documentazione e soddisfare la tua richiesta. Ad esempio, quando fai domande su come utilizzare altri AWS servizi come Lambda, AWS Transform potresti effettuare una chiamata interregionale per recuperare la AWS documentazione pertinente per rispondere alla tua domanda. La tabella seguente descrive le regioni verso cui le richieste possono essere indirizzate a seconda della geografia in cui ha avuto origine la richiesta.

Regione di origine	Regioni di destinazione
Stati Uniti orientali (Virginia settentrionale) (us-east-1)	Stati Uniti orientali (Virginia settentrionale) (us-east-1)
Europa (Francoforte) (eu-central-1)	Europa (Francoforte) (eu-central-1)
Europa (Londra) (eu-west-2)	Europa (Francoforte) (eu-central-1)
Asia Pacifico (Tokyo) (ap-northeast-1)	Europa (Francoforte) (eu-central-1)
Asia Pacifico (Sydney) (ap-southeast-2)	Europa (Francoforte) (eu-central-1)
Asia Pacifico (Seoul) (ap-northeast-2)	Europa (Francoforte) (eu-central-1)
Asia Pacifico (Mumbai) (ap-south-1)	Europa (Francoforte) (eu-central-1)
Canada (Centrale) (ca-central-1)	Europa (Francoforte) (eu-central-1)
Sud America (San Paolo) (sa-east-1)	Europa (Francoforte) (eu-central-1)

Questa impostazione è abilitata per impostazione predefinita. Un amministratore dell'account può modificare questa impostazione. La disattivazione di questa funzionalità comporta la perdita dell'accesso alle funzionalità che richiedono il recupero AWS Transform di conoscenze da altre regioni. Ciò potrebbe comportare risposte meno accurate.

Per disabilitare le chiamate interregionali effettuate da AWS Transform:

1. Alla prima configurazione AWS Transform, vai alla pagina Guida introduttiva e completa la configurazione. Per una AWS Transform configurazione esistente, vai alla pagina Impostazioni.
2. Attiva l'opzione Abilita chiamate interregionali per rispondere a domande generali AWS relative alla posizione off.

AWS Transform per l'inferenza interregionale di Windows

La tabella seguente mostra le Regioni di origine da cui puoi chiamare il profilo di inferenza e le Regioni di destinazione verso le quali possono essere instradate le richieste:

Regione di origine	Regioni di destinazione di inferenza
Stati Uniti orientali (Virginia settentrionale) (us-east-1)	Stati Uniti orientali (Virginia settentrionale) (us-east-1)
	Stati Uniti orientali (Ohio) (us-east-2)
	Stati Uniti occidentali (Oregon) (us-west-2)
Europa (Francoforte) (eu-central-1)	Europa (Francoforte) (eu-central-1)
	Europa (Stoccolma) (eu-north-1)
	Europa (Milano) (eu-south-1)
	Europa (Spagna) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (Parigi) (eu-west-3)
Asia Pacifico (Tokyo) (ap-northeast-1)	Asia Pacifico (Tokyo) (ap-northeast-1)
	Asia Pacifico (Osaka-Locale) (ap-northeast-3)
Asia Pacifico (Sydney) (ap-southeast-2)	Asia Pacifico (Sydney) (ap-southeast-2)
	Asia Pacifico (Melbourne) (ap-southeast-4)
Asia Pacifico (Seoul) (ap-northeast-2)	Tutte le regioni commerciali
Asia Pacifico (Mumbai) (ap-south-1)	Tutte le regioni commerciali
Canada (Centrale) (ca-central-1)	Tutte le regioni commerciali

AWS Transform per l'inferenza interregionale delle migrazioni

La tabella seguente mostra le Regioni di origine da cui puoi chiamare il profilo di inferenza e le Regioni di destinazione verso le quali possono essere instradate le richieste:

Regione di origine	Regioni di destinazione di inferenza
Stati Uniti orientali (Virginia settentrionale) (us-east-1)	Tutte le regioni commerciali
Europa (Francoforte) (eu-central-1)	Tutte le regioni commerciali
Europa (Londra) (eu-west-2)	Tutte le regioni commerciali
Asia Pacifico (Tokyo) (ap-northeast-1)	Asia Pacifico (Tokyo) (ap-northeast-1) Asia Pacifico (Osaka-Locale) (ap-northeast-3)
Asia Pacifico (Sydney) (ap-southeast-2)	Asia Pacifico (Sydney) (ap-southeast-2) Asia Pacifico (Melbourne) (ap-southeast-4)
Asia Pacifico (Seoul) (ap-northeast-2)	Tutte le regioni commerciali
Asia Pacifico (Mumbai) (ap-south-1)	Tutte le regioni commerciali
Canada (Centrale) (ca-central-1)	Tutte le regioni commerciali

AWS Transform per l'inferenza interregionale su mainframe

AWS Transform per mainframe utilizza l'inferenza geografica interregionale di Amazon Bedrock. Ciò significa che alcune chiamate potrebbero essere indirizzate al di Regioni AWS fuori della regione di origine. La tabella seguente mostra le Regioni di origine da cui puoi chiamare il profilo di inferenza e le Regioni di destinazione verso le quali possono essere instradate le richieste:

Regione di origine	Regioni di destinazione di inferenza
Stati Uniti orientali (Virginia settentrionale) (us-east-1)	Stati Uniti orientali (Virginia settentrionale) (us-east-1) Stati Uniti orientali (Ohio) (us-east-2) Stati Uniti occidentali (Oregon) (us-west-2)
Europa (Francoforte) (eu-central-1)	Europa (Francoforte) (eu-central-1)

Regione di origine	Regioni di destinazione di inferenza
	Europa (Stoccolma) (eu-north-1)
	Europa (Milano) (eu-south-1)
	Europa (Spagna) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (Parigi) (eu-west-3)
Europa (Londra) (eu-west-2)	Europa (Francoforte) (eu-central-1)
	Europa (Stoccolma) (eu-north-1)
	Europa (Milano) (eu-south-1)
	Europa (Spagna) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (Londra) (eu-west-2)
	Europa (Parigi) (eu-west-3)
Asia Pacifico (Tokyo) (ap-northeast-1)	Asia Pacifico (Tokyo) (ap-northeast-1)
	Asia Pacifico (Osaka-Locale) (ap-northeast-3)
Asia Pacifico (Sydney) (ap-southeast-2)	Asia Pacifico (Sydney) (ap-southeast-2)
	Asia Pacifico (Melbourne) (ap-southeast-4)
Asia Pacifico (Seoul) (ap-northeast-2)	Tutte le regioni commerciali
Asia Pacifico (Mumbai) (ap-south-1)	Tutte le regioni commerciali

Regione di origine	Regioni di destinazione di inferenza
Canada (Centrale) (ca-central-1)	Canada (Centrale) (ca-central-1) Stati Uniti orientali (Virginia settentrionale) (us-east-1) Stati Uniti orientali (Ohio) (us-east-2) Stati Uniti occidentali (Oregon) (us-west-2)
Sud America (San Paolo) (sa-east-1)	Tutte le regioni commerciali

AWS Transform Personalizzato

AWS Transform custom utilizza l'inferenza geografica interregionale di Amazon Bedrock. Ciò significa che alcune chiamate potrebbero essere indirizzate al di Regioni AWS fuori della regione di origine. La tabella seguente mostra le Regioni di origine da cui puoi chiamare il profilo di inferenza e le Regioni di destinazione verso le quali possono essere instradate le richieste:

Regione di origine	Regioni di destinazione di inferenza
Stati Uniti orientali (Virginia settentrionale) (us-east-1)	Stati Uniti orientali (Virginia settentrionale) (us-east-1) Stati Uniti orientali (Ohio) (us-east-2) Stati Uniti occidentali (Oregon) (us-west-2)
Europa (Francoforte) (eu-central-1)	Europa (Francoforte) (eu-central-1) Europa (Stoccolma) (eu-north-1) Europa (Milano) (eu-south-1) Europa (Spagna) (eu-south-2) Europa (Irlanda) (eu-west-1) Europa (Parigi) (eu-west-3)

Regione di origine	Regioni di destinazione di inferenza
Europa (Londra) (eu-west-2)	Europa (Francoforte) (eu-central-1)
	Europa (Stoccolma) (eu-north-1)
	Europa (Milano) (eu-south-1)
	Europa (Spagna) (eu-south-2)
	Europa (Irlanda) (eu-west-1)
	Europa (Londra) (eu-west-2)
	Europa (Parigi) (eu-west-3)
Asia Pacifico (Tokyo) (ap-northeast-1)	Tutte le regioni commerciali
Asia Pacifico (Sydney) (ap-southeast-2)	Asia Pacifico (Sydney) (ap-southeast-2)
	Asia Pacifico (Melbourne) (ap-southeast-4)
Asia Pacifico (Seoul) (ap-northeast-2)	Tutte le regioni commerciali
Asia Pacifico (Mumbai) (ap-south-1)	Tutte le regioni commerciali
Canada (Centrale) (ca-central-1)	Canada (Centrale) (ca-central-1)
	Stati Uniti orientali (Virginia settentrionale) (us-east-1)
	Stati Uniti orientali (Ohio) (us-east-2)
	Stati Uniti occidentali (Oregon) (us-west-2)

Crittografia dei dati in AWS Transform

Questo argomento fornisce informazioni specifiche AWS Transform sulla crittografia in transito e sulla crittografia a riposo.

AWS Transform fornisce la crittografia di default per proteggere i dati sensibili dei clienti archiviati con la crittografia utilizzando chiavi AWS proprietarie.

Tipi di crittografia

Crittografia dei dati in transito

La comunicazione tra i clienti AWS Transform e tra le relative dipendenze a valle è protetta mediante connessioni TLS 1.2 o versioni successive.

Important

Quando [Connect un account Discovery](#), AWS Transform crea un bucket Amazon S3 per tuo conto in quell'account. Quel bucket non è SecureTransport abilitato per impostazione predefinita. Se desideri che la policy del bucket includa il trasporto sicuro, devi aggiornare la policy. Per ulteriori informazioni, consulta [Best practice di sicurezza per Amazon S3](#).

Crittografia dei dati a riposo

AWS Transform archivia i dati inattivi utilizzando Amazon DynamoDB e Amazon Simple Storage Service (Amazon S3). Per impostazione predefinita, i dati inattivi vengono crittografati utilizzando soluzioni di AWS crittografia. AWS Transform crittografa i dati con crittografia utilizzando chiavi AWS di proprietà di AWS Key Management Service (AWS KMS). Non è necessario intraprendere alcuna azione per proteggere le chiavi AWS gestite che crittografano i dati. Per ulteriori informazioni, consulta la pagina [chiavi di proprietàAWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Tipo di dati	AWS-crittografia con chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
dati relativi al bucket del cliente	Abilitato	Abilitato
Input e output del cliente, come codice e documentazione archiviati in un bucket Amazon S3		
Negoziato di Artefatti	Abilitato	Abilitato

Tipo di dati	AWS-crittografia con chiave proprietaria	Crittografia con chiavi gestite dal cliente (opzionale)
Artefatti intermedi come parte della trasformazione del codice archiviati in un bucket S3		
Obiettivo del lavoro	Abilitato	Abilitato
L'intento del cliente per il lavoro archiviato in un bucket Amazon S3		
Messaggi di chat	Abilitato	Abilitato
Messaggi tra il cliente e AWS Transform archiviati in un bucket Amazon S3		
Base di conoscenza in chat	Abilitato	Abilitato
Dati indicizzati pertinenti AWS Transform e chat con i clienti archiviati in Amazon OpenSearch ed elaborati tramite Bedrock AWS		

Nota: il cliente può registrare la propria chiave gestita dal cliente (CMK) da utilizzare per crittografare tutti i tipi di dati sopra indicati.

Le chiavi gestite dal cliente sono chiavi KMS presenti nel tuo AWS account che crei, possiedi e gestisci per controllare direttamente l'accesso ai tuoi dati controllando l'accesso alla chiave KMS. Sono supportate solo le chiavi simmetriche. Per informazioni sulla creazione della tua chiave KMS, consulta [Creating keys](#) nella Developer Guide.AWS Key Management Service

Quando utilizzi una chiave gestita dal cliente, AWS Transform utilizza le concessioni KMS, che consentono agli utenti, ai ruoli o alle applicazioni autorizzati di utilizzare una chiave KMS. Quando un AWS Transform amministratore sceglie di utilizzare una chiave gestita dal cliente per la crittografia

durante la configurazione, viene creata una concessione per lui. Questa autorizzazione consente all'utente finale di utilizzare la chiave di crittografia per la crittografia dei dati a riposo. Per ulteriori informazioni sulle autorizzazioni, consulta [Autorizzazioni in AWS KMS](#).

AWS Chiavi possedute (impostazione predefinita)

Note

AWS chiavi di proprietà: AWS Transform utilizza queste chiavi per impostazione predefinita per crittografare automaticamente i dati di identificazione personale. Non è possibile visualizzare, gestire o utilizzare chiavi AWS di proprietà o controllarne l'utilizzo. Tuttavia, non è necessario effettuare alcuna operazione o modificare programmi per proteggere le chiavi che eseguono la crittografia dei dati. Per ulteriori informazioni, consulta le chiavi AWS possedute nella AWS Key Management Service Developer Guide.

La crittografia predefinita dei dati a riposo aiuta a ridurre il sovraccarico operativo e la complessità associati alla protezione dei dati sensibili. Allo stesso tempo, consente di creare applicazioni sicure che soddisfano i rigorosi requisiti normativi e di conformità alla crittografia.

Sebbene non sia possibile disabilitare questo livello di crittografia o selezionare un tipo di crittografia alternativo, è possibile aggiungere un secondo livello di crittografia rispetto alle chiavi di crittografia di AWS proprietà esistenti scegliendo una chiave gestita dal cliente quando si crea la trasformazione:

Chiavi gestite dal cliente (facoltative)

Chiavi gestite dal cliente: AWS Transform supporta l'uso di una chiave simmetrica gestita dal cliente che è possibile creare, possedere e gestire per aggiungere un secondo livello di crittografia alla crittografia esistente utilizzando chiavi AWS proprietarie. Avendo il pieno controllo di questo livello di crittografia, è possibile eseguire operazioni quali:

- Stabilire e mantenere le policy delle chiavi
- Stabilire e mantenere le policy e le sovvenzioni IAM
- Abilitare e disabilitare le policy delle chiavi
- Ruotare i materiali crittografici delle chiavi
- Aggiungere tag
- Creare alias delle chiavi
- Ruotare i materiali crittografici delle chiavi

- Aggiungere tag
- Creare alias delle chiavi
- Pianificare l'eliminazione delle chiavi
- Per ulteriori informazioni, consulta [Chiave gestita dal cliente](#) nella Guida per gli sviluppatori del Servizio AWS di gestione delle chiavi.

Note

AWS Transform abilita automaticamente la crittografia dei dati inattivi utilizzando chiavi AWS proprietarie per proteggere gratuitamente i dati di identificazione personale. Tuttavia, l'utilizzo di una chiave gestita dal cliente comporta dei AWS KMS costi. Per ulteriori informazioni sui prezzi, consulta i [AWS Key Management Service prezzi](#).

Per ulteriori informazioni su AWS KMS, consulta [Cos'è AWS Key Management Service?](#)

In che modo AWS Transform utilizza le sovvenzioni in AWS Key Management Service

AWS Transform richiede una concessione per utilizzare la chiave gestita dal cliente.

Quando crei un [Resource Name] crittografato con una chiave gestita dal cliente, AWS Transform crea una concessione per tuo conto inviando una CreateGrant richiesta a AWS Key Management Service. Le sovvenzioni AWS Key Management Service vengono utilizzate per AWS Transform consentire l'accesso a una chiave KMS in un account cliente.

AWS Transform richiede la concessione per utilizzare la chiave gestita dal cliente per le seguenti operazioni interne:

- Invia richieste [API KMS] AWS KMS a per verificare che l'ID della chiave KMS simmetrica gestita dal cliente inserito durante la creazione di [Nome risorsa] sia valido.
- Invia richieste [API KMS] per AWS KMS generare chiavi dati crittografate dalla chiave gestita dal cliente.
- Invia richieste [API KMS] a AWS KMS per decrittografare le chiavi dati crittografate in modo che possano essere utilizzate per crittografare i dati.

Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. Se lo fai, non AWS Transform sarai in grado di accedere a nessuno dei

dati crittografati dalla chiave gestita dal cliente, il che influirà sulle operazioni che dipendono da quei dati. Ad esempio, se si tenta di ottenere [Nome risorsa] da un [Nome risorsa] crittografato a cui non è AWS Transform possibile accedere, l'operazione restituirà un `AccessDeniedException` errore.

Creazione di una chiave gestita dal cliente

È possibile creare una chiave simmetrica gestita dal cliente utilizzando la console di AWS gestione o le AWS Key Management Service API.

Per creare una chiave simmetrica gestita dal cliente, segui i passaggi per la [creazione di una chiave gestita dal cliente simmetrica](#) nella Guida per gli sviluppatori.AWS Key Management Service

Per utilizzare la chiave gestita dal cliente con AWS Transform le tue risorse, nella policy chiave devono essere consentite le seguenti operazioni API:

kms: CreateGrant — Aggiunge una concessione a una chiave gestita dal cliente. Grants controlla l'accesso a una chiave KMS specificata, che consente l'accesso alle operazioni di concessione richieste. AWS Transform Per ulteriori informazioni sull'[utilizzo delle concessioni](#), consulta la Guida per gli sviluppatori di AWS Key Management Service .

Ciò consente di AWS Transform effettuare le seguenti operazioni:

- Chiama [KMS API ([GenerateDataKeyWithoutPlainText/GenerateDatakey](#))] per generare una chiave dati crittografata e archivarla, poiché la chiave dati non viene utilizzata immediatamente per crittografare.
- Chiama [KMS API ([Decrypt](#))] per utilizzare la chiave dati crittografata memorizzata per accedere ai dati crittografati.
- Configurare un principale ritirato per consentire al servizio di [RetireGrant](#).
- [kms: DescribeKey](#) — Fornisce i dettagli chiave gestiti dal cliente per consentire a [Service Name] di convalidare la chiave.

Crittografia per la modernizzazione di SQL

Durante il processo di [modernizzazione di SQL Server](#), AWS Transform crea risorse nel tuo account, come istanze EC2, cluster ECS, immagini ECR e oggetti S3. Hai la possibilità di fornire una chiave gestita dal cliente per crittografare i dati nel tuo account. Dovrai etichettare la tua chiave KMS con la chiave CreatedFor il valore AWSTransform. Questa politica di esempio elenca le autorizzazioni minime richieste nella politica chiave se non disponi di una politica di chiave predefinita. Se disponi di

una politica di chiave predefinita, devi comunque aggiornare manualmente la chiave KMS oltre alla politica delle chiavi predefinita per consentire a ECS di utilizzare la tua chiave.

```
"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"
      }
    }
  }
}
]

```

Crittografia per la migrazione del database

Durante il processo di migrazione del database, AWS Transform utilizza AWS Database Migration Service (DMS) per migrare i dati del database. Facoltativamente, puoi fornire una chiave gestita dal cliente per crittografare i dati del database durante la migrazione.

La seguente politica contiene tre dichiarazioni. La prima istruzione concede i permessi dell'account root per la AWS KMS chiave. La seconda istruzione consente al ruolo del connettore di convalidare la chiave durante il rilevamento. La terza istruzione consente al ruolo del connettore di utilizzare la chiave per le operazioni 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"
    }
  }
}
```

Utilizzo di chiavi KMS gestite dal cliente

Dopo aver creato una chiave KMS gestita dal cliente, un AWS Transform amministratore deve fornire la chiave nella AWS Transform console per utilizzarla per crittografare i dati.

Per configurare una chiave gestita dal cliente in cui crittografare i dati AWS Transform, gli amministratori necessitano delle autorizzazioni necessarie per l'utilizzo. AWS KMS

Per utilizzare funzionalità crittografate con una chiave gestita dal cliente, gli utenti devono disporre delle autorizzazioni per consentire l'accesso AWS Transform alla chiave gestita dal cliente.

Se visualizzi un errore relativo alle concessioni KMS durante l'utilizzo AWS Transform, probabilmente dovrai aggiornare le autorizzazioni per consentire AWS Transform la creazione di sovvenzioni. Per configurare automaticamente le autorizzazioni necessarie, vai alla AWS Transform console e scegli **Aggiorna autorizzazioni** nel banner nella parte superiore della pagina. Per consentire la creazione AWS Transform di sovvenzioni, devi aggiornare le autorizzazioni nella pagina della console. AWS Transform

Consenso AWS Transform accesso alle chiavi gestite dal cliente

La seguente dichiarazione politica di esempio concede agli utenti le autorizzazioni per accedere alle funzionalità crittografate con una chiave gestita dal cliente, consentendo AWS Transform l'accesso alla chiave. Questa politica deve essere utilizzata AWS Transform se un amministratore ha impostato una chiave gestita dal cliente per la crittografia.

Note

Queste informazioni non si applicano al flusso di lavoro di implementazione della modernizzazione di SQL Server tramite 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 miglioramento del servizio

Per contribuire a AWS Transform fornire le informazioni più pertinenti, possiamo utilizzare determinati contenuti AWS Transform, come le domande poste dall'utente AWS Transform e le relative risposte, per migliorare il servizio. Questa pagina spiega quali contenuti utilizziamo e come effettuare la disattivazione.

AWS Transform contenuti utilizzati per il miglioramento del servizio

Potremmo utilizzare determinati contenuti AWS Transform per migliorare il servizio. AWS Transform possiamo utilizzare questi contenuti, ad esempio, per fornire risposte migliori a domande comuni, risolvere problemi AWS Transform operativi, per il debug o per la formazione dei modelli.

I contenuti che AWS possono essere utilizzati per il miglioramento del servizio includono, ad esempio, le domande dell'utente, le risposte AWS Transform e il codice che generano. AWS Transform

Modalità per effettuare la disattivazione

Il modo in cui scegli di non AWS Transform utilizzare i contenuti per il miglioramento del servizio dipende dall'ambiente in cui lo utilizzi AWS Transform.

Per AWS Transform configurare una politica di disattivazione dei servizi AI in AWS Organizations. Per ulteriori informazioni, consulta le [Policy di rifiuto dei servizi di IA](#) nella Guida per l'utente di AWS Organizations .

Per disattivare la condivisione dei tuoi contenuti in Visual Studio IDE, utilizza la seguente procedura.

Vai a Strumenti -> Opzioni -> Kit di strumenti AWS -> Amazon Q

Attiva Condividi contenuti Amazon Q con AWS su True o False.

Per disattivare la condivisione dei dati di telemetria nel AWS Toolkit forVisual Studio, utilizza questa procedura:

1. In Strumenti, scegli Opzioni.
2. Nel riquadro Opzioni, scegli Kit di strumenti AWS , quindi seleziona Generale.
3. Deseleziona Consenti a AWS Toolkit di raccogliere informazioni sull'utilizzo.

Gestione delle identità e degli accessi per AWS Trasformazione

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Transform. AWS IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [In che modo AWS Transform funziona con IAM](#)
- [Identity-based esempi di policy per AWS Trasformazione](#)
- [Risoluzione dei problemi AWS Trasforma l'identità e l'accesso](#)
- [Utilizzo di ruoli collegati ai servizi per AWS Transform](#)
- [AWS politiche gestite per AWS Trasformazione](#)
- [AWS Riferimento alle autorizzazioni di trasformazione](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi AWS Trasforma l'identità e l'accesso](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [In che modo AWS Transform funziona con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta [Identity-based esempi di policy per AWS Trasformazione](#))

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come Centro identità AWS IAM (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Servizio di directory che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare Centro identità AWS IAM. Per ulteriori informazioni, consulta [Che cos'è il Centro identità IAM?](#) nella Guida per l'utente di Centro identità AWS IAM .

Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un ruolo utente a un ruolo IAM \(console\)](#) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per

maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Identity-based politiche

Identity-based le politiche sono documenti di policy sulle autorizzazioni JSON che alleggi a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Identity-based le politiche possono essere politiche in linea (incorporate direttamente in una singola identità) o politiche gestite (politiche autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Resource-based politiche

Resource-based le politiche sono documenti di policy JSON allegati a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

Resource-based le politiche sono politiche in linea che si trovano in quel servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): specifica il numero massimo di autorizzazioni per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- Policy di controllo delle risorse (RCP): imposta le autorizzazioni massime disponibili per le risorse degli account. Per ulteriori informazioni, consulta [Policy di controllo delle risorse \(RCP\)](#) nella Guida per l'utente di AWS Organizations .
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

In che modo AWS Transform funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Transform, scopri quali funzionalità IAM sono disponibili per l'uso con AWS Transform.

Funzionalità IAM	AWS Supporto per Transform
Identity-based politiche	Sì

Funzionalità IAM	AWS Supporto per Transform
Resource-based politiche	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Service-linked ruoli	Sì

Per avere una visione di alto livello di come AWS Transform e gli altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta [AWS i servizi che funzionano con IAM nella IAM User Guide](#).

Identity-based politiche per AWS Trasformazione

Supporta le policy basate sull'identità: sì

Identity-based le policy sono documenti relativi alle policy in materia di autorizzazioni JSON che puoi allegare a un'identità, ad esempio un utente IAM, un gruppo di utenti o un ruolo. Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

Identity-based esempi di policy per AWS Trasformazione

Per visualizzare esempi di politiche basate sull'identità di AWS Transform, vedere. [Identity-based esempi di policy per AWS Trasformazione](#)

Resource-based politiche all'interno AWS Trasformazione

Supporta le policy basate su risorse: no

Resource-based le politiche sono documenti di policy JSON allegati a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#). I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Azioni politiche per AWS Trasformazione

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di AWS trasformazione, consulta [Azioni, risorse e chiavi di condizione per AWS Transform](#) nel Service Authorization Reference.

Per visualizzare un elenco di azioni per AWS Transform custom, consulta [Azioni, risorse e chiavi di condizione per AWS Transform custom](#) nel Service Authorization Reference.

Le azioni politiche in AWS Transform utilizzano il seguente prefisso prima dell'azione:

```
transform
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
    "transform:action1",  
    "transform:action2"  
]
```

Per visualizzare esempi di politiche basate sull'identità AWS Transform, vedere. [Identity-based esempi di policy per AWS Trasformazione](#)

Risorse politiche per AWS Trasformazione

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse AWS Transform e dei relativi ARN e con quali azioni è possibile specificare l'ARN di ciascuna risorsa, [vedere Azioni, risorse e chiavi di condizione AWS per Transform](#) nel Service Authorization Reference.

Per visualizzare un elenco dei tipi di risorse e dei relativi ARN e con quali azioni è possibile specificare l'ARN di ciascuna risorsa AWS per Transform custom, [vedere Azioni, risorse e chiavi di condizione AWS per Transform](#) custom nel Service Authorization Reference.

Per visualizzare esempi di politiche basate sull'identità di AWS Transform, vedere. [Identity-based esempi di policy per AWS Trasformazione](#)

Chiavi relative alle condizioni delle politiche per AWS Trasformazione

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per visualizzare un elenco di chiavi di condizione AWS Transform e con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta [Actions, resources and condition keys for AWS Transform](#) nel Service Authorization Reference.

Per visualizzare un elenco di chiavi di condizione e con quali azioni e risorse è possibile utilizzare una chiave di condizione per AWS Transform custom, vedere [Azioni, risorse e chiavi di condizione per AWS Transform custom](#) nel Service Authorization Reference.

Per visualizzare esempi di politiche basate sull'identità di AWS Transform, vedere. [Identity-based esempi di policy per AWS Trasformazione](#)

ACL in AWS Trasformazione

Supporta le ACL: no

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AWS Trasformazione

Supporta ABAC (tag nelle policy): parzialmente

Attribute-based il controllo degli accessi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. È possibile allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AWS Trasformazione

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza temporanee in IAM](#) e [Servizi AWS compatibili con IAM](#) nella Guida per l'utente IAM.

Cross-service autorizzazioni principali per AWS Trasformazione

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Ruoli di servizio per AWS Trasformazione

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

 Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità AWS Transform. Modifica i ruoli di servizio solo quando AWS Transform fornisce indicazioni in tal senso.

Service-linked ruoli per AWS Trasformazione

Supporta i ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. Service-linked i ruoli appaiono nel tuo Account AWS account e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione dei ruoli collegati al servizio AWS Transform, consulta [Utilizzo di ruoli collegati ai servizi per AWS Transform](#)

Identity-based esempi di policy per AWS Trasformazione

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse AWS Transform. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS Transform, incluso il formato degli ARN per ciascun tipo di risorsa, consulta [Actions, Resources and Condition Keys for AWS Transform](#) nel Service Authorization Reference.

Argomenti

- [Best practice per le policy](#)
- [Utilizzo di AWS Console Transform](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Consenti agli amministratori di accettare una richiesta di connettore dall'account con AWS Trasformazione](#)

- [Consenti agli amministratori di assegnare gli utenti IAM Identity Center esistenti e di creare nuovi utenti IAM Identity Center a cui assegnare AWS Trasformazione](#)
- [Consenti agli amministratori di abilitare AWS Trasformazione](#)
- [Consenti agli utenti di accedere AWS Trasforma con credenziali IAM](#)

Best practice per le policy

Identity-based le politiche determinano se qualcuno può creare, accedere o eliminare le risorse AWS Transform nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e

consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di IAM.

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Utilizzo di AWS Console Transform

Per accedere alla console AWS Transform, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse AWS Transform presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l'AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
}
]
}

```

Consenti agli amministratori di accettare una richiesta di connettore dall'account con AWS Trasformazione

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-*"
  }
]
}

```

Consenti agli amministratori di assegnare gli utenti IAM Identity Center esistenti e di creare nuovi utenti IAM Identity Center a cui assegnare AWS Trasformazione

La seguente policy concede le autorizzazioni necessarie a un amministratore per gestire gli utenti e i gruppi di IAM Identity Center nella console Transform. AWS Con questa policy, un amministratore può assegnare e rimuovere utenti e gruppi, visualizzare i nomi visualizzati, creare nuovi utenti IAM Identity Center, gestire le assegnazioni delle applicazioni e configurare le impostazioni delle sessioni delle applicazioni.

```

{
  "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"
            }
        }
    }
]
}

```

Consenti agli amministratori di abilitare AWS Trasformazione

La seguente politica concede le autorizzazioni necessarie a un amministratore per abilitare e amministrare AWS Transform tramite la console. AWS Ciò include la gestione dei profili, la configurazione degli agenti e la gestione dei connettori. Questa politica è destinata esclusivamente agli amministratori e deve essere applicata ai responsabili fidati del tuo account.

```

{
    "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": "*"    
  }  
]  
}
```

Consenti agli utenti di accedere AWS Trasforma con credenziali IAM

La seguente policy concede un accesso principale IAM all'applicazione web e alle API AWS Transform utilizzando le credenziali IAM. Questa policy è necessaria per IAM-only l'accesso e per l'accesso IAM abilitato insieme a un provider di identità.

Sostituisci *region* e *profile-id* con i tuoi valori. *account-id* Puoi trovare l'ID del profilo nella console AWS Transform in Impostazioni.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowTransformAccess",  
      "Effect": "Allow",  
      "Action": "transform:AccessTransformProfile",  
      "Resource": "arn:aws:transform:region:account-id:profile/profile-id"  
    }  
  ]  
}
```

Per concedere l'accesso a tutti i profili di un account, usa un carattere jolly per l'ID del profilo:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowTransformAccessAllProfiles",  
      "Effect": "Allow",  
      "Action": "transform:AccessTransformProfile",  
      "Resource": "arn:aws:transform:region:account-id:profile/*"  
    }  
  ]  
}
```

 Note

L'azione `transform:AccessTransformProfile` consente l'accesso solo a AWS Transform. Le azioni all'interno delle aree di lavoro sono controllate dai ruoli dell'area di lavoro AWS Transform (amministratore, collaboratore, approvatore Read-only), non dalle politiche IAM. I ruoli di Workspace determinano ciò che un utente può fare, ad esempio creare posti di lavoro, gestire i collaboratori o approvare le attività.

Risoluzione dei problemi AWS Trasforma l'identità e l'accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS Transform e IAM.

Argomenti

- [Non sono autorizzato a eseguire un'azione in AWS Trasformazione](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere al mio AWS Trasforma le risorse](#)

Non sono autorizzato a eseguire un'azione in AWS Trasformazione

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa `my-example-widget` fittizia ma non dispone di autorizzazioni AWS Transform: `GetWidget` fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: AWS Transform: GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa `my-example-widget` utilizzando l'azione AWS Transform: `GetWidget`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'iam:PassRoleazione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a AWS Transform.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato marymajor tenta di utilizzare la console per eseguire un'azione in AWS Transform. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione iam:PassRole.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire l'accesso a persone esterne al mio Account AWS per accedere al mio AWS Trasforma le risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizzare tali policy per concedere alle persone l'accesso alle proprie risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Transform supporta queste funzionalità, consulta [In che modo AWS Transform funziona con IAM](#).

- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Utilizzo di ruoli collegati ai servizi per AWS Transform

AWS Transform utilizza ruoli collegati ai [servizi AWS Identity and Access Management](#) (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Transform Service-linked i ruoli sono predefiniti AWS Transform e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

Utilizzo di ruoli collegati ai servizi per AWS Transform

AWS Transform utilizza ruoli collegati ai [servizi AWS Identity and Access Management](#) (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Transform Service-linked i ruoli sono predefiniti AWS Transform e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

Un ruolo collegato al servizio semplifica la configurazione AWS Transform perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Transform definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Transform Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. In questo modo proteggi AWS Transform le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta [AWS i servizi che funzionano con IAM](#) e cerca i servizi con Sì nella colonna dei ruoli. Service-linked Scegliere Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Service-linked autorizzazioni di ruolo per AWS Transform

AWS Transform utilizza il ruolo collegato al servizio denominato [AWSServiceRoleForAWSTransform](#): questo Service-Linked ruolo offre a AWS Transform la capacità di fornire informazioni sull'utilizzo.

Il ruolo AWSServiceRoleForAWSTransform collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `transform.amazonaws.com`

La politica di autorizzazione dei ruoli denominata AWSServiceRoleForAWSTransform consente di AWS Transform completare le seguenti azioni sulle risorse specificate:

- `cloudwatch: PutMetricData`
 - Invia metriche personalizzate a for operations CloudWatch AWS Transform
 - Tieni traccia dei progressi della trasformazione, delle percentuali di successo e delle metriche delle prestazioni
 - Abilita il monitoraggio e la generazione di avvisi sui flussi di lavoro di trasformazione
- Inoltre: `DescribeApplication`
 - Visualizza i dettagli su un'applicazione specifica in Identity Center
 - Ottieni i metadati dell'applicazione come nome, descrizione, stato e configurazione
- Inoltre: `GetApplicationAssignmentConfiguration`
 - Recupera le impostazioni di configurazione delle assegnazioni per un'applicazione
 - Scopri come users/groups sono configurati per essere assegnati all'applicazione
- Inoltre: `ListApplicationAssignmentsForPrincipal`
 - Elenca tutte le applicazioni assegnate a un utente o gruppo specifico (principale)
 - Visualizza a quali applicazioni ha accesso una determinata identità
- Abilita la decrittografia dei KMS-encrypted dati in caso di accesso tramite IAM Identity Center. Funziona solo quando il contesto di crittografia contiene un ARN di istanza IAM Identity Center valido ed è necessario accedervi tramite gli endpoint del servizio IAM Identity Center.
- Consente la decrittografia dei KMS-encrypted dati in caso di accesso tramite Identity Store. Funziona solo quando il contesto di crittografia contiene un ARN Identity Store valido ed è necessario accedervi tramite gli endpoint del servizio Identity Store.
- `gestore dei segreti: GetSecretValue`

- Accedi ai segreti AWS Transform collegati ai servizi utilizzati per archiviare i segreti dei client per provider di identità esterni
- Risorsa: `arn:aws:secretsmanager:*:*:secret:transform-preprod!` *
- Condizione: deve essere di proprietà del servizio transform-preprod e deve essere accessibile dallo stesso account
- supporto:CreateCase, supporto:, supporto:DescribeCases, supporto:DescribeCommunications, supporto: AddCommunicationToCase ResolveCase
- Crea e gestisci casi di supporto premium dall'applicazione AWS Transform web
- Visualizza i dettagli e le comunicazioni dei casi
- Aggiungi comunicazioni e risolvi i casi di supporto

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta le [autorizzazioni dei Service-linked ruoli](#) nella Guida per l'utente IAM.

Creazione di un ruolo collegato ai servizi per AWS Transform

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un profilo per AWS Transform in AWS Management Console, AWS Transform crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando aggiorni le impostazioni, AWS Transform crea nuovamente il ruolo collegato al servizio.

Puoi anche utilizzare la console IAM o la AWS CLI per creare un ruolo collegato al servizio con il nome del servizio. `transform.amazonaws.com` Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, è possibile utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per AWS Transform

AWS Transform non consente di modificare il ruolo collegato al `AWSServiceRoleForAWSTransform` servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS Transform

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Note

Se il AWS Transform servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo `AWSServiceRoleForAWSTransform` collegato al servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Regioni supportate per AWS Transform ruoli collegati al servizio

AWS Transform non supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. È possibile utilizzare il `AWSServiceRoleForAWSTransform` ruolo nelle seguenti regioni. Per ulteriori informazioni, consulta [AWS Regions and endpoints](#).

Nome della Regione	Identità della Regione	Support in AWS Transform
Stati Uniti orientali (Virginia settentrionale)	us-east-1	Sì
Europa (Francoforte)	eu-central-1	Sì

Utilizzo di ruoli collegati ai servizi per AWS Trasforma personalizzata

AWS Transform Custom utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForAWSTransformCustom` per pubblicare metriche e log sul tuo account per tuo

conto. Queste metriche ti consentono di monitorare i conteggi delle trasformazioni, le latenze e i codici di stato direttamente nelle tue dashboard. I log forniscono visibilità sui problemi riscontrati durante le trasformazioni.

Questo [ruolo collegato al servizio](#) è predefinito da AWS Transform Custom e include solo le autorizzazioni necessarie al servizio. Non è necessario aggiungere manualmente alcuna autorizzazione e il ruolo può essere assunto solo da Transform Custom. AWS Per informazioni generali sui ruoli collegati ai servizi, consulta [Using service-linked roles](#) nella IAM User Guide.

Service-linked autorizzazioni di ruolo per AWS Trasforma personalizzata

Il ruolo `AWSServiceRoleForAWSTransformCustom` collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `transform-custom.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AWSServiceRoleForAWSTransformCustom` consente a AWS Transform Custom di completare le seguenti azioni sulle risorse specificate:

- `cloudwatch:PutMetricData` su tutte le risorse AWS
 - Pubblica le metriche operative in under the `AWS/TransformCustom` namespace
 - Tieni traccia del numero di trasformazioni, delle latenze e dei codici di stato
 - Limitato allo spazio dei `AWS/TransformCustom` nomi tramite la chiave `condition cloudwatch:namespace`
- `logs:CreateLogGroup` nel gruppo `logs:PutRetentionPolicy` di `log /aws/TransformCustom`
 - Crea il gruppo di CloudWatch log Logs per la pubblicazione dei log di trasformazione
 - Imposta le politiche di conservazione dei log nel gruppo di log
 - Previsto per `arn:aws:logs:*:*:log-group:/aws/TransformCustom` una `aws:ResourceAccount` condizione che garantisca l'accesso solo all'interno del tuo account
- `logs:CreateLogStream` `logs:PutLogEvents` sui flussi di log all'interno del `/aws/TransformCustom` gruppo di log
 - Crea flussi di log e pubblica eventi di log per le operazioni di trasformazione
 - Previsto per `arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*` una `aws:ResourceAccount` condizione che garantisca l'accesso solo all'interno del tuo account

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta le [autorizzazioni dei Service-linked ruoli nella Guida](#) per l'utente IAM.

Creazione di un ruolo collegato ai servizi per AWS Trasforma personalizzata

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando esegui una trasformazione utilizzando la CLI AWS Transform Custom, AWS Transform Custom crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando esegui una trasformazione utilizzando la CLI AWS Transform Custom, AWS Transform Custom crea nuovamente il ruolo collegato al servizio per te.

Puoi anche utilizzare la console IAM per creare un ruolo collegato al servizio con lo use case. `AWSServiceRoleForAWSTransformCustom` Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del servizio. `transform-custom.amazonaws.com` Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, è possibile utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per AWS Trasforma personalizzata

AWS Transform Custom non consente di modificare il ruolo `AWSServiceRoleForAWSTransformCustom` collegato al servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS Transform Custom

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente.

Il ruolo `AWSServiceRoleForAWSTransformCustom` collegato al servizio non crea risorse persistenti nel tuo account. Puoi eliminarlo direttamente senza alcuna pulizia delle risorse.

Se elimini questo ruolo e successivamente esegui una trasformazione utilizzando la CLI AWS Transform Custom, il ruolo collegato al servizio viene ricreato automaticamente.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al servizio.

AWSServiceRoleForAWSTransformCustom Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Regioni supportate per AWS Trasforma i ruoli personalizzati collegati ai servizi

AWS Transform Custom supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui AWS Transform Custom è disponibile. Per un elenco delle regioni supportate, consulta Regioni [supportate](#).

AWS politiche gestite per AWS Trasformazione

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. Le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando nel Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS Trasforma gli aggiornamenti per AWS policy gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per AWS Transform dal 1° marzo 2021.

Modifica	Descrizione	Data
AWSTransformInfrastructureExecutorAccessBatch : nuova policy	È stata aggiunta una nuova policy AWS gestita che concede le autorizzazioni necessarie per eseguire le	20 luglio 2026

Modifica	Descrizione	Data
	valutazioni e le trasformazioni di AWS Transform Continuous Modernization utilizzando AWS Batch, tra cui il caricamento del codice sorgente, il recupero dei risultati, il monitoraggio dello stato del processo Batch, la lettura dei log e la gestione delle pianificazioni di trasformazione.	
<u>AWSTransformInfrastructureExecutorAccessEC2</u> : nuova policy	È stata aggiunta una nuova policy AWS gestita che concede le autorizzazioni necessarie per eseguire valutazioni e trasformazioni di AWS Transform Continuous Modernization utilizzando Amazon EC2, tra cui il caricamento del codice sorgente, il recupero dei risultati, il monitoraggio dello stato dei lavori e la gestione dei piani di trasformazione.	20 luglio 2026

Modifica	Descrizione	Data
AWSTransformSecurityAgentExecutorAccess: nuova policy	È stata aggiunta una nuova policy AWS gestita che concede a AWS Transform Continuous Modernization le autorizzazioni necessarie per richiamare il servizio AWS Security Agent per le revisioni e la correzione automatizzate della sicurezza del codice, incluso il caricamento degli artefatti di scansione e il recupero dei risultati.	30 giugno 2026
AWSServiceRoleForAWSTransformCustom — Politica aggiornata	Sono state aggiunte CloudWatch le autorizzazioni di registro per consentire a AWS Transform custom di pubblicare i log nel gruppo di /aws/TransformCustom log del tuo account.	5 maggio 2026
AWSTransformCustomExecuteTransformations — Politica aggiornata	È stata aggiunta l'autorizzazione a creare il ruolo AWS Transform personalizzato collegato al servizio (AWSServiceRoleForAWSTransformCustom) per consentire l'emissione di CloudWatch metriche agli account dei clienti.	27 aprile 2026

Modifica	Descrizione	Data
AWSTransformCustomManageTransformations — Politica aggiornata	È stata aggiunta l'autorizzazione a creare il ruolo AWS Transform personalizzato collegato al servizio (AWSServiceRoleForAWSTransformCustom) per consentire l'emissione di CloudWatch metriche agli account dei clienti.	27 aprile 2026
AWSTransformCustomFullAccess — Politica aggiornata	È stata aggiunta l'autorizzazione a creare il ruolo AWS Transform personalizzato collegato al servizio (AWSServiceRoleForAWSTransformCustom) per consentire l'emissione di CloudWatch metriche agli account dei clienti.	7 aprile 2026
AWSServiceRoleForAWSTransformCustom : nuova policy	È stata aggiunta una nuova politica AWS gestita per il ruolo collegato al servizio personalizzato AWS Transform. Questa politica consente a AWS Transform custom di pubblicare e CloudWatch metriche sul tuo account.	23 marzo 2026
DBModProvisioningAndMigration : nuova policy	Questa politica garantisce funzionalità di provisioning e migrazione del database.	24 marzo 2026

Modifica	Descrizione	Data
DBModDiscoveryAndAssessment : nuova policy	È stata aggiunta una nuova policy AWS gestita che offre funzionalità complete di modernizzazione del database, scoperta e valutazione.	24 marzo 2026
AWSTransformCustomFullAccess : nuova policy	È stata aggiunta una nuova politica AWS gestita che fornisce l'accesso completo a AWS Transform custom.	5 dicembre 2025
AWSTransformCustomExecuteTransformations : nuova policy	È stata aggiunta una nuova policy AWS gestita che fornisce l'accesso per eseguire trasformazioni in AWS Transform custom.	5 dicembre 2025
AWSTransformCustomManageTransformations : nuova policy	È stata aggiunta una nuova policy AWS gestita che fornisce l'accesso alla creazione, all'aggiornamento, alla lettura e all'eliminazione delle risorse di AWS trasformazione in Transform custom, nonché all'esecuzione di trasformazioni.	5 dicembre 2025

Modifica	Descrizione	Data
AWSServiceRoleForAWSTransform — Politica aggiornata	Sono state aggiunte le autorizzazioni per accedere al segreto collegato al servizio AWS Transform utilizzato per archiviare il segreto del client per i provider di identità esterni. Sono state aggiunte le autorizzazioni per creare una richiesta di assistenza a premium dall'app web Transform. AWS	1 dicembre 2025
AWSTransformApplicationECSDeploymentPolicy — Politica aggiornata	Sono state aggiunte le autorizzazioni di ispezione dei ruoli IAM, la creazione di ruoli collegati al servizio ECS e le autorizzazioni KMS per il supporto della crittografia ECR.	22 novembre 2025
AWSTransformApplicationDeploymentPolicy — Politica aggiornata	Aggiunte le autorizzazioni di rete EC2, le autorizzazioni di ispezione dei ruoli IAM, le autorizzazioni per l'elenco dei bucket list di S3 e il supporto della crittografia KMS per funzionalità di implementazione avanzate.	22 novembre 2025
AWSServiceRoleForAWSTransform — Politica aggiornata	È stato aggiunto il supporto per le chiavi gestite dai clienti in IAM Identity Center.	17 settembre 2025

Modifica	Descrizione	Data
AWSTransformApplicationDeploymentPolicy : nuova policy	È stata aggiunta una nuova policy AWS gestita che consente a AWS Transform di distribuire applicazioni.NET trasformate creando e gestendo istanze Amazon EC2 CloudFormation , stack e risorse associate.	28 agosto 2025
AWSServiceRoleForAWSTransform — Policy aggiornata	È stata aggiunta una nuova politica.	15 maggio 2025

AWS politica gestita: AWSServiceRoleForAWSTransform

Questa politica è allegata al ruolo [AWSServiceRoleForAWSTransform](#) collegato al servizio (SLR).

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle autorizzazioni della policy, consulta [AWSServiceRoleForAWSTransform](#) la AWS Managed Policy Reference Guide.

AWS politica gestita: AWSServiceRoleForAWSTransformCustom

Questa politica è allegata al ruolo [AWSServiceRoleForAWSTransformCustom](#) collegato al servizio (SLR). Questo ruolo consente a AWS Transform custom di pubblicare CloudWatch metriche e registri sul tuo account per tuo conto.

Descrizione

Questa policy include le seguenti autorizzazioni:

- Amazon CloudWatch: consente di pubblicare le metriche nel CloudWatch AWS/TransformCustom namespace. Ciò consente il monitoraggio del numero di trasformazioni, delle latenze e dei codici di stato nei dashboard. CloudWatch

- Amazon CloudWatch Logs: consente di creare gruppi di log, flussi di log, impostare politiche di conservazione e pubblicare eventi di log nel gruppo di /aws/TransformCustom log. Ciò fornisce visibilità sui problemi riscontrati durante le trasformazioni.

AWS politica gestita: AWSTransformApplicationDeploymentPolicy

Questa policy consente a AWS Transform di distribuire applicazioni.NET trasformate creando e gestendo istanze Amazon EC2 CloudFormation , stack e risorse associate.

Descrizione

Questa policy include le seguenti autorizzazioni:

- CloudFormation— Consente di creare, aggiornare, eliminare e descrivere CloudFormation stack con nomi che iniziano con AWS Transform. Le operazioni dello stack sono limitate alle risorse contrassegnate con CreatedBy: AWSTransform e limitate allo stesso account. AWS
- Amazon EC2: consente di descrivere VPC, sottoreti, gruppi di sicurezza, immagini, istanze, tabelle di routing e gateway Internet. Consente l'esecuzione, l'avvio, l'arresto, la chiusura e la modifica delle istanze EC2, ma solo su richiesta. CloudFormation La creazione di tag è limitata a specifiche chiavi di tag consentite e solo durante le operazioni. CloudFormation
- AWS Identity and Access Management (IAM): consente di ottenere e passare ruoli IAM specifici per le istanze di distribuzione AWS Transform. Include le autorizzazioni per esaminare le politiche e gli allegati dei ruoli. L'accesso è limitato allo stesso account. AWS
- Amazon EC2 Systems Manager (SSM): consente di recuperare i parametri AMI Amazon Linux dall'archivio di parametri gestito e di AWS inviare comandi alle istanze. AWSTransform-tagged
- Amazon S3: consente la gestione degli oggetti nei bucket di distribuzione AWS Transform, inclusi i bucket di elenco e l'individuazione delle posizioni dei bucket all'interno dello stesso account. AWS
- AWS Key Management Service (KMS): consente operazioni di crittografia e decrittografia utilizzando chiavi KMS contrassegnate per AWSTransform, con restrizioni all'utilizzo dei servizi S3 ed EC2.

La policy implementa l'accesso con privilegi minimi tramite autorizzazioni a livello di risorsa, condizioni basate su tag, utilizzo di restrizioni di controllo del servizio, restrizioni a livello di account e dichiarazioni di negazione esplicite per impedire modifiche non autorizzate dei tag al di fuori delle operazioni. aws:CalledVia CloudFormation

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle [AWSTransformApplicationDeploymentPolicy](#) autorizzazioni delle policy AWS , consulta la Managed Policy Reference Guide.

AWS politica gestita: AWSTransformApplicationECSDeploymentPolicy

Questa policy consente a AWS Transform di distribuire applicazioni trasformate in Amazon ECS creando e gestendo cluster ECS, servizi, attività e risorse associate.

Descrizione

Questa policy include le seguenti autorizzazioni:

- CloudFormation— Consente di creare, aggiornare, eliminare e descrivere gli CloudFormation stack con nomi che iniziano con AWSTransform. Le operazioni dello stack sono limitate alle risorse contrassegnate con CreatedBy: AWSTransform e limitate allo stesso account. AWS
- Amazon ECS: consente di creare, aggiornare ed eliminare cluster ECS, servizi e definizioni di attività. Consente l'esecuzione di attività, l'elenco delle attività e la descrizione dello stato delle attività. Tutte le operazioni sono limitate alle risorse con nomi che iniziano con AWSTransform e contrassegnati con: AWSTransform. CreatedBy
- AWS Identity and Access Management (IAM): consente di ottenere e passare ruoli IAM specifici per le attività ECS (e). AWSTransform-Deploy-ECS-Task-Role AWSTransform-Deploy-ECS-Execution-Role Include le autorizzazioni per esaminare le politiche relative ai ruoli e creare il ruolo collegato ai servizi ECS quando necessario.
- Amazon CloudWatch Logs: consente di creare, eliminare e gestire gruppi di log con nomi che iniziano con //AWSTransform. aws/ecs Consente di recuperare gli eventi di registro per la risoluzione dei problemi delle applicazioni distribuite.
- Amazon ECR: consente di creare repository di contenitori con nomi che iniziano con awstransform per l'archiviazione delle immagini dei contenitori delle applicazioni.
- AWS Key Management Service (KMS): consente di creare sovvenzioni e generare chiavi dati per la crittografia ECR quando si utilizzano chiavi KMS gestite dal cliente.

La policy implementa l'accesso con privilegi minimi tramite autorizzazioni a livello di risorsa, condizioni basate su tag e restrizioni a livello di account per garantire che le operazioni siano limitate alle risorse all'interno dello stesso account. AWSTransform-managed AWS

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle autorizzazioni delle policy, consulta la Managed Policy Reference Guide. [AWSTransformApplicationECSDeploymentPolicy](#) AWS

AWS politica gestita: AWSTransformCustomFullAccess

Questa politica fornisce l'accesso completo a AWS Transform custom.

Descrizione

Questa policy include le seguenti autorizzazioni:

- AWS Transform Custom: consente tutte le azioni su tutte le risorse personalizzate AWS Transform. Ciò fornisce un accesso amministrativo completo al servizio.
- AWS Identity and Access Management (IAM): consente di creare il [ruolo personalizzato AWS Transform collegato al servizio](#) (`AWSServiceRoleForAWSTransformCustom`). Questo ruolo è necessario per consentire a AWS Transform custom di emettere CloudWatch metriche e log sul tuo account. L'autorizzazione ha lo scopo di consentire solo la creazione di questo ruolo specifico collegato al servizio.

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle autorizzazioni della policy, consulta [AWSTransformCustomFullAccess](#) la AWS Managed Policy Reference Guide.

AWS politica gestita: AWSTransformCustomExecuteTransformations

Questa politica fornisce l'accesso per eseguire trasformazioni in AWS Transform custom.

Descrizione

Questa policy include le seguenti autorizzazioni:

- AWS Transform Custom: consente lo streaming di conversazioni, l'esecuzione di trasformazioni e la gestione di campagne. Include le autorizzazioni per ottenere i dettagli della campagna, aggiornare lo stato dell'archivio delle campagne e aggiornare le campagne.
- AWS Identity and Access Management (IAM): consente di creare il ruolo personalizzato AWS Transform [collegato al servizio](#) (`AWSServiceRoleForAWSTransformCustom`). Questo ruolo è necessario per consentire a AWS Transform custom di emettere CloudWatch metriche e log sul tuo account. L'autorizzazione ha lo scopo di consentire solo la creazione di questo ruolo specifico collegato al servizio.

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle autorizzazioni della policy, consulta

[AWSTransformCustomExecuteTransformations](#) la AWS Managed Policy Reference Guide.

AWS politica gestita: AWSTransformCustomManageTransformations

Questa politica fornisce l'accesso alla creazione, all'aggiornamento, alla lettura e all'eliminazione delle risorse di AWS trasformazione in Transform custom, nonché all'esecuzione di trasformazioni.

Descrizione

Questa policy include le seguenti autorizzazioni:

- **AWS Transform Custom:** consente la gestione completa delle risorse di trasformazione, tra cui lo streaming di conversazioni, l'esecuzione di trasformazioni e la gestione dei pacchetti di trasformazione. Consente di creare, ottenere ed eliminare gli URL dei pacchetti di trasformazione e completare i caricamenti dei pacchetti.
- **Gestione della conoscenza:** consente di elencare, ottenere, eliminare e aggiornare gli elementi della conoscenza e le relative configurazioni e lo stato.
- **Gestione delle campagne:** consente di ottenere i dettagli della campagna, aggiornare lo stato dell'archivio delle campagne e aggiornare le campagne.
- **Etichettatura delle risorse:** consente di elencare, aggiungere e rimuovere tag per le risorse personalizzate AWS Transform.
- **AWS Identity and Access Management (IAM):** consente di creare il [ruolo collegato al servizio personalizzato AWS Transform](#) (). `AWSServiceRoleForAWSTransformCustom` Questo ruolo è necessario per consentire a AWS Transform custom di emettere CloudWatch metriche e log sul tuo account. L'autorizzazione ha lo scopo di consentire solo la creazione di questo ruolo specifico collegato al servizio.

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle autorizzazioni della policy, consulta

[AWSTransformCustomManageTransformations](#) la AWS Managed Policy Reference Guide.

AWS politica gestita: AWSTransformInfrastructureExecutorAccessBatch

Questa politica concede le autorizzazioni necessarie per eseguire le valutazioni e le trasformazioni di AWS Transform Continuous Modernization utilizzando Batch. AWS Collega questa policy a un ruolo

IAM nel tuo account. La CLI e l'agente AWS Transform Continuous Modernization assumono questo ruolo per caricare il codice sorgente, recuperare i risultati, monitorare lo stato dei processi Batch, leggere i log e gestire i piani di trasformazione.

Descrizione

Questa policy include le seguenti autorizzazioni:

- AWS Lambda: consente di richiamare e recuperare la configurazione di funzioni atx Lambda con prefisso che orchestrano il flusso di lavoro di trasformazione.
- Amazon S3: consente di caricare il codice sorgente in `atx-source-code-*` bucket e scaricare i risultati della trasformazione da bucket `atx-custom-output-*` e `atx-ct-output-*`
- AWS Key Management Service (KMS): consente la crittografia e la decrittografia dei dati utilizzando la chiave di crittografia Transform (). `AWS alias/atx-encryption-key`
- Amazon CloudWatch Logs: consente di leggere gli eventi dei log di esecuzione dei processi Batch e Lambda per il monitoraggio e il debug della trasformazione.
- Amazon CloudWatch: consente di ottenere ed elencare la dashboard della CLI AWS Transform per la visibilità operativa.
- AWS Batch: consente di descrivere ed elencare gli ambienti di elaborazione, le code di lavoro, le definizioni dei processi e lo stato dei processi.
- CloudFormation— Consente di descrivere ed elencare gli stack dell'infrastruttura AWS Transform per verificare lo stato dell'implementazione.
- API Resource Groups Tagging: consente di recuperare risorse con tag per scoprire l'infrastruttura AWS Transform nel tuo account.
- AWS Secrets Manager— Consente di recuperare e descrivere i segreti di AWS Transform memorizzati nel prefisso. `atx/`
- Amazon EventBridge Scheduler: consente di gestire i lavori di trasformazione pianificati all'interno del gruppo di `atx-ct` pianificazione.
- Amazon EC2: consente di descrivere la configurazione di VPC, sottorete, gruppo di sicurezza, tabella di routing e gateway NAT per la rete dell'ambiente di calcolo Batch.
- AWS Identity and Access Management (IAM): consente di leggere le configurazioni di ruolo con ATX prefisso e Atx prefisso per convalidare la configurazione dell'infrastruttura e passarle ad `AtxSchedulerInvocationRole` Amazon EventBridge Scheduler in modo che possa richiamare lavori pianificati.

La policy implementa l'accesso con privilegi minimi tramite autorizzazioni a livello di risorsa, condizioni basate su tag, la condizione e condizioni con ambito di servizio per garantire che le operazioni siano limitate alle risorse Transform all'interno dello stesso account.

```
aws:ResourceAccount iam:PassedToService AWS AWS
```

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle autorizzazioni della policy, consulta la [Managed Policy Reference Guide](#). [AWSTransformInfrastructureExecutorAccessBatch](#) AWS

AWS politica gestita: AWSTransformInfrastructureExecutorAccessEC2

Questa policy concede le autorizzazioni necessarie per eseguire valutazioni e trasformazioni di AWS Transform Continuous Modernization utilizzando Amazon EC2. Collega questa policy a un ruolo IAM nel tuo account. La CLI e l'agente AWS Transform Continuous Modernization assumono questo ruolo per caricare il codice sorgente, recuperare i risultati, monitorare lo stato dei lavori e gestire i piani di trasformazione.

Descrizione

Questa policy include le seguenti autorizzazioni:

- **CloudFormation**— Consente di descrivere gli stack dell'infrastruttura AWS Transform, gli eventi degli stack, le risorse dello stack e lo stato di rilevamento delle deviazioni, elencare gli stack e convalidare i modelli prima dell'implementazione. `CloudFormation`
- **Amazon EC2**: consente di descrivere istanze, AMI, VPC, sottoreti, gruppi di sicurezza, coppie di chiavi, tabelle di routing, gateway NAT e gateway Internet. Consente l'avvio e l'arresto delle istanze EC2 contrassegnate con. `atx-remote-infra: true`
- **Amazon EC2 Systems Manager (SSM)**: consente il monitoraggio dello stato di esecuzione dei comandi e l'esecuzione di comandi e sessioni AWS Transform-tagged sulle istanze, inclusa l'esecuzione del documento. `AWS-RunShellScript`
- **Amazon S3**: consente di gestire il codice sorgente e gli artefatti di output nei bucket AWS Transform, incluso il recupero, l'inserimento e l'eliminazione di oggetti e i bucket di elenchi.
- **AWS Key Management Service (KMS)**: consente la crittografia e la decrittografia dei dati utilizzando la chiave di crittografia Transform (). `AWS alias/atx-encryption-key`
- **AWS Secrets Manager**— Consente di recuperare e descrivere i segreti di trasformazione, come le credenziali del repository, archiviate sotto il prefisso. `atx/`

- Amazon EventBridge Scheduler: consente di gestire i lavori di trasformazione pianificati all'interno del gruppo di `atx-ct` pianificazione.
- API Resource Groups Tagging: consente di recuperare risorse con tag per scoprire l'infrastruttura AWS Transform nel tuo account.
- AWS Identity and Access Management (IAM): consente di passare il `atx-transform-role*` ruolo ad Amazon EC2 e poi ad `AtxSchedulerInvocationRole` Amazon EventBridge Scheduler e di leggere la configurazione del ruolo e del profilo dell'istanza per le istanze EC2.

La policy implementa l'accesso con privilegi minimi tramite autorizzazioni a livello di risorsa, condizioni basate su tag, condizioni e condizioni con ambito di servizio per garantire che le operazioni siano limitate alle risorse Transform all'`aws:ResourceAccount` interno dello stesso account.

`iam:PassedToService` AWS AWS

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle autorizzazioni della policy, consulta la [Managed Policy Reference Guide](#). [AWSTransformInfrastructureExecutorAccessEC2](#) AWS

AWS politica gestita: `AWSTransformSecurityAgentExecutorAccess`

Questa politica concede a AWS Transform Continuous Modernization le autorizzazioni necessarie per richiamare il servizio AWS Security Agent per le revisioni e la correzione automatizzate della sicurezza del codice. Associa questa policy a un ruolo IAM nel tuo account che la CLI e l'agente di AWS Transform Continuous Modernization assumono per caricare gli artefatti di scansione e recuperare i risultati.

Descrizione

Questa policy include le seguenti autorizzazioni:

- AWS Security Agent: consente di elencare gli spazi degli agenti, creare revisioni del codice, avviare lavori di revisione del codice, elencare e recuperare i risultati e avviare la correzione del codice. Queste azioni riguardano solo gli spazi degli agenti presenti nel tuo account.
- Amazon S3: consente di scaricare i risultati e i risultati della scansione dal `kct-security-agent-*` bucket e di caricare il codice sorgente per la scansione di sicurezza nel `security-scans/*` prefisso all'interno del bucket.
- AWS Identity and Access Management (IAM): consente di passare il `security-agent-*` ruolo al servizio AWS Security Agent in modo che possa eseguire la scansione.

La policy implementa l'accesso con privilegi minimi tramite autorizzazioni a livello di risorsa, bucket S3 e prefissi chiave, `s3:ResourceAccount` condizioni and e una condizione con ambito di servizio per garantire che le operazioni siano limitate alle risorse di `aws:ResourceAccount` Security Agent all'interno dello stesso account `iam:PassedToService`. AWS AWS

Dettagli delle autorizzazioni

Per visualizzare i dettagli [AWSTransformSecurityAgentExecutorAccess](#) sulle autorizzazioni delle policy, AWS consulta la Managed Policy Reference Guide.

AWS politica gestita: DBModDiscoveryAndAssessment

Questa policy offre funzionalità complete di modernizzazione del database, scoperta e valutazione per AWS Transform.

Descrizione

Questa policy include le seguenti autorizzazioni:

- Amazon EC2: consente di descrivere i componenti dell'infrastruttura tra cui istanze, VPC, sottoreti, gruppi di sicurezza, zone di disponibilità, endpoint VPC e gateway Internet.
- Amazon RDS: consente di descrivere istanze di database, cluster e gruppi di sottoreti. Consente di modificare i gruppi di sottoreti DB all'interno dello stesso account per la preparazione della migrazione. AWS
- Amazon RDS Data API: consente di abilitare e disabilitare gli endpoint HTTP e l'esecuzione di istruzioni SQL su cluster di database etichettati per il progetto di modernizzazione del database.
- AWS DMS— Consente di descrivere endpoint, istanze di replica, attività, sottoreti e istanze ordinabili. Consente di elencare fornitori di dati, profili di istanza e progetti di migrazione. Consente di descrivere le statistiche delle tabelle, le esecuzioni di valutazione e le operazioni dei modelli di metadati. Le operazioni dettagliate di descrizione e metadati sono limitate alle risorse contrassegnate per il progetto di modernizzazione del database.
- — Consente di elencare i segreti per scoprire le credenziali del database.
- AWS Identity and Access Management (IAM): consente di ispezionare ruoli di AWS DMS servizio specifici e le relative politiche associate. Include l'accesso alle policy AWS gestite in AWS DMS lettura.
- AWS Key Management Service (KMS): consente di elencare gli alias delle chiavi e descriverle. Consente la decrittografia dei segreti tramite l'integrazione, limitata allo stesso account. AWS

La policy implementa l'accesso con privilegi minimi tramite autorizzazioni a livello di risorsa, condizioni basate su tag e restrizioni a livello di account per garantire che le operazioni siano limitate alle risorse del progetto di modernizzazione del database all'interno dello stesso account. AWS

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle autorizzazioni delle policy, consulta la Managed Policy Reference Guide. [DBModDiscoveryAndAssessment](#) AWS

AWS politica gestita: DBModProvisioningAndMigration

Questa policy fornisce funzionalità di provisioning e migrazione del database per i progetti di modernizzazione del database AWS Transform. Include le autorizzazioni per creare e gestire l'infrastruttura di migrazione, fornire database di destinazione e archiviare i dati di migrazione.

Descrizione

Questa policy include le seguenti autorizzazioni:

- AWS DMS— Consente di creare e gestire sottoreti di replica, profili di istanze, fornitori di dati, progetti di migrazione, endpoint, istanze di replica e attività di replica. Include operazioni di conversione dello schema come l'importazione, la conversione, l'esportazione e la valutazione del modello di metadati. Consente la gestione del ciclo di vita delle istanze di replica (creazione, eliminazione, modifica, riavvio) e delle attività di replica (eliminazione, avvio, arresto, valutazione). Tutte le operazioni di scrittura sono limitate alle risorse contrassegnate per il progetto di modernizzazione del database.
- Amazon RDS: consente di creare sottoreti di database, cluster di database e istanze di database. Tutte le risorse devono essere contrassegnate per il progetto di modernizzazione del database.
- — Consente di creare, aggiornare e contrassegnare segreti con il prefisso di denominazione per la modernizzazione del database. Consente di recuperare valori segreti e descrivere i segreti per le risorse con tag.
- Amazon S3: consente di creare e gestire bucket e oggetti S3 per lo storage dei dati di migrazione. Include operazioni di etichettatura dei bucket, controllo delle versioni e ciclo di vita degli oggetti. Limitato ai bucket con il prefisso di denominazione per la modernizzazione del database.
- AWS Identity and Access Management (IAM): consente il trasferimento di ruoli di AWS DMS servizio specifici a servizi di conversione dello schema AWS DMS e la relativa conversione. Consente di creare il ruolo collegato al servizio Amazon RDS necessario per le operazioni del database.

La policy implementa l'accesso con privilegi minimi tramite autorizzazioni a livello di risorsa, condizioni basate su tag e restrizioni a livello di account per garantire che le operazioni siano limitate alle risorse del progetto di modernizzazione del database all'interno dello stesso account. AWS

Dettagli delle autorizzazioni

Per visualizzare i dettagli sulle autorizzazioni delle policy, consulta la Managed Policy Reference Guide. [DBModProvisioningAndMigration](#) AWS

AWS Riferimento alle autorizzazioni di trasformazione

Questa sezione fornisce informazioni sulle API utilizzate da AWS Transform e sul loro funzionamento.

Argomenti

- [AWS Trasforma le API](#)

AWS Trasforma le API

- `trasforma: BatchGetMessage`
- `trasformare: BatchGetUserDetails`
- `trasformare: CompleteArtifactUpload`
- `trasformare: CreateArtifactDownloadUrl`
- `trasformare: CreateArtifactUploadUrl`
- `trasformare: CreateAssetDownloadUrl`
- `trasformare: CreateConnector`
- `trasformare: CreateFeedback`
- `trasformare: CreateJob`
- `trasformare: CreateSession`
- `trasformare: CreateWorkspace`
- `trasformare: DeleteConnector`
- `trasformare: DeleteJob`
- `trasformare: DeleteSelfRoleMappings`
- `trasformare: DeleteUserRoleMappings`
- `trasformare: DeleteWorkspace`

- trasformare: DetectIsAllowedForOperation
- trasformare: GetConnector
- trasformare: GetFeedbackQuestions
- trasformare: GetHitITask
- trasformare: GetJob
- trasformare: GetLoginRedirectUri
- trasformare: GetUserDetails
- trasformare: GetUserPreferences
- trasformare: GetWebAppUrl
- trasformare: GetWorkspace
- trasformare: ListArtifacts
- trasformare: ListConnectors
- trasformare: ListHitITasks
- trasformare: ListJobPlanSteps
- trasformare: ListJobs
- trasformare: ListMessages
- trasformare: ListPlanUpdates
- trasformare: ListUserRoleMappings
- trasformare: ListWorklogs
- trasformare: ListWorkspaces
- trasformare: PutUserPreferences
- trasformare: PutUserRoleMappings
- trasformare: RevokeSession
- trasformare: SearchUsers
- trasformare: SearchUsersTypeahead
- trasformare: SendMessage
- trasformare: StartJob
- trasformare: StopJob
- trasformare: SubmitCriticalHitITask

- trasformare: SubmitStandardHitITask
- trasformare: TestReleaseTraitPreProd
- trasformare: TestReleaseTraitProd
- trasformare: UpdateHitITask
- trasformare: UpdateJob
- trasformare: UpdateWorkspace
- trasformare: VerifySession

Convalida della conformità per AWS Trasformazione

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione [Scope by Compliance Program Servizi AWS](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la [Documentazione AWS sulla sicurezza](#).

Resilienza in AWS Trasformazione

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

[Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS](#)

Oltre all'infrastruttura AWS globale, AWS Transform offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati.

AWS Transform e endpoint di interfaccia (AWS PrivateLink)

Puoi stabilire una connessione privata tra il tuo VPC e creare un AWS Transform endpoint VPC di interfaccia. Gli endpoint di interfaccia sono alimentati da [AWS PrivateLink](#), una tecnologia che consente di accedere in modo privato alla AWS Transform console senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect Il traffico tra il tuo VPC e AWS Transform non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più [interfacce di rete elastiche](#) nelle sottoreti.

Per ulteriori informazioni, consultare [Endpoint VPC di interfaccia \(AWS PrivateLink\)](#) nella Guida per l'utente di Amazon VPC.

Note

Per la PrivateLink documentazione AWS Transform personalizzata, consulta [AWS Transform endpoint personalizzati e di interfaccia \(AWS PrivateLink\)](#).

Considerazioni per AWS Transform Endpoint VPC

Prima di configurare un endpoint VPC di interfaccia per AWS Transform, assicurati di esaminare le [proprietà e le limitazioni degli endpoint dell'interfaccia nella](#) Amazon VPC User Guide.

Prerequisiti

Prima di iniziare una qualsiasi delle procedure sottostanti, assicurati di disporre di quanto riportato di seguito:

- Un AWS account con le autorizzazioni appropriate per creare e configurare risorse.
- Un VPC già creato nel tuo AWS account.
- Familiarità con AWS i servizi, in particolare Amazon AWS Transform VPC e.

Creazione di un endpoint VPC di interfaccia per AWS Transform

Puoi creare un endpoint VPC per il AWS Transform servizio utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consultare [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di Amazon VPC.

AWS Transform supporta i seguenti servizi endpoint VPC:

Nome del servizio	Endpoint	Nota
Piano di controllo	com.amazonaws. <i>region</i> .transform	
API Agentic	com.amazonaws. <i>region</i> .transform-agents	
Applicazione Web	com.amazonaws. <i>region</i> .api.transform	Richiesto per l'applicazione AWS Transform web. Questo endpoint deve avere il DNS privato abilitato (l'opzione Abilita nome DNS) in modo che api.transform. <i>region</i> .on.aws si risolva in un indirizzo IP privato nel tuo VPC.

Sostituiscilo *region* con la AWS regione in cui è installato il tuo AWS Transform profilo, ad esempio com.amazonaws.us-east-1.transform.

Note

Se utilizzi l'applicazione web, l'endpoint è obbligatorio. AWS Transform api.transform Per la guida completa alla configurazione, vedere [Accesso al AWS Transform applicazione web da un VPC](#).

Per ulteriori informazioni, consulta [Regioni supportate per AWS Transform](#) [Accesso a un servizio tramite un endpoint di interfaccia](#) nella Amazon VPC User Guide.

Utilizzo di un computer locale per connettersi a un AWS Transform endpoint

Questa sezione descrive il processo di utilizzo di un computer locale a cui connettersi AWS Transform tramite un AWS PrivateLink endpoint nel AWS VPC.

1. [Crea una connessione VPN tra il dispositivo on-premises e il VPC.](#)
2. [Crea un endpoint VPC di interfaccia per. AWS Transform](#)
3. [Configura un endpoint Amazon Route 53 in entrata.](#) Ciò ti consentirà di utilizzare il nome DNS del tuo AWS Transform endpoint dal tuo dispositivo locale.

Accesso al AWS Transform applicazione web da un VPC

Quando si utilizza AWS PrivateLink per accedere all' AWS Transform API in modo privato dal VPC, l'applicazione Web richiede una configurazione di rete aggiuntiva. Fornisce contenuti statici (HTML JavaScript, CSS) tramite i quali è necessaria CloudFront la connettività Internet. Le chiamate API dall'applicazione Web passano attraverso l'endpoint VPC e rimangono completamente private.

Questa guida mostra come configurare l'uscita Internet controllata dal tuo VPC in modo che l'applicazione web possa caricarsi mantenendo il VPC bloccato solo sui domini richiesti.

Come funziona

L'applicazione AWS Transform web utilizza due percorsi di rete:

- Chiamate API: quando interagite con l'applicazione Web (avvio di lavori, visualizzazione delle aree di lavoro e così via), il browser invia le richieste API `aapi.transform.region.on.aws`. Con l'endpoint `com.amazonaws.region.api.transform` VPC e il DNS privato abilitati, queste richieste vengono risolte in un indirizzo IP privato nel tuo VPC e non escono mai dalla rete. AWS
- Contenuto statico: i file HTML e CSS dell'applicazione Web vengono forniti tramite JavaScript CloudFront `tenant-id.transform.region.on.aws`. Il caricamento di questi file richiede la connettività a Internet, poiché la distribuzione CloudFront dei contenuti è disponibile solo sulla rete Internet pubblica.
- Autenticazione: vengono utilizzati i flussi di accesso di AWS IAM Identity Center `region.signin.aws`, che richiedono anche la connettività Internet.

Per abilitare l'applicazione Web mantenendo la sicurezza, è possibile creare un percorso di uscita controllato utilizzando AWS Network Firewall con filtro basato sul dominio. Ciò consente al VPC di

raggiungere solo i domini specifici richiesti dall'applicazione Web bloccando tutto il resto del traffico Internet.

Architecture

Il diagramma seguente mostra il percorso di rete per il traffico delle applicazioni 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

Il Network Firewall deve vedere entrambe le direzioni del traffico (routing simmetrico) per eseguire l'ispezione TLS SNI. È necessario configurare un percorso di ritorno nella sottorete NAT Gateway che invii il traffico destinato alla sottorete privata attraverso il firewall. In caso contrario, le regole di filtraggio basate sul dominio non funzioneranno.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un AWS account con autorizzazioni per creare risorse VPC, Network Firewall e gateway NAT.
- Un VPC con una sottorete privata in cui vengono eseguite le istanze o i carichi di lavoro.

- Un gateway Internet collegato al VPC (o le autorizzazioni per crearne uno).
- Un endpoint AWS Transform VPC per `com.amazonaws.region.api.transform` con DNS privato abilitato. Questo è l'endpoint utilizzato dal client del browser dell'applicazione Web. Per istruzioni sulla creazione di endpoint, vedere. [AWS Transform e endpoint di interfaccia \(AWS PrivateLink\)](#)

Configurazione della policy degli endpoint VPC

Se il tuo endpoint `com.amazonaws.region.api.transform` VPC ha una policy endpoint personalizzata, devi aggiungere un'istruzione che consenta le operazioni. AWS Transform In caso contrario, l'applicazione Web non sarà in grado di effettuare chiamate API tramite l'endpoint.

Aggiungi la seguente dichiarazione alla tua policy sugli endpoint VPC. Sostituisci `AWS_TRANSFORM_PROFILE_ARN` con il tuo profilo di AWS Transform servizio ARN, che puoi trovare nella AWS Transform console nella pagina Impostazioni.

```
{
  "Statement": [
    {
      "Sid": "AllowAWSTransform",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalArn": [
            "AWS_TRANSFORM_PROFILE_ARN"
          ]
        }
      }
    }
  ]
}
```

Note

Se il tuo endpoint VPC utilizza la policy predefinita (accesso completo), non sono necessarie modifiche e puoi saltare questo passaggio.

Configurazione dell'uscita controllata da Internet

Completa i seguenti passaggi per configurare Network Firewall con filtri basati sul dominio per l' AWS Transform applicazione Web.

Passaggio 1: Creare la sottorete del firewall

Crea una piccola sottorete /28 dedicata all'endpoint Network Firewall. Questa sottorete deve trovarsi nella stessa zona di disponibilità della sottorete privata.

```
aws ec2 create-subnet \  
  --vpc-id your-vpc-id \  
  --cidr-block firewall-subnet-cidr \  
  --availability-zone your-az \  
  --region region
```

Fase 2: Creare una sottorete pubblica per il gateway NAT

```
aws ec2 create-subnet \  
  --vpc-id your-vpc-id \  
  --cidr-block public-subnet-cidr \  
  --availability-zone your-az \  
  --region region
```

Fase 3: Configurare la tabella di routing della sottorete pubblica

Crea una tabella di routing per la sottorete pubblica che indirizza il traffico Internet verso il gateway 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 igw-xxxxxx \  
  --region region
```

```
--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
```

Fase 4: Creare il gateway NAT

```
# Allocate an Elastic IP  
EIP=$(aws ec2 allocate-address --domain vpc \  
  --region region --query 'AllocationId' --output text)  
  
# Create NAT Gateway in the public subnet  
NAT_ID=$(aws ec2 create-nat-gateway \  
  --subnet-id public-subnet-id \  
  --allocation-id $EIP \  
  --region region \  
  --query 'NatGateway.NatGatewayId' --output text)  
  
# Wait for NAT Gateway to become available (~2 minutes)  
aws ec2 wait nat-gateway-available \  
  --nat-gateway-ids $NAT_ID --region region
```

Passaggio 5: Creare il gruppo di regole Network Firewall

Crea un gruppo di regole statico che consenta il traffico solo verso i domini richiesti dall' AWS Transform applicazione Web.

```
aws network-firewall create-rule-group \  
  --rule-group-name transform-webapp-domains \  
  --type STATEFUL \  
  --capacity 100 \  
  --rule-group '{
```

```

"StatefulRuleOptions": {
  "RuleOrder": "STRICT_ORDER"
},
"RulesSource": {
  "RulesSourceList": {
    "Targets": [
      ".cloudfront.net",
      ".transform.region.on.aws",
      "region.signin.aws",
      ".s3.region.amazonaws.com",
      "oidc.region.amazonaws.com",
      "portal.sso.region.amazonaws.com",
      "assets.sso-portal.region.amazonaws.com",
      "directory-id.awsapps.com"
    ],
    "TargetTypes": ["TLS_SNI", "HTTP_HOST"],
    "GeneratedRulesType": "ALLOWLIST"
  }
}
}' \
--region region

```

region Sostituiscilo con la AWS regione in cui è installato il tuo AWS Transform profilo (ad esempio, `us-east-1`). Sostituiscilo *directory-id* con il tuo ID di directory IAM Identity Center (ad esempio, `d-1234567890`). Puoi trovare l'ID della tua directory nella console IAM Identity Center.

La tabella seguente spiega i domini consentiti.

Dominio	Scopo
<code>.cloudfront.net</code>	CloudFront CDN: fornisce risorse statiche delle applicazioni Web (CSS/JavaScript, immagini)
<code>.transform. <i>region</i>.on.aws</code>	URL del tenant dell'applicazione Web: il browser carica la pagina iniziale da questo dominio tramite CloudFront
<code><i>region</i>.signin.aws</code>	Pagina di reindirizzamento dell'accesso SSO
<code>.s3.<i>region</i>.amazonaws.com</code>	URL predefiniti S3: caricamenti e download di artefatti
<code>oidc.<i>region</i>.amazonaws.com</code>	Scambio di token OIDC per l'autenticazione SSO

Dominio	Scopo
portal.sso. <i>region</i> .amazonaws.com	Pagina di accesso al portale SSO
assets.sso-portal. <i>region</i> .amazonaws.com	Risorse statiche del portale SSO (CSS,) JavaScript
<i>directory-id</i> .awsapps.com	Portale IAM Identity Center per la tua organizzazione

Note

La `.cloudfront.net` wildcard consente il traffico verso qualsiasi CloudFront distribuzione, non solo verso l'applicazione AWS Transform web. Un filtro di dominio più ristretto non è possibile perché gli IP CloudFront edge sono condivisi tra le distribuzioni e l'ispezione TLS SNI non è in grado di distinguere le singole distribuzioni all'interno dello stesso dominio.

Note

Le chiamate API devono essere eseguite `api.transform.region.on.aws` AWS PrivateLink e non richiedono l'uscita da Internet. Non sono influenzate dal firewall.

Fase 6: Creare la politica del firewall

La policy deve utilizzare la valutazione delle STRICT_ORDER regole con `drop_established` come azione predefinita. Ciò garantisce che tutto il traffico che non corrisponde alla lista consentita venga eliminato.

```
# 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
```

Fase 7: Creare il 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
```

Fase 8: Ottenere l'ID dell'endpoint del firewall

```
FW_ENDPOINT=$(aws network-firewall describe-firewall \
  --firewall-name transform-webapp-firewall \
  --region region \
  --query "FirewallStatus.SyncStates.\"your-az\".Attachment.EndpointId" \
  --output text)
echo "Firewall endpoint: $FW_ENDPOINT"
```

Fase 9: Configurazione della tabella di routing della sottorete del firewall

Instrada il traffico collegato a Internet dalla sottorete del firewall al gateway 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
```

Passaggio 10: Aggiornare la tabella di routing della sottorete privata

Indirizza tutto il traffico diretto a Internet dalla sottorete privata attraverso il firewall.

```
aws ec2 create-route \  
  --route-table-id private-subnet-route-table-id \  
  --destination-cidr-block 0.0.0.0/0 \  
  --vpc-endpoint-id $FW_ENDPOINT \  
  --region region
```

Se esiste già una route predefinita, usa invece di. `replace-route create-route`

Fase 11: Aggiungere il percorso di ritorno simmetrico (obbligatorio)

Important

Questo passaggio è fondamentale. Network Firewall utilizza l'ispezione TLS SNI e deve vedere entrambe le direzioni di una connessione TCP. Aggiungi una route nella tabella di routing della sottorete NAT Gateway che invia il traffico di ritorno destinato alla sottorete privata attraverso il firewall.

```
aws ec2 create-route \  
  --route-table-id $PUB_RTB \  
  --destination-cidr-block private-subnet-cidr \  
  --vpc-endpoint-id $FW_ENDPOINT \  
  --region region
```

private-subnet-cidr Sostituiscilo con il blocco CIDR della tua sottorete privata (ad esempio,).
`10.0.144.0/20`

Senza un routing simmetrico, il firewall vede solo una direzione del traffico. Il motore di ispezione TLS non è in grado di estrarre l'indicazione del nome del server (SNI) dall'handshake TLS e tutte le regole basate sul dominio falliranno automaticamente.

Passaggio 12: rimuovere la route predefinita IPv6 (se presente)

Se la tabella di routing di sottorete privata ha una route predefinita IPv6 (`:::/0`) che punta direttamente a un gateway Internet, ignorerà il firewall per quanto riguarda le destinazioni. IPv6-capable Rimuovilo:


```
aws ec2 delete-route \  
  --route-table-id private-subnet-route-table-id \  
  --destination-ipv6-cidr-block ::/0 \  
  --region region
```

Verifica

Da un'istanza nella sottorete privata, verificate la configurazione:

```
# 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)
```

Risoluzione dei problemi

Le chiamate API a `api.transform` sono bloccate dal firewall

Il dominio `api.transform.region.on.aws` dovrebbe trasformarsi in un indirizzo IP privato tramite l'endpoint VPC e non dovrebbe raggiungere il firewall Internet.

- Verifica di aver creato l'endpoint `com.amazonaws.region.api.transform`
- Verifica che il DNS privato sia abilitato sull'endpoint:

```
aws ec2 describe-vpc-endpoints \  
  --filters "Name=service-name,Values=com.amazonaws.region.api.transform" \  
  --query 'VpcEndpoints[*].[State,PrivateDnsEnabled]' \  
  --output table
```

Output previsto: `available` | `True`

L'applicazione Web non viene caricata (timeout della connessione)

- Verifica che la tabella di routing della sottorete privata abbia una `0.0.0.0/0` route che punta all'endpoint del firewall.
- Verifica che la tabella di routing della sottorete del firewall abbia una `0.0.0.0/0` route che punta al gateway NAT.
- Verifica che il gateway NAT sia in uno stato `available`

Non-allowlisted i domini non sono bloccati

- Verifica la presenza di un `::/0` percorso IPv6 che punti al gateway Internet. Questo aggira il firewall. Rimuovilo (passaggio 12).
- Verifica che il routing simmetrico sia configurato. La tabella di routing della sottorete NAT Gateway deve avere una route di ritorno attraverso il firewall per la sottorete privata CIDR (Fase 11).
- Verifica che la politica del firewall utilizzi `STRICT_ORDER` con `drop_established` e `alert_established` come azioni predefinite.

Considerazioni sui costi

Risorsa	Costo approssimativo
Network Firewall	~\$0. 395/hr (~\$288/month) per zona di disponibilità
Gateway NAT	~\$0. 045/hr (~\$33/month) + spese di elaborazione dei dati
IP elastico (IPv4 pubblico)	~\$0. 005/hr (~\$3. 60/month)
Elaborazione dei dati tramite Network Firewall	\$0. 065/GB
Elaborazione dati NAT Gateway	\$0. 045/GB

Il costo base stimato è di circa \$ 325/month per una singola implementazione in una zona di disponibilità. Per le implementazioni di produzione, implementa il firewall, il gateway NAT e le sottoreti associate in ogni zona di disponibilità in cui esistono sottoreti private.

Pulizia

Per rimuovere tutte le risorse create da questa guida, esegui i seguenti comandi in ordine inverso. Sostituisci i segnaposto con gli ID delle risorse della tua distribuzione. Puoi trovare questi valori nella Console di AWS gestione o utilizzando `describe` i comandi delle fasi di configurazione.

```
# 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
```

Monitoraggio AWS Trasformazione

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Transform e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per guardare AWS Transform, segnalare quando qualcosa non va e intraprendere azioni automatiche quando appropriato:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. È possibile raccogliere e tenere traccia dei parametri, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).
- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi file di log da istanze Amazon EC2 e altre CloudTrail fonti. CloudWatch I log possono monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la [Amazon CloudWatch Logs User Guide](#).
- Amazon EventBridge può essere utilizzato per automatizzare AWS i tuoi servizi e rispondere automaticamente agli eventi di sistema, come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali operazioni automatizzate intraprendere quando un evento corrisponde a una regola. Per ulteriori informazioni, consulta [Amazon EventBridge User Guide](#).
- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la [Guida per l'utente AWS CloudTrail](#).

Registrazione dei log AWS Trasforma le chiamate API utilizzando AWS CloudTrail

AWS Transform è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in AWS Transform. CloudTrail acquisisce tutte le chiamate API per AWS Transform come eventi. Le chiamate acquisite includono chiamate dalla console AWS Transform e chiamate di codice alle operazioni dell'API AWS Transform. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Transform. AWS Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata a AWS Transform, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

AWS Trasforma le informazioni in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in AWS Transform, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi del tuo Account AWS, inclusi gli eventi di AWS Transform, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un percorso](#)
- [CloudTrail servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Comprensione AWS Trasforma le voci dei file di registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Notifications

AWS Transform fornisce notifiche e-mail per tenerti informato sulle modifiche all'accesso allo spazio di lavoro, sugli aggiornamenti sullo stato dei lavori e sulle richieste di collaboratori in sospeso.

Notifiche via e-mail

Le notifiche e-mail sono abilitate per impostazione predefinita e vengono inviate agli utenti che dispongono di autorizzazioni di sola lettura o superiori per un lavoro. Gli utenti possono modificare le proprie preferenze di notifica. Esistono tre categorie di notifiche e-mail:

- Aggiornamenti sull'accesso all'area di lavoro

Ricevi una notifica quando vieni aggiunto a una nuova area di lavoro e quando il tuo ruolo viene modificato all'interno di un'area di lavoro.

- Email riassuntive giornaliere

Riceverai un'email riassuntiva giornaliera alle 9:00 ora del Pacifico che riassume i lavori in corso se hai lavori attivi con una o più richieste di collaboratori aperte obbligatorie. L'e-mail include una tabella che mostra il nome dell'area di lavoro, il nome del lavoro, lo stato del lavoro, i dettagli della richiesta di collaborazione e le azioni richieste (limitate a 10 righe)

Note

Le e-mail riassuntive giornaliere vengono inviate solo per i lavori che hanno richiesto richieste di collaborazione. Le richieste facoltative dei collaboratori non attivano le e-mail di riepilogo.

- Aggiornamenti sullo stato del lavoro

Ricevi un'email quando un lavoro a cui hai accesso viene completato o fallito.

- Aggiornamenti delle richieste di Collaborator

Ricevi un'email ogni volta che un'attività richiede il tuo input, revisione o approvazione.

Gestione delle notifiche e-mail

È possibile modificare le preferenze di notifica e-mail nell'applicazione Web facendo clic sul pulsante Impostazioni nell'angolo in alto a destra dell'applicazione e scegliendo Impostazioni di notifica.

La pagina delle impostazioni di notifica fornisce i seguenti controlli:

Tipo di notifica	Description	Impostazione predefinita
Aggiornamenti di Workspace Access	Ricevi e-mail quando aggiungi un'area di lavoro o quando il tuo ruolo viene modificato all'interno di un'area di lavoro	Abilitato
Daily Collaborator Request Request	Ricevi un riepilogo giornaliero delle richieste di lavoro aperte da parte di collaboratori in spazi di lavoro accessibili	Abilitato

Tipo di notifica	Description	Impostazione predefinita
Aggiornamenti sul completamento del lavoro	Ricevi e-mail quando un lavoro viene completato o o non va a buon fine	Abilitato
Aggiornamenti delle richieste dei collaboratori	Ricevi e-mail quando è richiesto un input o un'approvazione da parte tua	Disabilitato

Puoi utilizzare un'impostazione generale per abilitare o disabilitare tutte le notifiche o configurare i singoli tipi di notifica separatamente.

Quote per AWS Trasformazione

Il tuo AWS account ha delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota è. Region-specific Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per visualizzare le quote per AWS Transform, apri la console [Service Quotas](#). Nel riquadro di navigazione, scegli AWS servizi e seleziona AWS Trasforma.

Per richiedere un aumento delle quote, consultare [Richiesta di aumento delle quote](#) nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo di [aumento del limite](#).

Il tuo AWS account ha le seguenti quote relative a AWS Transform.

Carico di lavoro	Dimensione	Quota	Regolabile	Description
Platform (Piattaforma)	Spazi di lavoro Regione AWS per ogni account abilitato AWS Transform	100 aree di lavoro per ciascuna supportata Regione AWS	Sì	Il numero massimo di aree di lavoro per account AWS Transform abilitato per Regione AWS
Migrazione a VMware	Numero di server per ogni ondata	Ogni ondata: 150 server	No	Il numero massimo di server in un'ondata
Mainframe	Lavori simultanei per ogni account IAM Identity Center	10 lavori per ogni regione supportata	Sì	Il numero massimo di job mainframe simultanei in un account IAM Identity Center

Carico di lavoro	Dimensione	Quota	Regolabile	Description
	Righe di codice per ogni lavoro	3.000.000 di righe di codice per ogni regione supportata	No	Il numero massimo di righe di codice per ogni processo.
	Analisi delle righe di codice mensili	100.000.000 di righe di codice per ogni regione supportata	Sì	Il numero massimo di righe di codice per l'obiettivo del lavoro Analyze Code in un mese solare
	Generazione di documenti aziendali (righe di codice mensili)	50.000.000 di righe di codice per ogni regione supportata	Sì	Il numero massimo di righe di codice per l'obiettivo di lavoro Business Documentation Generation in un mese solare
	Generazione di documenti tecnici (righe di codice mensili)	50.000.000 di righe di codice per ogni regione supportata	Sì	Il numero massimo di righe di codice per l'obiettivo del lavoro Generazione di documentazione tecnica in un mese solare

Carico di lavoro	Dimensione	Quota	Regolabile	Description
	Trasformazione di righe di codice	10.000.000 di righe di codice per ogni regione supportata	Sì	Il numero massimo di righe di codice trasformate in un mese di calendario
	Scomposizione delle righe di codice mensili	50.000.000 di righe di codice per ogni regione supportata	Sì	Il numero massimo di righe di codice per l'obiettivo del lavoro di decomposizione in un mese solare
	Reforgia righe di codice mensili	50.000.000 di righe di codice per ogni regione supportata	Sì	Il numero massimo di righe di codice per l'obiettivo di lavoro di Reforge in un mese solare
	Righe di codice mensili estratte dalla logica aziendale	50.000.000 di righe di codice per ogni regione supportata	Sì	Il numero massimo di righe di codice per l'obiettivo del lavoro Extracted Business Logic in un mese solare

Carico di lavoro	Dimensione	Quota	Regolabile	Description
.NET	Righe di codice mensili.NET (web e IDE)	1.000.000 di righe di codice per ogni regione supportata	Sì	Il numero massimo di righe di codice dell'applicazione.NET che possono essere trasformate in un mese solare in ogni account IAM Identity Center supportato o Regione AWS
	Lavori.NET simultanei con l'estensione Microsoft Visual Studio per ogni account IAM Identity Center	10 lavori per ogni regione supportata	Sì	Il numero massimo di processi di trasformazione.NET simultanei in ciascuno Regione AWS dei quali è supportato un account IAM Identity Center quando si utilizza l'estensione Microsoft Visual Studio.

Carico di lavoro	Dimensione	Quota	Regolabile	Description
	Lavori web.NET simultanei per ogni account IAM Identity Center	5 lavori per ogni regione supportata	Sì	Il numero massimo di processi di trasformazione.NET simultanei in ciascuno Regione AWS dei quali è supportato un account IAM Identity Center quando si utilizza l'app web AWS Transform.
Trasformazioni personalizzate	Definizioni di trasformazione personalizzate	1.000	Sì	Il numero massimo di definizioni di trasformazione personalizzate
	Dimensione della definizione di trasformazione personalizzata	10 MB	No	La dimensione totale massima di tutti i file inclusi nella definizione di trasformazione, inclusi i riferimenti ai documenti.

Carico di lavoro	Dimensione	Quota	Regolabile	Description
	Richieste di conversazione CLI mensili di trasformazione personalizzata	1.000.000	Sì	Il numero massimo di richieste di conversazione di trasformazione personalizzate effettuate nella CLI consentito in un mese di calendario
Valutazione	Limite di numero di server per ogni valutazione	Ogni valutazione: 30.000 server	No	Il numero massimo di server in un singolo processo di valutazione

Regioni supportate per AWS Transform

Note

Se effettui una richiesta che richiede il recupero AWS Transform di informazioni da una regione opt-in non elencata in questa pagina, AWS Transform puoi effettuare chiamate verso quella regione. Per gestire l'accesso alle Regioni verso cui AWS Transform è possibile effettuare chiamate, vedi. [Sicurezza in AWS Trasformazione](#)

Questo argomento descrive Regioni AWS dove è possibile utilizzare AWS Transform. Per maggiori informazioni in merito Regioni AWS, consulta [Specificare cosa può utilizzare il Regioni AWS tuo account](#) nella Guida Gestione dell'account AWS di riferimento.

I tuoi dati potrebbero essere elaborati in una regione diversa da quella in cui li utilizzi AWS Transform. Per informazioni sull'elaborazione interregionale in AWS Transform, vedere [Cross-region elaborazione](#). Per informazioni su dove vengono archiviati i dati durante l'elaborazione, consulta [Protezione dei dati](#).

Supportata Regioni AWS (abilitato per impostazione predefinita)

È possibile creare AWS Transform aree di lavoro nel modo seguente Regioni AWS. Queste regioni sono abilitate per impostazione predefinita: non è necessario abilitarle prima dell'uso. Per ulteriori informazioni, consulta [Regions that are enabled by default](#).

- Stati Uniti orientali (Virginia settentrionale)
- Europa (Francoforte)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Europa (Londra)
- Asia Pacifico (Seul)
- Canada (Centrale)
- Sud America (San Paolo) - Solo agenti di modernizzazione del mainframe

L'area di lavoro in cui si crea un lavoro determina il tipo Regione AWS di lavoro. Per creare un lavoro in una regione diversa, è necessario utilizzare un'area di lavoro diversa nella regione desiderata.

Per i progetti VMware, la regione dell'area di lavoro viene utilizzata per il rilevamento. Tuttavia, è possibile specificare una regione diversa come destinazione della migrazione. La regione di destinazione è quella in cui vengono ospitati i carichi di lavoro al termine della migrazione. Per ulteriori informazioni sulle Regione AWS considerazioni relative alle migrazioni a VMware, incluso l'elenco delle possibili regioni di destinazione, consulta. [the section called “Regioni target supportate”](#)

AWS supporto per AWS Transform

AWS Transform ti consente di creare e gestire i casi di AWS Support tramite la chat in caso di problemi durante i processi di trasformazione. I tuoi casi vengono automaticamente arricchiti con il contesto lavorativo e inoltrati al team di supporto appropriato. Se sei un cliente attivo di Countdown Premium, il tuo tecnico designato ti contatterà per gestire la risoluzione dei problemi. Scopri di più in [AWS Countdown Premium](#). Altrimenti, il tuo caso verrà esaminato dal team di AWS Transform supporto nella sua coda di assistenza.

Prerequisiti

Prima di poter utilizzare la gestione dei casi di assistenza, devi:

- Un piano di AWS supporto attivo: Business On-Ramp, Enterprise o Enterprise
- Un' AWS Transform applicazione esistente

Abilitazione della gestione dei casi di supporto

1. Apri la AWS Transform console.
2. Nel pannello di navigazione scegli Impostazioni.
3. In Supporto, scegli Enable Support case management.
4. Scegli Save changes (Salva modifiche).

AWS Transform utilizza un ruolo collegato al servizio (SLR) per creare e gestire i casi di supporto per tuo conto. Non sono richieste autorizzazioni IAM aggiuntive.

Creazione di un Support Case

Per creare una richiesta di assistenza, usa l'interfaccia di chat:

1. Chiedi di creare una richiesta di supporto. Ad esempio:
 - «Crea una richiesta di supporto per il mio lavoro di trasformazione fallito»
 - «Ho bisogno di aiuto con gli errori sul lavoro, crea un caso»
2. La chat richiede le informazioni richieste:

- Una breve descrizione del problema
- Una descrizione dettagliata

3. Conferma la creazione del caso quando richiesto.

Il caso viene compilato automaticamente con il contesto del processo di trasformazione, tra cui:

- Job ID e stato
- Metadati Job
- Registri di esecuzione del lavoro (log di lavoro)
- Job plan

Il caso viene assegnato automaticamente in base al tipo di lavoro e alla categoria di problema.

Visualizzazione dei casi di supporto

Per visualizzare i tuoi casi di assistenza, richiedi la chat:

- «Elenca i miei casi di assistenza»
- «Mostrami casi di supporto aperti»
- «Qual è lo stato dei miei casi?»

La chat mostrerà:

- ID del caso
- Subject
- Stato, ad esempio Aperto, In sospeso, Risolto o Chiuso
- Data dell'ultimo aggiornamento
- ID del lavoro associato

Per visualizzare i dettagli di un caso specifico:

- «Mostrami i dettagli del caso [case-id]»
- «Qual è l'ultimo aggiornamento su case [case-id]?»

Aggiungere comunicazioni a un caso

Per aggiungere un messaggio a un caso esistente:

1. Chiedi alla chat: «Aggiungi un messaggio a case [case-id]»
2. Fornisci il tuo messaggio quando richiesto.
3. La chat confermerà che il messaggio è stato aggiunto.

Riceverai notifiche quando AWS Support risponderà al tuo caso.

Risolvere un caso

Per risolvere un caso di assistenza:

1. Chiedi alla chat: «Risolvi il caso [case-id]»
2. Conferma la risoluzione quando richiesto.

Note

Puoi risolvere solo i casi che sono stati risolti da AWS Support.

Disattivazione della gestione dei casi di Support

1. Apri la AWS Transform console.
2. Nel pannello di navigazione scegli Impostazioni.
3. In Supporto, scegli Disable Support case management.
4. Scegli Save changes (Salva modifiche).

Note

La disattivazione della gestione dei casi di Support rimuove l'interfaccia di gestione dei casi basata sulla chat ma non chiude i casi esistenti. Puoi comunque accedere ai tuoi casi tramite il AWS Support Center.

Utilizzo: telemetria

Il plug-in AWS Transform IDE, AWS Transform Agent Skill e AWS Transform Kiro Power raccolgono la telemetria di utilizzo per impostazione predefinita durante l'esecuzione della trasformazione. La telemetria è composta da diversi punti dati, come il nome IDE (ad esempio, VS Code o Kiro), il nome dell'agente AI (ad esempio, Claude Code o OpenAI Codex) e la modalità di esecuzione (locale o remota). Questi dati vengono utilizzati da AWS Transform per dare priorità ai test di compatibilità, nonché alla latenza e all'affidabilità.

Per disabilitare la telemetria, comunica all'agente durante la sessione di chat che non desideri che venga emessa la telemetria. Questo opt-out si applica solo alla sessione di chat corrente e deve essere ripetuto per ogni nuova sessione. Se stai eseguendo direttamente la CLI AWS Transform, imposta la variabile di `ATX_DISABLE_TELEMETRY=true` ambiente.

Dati operativi

Potremmo raccogliere segnali operativi relativi all'utilizzo di AWS Transform, ad esempio le funzionalità utilizzate, i registri degli errori e le metriche basate sul feedback in linguaggio naturale (ad esempio se hai approvato la procedura con un piano di trasformazione o fornito istruzioni per iterare un piano proposto) per fornire il servizio e valutare le prestazioni del servizio.

Log delle modifiche

La tabella seguente descrive le versioni e gli aggiornamenti importanti di AWS Transform.

Data	Titolo	Description	Link
2026-07-16	AWS Transform for Migrations aggiunge un rapporto di riepilogo dell'area di lavoro scaricabile	AWS Transform for Migrations ora consente di generare un rapporto di riepilogo dell'area di lavoro come PDF scaricabile. Il rapporto consolida i dati di tutti i processi di migrazione e nel tuo spazio di lavoro, inclusi lo stato dei lavori, l'avanzamento delle fasi del flusso di lavoro, la pianificazione delle ondate, la migrazione della rete, la configurazione delle landing zone, l'avanzamento del rehost e gli artefatti prodotti.	Download di un rapporto di riepilogo sull'area di lavoro
2026-07-03	AWS Lo strumento Transform Discovery aggiunge il supporto del database Oracle	Lo strumento di rilevamento AWS Transform ora raccoglie metadati Oracle dettagliati direttamente dai database su VMware e server bare Hyper-	Individuazione del database Orac

Data	Titolo	Description	Link
		V metal. Puoi scoprire le istanze Oracle tramite connessioni SQL dirette. Lo strumento raccoglie l'enumerazione di Container Database/ Pluggable Database (CDB/PDB), l'inventario dei componenti e il dimensionamento dei file di dati. Inoltre, acquisisce i flag di topologia per Real Application Clusters (RAC), Data Guard e l'architettura multitenant. Se non hai configurato le credenziali del database, lo strumento torna al rilevamento. OS-level Sono supportate tutte le versioni di Oracle.	

Data	Titolo	Description	Link
2026-06-22	Sud America (San Paolo) Supporto regionale per gli agenti di modernizzazione dei mainframe	AWS Transform for mainframe modernization agent è ora disponibile nella regione del Sud America (San Paolo) (sa-east-1). Aggiunto sa-east-1 alle regioni supportate e alle tabelle di inferenza tra regioni.	Regioni Cross-region supportate, inferenza
22/06/2020	AWS Le migrazioni i Transform for VMware supportano la localizzazione	AWS Le migrazioni di Transform for VMware ora supportano la localizzazione. È possibile modificare la lingua di visualizzazione dell'applicazione Web quando si lavora con i flussi di lavoro di migrazione VMware scegliendo l'icona Impostazioni e selezionando la lingua preferita.	Impostazioni di localizzazione

Data	Titolo	Description	Link
2026-06-18	AWS Transform for Migrations supporta tutte AWS le regioni commerciali come obiettivi di migrazione	AWS Le migrazioni di Transform for VMware supportano tutte le regioni AWS commerciali come obiettivi di migrazione, esclusi il Medio Oriente (Bahrein) e il Medio Oriente (Emirati Arabi Uniti). Un'area di destinazione della migrazione è la AWS regione in cui vengono distribuite le risorse migrate, comprese le zone di destinazione, l'infrastruttura di rete e il rehosting dei server.	Regioni target di migrazione supportate

Data	Titolo	Description	Link
18/06/2020	AWS Transform for Migrations consente di allegare ENI esistenti al modello di lancio	AWS Transform consente di collegare le interfacce di rete elastiche (ENI) esistenti al modello di lancio per la migrazione. AWS Transform mostra tutti gli ENI esistenti presenti nell'account di destinazione e puoi etichettarli in modo che siano disponibili per l'uso tramite la configurazione di avvio al momento dell'avvio delle istanze.	Etichettatura delle risorse ENI per la migrazione
18/06/2020	AWS Transform for Migrations consente di configurare le impostazioni di replica e avvio	AWS Transform consente di configurare le impostazioni di replica e le impostazioni di avvio per la migrazione. È possibile impostare la configurazione per l'account di destinazione o su server di origine specifici.	Impostazioni di replica e avvio

Data	Titolo	Description	Link
2026-06-17	Model-to-model valutazione della migrazione per carichi di lavoro di intelligenza artificiale generativa	AWS Transform offre ora una trasformazione personalizzata per la migrazione da modello a modello. La trasformazione valuta i carichi di lavoro di intelligenza artificiale generativa. Produce un piano di migrazione e per il passaggio da fornitori di terze parti ad Amazon Bedrock. L' AI-powere d agente analizza la tua base di codice per identificare ogni SDK e modello AI in uso. L'agente raccoglie i requisiti di migrazione e tramite domande interattive. Quindi associa i modelli agli equivalenti di Amazon Bedrock con confronti trasparenti dei costi e modifiche al codice pronte per la produzione. Supporta le migrazioni da OpenAI, Google Gemini, l'utilizzo diretto di Anthropic SDK e modelli open	Cosa c'è di nuovo nel post, Trasformazioni personalizzate

Data	Titolo	Description	Link
		source tramite LiteLLM o Ollama. Gestisce integrazioni SDK dirette e modelli integrati nel framework, inclusi CrewAI e livelli di routing multiprovider. LangChain LlamaIndex LangGraph Disponibile senza costi aggiuntivi oltre AWS ai prezzi standard di Transform .	

Data	Titolo	Description	Link
2026-06-16	AWS Transform for mainframe offre un flusso di lavoro di reimmaginazione tracciabile	AWS Transform for mainframe offre ora un'esperienza di reimmaginazione connessa e tracciabile, dalla valutazione alla generazione del codice. Le aziende che utilizzano z/OS COBOL e PL/I carichi di lavoro possono valutare il proprio portafoglio per identificare funzioni aziendali discrete, estrarre regole aziendali, generare requisiti pronti per lo sviluppo e produrre codice nativo del cloud tracciabile in un unico flusso di lavoro connesso. Ogni requisito risale al codice sorgente per una completa verificabilità.	Qual è il nuovo post, Documentazione

Data	Titolo	Description	Link
2026-06-16	AWS Transform ora supporta Amazon FSx for NetApp ONTAP come storage di destinazione (anteprima pubblica)	Ora puoi migrare i carichi di lavoro di storage a blocchi su Amazon FSx for NetApp ONTAP oltre ad Amazon EBS come parte del rehosting dell'elaborazione. AWS Transform replica i dati di storage a blocchi direttamente sui volumi FSx for ONTAP all'interno della stessa ondata di migrazione che gestisce elaborazione e rete.	Cosa c'è di nuovo post, Documentazione

Data	Titolo	Description	Link
2026-06-05	Supporto per la valutazione del TCO di Amazon RDS for SQL Server	Ora puoi stimare i costi durante la migrazione di database SQL Server locali su Amazon RDS for SQL Server. Utilizza la valutazione del AI-powered TCO di AWS Transform per analizzare il tuo ambiente e ottenere consigli ottimali sulle istanze di database. La valutazione supporta le opzioni Bring Your Own Media (BYOM) e License Included (LI) con Database Savings Plans per un risparmio fino al 20%.	Qual è il nuovo post, Documentazione
2026-06-04	AWS Lo strumento Transform Discovery ora è supportato come fonte di input per la migrazione di rete	Ora puoi utilizzar e lo strumento di rilevamento AWS Transform come fonte per la migrazione e di rete insieme a ModelizeIT, abilitando migrazioni di rete ibride per ambienti che eseguono carichi di lavoro VMware e non VMware.	Guida per l'utente

Data	Titolo	Description	Link
2026-05-27	AWS La documentazione personali zzata di Transform aggiunge esempi di competenze e best practice sul lato client	La documentazione sulle competenz e lato client ora include esempi pratici per la conformità con Dockerfile, la sicurezza della migrazione dei database, l'applicazione delle policy Terraform e gli aiutanti di deprecazione delle API, oltre alle migliori pratiche per lo sviluppo e la condivisione delle competenze.	Documentazione
2026-05-22	Nuove funzionalità di valutazione della migrazione degli agenti ora disponibili con Transform AWS	AWS Transform offre ora funzionalità avanzate di valutazione della migrazione, tra cui scenari ipotetici , ipotesi personalizzabili, supporto flessibile dei formati di file e diverse nuove funzionalità di valutazione del costo totale di proprietà (TCO).	Qual è il nuovo post, Documentazione

Data	Titolo	Description	Link
2026-05-20	AWS Transform rileva i VPC esistenti durante la revisione della migrazione di rete	AWS Transform ora rileva i VPC esistenti nell'account di destinazione durante la revisione della migrazione di rete. Puoi vedere i VPC esistenti insieme ai tuoi VPC mappati, identificare i conflitti CIDR e risolverli prima della distribuzione.	Documentazione
2026-05-14	AWS Gli agenti di trasformazione sono ora disponibili in Kiro, Claude, Cursor e Codex	AWS Gli agenti Transform sono ora accessibili tramite Kiro power, i plugin per agenti e il server AWS Transform MCP, permettendo agli sviluppatori di utilizzare le funzionalità di trasformazione direttamente dal loro ambiente di sviluppo preferito.	Cos'è il nuovo post

Data	Titolo	Description	Link
2026-05-14	AWS Transform introduce il toolkit Agent Builder per la creazione di agenti di trasformazione personalizzati	I partner e i clienti possono ora creare, condividere e registrare agenti di trasformazione specializzati utilizzando il toolkit Agent Builder Kiro power, che integra strumenti e flussi di lavoro personalizzati con Transform. AWS	Cos'è il nuovo post
2026-05-14	AWS Transform aggiunge un assistent e AI agentic al AWS Toolkit for Visual Studio	Gli sviluppatori.NET possono ora modernizzare le applicazioni attraverso un'esperienza conversazionale guidata passo dopo passo direttamente in Visual Studio, con il contesto completo preservato su IDE e console web.	Cos'è il nuovo post

Data	Titolo	Description	Link
2026-05-14	AWS Transform ora supporta i negozi di manufatti di proprietà dei clienti	Puoi configurare il tuo bucket Amazon S3 e, facoltativamente, crittografare gli artefatti con la tua chiave AWS KMS, dando il pieno controllo su dove vengono archiviati gli artefatti di trasformazione.	Qual è il nuovo post, Guida per l'utente

Data	Titolo	Description	Link
2026-05-14	AWS Transform aggiunge raccomandazioni sulla strategia di migrazione (7R)	Con AWS Transform , ora puoi analizzare l'inventario scoperto e ottenere consigli sulla strategia di migrazione e per ogni server e applicazione. Le raccomandazioni seguono le sette strategie di migrazione e (7R) standard del settore. Ogni raccomandazione include un servizio AWS target consigliato, un punteggio di affidabilità e il motivo alla base. Puoi generare un dashboard HTML interattivo, un PDF o un PowerPoint output Microsoft.	Raccomandazioni 7Rs

Data	Titolo	Description	Link
2026-05-11	AWS Transform aggiunge funzionalità di containerizzazione durante le migrazioni	AWS Transform ora supporta la riplatforming delle applicazioni sui container durante la migrazione e, l'automazione della generazione di Dockerfile, la creazione di immagini dei container con scansione CVE e la distribuzione su Amazon ECS o Amazon EKS.	Qual è il nuovo post , Guida per l'utente
2026-05-01	AWS Transform ora offre agenti di migrazione BI per Power BI e Tableau a Quick	Partner-built gli agenti di Wavicle Data Solutions convertono le dashboard di Power BI e Tableau in risorse Quick all'interno del flusso di lavoro Transform. AWS	Cos'è il nuovo post
2026-04-21	AWS Transform custom è ora disponibile in sei regioni aggiuntive AWS	AWS Transform custom si espande in Asia Pacifico, Canada ed Europa (Londra), raggiungendo un totale di otto AWS regioni.	Qual è il nuovo post

Data	Titolo	Description	Link
2026-04-15	AWS Transform aggiunge la creazione di landing zone all'interno dei flussi di lavoro di migrazione	Aggiunta la creazione di landing zone direttamente all'interno dei flussi di lavoro di migrazione. AWS Transform verifica la presenza di una base esistente, consiglia le strutture delle unità organizzative (OU) e gli account di destinazione e offre un'implementazione completamente automatizzata o i formati di output Infrastructure as Code (IaC) (CloudFormation AWS CDK o Landing Zone Accelerator (LZA)).	Qual è il nuovo post, Documentazione

Data	Titolo	Description	Link
2026-04-15	AWS Transform aggiunge diagrammi e report di pianificazione della migrazione	Ora puoi generare diagrammi interattivi e report analitici durante la pianificazione della migrazione. I tipi di diagrammi includono mappe della topologia di rete, grafici delle dipendenze e delle applicazioni, diagrammi di Gantt a onde e diagrammi generali. I tipi di report includono valutazioni del rischio, raccomandazioni 7R e report analitici personalizzati. Gli output sono disponibili come file HTML, PDF o Microsoft PowerPoint (.pptx) interattivi.	Creazione di diagrammi e rapporti
2026-04-14	AWS Transform è ora disponibile in Kiro e VS Code	AWS Le trasformazioni personalizzate Transform sono ora accessibili da Kiro e VS Code, con lo stato del lavoro condiviso tra le superfici IDE, CLI e console Web.	Qual è il nuovo post

Data	Titolo	Description	Link
2026-04-10	AWS Transform aggiunge DHCP con mappatura dei gruppi di sicurezza per la migrazione di rete	È stato aggiunto il supporto per DHCP con mappatura dei gruppi di sicurezza durante la migrazione di rete. Se disponi di carichi di lavoro di DHCP-enabled migrazione, ora puoi assicurarti che le tue regole di sicurezza rimangano valide dopo la migrazione e. Ciò vale sia per il riferimento ai gruppi di sicurezza in-VPC che per le regole in uscita tra VPC e più account tramite Transit Gateway.	Documentazione
2026-03-31	AWS Transform custom annuncia la disponibilità generale dell'analisi automatizzata del codebase	La trasformazione completa dell'analisi della codebase raggiunge la disponibilità generale, generando documenti sull'architettura, report sui debiti tecnici e consigli di modernizzazione in qualsiasi lingua.	Cos'è il nuovo post

Data	Titolo	Description	Link
2026-03-31	AWS Transform custom introduce nuove trasformazioni gestite per modernizzare il codice su larga scala	Sono state aggiunte sette nuove trasformazioni gestite, tra cui Node.js aggiornamenti (disponibilità generale), ottimizzazione Java, migrazione e Log4j, aggiornamenti Angular e aggiornamenti Angular-to-React Vue (accesso anticipato).	Qual è il nuovo post
2026-03-20	AWS Transform aggiunge API pubbliche per la migrazione di rete	Aggiunte API pubbliche per la migrazione di rete, che consentono ai partner e all'accesso programmatico alle funzionalità di migrazione della rete.	Documentazione di riferimento delle API
14/01/2020	AWS Transform custom aggiunge AWS PrivateLink supporto e si espande in Europa (Francoforte)	AWS Transform custom ora supporta l'accesso privato a VPC AWS PrivateLink ed è disponibile in Europa (Francoforte) oltre che negli Stati Uniti orientali (Virginia settentrionale).	Qual è il nuovo post

Data	Titolo	Description	Link
2025-12-23	AWS Transform consente la conversione della rete per le migrazioni ibride dei data center	AWS Transform for VMware converte automaticamente le configurazioni di rete dei data center ibridi (VLAN, intervalli IP) in AWS VPC, sottoreti e gruppi di sicurezza senza mappatura manuale.	Cos'è il nuovo post
2025-12-01	AWS lancia AWS Transform custom per accelerare la modernizzazione dell'intera organizzazione	AWS Transform custom raggiunge la disponibilità generale, consentendo alle organizzazioni di automatizzare trasformazioni di codice ripetibili su larga scala tramite un singolo comando CLI.	Cos'è il nuovo post
2025-12-01	AWS Transform aggiunge nuove funzionalità di intelligenza artificiale agentica per le migrazioni VMware aziendali	AWS L'agente VMware di Transform può ora scoprire ambienti locali, mappare le dipendenze, generare piani di migrazione ed eseguire la migrazione tra HyperV, Nutanix, KVM e target bare-metal.	Cos'è il nuovo post

Data	Titolo	Description	Link
2025-12-01	AWS Transform lancia un agente AI per la modernizzazione completa di Windows	Un nuovo agente Windows completo automatizza la trasformazione delle app.NET e dei database SQL Server in Aurora PostgreSQL, distribuendoli in contenitori su Amazon ECS o EC2 Linux.	Cos'è il nuovo post
2025-12-01	AWS Transform espande le funzionalità di trasformazione.NET e migliora l'esperienza degli sviluppatori	AWS Transform aggiunge il supporto di.NET 10, il porting ASP.NET Web Forms to Blazor e un'esperienza IDE interattiva avanzata tramite AWS Toolkit for Visual Studio.	Qual è il nuovo post
2025-12-01	AWS Transform for mainframe offre nuove funzionalità di automazione dei test	AWS Transform for mainframe introduce la generazione automatizzata di piani di test, script di raccolta dei dati di test e l'automazione dei test case per accelerare i test di modernizzazione del mainframe.	Cos'è il nuovo post

Data	Titolo	Description	Link
2025-12-01	AWS Transform for mainframe ora supporta la reimmaginazione delle applicazioni	La nuova analisi dei dati e delle attività e le funzionalità di estrazione della logica aziendale consentono o la scomposizione delle applicazioni mainframe legacy in architetture native del cloud.	Cos'è il nuovo post
2025-11-13	AWS Transform automatizza la configurazione di rete Landing Zone Accelerator	AWS Transform for VMware genera automaticamente file YAML di LZA-compatible rete, semplificando la configurazione dell'infrastruttura a cloud multi-account dagli ambienti VMware.	Qual è il nuovo post
2025-07-16	AWS Transform for mainframe introduce funzionalità avanzate di refactoring del codice e di business logic	AWS Transform for mainframe aggiunge la disponibilità generale del refactoring (ristrutturazione del codice) e un'estesa estrazione della logica aziendale a livello di applicazione per migliorare la qualità del codice.	Cos'è il nuovo post

Data	Titolo	Description	Link
2025-05-15	AWS Transform for VMware è ora disponibile a livello generale	AWS Transform for VMware, un servizio di intelligenza artificiale agentica che automatizza l'intero ciclo di vita della modernizzazione di VMware, dalla scoperta all'implementazione, raggiunge la disponibilità generale.	Cos'è il nuovo post
2025-05-15	AWS Transform for mainframe è ora disponibile a livello generale	AWS Transform for mainframe, il primo servizio di intelligenza artificiale agentica per modernizzare z/OS le applicazioni IBM su larga scala, raggiunge la disponibilità generale con nuove funzionalità di analisi, scomposizione e gestione dei lavori.	Cos'è il nuovo post

[Scarica questi dati.](#)

Cronologia dei documenti per AWS Guida per l'utente di Transform

La tabella seguente descrive la cronologia dei documenti per la AWS Transform User Guide.

Modifica	Descrizione	Data
Modernizzazione continua, analisi e correzione del portafoglio.	È stato aggiunto un nuovo capitolo che documenta la funzionalità di modernizzazione continua AWS Transform (atx ctsottocomandi) per l'analisi e la correzione automatizzate del codice. Vedi la modernizzazione continua.	3 giugno 2026
Rete Brownfield: visibilità dei VPC esistenti	È stato aggiunto il rilevamento VPC esistente durante la revisione della migrazione di rete. AWS Transform rileva automaticamente i VPC già distribuiti nell'account di destinazione e segnala i conflitti CIDR con i VPC mappati. Vedi i VPC esistenti nel tuo account di destinazione.	18 maggio 2026
Sono stati aggiunti il formato delle competenze, le competenze lato client e i registri dei subagenti per Transform custom AWS	Le definizioni di trasformazione ora utilizzano il formato delle competenze (SKILL.mdcon frontespizio YAML e cartella opzionale). references/ Sono state aggiunte competenze lato client per estendere l'agente	11 maggio 2026

con funzionalità aggiuntive e registri dei subagenti per migliorare il debug. Richiede la versione CLI 2.0 o successiva. Vedi [Definizioni e Client-Side competenze di trasformazione](#).

[Aggiunta la containerizzazione del codice sorgente](#)

AWS Transform ora può containerizzare le tue applicazioni utilizzando l'intelligenza artificiale generativa. Fornisci il codice sorgente da repository Git o caricamenti zip e AWS Transform lo analizza, genera artefatti Docker, pubblica immagini dei container su Amazon ECR, genera l'infrastruttura come codice e la distribuisce su Amazon Elastic Container Service o Amazon Elastic Kubernetes Service. Vedi [Containerizzazione del codice sorgente](#).

7 maggio 2026

[Aggiunte operazioni di ottimizzazione della rete e consigli guidati](#)

Fase 5 aggiunta: revisione e ottimizzazione della rete, con operazioni su VPC e sottorete (eliminazione, esclusione, unione, divisione, ridimensionamento, ridenominazione, modifica dell'indirizzo IP) e consigli guidati per la standardizzazione dei nomi, la revisione dell'ambito, il corretto dimensionamento della capacità, la revisione della sicurezza e il consolidamento del VPC. [Vedi Revisione](#) e ottimizzazione della rete.

27 aprile 2026

[AWS Transform custom è disponibile in 6 nuove regioni](#)

[È stato aggiunto il supporto per ca-central-1, eu-west-2, ap-northeast-1, ap-northeast-2, ap-southeast-2 e ap-southeast-2 in Transform custom.AWS](#)

21 aprile 2026

[Documentazione aggiornata sulle autorizzazioni dei connettori](#)

È stata aggiunta una suddivisione dettagliata delle autorizzazioni per il Account AWS connettore di destinazione, che copre S3, MGN, le autorizzazioni di Migration Hub, la migrazione del carico di lavoro e il provisioning dell'infrastruttura delle landing zone. Vedi [Connect target Account AWS s.](#)

19 aprile 2026

[Tipi di job di migrazione VMware aggiornati](#)

Sono stati aggiunti i tipi di job Discovery and Migration Planning, Landing zone e Landing zone, rete e migrazione dei server. Migrazione di rete rinominata solo in Network Migration e Migration planning to Build migration plan. Vedi i tipi di job di [migrazione a VMware](#).

19 aprile 2026

[Oggetti Restructured Connects Account AWS](#)

Ha ristrutturato la configurazione del connettore in tre fasi: selezione del tipo di migrazione, accordo MAP e configurazione del connettore, incluse le aree di destinazione supportate, i ruoli degli account, le linee guida per gli amministratori delegati e i ruoli IAM. Vedi [Connect target Account AWS](#).

19 aprile 2026

[Sono state aggiunte altre aree target dedicate esclusivamente alla migrazione dei server](#)

Sono state documentate 14 aree commerciali aggiuntive e disponibili per i lavori di migrazione dei server senza migrazione di rete, con obbligo di lista consentita fino al terzo trimestre 2026. [Vedi Regioni target supportate](#).

19 aprile 2026

Aggiunto il capitolo Migrate servers	È stato aggiunto un nuovo capitolo sui server Migrate che copre l'intero flusso di lavoro di rehosting, tra cui la struttura degli account, i ruoli IAM, la configurazione dell'amministratore delegato, l'implementazione dell'agente di replica, il test e il cutover.	19 aprile 2026
Aggiunto il capitolo Costruisci landing zone	È stato aggiunto il nuovo capitolo Build landing zone con dettagli sulle autorizzazioni dei connettori per il provisioning delle zone di atterraggio.	19 aprile 2026
Mappatura e referenziazione dei gruppi di sicurezza	Sono state aggiunte strategie di mappatura dei gruppi di sicurezza (MAP, MAP_DHCP, SKIP) e documentazione di riferimento ai gruppi di sicurezza per Migrate network.	13 aprile 2026
Auto-conversion per tipi di file di rete non supportati	È stato aggiunto il supporto per la conversione automatica di tipi di file di configurazione di rete non supportati in Migrate network.	6 aprile 2026
Aggiunta la politica chiave KMS per la migrazione del database	È stata aggiunta la sezione Crittografia per la migrazione del database .	26 marzo 2026
Nuova AWS politica gestita documentata	DBModProvisioningAndMigration Sezione aggiunta.	24 marzo 2026

Nuova AWS politica gestita documentata	DBModDiscoveryAndAssessment Sezione aggiunta.	24 marzo 2026
Generazione di diagrammi di rete	Aggiunta la generazione opzionale di diagrammi di rete (formati Mermaid e PNG) a Migrate network.	18 marzo 2026
Supporto per firewall e file di configurazione SDN	È stato aggiunto il supporto per i file di configurazione Palo Alto Networks, Fortinet FortiGate e Cisco ACI per la migrazione di rete in Migrate network.	11 febbraio 2026
Etichettatura personalizzata per le risorse di rete	È stato aggiunto il supporto di tagging VPC-level personalizzato e a livello di processo per la migrazione di rete in Migrate network.	28 gennaio 2026
Documentazione di supporto aggiunta	È stato aggiunto AWS il supporto per la sezione.	23 dicembre 2025
Nuove AWS politiche gestite documentate	AWSTransformCustomFullAccessAWSTransformCustomManageTransformations Sezioni AWSTransformCustomExecuteTransformations aggiunte e.	7 dicembre 2025
Migrazione a VMware	È stata aggiornata la sezione sulla migrazione a VMware.	1 dicembre 2025

Politica AWS gestita aggiornata	È stata aggiornata la AWSServiceRoleForAWSTransform documentazione per riflettere le autorizzazioni aggiunte.	1 dicembre 2025
Regioni supportate	È stato aggiornato l'argomento Regioni supportate .	1° dicembre 2025
Modernizzazione del mainframe	È stata aggiornata la sezione sulla modernizzazione del mainframe .	1 dicembre 2025
Iniziare	È stato aggiornato l'argomento Guida introduttiva .	1 dicembre 2025
Full-stack Modernizzazione di Windows	È stato aggiunto l'argomento sulla modernizzazione di Full-stack Windows , che include la sezione.NET aggiornata e la nuova sezione sulla modernizzazione di SQL Server .	1 dicembre 2025
Strumento di scoperta	È stata aggiunta la sezione degli strumenti Discovery .	1 dicembre 2025
Politica AWS gestita aggiornata	Aggiornamento AWSTransformApplicationECSEmploymentPolicy con autorizzazioni estese di ispezione dei ruoli IAM, creazione di ruoli collegati ai servizi ECS e autorizzazioni KMS per il supporto della crittografia ECR.	22 novembre 2025

Politica AWS gestita aggiornata	Aggiornamento AWSTransformApplicationDeploymentPolicy con autorizzazioni aggiuntive per il networking EC2, l'ispezione dei ruoli IAM, la gestione dei bucket S3 e le autorizzazioni di crittografia KMS.	22 novembre 2025
Collezionista Discovery	È stato aggiunto lo strumento di scoperta AWS Transform> documentazione .	31 ottobre 2025
Aggiunto diagramma dell'architettura di migrazione VMware	È stato aggiunto un diagramma dell'architettura di migrazione VMware in Migrate network .	23 ottobre 2025
Aggiornamento dei risultati della migrazione a VMware	Informazioni aggiornate sui risultati della migrazione in Migrate network.	12 ottobre 2025
Aggiornamento dei risultati della migrazione a VMware	Informazioni aggiornate sui risultati della migrazione in Migrate network.	12 ottobre 2025
Documentazione del connettore S3	Aggiunta la documentazione del connettore S3 per l'app web.NET.	8 ottobre 2025
Argomento sui nuovi connettori utente	Argomento sui connettori utente aggiunto.	21 settembre 2025
Politica AWS gestita aggiornata	È stata aggiornata la AWSServiceRoleForAWSTransform documentazione.	17 settembre 2025

Supporto per la valutazione dello storage	Aggiunto il supporto dei file NetApp Data Infrastructure Insights (DII) per le valutazioni dello storage .	2 settembre 2025
Aggiornamento delle regioni target	Aggiunte tre regioni target supportate .	31 agosto 2025
Aggiornamento della policy gestita	Sono state aggiunte le autorizzazioni di sola lettura di IAM Identity Center da utilizzare. AWSServiceRoleForAWSTransform	29 agosto 2025
Nuova AWS politica gestita documentata	AWSTransformApplicationDeploymentPolicy Sezione aggiunta.	28 agosto 2025
endpoint dell'interfaccia	È stato aggiunto l'argomento relativo agli endpoint dell'interfaccia .	9 luglio 2025
Versione iniziale	Versione iniziale della AWS Transform User Guide.	15 maggio 2025

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.